NRENs CLOUD ARCHITECTURE FRAMEWORK (NRENs-CAF): ENHANCING CLOUD CONNECTIVITY AMONG NATIONAL RESEARCH EDUCATION NETWORKs IN SADC

A DISSERTATION SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY IN SCIENCE

(COMPUTER SCIENCE)

OF

THE UNIVERSITY OF NAMIBIA

BY

NALINA SURESH

200639501

MARCH 2016

Main Supervisor: Prof. Jameson Mbale (Copperbelt University)

Co-supervisor: Prof. Alfredo Terzoli (Rhodes University)

ABSTRACT

The development of Science, Technology and Innovation (STI) infrastructure and distribution of Information Communication Technologies (ICTs) to all components of societies are of significant importance to leverage a faster socio-economic development in Africa. The continuous technological changes have influenced service delivery in various sectors. The emergence of new technologies within the education sector has prompted for a review of the way research is conducted among NRENs. Developed countries NRENs were adopting Cloud computing technology, which had been consequently motivating the research in developed countries on related technologies by both the industry and the academia. These new technologies assist in accessing information and have the power to transform the teaching, learning and research paradigm.

The flexibility of pay-as-you-go combined with an on-demand scalable model is changing the NREN computing and driving them to adopt Cloud technology. Notwithstanding its benefits, the transition to this computing paradigm raised serious security concerns, which were the subject of several studies. The new concepts that Cloud computing introduced, such as multi-tenancy, resource sharing, Virtualization and outsourcing, created new challenges for the security community. Other challenges playing a major role in slowing down and impacting its acceptance included poor resources such as internet connectivity, lack of technologies, lack of human resources, funding and economic reasons. Although security concerns form the biggest challenge,

problems associated with availability, performance, cost, interoperability and regulatory issues come very close to security issues as the perceived set of challenges associated with Cloud adoption.

This study took an in-depth look at the current state of SADC NRENs and found that little had been explored in developing countries particularly in SADC region. Alternatively, there was no clear strategy, guidelines nor reference architecture/framework to enhance Cloud computing within NRENs in SADC. Furthermore, it was found that lack of political support for Cloud initiatives, stringent regulations (for instance on data crossing the borders), issues with Service Level Agreements (SLAs) and security infrastructure to mention a few were the factors hindering the adoption of Cloud technology by NRENs.

A survey study in the form of an exploratory quantitative research design was used. On the other hand, a descriptive non-experimental quantitative approach was chosen and a survey was conducted through the use of questionnaires. This was supported by document review on current emerging Cloud techniques. Close to fifty (50) participants from Eight (8) SADC NREN member countries that formed their NRENs was engaged in this study. There is no doubt that NRENS in the region are not effectively utilizing Cloud based technology. However, this study proposed some modern Cloud based approaches that could be adopted. Further, an explanation on how NRENs could be consolidated on a common Cloud platform was also provided.

The research sample size of fifty (50) participants from Eight (8) SADC countries, who have formed their NRENs were engaged. The data was analyzed using SPSS version 21 (Statistical Packages for the Social Sciences). A p value <0.05 was considered as statistically significant. Data analysis was initiated with a check of the outliers, missing data and normality through correlation values that could affect relations between variables.

In view of the above, NRENs Cloud Architecture Framework, which in this study is abbreviated as NRENs-CAF, was conceived to design a Cloud based architecture framework for NRENs in SADC region. An overview of existing NRENs in both developed and developing country was reviewed. The main objective of this study was to design an NRENs-CAF that would envision the transition of every NREN into Cloud based system and make them interoperable with each other. The study also aimed to harness Cloud technology in such a way that it facilitated research in tertiary institutions and enhance the collaboration among SADC NRENs. The NRENs-CAF intended to design a framework with new components to support Cloud connectivity and service delivery. Overall, the NRENs-CAF was proposed to build and deliver highly interconnected and high performance networks for Universities and other Educational and Research Institutions more specifically among SADC that enable them to share educational resources and collaborate within and globally.

TABLE OF CONTENTS

ABSTRACT ii

TABLE OF CONTENTS v

LIST OF TABLES x

LIST OF FIGURES xi

LIST OF ACRONYMS xiii

ACKNOWLEDGEMENT xv

DEDICATION xvii

DECLARATION xviii

LIST OF PUBLICATIONS xix

CHAPTER 1: INTRODUCTION 1

1.1 Background 1

1.2 Orientation of the Study 2

1.3 Statement of Problem 8

1.4 Research Questions 9

1.5 Significance of the Study 10

1.6 Limitations of the Study 10

1.7 Research Methodology 11

1.8 Definition of Terms 11

1.9 Outline of Thesis 13

1.10 Summary 15

CHAPTER 2: LITERATURE REVIEW 16

2.1 Introduction 16

2.2 Developed Countries' in Perspective of NRENs 19

2.3 NRENs in Developing Countries 37

2.4 Cloud Adoption and Initiatives in Africa 52

2.5 Challenges of Cloud Computing in Perspective of Developing Countries 56

2.6 Critical Analysis of Literature Review 60

2.7 Cloud Standardisation Overview 64

2.8 Related work/Existing Framework 68

2.9 Summary 70

CHAPTER 3: RESEARCH METHODOLOGY 71

3.1 Introduction 71

3.2 Research Purpose 74

3.3 Research Approach 75

3.4 Research Strategy 75

3.5 Research Design 76

3.6 Population 77

3.7 Sample 78

3.8 Research Instruments 78

3.9 Procedure 78

3.10 Data Analysis 79

3.11 Reliability and Validity 80

3.12 Research Ethics 81
3.13 Conclusion 82
3.14 Summary 82
CHAPTER 4: RESEARCH FINDINGS 83
4.1 Introduction 83
4.2 Data Structure 84
4.3 Summary 105
CHAPTER 5: DATA ANALYSIS AND DISCUSSION 106
5.1 Statistical Inferences (Correlation of variables) 106
5.2 Discussions 111
5.2.1 Resources 111
5.2.1.1 Cloud Deployment and Service Delivery Models 113
5.2.1.2 Reasons and Steps for NRENs to Adopt Cloud 113
5.2.1.3 Benefits and Purpose that NRENs Use Cloud Computing 114
5.2.2 Challenges faced by SADC NRENs in adapting Cloud Computing 114
5.2.3 Architecture 117
5.3 Summary 119
CHAPTER 6: PROPOSED NRENs CLOUD ARCHITECTURE FRAMEWORK (NRENs-CAF) FOR SADC NRENs 120
6.1 NRENs-CAF Architecture 122
6.1.1 Main Architectural Components 127

6.1.2 Supporting Architectural Components 127
6.1.1.1 Cloud Services Model (CSM) 127
6.1.1.2 Cloud Control and Management Plane (CCMP) 137
6.1.1.3 Cloud Federation System (CFS) 142
6.1.1.4 Cloud Operation Framework (COF) 147
6.1.1.5 Trusted Cloud Security Framework (TCSF) 149
6.1.2.1 E-Scientific or Enterprise Collaborative Cloud Infrastructure (ECI) ... 153
6.1.2.2 Virtual Resources (VRs) 154
6.1.2.3 Inter Cloud Infrastructure (ICI) 155
6.1.2.4 Resource Provider 156
6.1.2.5 Campus Network/NRENs 156
6.1.2.6 Cloud IaaS and PaaS Provider 157
6.2 Summary 157
CHAPTER 7: CONCLUSIONS AND RECOMMENDATIONS 158
7.1 CONCLUSION 158
7.1.1 Research Question One: “What were the resources that could be used to establish Cloud architecture in the SADC NRENs?” 158
7.1.2 Research Question Two: “What Cloud service architecture was suitable for interconnection among NRENs in the SADC region?” 159
7.1.3 Research Question Three: “What were the challenges faced by SADC NRENs with regards to establishing Cloud services?” 160
7.2 RECOMMENDATIONS 160

7.2.1 Cross Border Regulations 160

7.3 FUTURE RESEARCH 161

7.4 Summary 161

REFERENCES..... 162

APPENDIX A - RESEARCH QUESTIONAIRE 180

APPENDIX B - AAA VULNERABILITIES 184

APPENDIX C - Confidentiality, Integrity and Availability (Triad C.I.A: Security Reference Model) 185

APPENDIX D - Open Research Challenges 189

GLOSSARY..... 194

LIST OF TABLES

Table 2.1: List of Government Initiatives of Cloud Computing in African Continent (Maaref, 2013) 53

Table 4.1: Statistics by respondents 84

Table 5.1: Correlation between Virtualization and Security 106

Table 5.2: Correlation Between Virtualization and Availability 108

Table 5.3: Correlation Between Standardisation and Interoperability 109

Table 5.4: Correlation Between Virtualization and Collaboration 110

Table 5.5: Summary of Challenges faced by SADC NRENs in adapting Cloud computing Technology 151

LIST OF FIGURES

Figure 3.1: Summary of Research Methodology 73

Figure 4.1: Occupational Position 85

Figure 4.2: NREN Population 86

Figure 4.3: NREN on Cloud 87

Figure 4.4: IT Infrastructure/Technologies 88

Figure 4.5: NRENs Willingness 89

Figure 4.6: Functioning of the NRENs 90

Figure 4.7: NRENs Collaboration 91

Figure 4.8: Cloud Models 91

Figure 4.9: Cloud Service Models 92

Figure 4.10: Reasons for NRENs not on Cloud 93

Figure 4.11a: Steps to be taken by NRENs to Adopt Cloud Computing 94

Figure 4.11b: Factors to be taken by NRENs to Adopt Cloud Computing 95

Figure 4.12a: Benefits of Cloud Services in NREN 96

Figure 4.12b: Purpose of Cloud Services in NREN 97

Figure 4.13: CSP Security 98

Figure 4.14: Security Concerns 98

Figure 4.15: Type of Security Measures 99

Figure 4.16: Scalability 100

Figure 4.17: Network Scalable Architecture 101

Figure 4.18: Governance Issues 102

Figure 4.19: Interoperability Issues 103

Figure 4.20: Challenges 104

Figure 5.1: Virtualization versus Security 107

Figure 5.2: Virtualization versus Availability 108

Figure 5.3: Standardisation versus Interoperability 109

Figure 5.4: Correlation Comparing Virtualization and Collaboration 110

Figure 5.5: Challenges faced by SADC NRENs in adapting Cloud Computing 115

Figure 6.1: NRENs-CAF Cloud Operation Framework 126

Figure 6.2: Reference CSM Architectural Model and its Protocol Stack (adapted from (GEANT3 Project), (NIST SP 500-292. Cloud Computing Reference Architecture), (ITU-T JCA-Cloud activity), (GEYSERS project: Demchenko, Y., et al., 2012)) 129

Figure 6.3: CCMP Architectural Model (adapted from GEYSERS project: Demchenko, Y., et al., 2013) 139

Figure 6.4: : CFS Architectural Model (adapted from GEYSERS project: Makkes, M. X., et al., 2013) 144

Figure 6.5: TCSF Architectural Model (adapted from (Cloud Security Alliance reference model (CSA)), (Common Security Services Interface (CSSI)), (GEYSERS project: Ngo, C., et al., 2012)) 151

LIST OF ACRONYMS

CAF: Cloud Architecture Framework.

CCMP: Cloud Control and Management Plane.

CDMI: Cloud Data Management Interface.

CE: Cloud Environment.

CFS: Cloud Federation System.

CIA: Confidentially, Integrity and Availability.

COF: Cloud Operation Framework.

CSA: Cloud Security Association.

CSM: Cloud Services Model.

CSP: Cloud Service Provider.

ETSI: European Telecommunications Standards Institute.

FedIDP: Federated Identity Provider.

GÉANT: Gigabit European Academic Network Technology.

GW: Gateway.

HPC: High Performance Computing.

IaaS: Infrastructure as a Service.

ICT: Information Communication Technology.

IEEE: Institute of Electrical and Electronics Engineer.

IETF: Internet Engineering Task Force.

IP: Internet Protocol.

IT: Information Technology.

ITU: International Telecommunication Union.

IX: Internet Exchange.

LAN: Local Area Network.

NIST: National Institute of Standards and Technology.

NREN: National Research and Education Network.

OGSA: Open Grid Services Architecture

OX: Optical Exchange.

PaaS: Platform as a Service.

PoP: Point of Presence.

QoS: Quality of Services.

SaaS: Software as a Service.

SADC: Southern African Development Community.

SLA: Service Level Agreement.

SSO: Single-Sign-On.

TCSF: Trusted Cloud Security Framework.

TERENA: Trans European Research and Education Networking Association.

TTP: Trust Third Party.

VM: Virtual Machine.

VPN: Virtual Private Network.

VR: Virtual Resource.

WACS: West African Cable System

XML: Extensible Markup Language.

ACKNOWLEDGEMENT

I am very grateful to my supervisor Professor Jameson Mbale for his continued support, direction and never ending encouragement during the entire period of my PhD work. It has been a great honour and opportunity to have been able to study under his supervision and expertise and I have really learnt a lot from him.

I would also like to acknowledge and express my sincere gratitude to my co-supervisor Prof. Alfredo Terzoli and the Associate Dean of School of Computing Dr. Kauna Mufeti for their continuous support and encouragement.

I would also like to acknowledge my appreciation and gratitude to all my colleagues of School of Computing (UNAM) for their help and support provided during my study, directly or indirectly.

Further, I would also like to acknowledge the Post Graduate Students for their encouragement and inspiration for working as a team and motivating each other during this challenging time to complete the programme.

Additionally, I would like to express my deep and enduring gratitude to my family (from my family and my husband's family) and friends. Special thanks go to my late parents, my in-laws, my beloved husband Kaggere. S. Suresh and our loved daughter Bindiya. K. Suresh for their endless support, encouragement and understanding.

I would also like to acknowledge and express my sincere gratitude to our family friend Deepak. A. N for providing a great assistance.

Lastly, I am also very thankful to everyone else who gave me any assistance in one way or another.

DEDICATION

This report is dedicated to God Almighty.

DECLARATION

I, Nalina Suresh, declare hereby that this study **"NRENs CLOUD ARCHITECTURE FRAMEWORK (NRENs-CAF): ENHANCING CLOUD CONNECTIVITY AMONG NATIONAL RESEARCH EDUCATION NETWORKs IN SADC"** is a true reflection of my own research, and that this work or part thereof has not been submitted for a degree in any other institution of higher education.

……. [Signature] Date……..

LIST OF PUBLICATIONS

Suresh, N., Mbale, J. (2015). *NRENs Cloud Infrastructure Framework (NRENs-CLIF): Case study of SADC region*. 7th Annual conference of UbuntuNet Alliance, Lusaka, Zambia: UbuntuNet connect, *NUANCE*.

Suresh, N., Mbale, J., Terzoli, A., & Mufeti, T. K. (2015). Enhancing Cloud Connectivity among NRENs in the SADC region through a Novel Institution Cloud Infrastructure Framework (ICIF). *International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, 179-184, doi: 10.1109/ETNCC.2015.7184830.

CHAPTER 1: INTRODUCTION

The chapter provided an overview of the research topic, statement of the problem(s), research questions, significance of the study, scope, limitations, research methodology and summary of the findings. It further presented the outline of the rest of chapters in the dissertation.

1.1 Background

The evolution of Cloud computing for Information Technology (IT) or computational resources provisioning had led to a significant shift in the IT industry. This shift prompted interest from different organisations, institutions and users to take its advantages. Hence, in this study, NRENs Cloud Architecture Framework was introduced and abbreviated as NRENs-CAF. This model is a proposed conceptual architectural theoretical framework which aided the transition of non-Cloud based SADC NRENs into Cloud system. As a result made them interoperable with each other in the way IT services are designed and managed efficiently.

According to Vaquero, Rodero, Merino, Caceres, and Lindner (2008), Clouds are a large pool of easily usable and accessible virtualized resources such as hardware, software, development platforms, communication, network and/or services through the Internet from anywhere, anytime and using any internet enabled device. In addition, they described that these resources were dynamically reconfigured to adjust to a variable load (scalability), and also to allow for optimum resource utilization. They added that pool of

resources was typically exploited by a pay-per-use model in which guarantees were offered by the infrastructure provider by means of customized Service Level Agreements (SLAs). Further, they stated that "Cloud computing was itself a Virtualization of resources and Cloud users could use software, platform, infrastructure, communication and network as a service without knowing where these resources were being managed and their location". They emphasized that Virtualization was a key component of the recent influx of new Cloud computing technologies in the market and was the key to optimizing the resources. Therefore, NRENs-CAF can adopt Cloud technology to leverage resource(s) sharing among the NRENs irrespective of their location.

1.2 Orientation of the Study

Over the past few years, Cloud computing had been a popular phrase in the Information Communication Technology (ICT) industry in Africa. In recent times, it had become one of the most talked about technologies and it had received a lot of attention. IT development, implementation and usage had always been propounding major challenges to organisations, from the perspective of both cost and resource sharing. According to Mell and Grance (2011), Cloud computing is a new paradigm of computing which had emerged as one of the advanced technologies. Cloud computing allowed the IT world to use computing resources effectively and efficiently.

According to Iyengar, Jeyanthi and Shabeeb (2011), users of the Cloud had unlimited computing power at their disposal when they needed it and they could access all their IT

resources anytime and anywhere with any Internet-enabled device. In addition, Rizzo (2013) stated that Cloud computing technology had generated considerable hype in Africa and had become an integral part of the educational organisations. Further, the ITU (2012) report highlighted that the Cloud computing technology was already either in use by many African countries or in the course of being implemented. This confirmed the trend towards development of the Cloud computing in SADC.

The ATICS Report (2006) described Internet connectivity in Southern Africa using three characteristics namely too little, too expensive and poorly managed. The report further stated that the lack of IT resources had proven to be a bottleneck for resource sharing among academic institutions worldwide. In view of the above report, Twinomugisha (2007) further described that high cost of connectivity was one of the factors hampering the learning institutions in their pursuit of resource sharing. In support of these reports, SADC was not an exception.

According to Aluoch (2006), connectivity in Africa was poor, unreliable, scarce and very expensive, and where available, was almost never dedicated and users had to contend with frequent service outages conflated with very slow speeds. The author also revealed the result of the 2006 African Tertiary Institutions Connectivity Survey (ATICS) which indicated that Universities in Africa, on an average pay about forty US Dollars and fifty cents ($40.50) per kilobits per second (kbps) per month while some institutions pay thirty-six US Dollars ($36) per kilobits per second (kbps) for bandwidth. They also pointed out that these figures are very high compared to users in North

America who are on megabit and Gigabit speeds and pay much less, that is ten US Dollars ($10) per month for three megabits per second (3Mbps) for Digital Subscribers Line (DSL) link. In support of the above, cost for bandwidth is still high in the SADC region hence Cloud computing is more cost effective.

The NUENCE Report (2008) gave a summary of bandwidth against costs in Africa as on an average of one million two hundred and fifty thousand US Dollars ($1.25m) per month for seven hundred and seventy megabits per second (770Mbps) shared among one hundred and sixty-three (163) institutions. Mbale (2009) stated that "there was a high demand for the use of approximately an average of five Gigabits per second (5Gb/s) amount of data communication in learning institutions in Sub-Saharan Africa". From these statistical figures, Mbale, Kauna, and Victor (2013) stated that the demand and acquisition of an exorbitant budget pose a challenge to the SADC institutions in addition to the scarcity of resources.

Karanja G. (2006) recommended the formation of a consortium to purchase bandwidth as an obvious initiative for the immediate future. This had proven to be a successful strategy, by negotiating bulk discounts. This association has lowered the price paid by some African Higher Education Institutions (HEIs) for their bandwidth from as much as fifty thousand US Dollars ($15,000) per Mbps per month to two thousand three hundred and thirty US Dollars ($2,330).

Furthermore, Mbale et al. (2013) stated that the concept of the consortium was established to mitigate cost and connectivity challenges. Some examples of these

African consortia were: the Partnership for Higher Education in Africa, involving eight (8) Universities; HEIs in Western and Central Africa comprising of hundred (100) institutions; and the initiatives for the formation of National Research Education Networks (NRENs). Mbale (2009) described these NRENs as consortium within the designated architectures for bargaining the resources and share it at more affordable price. Several NRENs such as Zambia Research Education Network (ZAMREN), Tertiary Education Network of South Africa (TENET), Tanzania Research Education Network (TERNET), Malawi Research Education Network (MAREN) and Namibian NREN (XNet), to mention a few, were established in SADC (Mbale, 2009).

Mbale (2014) further, stated that the above mentioned organisations could pool their resources together in a way that would exploit technologies such as Cloud computing. He further noted that until recent, very little effort had been made in developing countries with regard to the utilization of Cloud computing. In support of the above, besides the limited information available pertaining to the NRENs' environments, it is evident that, so far, there was no dedicated research on Cloud computing issues and challenges in SADC, and particularly in Namibian NREN environments. According to the data from the World Bank Report by Gallagher (2012), out of one billion people in Africa, over 740 million people use Internet. In view of the above, the challenges in SADC could be best solved by a proposed integrative architecture framework linking the various NRENs over the unified Cloud. Therefore, this highlighted the need for NRENs-CAF framework.

The International Telecommunication Union Report (ITU, 2012), stated that the situation in Africa was characterized by relatively favourable network infrastructure development with constantly improving international connectivity. The report also highlighted that where connectivity to the international telecommunication network was concerned, several international cables made landfall on each side of the continent, favouring the growth of telephone and Internet traffic and the emergence of an ever-increasing number of shared data processing centres. Moreover increasing the physical proximity between Cloud computing resources and the end user will produce immediate savings in bandwidth budgets while accelerating access to Cloud computing resources (ITU, 2012). In support of the above, the demand for connectivity across Africa, and for that matter SADC, remains a non-trivial problem which compels the NRENs to move towards Cloud computing technology. Further, the adoption of Cloud framework in SADC could also benefit the different member countries through the use of common data processing centers.

According to Weber (2011), one of the most frequently cited reasons offered by organisations for adopting Cloud services was access computing resources on a pay-as-you-go basis. He added that this was achieved without the need for any major investment in IT infrastructure and skills. Weber also gave an example citing small and medium scale organisations that did not have the financial power to invest in ICT infrastructure but took advantage of the numerous services that Cloud computing offered.

Kuyoro, Ibikunle, and Awodele (2011) pointed out that security issues in Cloud computing had played a major role in slowing down its acceptance. In addition, Mbale et al. (2013) stated that security was ranked first as the primary challenge of Cloud computing. Also, Mircea and Andreescu (2010) observed that despite the proliferation of Cloud computing, there were concerns about the security and data protection risks. Therefore, this study aims at addressing security and data protection concerns in Cloud- based systems for the benefits of SADC NRENs.

Gabriella et al. (2013) stated that interoperability issues were considerable barriers and challenges to be overcome in order to achieve Cloud infrastructure. The authors also stated that the proliferation of lack of standards and interoperability reduced the potential benefits of Cloud services. Similarly, this study adopted the best practices of Cloud technologies standards to facilitate the seamless sharing and exchange of data between heterogeneous technologies within and among SADC NRENs.

Apart from standards and interoperability challenges, cross-border issues also posed threats. Szegedi (2011) emphasized that standardisation policies were a challenge for cross-border connectivity. Gabriella et al. (2013) confirmed that the most relevant cross-border initiatives of Cloud services were necessary to ensure the adoption and effectiveness of Cloud computing in NRENs. Henceforth, NRENs-CAF ensured the adoption of standardised policies to facilitate cross-border issues.

In summary, NRENs-CAF enhanced Cloud connectivity among NREN networks in SADC region by improving communication, collaboration, reduced bandwidth and IT

infrastructure costs. Other major challenges that confronted Cloud computing were security, interoperability, standardisation, legal and compliance issues. The rationale for such a framework was to motivate SADC NRENs to embrace Cloud based solution. Hence, the study was carried out on the existing NRENs and their initiatives, design and experiences were used as a reference model in designing the NRENs-CAF.

1.3 Statement of Problem

Katz, Goldstein, and Yanosky (2009) stated that many NRENs in the developed countries were joining Cloud-based services to stay organized and connected. Whilst Thorsteinsson, Page, and Niculescu (2010) emphasized that Cloud-based solutions were effective in supporting collaborative and cooperative learning. However, this was not the case with developing countries in the SADC region (Mbale, 2012). For instance, Tertiary Education Network of South Africa (TENET), Zambia Research Education Network (ZAMREN), Tanzania Research Education Network (TERNET) and Xnet Development Alliance Trust (Xnet) of Namibia, all had isolated infrastructure outside the boundaries of their respective countries. In addition, Mbale (2012) stated that until recently there had been no indication that any efforts were being made by the SADC NRENs towards embracing the new Cloud computing technology.

In support of the above, there are no Cloud computing reference architecture frameworks for SADC NRENs. Other critical issues that were observed included the existing NRENs' IT infrastructures being operated in isolation. There are also no indications made by the concerned countries towards embracing Cloud computing

technologies. Other problems emanating to this effect included no dedicated Cloud computing research or initiatives among SADC NRENs. Furthermore, the absence of research collaboration hindered the exchange of viable educational material among members. As evident above, the lack of strategic guidelines to address compliance issues on cross- border connectivity and lack of reference architectural framework among SADC NRENs restricts the adoption of Cloud computing technologies among the members.

Overall, this study introduced NRENs-CAF, which assessed the prevailing status of SADC NRENs on legacy technologies. It further determined the best possible approaches to transforming the traditional IT infrastructures into Cloud based framework. The study investigated the adoption of Cloud technologies using NRENs-CAF to initiate research collaboration among the members.

1.4 Research Questions

The study herein answered the following questions:

1.4.1 How can the SADC NRENs resources be utilized to establish Cloud architecture framework to facilitate research collaboration?

1.4.1.1 What are the resources that can be used to establish Cloud architecture framework in the SADC NRENs?

1.4.1.2 What are the challenges faced by SADC NRENs with regards to establishing Cloud-based services?

1.4.1.3 What Cloud service architecture is suitable for interconnection of NRENs in the SADC region?

1.5 Significance of the Study

The study was to determine the resources which would be used to establish Cloud architecture framework for SADC NRENs. Moreover, NRENs-CAF was developed as a platform for integrating these NRENs through the Cloud. Furthermore, the research addressed the security, interoperability and governance challenges in the establishment of Cloud services. Insights from the study have the potential to help the ICT policy makers to utilize this framework.

1.6 Limitations of the Study

Due to the nature of the research topic and other constraints in terms of logistics, the researcher limited the study to NRENs on the SADC region. This was compounded by geographical proximity of the NRENs. The main challenge for the study was the reluctance of the organisations to share confidential information with the researcher. In addition, there was limited literature in SADC in this area of study. There were also challenges with conducting focus group discussions due to the distances between the different NRENs.

1.7 Research Methodology

A survey study in the form of an exploratory quantitative research design was used. On the other hand, a descriptive non-experimental quantitative approach was chosen and a survey was conducted through the use of questionnaires. A structured questionnaire was used to collect data regarding the existing NRENs in SADC region to explore their initiatives and challenges faced in moving towards Cloud computing technology. Hence, for purposes of this study, a survey (online survey) strategy was used since the research tried to design a theoretical architectural framework from the reference models for the development of Clouds among SADC NRENs. A purposive sampling technique was used to select the participants from the SADC NRENs population. Descriptive statistical methods were used, and the relationship between variables were established and analysed to identify the resources required and challenges faced to design a Cloud architectural framework. The data were analysed using Statistical Program for Social Scientists (SPSS) and the results were presented graphically.

1.8 Definition of Terms

The following terms were frequently used in the study.

Cloud Computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that could be rapidly provisioned and released with minimal management effort or service provider interaction (Glenn et al., 2009).

Community Clouds: The Cloud infrastructure which is shared by several organisations (Glenn et al., 2009).

Confidentiality: Not all data owned by the company should be made available to the public (Greene, 2005).

Hybrid Clouds: An environment consisting of internal or external providers where an organisation may run non-core applications in a public Cloud while maintaining core applications and sensitive data in-house in a private Cloud (Glenn et al., 2009).

Infrastructure as a Service (IaaS): The Cloud model that provided infrastructure components to clients. Components included virtual machines, storage, networks, firewall, load balance, and so on (Glenn et al., 2009).

Interoperability: The issue under Governance Domains in Cloud computing that discusses the movement of data from one provider to another or bringing it back to the enterprise (Mather, Kumaraswamy and Latif, 2009).

Integrity: Protecting data from being tampered with by an unauthorized source (Greene, 2005).

Platform as a Service (PaaS): The Cloud model that delivered a pre-built application platform to the client or organisation (Glenn et al., 2009).

Public Clouds: The Cloud infrastructure available to the general public (Mather et al., 2009).

Private Clouds: The Cloud infrastructure available solely for a single organisation, also called as Internal Cloud (Velte et al., 2009).

Software as a Service (SaaS): The Cloud model that provided ready online software solutions (Glenn et al., 2009).

Service-Level Agreement (SLA): Part of a service contract, where the level of service was formally defined (Mather et al., 2009).

Virtualization: The creation of a virtual environment that supported the creation and maintenance of the virtual operating system, storage devices, applications, or network resources (Mather et al., 2009).

Virtual Machine (VM): A server emulating real hardware for an unmodified guest operating system (Velte et al., 2009).

1.9 Outline of Thesis

CHAPTER 1: INTRODUCTION

The chapter focuses on the orientation of the study, the problem statement, the research questions, significance of the study, limitations of the study, and a brief summary of the methodology used. This chapter introduces the opportunity for Cloud Computing to facilitate research collaboration among NRENs in SADC and the need to better understand how Cloud infrastructure can be used to address resource challenges.

CHAPTER 2: LITERATURE REVIEW

The chapter deals with the review of related work by providing a comprehensive theoretical knowledge of existing SADC NRENs on Cloud and identifies gaps in that context. Furthermore, it will support the contextualising of the NRENs-CAF framework.

CHAPTER 3: RESEARCH METHODOLOGY

The chapter presents the approach and research methodology used in the study that includes the research approach, research strategy, research design, sampling, data collection, data analysis, validity and reliability, ethical considerations and conclusion.

CHAPTER 4: RESEARCH FINDINGS

The chapter presents the analysis of data that is collected by means of questionnaires. It includes the presentation of results and findings in graphical form. The validity and reliability of the results are also discussed.

CHAPTER 5: DATA ANALYSIS AND DISCUSSION

The chapter discusses the research findings of the data analysis in relation to the research questions posed in the thesis and links them with literature review where applicable.

CHAPTER 6: PROPOSED NRENs CLOUD ARCHITECTURE FRAMEWORK (NRENs-CAF) FOR SADC NRENs

The chapter discusses and presents the proposed conceptualized theoretical architectural framework model named Institutional Cloud Infrastructure Framework (NRENs-CAF) for SADC NRENs.

CHAPTER 7: CONCLUSIONS AND RECOMMENDATIONS

The Chapter provides recommendations depending on the findings of the study and further provides recommendations on the legal framework, Data center, standards, Interoperability and security. Furthermore, the study suggests future research on the global connection of NRENs-CAF to international gateway or networks.

1.10 Summary

This chapter introduces the opportunity for Cloud Computing to facilitate research collaboration by NRENs in SADC and the need to better understand how Cloud infrastructure can be used to address resource challenges. Furthermore Research Questions and Objectives of the research are identified.

In chapter two, the literature review will be discussed in relation to the current knowledge available that is relevant to the study aim, and research questions of this thesis.

CHAPTER 2: LITERATURE REVIEW

The chapter presented the review of related work in relevance to the study. Primary (research articles, dissertations, reports, policies) and secondary sources (text books, articles) were used to derive the related work of the study. Firstly, the chapter introduced the different NREN's and then discussed their Cloud initiatives. These included the description of NREN's, the current Cloud architecture models used, their security benefits and risks, their interoperability and the governance issues involved in few developed and developing countries, in particular, SADC NREN's.

2.1 Introduction

The literature review presented the current knowledge available that is relevant to the study aim and research questions outlined in chapter one. The chapter introduced a review of the different available NREN models and a summary. Further, this chapter deliberated on the different descriptions of Cloud computing technology and its services and then discussed trends, benefits and challenges of NRENs-CAF in SADC NRENs environment. A collection of primary and secondary literature resources were used to obtain relevant facts and background information on different aspects of NRENs-CAF that relates to the study.

Echezona and Ugwuany (2010) discussed the University's roles as research, evaluation, information transfer, and technology development are therefore critical to social progress and economic growth. Therefore, University strategic planning should pay

special attention to the challenge of accessing current scientific knowledge at an affordable cost. They further stated that many initiatives have taken place to get Africa interconnected to the "information superhighway". They also pointed out that NGOs, telecommunication companies, philanthropic organisations and some countries of the developed world have extended their services to ICT development in Africa. Echezona and Ugwuany (2010) narrated that the partnership for higher education in Africa has helped an organisation of thirteen (13) African Universities to cover connecting costs. They also emphasized that some African countries through their Universities had made appreciable efforts, individually and collaboratively, at establishing affordable ICT links which invariably improves Internet connectivity.

Further, they went on to say most of the initiatives have been realized through the formation of National Research and Education Networks (NRENs), and Regional Research and Education networks. Their financial positions have limited their activities to the acquisition of Very Small Aperture Terminal (VSAT) at an affordable price through the economies of scale offered by consortium formation (Echezona and Ugwuany, 2010). Hence, NRENs-CAF facilitates the SADC NRENs to avail Cloud services on this common architecture that enhances collaboration and connectivity for resource sharing at an affordable price.

In today's highly competitive environments, organisations are looking for ways and means to operate efficiently so as to cut cost and maximize profit. A new paradigm Cloud computing, emerged to change the old ways of computing. Cloud computing,

which emerged as one of the enabling technologies, allowed the IT world to use computer resource effectively and more efficiently at reduced IT cost (Mell and Grance, 2009). This meant that users of the Cloud had the luxury of unlimited computing power at their disposal when they needed it. Weber (2011) specified that the demand for connectivity across Africa was driving the development of sophisticated systems to boost performance and facilitate mobility which was both key priorities for consumers.

Furthermore, Weber (2011) declared that although Cloud computing had gained much importance and presents an attractive proposition for the organisation, necessary precautions and stringent care must be taken to ensure that confidentiality, integrity and availability of information are not compromised in the Cloud environment. Cloud computing provides opportunities for upcoming African entrepreneurs who could invest in acquiring servers as well as data storage computers to provide Cloud services (Weber, 2011). In support of the above, the NRENs could take advantage of the numerous services that Cloud computing offered to gain the competitive edge for improved collaboration and resource sharing.

According to Sultan (2010) governments and non-governmental organisations were wagering that Cloud-based technology could help transform their economies and societies, which translated into improvements in education, public health, and the environment. It sounded great, but making the Cloud work in Africa and for that matter SADC remained a non-trivial problem because of the challenges that existed. However, these very challenges made Africa an increasingly attractive region for Cloud

computing, especially for mobile applications. Moreover, Sultan (2010) explained that apart from the general issues that confronted Cloud computing such as security and legal, there existed numerous challenges distinct to the African market that needed to be addressed to realize the potential of Cloud computing. Due to the above reasons, it was important to incorporate NRENs-CAF as a model to embrace Cloud computing among SADC NRENs.

2.2 Developed Countries' in Perspective of NRENs

There are a number of NRENs in developed countries and different technologies were used to inter connect members in order to collaborate and share resources. The different NRENs include:

2.2.1 Greek Research Educational Network (GRNET)

According to Koukis (2012), Greek Research Educational Network (GRNET) provided innovative networking and computational services to the Greek Research and Education (GRE) community, as well as supporting the development of ICT. He identified three (3) important reasons for investing in Cloud services namely legacy, community needs and paving the way for the Public Sectors.

Firstly, in terms of legacy, Koukis (2012) stated that involvement with computational services was not something new for GRNET. In addition to its well-established role as the NREN, GRNET also operated the country's National Grid Initiative (NGI) providing computational infrastructure to its member institutes using Infrastructure-as-a-

Service (IaaS) platform. Further, the above author emphasized that Cloud initiatives may be considered as a logical extension to its core business. Initially, GRNET deployed Software-as-a-Service (SaaS) platform in which end users deployed services by configuring only the parameters related to their institutions Koukis (2012). Secondly, in reference to community needs, Koukis (2012) stated that the phenomenon of understaffed Network Operation Centres (NOCs) in many institutions or departments was common which raised the poor quality of services and support. Thirdly, in view of paving the way for the public sector, Koukis (2012) stated that a potential beneficiary of this initiative may be to the Greek Public Sector. Therefore, GRNET was developing an open source IaaS platform that integrated into their existing Data Centre and offered Virtualization capabilities. He said it was expected that the transfer of physical machines to virtual ones would save tremendous amounts of investment in future, which was the highest priority of the Greek Government.

Similarly, NRENs-CAF may face the similar challenges as GRNET in terms of legacy and disparate systems in the various institutions as well as the non-existence of cooperative framework for NRENs in SADC. Henceforth, NRENs-CAF would conduct strategic evaluations of each service delivery models, namely: SaaS, PaaS and IaaS (SPI), CaaS, NaaS and XaaS (anything) as a service in view of the challenges in SADC NRENs before choosing them. Hence, NRENs-CAF proposed a theoretical Cloud architectural framework that would enable these NRENs to benefit from Cloud connectivity services.

According to Wind (2011), the GRNET was implemented through the initiative called "Okeanos project" by the whole Greek research and academic community. Wind (2011), further stated that the goal of that project was to deliver a production quality IaaS and to offer virtual computing resources at a pay-per-use fee. In addition, he identified that the software powering Okeanos was available via an open source license. Concurrently, Wind (2011) described that the Okeanos offers its user's access to Virtual Machines, Virtual Ethernets, Virtual Disks, and Virtual Firewalls through a simple web-based Graphical User Interface (GUI). He further explained that Okeanos was conceived to offer its users easy and secure access to GRNET's data centers by focusing on user friendliness and simplicity while being able to scale up to the thousands of Virtual Machines, users, and terabytes of storage.

Furthermore, Wind (2011) indicated that the Okeanos system was currently in alpha testing phase and not yet a production system. In the same way, this study provided integrated Cloud architecture framework for SADC NRENs by interoperating with non-Cloud IT infrastructure to enhance connectivity and collaboration enabling its members to access Cloud computing resources and services. In addition, NRENs-CAF explored open source platform aligned within the Triad C.I.A. which is "Confidentiality," "Integrity" and "Availability" a service security objectives model (see Appendix C). Bendandi (2010) also stated that there was a strong need to improve security practices and many Cloud customers would buy Cloud computing services on the basis of the reputation for confidentiality, integrity and the level of resilience of the security services offered by a provider.

In support of GRNET, NRENs-CAF suggested an architectural component that ensures tangible secure access and data security. Furthermore, it recommended the adaptation of scalable infrastructure networks' architecture with dynamic elasticity and scalability properties which monitors a customer's infrastructure and scales it on-demand so that Cloud services could be elastically provisioned.

2.2.2 Netherlands Research Educational Network (SURFnet)

According to Van der Pol and Dijkstra (2013), Netherlands Research Educational Network which was founded by SURF foundation called as SURFnet had embraced Cloud computing. They further stated that online collaboration was not just within individual institutions but also between them, which gave value added for higher education and collaborative research. Similarly, NRENs-CAF would embrace Cloud computing technology to enhance collaboration within and among SADC NRENs.

Van der Pol and Dijkstra (2013) also described that the initiative of SURFnet was done in two phases. In phase one, SURFnet undertook a number of internal organisational changes in their existing procurement policies. They added that a new vendor management team was created to negotiate with Cloud vendors and to maintain the relationship with these third parties on behalf of the whole SURFnet community.

Additionally, in phase two, the first set of 'experiments' and small-scale deployments were started using commercial Cloud service providers. Van der Pol and Dijkstra (2013) added that organisations of higher education moved to the Cloud together, via SURF.

They further explained that in SURFnet all generic IT services in higher education and research were provided by Public Cloud as much as possible, but when the required services were not available in the public Cloud, or when they could not be used due to legal considerations, community Cloud services would be used. Further, the authors said users should be able to decide which devices and applications they used and depending on this, they would be able to choose between multiple Cloud vendors and services provided with an excellent infrastructure, which interconnected these services.

In the same way, this study provided architectural framework defining specific initiatives that consolidated SADC NRENs and enhanced Cloud connectivity among them. Therefore, NRENs-CAF suggested a Community Cloud deployment model, which would allow shared Cloud services among SADC NREN members. This architecture not only supported these specific organisations but also offered managed hosted services. This implied that NRENs-CAF would manage the architecture by providing few controls such as security, integrity and availability.

With reference to SURFnet, Van der Pol and Dijkstra (2013) stated that Hybrid Cloud architecture had been a way to take advantage of the benefits of computing resources. However, there were challenges like how to integrate with Cloud environments and maintain control over security and performance. Nevertheless, NRENs-CAF would have a customized Service Level Agreement (SLA) between the consumer that is between SADC NRENs and Cloud Service Provider (CSP). This SLA incorporated security controls and their scope, service level agreement; privacy or confidentiality,

interoperability issues, compliance mandates and audit will be well-defined and were to be dealt with legally in contracts. In support of this, Kuyoro et al. (2011) also discussed the well-known security issues such as data loss, phishing and botnets running remotely in a collection of machines, and posed serious threats to organisation's data and software. They also discussed other challenges such as costing models, SLA's deciding what to migrate and Cloud interoperability issues.

Consequently, NRENs-CAF recommends architectural component named Trusted Cloud Security Framework (TCSF) as shown in Figure 6.1, where security component was integrated into the design that allowed secure access, which is not as with traditional infrastructure. TCSF will provide a basis for all secure operations among the components in NRENs-CAF architecture. As a result, a comprehensive TCSF can simplify and strengthen the security of networks, data and applications that can help mitigate security risks and compliance.

Further, Ngo, Demchenko, and de Laat (2012) added that the Common Security Services Interface (CSSI) should be defined and also facilitated for dynamically provisioning the virtualized security services. Also, NRENs-CAF was designed to operate under the supervision of the community or representatives which acted as a policy authority for security and operational practices. In this case, NRENs-CAF provides a clearinghouse service for SLA and policies.

2.2.3 Malaysian Research and Education Network (MYREN)

According to Luo, Lin, Chen, Yang, and Chen (2011), the Malaysian Research and Education Network (MYREN) was a Government-funded program which provided a dedicated high-speed network for it's eighty-eight (88) members across Malaysia. The author further stated that members of MYREN included tertiary institutes, polytechnics, community colleges, research entities and scientific laboratories to share resources within a high-capacity broadband network. Moreover, the author stated that MYREN provided extensive communication among its members and with other Research Educational Networks (RENs). Further, the author identified that MYREN Cloud implemented Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), Infrastructure -as-a-Service (IaaS) and an MYREN-Cloud portal to connect its member institutions to Cloud. Similarly, NRENs-CAF forms a standardized consortium of SADC NRENs facilitating Cloud services over the closed network. A Cloud Services model (CSM) framework for inter-cloud infrastructure was incorporated into NRENs-CAF with regard to the choice of Cloud service delivery models over this community Cloud as shown in Figure 6.1.

Liu, Tong, Mao, Bohn, Messina, Badger, and Leaf (2011) explained the existing scenario of MYREN stating that current offering included only basic SaaS services through servers running on open source platform, and MYREN Cloud was planning to deploy Compute-as-a-service (CaaS) for future releases. The author further observed that security issues in MYREN still needed to be addressed for reliable operation.

On the contrary, NRENs-CAF proposed to deploy XaaS delivery model mainly focusing on SPI, CaaS, NaaS and with incorporating of a Cloud Security Framework (TCSF) that evaluates the eight (8) main security requirements, namely: Identification, Authentication, Authorization, Audit (AAA) services, Confidentiality, Integrity, Non-repudiation, and Availability. The TCSF was based on a per Cloud service delivery and deployment model in line with the one of best practices from ISO/IEC 27002 and CSA 2010. The former discussed the mapping of Cloud model to the AAA controls, whereas the latter discussed comparing security controls to a compliance framework.

According to Szegedi (2011), MYREN stored data on servers that were located in Malaysia in their private Cloud. He further added that a major plus point advantage for using MYREN Cloud is that researchers were often concerned with safeguarding their intellectual property and would have preferred having their material located inside the country borders. The author further pointed out that there was no guarantee that data was better protected internally comparing to public Cloud.

However, NRENs-CAF would address the above challenges by recommending the need for a clear list of compliance requirements before considering Cloud service providers. Hence, the organisations have the flexibility and control over choosing the compliance regulations that best suites to their data exchange and security requirements. NRENs-CAF further provided recommendations on cross-border issues associated with data exchange including variations in data protection regulations. These recommendations

included best practices in the line of the work being done by ITU's Standardization Sector in the field of Cloud computing.

2.2.4 Trans-European Research and Education Networking Association (TERENA)

According to Szegedi (2013), the Trans-European Research and Education Networking Association (TERENA) was established in Amsterdam, Netherlands. The author further described that the TERENA adopted best practices and fostered collaborations among NRENs on data storage, data management, and data security. He defined the pilot project as a software platform which offered the ability to easily connect both private and public Cloud providing storage capabilities and services to the participating NRENs. In addition, the author identified that the primary aim of that pilot project was to explore possible deployment scenarios for a trusted storage service tailored for research and education community. He concluded that TERENA pilot was a success and up running Cloud model. The author further stated that from this architecture, TERENA could be considered as a distributed storage middleware platform installed at the edges of the client domains, preserving storage service reliability or trust within the domain. Further, he described that this type of trusted Cloud had storage service diversification through availability, reliability and SLA variations tailored to the organisational needs.

Yasinsac and Irvine (2013) described trustworthy systems as those that performed as expected even under typical conditions, such as, operational errors, human interaction or hostile disruption. Further, they argued that the difference between trustworthy systems

and the classical security perspective was that the latter worked towards advancing the organisational mission using security discovery. They further stated that trust-based systems balance security with other activities in order to ensure the continuity of an organisation and achievement of the objectives. That implied trustworthiness was related to reliability, which referred to system performance. Chow, Golle, Jakobsson, Shi, Staddon, Masuoka, and Molina (2009) described that there will be the potential lack of control and transparency when a third party held the data, which required a high level of trust on the part of a customer towards a service provider.

Hence, NRENs-CAF adopted an integrative security framework TCSF to assess security challenges and it also aimed to mitigate risks of network security, intellectual property, securing access and data transmission. Similar to TERENA it incorporated the middleware platform between SADC NRENs and the Cloud. In addition, NRENs-CAF embraced well-defined SLA's with respect to architecture, security, governance and interoperability tailored to tackle the data security issues towards the goal of more secure, reliable and trustworthy Cloud environments.

2.2.5 National Research and Education Network (JANET) in the UK

According to Carminati (2001), National Research and Education Network in the United Kingdom (UK) known as JANET, was connected to continental network GEANT which is the umbrella organisation for European research networks. The author further described that JANET had high performance and it was a well-managed backbone link developed by Association of African Universities (AAU) under UbuntuNet Alliance

which was one of the largest research and education networks. GEANT utilized high speed, capacity infrastructures and provided advanced services. In addition, he said that JANET was a nationally funded system and it focused more towards national high priority funded research rather than education, collaborating with the European Union (EU) Research Networks which were specifically working on high priority large-scale research projects for the UK. On the contrary, NRENs-CAF may not be funded nationally, but could be supported by the various SADC NREN member countries with an emphasis on education and research collaborations amongst those institutions in the region. Salmon (2009) further stated that JANET had created additional fibre optic access systems that brought together all research institutions as well as information clusters within the UK. He said it connected them to a very high-speed optics fibre connection, which also provided grid computing service of Gbps data transfer between grid systems.

According to Zaipuna, (2008), most SADC countries had a very good national fibre infrastructure. He further stated that since the submarine cable "West African Cable System" (WACS) connectivity landed in few African countries, it was easier for NRENs to connect other nations outside their borders. Further, terrestrial fibre networks could connect member institutions to the last-mile distribution of the fibre network to its member Routers (Zaipuna, 2008).

Therefore, NRENs-CAF could take advantage of the existing WACS, the new submarine cable infrastructure and regional fibre optics backbone networks that connect

SADC NRENs platform to the international gateway. This data communication network infrastructure would facilitate last-mile connectivity thus, enhancing Cloud connectivity services and resource sharing.

Salmon (2009) further stated that JANET had created dedicated security response teams which handled any kind of security threats or risks pertaining to that system. He continued that a number of different security and authentication approaches had been developed to allow similar mitigation. Moreover, he added that JANET used multi secure service that was Single Sign-On (SSO) authentication mechanism across Universities, Cloud, and applications.

In view of the above, NRENs-CAF proposed Computer Security Incident Response Team (CSIRT) placed within Network Operations Center (NOC). This would enhance monitoring and analyzing of network health to detect security incidents and employ similar authentication approaches to allow its members to easily gain network access to other member sites through that security scheme. In support of this, Tripathi and Mishra (2011) stated that it was complex to manage and create multi-level authentication mechanisms for several services. They indicated that SSO techniques addressed these issues.

Salmon (2009) further explained that JANET was working with the pilot framework to bring convergence among NRENs under European Union Science and Research Council (EPSRC) centers along with industrial connectivity. He further stated that JANET was looking forward to creating bandwidth on demand service and made it into public

service creating EU NRENs secured, standard and infrastructure intensive capable platform better than commercial network available in the UK. He added that JANET was presently dealing more with end-to-end security of applications, confidential data reliability and performance issue.

Similarly, NRENs-CAF converged the SADC NRENs on a standard infrastructure forming a consortium to serve Cloud connectivity among them and for industrial research collaboration. Further in support of the JANET, NRENs-CAF proposed to adopt similar initiatives with a vision of becoming a private Cloud service provider. In future, NRENs-CAF may switch to become a commercialized provider for sustainability purposes. Further, since the ITU standardization sector worked towards telecom standards for Clouds, NRENs-CAF adopted these recommendations to become a private Cloud provider.

2.2.6 Australian Research Educational Network (AARNET)

According to Korporaal (2009), Australian AARNET network was built on a framework which was similar to ARPANET research network, which eventually became the Internet. The author further stated that AARNET modeled directly to match ARPANET specifications initially. He further added that this network was built with minimal government funds but directly funded by University and was the main NREN in Australia. He further described that AARNET created a set of member organisations formed by its own NREN community. In addition, he stated that AARNET was a private University network created by consortia of Universities and it was not available

to industry or public, but it had absolute control with respect to that University consortium. Moreover, he reported that AARNET was moving towards creating high-speed optical fibre backbone connectivity interconnect networks, mostly built to collaborate with the Indian AIRNET and Chinese networks. Basically, these countries dominate the traffic starting from hundred (100) Gbps to eight (8) Tbps of this network due to the size and number of educational institutions in that region.

Korporaal (2009) further described that AARNET currently aimed for a stronger interactive network with NRENs in New Zealand, North Korea, India, China, Singapore and the northern part of Asia. Furthermore, he explained that AARNET had a slightly different application targeting research in a specific area completely with different applications such as big data, astronomical space application, biological systems like genetics, marine sciences and terrestrial ecological systems. He stated basically that AARNET provided video conferencing capabilities for healthcare institutions in the country and managed by University consortium. He further mentioned that AARNET had also created a virtual private network between Universities.

Similar to AARNET, NRENs-CAF formed a consortium among SADC NRENs and expanded collaboration between specific groups of researchers, academics and other scholars. Hence, NRENs-CAF suggested an E-Scientific or Enterprise Collaborative Cloud Infrastructure (ECI) as shown in Figure 6.1, which would be accessible only within that group enabling scientific and unique applications resource sharing. Moreover, the NRENs-CAF aggregated On-demand Cloud services on Inter Cloud

Infrastructure (ICI) via the internet access from all its users. Further, more bandwidth for the same amount of money spent by the institutions would be achieved by taking advantage of the new submarine cable, WACS, and regional fibre optic networks as the backbone infrastructure. This would favour the growth of telephone and Internet traffic and the emergence of an ever-increasing number of shared data processing centres. Moreover increasing the physical proximity between Cloud computing resources and the end user will produce immediate savings in bandwidth budgets while accelerating access to Cloud computing resources (ITU, 2012).

Korporaal (2009) further stated that AARNET was a world class National Research and Education Network which had transformed life in Australian Universities and revolutionised the ability of scientists and researchers to operate in Australia and still be part of the world community. He continued that AARNET had transformed itself from an organisation using commercial capacity to provide services to its members. On behalf of its members, AARNET has actively collaborated with infrastructure owners and ISPs in every state and internationally to secure the last mile access.

According to Aarnet (2015) report, AARNET was an active member of the global community of National Research & Education Networks (NRENs) that supported collaborative, cutting-edge, data-intensive research and education. In addition, the report highlighted that this “network of networks” connected members included Universities, research organisations, schools, vocational training providers, health and cultural

organisations among its member states such as Australia Darwin, Brisbane, Sydney, Canberra, Adelaide, Hobart, Fiji to mention few.

Fell (2014) stated that AARNET4 was the replacement of AARNET for new applications and services for its customers that provide faster and cheaper networking. The author further added AARNET4 built out the underlying optical transmission network to support up to eighty (80) channels each of hundred (100) Gbps. Additionally, it interconnected the various inter capital legs which allowed more dynamic redundancy and provisioned Cloud services & applications. He further stated Cloud services leveraged the network's capabilities and included a range of innovative solutions for data storage and sharing, video conferencing, unified communications and roaming. Moreover, AARNET4 collaborated with its global research network partners and service providers and delivered cost-effective access to a wide range of Cloud-based resources through approaches like Peering with organisations such as Microsoft, YouTube, Google, Akamai and Amazon Web Services, made content from these entities on-net.

Further, Fell (2014) expressed that AARNET4 partnered with vendors such as Box, Amcom and Zoom, to customise enterprise products and services for Australia's research and education community; Build services, such as the AARNet Mirror, CloudStor and Eduroam, to meet the particular needs of the research and education community. CloudStor web interface provided infrastructure, platform, system security as a service, data replication at geographically distributed storage nodes for high

reliability, availability and provided integration with identity and access management and federated authentication systems (Fell, 2014).

From the above discussions, AARNET has to enhance its collaboration with global NREN partners to plan and develop R&E network inter connectivity on a global scale to meet the future needs of research and education worldwide. In view of this NRENs-CAF proposed an integrative architectural framework that consolidated all SADC NRENs across her border over a common Cloud Services Model (CSM) that enhanced collaboration among its member NRENs (refer to Figure 6.1).

2.2.7 New York Research Educational Network (NYU-NET)

NYU-NET is the National Research and Education Network in the United States (US), which according to Rose (2009), started off as a government funded project (namely Internet 1) and eventually underwent privatization. He said changes were made to the network structure to offset costs incurred by purchasing the Internet from commercial service providers, which was too expensive. He continued that NYU-NET created a separate backbone infrastructure (namely Internet 2), which connects to all major NRENs such as GEANT, Ubuntu Alliance, to mention a few. The author stated that Universities that created this NREN converted the network to a completely privatized organisation, which is today providing commercial offerings with better and more reliable network services for education to both academia and research. Further, the NYU-NET adopted the Internet standard policy to switch from proprietary protocol networks architecture to standard TCP/IP architecture. Additionally, they started as a

consumer and moved to form a bandwidth (BW) consortium and later commercialized and created companies independent of federal funding.

Unlike NYU-NET, the commercialization is not feasible with NRENs-CAF because it depends on the maturity of both legal frameworks and Cloud ecosystem. Further, NRENs-CAF recommended few policy decision changes and attempts to remain up to date with evolving internet privacy and confidentiality requirements. Similar to NYU-NET, NRENs-CAF could be switched from consumer to Bandwidth Consortium to its own private service provider for sustainability.

According to Meyer (2012), Internet-2 was a separate network, technically stable, offering high bandwidth and different qualities of service for experimental applications. Correspondingly Internet2, an advanced networking consortium led by the research and education community partnered with SHI International and Box to deliver new Internet 2 SHI International. He further mentioned that the consortium associated with Box to delivered new Internet2 NET plus Cloud computing and other services to faculty, staff, and students of Internet2 member Universities across the country.

Furthermore, the author reported the technicality of the Internet2 as HP Cloud service provided a private community Cloud suite of infrastructure services designed to meet the required levels of security, performance, and availability for higher education. In addition Meyer (2012) described that Box Internet2 NET plus Box service is a customized offering that was secure, scalable content-sharing and a collaboration platform. The author stated this would integrate with campus provisioning and security

requirements and provide a higher education legal agreement, all bundled together as an agreement for Internet2 NET2 among Common members. Meyer (2012) further described that Internet2 NET plus Box service included: ability for users to access, store, and share resources anywhere, anytime, and on any device; storage based on institutional subscription level, device access and support; administrative interface for managing and reporting on Box content; and support for University to protect information and ensure the privacy of personal data.

According to Katz, Ackerman, Hanss, & Corbato (2010), the areas that needed to be addressed in the Internet2 included stronger forms of authentication, access control mechanisms, improved audit capabilities, privacy tool to protect confidential information, scalable techniques to provide bandwidth guarantees on demand and dynamically reconfigurable broadband technologies for the 'last mile'. In view of the above, NRENs-CAF recommends the incorporation of the identity and access management in TCSF and federated authentication systems included in Cloud Federation System (CFS) as shown in Figure 6.1 integrated in its framework.

2.3 NRENs in Developing Countries

There are a few developing countries which have formed their NRENs with different technologies to interconnect members in order to collaborate. However, they are faced with challenges as discussed below.

2.3.1 Xnet Development Alliance Trust of Namibia

According to Xnet Development Alliance Trust (2000), the infrastructure was created to link the Ministry of Education, Telecom Namibia and SchoolNet in order to provide subsidized and affordable connectivity to tertiary institutions, libraries and Ministry of Education's regional offices in Namibia. They emphasized that Educational Network (Edunet) was created within the Xnet structure to become the Internet Service Provider (ISP) for all educational institutions in Namibia. Hence, Edunet only addressed Internet connectivity to primary, secondary and teachers' colleges and lacked particular educational portal facilities. However, this model did not cater for sharing of resources among tertiary institutions. It shows no progress of moving towards Cloud computing.

According to Kuria (2013), the Xnet Development Alliance Trust was established as a connectivity provider for schools and expanded its operations to include all educational institutions. Further, he stated that through partnerships with telecommunications operators in the country, Xnet was able to secure subsidised pricing on behalf of its beneficiaries that included tertiary institutions, libraries, teachers' resource centres, vocational training centres as well as schools. Beyond connectivity, services such as e-Learning, email provisioning, website hosting, spam filtering to mention few were possible through the Xnet ISP.

Kuria (2013) further stated that it made sense, given the educational beneficiaries already connected, for Xnet to seek membership with the UbuntuNet Alliance and became an NREN. As members of the NREN, these institutions would benefit from

lower costs of bandwidth. The national bandwidth linkages would be established between member institutions, that led to collaborated research projects between institutions and developed local research and the capacity building for research in Africa and more importantly, to conserve international bandwidth (Kuria, 2013).

In addition, he stated that Xnet being the last entrant into the UbuntuNet Alliances arena. This NREN had to consider costs of ISP equipment, cross-border connections to the closest UbuntuNet routers, meetings with potential beneficiaries, staffing needs to mention few. The cost of setting up can be daunting especially for an institution in its infancy stage.

According to the Telecom Namibia, TN (2013) Annual Report, the role of TN was towards creating a Namibian 'Knowledge Society' that provided accessible and affordable bandwidth connectivity, improving the access to information, enabling shared resources, stimulating innovation through research, creating new opportunities for employment, and providing a catalyst for multi-stakeholder efforts to e-education and health institutions. Further, TN (2013) highlighted that together with Xnet, Ministry of Education, University of Namibia and the Namibia University of Science and technology continued collaboration regarding the NREN of Namibia. In addition, the TN (2013) reported that the education network was redesigned that allowed for greater control and management over bandwidth for the education sector whilst streamlining operations. Moreover, the TN Data Centre had new storage racks, some were earmarked for the Xnet ISP. Additionally, TN provided a subsidy to Xnet and the discount on

broadband packages. Therefore, Xnet Development Alliance Trust or Xnet rolled out high-speed Internet connectivity to schools, local Universities and research institutions (TN, 2013).

Further, this report stated that the Ministry of Education upgraded all existing broadband connections to schools from three hundred and eighty-four (384) Kbps to one (1) Mbps due to the discount pricing offered by TN on broadband. Further, TN (2013) had proposed an order with Xnet for the installation of broadband at three hundred (300) new schools. Further TN report stated that Namibia University of Science and technology (NUST) had migrated all their regional centre links to Xnet spanning a total of eleven (11) sites across the country with links ranging from one (1) Mbps to seven (7) Mbps. Hence, with time, it was expected that UNAM and the International University of Management (IUM) would follow suit.

According to TN (2013) report, a few education and research institutions were connected through the EASSy cable on the East Coast but Namibia and Zambia were not connected through the West Coast. Further, this report stated that TN had negotiated with Uganda and as a consequence, pricing on the East Coast was greatly reduced. Correspondingly, TN had put forward a bid to the UbuntuNet Alliance to provide bandwidth to education and research institutions in Namibia via WACS. This report stated that after launching Swakopmund WACS landing Station, TN had delivered on this by supplying various public services with discounted bandwidth connectivity.

Further, Kuria (2013) emphasized that with the advent of Cloud computing, the more established NRENs considered hosting services on behalf of start-up NRENS to allow them an opportunity to concentrate on growing capacity. Furthermore, this eliminated the need for the NREN to have to procure equipment immediately, or to hire additional staff from the onset. Moreover, when the NREN had grown enough to a position that could support additional staff, the transition from the supported NREN to an independent institution would be better planned and less stressful.

However, Xnet model is in its infancy in forming its NREN and collaborating among tertiary institutions. Henceforth, NRENs-CAF would assist the Xnet, which is the NREN of Namibia to deploy Cloud services to collaborate and secure high-speed connectivity between tertiary institutions. Such deployed Cloud services would be extended to other SADC NRENs on a consolidated unified platform which would facilitate inter-cloud collaboration.

2.3.2 Zambia Research and Educational Network (ZAMREN)

Mbale (2008) described the Zambia Research and Educational Network (ZAMREN) architecture that was divided into two operational zones: The Southern zone (SZ) distribution hub which was managed by University of Zambia (UNZA), and Northern Zone (NZ) by Copperbelt University (CBU). He explained that ZAMREN leased the fiber network from Zambia Electricity Supply Corporation (ZESCO), Copperbelt Energy Corporation (CEC) and Zambia Telecommunications Company Limited (ZAMTEL).

Further, Mbale (2008) had described that the implementation of ZAMREN was done in three (3) phases. In addition, he discussed that Phase 1 involved connection from the ZESCO and CEC substation fiber networks to the selective institutions that served as distribution hubs. Phase 2 involved inter connection of NRENs from the neighbouring countries, such as Angola, Botswana, Namibia, Malawi, Mozambique and Zimbabwe, through ZESCO fibre cable. Lastly, Phase 3 involved connection to nations outside her borders, especially the Eastern Africa Submarine Cable System (EASSy).

Mbale (2008) added that such types of NRENs did not have a complete national fibre backbone. He further indicated that places where power lines did not exist, the digital Microwave links or VSAT connections were deployed. ZAMREN was registered in the year 2007 as a not for profit association and operationalised in June 2012 when ZAMREN was connected to Ubuntunet Alliance PoP in South Africa (Mkandawire, 2013).

According to Khunga (2012), TENET and CEC-Liquid Telecom, a telecommunications company with optical fibre network in most of the Southern African countries, completed a cross-border link between TENET and ZAMREN with an initial capacity of hundred and fifty-five (155) Mbps. Further, he described that this link was between the ZAMREN NOC at the University of Zambia in Lusaka, Copperbelt University and the TENET node in Johannesburg had gone via Zimbabwe, formed the first research and education cross-border link in Africa.

Consequently, Khunga (2012) stated that ZAMREN is the first, authentic landlocked NREN that operated a cross-border link in sub-Saharan Africa, if not the whole of Africa. The circuit was extended to the UbuntuNet Alliance PoP router in Mtunzini via the SANReN network in South Africa then uses capacity made available by TENET on the SEACOM submarine cable as onward connection to the UbuntuNet Routing Hub in London, which had further connected to GEANT - "at the heart of global research networking" (Martin, 2012). He continued describing, Mulungushi University would be connected in future as will other research and education institutions. ZAMREN is the fourth NREN to connect to UbuntuNet Alliance infrastructure that allowed researchers, lecturers and students in Zambia to participate fully in global research and education networking activities.

According to Kunda and Khunga (2014), the introduction of NRENs provided opportunities for Universities and Research Institutions in Africa for increased research and publications through increased Internet bandwidth, collaborative research and availability of resources through e-libraries. They further explained, however, some Universities in landlocked countries had not yet been able to take advantage of the full potential of ICTs in the delivery of actual education and learning, because of the challenges of implementing NRENs and Zambia is not an exception.

According to Kunda and Khunga (2014), the challenge of landlocked African countries included lack of direct access to the sea cable thus making Internet cost high and needed to negotiate with neighboring countries for connectivity. Further, they stated that

economic and human development indicators for landlocked countries in Africa were generally worse than those for maritime neighbours because of dependence on other countries transit routes for access to overseas markets and to the Internet. The authors further described that dependence over the transit state necessarily implied dependence on peace and stability within transit countries and high transaction costs were perceived as the result of "transit charges" but also the difficulties to benefit from regional adequate infrastructure.

Furthermore, Kunda and Khunga (2014) stated that delays and even, more importantly, the low degree of reliability and predictability of services create massive disincentives to invest and higher total logistics costs. They further explained that a landlocked country depends on the ICT infrastructure of the transit country and therefore if there were new technology introduced and the transit country does not invest in that technology means that the landlocked will not benefit from the new technology and hence, the cost of ICT services in a landlocked country is much higher than its maritime neighbor. In addition Mkandawire (2013) stated that ZAMREN service portfolios were limited to traditional mail hosting & relaying, spam filtering, domain, web hosting and Data Centres which were also provided by commercial ISPs.

According to Kunda and Khunga (2014), ZAMREN had future plans of providing advanced or distinguishable value added ICT services such as EDUROAM, Federated Identity, High Performance Computing (HPC) & Cloud Computing, establish and operationalize a Computer incidence response mechanism and automated standard

Internet services. NRENs-CAF facilitates NREN's connection to nations outside borders and established Cloud architectural services. The Cloud computing technologies provided by NRENs-CAF would reduce the IT cost for the landlocked countries' NRENs.

In addition, NRENs-CAF can take advantage of the existing WACS, the new submarine cable infrastructure to connect other nations outside their borders. Thus, NRENs-CAF would consolidate land lock SADC member countries on a unified platform and enhance regional and international collaboration. Further, NRENs-CAF integrates with campus provisioning and security requirements enabling security framework; and recommends a higher education legal agreement and policy framework, all bundled together as an agreement for NRENs-CAF among SADC members.

2.3.3 Tertiary Education and Research Network (TENET) of South Africa

Afrinic.net (2008) categorizes TENET under well-established NRENs. The Afrinic public policy explained that TENET, which had been the country's de facto NREN since the year 2000, was owned by tertiary education institutions themselves. They said the network was built and managed by Telecommunications South Africa (TELKOM). Moreover, Sybrand (2009) described that later in the year 2005, South African National Research Network (SANReN) was integrated with TENET, but both were not fully converged. He also stated that TENET focused on the needs of tertiary education, whilst SANReN was envisaged as playing a major role in promoting research.

According to TERENA (2012) report, TENET was the core of the NREN network that operated SANReN and served hundred and seventy (170) sites of fifty-five (55) research and education institutions. Further, this report stated that TENET had a collaboration agreement with the Centre for Scientific and Industrial Research (CSIR) under contract to the Department of Science and Technology (DST) to operate SANReN. Consequently, this report stated SANReN national backbone was provided to Meraka by Neotel and Telkom SA comprised a multi-gigabit national backbone ring interconnected major nodes in the country, including several metropolitan rings.

Further, this report described that TENET connected a number of campuses via low-speed rented access circuits, and some thirty-six (36) smaller sites via Asymmetric digital subscriber (ADSL) lines and a shared connection between Telkom's ADSL network and the TENET gateway in Johannesburg. Moreover, TENET operated a network that used two different submarine circuits that provided intercontinental connectivity to the UbuntuNet network in Europe. These were: A ten (10) Gbps circuit on the SEACOM submarine cable that terminates at the SEACOM landing Station at Mtunzini extended to the SANReN backbone node at Durban, and at the UbuntuNet Hub in Amsterdam; and a six (6) Gbps circuit on the WACS submarine cable that terminated at the SANReN backbone node in Cape Town and at the UbuntuNet Hub in Telecity, London. Dark Fibre Africa supplied SANReN's optical fibre that ringed networks in Johannesburg, Pretoria, Bloemfontein, Cape Town, Port Elizabeth, East London and Durban and back to Pretoria (TERENA, 2012).

According to TERENA (2012) report, TENET also operated a network that included: the GEN3 MPLS (Multiprotocol Label Switching) network and Metro-E circuits provided by Neotel; IP Connect bandwidth into the ADSL Cloud, and various optical fibre and wireless access circuits connected some ninety (90) urban campuses to the backbone. In addition, this report indicated that dedicated access circuits included ten (10) Gbps long-haul circuits to the radio astronomy and space operation centres at Hartebeeshoek, Sutherland and the radio astronomy site at Carnarvon.

Greaves (2013) reported that TENET operated transit and peering links in Cape Town, Johannesburg, London and Amsterdam gateways and included a connection to the European research and education network, GEANT. In addition, TENET operated UbuntuNet gateways in Mtunzini, London and Amsterdam contracted to the UbuntuNet Alliance. He further stated that TENET secured global interconnectivity with other NRENs worldwide and also to the major London and Amsterdam Internet Exchanges.

According to Ajayi and Ajayi (2011), the main purpose of TENET was to secure, for the benefit of South African Universities, technikons and associated research and support institutions. In addition, they stated that TENET involved entering into and managing contracts with service providers and institutional users. They added that TENET was actively engaged in the construction of access networks connected to the SANReN network that provided Internet and IT services. They said the services involved inter-alia, high-speed Internet access, inter-campus connectivity, ancillary operational

functions in support of service delivery and the provision of other value-added services needed in support of higher education and research in South Africa. Further, they stated, however, this NREN facilitated in sharing contents between members and provided their clients with research networks and the Internet, without necessarily providing robust and secured networks using minimal hardware solutions.

According to Lotz, L. (personal communication, September 4, 2015), TENET concentrated on connectivity aimed at bringing down the high cost of connecting member Institutions. Thus, the NREN would boast very high connectivity speeds and facilitated access by the members to both each other's resources available both nationally and internationally. The author further stated that the SANReN network currently had no Cloud based services offered to their member institutions. This NREN offered other auxiliary services such as domain name registration and mirror services. He further asserted that there was use of Cloud by member institutions without the need for NREN involvement as a result of the big network pipes. Institutions on the network made use of Cloud based Email and office products from most of the big providers such as Google and Microsoft. In addition, he stated that security was still a major concern when the critical data was carried by a third party Cloud provider.

Further Lotz stated that Cloud computing in South Africa was in its early growth stages and the NRENs were in a quandary about Cloud Services. Further, he described that; TENET in future would get involved more closely in Cloud services. A few of the institutions were starting up a Cloud Service called African Research Cloud were in its

infancy and seeks to look at providing the kinds of services that are not available from the Amazons, Googles and Microsoft to name a few. In addition, he stated that there could be a proposed opportunity to turn this NREN into a Federated Identity based service that can serve the research community across Africa later as it matures.

In view of above Greaves (2013) explain the service development challenge as TENET and SANReN had to focus on the provision of specialised, targeted value-added services that University and research institutions require. Such services include, for example, the use of very high speed connectivity; un-routed point-to-point circuits ("light paths") for moving very large datasets to or from anywhere in the World; high quality video conferencing; and the establishment of trust federations in which many institutions agree to provide each other's staff and students access to each other's electronic resources, library and computing resources, using federated authentication and authorisation schemes. Federated Identity Management (FIdM) amounts to having a common set of policies, practices and protocols in place to manage the identity and trust into IT users and devices across organisations. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly and without the need for completely redundant user administration (Greaves, 2013).

According to the (TENET, Interview 26 June 2012), some of its University clients were considering moving dedicated e-mail services onto the web, but without sufficient confidence in moving entire administrative systems or resource bases onto the Cloud.

Further, in this interview, it was stated that some Universities were willing to move onto the Cloud but reliable and redundant international connectivity remained a challenge. In addition, this interview asserted that data privacy and security of Cloud services were of some concern amongst Universities, but potential cost saving could be a more influential driver of Universities onto the Cloud.

According to Greaves, companies have started to transition their IT departments to private Clouds. He added, while concerns surrounding security and privacy of data continue to hamper the adoption of public Cloud services, the cost pressures were expected to force companies to increasingly move some applications onto public Clouds in order to streamline costs. He further explained, many large companies that had adopted Virtualization technologies are beginning to realise that Cloud computing has significant efficiency gains and had the potential to enhance widespread activities such as education and innovation.

However, based on the above, it is evident that TENET and SANReN had not been consolidated for better collaboration among its members. It is also observed that TENET has not adopted Cloud computing technology fully, except for email services from public Cloud. TENET has shown a major concern for security and integrity of their data owned by Cloud service provider. Henceforth, NRENs-CAF uses the reach out experience of the Grid and Internet community and possibly following the same architecture patterns as Internet and Grid/OGSA, include providing functionalities for creating Virtual Organisation (VO) based architecture NRENs-CAF (refer to Fig 6.1).

This complements the components of the proposed NRENs-CAF facilitating the transformation of the existing non-Cloud IT systems to Cloud infrastructure for improved computing resources and services; and consolidation of SADC NRENs for efficient collaboration and standardization.

In the same vein, NRENs-CAF proposes incorporation of Trusted Cloud Security Framework (TCSF) architectural component in the layered NRENs-CAF Framework that would address data security issues based on Cloud Security Alliance (CSA 2010) security reference model; and Cloud Federation System (CFS) component has the potential to assist federation between different Cloud domains and inter-cloud domains through Federated identity management (FIdM) based on IEEE standardisation activity to define inter-cloud Federation framework, The ITU-T Focus Group on Cloud Computing (FG-Cloud), NIST Cloud Computing Reference Architecture (CCRA) and ISO/IEC 27000 series of best practices. It further proposes an E-Science Cloud Infrastructure (ECI) architectural component for sharing highly scientific projects and e-research. Finally last but not the least NRENs-CAF rather acts as Consortiums of Cloud customers among SADC NRENs. Further, NRENs-CAF recommends content delivery or management for interaction and knowledge dissemination. Henceforth, NRENs-CAF facilitates the transformation of the existing non-Cloud IT systems to Cloud infrastructure for improved computing services, standardization and convergence.

2.4 Cloud Adoption and Initiatives in Africa

According to Kwofie (2010), MTN Africa launched a pilot Cloud service project which targeted small and medium enterprises (SMEs) in six (6) African countries, namely: Ghana, Cameroon, Cote d'Ivoire, Nigeria, Uganda and South Africa. The project aimed at enabling SMEs in Africa to operate efficiently by offering suitable ICT solutions. The author further added that Dataflex partnered with Intelledox, one of Nigeria's premier IT companies, and added Cloud computing technology to its list of services in order to provide secure, flexible and reliable services for its users.

According to Maaref (2012), Cloud Security was one of the major establishments in the wake of Cloud computing in Africa and it had been the Africa Cloud eXchange (ACX) established by Teraco, a leading IT service provider in South Africa which provided access to Cloud services with secure Data Center environment. The Author explained that ACX facility had connections to all the undersea cables offering a combined twenty-eight (28) landing points along the East and West coasts of Africa, as well as all major carriers operated in South Africa and several active Cloud providers. It was anticipated that the ACX would make South Africa the central hub for international access providers and Cloud services for other African countries (Maaref 2012).

According to Hinde & Belle (2012), the organisations in an emerging economy such as South Africa were adopting Cloud computing solutions quite aggressively. In addition, they stated that in Ghana, the awareness created by Cloud service providers had seen an increase in Cloud adoption by various organisations. Hence, it can be deduced that the

rate of adoption of Cloud services had increased and there was an urgent need to address the challenges and security issues that these organisation faced in the Cloud.

According to Maaref (2010), there were numerous efforts by various governments in Africa that helped to meet the IT needs of those organisations. Various private companies had also taken key initiatives to bring Cloud computing services to the door steps of enterprises in different operating fields. Table 2.1 shows a list of government initiatives taken to favour the emergence of Cloud computing in the African countries surveyed by the author for the International telecommunication Union (ITU).

Table 2.1 List of Government Initiatives of Cloud Computing in African Continent (Maaref, 2013)

COUNTRY	**INITIATIVES**
(1) Ghana	➢ The country had access to SAT3 through Vodafone Ghana. The country had four submarine fiber optic landing station (Vodafone Ghana, Mainone, Glo, and MTN Ghana). Enactment of public disclosure laws.
(2) Mali	➢ A Technopole was established to accommodate certain Cloud computing services.

(3) Rwanda	➢ High performance computing through center Rhapta ICT city was proposed to be in Dar es Salaam.
(4) Gabon	➢ The country had access to SAT3 through Gabon Telecom. The Government had launched a vast program to make Gabon a hub for ICT services. ➢ Participation in the Central Africa Backbone (CAB) was led by CEMAC and financed by the World Bank. The aim of the project was to interconnect the countries of the CEMAC area using fibre-optic high-speed links.
(5) Cape Verde	➢ The Government's program comprised a cluster of ICT development strategies. This was the outsourcing of a data centre and technology parks.
(6) Burkina Faso	➢ The Government had taken the major initiative of implementing a regulatory framework that was favorable to Cloud computing.

(7) Burundi	➢ The Government participated in regional and international conferences and workshops on Cloud computing. The Government planned to recruit a Cloud computing experts to assist it in the feasibility study for and implementation of whatever would be necessary to introduce Cloud computing in Burundi.
(8) Togo	➢ The Government had taken initiative within the framework of the e-Government project implemented in Togo. Discussions were under way with a view to possibly make Cloud computing services available to the generic public.
(9) Namibia	➢ The Government had undertaken initiative to launch Windhoek Internet Exchange Point (WIXP) which was established with the support of African Internet Exchange System (AXIS) programme, a project of the African Union implemented by the Internet Society. WIXP was managed by the IXP Association of Namibia that was established as a non-profit organisation in order to manage the IXP using the multi-

	stakeholder process. The Internet Society's Africa interconnection and Traffic Exchange programme had been actively supporting the development of IXPs to facilitate a robust domestic ICT sector in Namibia.

From Table 2.1, one can see that there were several initiatives that influenced the adoption of Cloud computing among SADC NRENs. Further, these initiatives served as a reference that was taken into considerations during the establishment of NRENs-CAF.

2.5 Challenges of Cloud Computing in Perspective of Developing Countries

Research and innovation in the developing countries were much lower than developed countries. Sharing of research resources was the main reason for developing an NREN, but most of the educational organisations in the developing countries had limited research resource.

The main challenges which most of the developing countries faced, included lack of good network infrastructure, high cost of ICT services, lack of enough budgets, low support by the government, interoperability challenges, lack of sustainable wired and wireless network, political will and policy instability, and poor quality of services (Boateng, 2009).

In the view of above, Salim (2014) stated that NRENs of developing countries had weaknesses and challenges, lack of sustainable resources, sustainable governance

structure, and realistic long term vision, strategy and policies. He further stated formulation of a clear framework for the sustainability of NRENs of developing countries and formulation of a strategy for sustainability should be the near future work.

Based on the Trans European Research and Education Networking Association (TERENA) analysis in 2012 and the Strengths, Weaknesses, Opportunities and Challenges (SWOC) analysis of UbuntuNet Alliance in 2013, the first problem that TERENA pointed was that most of the NRENs of developing countries lacked strategic planning and long term vision. In addition, SWOC analysis stated that most of NREN organizers focused more in the networking and connection, but they were not focused on the services. The second problem that TERENA pointed out was that NRENs were more dependent on the governmental funds or project based funds which caused more bottleneck and problems (Dyer & Haver, 2012).

Therefore, the aim of this study was to explore the source of challenges of SADC NRENs in the developing countries and design an architectural framework for NRENs to take the opportunity of Cloud computing services that will address the major challenges faced by SADC NRENS, such as, Infrastructure, Security Interoperability, Governance and Cost.

According to Barry (2008), NRENs are important for Africa because they are possible means for African scientists to connect to each other and for global research teams to move from an era of isolation to an era of research collaboration. However, this can only occur when publicly available bandwidth becomes affordable for Universities and

making broadband infrastructure and services available and affordable. Kotecha (2012) supports that the rapid emergence of national and regional Research and Education Networks (RENs) as the organisational vehicles for inter-institutional collaboration. However, a major constraint to be dealt with the way to high-speed connectivity had long been evident: lack of campus-level infrastructure and facilities for bandwidth management.

Kotecha (2009) further explains that the challenges associated with campus-level networks in Southern African institutions include the uneven mix of technologies as a result of donations from partner institutions in developed countries; demands for continuous upgrading of systems to keep pace with technological developments and user needs; and the multiple purposes to which scarce ICT resources must be applied, including administration, teaching and learning, research, and special scientific applications. He further explained higher education leadership challenges in the SADC region: as the absence of funding and appropriate funding mechanisms; poor ICT infrastructure; lack of planning capacity, policy, e-science systems and regulatory capacity; poor and outdated research infrastructure.

According to the Regional Infrastructure Development Master Plan ICT Sector report (2012), the Consolidation of Regional Communications Infrastructure ensures that the region is fully interconnected nationally, regionally and globally through reliable, affordable high capacity. Fibre optic links in SADC needs to be augmented with the provision of high speed connectivity within and between research institutions in the

region and to the rest of the world (campus, national and regional) research and education networks (RENs). However, this report also describes, in some SADC member countries there were also serious shortcomings in the services offered by the operators as regards the main quality indicators, for example, on-time delivery, reliability and security.

Furthermore, this report described, the key ICT gaps that need to be addressed under e-Services and applications are: limited collaboration at national and regional levels between research institutions; High cost of access devices and software, low levels of ICT manufacturing capacity, lack of an integrated approach to planning, implementation and delivery of infrastructure, leading to waste of resources through lack of low cost access to ICT services. In addition, this report explained, e-Services development in SADC can be achieved by assessment of potential savings from sharing costs of software development, bulk purchases of Bandwidth capacity and equipment between member countries, and adopting a shared national or regional Cloud computing architecture. This report further states Research, Innovation and ICT development includes shared R&D, Potential collaboration on developing Open Content distribution networks to integrate Cloud and content services into one seamless service offering. In addition, this report stated that support for Cloud based network deployment in some SADC member countries was necessary.

2.6 Critical Analysis of Literature Review

This section synthesises the literature review as it enables the critical analysis of the documents reviewed. Standardized best practices and existing frameworks are discussed below with relevance to NRENs-CAF.

2.6.1 NRENs Situation in Developed Countries

The gaps identified from the reviewed literature with respect to some developed country NRENs were: either these NRENs were developed by the international bodies like Association of African Universities (AAU) body under UbuntuNet Alliance which were one of the largest research and education networks such as GEANT, DANTE, and European Union (EU) Research Networks to mention few. Hence, such NRENs are not independent and limit its collaboration with other NRENS outside their borders. The NRENs that are formed on their own were working isolated serving or forming consortium among its own members inside the country borders. In addition, some NRENs deploy only SaaS services in which end users deployed services by configuring the parameters related to their institutions and forming just a Cloud portal to connect its member institutions to Cloud. All these NRENs have raised the concern of security, data reliability and integrity of their organisational data. Therefore, security issues in these NRENs still needed to be addressed for reliable operation.

Further, it is observed that some of these NRENs adopted community and hybrid Cloud models. However, there were challenges like how to integrate or interoperate with

different Cloud domains and different Cloud providers for common management, federation and orchestration of services and maintain control over security and performance. Some NRENs avail services from third party CSP's and in this case, trust within the domain is the prime concern. In addition, some of these NRENs form a consortium expands collaboration between specific groups of researchers, academics and other scholars. There are few NRENs with state-of–art and have success stories delivering cost-effective access to a wide range of Cloud-based resources through approaches like; Peering with organisations such as Microsoft, YouTube, Google, Akamai and Amazon Web Services, made content from these entities on-net; Partnered with vendors such as Box, Amcom and Zoom, to customise enterprise products and services. These NRENs build services, such as the CloudStor and Eduroam, to meet the particular needs of the research and education community.

2.6.2 NRENs Situation in Developing SADC Countries

The gaps identified from the reviewed literature with respect to some developing country NRENs were: The NRENs in some developing countries are not formed or it was in its infancy in forming its NREN. These NREN models did not cater for sharing of resources among tertiary institutions. The countries where NRENs are formed, some shows no sign or start-up in regards of moving towards Cloud computing. However, few NRENs that claimed to be on Cloud were limited to traditional mail hosting & relaying, Spam filtering, Domain & Web hosting, Data Centres which were also provided by commercial ISPs. Some of these NRENs had provided services like data center, video

conference, e-library and technical support. Even though these NRENs is providing different services to their members, it still needs integration of other services, and service delivery based on the new model of computing, which is Cloud based computing, for a better service delivery strategy and strategic utilization of resources.

Few developing country NRENs plan in future to provide advanced or distinguishable value added ICT services such as EDUROAM, federated identity, High Performance Computing (HPC) & Cloud Computing. Security was still a major concern when the critical data was carried by a third party Cloud provider. However, confidence in the prevailing legal systems in African countries remained at an unsatisfactory level in terms of data availability, integrity and confidentiality.

2.6.3 Cloud Computing in African Situation

In Africa, several Cloud computing projects are already under way or under study. Among these projects, the most solid are the result of partnerships between international players and African economic operators. The Account also has to be taken, of course, of the circumstances specific to Africa, where the human, technical and financial resources that are available to, or within easy reach of the African players often fall short of the requirements imposed by this new technology.

In an article recently published in the journal “Les Afriques”, Raphaël Nkolwoudou, Associate Counsel Azaniaway Consulting, explains that Cloud computing is suited to the African continent by reason of the concentration of infrastructures, availability of IT

competencies and ease of implementation. There is, however, one prerequisite, which is to speed up the development of electronic communication infrastructures. He adds that among the specific benefits of Cloud computing in Africa, two, in particular are liable to make a significant contribution to reducing the digital divide, namely: The ability to have immediate access to the latest innovations; The possibility for an organisation to do away with heavy investment in infrastructure, particularly where computation centers are concerned, given the unreliability of the electric power supply in Africa.

2.6.4 ICT Development in African Situation

The situation in Africa is characterized by relatively favorable network infrastructure development with constantly improving international connectivity. In recent years, several international cables have made landfall on each side of the continent, favoring the growth of telephone and Internet traffic and the emergence of an ever-increasing number of data centers. This development, initially driven by the very rapid expansion of mobile telephony, has been boosted by the high-capacity requirements stemming from the introduction of broadband technology. The resulting data exchanges on the different networks call for ever-expanding data storage capacities something that can only be managed virtually, via the web. However, all of this is not without problems, be they problems which hinder the normal operation of existing data centers or development of new ones.

A report produced by the Hedera Technology consultancy firm on the Internet in Africa points to shortcomings associated with poor quality of service due to under-investment

in communication networks, making it difficult to abide by clauses guaranteeing quality levels and access speeds for Cloud computing services. At the same time, the use of ICTs in Africa is continuing to produce exponential growth in this sector. With a young population that is set to double by 2050, we are still likely to see very positive ICT market growth rates in all African countries. Despite the constraints (lack of infrastructure, power-supply problems, etc.) that are hampering ICT development in some parts of Africa. The African Cloud computing market appears, paradoxically, to be "benefiting" from those constraints and the continent is experiencing the opening up of considerable opportunities where this new IT model is concerned. The fact is that the major players in the international Internet and server industry spheres have already positioned themselves in the African market. In South Africa, new companies have opened two data centers, in Cape Town and Johannesburg. These represent an attractive opportunity for international companies, which see in them a very low-cost alternative to European centers.

2.7 Cloud Standardisation Overview

This section describes some Cloud related standards which are reviewed in this literature review.

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) that defines the Cloud computing Reference Architecture (CCRA) is a conceptual and standard base model in

Cloud Computing. The limitation of the current CCRA is that it is not suitable for defining required security infrastructure and its integration with main Cloud services or infrastructure that can be potentially by heterogeneous multilayer and multi-domain.

IEEE Intercloud Working Group (IEEE P2302)

The limitation of the IEEE P2302 architecture and approach is that it tries to closely imitate the Internet approach in building hierarchically interconnected infrastructure by adding an additional inter-cloud layer to support inter-cloud communications at networking and messaging levels. However, this architecture lacks addressing specific problems in inter-cloud integration, management and operation. This architecture tries to replicate the Content Distribution Network (CDN) approach but doesn't address the generic problems with interoperability and integration of the heterogeneous multi-domain and multi-provider Cloud base infrastructure. This approach has a limited scope by attempting to address a hypothetical scenario when all resources and applications are located and run in multiple Clouds and they need to be federated similar to Content Distribution Network (CDN).

ITU-T Cloud Network Infrastructure Model

The model also analyses the Cloud technology benefits from telecommunication perspectives and discuss scenario with inter-cloud peering federation and brokering. The ITU-T proposes the model for Cloud network infrastructure that included core transport network, intra-cloud network, and inter-cloud network. Issues related to network

interface cards (NIC) Virtualization and virtual machines migrations are discussed. The documentation on ITU-T provides suggestions for Cloud network topology design and definition of the virtualised network components such as Cloud switch and Cloud routes.

Generalized Architecture for Dynamic Infrastructure Services (GEYSERS)

GEYSERS project provides a basis for defining the proposed Inter-cloud architecture. The architectural framework for Cloud based infrastructure services provisioned on-demand being developed in the framework of the GEYSERS project that is used as a basis for building multilayer Cloud services integration framework that allows optimized provisioning of both computing, storage and networking resources. GEYSERS provided multi-domain, inter provider network and IT resources to users. They are managed by the consistent, dynamically provisioned security and access control policies.

IBM Cloud Computing Reference Architecture 2.0

IBM CCRA provides implementation, interfaces and programming models with the IBM tools and platforms.

2.7.1 Security Reference Model

Cloud Security Alliance reference model (CSA 2010)

This model maps the Cloud model to the Security Control & Compliance model separately.

Service Delivery Models Security (SDMS)

This model maps six security requirements against Cloud deployment models and Cloud service delivery models separately.

Confidentiality, Integrity and Availability (C.I.A) Security Reference model

This model is a way of describing the information security level of a system; the model dates back to mainframe computing. The term C.I.A. Security Model is synonymous with the terms C.I.A. Triad and C.I.A. Triangle.

ISO/IEC 27002

This model has the ability to map Cloud models to control frameworks which are the key to initiating, implementing, maintaining and improving information security within the organisation.

European Network and Information Security Agency (ENISA)

According to Barroso, D. (2007), this model worked with the security issues in Cloud Computing and analyzed the most critical security risks while adopting Cloud

Computing and which should be kept in mind before switching to Cloud Computing. The ENISA presented the risks which are involved with Cloud security while adopting Cloud Computing.

2.8 Related work/Existing Framework

There are not many or none academic research on Cloud architecture framework for SADC NRENs. Most of the research's are focused on analysis and improvement of the general Cloud architecture that is defined by NIST CCRA. A few works (Zhang and Zhou 2009; Shan et al. 2012; Takefusa et al. 2011; Bosch et al. 2011; IBM CCRA) are trying to apply more conceptual approach to defining Cloud based infrastructure services, but their scope is rather focused on one or another specific problem. Zhang and Zhou proposed the Cloud Computing Open Architecture (CCOA) based on SOA and Virtualization and derives ten interconnected architectural models, but it doesn't go further with suggesting implementation. Shan et al., explores an approach to describe the inter-cloud operations based on the New Generation Service Overlay Network (NGSON), but the proposed solutions are rather focused on the content delivery overlay networks. Takefusa et al. (2011) described the GridARS system that can provision heterogeneous performance assured virtual infrastructure over inter-cloud environment. However, the proposed solution is primarily focused on the optimal VM deployment and lower level underlying network communication.

Bosch et al. (2011) presented by Alcatel-Lucent Bell Labs provided an interesting point of view of the telecom industry on adoption of Cloud technologies to building Cloud

based telecom infrastructures what confirms the Clouds potentiality to provide a basis for the complex infrastructures Virtualization and infrastructure services mobility and on-demand provisioning. Industry research and development are mostly focused on adopting the NIST CCRA to their inter-cloud Architecture Framework for Heterogeneous Multi-Provider Cloud based Infrastructure Services Provisioning. Industry research and development are mostly focused on adopting the NIST CCRA to their business practices and platforms. A good example is the IBM Cloud Computing Reference Architecture 2.0. IBM CCRA provided a lot of useful detail on CCRA implementation, interfaces and programming models with the IBM tools and platforms. Based on the above models, the NRENs-CAF also designed for heterogeneous Cloud

Security Services Lifecycle Management (SSLM) Model

This model discusses conceptual issues, basic requirements and practical suggestions for designing dynamically configured security infrastructure provisioned on demand as part of the Cloud-based infrastructure. According to Demchenko et al. (2013), the SSLM model addressed specific on-demand infrastructure service provisioning security problems that can be solved by introducing special security mechanisms to allow security services synchronisation and binding to the Virtualization platforms'. In particular, this model discusses the design and use of a security token service for federated access control and security context management in the generically multi-domain and multi-provider Cloud environment. This model also adopts some components from the proposed dynamically provisioned access control infrastructure

(DACI) architecture and defines the necessary security mechanisms to ensure consistent security services operation in the provisioned virtual infrastructure. Therefore, NRENs-CAF adapted security component from this SSLM model.

2.9 Summary

In chapters one and two, the research problems were globally contextualized and focused down to the current state of SADC NRENs. The literature review provided deeper insight into the different NREN's and their Cloud initiatives, descriptions, the current Cloud architecture models, their security benefits and risks, their interoperability and the governance issues involved in few developed and developing countries, in particular, SADC NREN's. This chapter also described Cloud Adoption and Initiatives in some African countries. It also highlighted on Challenges of Cloud Computing in Perspective of Developing Countries.

The following chapter describes the research methodology used through research strategies.

CHAPTER 3: RESEARCH METHODOLOGY

The chapter presented the methodology applied in this study. The presentation of the research methodology included a brief introduction, discussion of the research design, population sample, research instruments used, data collection procedure and an overview of the data analysis, validity and reliability of data, and ethical considerations.

3.1 Introduction

This study used a quantitative research design to investigate the current status and possible usage of Cloud computing technology among SADC NRENs; identifying challenges faced by them in establishing institutional Cloud Services and recommends an integrative architecture for SADC NRENs. Furthermore, Creswell (2003) defines quantitative research as a type of research that is explaining phenomena by collecting numerical data that are analyzed using mathematically based methods. In addition, Welman, Kruger and Mitchell (2005) stated that quantitative research examines the relationships that occur between two or more variables. Moreover, quantitative research designs support a descriptive framework for different variables in the study for explorative purposes. Furthermore, the positivist research strategy was used for the quantitative non-experimental research survey that includes the gathering and analysis of quantitative data for the study.

Cooper and Schindler (2004) indicated that quantitative studies are designed for breadth rather than depth. quantitative or positivist studies attempt to capture a population's characteristics by making interpretations and inferences from a sample's characteristics. Generalisations about findings are then made and presented based on the representativeness of the sample and the validity of the design. On the other hand, Marlow (1993) stated that qualitative research is characterized by the use of large samples, standardized measures, a deductive approach, and highly structured interview instruments to collect data for hypothesis testing. Hence, qualitative methods may be more useful in hypothesis-testing research which was not the intention of this study. Henceforth, this study employs a limited positivist epistemological approach where the level of generalisations and interpretations are limited to a descriptive framework. The limitations are as a result of the sample size that was possible for this type of a study and the limited response from the respondents. Thus, the study aimed at making inferences of integrating NRENs-CAF among SADC.

According to Darlaston and Jones (2007), the ability to identify the relationship between the epistemological foundation of a research and the methods employed in conducting the study is critical in order for research to be truly meaningful. Therefore, the researcher adopts a positivist epistemological stance that aims to identify resources and challenges of integrating NRENs-CAF among SADC NRENs, which is also consistent with a quantitative research mode.

This research was approached by firstly observing an overall presentation of the strategy, the research methods, data collection, data analysis tools and research ethics. The right research strategy was then identified based on the research questions chosen. The overall research methodology includes components such as Research Purpose, Research Approach, Research Strategy and Research Methodology used in this study, which is presented in Figure 3.1 and each of this components was explained further with relevance to this work.

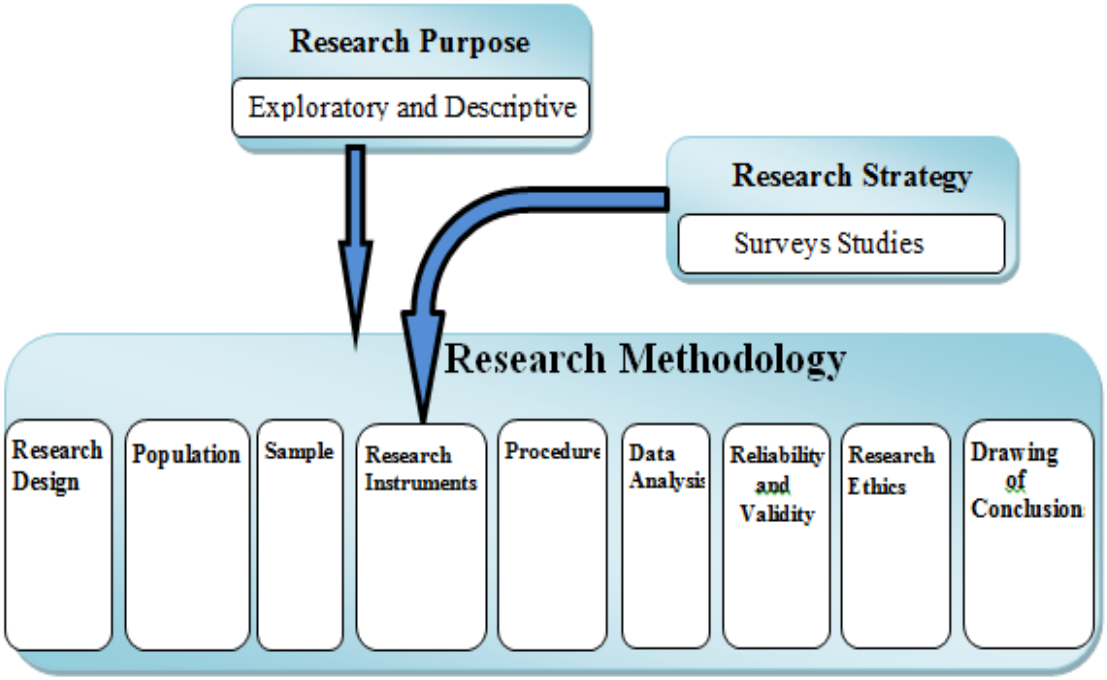

Figure 3.1: Summary of Research Methodology

3.2 Research Purpose

Saunders, Philip and Adrian (2010) distinguished research purposes according to the overall objectives. They further explained that exploratory research was often conducted when the research problem was not clearly defined yet or knowledge was vague. The authors stated that a search of the literature, interviewing experts in the subject and conducting focus group interviews were the three principle ways of exploratory research. Furthermore, the survey is a technique widely used for quantitative data collection in IS/IT research and could be used for exploration, description or explanation purposes (Pisonneault & Kraemer, 1993). Moreover, Bryman (2001) indicated that survey is an appropriate means of collecting data under three conditions: (i) when the goals of the research call for quantitative data, (ii) when the information sought is reasonably specific and familiar to the respondents, and (iii) when the researcher has considerable prior knowledge of particular problems and the range of responses likely to emerge.

However, in this study, the researcher used an online survey questionnaire to obtain expert views from the management personnel in the eight SADC countries that have functional NRENs. A literature or document review search was also done but due to some logistical challenges, focus group discussions, key informant interviews could not be done. The questions used in the questionnaire were mostly structured and closed with a few open ended.

3.3 Research Approach

Richard (2013) distinguished research approach as deductive and inductive approach. These two research approaches relate to quantitative and qualitative research designs respectively. Given that the nature and purpose of this study was to explore, describe and understand the situation with regards to usage of Cloud computing in the different NRENs, a quantitative research design was adopted with a focus on getting descriptive rather than deductive results. This was achieved through document review, frequency table and bar charts. Barring the logistical challenges such as travelling allowance and geographical disparity to reach out to these NRENs that were faced in trying to arrange for focus group discussions, a mixed design would have been best for this purpose. However, since there are no focus group discussions, no key informant interviews, etc. this leaves with one option, that is, a quantitative approach.

3.4 Research Strategy

A research strategy served as a general plan for acquiring knowledge and data that solved the research questions. Saunders et al. (2011) identified different strategies among which surveys and case Studies were foremost important in the research study. They further explained that surveys allowed the collection of a large amount of data from a sizeable population in an economical way. In addition, the authors also explained that case studies involved an empirical investigation of a particular contemporary phenomenon within its real life context using multiple sources of evidence. Hence, the strategy applied in this study was a mix of surveys and case studies as the research tried

to design a framework from the reference standardised models and existing frameworks for the development of Cloud architecture framework for SADC NRENs.

3.5 Research Design

The research employed a non-experimental research design that was descriptive in nature. Maree (2007) stated that non-experimental designs are mainly used in descriptive studies in which the units that have been selected to take part in the research are measured on all the relevant variables at a specific time. In light of Maree (2007), this study is mainly based on a quantitative survey design although the researcher was open and willing to use the mixed design, that is, both quantitative and qualitative research designs. Furthermore, Maree (2007) argued that surveys are done in order to obtain quantitative information that can be used to describe or explore research topics.

Therefore, this study used the descriptive strategy to discuss and interpret findings. By using descriptive research strategy, the study described the relationship between; the resources required, enhancing collaboration, and the possible challenges it may experience. On the quantitative approach, a structured questionnaire is used to collect data regarding the existing NRENs in SADC region to explore their initiatives, resources required and challenges faced in moving towards Cloud computing. This data assisted in designing the proposed NRENs-CAF framework. The questionnaire was administered online and hence, most questions in the questionnaire were deliberately made close ended so as to reduce item non-response.

According to the Saunders et al. (2011), literature research was used for evaluation and assessing current methodologies for investigation and description of use case scenarios. Further, they stated that a literature search assisted in acquiring knowledge about. In general, literature search was used for ad-hoc problems and research on specific knowledge. The outcomes helped to study the existing NRENs and current Cloud computing standards and services to design and improve the proposed framework (NREN-CAF).

3.6 Population

Sekaran and Bougie (2010) defined research population as the entire group of persons or set of objects and events of interest to the researcher. Therefore, the targeted population comprised of all personnel from the IT Departments, computer centers, network managers, network administrators and network technicians from the respective Network Operating Centres (NOCs) in the fifteen (15) countries in the SADC region. However, out of the fifteen (15) countries, only eight (8) had their NRENs formed such as Malawi Research and Education Network (MAREN), Tanzania Education and Research Network (TERNET), Mozambique Research and Education Network (MoRENet), Congolese Research and Education. Network (Eb@le), Research and Education Network for Academic and Learning Activities of Madagascar (iRENALA), TENET, ZAMREN and XNet of Namibia, were targeted for the study. Thus instead of targeting all personnel in the 15 member countries, this study focused on the personnel from the eight (8) member countries which have formed NRENs.

3.7 Sample

The sample for this study was derived from the NRENs personnel in the eight (8) member countries. A purposive sampling technique is used to select the participants from the SADC NRENs study population. Three (3) online questionnaires were sent to each of the eight (8) NRENs targeted to sample twenty-four (24) IT personnel in these different NRENs. Out of these twenty-four (24), only thirteen (13) responded giving a response rate of 42%. This response rate is, however, consistent with self-administered and online questionnaire response rates (Struwig & Stead, 2004).

3.8 Research Instruments

The study used questionnaires to collect primary data from the targeted respondents. The questionnaire had structured questions consisting of close-ended, multiple responses, Dichotomous, Scaled-response and Ranking type of questions. According to Struwig and Stead (2004), Likert type scale was linked to a number of statements to measure perceptions. Therefore, in this study, some of the research questions were constructed based on the standard Likert scale model (see Appendix A)

3.9 Procedure

The structured questionnaires were sent to the targeted respondents electronically and administered via email obtained from UbuntuNet Alliance website, conference attendance from respective NRENs and through online Lime Survey software which

was deployed through the University of Namibia (UNAM) domain to receive the responses.

3.10 Data Analysis

Struwig and Stead (2004) stated that in order to make sense of raw data, first it was necessary to summarise it. The data received from respondents were classified and tabulated and were imported into IBM SPSS 21 software for further analysis. Moreover, they stated that descriptive statistics provided statistical summaries of data. In support of this, descriptive statistical methods were used to identify and analyse the resources used to establish Cloud architecture framework for SADC NRENs. In addition, the authors Struwig and Stead (2004) stated that Correlation analysis was used to establish whether the variables were related to each other. In this study, Spearman's rho correlation techniques were used to explore the relationships between selected variables to obtain a numerical value for the strength of such correlations.

Thus, in this study, these techniques were used to establish the significant relationship between Cloud Service architecture with respect to security, Virtualization, interoperability, collaboration and availability in perspective of SADC NRENs. However, the ranking method was used to analyse the challenges identified in order to design the Cloud architecture framework. The graphs from the IBM SPSS 21 were exported to the Microsoft Excel and mapped to the table. Charts and graphs were used to analyse the tabulated results. The findings of the study identified the necessary

needs, challenges and the gaps that helped in designing the NRENs-CAF and are presented in chapter four of the research thesis.

3.11 Reliability and Validity

The research instruments were tested for content validity. Struwig and Stead (2004) defined content validity as "the extent to which the items reflect the theoretical content domain of the construct being measured". In view of this, the content validity was ensured in the study through literature review and was determined by experts' like supervisors and industry opinion in the development of the questionnaire. Furthermore, Struwig and Stead (2004) stated that test-retest reliability could be used to determine the degree to which the test scores were reliable.

In addition, they stated that the reliability of numerical experiment data could be strengthened by maximizing the data collection process and by maintaining consistency of the output. The questionnaire is developed under the guidance of the supervisor and piloted. The degree of agreement between the supervisor and the expert determined the reliability of the questionnaire. The questions were pre-tested using University students. After the piloting phase, the problem questions were adjusted for some slight ambiguities and other related issues in order to enhance the reliability and validity of the instrument. Welman et al. (2005) stated that if the research finding could be repeated, it is reliable. On the other note, Maree (2007) described reliability as the extent to which a measuring instrument is repeatable and consistent.

Henceforth, the inter-rated reliability is used to rate uniformity of the questionnaire. The online survey questionnaire is structured in such a way that only valid responses were captured from the respondent. Filtering is used to enhance valid responses for some particular questions which needed particular information. Before data analysis was done, data cleaning and consistency checks in the captured information were done through the use of cross-tabulations and frequency tables. Values that were inconsistent with what was expected for particular questions were dealt with accordingly, that is, either removed or corrected.

3.12 Research Ethics

Relevant permission concerning data collection was also obtained from the various NREN managements. Considering that SADC NRENs had different laws, rules, and practices, caution was taken to ensure that these regulations were not violated during the study. The purpose of the study was explained before commencing the interviews and administering the questionnaires. Respondents were also assured that the information provided would be treated with confidentiality and anonymity. The data collected was purely used for academic purposes. After the research is granted permission to go ahead with the data collection process, an official letter was obtained from the supervisor of an affiliated University. The purpose of the letter was to show potential respondents the authenticity of the study being carried out and constitute the ethical clearance by the institution. Sources for secondary data were acknowledged.

3.13 Conclusion

The chapter presented the methodology that was used in the study. The research design strategy, research design, sampling procedures, data collection methods and data analysis used in the study was explained. The research type was described and justified as quantitative. The reliability and validity of the questionnaire were affirmed. Finally, the ethical considerations during collecting data were indicated.

3.14 Summary

This chapter addressed the research design, population, sample and research instruments used to study the research questions. The research design described the quantitative research approach that is followed to answer the research questions. The quantitative research conducted used both explorative and survey study methods to gather data from the population. The population sample consisted of IT managers and staff that are responsible for their respective NRENs. The population sample is obtained using purposive sampling technique. The research instruments are developed to guide and assist in the processing of the data gathered that includes a study reference framework of existing models and structured questionnaire.

The following chapter discussed results and findings in relation to the research questions. Results of an in-depth analysis of SADC NRENs surveyed were presented in chapter four.

CHAPTER 4: RESEARCH FINDINGS

The chapter presented the statements of analysis for the data collected through qualitative and quantitative methods. The results of the study are reflected by way of tables, charts, graphs and statistical data to describe the information presented with a view towards answering the Research Questions.

4.1 Introduction

In this chapter, the results of the data analysis are presented. The data were collected and then processed in response to the problems posed in chapter one of this study. The research objectives drove the collection of data and hence data analysis and interpretation. The study focused on investigating the current state of various SADC NRENs' infrastructure and to identify the resources required as well as the challenges of integrating SADC NREN through NRENs-CAF. It identifies the gap and finally recommends a suitable ICI architecture.

The primary data analysis dealt with a detailed statistical analysis of the data followed by the presentation of results and findings. Data from the questionnaires was first coded and then entered into SPSS (Statistical Program for Social Scientists). In SPSS, descriptive statistics such as frequencies were used to establish the data structure. Then pie charts, bar graphs and histograms were generated in Microsoft Excel to present the data.

In this work, eight (8) SADC NRENs were purposively selected for the study. This was based on their NRENs formation, the infrastructure they had possessed and their willingness to answer the questions posed in the questionnaire. Two NRENs, namely: TENET and Xnet were considered as the prime participants. TENET had made substantial development locally and connected overseas to other NRENs through Geant or any other international Gateway point. On the other hand, Xnet was considered as it had limited development. Another reason for the choice of this NREN was the fact that it was also a Namibian NREN where the study was conducted.

4.2 Data Structure

There are a number of respondents from SADC NRENs. However, few responses outside SADC NRENs are also considered as shown in table 4.1.

Table 4.1: Statistics by respondents

COUNTRY	NAME OF THE NREN	NUMBER OF RESPONDENTS
SOUTH AFRICA	TENET	1
NAMIBIA	Xnet	2
ZAMBIA	ZAMREN	2
ETHIOPIA	EthERNet	2
MALAWI	MEDCOL	1
TANZANIA	TERNET	1
MOZAMBIQUE	MoRENet	1
KENYA	KENET	1
UGANDA	RENU	1
SUDAN	SudREN	1

4.2.1 Occupational Position of the NREN Respondents

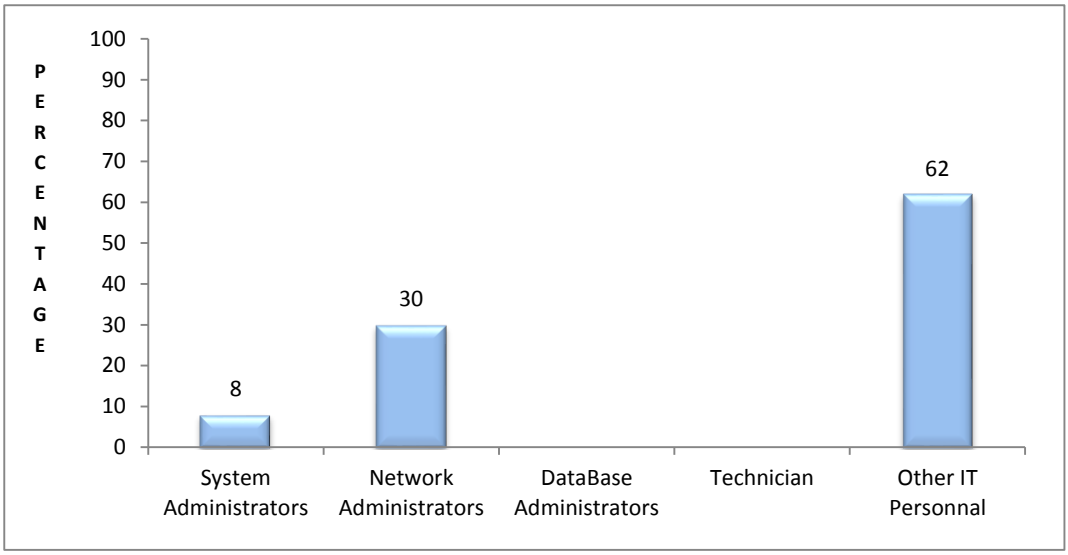

Figure 4.1: Occupational Position

Figure 4.1 illustrated the percentage of IT personnel by their occupational positions who participated in the study. The figure indicated that four (30.1%) of the respondents in the study were Network Administrators followed by System Administrators with one (7.7%). In addition, other IT personnel identified themselves as Trust Secretary, Chief Technical Officer (CTO), Managers, Directors, Chief Executive Officer were eight (61.5%) respectively; while none of the participants (0%) were Database Administrators and Technicians. The positions occupied by the respondents were directly relevant to the study because only high ranking employees provided critical information such as insight of their network architecture, policy details and confidential information. The other data were easily obtained from all IT personnel.

4.2.2 Size of the Population of the NREN

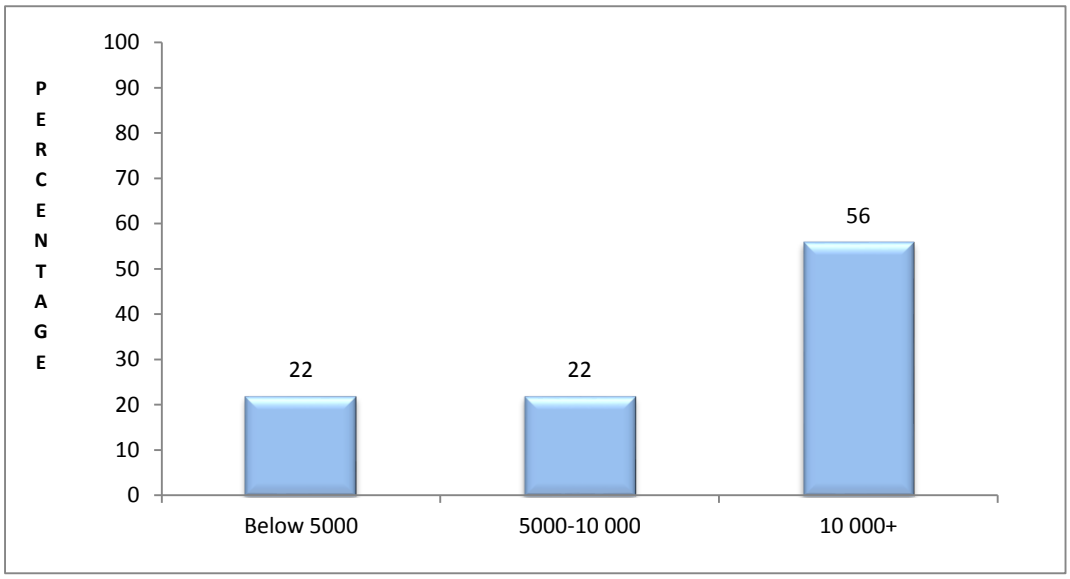

Figure 4.2: NREN Population

Figure 4.2 shows the size of the population from the connected campus networks of the respective NRENs. The NRENs that had below 5000 member institutions were two (22.4%) and between 50 000 and 10 000 were also at two (22.4%). The maximum size of the NRENs that had the size above 10 000 member institutions was ranked in five (56.1%). Four (30.8%) were missing values.

From Figure 4.2, it was notable that the size of the NRENs were growing. Hence, NRENs could take the opportunity to incorporate the benefits of the Cloud computing technology among its members. In addition, the data labeled on the graphs were approximations in relation to the population size of the surveyed NRENs.

4.2.3 NRENs with Cloud Computing Technology

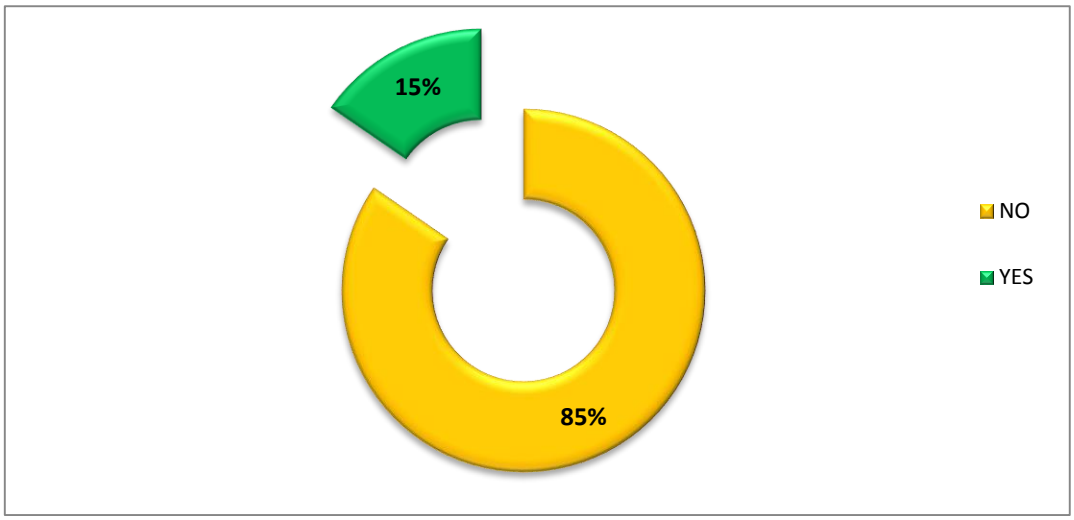

Figure 4.3: NREN on Cloud

According to Figure 4.3, only two (15.4%) of targeted respondents said their organisations had implemented Cloud technology while the majority of the respondents eleven (84.6%) confirmed that their NRENs had not deployed the technology.

From the Figure 4.3, it was noteworthy that the majority of NRENs have not adopted the Cloud computing technology Further from Figure 4.3, it was clear that very little effort was made by SADC NRENs to embrace Cloud technology. This is a good illustration of the successful startup of Cloud computing technology among SADC NRENs Therefore, the proposed Cloud architecture framework NRENs-CAF can allowed the SADC NRENs to use the new IT paradigm; Cloud computing technology.

4.2.4 IT Infrastructure/Technologies Used in NREN

Figure 4.4 depicted a clustered graph for the different Cloud computing technologies deployed in various NRENs.

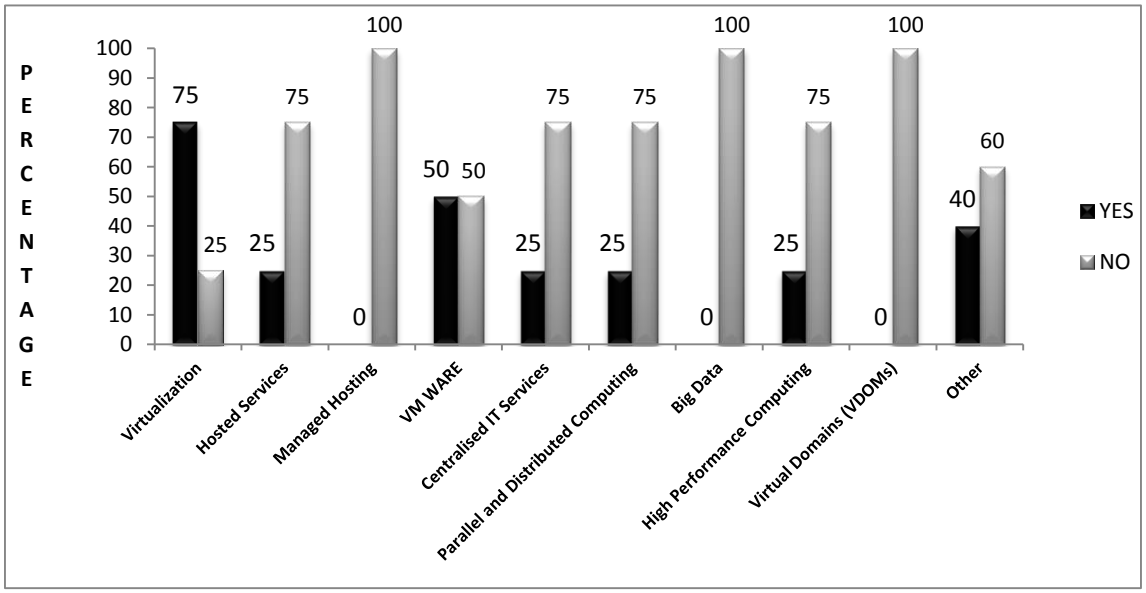

Figure 4.4: IT Infrastructure/Technologies

Each of the following sub categories for different infrastructure technologies was posed to the targeted respondents and the percentages presented above were in accordance with the Figure 4.4. Firstly, Virtualization, three (75%) of respondents ranked that their NREN utilized the technology and one (25%) indicated that they did not use it. Secondly, the Hosted Services, one (25%) of respondents indicated that their NRENs utilized the technology and three (75%) not. It was again observed from the figure that technologies such as Centralized IT services, Parallel and Distributed Computing and High Performance Computing (HPC) followed the same data pattern as Hosted services. Thirdly, with Managed Hosting, none (0%) of their NRENs utilized the technology. It

was also observed that Big Data and VDOMs also fell under the same category. Fourthly, with VMWARE, two (50%) respondents indicated that their NREN utilized the technology while the other (50%) did not use it. Finally, two (40%) respondents recorded that they used other kind of IT infrastructure and technologies.

Figure 4.4, indicated that IT infrastructure services used among responded NRENs were supportive of moving towards Cloud infrastructure. These technologies were used to support, or are served by Cloud Computing and not Cloud services by themselves. These are used to create the Cloud infrastructure. The researcher examined whether they were part of NREN so that creating a Cloud with existing technology could be easier.

4.2.5 Willingness of the NRENs to Deploy Cloud Computing Technology

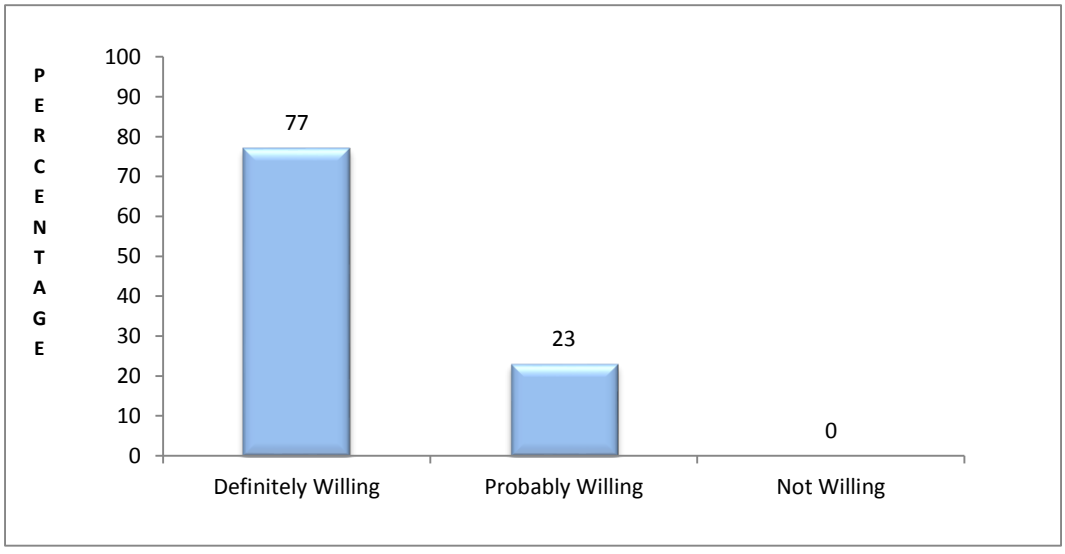

Figure 4.5: NRENs Willingness

Figure 4.5 shows the respondent's willingness to implement Cloud technology. Ten (76.9%) respondents pointed out that their NRENs were definitely willing to implement

Cloud technology while three (23.1%) responded as probably willing to adopt it. Due to the supportive IT infrastructure services as explained in Figure 4.4, most of the non-Cloud based SADC NRENs showed the willingness to adopt Cloud computing technology and services in their NRENs to provide shared IT platforms.

4.2.6 Effective Functioning of NRENs

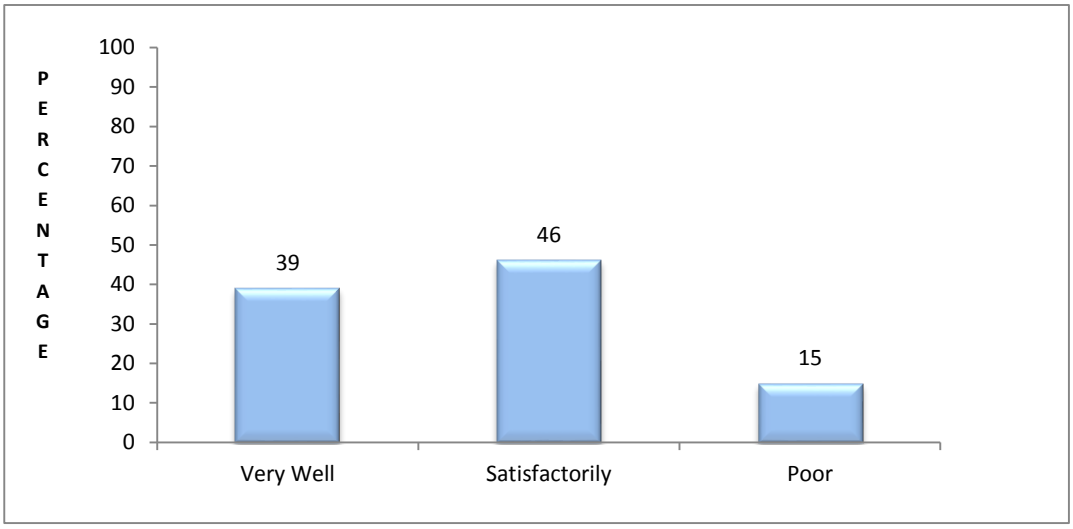

Figure 4.6: Functioning of the NRENs

The respondents were asked to express their opinions about the current functioning of their NRENs. Figure 4.6 shows that of all the participants who answered the question, the majority six of (46.2%) felt that their NREN were functioning satisfactorily, followed by very well scoring five (38.5%) and poorly functioning ranked at two (15.4%). In addition, Figure 4.6 shows that few NRENs are functioning with their traditional or non-cloud based IT infrastructure, nevertheless of limitations.

4.2.7 Collaboration with other NRENs

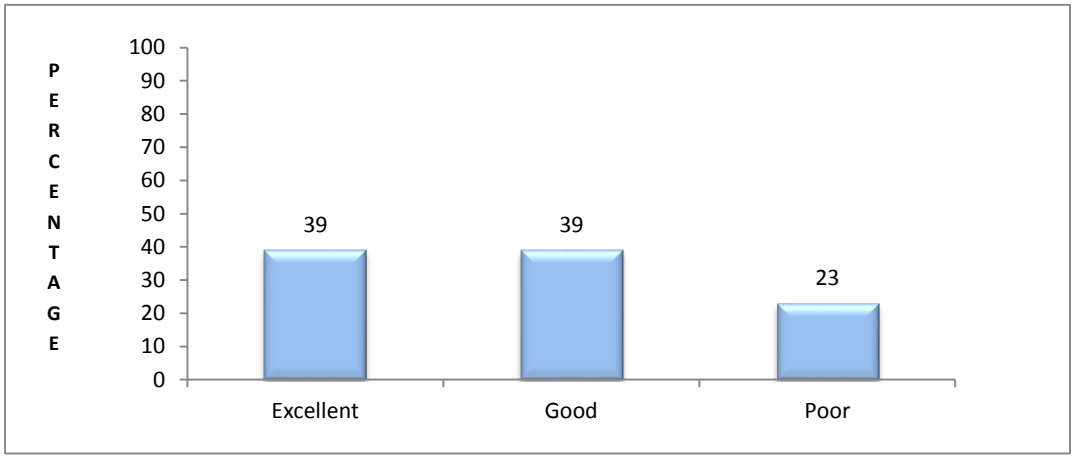

Figure 4.7: NRENs Collaboration

According to Figure 4.7, only five (38.5%) of NRENs had excellent and good collaboration while three (23.1%) were ranked poorly with their peer NRENs. Figure 4.7 informed that most of the SADC NRENs are functioning in isolation and hence the introduction of NRENs-CAF would improve communication and collaboration between NRENs.

4.2.8 Cloud Models Deployment by NREN

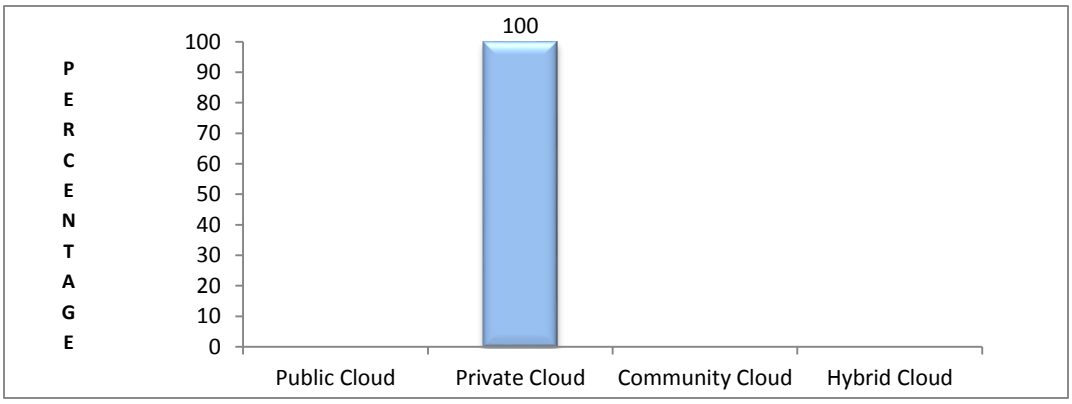

Figure 4.8: Cloud Models

Figure 4.8 shows that out of 15% who used Cloud technology among targeted respondents, 100% of them responded that they deployed private Cloud model. That is two (100%) respondents pointed out that their NRENs deployed private Cloud model. Again eleven (84.6%) did not respond or gave mislead answers. Furthermore, Figure 4.8 explained that the NRENs using Cloud have their own networking, computing and storage resources. This could provide Cloud services that can build its members to form consortia of NRENs. It was found that organisations feel confident when they store data internally because they have full control over it.

4.2.9 Cloud Services Delivery Models Used by NRENs

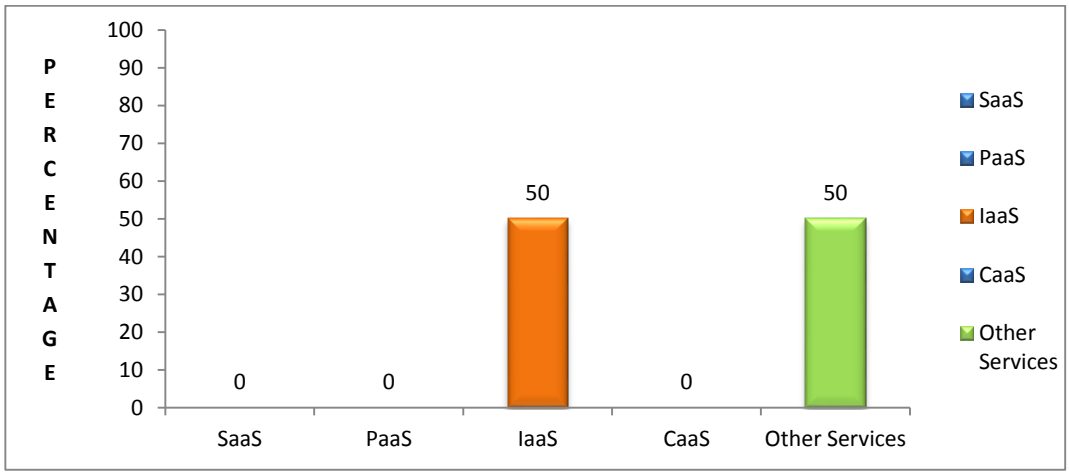

Figure 4.9: Cloud Service Models

Figure 4.9 shows that out of 15% who used Cloud technology among targeted respondents, one (49.7%) affirmed that they used IaaS service delivery models; while the other one (49.7%) declared that they used other types of Cloud service delivery models such as CaaS, NaaS or Anything-as-a-Service (XaaS). It is noted that none of

the organisations use SaaS or PaaS Systems (Around eleven (84.6%) did not respond or gave misled answers). Cloud computing can be utilized either for infrastructure, platform, network, communication, software or anything as a service (XaaS). It was noteworthy that IaaS is the core for creating private Clouds.

4.2.10 Reasons why NRENs had not Adopted Cloud Computing Technology.

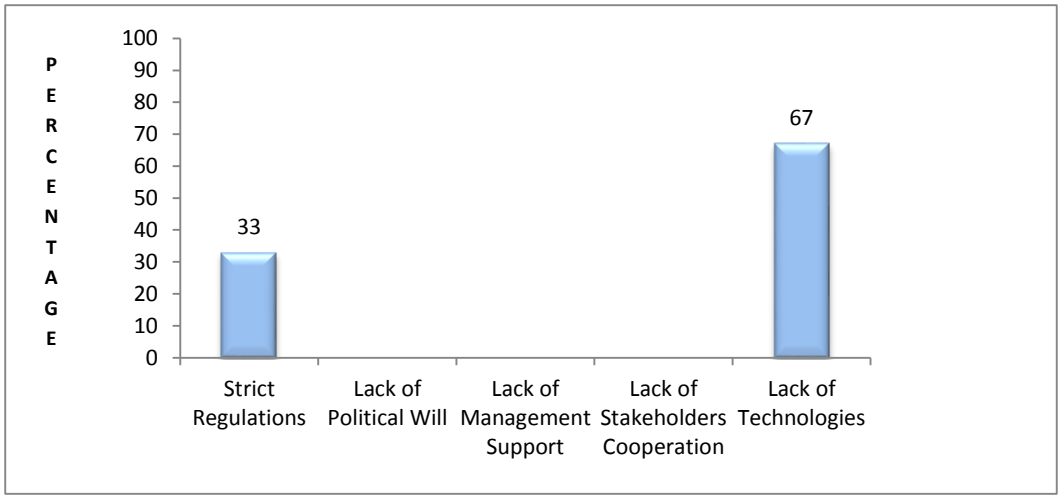

Figure 4.10: Reasons for NRENs not on Cloud

Figure 4.10 shows that, out of 15% who used Cloud technology among targeted respondents, four (66.5%) asserted that the reason for their NRENs not being embraced Cloud, were lack of technologies and the rest two (32.5%) reasoned as strict regulations. On the other hand, lack of political will, management support and stakeholders' cooperation were voiced at 0% and seven of 53.8% were missing values. From Figure 4.10, it is clear that backward compatibility in IT technology and compliance with legal

and regulatory ambiguity would not be a supportive variant for NRENs to adopt Cloud technology.

4.2.11 Steps and Factors to be considered by NRENs to Adopt Cloud Computing

The following section was categorized into two sub-categories, namely: the Steps and Factors to be taken into consideration by NRENs adoption to Cloud Computing.

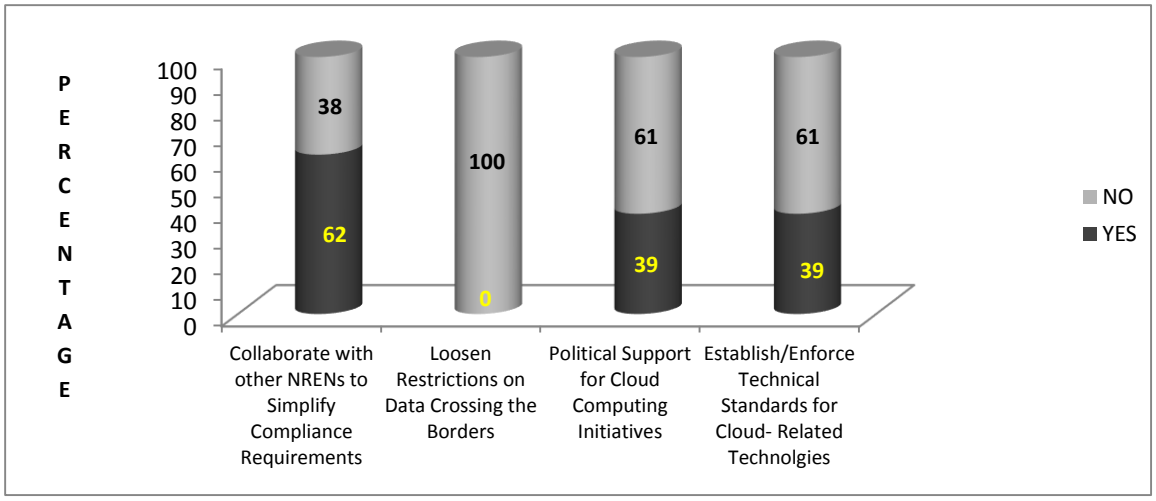

Figure 4.11a: Steps to be taken by NRENs to Adopt Cloud Computing

Figure 4.11a shows category 1 which dealt with the steps to be taken by NRENs to speed up NRENs adoption to Cloud computing. The Figure 4.11a indicates that the highest priority was given to Collaborate with other NRENs by simplifying the complexity of the compliance requirements, and it stood at eight (61.5%). Both stronger executive and political support for Cloud computing initiatives and establishing or

enforced technical standards for Cloud-related technologies stood at (38.5%) and none (0%) for loosening restrictions on customer or employee data crossing borders.

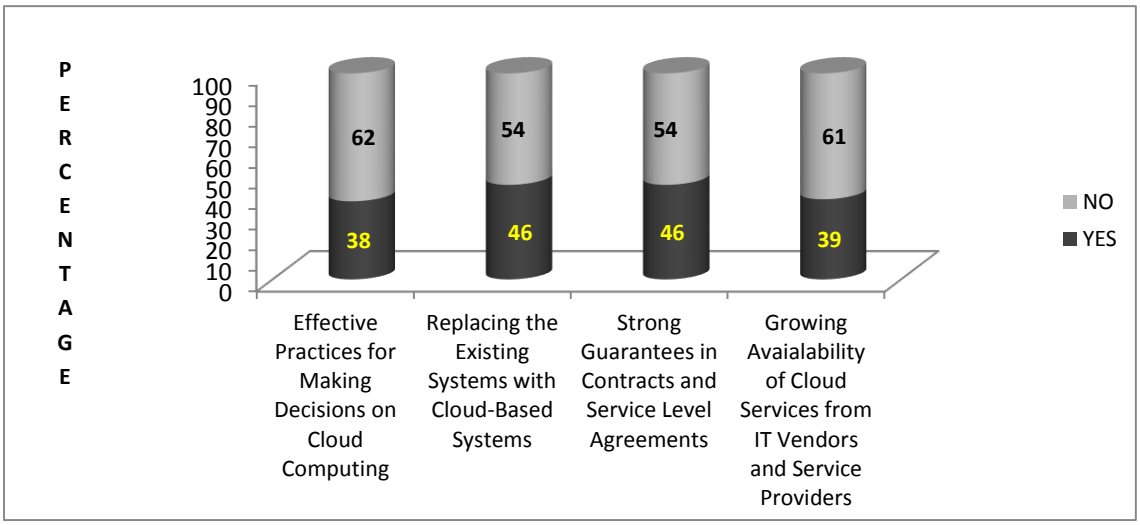

Figure 4.11b: Factors to be taken by NRENs to Adopt Cloud Computing

Figure 4.11b shows category 2 which dealt with the factors that would speed up NRENs adoption of Cloud computing. From the Figure 4.11b, it was evident that factors such as stronger executive support for Cloud computing initiatives, effective governance practices for making decisions on Cloud computing and growing availability of Cloud services from well-known IT vendors and service providers were all rated at five (38.5%). Furthermore, replacing and interoperating the non-cloud based IT systems with Cloud-based systems and stronger guarantees or protections in contracts and Service Level Agreements (SLA's) were rated at six (46.2%).

From Figure 4.11a and 4.11b, it is clear that the factors such as strong executive support for Cloud initiatives, establishment of standards for Cloud-related technologies, strong guarantees in contract, SLA's, effective governance practices for making decisions on Cloud computing, replacing the non-Cloud based IT systems to Cloud-based systems and to mention a few, would speed up NRENs adaptation of Cloud Computing.

4.2.12 Benefits and Purpose of Cloud Services in NRENs

The following section was categorized into two sub-categories, namely: the benefits and purpose of employing Cloud services in NRENs. Each category was posed to the targeted respondents and was asked to rate the levels of benefits and purpose.

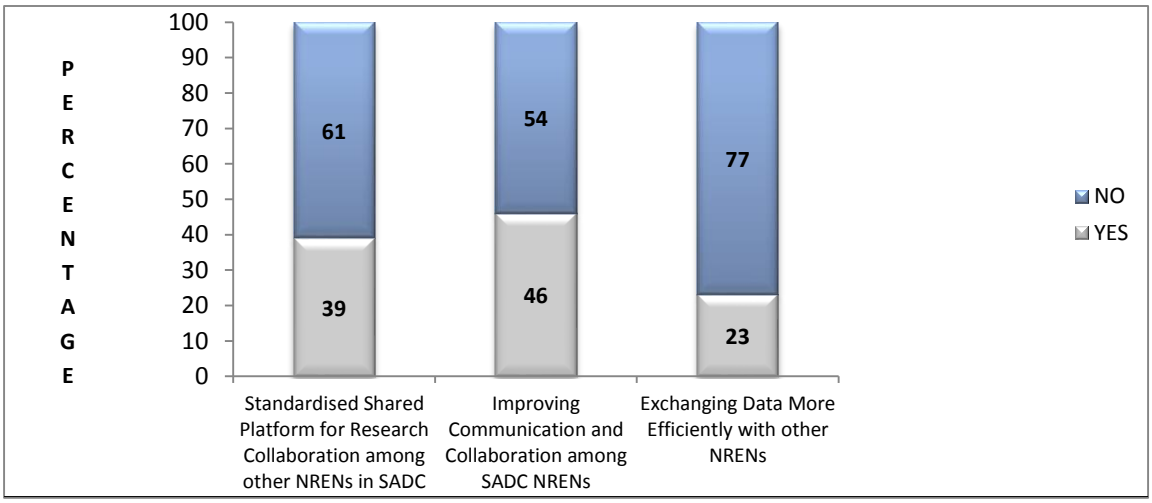

Figure 4.12a: Benefits of Cloud Services in NREN

Figure 4.12a shows category 1 which was the benefits of Cloud services. Out of 15% who used Cloud technology, around five (39%) were in favour of providing a standardized shared platform for research collaboration. About six (46%) ranked for

improving communication and collaboration among other NRENs in SADC and its users and three (23%) rated for exchanging data more efficiently with outside organization.

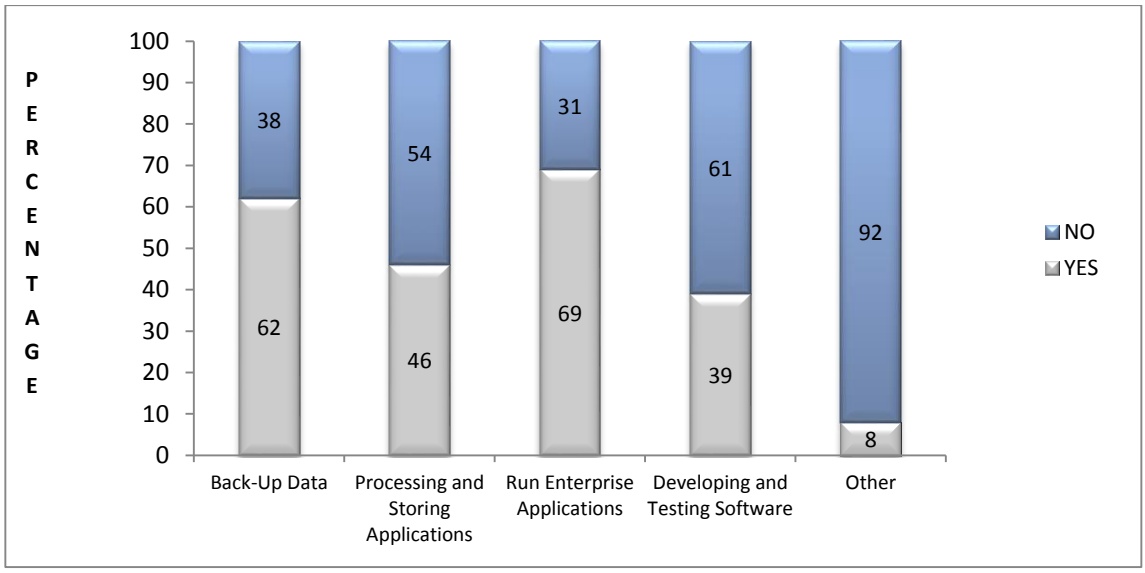

Figure 4.12b: Purpose of Cloud Services in NREN

Figure 4.12b shows category 2 which was the purpose of using Cloud services. About eight (62%) indicated that they used Cloud computing for backing up data, six (46%) use for processing and storing applications, nine (69%) for running enterprise applications, five (39%) use for developing and testing software and one (8%) claimed they used Cloud computing for other purposes.

Figure 4.12a and 4.12b explained that the important benefits of using Cloud services were improving communication and collaboration between NRENs, providing a standardised platform, exchange data more efficiently with other NRENs and reducing capital expenditures.

4.2.13 Security Provided by CSP

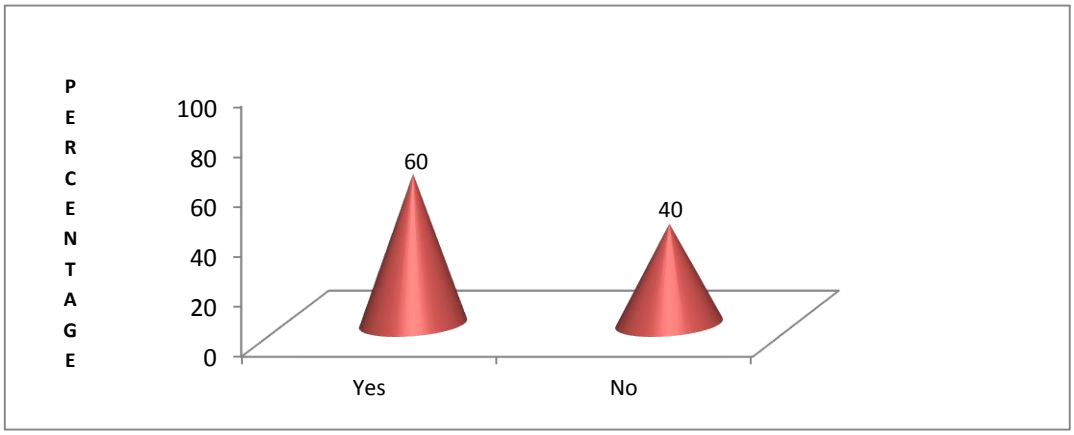

Figure 4.13: CSP Security

Figure 4.13 shows that out of 15% who used Cloud technology the respondents indicated three (60%) of satisfaction on security issues provided by Cloud providers and two (40%) of non-satisfaction was shown. Eight (61.5%) were missing values.

4.2.14 Concerns About Security Issues when NRENs were Using Cloud Services

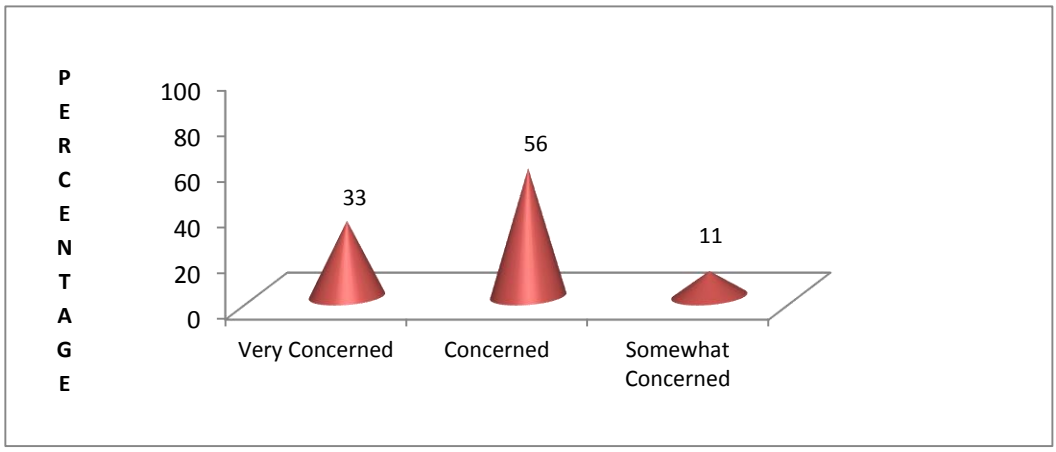

Figure 4.14: Security Concerns

From Figure 4.14 above, the severity of concern over Cloud security fluctuated from

different NRENs respondents. However, out of 15% who used Cloud technology majority five (55.6%) pointed out concerned about the security features, functionality and performance of Cloud services. Nearly three (33.13%) were very concerned and minimum of one (11.3%) were somewhat concerned about the security provided by CSP. Four of (30.8%) were missing values.

NRENs that were on Cloud are concerned with challenges to their data integrity and confidentiality issues on the Cloud. Organisations feel confident when they store data internally because they have full control over it. Although there is no guarantee that data is better protected internally compared to the public Cloud. In fact, there is a possibility that data could be even safer in the public Cloud because public Cloud providers may pose a higher level of data security expertise as compared to their customers.

4.2.15 Security Measures Applied to NRENs

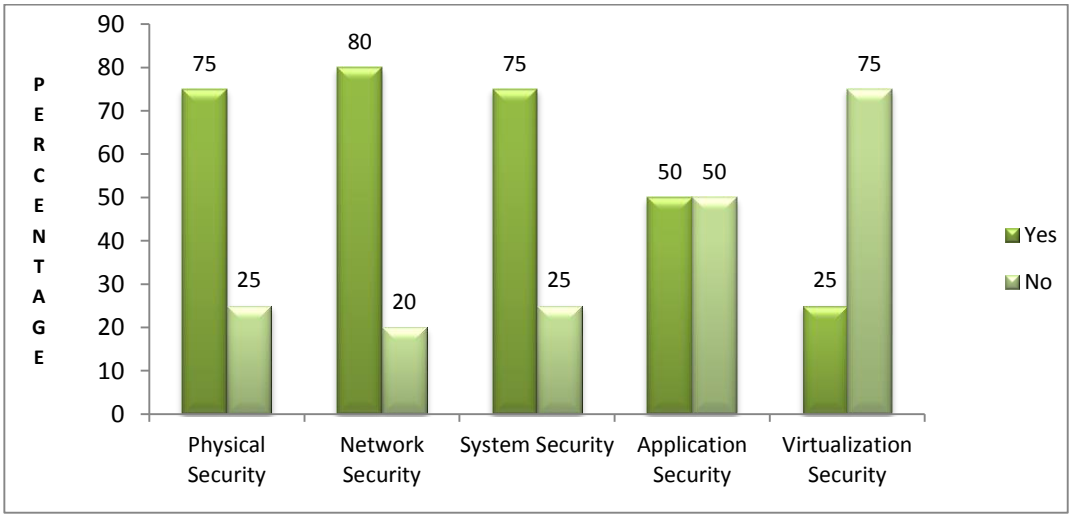

Figure 4.15: Type of Security Measures

As depicted in Figure 4.15, out of 15% who used Cloud technology, 75% voiced that they used Physical and System Security whereas 25% said they did not incorporate those measures. About 80% of them used Network Security and 20% not. Again, 50% said that they used Application Security while 50% said they did not. Furthermore, it was evident that 25% NRENs were using Virtualization Security while 75% did not.

4.2.16 Network Architecture Scalability

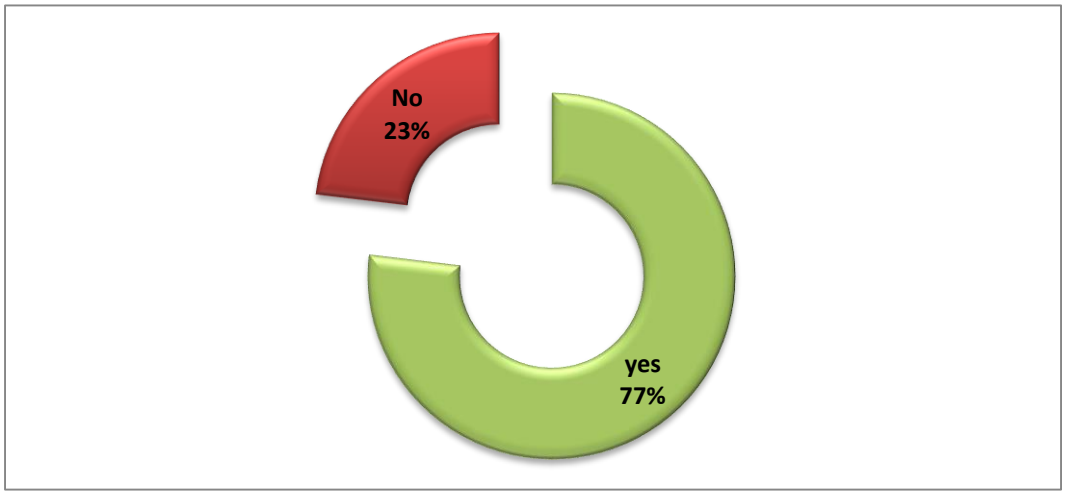

Figure 4.16: Scalability

From Figure 4.16, it was evident that ten (76.9%) marked their network architecture scalable and three (23.1%) marked them as non-scalable. However, one of the prerequisites for deploying applications on the Cloud is that it should be dynamically scalable on demand architecture for optimum performance. Scalability is the capability of a network, to handle a growing topology and the amount of traffic.

4.2.17 Type of Scalable Architectures Used in NRENs

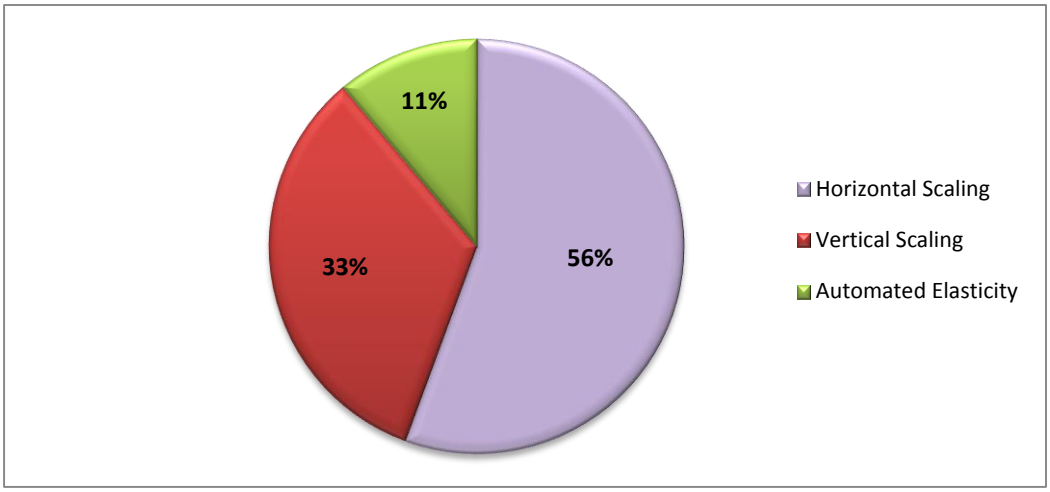

Figure 4.17: Network Scalable Architecture

Figure 4.17 shows that five (55.6%) of NRENs adopted Horizontal Scaling, whereas, three (33.1%) used Vertical Scaling and one (10.7%) used Automated Scaling. Four (30.8%) were missing values.

The scalable architecture was being able to scale on demand, providing for high availability, resiliency and having sufficient safeguards against failures. Scalable architectures are responsible for balancing the incoming traffic among compute instances in the Cloud. Further, the load balancer will automatically forward network traffic to other servers increasing the performance and the computational capacity without affecting other network/system components.

4.2.18 Governance Issues Would be Considered while Providing Cloud Services

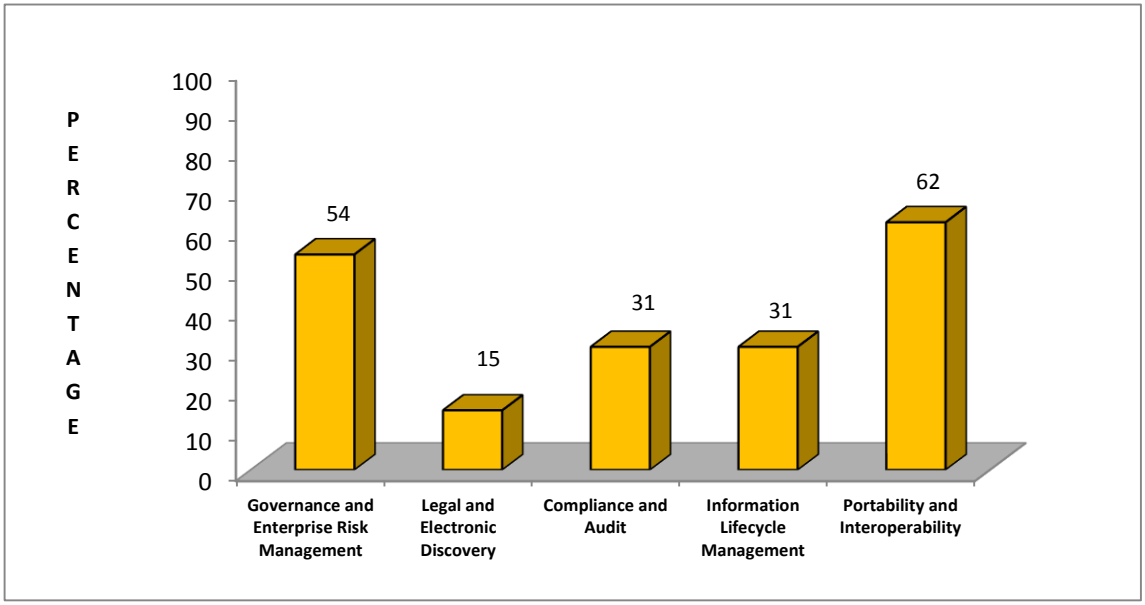

Figure 4.18: Governance Issues

Figure 4.18 shows that among all the targeted respondents who answered the question, it was evident that governance and risk management were ranked seven (53.8%). Legal or regulatory and electronic discovery were at two (15.4%). The compliance with legal regulatory and auditing requirements was ranked at four (30.8%), information lifecycle management was rated at four (30.8%). Portability and interoperability were ranked the maximum at eight (61.8%). From Figure 4.18 it was clear that if the NRENs were to be connected across the border, the need of legal and compliance, Governments regulatory, SLA's and governance were a few issues that played a major role. Further, such mandatory terms and conditions are necessary to regulate the ease of technology exchange crossing the borders of the NRENs countries, for data security and availability of service.

4.2.19 Measures to Address Interoperability Issues

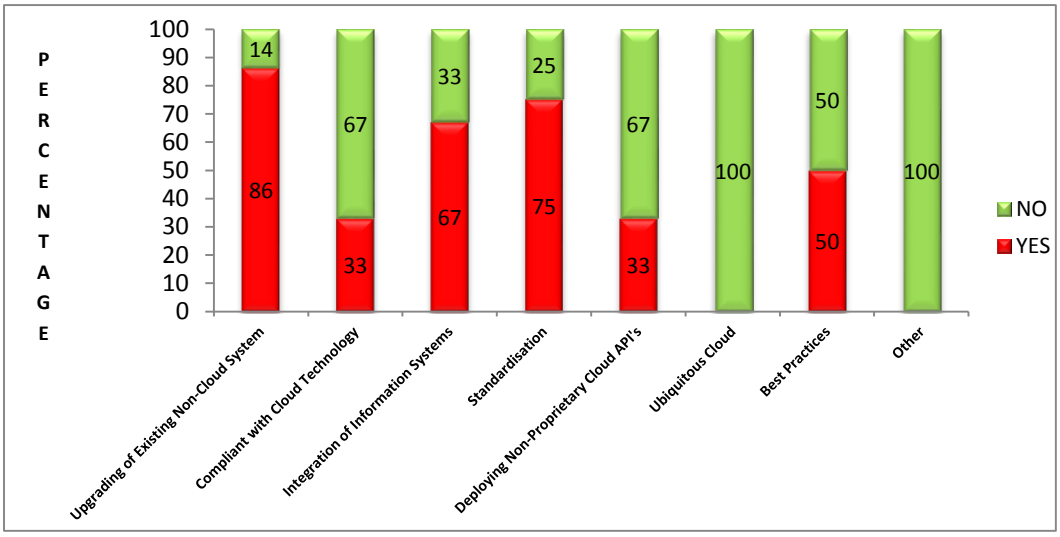

Figure 4.19: Interoperability Issues

Figure 4.19 shows all the targeted respondents who answered the questions. About 86% was asserted that upgrading of the existing non-cloud IT systems as prime measure should be taken to address Interoperability issues. In addition, about 33% was ranked for an overhaul of major parts of the infrastructure to compliant with the Cloud technology and deploying non-proprietary Cloud API's. Integration of Information Systems stood at 67%. Standardization was another major issue to address Interoperability and was indicated at 75%. Adopting best Interoperable practices stood at 50%. Ubiquitous nature of the Cloud and other measures were opted (0%).

Figure 4.19 shows that Interoperability between disjoint technologies would be a challenge to transform non-cloud based technology to Cloud technology. Other

technical concerns include the integration of Cloud computing technology with existing systems and a lack of industry standards.

4.2.20 Rate of Challenges Ascribed to Cloud.

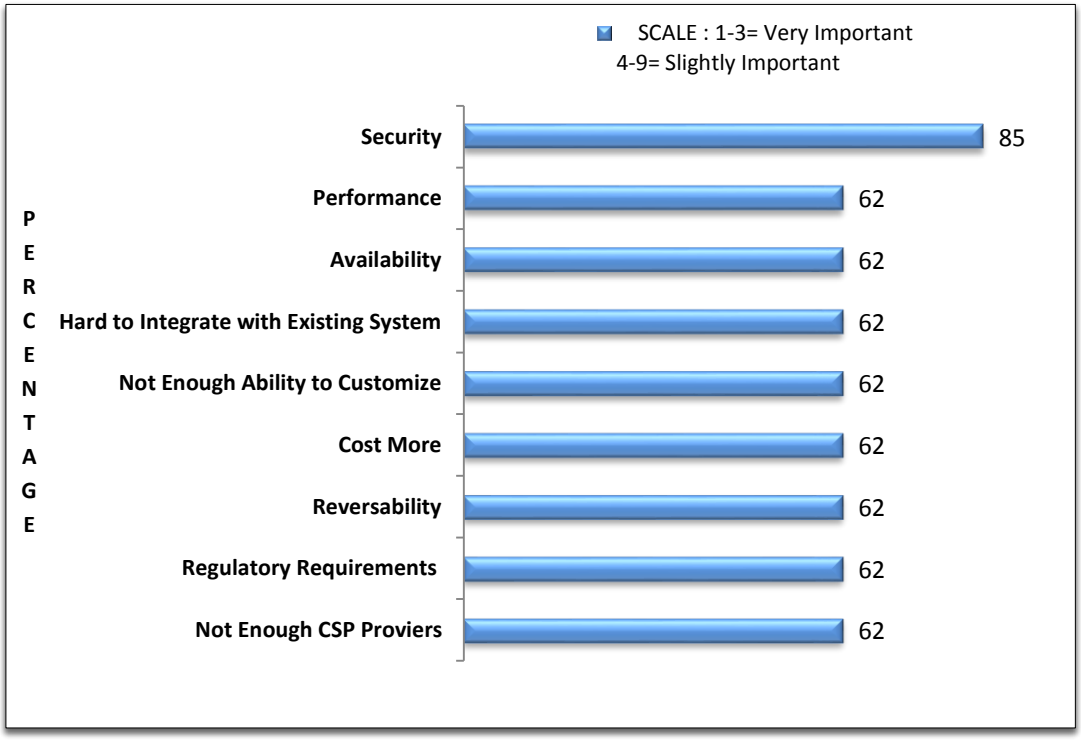

Figure 4.20: Challenges

Figure 4.20 shows how the targeted respondents judged the following statistical figures of challenges pertaining to Cloud computing. Out of 15% who used Cloud technology, Security was highlighted by eleven (85%) of the respondents. Whilst availability, hard to integrate with existing IT systems, inadequate ability to customise, on demand cost, reversibility, regulatory requirements and not enough Cloud suppliers were all ranked at two (62%).

It is clear from Figure 4.20 that although many concerns like cost, availability, performance, compliance, regulatory issues are related to Cloud, but major concerns were about securing and Integrity of their data and ownership of the IT infrastructure. The main concerns for SADC NRENs stakeholders were the availability of high-speed access, followed by the issue of systems security. It is also noteworthy that issues pertaining to data protection ranked high that call for significant improvements as to ensure high-quality access to Cloud computing services. Infrastructures, high speed networks and data centres once again confirmed the prerequisites for the success of Cloud computing

4.3 Summary

The analyses of the data gathered from questionnaire and results of an in-depth analysis of SADC NRENs surveyed were presented in this chapter. The data analysis focused on the questionnaire perceptions of the current status of SADC NRENs. Further, addressing what resources can be used to establish institutional Cloud infrastructure and the challenges faced by SADC NRENs with regards to establishing institutional Cloud services.

The next chapter emphasized on the related discussions focused on establishing relationships between variables and discussed the findings for each sub-research questions in relation to the findings. This chapter interpreted some of the results and relationships found during Data Analysis.

CHAPTER 5: DATA ANALYSIS AND DISCUSSION

The Chapter discussed the data analysis findings of the study. It also interpreted some of the results and relationships found during Data Analysis.

5.1 Statistical Inferences (Correlation of variables)

The coded data was analyzed by means of Spearman's correlation analysis at significance level of 0.05 in order to determine the significant relationship of the variables such as; security, Interoperability, availability, collaboration and Virtualization. These variables were interpreted accordingly and were possibly linked to literature review to gain a full understanding of both primary research data and secondary research.

Table 5.1: Correlation between Virtualization and Security

Correlation of Virtualization and Security			Virtualization	Security
Spearman's rho	Virtualization	Correlation Coefficient	1.000	-.272
		Sig. (2-tailed)		.728
		N	4	4
	Security	Correlation Coefficient	-.272	1.000
		Sig. (2-tailed)	.728	
		N	4	13

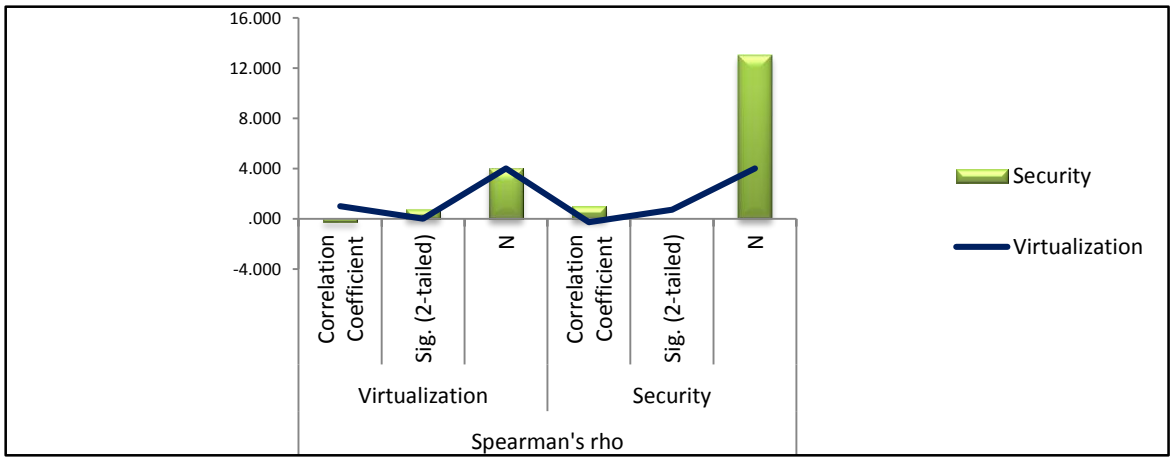

Figure 5.1: Virtualization versus Security

Table 5.1 was mapped onto the graph as shown in Figure 5.1. From the figure, it is clear that there is a significant relationship between Virtualization and Security. Based on the Figure 5.1, it is evident that with the increased use of Virtualization, security concerns also increases; which are also indicated by the respondents (Figure 4.20). According to Demchenko, Ngo, de Laat, Wlodarczyk, Rong, and Ziegler (2011), Dynamically provisioned Access Control Infrastructure (DACI) supports and build consistent security services provisioned on-demand. Further, Ngo et al. (2012) stated that acquisition of security infrastructure recommendations, Dynamic Access Control Infrastructure recommendations (DACI) which made it more efficient to manage security related information that created consistent security infrastructure on-demand systems. Subsequently, the study recommended an integrative architecture to ensure data security and integrity through secured TCSF component in the NRENs-CAF framework (refer to Figure 6.1).

Table 5.2: Correlation Between Virtualization and Availability

Correlations of Virtualization and Availability			Virtualization	Availability
Spearman's rho	Virtualization	Correlation Coefficient	1.000	.816
		Sig. (2-tailed)		.184
		N	4	4
	Availability	Correlation Coefficient	.816	1.000
		Sig. (2-tailed)	.184	
		N	4	10

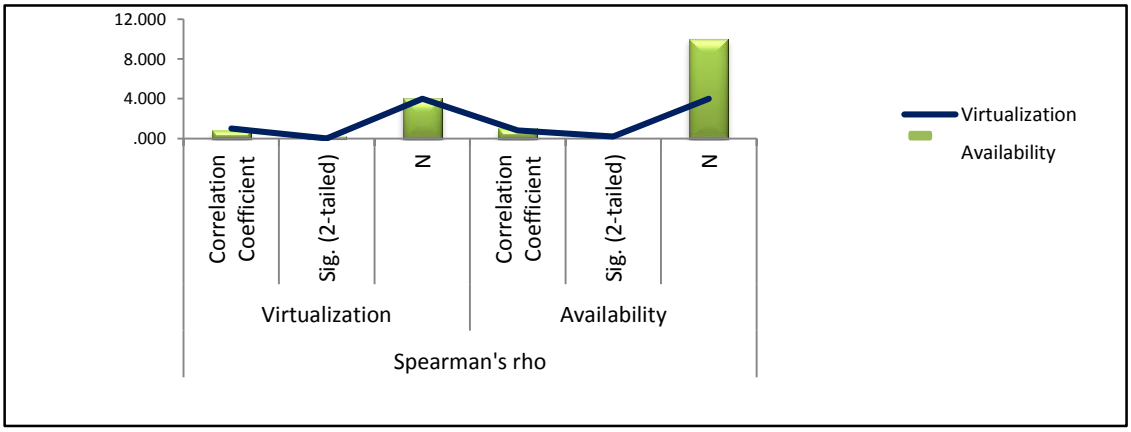

Figure 5.2: Virtualization versus Availability

Figure 5.2 was derived from the correlation Table 5.2. It was clear that Virtualization and availability had directly proportional relation. This implies that the Virtualization increases Availability. Figure 4.20 shows that 62% of respondents stated that their major concern was Availability which was slowing their NRENs ability to deploy Cloud computing technologies. This stresses the need for NRENs-CAF that recommended the integration of the best practices in line with Triad C.I.A model (see section 2.7, 2.8 &

Appendix C), where availability of resources at all-time was ensured without experiencing the downtime.

Table 5.3: Correlation Between Standardisation and Interoperability

Correlation of Standardisation and Interoperability			Standardisation	Interoperability
Spearman's rho	Standardisation	Correlation Coefficient	1.000	
		Sig. (2-tailed)		
		N	12	8
	Interoperability	Correlation Coefficient		
		Sig. (2-tailed)		
		N	8	8

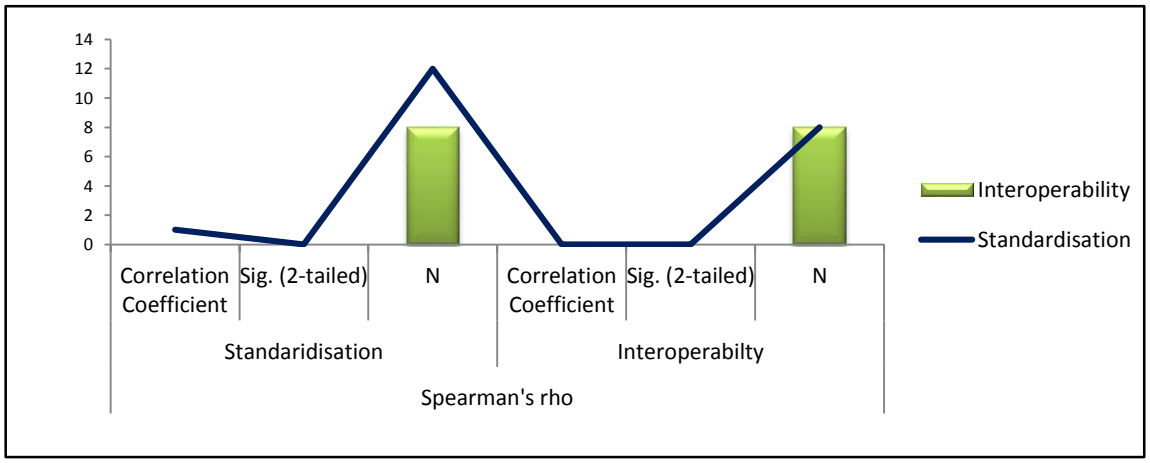

Figure 5.3: Standardisation versus Interoperability

The correlation Table 5.3 was plotted in Figure 5.3 where Standardisation and Interoperability had a significant relation to each other. However, referring to Figure 4.19, it was observed that 75% of respondents agreed with that. In addition, the best practice of IEEE InterCloud Working Group (IEEE P2302) explained that Standards

created a consistent platform or infrastructure to make interoperability more viable. Hence, NRENs-CAF adopted those recommendations from Cloud standardization models (see section 2.7 & 2.8) to integrate CFS component (Figure 6.1) to ensure better interoperability between organisations and among themselves.

Table 5.4: Correlation Between Virtualization and Collaboration

Correlation between Virtualization and Collaboration			Virtualization	Collaboration
Spearman's rho	Virtualization	Correlation Coefficient	1.000	-1.000**
		Sig. (2-tailed)		
		N	4	4
	Collaboration	Correlation Coefficient	-1.000**	1.000
		Sig. (2-tailed)		
		N	4	13

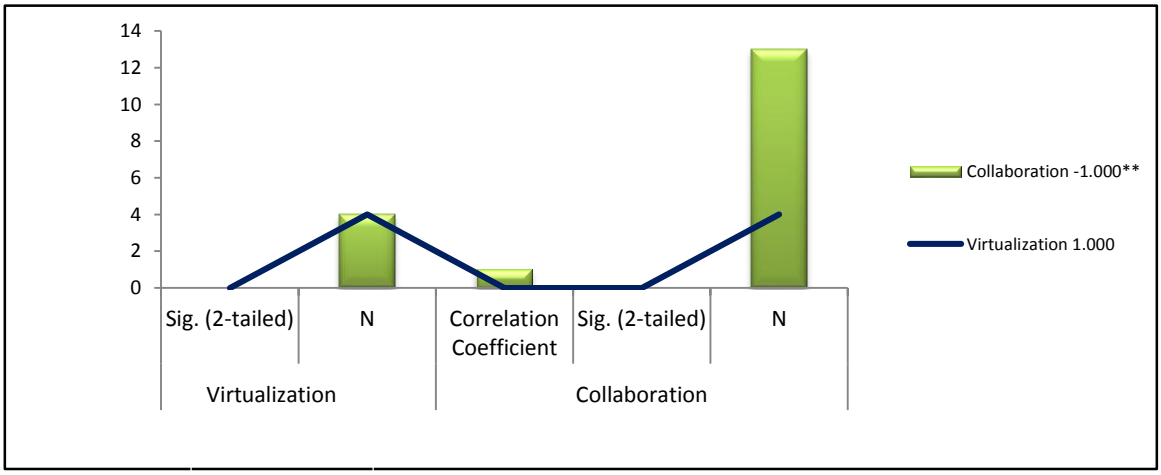

Figure 5.4: Correlation Comparing Virtualization and Collaboration

Figure 5.4 which is the graphical representation of Table 5.4 indicated that Collaboration improved with Virtualization technology among NRENs. As it is evident in Figure 4.12a, Cloud services benefits in improved collaboration. Furthermore, from Figure 4.7 it was noted that only 62% of the organisations indicated that they would like to form collaborations. Consequently, collaboration would improve the mobility of resources from one location to another, provided by Virtualization. In addition, resource sharing was much simpler in Virtualization technology which is one of the solutions to Cloud computing, compared to traditional or non-cloud based technology.

5.2 Discussions

This section discussed the findings for each sub-research questions that addressed resources that could be used, challenges faced by SADC NRENs and Cloud infrastructure suitable to establish NRENs-CAF for SADC NRENs from the data analysis and findings of the study that drove the designing of the proposed architecture.

5.2.1 Resources

According to Figure 4.6, 46% of the total number of respondents who used Cloud technology indicated that their NRENs were functioning satisfactorily. About 39% of NRENs had excellent collaboration with other NRENs; whilst, 15% indicated that they had poor collaboration with their peer NRENs as shown in Figure 4.7. The reasons for that seemed to be poor resources such as internet connectivity, lack of human resources, funding, political will, strict regulations, restrictions on data crossing the borders, lack

of technical standards that support Cloud technologies, Compatibility with the existing systems, Strong SLA's, interoperability, not enough CSP's footprint in their nations, economic reasons and so on (Figure 4.10, Figure 4.11(a), Figure 4.11(b), Figure 4.20, Figure 5.5 and section 2.5). Consequently, the findings were in support of Karanja (2006) who recommended the initiative of forming NRENs consortium to purchase bandwidth by negotiating a bulk discount, associated with lowering of price on acquiring of ICT services. Further, ITU (2012) recommended that in order to significantly reduce the costs of bandwidth and also to improve the speed of access to Cloud computing resources, it was strongly encouraged the adoption of Cloud computing and the establishment of data centres in Africa. This will reduce the costs of access to services and improve service quality.

In addition, out of the total respondents who used Cloud technology, 75% respondents indicated that their NRENs utilized Virtualization technology(s) as shown in Figure 4.4. The researcher further observed that NRENs which were not on Cloud shows 77% of willingness to deploy Cloud Computing technology as presented in Figure 4.5. Hence, those NRENs which displayed that they already deployed some Virtualization technologies gives much better preparedness and facilitates adaptation of Cloud computing system much faster. On the other hand, NRENs-CAF would facilitate those NRENs willing to deploy Cloud technology.

5.2.1.1 Cloud Deployment and Service Delivery Models

From Figure 4.8 and 4.9, it was clear that the NRENs, which were on Cloud, deployed private Cloud with IaaS model. According to Mather et al. (2009), SPI was an acronym that represented the three major services provided in public Cloud computing: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). They also stated that IaaS was the fundamental platform for any Cloud system. According to ITU (2012), Cloud computing can be utilized for infrastructure, platform, network, communication, software or anything as a service (XaaS). It was noteworthy that IaaS is the core for creating any private Clouds. However, NRENs-CAF recommended provisioning XaaS as a service delivery to its member NRENs.

5.2.1.2 Reasons and Steps for NRENs to Adopt Cloud

The study revealed that some NRENs that were not on Cloud, reasoned out that strict regulations and lack of technologies were the factors hindering the adaptation of Cloud as shown in Figure 4.10 and 4.11. Such restrictions hindered the NREN organisations' preparedness for technology infrastructure towards Cloud computing. Steps such as (i) upgrading from traditional IT infrastructure, (ii) collaborating with other NRENs to simplify compliance requirements, (iii) relaxing of restrictions on data crossing the borders, (iv) establishing political and management support for Cloud initiatives, and (v) having strong guarantees in contracts and SLA's, to mention a few were done in consultations with IT industry, Cloud users and International Standards bodies. This

clarified the rules by which organisations must have operated and enabled them to move forward.

5.2.1.3 Benefits and Purpose that NRENs Use Cloud Computing

An interesting finding of this study was that NRENs explored Cloud services to improve communication and collaboration by exchanging resources more efficiently. This also stemmed from the need for a standardised platform to run enterprise software applications, within and among outside NRENs.

5.2.2 Challenges faced by SADC NRENs in adapting Cloud Computing

The study revealed that 15% of the total number of respondents used Cloud technology, while 85% of the NRENs did not implement Cloud technology as illustrated in Figure 4.3. Some of the reasons for that were associated with the factors or challenges such as security, availability, integrity, performance, cost, interoperability, governance (see Appendix D). Figure 5.5 summarised the research findings of Figure 4.18 and 4.2, which illustrated the ranking of various Cloud computing challenges that have bearings on the proposed solution. Table 5.5 indicates the summary of all the research findings with respect to the challenges faced by SADC NRENs in adopting Cloud computing technology.

Table 5.5: Summary of Challenges faced by SADC NRENs in adapting Cloud computing Technology

Security	Availability	Performance	Lack of Interoperability standards	Hard to Integrate with Existing System	Cost More	Governance	Regulatory Requirements
85%	62%	62%	75%	62%	62%	75%	62%

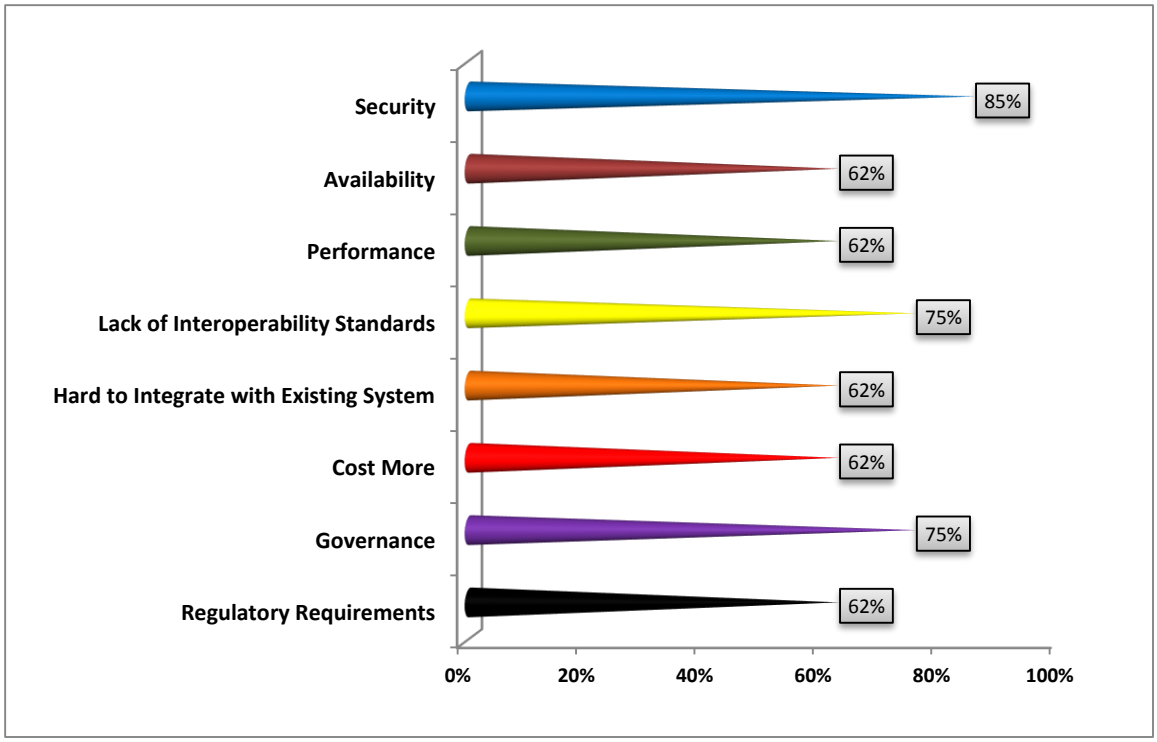

Figure 5.5: Challenges faced by SADC NRENs in adapting Cloud Computing

From the survey conducted, Figure 5.5 outlined the perceived challenges and issues associated with Cloud computing (Table 5.5) and on-demand computing models from a total of thirteen (13) respondents among eight (8) NRENS. The data in Figure 5.5 shows

that security concerns were the highest among the respondents with a majority of the test group responding with a scale of four (4) being slightly concerned, to one (1) being very concerned as shown in Figure 4.20. The reason would be the trust with the CSP on their data and also, the NRENs felt insecure about losing their ownership of their data. It was recommended that the trust would be established through strict and guaranteed contracts in SLA's. Although security concerns form the biggest challenge, problems associated with availability, performance, cost, interoperability and regulatory issues were very close to security issues. These are also the perceived set of challenges associated with Cloud adoption (Sultan, 2010).

From the available data, it was also notable to see that integration and rollback issues, as well as the lack of standards and difficulty in customization, were among the prominent concerns. The very same challenges made adoption of Cloud or on-demand computing models more difficult. In reference to the above, Kuyoro et al. (2011) presented the statistical evidence by stating that with regard to the development of Cloud computing in Africa, the main concern for their stakeholders was the availability of high-speed access and followed by issues of security.

The study also revealed that 85% of the respondents felt that these very challenges played a major role in slowing down the acceptance of Cloud computing technology in their NRENs. From these statistics, it was deduced that SADC NRENs were actually inclined and taking active initiative towards Cloud implementation.

5.2.3 Architecture

According to Figure 4.5, around ten (77%) of respondents pointed out that their NRENs were definitely willing to implement Cloud technology. Figure 4.8 shows that out of 15% who used Cloud technology among targeted respondents voiced that they deployed a private Cloud model. It is to be noted that this is inaccurate as they were found using Public Cloud services rendered by Google Apps, Dropbox etc., from many other service providers.

Figure 4.18, shows that about 31% respondents expressed their concern on the need for strong information lifecycle management while providing network services. In addition, affirming that lack of lifecycle management practices would adversely affect the privacy of data over the Cloud.

Based on the results and findings (chapter 4) and section 5.2 (chapter 5), it was found that it is necessary to design an architectural framework NRENs-CAF connecting SADC NRENs community on a common Cloud infrastructure associated with Cloud computing standards (section 2.7) and existing frameworks (section 2.8). Since most IT infrastructure is heterogeneous including their workstations and servers, the existing framework (section 2.8) is suitable to deal with such heterogeneity to maximize resource utilization in an effective manner. NRENs-CAF also adopts few components from the Cloud standardization framework (section 2.7) and was built on the service-oriented architecture which gave its extensibility to integrate different types of Clouds. Mainly, different standards and recommendations were used as best practices reference models

(section 2.7 & 2.8) in this study. Below a few of the different standards and recommendations are listed:

- IEEE P2302 Working Group recently published a draft Standard on InterCloud Interoperability and Federation (SIIF) that proposed an architecture that defined topologies, functions, and governance for Cloud-to-Cloud interoperability and federation (Ortiz, 2011).

- NIST SP 500-292, Cloud Computing Reference Architecture v1.0 were NIST was active in fostering Cloud computing practices that supported interoperability, portability, and security requirements that were appropriate and achievable for important usage scenarios (Liu et al., 2011). In view of the above, NIST standards gave specific recommendations for Cloud computing Technology.

- The ITU-T Focus Group on Cloud Computing (FG-Cloud) was established to identify the telecommunication aspects, i.e. the transport via telecommunication networks, security aspects of telecommunications, service requirements and so on, in order to support Cloud services/applications and suggest the further studies and ITU-T standardization activities (Bernstein, Ludwigson, Sankar, Diamond, & Marrow, 2009). In view of that ITU-T focused on standarisation or Telecommunications network infrastructure for the optimization of Cloud systems. In addition, ITU-T Cloud Network Infrastructure model provided

suggestions for Cloud network topology designed and defined for the Virtualized network components such as Cloud switch and routers (Bureau, 2010).

Therefore, data was analysed for the resources required, services offered, interoperability architecture and network topology required in the future.

The interpretation of results as presented in chapter four and the statistical inference in chapter five had implications on the current investigation and the proposed framework NRENs-CAF. This framework stresses more on the resources needed and the challenges. Subsequently, the study recommends suitable integrative service oriented Cloud architecture framework to ensure data integrity through secured NRENs-CAF architecture as shown in Figure 6.1.

5.3 Summary

The data analyses findings of Chapter 4 were discussed and presented in this chapter in relation to the three research questions and objectives posed in this thesis.

The following chapter presented a proposed theoretical Cloud architectural framework named NRENs-CAF model created from the data analysis findings and relevant literature review.

CHAPTER 6: PROPOSED NRENs CLOUD ARCHITECTURE FRAMEWORK (NRENs-CAF) FOR SADC NRENs

The Chapter introduced the overlay of proposed Institutional Cloud architecture Framework and its layered architecture. It further discussed the components in the architecture; their operations and functionality. The architecture enhanced Cloud connectivity among national research education networks in SADC NRENs. Furthermore, the content of the Section answered the research questions, objectives and acknowledged the Literature Review.

Based on the major findings of this study (Figure 4.1- Figure 4.20) it is evident that eight (8) of fifteen (15) SADC member countries had their NRENs formed. Furthermore, respondents indicated that only 15% of them were on Cloud usage (Figure 4.3) with basic Cloud services attributed by little access and collaboration among SADC NRENs. In addition, the challenges and the reasons for not embracing Cloud are highlighted (Figures 4.10, 4.11a, 4.11b, 4.20 & 5.5). This stresses more, the need for NRENs-CAF integration among them to make Cloud services, applications, computing resources, standardisation, interoperability and data security accessible to empower research collaboration among NRENs-CAF members. In addition, to reap the benefits of the emerging IT paradigm that is the Cloud computing technology. Subsequently, the study recommended and proposed a service oriented theoretical integrative architecture framework for SADC NRENs to ensure collaboration, reliable connectivity, standardisation, interoperation and data integrity through secured infrastructure.

NRENs-CAF is a high level heterogeneous middleware and associated with the existing frameworks such as SSLM (section 2.7 & 2.8) that in turn based on Cloud computing standards (section 2.7 and section 5.2.3). Hence, NRENs-CAF framework is adopted from existing best practices and standard frameworks and improvised on the identified gaps and design that is relevant to the scope and significance of this study. Figure 6.1 is a high-level design of proposed NRENs-CAF framework.

NRENs-CAF built an Inter Cloud Infrastructure (ICI) system which aided the transition of NREN into Cloud system and made them interoperable with each other. ICI was a combination of multi Cloud domain, multiple Cloud service providers and multiple NRENs that evolved into Cloud; hence, the need for a unified system which is NRENs-CAF in this case. NRENs-CAF created a framework to support Cloud services by interconnecting SADC NRENs to the Cloud service architecture that made NRENs interoperable with each other by enabling end-to-end connectivity.

The NRENs-CAF intended to create a framework to support Cloud services by interconnecting SADC NRENs and also to bridge the gap between the two major components of the Cloud services infrastructure: (i) Cloud Service Provider (CSP) infrastructure that typically has a global footprint and is intended to serve the global customer community; and (ii) Cloud Services Delivery Infrastructure (CSDI) which in many cases requires dedicated local infrastructure and Quality of Services (QoS) that cannot be delivered by the public Internet infrastructure. In both cases, there was a need for joining CSP infrastructure and local access network, in particular, for solving the

‘last mile’ problem in delivering Cloud services to customer locations and individual (end-) users.

NRENs-CAF used the ‘reachout’ experience of the Grid and Internet community and possibly following the same architecture patterns as Internet and Grid/OGSA. NRENs-CAF provided functionalities for creating Virtual Organisation (VO) based infrastructures. This framework is a proposed theoretical framework and is adapted from best practices, standards, existing frameworks and document review and is improvised in the required aspect based on the results and the scope of this study. The NRENs-CAF was proposed to build and deliver highly interconnected and high performance networks for Universities and other Educational and Research Institutions more specifically among SADC that enable them to share educational resources and collaborate both within SADC and globally. However, NRENs-CAF is not implemented.

6.1 NRENs-CAF Architecture

The proposed NRENs-CAF Architecture is a heterogeneous framework which is both multi-domain as well as multi Cloud provider in nature. The architecture possessed the ability to specific resource and applications provisioning and it managed, monitored and maintained critical functions. Such abilities helped the system attain functional reliability and made it fault tolerant. This system integrated, federated and interoperated the services and applications and attained highly secure access. The system architecture of NRENs-CAF inter-cloud consisted of components that are logically grouped

according to their functionality and the way they integrated with the entire end-to-end system.

General Requirements of NRENs-CAF

The proposed NRENs-CAF architecture should address the interoperability and integration issues in the current and emerging heterogeneous multi-domain and multi-provider Clouds. Further, this could host modern and future critical enterprise and e-Science infrastructures and applications, including integration and interoperability with legacy campus and enterprise infrastructure. In view of NIST Cloud Computing Reference Architecture (CCRA) and ITU-T JCA-Cloud activity, the proposed NRENs-CAF also addressed the following goals, challenges and requirements are:

- Should support communication between Cloud applications and services belonging to different service layers (vertical integration), between Cloud domains and heterogeneous platforms (horizontal integration).
- Necessary to be compatible and provide multi-layer integration of existing Cloud service models: IaaS, PaaS, SaaS and Apps Clouds.
- Required to support inter-Cloud control and management functions for better Cloud services and network Integration.
- Should support Cloud services and infrastructures provisioning on-demand and their lifecycle management, including composition, deployment, operation, and monitoring, involving resources and services from multiple providers.
- Necessary to provide a framework for heterogeneous inter-cloud federation

- Facilitate interoperable and measurable intra-provider infrastructures
- Explicit/Guaranteed intra and inter-cloud network infrastructure provisioning (as NaaS service model).
- Support existing Cloud Provider operational models and provide a basis for new forms of infrastructure services provisioning and operation.

Based on the requirements and overall findings, NRENs-CAF used the reach experience of the Grid and Internet community and possibly followed the same architecture patterns as Internet and Grid/OGSA, included providing functionalities that created Virtual Organisation (VO) based integrative architecture. According to Josey (2009), The Open Group Architecture Framework (TOGAF) provides a generic architectural framework, defining standard building blocks that can be used in conjunction with a variety of specific methodologies.

Similarly, NRENs-CAF followed TOGAF to build the architecture. The intended NRENs-CAF functionality associated with the general Inter Cloud Access and Delivery Infrastructure (ICADI) as defined by the inter-cloud Architecture Framework (Demchenko et al., 2012 and Demchenko et al., 2013). However, the NRENs-CAF may limit its services to Layer 0 through Layer 2 to remain transparent to current Cloud services model.

Furthermore, the proposed architecture was based on the Generalized Architecture for Dynamic Infrastructure Services GEYSERS and GEANT3. In support of this Ngo et al. (2013) had proposed the inter-cloud Architecture Framework. In continuation,

this framework had contributed to a number of standardisation bodies, in particular, the Open Grid Forum Research Group on Infrastructure Services On-Demand provisioning (ISOD-RG) and Internet Engineering Task Force (IETF) on Cloud Architecture Framework definition. In addition he stated that these standards are commonly generic and accepted by industry provide a basis for lower level Cloud services architecture and could be directly incorporated. Therefore, based on Ngo et al. (2013) and Demchenko et al (2012) model, few inter related components were incorporated into the proposed NRENs-CAF that addressed different issues in heterogeneous Cloud environment integration (Figure 6.1).

In view of the above, the proposed Cloud Architecture Framework included components that separated all functions related to the Cloud services design, control, management and operations into orthogonal groups. Therefore, the NRENs-CAF architecture is categorised into models or logical groupings. Figure 6.1 depicted the overlay of operational and functional components of the proposed NRENs-CAF Architecture. This overlay architecture of NRENs-CAF is represented as Cloud Operations Framework (COF).

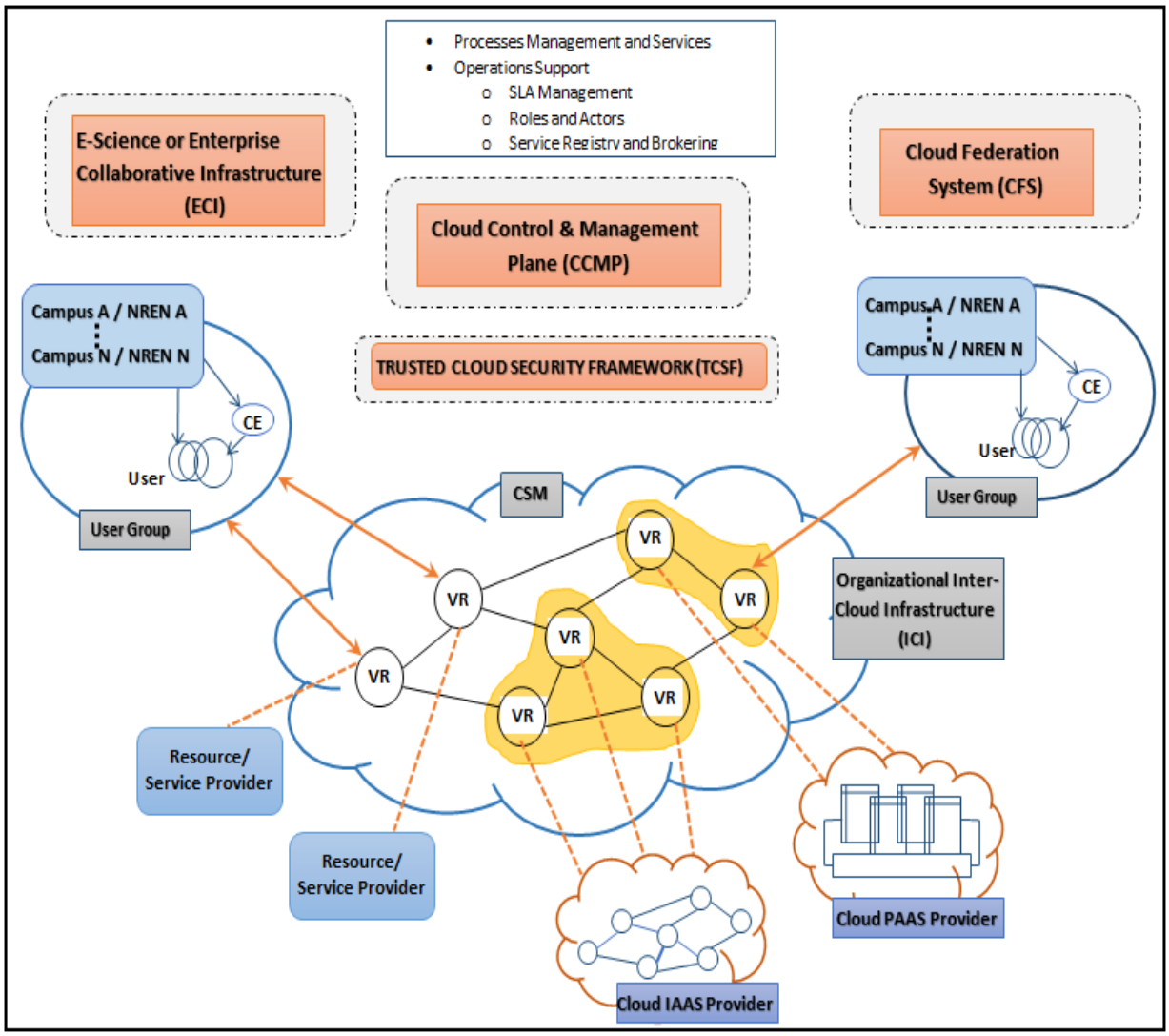

Figure 6.1: NRENs-CAF Cloud Operation Framework

Hence, from the requirements (section 6.1.1) the following complementary components of the proposed inter-cloud architecture were defined. Further, NRENs-CAF was decomposed into main architectural components and other supporting entities or internal supporting architectural elements. Each component of the architecture was listed and discussed individually in the following Sections.

6.1.1 Main Architectural Components

- Cloud Services Model (CSM)
- Cloud Control and Management Plane (CCMP)
- Cloud Federation System (CFS)
- Cloud Operation Framework (COF)
- Trusted Cloud Security Framework (TCSF)

6.1.2 Supporting Architectural Components

- E-Science or Enterprise Collaborative Infrastructure (ECI)
- Virtual Resource (VR)
- Inter Cloud Infrastructure (ICI)
- Resource Service provider
- Campus Network
- Cloud IaaS/PaaS provider

6.1.1.1 Cloud Services Model (CSM)

Cloud Services Model (CSM) was the central component of NRENs-CAF architecture. The proposed architecture and approach tried to closely imitate Internet approach in building hierarchically interconnected infrastructure for Internet protocol based services to support inter-cloud communication. However, there needed an additional inter-cloud layer, CSM that provided a Virtualization platform for IT and network services. CSM

allowed the entire infrastructure instantiation together with related protocols and core infrastructure services related to control and management functions (Ngo et al., 2012).

CSM was associated with vertical and horizontal integration and was composed of functional or operational layers that made up the CSM. It was split up into different layers and analysed for the required resources at each of those layers. At the same time, the Inter Cloud architecture requires a number of functionalities, protocols and interfaces to support its operation. In view of this, CSM was classified into six (6) different horizontal layers creating a Cloud with the protocol stack. In addition, depending on cross layer functionality, all the six layers were grouped into three (3) different vertical planes as indicated in Figure 6.2. The CSM component was adapted from "Inter-cloud architecture for interoperability and integration in the General InterCloud Architecture: GEYSERS and GEANT3 project" (Demchenko, Y., Ngo, C., de Laat, C., Makkes, M. X., and Strijkers, R., 2012).

Consequently, CSM defined the different Cloud service models that were used in Cloud computing system, such as SaaS, PaaS or IaaS (SPI) resources. It also explained the types of resources that were utilized by the Cloud system and their general requirements. Basically, these were directory services provided by the Cloud computing system. Ngo et al. (2012) explained that both vertical and horizontal integration is necessary in order to have an understanding of both operational and functional requirements of these service delivery models. Hence, all the services interacted and

integrated and made them compatible with each other so that a common kind of understanding reached between the components in CSM.

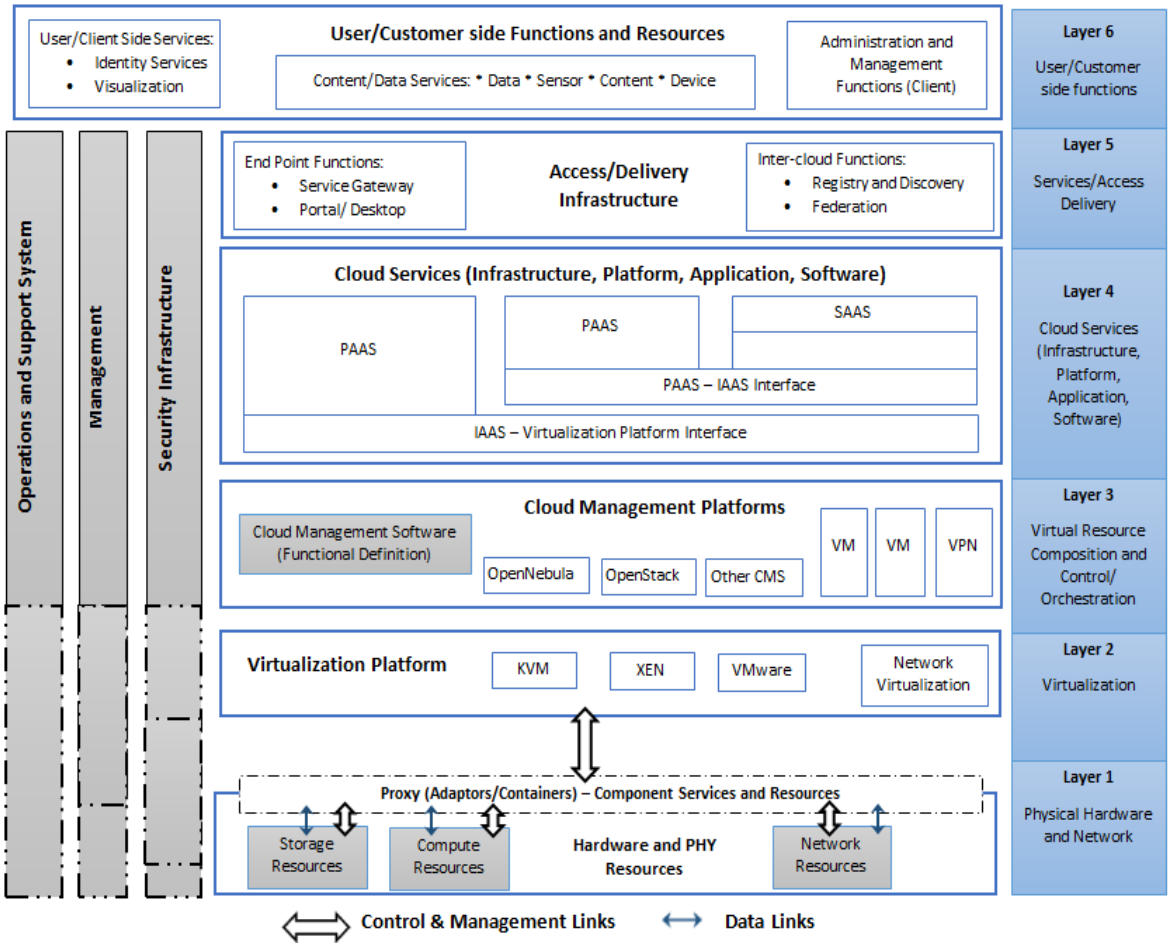

Figure 6.2: Reference CSM Architectural Model and its Protocol Stack (adapted from (GEANT3 Project), (NIST SP 500-292. Cloud Computing Reference Architecture), (ITU-T JCA-Cloud activity), (GEYSERS project: Demchenko, Y., et al., 2012))

Further, CSM was split-up into in three different planes and their functionalities were required at each layer. CSM was classified into six (6) different horizontal layers as

shown in Figure 6.2. The six horizontal layers or planes were defined and grouped according to their related functionality as described below:

a) Layer 1: Physical Platform (L1)

b) Layer 2: Cloud Virtualization (L2)

c) Layer 3: Cloud Resources Composition and Orchestration (L3)

d) Layer 4: Cloud Services (L4)

e) Layer 5: Access/Delivery Infrastructure (L5)

f) Layer 6: User/Customer Side Resources and Services (L6)

In addition, the six (6) horizontal layers basically created a Cloud with the protocol stack, depending on cross layer functionalities. All these six layers were grouped into three (3) different vertical planes as indicated in Figure 6.2. The three vertical planes or cross-layer infrastructures were defined to group related functionality in all the CSM layers. Basically, all of these vertical planes performed cross functional operations, management, controls and security. The vertical planes integrated with those three (3) layers in different ways are.

- Plane 1: Cloud Management Plane represented by Cloud Control and Management Framework.
- Plane 2: Operations Support System represented by Cloud Operations Framework.
- Plane 3: Security Infrastructure that was defined as Trusted Cloud Security Framework.

Physical Platform Layer (L1):

a) The lowest first layer, in this case, is the Physical layer named as L1 as shown in Figure 6.2. This layer included different physical resources such as storage, computing, networking for the entire network infrastructure, and it would provide the required network capacity and bandwidth. There was a need to interface the physical layer structure with Virtualization layer. Hence, both of these layers fell under the resources and services layer. The physical layer also provisioned special interfaces or adaptors functionality to link/connect and communicate with Cloud Virtualization layer using any Virtualization technology or a platform. All of these physical resources were connected to Virtualization platform using a set of interfaces or links.

On Figure 6.2, there were two sets of links, the black and white double sided arrow structures. Those links were used by end users to transmit and communicate information or data. All user generated traffic would be transmitted over data links, whereas, system information, messaging, and signaling will be sent over control and management links. Between L1 and L2, there was an adaptation layer where there were a set of proxies or adopters used to interconnect Virtualization platform with physical layer platform or structure.

b) Cloud Virtualization Layer (L2):

This layer customised the Virtualization platform for all non-hardware resources that were completely virtualized and interacted with lower layer structure. The layer had a Virtualization system or virtual operating system platform. The author outlined some examples of those platforms such as VM platform, Kernel Virtualization using Kernel Virtual machine (KVM), Xen Virtual Machine Monitor, VMware EXSi or any other Networking Virtualization technologies that helped create individual VM ecosystems. Those VMs were grouped and tasked with performing a specific set of services that occurred in Cloud Management Plane (CMP) which was the virtual resource composition and control (orchestration).

c) Cloud Virtual Resources Composition and Orchestration Layer (L3):

This layer combined multiple Virtual Machine resources (VRs) and grouped them into logical entities. The group of VRs could be utilised to enhance the performance or delivery of a particular service. Cloud Management Software (CMS) included openstack, openNebula and other commercial or proprietary content management system. CMS grouped virtual machines together, created virtual resource, virtual servers, virtual networks. It also created Virtual Private Networks (VPNs) between those logically or composed entities that operated at Layer 3.

Cloud Management Software (CMS) also provided additional services to interconnect the VRs group and eventually created Inter Cloud Infrastructure (ICI)

as indicated in figure 6.1. There, it was demonstrated how the VRs were composed into different groups and the orchestration occurred between those VRs groups. The layer was represented by the Cloud Management Software (CMS) and included additional services for combined Inter Cloud Infrastructure (ICI) composition and orchestration. The layer L3 included Cloud Virtualized resources composition, control and orchestration.

d) Cloud Services Delivery Layer (L4):

On top of L3 was Cloud services delivery layer associated with different service delivery model which forms layer 4 (L4). The Cloud Services Delivery Model included either pure IaaS on virtualized platform, PaaS to IaaS interface interconnected PaaS & IaaS layer or SaaS ran on the top of PaaS platform which was directly connected to IaaS. At that juncture, IaaS infrastructures depended on PaaS for its deployment and PaaS, in turn, depended on SaaS for its deployment.

The layer included different types of Cloud services, such as IaaS, PaaS and SaaS that were exposed to upper customer facing layer via standard interfaces while potentially using non-standard internal and lower facing interfaces. This layer decides which standard interfaces would be applicable to each service delivery model and communication between them could happen either through standard or proprietary interfaces.

e) Access/Delivery Infrastructure Hosting (L5):

In Layer 5 (L5), which was the user Access or Delivery Infrastructure, users interfaced to Cloud services layer (L4) on one side and user or customer side resources (L6) interfaces on the other. The layer consisted of different components, operational activities and functions that provided access to Cloud services/resources and interconnected multiple Cloud domains which delivered services to end user(s).

In that layer, there were two different functions, one part looked at the end point functions and the other one was inter-Cloud functions. The end point functions looked at interconnectivity between two different end points and service forwarding occurred through the Service GateWay (GW) or service portal. Whereas, the inter functions are presented for end-users to access Cloud services. It required some additional components such as a registry system which registered all the services provided by each individual Cloud system, and a mechanism to discover those services. For example accessing a service of L2 from L1 requires service discovery mechanisms which help discover what services are provided by L2.

Layer 5 (L5) also looked at Federated infrastructure that required federating access among different Cloud system which used different authentication mechanism and different security mechanism. Hence, this layer federated and created single sign-on capability between two different Cloud systems.

f) User/Customer Side Resources and Services (L6):

Layer 6 Provides direct connectivity to Access/Delivery Infrastructure through the user/customer functions or the user access network. This layer was located in and provided by the customer's enterprise or campus network to support their integration with the Cloud based infrastructure. Those included identity management, infrastructure administration, data services and visualization.

User side or customer side system/resources were split up into different sets of roles and privileges such as user or client services that provided identity services management, visualized certain type of data, access to the specific portal and also had administration and management functions. Data service enabled users to have access to like computing access, storage access, processing access, and the type of data used for visualization and retrieval. Administrators gained an elevated set of services that provided for the completely different type of user either system/network administrators, Cloud administrators, and management teams. The layer split up the content services into data, different sets of contents, sensor information and device information. Different types of information were monitored from the layer and presented to specific users with particular privileges.

Further, these six (6) horizontal layers that are explained above were grouped into three (3) different vertical planes depending on cross layer functionalities across CSM layers. These three (3) vertical planes are explained below.

i) Cloud Management Plane Represented by CMP

The First plane was Cloud Management Plane (CMP) had it's vertical cross layer presence from L2 to L5 and had management interfaces with mandatory implementations and optional in layer L1 as illustrated in Figure 6.2. The layer controlled and provided management level signaling and all associated functions.

ii) Cloud Operations Support System Represented by COF

The second plane constituted operation and support system, which had its vertical cross layer presence from L3 to L5, and had operational interfaces with mandatory implementation and optional from layer L1 to L2 as depicted in Figure 6.2. The layer provided support and operations, management, monitoring, maintenance capabilities that were orchestrated through Cloud Management software. The layer automatically interacted with Cloud Operations Framework (COF) that formed an operation and support system.

iii) Security Infrastructure that was Defined in as TCSF

Security layer structure or security plane which also had its vertical presence from L2 to L5 had mandatory security infrastructure and optional in L5. This security infrastructure is managed by Trusted Cloud Security Framework (TCSF). Security requirements and control varied between the layers, horizontally and vertically. Consequently, TCSF had mandatory security infrastructure all the way from

Virtualization platform to services, access or deliver infrastructure just before delivering those services to end user.

6.1.1.2 Cloud Control and Management Plane (CCMP)

CCMP was an isolated system associated on the top of CSM. Basically, this model integrated all the inter-Cloud application system with the infrastructure control and management system. That was a control and management system platform emphasizing on common control and management plane where all of the services were integrated seamlessly with CCMP.

The CCMP provided a logical and functional interface between different Cloud service layers running in different Cloud domains providing single control and management domain to heterogeneous inter-cloud infrastructure for the standardisation of interlayer interfaces. CCMP ensured sufficient control and management associated with inter Cloud signaling between applications and Cloud system. CCMP also supported messaging, monitoring all physical and virtual infrastructural resource, dynamic configuration and management which was configuring hardware, software, virtual resources, session management, and synchronisation of the distributed heterogeneous Cloud platforms. Apart from CCMP providing run-time optimization, it provides for VM integrations and migrations to specific locations for better load handling. Resource scaling or descaling operation, resource management that was resource allocation and de-allocation, job management or process management, were taken care by CCMP.

To perform signaling, monitoring, configuration or synchronization between different Cloud platforms, in that case, IaaS was different from PaaS domain. Figure 6.3 illustrates a case when two different Cloud domain IaaS and PaaS need to interact allowing applications from one domain to control underlying virtualised resources and infrastructure in another domain. However, in order to make communication between such domains, the use of specific functional components was defined. The overlay Architecture of CCMP was illustrated in Figure 6.3. This component was partly adapted on the top of the core architecture from "InterCloud Control and Management Plane in the general interCloud architecture: GEYSERS project" (Demchenko, Y., Ngo, C., Laat, D. C., Garcia-Espin, J. A., Figuerola, S., Rodriguez, J., Contreras, L. M., Landi, G., & Ciulli, N., 2013).

6.1.1.2.1 The Main Functional Components of CCMP

- **Cloud Resource Manager:** controlled the resources that were provided by IaaS and PaaS domain. In addition, control common resources available to both the domains and end users.
- **Network Infrastructure Manager:** took care of all the network resources that were available to CCMP.
- **Virtual Infrastructure Composition and Orchestration:** provided access to VRs and grouped all those VRs and made communication between those VR groups possible.

- **Services and Infrastructure Lifecycle Management (that could be also a part of the Composition and orchestration layer):** created and initialised VM, made them operational and finally termination of those VM resources.

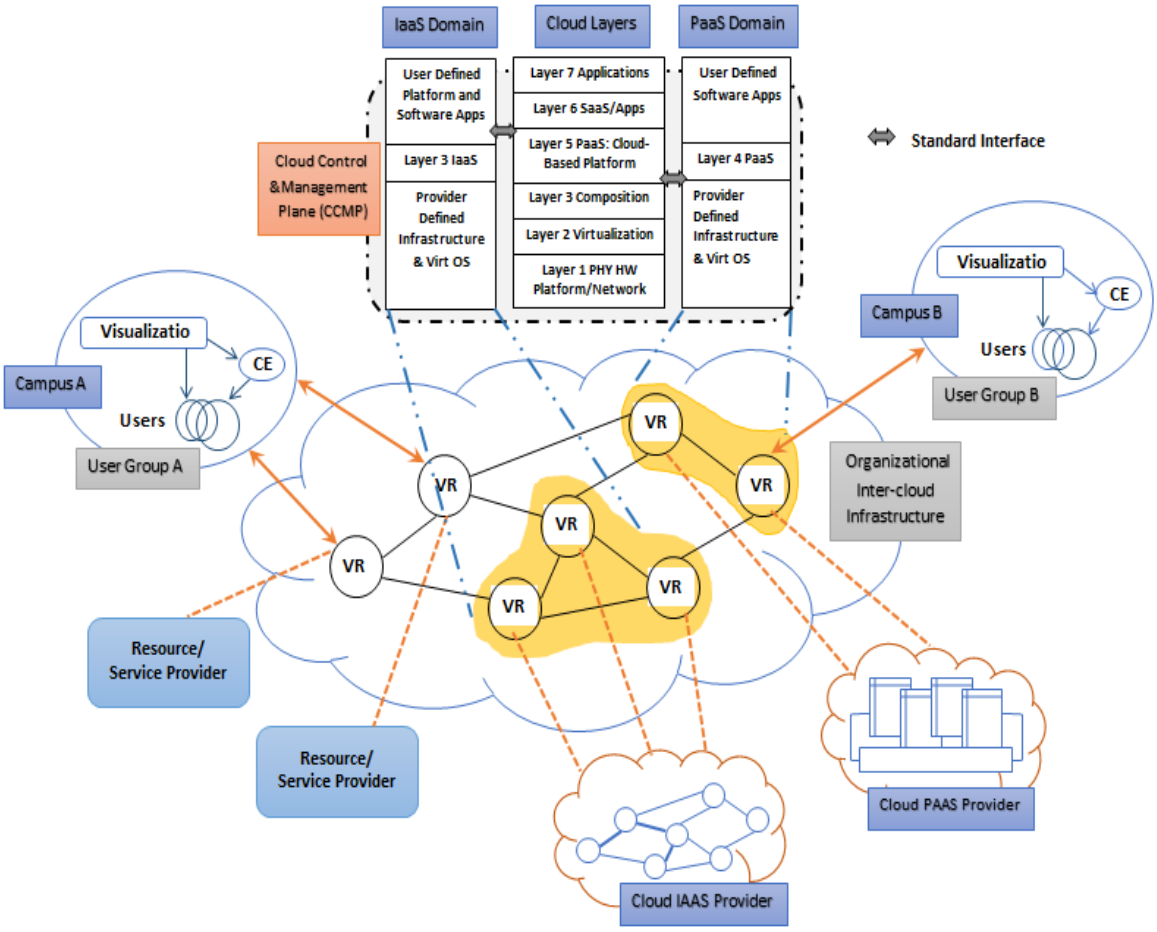

Figure 6.3: CCMP Architectural Model **(adapted from GEYSERS project:** Demchenko, Y., et al., 2013)

6.1.1.2.2 CCMP Interfaces Support and their Functionalities:

- **Inter-/Cross-layer Control and Signaling:** communication occurred between domains or within the same domain required inter domain or cross layer interface and signaling respectively that provided by the Cloud computing control and management interface. For this to occur, it was recommended to have common control and signaling protocol and interfaces.
- **Monitoring:** provided VR capabilities such as monitoring all physical and virtual infrastructural resource.
- **Location:** handled the location management of VRs from either service or resource provider.
- **Topology**: Infrastructure Management for recognizing the type of topology created by VRs or compute cluster.
- **Configuration and Protocols Management**: configured VRs and protocol management for different domains.

All those Interfaces and their functionalities that were incorporated or implemented using either open interfaces and standard protocols or non-standard proprietary implementation. The particular interface utilized only by a specific set of users mostly system administrators, network administrators, monitoring and auditing personnel, system managers that utilizing the particular infrastructure of CCMP.

6.1.1.2.3 Example of CCMP Use Case Scenario:

CCMP also looked at specific types of scenarios where it was required to interoperate between different service delivery platforms. Since that was an inter Cloud infrastructure which meant different types of VRs provided by different service provider. An Example of such Scenario was an IaaS service provider/domain that required to communication with PaaS domain. That scenario actually utilized different types of interfaces; either standard or proprietary interfaces, and was able to communicate between those completely different VRs.

In the communication process between each of these domains, service orchestration occurred between IaaS and PaaS domain. Such service orchestration was taken care by these Cloud layers. In order for IaaS and PaaS to communicate with Cloud layer, that occurred either over standard interfaces using standard open protocols like openCloud, CDM or OCCI over the proprietary interface. Nevertheless, it was ensured that each of this disparate domain able to communicate with each other in a seamless form which was generally taken care by CCMP. Communication between domains was automatically translated into standard or proprietary based formats to enable Cloud Services to communicate from one domain to another.

6.1.1.3 Cloud Federation System (CFS)

CFS was able to interconnect and federate between multiple Cloud systems to access the resources or services of a secondary Cloud. Therefore, operational and administrative controls were required to forward services, user credentials, authentication credentials, keys from one Cloud system to another. Hence, CFS provided interaction between two different domains, either operational or administrative domains.

NRENs-CAF Architecture provided CFS working on the inter Cloud infrastructure to enable interoperation between multiple domains to create logical structures between domains. So, CFS was extended to provide multiple services on multiple domains with an NRENs-CAF membership. CFS communicated between different Cloud computing systems by providing single sign-on capabilities for privileged users who could access services from two different Cloud systems.

Additional infrastructure was required to interconnect two different Cloud systems, but they could be part of the same service delivery infrastructure. Hence, some additional federation systems were created to forward services between domains.

Cloud Infrastructures that independently managed virtual resources or multiple domains had individual components that belonged to different Cloud providers like public, private and hybrid Clouds. That Federation system interacted with such external systems using commonly understood formats for service definition, provisioning, deployment. It

further took care of those features required for Cloud providers and administrative domains.

CSF federated services, applications and all associated semantics for translation, management of namespaces, translation of namespaces from one Cloud to another system. Apart from that, other additional services were assigning priorities, resource requirements that needed to be performed at the Gateway (GW).

CFS integrated multiple Cloud systems that were independent of each other. It also provided independent services and resources to one another and that integration was possible using federation infrastructure. Thus, in association with CFS, a number of functional components were required for integration.

On top of that, each of these functional components that communicated with one other, required specific protocols and interfaces as illustrated in Figure 6.4. This component was necessary and partly adapted on the top of the core architecture from "InterCloud Federation Framework for Multi-provider Cloud Services Integration in the general InterCloud architecture: GEYSERS project" (Makkes, M. X., Ngo, C., Demchenko, Y., Stijkers, R., Meijer, R., and de Laat, C., 2013). Further, CFS supported federation at the level of services, semantics, and namespaces, assuming necessary gateway or federation services.

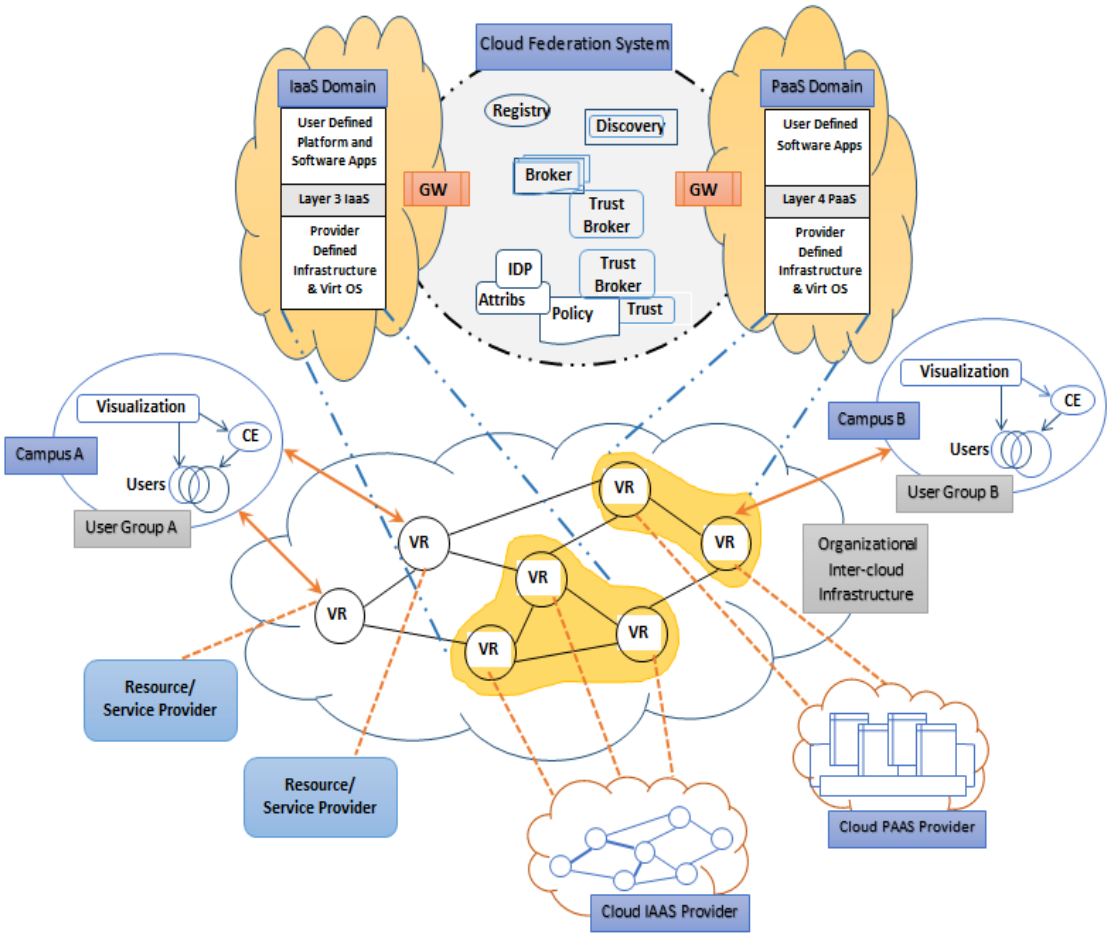

Figure 6.4: CFS Architectural Model (adapted from GEYSERS project: Makkes, M. X., et al., 2013)

6.1.1.3.1 Protocols and Interfaces of CFS

- **Service brokers:** communicated different services to different parts of this Cloud system. One service from one Cloud forwarded to another Cloud system through the service broker.
- **Trust broker:** brokering trust information, user trust or communication protocol trust, encryption information, key management was performed by trust brokers.

- **Registry services and discovery services:** maintained list of all the services and resources that were provided by specific independent Cloud systems. They also provided interfaces for discovering those services.
- **Identity provider:** federated identity information of different users between Cloud domains. Different independent Cloud systems should recognize and federate the same identity information of different users between Cloud domains. That required federated attribute authority which had a common understanding of user credentials and user related information associated with all of those Cloud systems.
- **Policy authority:** enforced common policies to all of those inter Cloud systems. It also optionally enables trusted third parties for extending services to one of these Cloud domains.
- **InterCloud GW system:** associated with performing translational capabilities. It automatically translated appropriate request query, protocols, any kind of messaging, communication signaling, and performed data format translation between Cloud domains. It made request/query sent by one Cloud domain which was understandable to other domains.

6.1.1.3.2 CFS Definition and Components:

The CFS communicated or performed federated access to two different Cloud domains IaaS and PaaS and for that to occur, CFS required the following:

- **Registry of services:** maintained list of services that were available on domain1 which was IaaS as well as the services available in domain 2 which was PaaS.

- **Discovery system:** a common set of procedures used by either domain1 or domain2 to discover services from one domain to another.
- **Brokering system:** translated or broker service request from one domain/entity to another domain. GW itself was responsible for the translation of all request and queries from domain to another domain using standard or non-standard interfaces. It also translated domain information to some common translation using, for example, XML translational service.
- **Trust broker:** broker trust related information like authentication, identity, credentials, and user privileges. It also brokers trust between completely different systems by managing and forwarding keys, sharing keys, generating keys and its life time management.
- **Identity provider:** had a set of attributes that assisted to understand which user's had what type of services and in which domain.
- **Policy enforcement system:** enforced policies on a system wide basis irrespective of which domain the services provided.

6.1.1.3.3 CFS Also Requires a Certain Set of Interfaces that Provide Some Functionalities (reference Figure 6.4):

- **Names and attributes resolution, translation and management:** name and attributes on the Cloud domain defined and translated corresponding domain that was accessed.
- **Publishing and subscription:** published services from one domain to another, and was required to provide an interface to enable this discovery service.
- **Discovery Trust/key management:** key management between domains, defining trust boundaries.
- **Federation, delegation and trust management:** federated services and provided infrastructure for associated life cycle management. That took care of federation components like initiation, operation and termination.

6.1.1.4 Cloud Operation Framework (COF)

COF was associated with multi provider infrastructure operation, routine operations and work flow. It was also related to SLA management, monitoring whether meeting the targets or not, operational related information, monitoring, engagement and accounting. COF had its own set of well-defined user roles and responsibilities that worked in resource operation and management framework. COF roles were owned by management or operational entity or by an entity which actually owned that particular Cloud computing system through ownership or a stake holding.

COF required support from and interacted with CCMP and CFS. COF monitored the operations performed by all other models. COF was external to the Cloud services model and it supervised how those services were delivered, managed, signaled. COF took care of routine operations and concentrated on the functionalities that provided routine operations. It defined clearly the roles and responsibilities of specific users and what they were required to interact with and support. COF oversaw the complete operations of CSM, CCMP and CFS.

COF had Service broker and registry which determined what services were currently available, operational and inactive. All these information were obtained using service broker through service registry where all the services were registered. Apart from this, addition components were required like service providers or resources provider.

6.1.1.4.1 COF also Require some Interfaces and supported the Following Functionalities:

The interfaces performed the following specific tasks:

- **Service Provisioning**, deployment, decommissioning (or Termination)
- **SLA management and negotiation:** also needed to keep track of SLA related information during the operation. That was to ascertain whether terms and condition set forth by SLAs were being met or not and even SLA negotiations could take place here in certain scenarios.

- **Services Lifecycle and metadata management:** any kind of additional information or metadata that was transmitted during this operational phase was managed in a secure way.

6.1.1.5 Trusted Cloud Security Framework (TCSF)

TCSF was a cross functional entity and that involved interaction with multiple layers in the protocol architecture. TCSF was applicable to many layers at different levels of service. All security controls were consolidated into one single TCSF and ensured that integration of all of the security services associated with different layers in the CSM. This would not only ensure that security operations are being performed in a reliable and efficient way inside NRENs-CAF architecture, but it would also ensure security when interacting with third party systems through the CFS. TCSF provided capabilities for secure operations among all of these components associated with Inter Cloud Architecture (ICA).

TCSF would provide a basis for all secure operations among the components that were present in NRENs-CAF architecture. So, it took care of integration with multiple Cloud layers. In fact, the TCSF Interface was implemented for different layers and it created encapsulation for the entire COF.

In terms of TCSF, some additional definitions required were cross functional mechanism and controls operating in multiple layers at the same time. In addition, each different layer of that particular protocol or Cloud stack had different requirements.

Therefore, all security mechanism expected from the end user associated with that particular Cloud computing system were defined through SLA system.

It was emphasized that different security controls and services were integrated into multiple layers of the Cloud stack starting directly from Virtualization platform and be implemented all the way up to the user access network. For each security service that was implemented, it was required to provide fine grain control at each layer so that, the services were made less vulnerable to any kind of security threats. Note that, there were different components that required security controls as shown in Figure 6.5. This TCSF component was based on best practices and standards such as: "Common Security Services Interface (CSSI), Cloud Security Alliance reference model (CSA) and the security infrastructure for dynamically provisioned virtualized security services" also referenced by (Ngo, C., Membrey, P., Demchenko, Y., & de Laat, C., 2012).

- Starting from the end user, information security needed to be provided in the form of isolation.
- Data/information security: to be secured all times whether it is internal to Cloud system, between Cloud systems or between Cloud system and the Internet; nevertheless, in all the three scenarios, it must be protected.
- Any kind of data/information processing that was performed such as upload, processing of information, store and stream/visualization, needed to be protected.
- Policies associated with security requirements were enforced on a system wide basis.

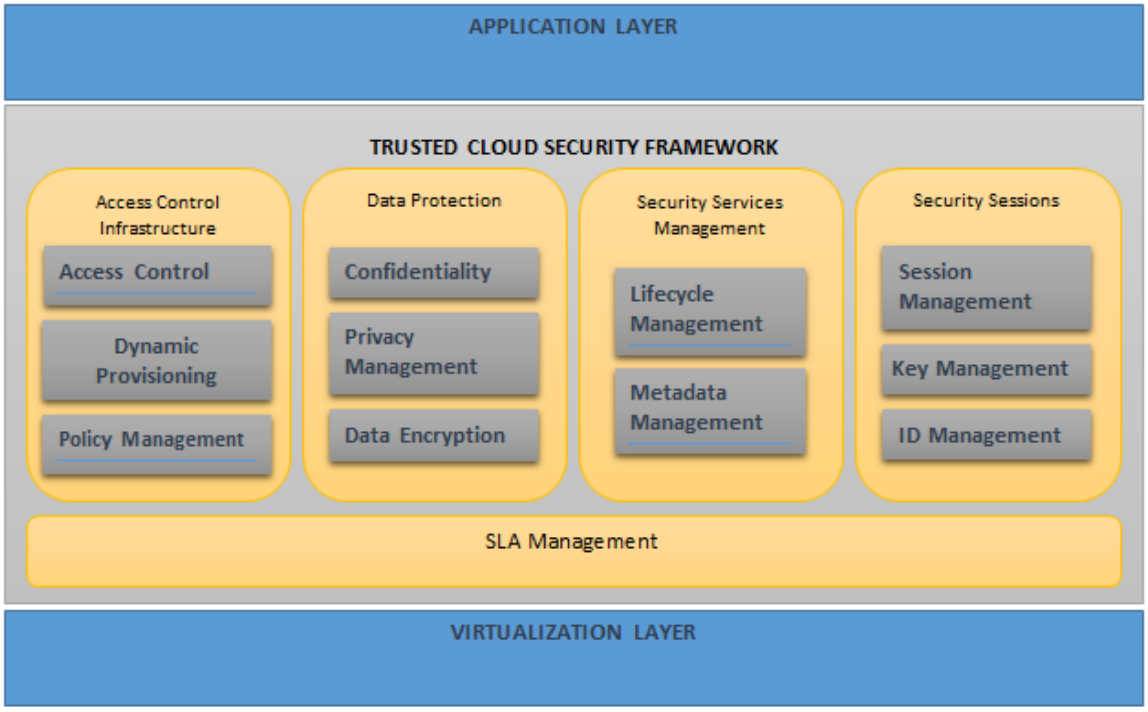

Figure 6.5: TCSF Architectural Model (adapted from (Cloud Security Alliance reference model (CSA)), (Common Security Services Interface (CSSI)), (GEYSERS project: Ngo, C., et al., 2012))

The following problems and challenges were identified when trying to build security infrastructure specifically for the inter Cloud environment to interconnect multiple Cloud domains:

- There were issues associated with data protection that meant data stored and "on-wire" (data in transit); that included, besides the traditional confidentiality, integrity, access control services, also data lifecycle management and synchronization need to be addressed.

- Access control infrastructure helped to create fine grain control associated with access control policies and that helped define end user privileges in a secure fashion.
- Security services lifecycle management with respect to security included the creation and destruction of metadata information, managing properties associated with security information, bound to specific service, how they are replenished, destroyed, renewed and transmitted.
- Security sessions information management was specifically for end user sessions. This should be secured together with its life cycle management and its associated security.
- Federation and identity management: provided trusted service.
- Trust and key management for all provisioned resources: Any kind of trust related information like signatures or certificates needed to be exchanged and it had to be done in a dynamic fashion.
- SLA management: the scope of the security definition in terms of SLA system.

The Dynamic Access Control Infrastructure (DACI) made it more efficient to manage security related information and it was creating a consistent security infrastructure specifically for on-demand systems (Ngo et al, 2012). In view of the above commonly used security practices, the security solutions and supporting infrastructure supported consistent security mechanisms used in specific scenarios like session handling and session management.

6.1.2.1 E-Scientific or Enterprise Collaborative Cloud Infrastructure (ECI)

Figure 6.1 illustrated the typical framework example of building project oriented to e-Science or enterprise collaborative infrastructure (ECI). That was specialized infrastructure that included dedicated transport network. It had the capabilities of provisioning resources and specific services on-demand that was utilized by the University, research and educational networks. ECI was used for large scale technical experimentation and was used for small or medium scale scientific experiment. That particular work flow involved campus or enterprise proprietary infrastructure. In addition, it incorporated components of Cloud services that were Cloud based computing, storage, instrumentation, visualization systems, interconnecting network infrastructure and users represented by user clients.

6.1.2.1.1 Example of use case scenarios for ECI

In Figure 6.1, there were two localised infrastructures. For example, two different campuses, campus A and B, had two different user groups. Both campuses collaborated jointly on a scientific experimentation project using ECI infrastructure. In addition to scientific experimentation, they also required some capabilities and services provided by the Cloud infrastructure such as Virtual resources (VRs) which provided specialised functions such as filtering, visualization and data processing.

6.1.2.2 Virtual Resources (VRs)

Every resource in the NRENs-CAF was treated as a virtual resource that was handled and controlled easily. Note that a virtual resource could be software, a platform or an API. The virtual resources were grouped together and created a complete service. Various VRs were configured in different logical topology or structures such as hierarchical or flat structures in that particular Cloud system and was referred to as Inter Cloud Infrastructure (ICI). That created a centralised resource controller/manager for all VRs that were interconnected depending on the resource/service provider. ICI had to oversee all the processing, storage, data distribution/presentation requirements with respect to all NRENs. These VRs could be provided externally to the organisation through a trusted third party entity providing SaaS, PaaS and IaaS (SPI) platform. VRs would be provided by Universities/campuses provided by scientific infrastructure.

Interconnection of the VRs provider associated with certain resource group established the ability to integrate and interoperate with each other and that has what created Inter Cloud Infrastructure (ICI). Hence, there is a need to have sufficient controls and interfaces to make this interoperability possible. Additionally, SADC NRENs could be encouraged to continue collaborating through NRENs-CAF infrastructure in order to share resources through the inter Cloud System of VRs.

6.1.2.2.1 Use Case Scenarios of VRs

In Figure 6.1, one side VRs were provided by Campus A on another side they were provided by campus B. Among those, one VR could run the entire scientific infrastructure (ECI). On the user side or infrastructure side, there were SPI or anything as a service (XaaS) providers that had its own network infrastructure and could be integrated to the NRENs-CAF that provided specific VRs. So, anything and everything in that Cloud was made available as VR. That meant, irrespective of services/resources through VMs or access to physical infrastructure through Virtualization technologies or access to SPI or Scientific infrastructure, all of those were virtual infrastructure. Each of those VRs was interconnected in some logical fashion that created ICI. Therefore, VRs could either be storage, computing and networking resources which were allocated to perform some specialised processing.

6.1.2.3 Inter Cloud Infrastructure (ICI)

ICI allowed campus or NRENs to access the central Cloud that was the COF. In Figure 6.1, there were two localised infrastructures, campus A and B, where they had different user groups which were required to collaborate with each other. These were jointly carrying on scientific experimentation utilizing common scientific infrastructure ECI. In addition to scientific experimentation, it was also required to have some capabilities and services provided by ICl. Therefore, ICI are the interconnectivity of VRs.

6.1.2.4 Resource Provider

On the NRENs-CAF Architecture (see Figure 6.1) each and every type of service (for e.g. Software/Platform/Infrastructure) were provided by a resource/service provider. These providers were either internal or external Cloud system. In contrast, SPI providers were always internal to the Cloud system and only provided a particular type of service to the Cloud users.

VRs were also provided by either resource service providers that were internal or external to the organisation through trusted third party (TTP) organisation or entities that were part of the VR infrastructure. Any external resource providers could be integrated to provide VRs through NRENs-CAF system provided they met certain criteria. The specific University provided specific resources that could be virtualized.

Note that, small scientific infrastructure was part of the campus network where a part of that processing requirements and outcome of the infrastructure were moved as VRs on Cloud. Also, take cognisance that VRs were generic in nature having the flexibility of interconnecting different type of VRs provided by different organisational members of NRENs-CAF or Trusted third party provider.

6.1.2.5 Campus Network/NRENs

Campus networks or NRENs, research institutions and University research labs to mention a few were connected to NRENs-CAF, apart from service provided by NRENs-CAF to its members were possible for those campuses to access service provided by

another third party provider such as CSP. These are some examples of systems that required dedicated service delivery infrastructure specific to Universities and NRENs.

6.1.2.6 Cloud IaaS and PaaS Provider

VR could be provided by either IaaS, PaaS providers. That could be either internal or external to the organisation. SPI could be third party provider vendors and need not necessarily be Universities or any specific institutions. CSP or campus or end user had owned network infrastructure and that could be integrated to NRENs-CAF and provide specific VRs.

6.2 Summary

The chapter discussed the proposed heterogeneous Cloud Architecture Framework (NRENs-CAF) together with the data analysis findings that formed the basis for the design of the architecture. The NRENs-CAF served as an architectural blueprint that established resource sharing, collaboration, standardisation, interoperability and secured Cloud within the SADC NRENs. The NRENs-CAF architecture presented incorporates majority of the goals, challenges and requirements.

The following chapter presented the conclusions and recommendations made in the study. These were based on the results of the study, literature and data analysis. In this chapter the suggestions for future research were also presented.

CHAPTER 7: CONCLUSIONS AND RECOMMENDATIONS

The Chapter presented the conclusions and recommendations drawn from the findings of the study. The Chapter also provided recommendations that were done to curb some of the shortcomings found during the study. Finally, it served as a guide for further research directions that could be explored in the near future.

7.1 CONCLUSION

The research aimed at transforming the existing SADC NRENs traditional IT to Cloud infrastructure. In addition, it allowed the creation of a common infrastructure that provided all the services through NRENs-CAF architecture and it ensured interoperability between different NRENs. The conclusions were discussed in relationship to the research questions. The research questions guided the research and data analysis.

7.1.1 Research Question One: "What were the resources that could be used to establish Cloud architecture in the SADC NRENs?"

From the data analysis discussion of Chapter 5, the first research question aimed at identifying the resources that were essential for establishing Cloud architecture framework for the SADC NRENs. The study identified the necessary resources (see Figure 4.10 and 4.11b) to develop the NRENs-CAF. Those were: minimum threshold level of technological infrastructure, human resources, internet connectivity, security infrastructure and framework, legal frameworks, SLA's, political will, funding and

economic reasons. Hence, the introduction of NRENs-CAF has the potential to transform the SADC NRENs into Cloud based platform. It determined the best possible approaches for transforming the current infrastructures into Cloud model (see Figure 6.1).

7.1.2 Research Question Two: "What Cloud service architecture was suitable for interconnection among NRENs in the SADC region?"

The second research question aimed at ascertaining what Cloud service architecture was suitable for interconnection among NRENs. In the study (see Figure 4.3 and 4.4), it was found that some of the NRENs used Virtualization to maximize the logical computing resources of their IT infrastructure. Hence, virtualization was one of the key drivers to adopt Cloud computing technology. Therefore, those NRENs which were using virtualization in their IT infrastructure were in a much better position to adopt Cloud computing technology faster and easier. In that regard, NRENs-CAF considered developing a unified platform that was for SADC NRENs (see section & Figure 6.1).

Chapter 6 presented a proposed architecture which developed the Cloud framework for SADC NRENs. The architecture incorporated all the necessary components that were deemed necessary for the development of NRENs-CAF as derived from the literature reviewed.

7.1.3 Research Question Three: "What were the challenges faced by SADC NRENs with regards to establishing Cloud services?"

The third research question attempted to identify the challenges faced by SADC NRENs with regards to establishing Cloud services. The study identified (see Figure 4.20 of Chapter 4 and Figure 5.5 of Chapter 5), various challenges such as security, interoperability and policies. Therefore, those challenges were addressed by incorporating components like TCSF, COF, CCMP and CFS associated with the NRENs-CAF architecture (see Sections 6.1.1.2, 3, 4 & 5) of Chapter 6. Hence, NRENs-CAF made the transition from non-cloud based to Cloud-based IT infrastructure easier thus, enhanced the NRENs' willingness to embrace it.

7.2 RECOMMENDATIONS

7.2.1 Cross Border Regulations

To ensure an effective regulatory development in the field of Cloud computing, it was recommended to all SADC Governments to adopt a new regulatory approach. Emphasis was made to regulate the ease of technology exchange crossing the borders of the NRENs countries. In addition, contractual requirements associated with the specific features of Cloud computing services were recommended such as mandatory terms and conditions in service outsourcing contracts; quality control, personal data protection, data security and availability of service. Therefore, the need of SLA between the SADC NRENs and service providers.

7.3 FUTURE RESEARCH

It was evident that the research mainly concentrated in building a suitable Cloud infrastructure for connecting SADC NRENs through NRENs-CAF to Cloud. In addition, NRENS-CAF would utilize the connectivity facility provided by WACS cable that has landed in few African countries where the connectivity would be faster and cheaper. In that light, it was highly recommended that the same study could be extended to connecting those NRENs to the international gateway. In view of the above, the study could explore terrestrial fibre networks connecting member institutions to the last-mile distribution of the fibre network and providing NRENs-CAF services more effectively.

7.4 Summary

This Chapter provided the conclusions drawn from the findings of the study. The Chapter also provides recommendations that can be done to curb some of the shortcomings that were found. Finally, it gives a guide for further research that could be carried out.

REFERENCES

Aarnet. (2015). Global research network. Retrieved from https://www.aarnet.edu.au/network-and-services/global-research-network

Afrinic.net. (2008). Research and education networking in Africa. Internet Number Resources and African Academia. Proceedings of eleventh International conference on Afrinic Public Policy Meeting. Retrieved from http://meeting.afrinic.net/afrinic11/slides/day3/African_Academia_20091126.pdf

Ajayi, O., & Ajayi, I. (2011). Fostering a Secure Framework for National Research and Education Network. Proceedings of the fourth International annual conference on UbuntuNet Connect: Access for success, Nairobi, Kenya: UbuntuNet Alliance.

Aluoch, A. A. (2006). The search for affordable quality Internet connectivity for Africa Universities, *AAU Newsletter*. *12*(3), 8-10.

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2012). Cloud Computing Synopsis and Recommendations. *National Institute of Standards and Technology (NIST) Computer Security Division, 1*, 800-146.

Barroso, D. (2007). Botnets-the silent threat. *European Network and Information Security Agency (ENISA), ACM, 3*, 15-171.

Barry, B. (2008). Research and educational networking in sub-Saharan Africa–An update, Presentation for Fall 2008 Internet2 Member Meeting, New Orleans. Retrieved from https;//wiki.internet2.edu/confluence/download/attachments/235/20081015-Ren-in-Sub-Saharan-Africa-BBarry.pdf

Bendandi, S. (2009). Cloud computing: Benefits, risks and recommendations for information security. Retrieved from http://www.scribd.com/doc/23185511/Cloud-Comuting-benefits-risks-and-recommendations-for-information-security.pdf

Bernstein, D., Ludvigson, E., Sankar, K., Diamond, S., & Morrow, M. (2009). *Blueprint for the InterCloud-protocols and formats for Cloud computing interoperability.* The fourth International Conference on: In Internet and Web Applications and Services (ICIW'09), *IEEE,* 328–336.

Boateng, O. (2009). Information Technology in Developing Countries. International Federation for Information Processing, *IEEE, 19*(3), 3-4.

Bosch, P., Duminuco, A., Pianese, F., & Wood, T. L. (2011). Telco clouds and virtual telco: Consolidation, convergence, and beyond. International Symposium on: In Integrated Network Management (IM). *IFIP/IEEE*, 982-988. doi: 10.1109/IM.2001.5990511

Brunette, G., & Mogull, et al, R. (2009). Security guidance for critical areas of focus in Cloud computing v2. 1. *Cloud Security Alliance,* 1-76.

Bryman, A., (2001). *Social Research Methods*, Oxford: Oxford University Press.

Bureau, I. T. S. (2010). *Activities in Cloud computing standardization*. Repository v1, May, 13.

Carminati, F., et al (2014). Geant users guide.CERN program Library, 12. Retrieved from http://www.googlescholar.pdf

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling data in the Cloud: outsourcing computation without outsourcing control. Proceedings of the workshop on Cloud computing security (CCSW '09). *ACM*, 85-90. doi: 10.1145/1655008.1655020

Cisco, C. (2010). *Annual security report*. San Jose, California, USA: Author

Cloud Computing Reference Architecture,1.0 (NIST SP 500-292). Retrieved from http://collaborate.nist.gov/twikicloudcomputing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292-090611.pdf

Cooper, D. R. and Schindler, P.S. (2004). *Business Research Methods*. TataMcGraw Hill.

Creswell, J. (2003). *Research design: qualitative, quantitative and mixed methods approaches (2nd ed.)*. Thousand Oaks, CA: SAGE Publications.

Darlaston-Jones, D. (2007). Making connections: The relationship between epistemology and research methods. The Australian Community Psychologist, *19*(1), Retrieved from https://groups.psychology.org.au/Assets/Files/Darlaston-Jones_19%281%29.pdf

Demchenko, Y., Ngo, C., de Laat, C., Garcia-Espin, J. A., Figuerola, S., Rodriguez, J.,… & Ciulli, N. (2013). InterCloud Architecture Framework for Heterogeneous Cloud based Infrastructure Services Provisioning On-Demand. In L. Barolli, F. Xhafa, M. Takizawa, T. Enokido, & H. H. Hsu (Eds.). *Proceedings of twenty-seventh International Conference on Advanced Information Networking and Applications Workshops* (pp.777-784). Barcelona, Spain. NJ: *IEEE*.

Demchenko, Y., Ngo, C., de Laat, C., Lopez, D. R., Morales, A., & García-Espín, J. A. (2013). Security infrastructure for dynamically provisioned cloud infrastructure services. *International Journal of Privacy and security for cloud computing, IEEE,* 167-210.

Demchenko, Y., Ngo, C., de Laat, C., Makkes, M. X., & Strijkers, R. (2013). InterCloud architecture framework for heterogeneous multi-provider Cloud based infrastructure services provisioning. *International Journal of Next-Generation Computing, IEEE, 4*(2).

Demchenko, Y., Ngo, C., Makkes, M. X., Strijkers, R., & de Laat, C. (2012). Defining inter-cloud architecture for interoperability and integration. In W. Zimmermann,

Y. W. Lee, & Y. Demchenko (Eds.). *The third International conference on Cloud Computing, GRIDs, and Virtualization* (pp.174-180), Nice, France. Wilmington: *IARIA, IEEE*.

Dyer, J., & Haver, M. (2012). The Future Roles of NRENs. Brussels: TERENA. Retrieved from http://www.google scholar.pdf

Echezona, R. I., & Ugwuanyi, C. F. (2010). "African University libraries and Internet Connectivity: Challenges and the way forward." Retrieved from http://digitalcommons.unl.edu/libphilprac/421

Erdogmus, H. (2009). Cloud computing: does nirvana hide behind the nebula? Software, *IEEE, 26*(2), 4–6.

Fell, L. (2014). Australia's National Research and Education Network. *Telecommunications Journal of Australia (TJA), 62*(5), 3–27.

Gabriella, C., Massimiliano, C., Steve, C., Marcello, B., Silvana, M., Stephanie, P., & Nicholas, F. (2013). *Cloud for science and public authorities: A study prepared for the European commission DG Communications Networks, Content & technology*. European Commission, doi: 10.2759/25446

Gallagher, S. (2012), How Africa is embracing "the cloud" on its own terms. *World Bank Report*. Nairobi, Kenya

GEANT. GEANT 3 Project. Retrieved from http://www.geant.net/pages/home.aspx

GEYSERS. GEYSERS Project. Generalised Architecture for Dynamic Infrastructure Services. Retrieved from http://www.geysers.eu

Global e-Schools & community initiative. (2007). National Research and Education Networks in Africa. Retrieved from http://www.gesci.org/old/files/2008_Annual Report /annual_report.pdf

Greene, S. (2005). Security Policies and Procedures, Principles and Practices: *Security Series.* Prentice-Hall, Inc

Greaves, B. D. (2013). *Tertiary Education And Research Network of South Africa (TENET) Annual Report*, South Africa: Author.

Hinde, C. & Belle, J. V (2012). Cloud computing in the South African summit. Retrieved from ttps:www.academia.edu/3036522/Cloud_Computing_in_South_ African_SMMEs_Risks_and_Rewards_for_Playing_at_Altitude

IBM CCRA. Cloud Computing Reference Architecture 2.0.

IEEE P2302. Standard for InterCloud interoperability and federation (SIIF). Retrieved from http://standards.ieee.org/develop/project/2302.html

Inc, S. (2009). Cloud computing: Benefits, risks and recommendations for information security. *Springer Berlin Heidelber*. doi: 10.1007/978-3-642-16120-9_9

Interview with Martin, Duncan**.** Cape Town: TENET, 26 June 2012, Vol. 3.

ISO/IEC 27002. Information technology - Security techniques - Code of practice for information security controls (2nd ed.). Retrieved from http://www.iso27001security.com/html/27002.html

ITU (2012). International Telecommunication Union (ITU): *Cloud Computing in Africa Situation and perspectives Report.* Geneva, Switzerland: Author

ITU-T Cloud (2012). FG Cloud Technical Report. Retrieved from http://www.itu.int/en/ITU-T/focusgroups/cloud/Documents/FG-coud-technical-report.zip.

Iyengar, Jeyanthi, N., Shabeeb, & Hena, N. C. S. (2012). A study on security threats in Cloud. *International Journal of Cloud Computing and Services Science (IJCLOSER), 1*(3), 84–88.

Josey, A. (2009). *Togaf version 9.1* enterprise edition - an introduction. The Open Group, 11.

Karanja, G. (2006). *The African Tertiary Institutions Connectivity Survey Report (ATICS).* Cyberplex Africa. Botswana.

Katz, R. N., Goldstein, P. J., & Yanosky, R. (2009). Demystifying Cloud computing for higher education. *EDUCAUSE* Centre for Applied Research Bulletin. ISBN 978-1-4666-4632-2.

Khunga, U. (2012). UbuntuNet Alliance: ZAMREN and TENET form the first UbuntuNet cross-border link. Retrieved from http://primeurmagazine.com/weekly/AE-PR-08-12-99.html

Korporaal, G. (2009). AARNet: 20 Years of the Internet in Australia. *AARNet*, *20*(7).

Kotecha, P. (2012). Higher Education in the Southern African Region: Current trends, challenges, and recommendations. Johannesburg, South Africa, *SAURA, 5*, 55-66.

Koukis, V. (2011). Greek Research and Technology Network. The International Conference on Cloud Computing Technology and Science (CloudCom). Retrieved from https://okeanos.grnet.gr/vkoukis-okeanoscloudcm.pdf

Kunda, D., & Khunga, B. (2014). Implementing national research and education Networks (NRENs) in land locked African countries: Critical success factors. Proceedings of 7th annual conference on Research and Education networking. Retrieved from UbuntuNet Alliance, Zam_tnc15_paper_Tnc15PaperImplementingENRENInLandlockedAfricanCountriesv3.pdf

Kuria, W. (2012). NREN Opportunities and Challenges: the Xnet Development Alliance Trust experience. Educational Technology Debate (ETD). Retrieved from http://edutechdebate.org

Kuyoro, S., Ibikunle, F., & Awodele, O. (2011). Cloud Computing security issues and challenges. *International Journal of Computer Networks (IJCN)*, *3*(5).

Kwofie, B. (2012). Cloud computing opportunities, risks and challenges with regard to information security in the context of developing countries. (*Master's Thesis, Luleå University of Technology, Ghana)*

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST Cloud computing reference architecture. *NIST special publication*, 500-292. Retrieved from http://www.nist.gov/customcf/get_pdf.cmf?pub_id=909505

Luo, S., Lin, Z., Chen, X., Yang, Z., & Chen, J. (2011). Virtualization security for Cloud computing service. *International Conference on Cloud and Service Computing (CSC), IEEE*, 174–179.

Maaref, S. (2013). Cloud computing in Africa situation and perspectives. Retrieved from http://www.googlescholar.pdf

Makkes, M. X., Ngo, C., Demchenko, Y., Strijkers, R., Meijer, R., & de Laat, C. (2013). Defining InterCloud Federation Framework for Multi-provider Cloud Services Integration. *In Cloud Computing.* The fourth International Conference on *Cloud Computing, Grids, and Virtualization. Valencia, Spain. Wilmington: IARIA, IEEE,* 185-190

Maree, K. (2007). *First Steps in Research,* Pretoria, Van Schaik Publishers.

Marlow, C. (1993*). Research Methods*. Pacific Grove, CA: Brooks/Cole.

Martin, D. (2013). Implementing effective controls in a mobile, agile, cloud-enabled enterprise. *IEEE: Security & Privacy*, *1*(5), 13–14.

Martin, D. H. (2012). Newsletter of UbuntuNet Alliance: Networks, Collaboration, education. *International Science Grid this week (ISGTW)*, *7*(9), E1, E4.

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

Mbale, J. (2008). *Zambia Research and Education Network (ZAMREN) formation of an emerging academic networking strategy*. Proceedings from the International Conference on African Research and Education Network Infrastructure (WCRAN). Tunisia: Ubuntunet

Mbale, J. (2009). Formation of Namibia Research and Education Network (NAMREN). Retrieved from http://www.ubuntunet.net

Mbale, J. (2014). Cloud Computing and Virtualization Technologies in Libraries. *The University Library Electronic Identities Authentication System (UL-EIDA): Enhanced by Segmented Virtual Machines and VLANs for Development in Sub-Saharan.* Washington DC: Global book series Advances in Library and Information Sciences (ALIS). doi:10.4018/978-1-4666-4631-5.ch010

Mbale, J., Kauna, M., & Victor, H. (2013). Examining ubiquitous security. Capital issues in implementing a campus-system-as-a-service (CSaaS) model in the Cloud computing age: Case study sub-Saharan region. *International Research Journal of Computer Science and Information Systems (IRJCSIS)*, *2*(2), 18–24.

Mell, P., & Grance, T. (2009). The NIST definition of Cloud computing. *National Institute of Standards and Technology, IEEE, 53*(6), 50-60.

Meyer, L. (2012). Internet2 to Deliver New Higher Ed Cloud Services report. Campustechnology Magazine. Retrieved http://www.campustechnologymagzine.com/ research/.aspx

Mircea, M., & Andreescu, A. I. (2010). Using Cloud computing in higher education: A strategy to improve agility in the current financial crisis. *Journal of International Business Information Management Association*, *3*, 1-14.

Mkandawire, S. (2013). *Survival of National Research and Education Networks (NRENs) in a competitive market of Africa: A Case Study of the Zambia Research and Education Network (ZAMREN)* 6th annual conference on: Networks, Collaboration, education: UbuntuNet Alliance, 185-192.

News letter of UbuntuNet Alliance (NUENCE) (2008). Networks, Collaboration, Education, *NUANCE*. *9*(3).

Ngo, C., Demchenko, Y., & de Laat, C. (2012a). *Toward a dynamic trust establishment approach for multi-provider InterCloud environment*. The fourth International Conference on: In Cloud Computing Technology and Science (CloudCom), *IEEE,* 532-538.

Ngo, C., Membrey, P., Demchenko, Y., & de Laat, C. (2012b). *Policy and context management in dynamically provisioned access control service for virtualized Cloud infrastructures.* Seventh International Conference on: In Availability, Reliability and Security (ARES), *IEEE*, 343–349.

Ngo, C., Membrey, P., Demchenko, Y., and de Laat, C. (2011). *Security framework for virtualised infrastructure services provisioned on-demand.* The third International Conference in Cloud Computing Technology and Science (CloudCom), *IEEE*, 698-704.

Nisbett, R. E. (1993). Rules for reasoning. Retrieved from http://www.googlescholar.pdf

NIST SP 500-292, Cloud Computing Reference Architecture, v1.0. Retrieved from http://collaborate.nist.gov/twikiCloudcomputing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf

O'Kane, P., Sezer, S., and McLaughlin, K. (2011). Obfuscation: The hidden malware. *Security & Privacy, IEEE, 9*(5), 41–47.

Ortiz Jr, S. (2011). The problem with Cloud computing standardisation.*Computer*, *44*(7), 13–16.

Pearce, M., Zeadally, S., & Hunt, R. (2013). Virtualization: Issues, security threats, and solutions. *ACM Computing Surveys (CSUR)*, *45*(2), 17.

Pisonneault, A. and Kraemer, K.L. (1993). Survey research methodology in management information systems: an assessment, *Journal of Management Information Systems, 10*(2), 75-106.

Rasmusson, L. and Aslam, M. (2012). *Protecting private data in the Cloud*. In Proceedings of the 2nd International Conference on Cloud Computing and Services Science, *CLOSER 2012*.

Regional Infrastructure Development Master Plan ICT Sector report: *SADC Towards a Common Future*. (2012). Moputo, Mazambique: Author

Richard, E. N. (2013). Rules for reasoning. Psychology Press. Retrieved from http://www.google scholar.pdf

Rizzo, T. M. (2013). The business case for Cloud. Retrieved from http://www.googlescholar.pdf

Rose, M. T. (2009). Nysernet white pages pilot project: Status report. *Technical report*. *NYSERNet* report no. 89_12_31_1.

Salim, S. (2014). Sustainability of National Research and Educational Networks (NRENs) in developing countries. (*Doctoral Dissertation, Tallinn University, Bangladesh)*

Salmon, D. (2009). Prospects for a future Janet. *The 8th Inter-national conference e-VLBI Workshop, 1*, 48.

Saunders, M. N. K., Saunders, M., Lewis, P., & Thornhill, A. (2011). *Research methods for business students* (5th ed.). India: Pearson Education India.

Sekaran, U. & Bougie, R. (2010). *Research Methods for Business: A Skill Building Approach* (5th ed.). Netherlands: John Wiley & Sons,

Shan, C., Heng, C., & Xianjun, Z. (2012). Inter-cloud operations via NGSON. *Communications Magazine, IEEE, 1*(50), 82–89.

Struwig, F.W., & Stead, G.B. (2004). *Planning, Designing and Reporting Research*. Cape Town: Pearson Education South Africa.

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

Sybrand, A. B. (2009). The Conceptualization, Design and Implementation of a National Research and Education Network (NREN). (*Master's thesis, University of Stellenbosch)*

Szefer, J., Keller, E., Lee, R. B., and Rexford, J. (2011). Eliminating the hypervisor attack surface for a more secure Cloud. In Proceedings of the eighteenth ACM conference on Computer and communications security, *ACM, 50*(7), 401–412.

Szegedi, P. (2011). NREN's perspective on storage and Clouds. *IEEE Communications Magazine, 49*(7), 54–61.

Szegedi, P. (2013). TERENA trusted Cloud drive facility. *TERENA TF-Storage meeting: Pilot project report*. Berlin, Germany.

Takefusa, A., Nakada, H., Takano, R., Kudoh, T., & Tanaka, Y. (2011). *Gridars: a grid advanced resource management system framework for InterCloud*. The Third International Conference in Cloud Computing Technology and Science (CloudCom). *IEEE*, 705-710

TENET (2013). The tertiary education and research network of South Africa. *TENET Annual Report*, Cape Town, South Africa: Author

TERENA. (2012). A study on the prospects of the internet for research and education 2014-2020: *ASPIRE Report*, Europe: Author.

The African Tertiary Institutions Connectivity Survey Report (ATICS). Association of African Universities (AAU) in collaboration with International Development Research Centre (IDRC). Europe. Retrieved from http://www.actics.info.pdf

Thompson, J. (1998). Web-based enterprise management architecture. *Communications Magazine, IEEE, 36*(3), 80–86.

Thorsteinsson, G., Page, T., & Niculescu, A. (2010). Using virtual reality for developing design communication. *Journal of Informatics and Control*, *19*(2), 93–106.

TN. (2013). *Annaul Report* . Windhoek, Namibia: Author.

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

Twinomugisha, A. (2007). *Global e-Schools & community initiative (GeSCI).* National Research And Education Networks In Africa. Canada. Retrieved from http://www.gesci.org/old/files/2008_AnnualReport/annual_report.pdf

Van der Pol, R., & Dijkstra, F. (2013). *Network and capacity planning in Surfnet6*. Netherlands: TNC 2013.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the Clouds: towards a Cloud definition. *ACM SIGCOMM Computer Communication Review*, *39*(1), 50–55.

Velte, T., Velte, A., & Elsenpeter, R. (2009). *Cloud computing, a practical approach*. USA: McGraw-Hill, Inc,

Weber, A. S. (2011). Cloud computing in education in the Middle East and North Africa (mena) region. Can barriers be overcome? In Conference proceedings of "eLearning and Software for Education" (eLSE), 1(5), 565–570.

Welman, C., Kruger F., Mitchell B. (2005). *Research Methodology* (3rd ed.). Oxford University Press, Capetown.

Wind, S. (2011). Open source Cloud computing management platforms: Introduction, comparison, and recommendations for implementation. Conference on: *In Open Systems (ICOS.), IEEE,* 175-179.

Xiao, Z. & Xiao, Y. (2013). Security and privacy in cloud computing & Communications. *Surveys & Tutorials, IEEE*, *15*(2), 843–859.

Xnet Development Alliance trust. (2000). *Namibian Public Service network plan Strategic Action Plan: Xnet Development Alliance trust report.* Windhoek, Namibia: Author.

Yasinsac, A., & Irvine, C. (2013). Help! is there a trustworthy-systems doctor in the house? *Security & Privacy*, *11*(1), 73–77.

Zaipuna, Y. (2010). Directnews.com on Information and communication technologies.

Citizen newspaper. Retrieved from https://communicationsdirectnews.com

Zhang, L., & Zhou, Q. (2009). CCOA: The International Conference in Cloud computing open architecture. *In Web Services(ICWS), IEEE*, 607–616

APPENDIX A - RESEARCH QUESTIONAIRE

QUESTIONNAIRE

NRENs Cloud Architecture Framework (NRENs-CAF): Enhancing Cloud Connectivity Among National Research Education Networks In SADC

The purpose of this questionnaire is to help collect data for the study. Kindly complete the section that applies to you.

All responses are **ANONYMOUS and CONFIDENTIAL**

*Please **tick** where appropriate and you can **tick** more than one item where necessary or **write** your responses in the spaces provided.*

1. Occupational position?

System Admin ☐ Network Admin ☐ DB admin ☐ Technician ☐

Other (specify)…….....**..**

2. Size of Population in your NREN: Below 5000 ☐ 5000-10000 ☐ 10000+ ☐

3. Is your NREN on Cloud?

Yes ☐ No ☐

4. If **Yes**, what IT infrastructure/Technologies used in your NREN?

Virtualization ☐ Hosted servers ☐ Managed hosting ☐ VMWare ☐

Centralise IT services ☐ Parallel and distributed computing ☐ Big data ☐

High performance Computing (HPC) ☐ Multitenancy ☐

Virtual Domains (VDOMs) ☐

Other (specify)…….....

5. To what extent is your NREN willing to deploy Cloud computing services?

Definitely willing ☐ probably willing ☐ Not willing ☐

6. How effective is your NREN functioning?

Very well ☐ satisfactorily ☐ poor ☐

7. How is the collaboration with other NRENs?

Excellent ☐ good ☐ poor ☐

8. If **Yes to Question 3**, indicate which 'Cloud deployment models' your NREN uses?

Public Clouds ☐ Private Clouds ☐ Community Clouds ☐

Hybrid Cloud ☐

9. If **Yes to Question 3**, Which 'Cloud computing services' are used by your NRENs?

SaaS ☐ PaaS ☐ IaaS ☐ CaaS ☐

Other (specify)…….....**...**

10. If **No to Question 3**, select the reason(s) why?

Strict regulations ☐ Lack of Political will ☐ Lack of management support ☐

Lack of stakeholders cooperation ☐ Lack of Technologies ☐

11. What next steps should NRENs take, if Cloud computing is to be adopted?

Collaborate with other NRENs to simplify Compliance requirements ☐

Loosen restrictions on Data crossing the borders ☐

Stronger executive/political support for Cloud computing initiatives ☐

Establish/enforce technical standards for Cloud-related technologies ☐

Effective practices for making decisions on Cloud computing ☐

Replacing the existing systems with Cloud-based systems ☐

Strong guarantees in contracts and service level agreements ☐

Growing availabiltiy of Cloud services from IT vendors and service providers ☐

12. For what purpose will your NREN use Cloud computing?

Providing Standardised shared platform for research collaboration among other NRENs in SADC ☐

Improving communication, productivity and collaboration among NRENs and users ☐

Exchanging data more efficiently with outside organisation ☐

Backing up data ☐

Processing and storing applications ☐

Run enterprise applications ☐

Developing and testing software ☐

Other (specify)…….....

13. If **Yes to Question 3**, are you satisfied with the security provided by Cloud providers?

Yes ☐ No ☐

14. If **No to Question13,** rate how concerned your organisation is about data security, privacy or confidentiality issues when it comes to using any of the Cloud service models.

Very concerned ☐ Concerned ☐ Somewhat concerned ☐

15. If **Yes to Question13**, which security measures are applied to your NREN? (you can select more than one item)

Physical Security ☐ Network Security ☐ System Security ☐

Application Security ☐ Virtualization Security ☐

16. Is your network architecture scalable ?

Yes ☐ No ☐

17. If **Yes ,** what Scalable Architectures are applied to your NREN?

Horizontal Scaling ☐ Vertical Scaling ☐ Automated elasticity ☐

18. Did you think of Governance Issues while providing network services? Issues like:

Governance and Enterprise Risk Management ☐

Legal and Electronic Discovery ☐

Compliance and Audit ☐

Information Lifecycle Management ☐

Portability and Interoperability ☐

19. What measures have you NREN taken to address Interoperability issues?

Upgrading of conventional/ existing legacy infrastructure ☐

Overhaul major part of the infrastructure to compliant with the Cloud Technology ☐

Integration of Information Systems ☐

Standardisation ☐

Deploying Non-proprietary Cloud API's ☐

Ubiquitous nature of the Cloud ☐

Share best-of-breed operational practices ☐

Other (specify)…….....

20. Rate the challenges/issues ascribed to the Cloud'.(Number these items in order of importance i,e 1,2,3,4,5,6,7,8,9 with 1 being the most important and 9 the least important)

Security ☐

Performance ☐

Availability ☐

Hard to integrate with in-house IT ☐

Not enough ability to customize ☐

Worried on-demand will cost more ☐

Bringing back in-house may be difficult ☐

Regulatory requirements prohibit Cloud ☐

Not enough suppliers yet ☐

THANK YOU!!!

APPENDIX B - AAA VULNERABILITIES

A poor system for Authentication, Authorization and Accounting, could facilitate unauthorized access to resources, privileges escalation, impossibility of tracking the misuse of resources and security incidents in general, etc, through:

- Insecure storage of Cloud access credentials by the customer.
- Insufficient roles available.
- Credentials stored on a transitory machine

Furthermore, the Cloud makes password based authentication attacks (trend of fraudster using a Trojan to steal corporate passwords) much more impactful since corporate applications are now exposed on the Internet. Therefore, password-based authentication will become insufficient and a need for stronger or two-factor authentication for accessing Cloud resources will be necessary.

APPENDIX C - Confidentiality, Integrity and Availability (Triad C.I.A: Security Reference Model)

The Confidentiality, Integrity and Availability (C.I.A) security model is a way of describing the information security level of a system; the model dates back to mainframe computing (Whitman & Mattord, 2004). The term C.I.A. Security Model is synonymous with the terms C.I.A. Triad and C.I.A. Triangle (Brunette & Mogull, 2009; Greene, 2006; Whitman & Mattord, 2004). The C.I.A. acronym stands for *"confidentiality," "integrity," and "availability"* (Gilliam, 2004). Data stored electronically in computers are valuable assets and should be protected against unauthorized disclosure, unauthorized tampering or destruction and obstructions to availability; attacks against one or more of these items are considered an attack on an organisation's information security (Greene, 2006).

Confidentiality refers to the ability to control the access to information that should remain secret to those individuals or groups who are not authorized to view that information (Pfleeger & Pfleeger, 2007; Whitman & Mattord, 2004). In addition, only those individuals who have a demonstrated need may access such materials (Whitman & Mattord, 2004). Confidentiality of information is also defined as secrecy or privacy (Pfleeger & Pfleeger, 2007). Ensuring confidentiality or the secrecy of sensitive materials such as intellectual property or records is a critical issue (Gilliam, 2004). Many organisations consider their intellectual property more valuable than physical assets, so establishing and maintaining policies and mechanisms that guard intellectual

property is a critical part of maintaining competiveness (Liu & Kuhn, 2010). The failure to ensure the confidentiality of data stored within an electronic system results in an organisation experiencing a damaged reputation, embarrassment or even possible legal ramifications (Stoneburner et al., 2002).

In Cloud computing systems confidentiality is related to the areas of "... *intellectual property rights, covert channels, traffic analysis, encryption, and inference"* (Krutz & Vines, 2010, p. 63). Intellectual property is protected by copyright laws which protect inventions, designs, art, music and literary works (Krutz & Vines, 2010). A covert channel is an unauthorized and unintended communications session that allows the exchange of information (Krutz & Vines, 2010). Traffic analysis is the process of examining the volume, source and destinations of network traffic to make inferences about what types of information is being transmitted (Krutz & Vines, 2010). Encryption is the scrambling of messages into code to guard against eavesdropping (Krutz & Vines, 2010). Inference is the ability for individuals to gain information about data stored out of reach at a higher security level by analyzing the data that they do have access to (Krutz & Vines, 2010).

Integrity of information requires that three conditions are met:

- Unauthorized persons or systems cannot modify data;
- Authorized persons or systems cannot make unauthorized changes to data; and

- The data is internally and externally consistent, that is the internal structures within the data are consistent and the relation of this data to the real world is consistent (Krutz & Vines, 2010).

In addition, integrity refers to the quality of stored information that ensures that it is not corrupt, and exists in whole (Whitman & Mattord, 2004). Loss of data integrity can result from malicious or accidental damage, corruption, destruction, alteration or other tampering (Gilliam, 2004; Whitman & Mattord, 2004). If the loss of data integrity is not corrected, then the continued use of the compromised data can lead to faulty organisational decisions, other inaccuracies, or even fraud (Stoneburner et al., 2002).

Availability refers to the ability of an authorized user or system to access data and information processing services without difficulty (Whitman & Mattord, 2004). Since availability entails access to data and data processing services, it is harder to define than confidentiality and integrity (Pfleeger & Pfleeger, 2007). A system is available if:

- There is a timely response to a request,
- All requestors are treated equally,
- The service employs fault tolerance to minimize downtime due to hardware failure, and
- The system is easily accessed and appropriate mechanisms are in place to handle simultaneous access, deadlocks, and exclusive access (Pfleeger & Pfleeger, 2007).

In the realm of Cloud computing, CSPs define availability merely as the ability to connect to their services over the network (Habib, Ries, & Muhlhauser, 2010).

Availability is analogous to the library patron who expects access to the correct materials after providing the required identification or authorization (Whitman & Mattord, 2004). Any degradation of data availability can quickly affect an organisation's efficiency and operational effectiveness when end users are expected to be productive (Stoneburner et al., 2002). An example of the loss of availability is illustrated by the case of an employee changing the name of an important file in a credit union's computer system. Although the credit union still owned the file, it was not accessible to the computer system and this stopped all production (Bosworth, 2002). The loss of availability ranges from temporary loss of access all the way up to complete and permanent destruction of the data with no chance of repair or recovery (Bosworth, 2002).

APPENDIX D - Open Research Challenges

Cloud computing is definitely an attractive technology and is capable of delivering on-the-fly extraordinary capabilities in the form of measurable services. The inherent business model allows for enterprises to monetize their businesses, saving costs and raising productivity and profits. Clouds will surely continue to rise and the IT industry will heavily rely on it for supporting enterprise computing and the IoE.

1.1 Public vs. Private Clouds

The shift to Clouds still comprises a difficult decision. Several security issues provide good reasons for some not to move their data to Cloud environments, especially public Clouds. The Alert Logic State on Cloud Security Report (AlFardan et al., 2013) depicts the top three incident occurrence as web application attacks, brute-force attacks and vulnerability scanning in Cloud environments.

There is lower threat diversity in Clouds than in enterprise data centers, meaning that are more different types of threats in enterprise networks. That is mainly due to the APT threats that target private companies for espionage. Thus, on one hand, it is safer to opt for private Cloud solutions, like Nebula One (Erdogmus, 2009), but on the other, it is more probable to see sophisticated attacks on enterprise networks. In addition, private Clouds bring higher costs, in part defeating the purpose of the utility-based Cloud business model. In either case, Cloud users still have to cope with issues of the software, storage and computing, Virtualization, network and access categories of the taxonomy.

From the Internet and services category, issues of web services and web technologies also apply in this case, and the human factor should never be set aside when discussing security is not a technical solution alone.

1.2 Storage/Computing Challenges

Outsourcing storage and computing tasks raise several hardware-related and trust issues. Losing control over the servers and all data transfers within the Cloud network calls for secure storage and computing mechanisms, as well as auditing techniques. Integrity-checking techniques have been around for long, but are not adequate for tackling Cloud storage. (Xiao and Xiao, 2013) overviewed Provable Data Possession (PDP) and Proofs of Retrievability (PoR) approaches, and they concluded that these approaches can only be applied to static files, therefore not being applicable in Cloud systems. However, the research community started working towards dynamic approaches, which now include scalable PDP and dynamic PDP, but neither of them offers a complete set of characteristics that embrace all Cloud requirements, such as public verifiability.

1.3 Virtualization Challenges

To address the Virtualization issues, there is effort on devising stronger VMM solutions. As (Pearce et al., 2013) pointed out, Virtualization issues should be handled with care and forethought. A strong solution can address confidentiality, integrity, and availability, but failures on one of these are enough to trigger potentially disastrous results. VMMs are large and complex while having thousands of lines of code. They

mediate the creation and deletion of VMs, provide VMs with virtual resources, isolate running components as best as they can, define virtualized networking, and provide the necessary virtual devices to route virtual traffic. They are a middleware layer between host OSes and guest OSes, hence revealing a considerable attack surface. There are four main research areas related to VMMs security (Szefer et al., 2011), with one of them being now unsuitable, which will not be discussed herein.

1.4 Malware Challenges

Albeit mobility is a certain future for enterprise and Cloud connectivity, and the fact that Android malware grew 2577% in 2012, mobile malware only takes a 0.42% slice out of the top web malware threats for 2012 (Cisco, 2010). Nevertheless, adequate attention should be given to each propagation medium. Malware writers are focusing on evasion techniques rather than finding ways into internal systems, because that is almost taken for granted, probabilistically speaking. Strength is being put on the Return On Investment (ROI). Thus, malware camouflage behavior might pave the path for next generation malware, and this definitely concerns virtualized environments as malware can change behavior on-the-fly if it detects such a presence, and the Trojan (O'Kane et al., 2011).

1.5 Web Access Challenges

In terms of web-based technologies, there is a wide attack vector associated with the techniques used to deliver applications over the Internet. For a start, web pages deliver

mechanisms to outcome the flaws of underlying standards and protocols, such as HTTP statelessness. Not only that, but programmers usually oversee web-related security measures in exchange for more fancy functionality.

In such case, input validation is many times not correctly implemented, leaving behind holes for injecting SQL or JavaScript code. In addition, XSS and URL-guessing attacks explore the fragile GET method. Injection remains the main issue related to web applications, but XSS is a growing trend in general. Nonetheless, even POST can be subverted by manipulating HTML hidden fields or stealing cookies. On top of those, HTTP should always be used over TLS, despite the existing attacks on the protocol. To mitigate web applications vulnerabilities, (Martin, 2013) suggested fostering software development teams with adequate security training. An SDLC must follow a solid approach by integrating security controls directly into the SaaS application stack. For instance, Data Loss Prevention (DLP) should be best deployed natively in the software. Moreover, intelligent logs must also be deployed, in order to then correlate them in a better way, ultimately resulting in a better and more focused perspective of a network health.

1.6 Network Perimeter Challenges

Cloud computing changes the networking perimeter and the underlying network security devices. Cloud computing is a synonym of literally moving almost everything to the Cloud, including applications for internal purposes or for enterprise customers, and data. To make all this available, a wide range of distinct types of connectivity is put in place.

On top of that, but both the Cloud and enterprise networks become lively dynamic with a plethora of devices generating traffic.

1.7 Auditability and Trust Challenges

As extensively discussed in this article, trust is a barrier that transversely extends throughout the whole Cloud components and stakeholders. The authors invoked the term mutual auditability to refer to collaborative monitoring with the purpose of proving reciprocal trustworthiness. In other words, rather than focusing the auditability in the customer-provider direction, a bidirectional approach is adopted. This can improve incident response and recovery times since both providers and customers can be the source or target of an attack. Moreover, (Rasmusson and Aslam, 2012) have provided a novel solution that uses Trusted Platform Module (TPM) technology to prevent a provider from eavesdropping VMs.

1.8 Standards/Open-Source Challenges

The rapid adoption of Cloud computing resulted in a many Cloud proprietary formats developments, in turn giving out the fear of vendor lock-in. The need to standardize formats in Clouds is clear. To that end, leaders around the world started to work on various open standards. The Open Data Center Alliance (ODCA), founded in 2010, aims to speed up the migration of current Cloud environments to interoperable and standardized Cloud systems, and the Open Cloud Initiative (OCI) (Zhang and Zhou, 2009) aims to legally regulate such standards.

GLOSSARY

Amazon Web Services (AWS): This is a selection of Cloud computing services offered over the Internet by Amazon.com.

Application Programming Interface (API): These are interfaces for programmers to access and manipulate Cloud resources.

Application Security: This is the security issue under Operational Domains in Cloud computing that discusses as how to secure the application software which is running in the Cloud or being developed in Cloud.

Architecture: Representation of the structure of a system that describes the fundamental organisation of its components, their relationships and the principles that guide its design and evolution.

Authentication: Determining the identity of an individual or computer system.

Authorization: Granting access rights to resources or functions.

Big Data: It is an all-encompassing term for any collection of data sets so large and complex that it becomes difficult to process using traditional data processing applications.

C.I.A. Triad: Stands for Confidentiality, Integrity and Availability.

Cloud Application: A software program that is not run from on-premises computer hardware, but it is run on remote systems via the Internet.

Cloud Client: It is a computing device for Cloud computing.

Cloud Operating System (COS): It is a development environment for applications.

Cloud Provider: It is a provider that makes data processing services such as storage, software, or an operating system available to others over a network.

Cloud Service Architecture (CSA): It is an architecture in which applications act as services on the Internet.

Cloud Service Provider: A Cloud service provider is a vendor of Cloud computing services available over the Internet.

Cloud-Oriented Architecture (COA): It is a software development architecture that is intended to support incorporating Cloud computing components.

Cloudware: Software that is intended to create, deploy, and maintain applications in a Cloud computing environment.

Compliance and Audit: This is the security issue under Governance Domains in Cloud computing that addresses about maintaining and proving compliance when organisations move to Cloud computing.

Consortium: is an association of two or more individuals, companies, organisations or governments (or any combination of these entities) with the objective of participating in a common activity or pooling their resources for achieving a common goal.

Data Center (DC): A data center (sometimes spelled datacenter) is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business.

Data Center Operation: This is the security issue under Operational Domains in Cloud computing that discusses the evaluation of provider's data center and architecture.

Domain Name System (DNS): A DNS system associates domain names with IP addresses.

Elastic Compute Cloud (EC2): This is an Amazon commercial Web Services that allows customers to rent computers on which to run their own computer applications.

Elasticity: Means the Cloud infrastructure scales it on-demand services.

Encapsulation: Defining an application and all of its dependencies and then locating them in a physical, isolated folder.

Encryption and Key Management: This is the security issue under Operational Domains in Cloud computing that identifies the proper encryption usage and scalable key management.

Federation and Orchestration: Cloud federation is the idea of interconnecting various Cloud computing services or environments (usually from different service providers) for the purpose of creating more efficient and on-demand services. Cloud federation needs different service/resource providers to provide computing resources to other providers. These resources can become a temporary or permanent extension of that provider's Cloud computing environment, depending on the specific federation agreement between providers. On the other hand, Cloud orchestration uses software called "orchestrator" which is used to manage the Cloud interconnections and interactions among different Cloud units. A Cloud orchestrator can be used to create interconnection workflows to connect various automated processes and associated virtual resources.

GateWay: Gateway is a router or a proxy server that routes between networks.

Governance and Enterprise Risk Management: This is the security issue under Governance Domains in Cloud computing that deals with the ability of the organisation to governing and measuring enterprise risk caused by Cloud computing.

Hardware Virtualization: Software that emulates hardware to allow multiple operating systems to run on the same physical machine.

Hypervisors or Virtual Machine Monitor (VMM): software that controls the layer between the hardware operating systems.

Incident Response, Notification and remediation: This is the security issue under Operational Domains in Cloud computing that addresses the items that should be in place at both provider and user levels to ensure proper incident handling and forensics.

ISO/IEC - International Organization for Standardization/International Electro technical Commission

Last-mile: Last-mile technology is any telecommunications technology that carries signals from the broad telecommunication backbone along the relatively short distance (hence, the "last mile") to and from the customers or clients.

Legal and Electronic Discovery: This is the security issue under Governance Domains in Cloud computing that addresses the legal issues when organisations adopt Cloud computing.

Load Balancing: Load balancing provides a single point of access to multiple servers that run behind it.

Managed Hosting: This is the type of Clouds are hosted or managed by third party providers or managed by another organisation.

Multi-tenancy: This Refers to the feature of being capable of running multiple instances on the same shared platform. Each instance can be accessed by one or more users, called tenants.

Operating System Virtualization: The creation of a separate run-time environment within the same operating system.

ParaVirtualization: It is a virtual server technique that emulates hardware for the guest operating system.

Physical-to-Physical Migration (P2P): Moving a complete operating system environment and installed applications from one physical server to another.

Portability and interoperability: This is the security issue under Governance Domains in Cloud computing that discusses the movement of data from one provider to another or bringing it back to the enterprise.

PreVirtualization: It is a technique for combining the performance of traditional Virtualization with ParaVirtualization

Scalability: The ability of a system to increase the workload on its current resources.

Secure Shell (SSH): Enables secure communications over a computer network using a network protocol that allows data to be exchanged between two networked devices using data encryption.

Server Virtualization: Software that enables the ability to host multiple operating systems on a single hardware platform.

SPI: An acronym that represents the three major services provided in public Cloud computing: SaaS, PaaS and IaaS.

Storage Virtualization: The abstraction of physical storage from logical storage.

Symmetric Encryption: The encryption of data, using a single secret key for both the encryption and decryption processes.

Utility Computing: A metered computer service in which applications and or storage is available on a needed basis.

VDOMs: Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.

Virtual Appliance: It is a fully preinstalled and preconfigured.

Virtual Private Cloud (VPC): Analogous to a virtual private network (VPN), but the Cloud version of it.

Virtual-to-physical Migration (V2P): The method of installing a virtual operating system applications and data onto a physical server.