University of Venda

CYBERSECURITY FRAMEWORK FOR CLOUD COMPUTING ADOPTION IN RURAL BASED TERTIARY INSTITUTIONS

BY:

PATALA NAJIYABANU NOORMOHMED

STUDENT NUMBER: 11634215

SUBMITTED IN ACCORDANCE WITH THE REQUIREMENTS FOR THE DEGREE OF:

MCOM MASTERS – BUSINESS INFORMATION SYSTEMS

IN THE

DEPARTMENT OF BUSINESS INFORMATION SYSTEMS

SCHOOL OF MANAGEMENT SCIENCES

UNIVERSITY OF VENDA

SUPERVISOR: PROF A. KADYAMATIMBA …….

CO-SUPERVISOR: MR S. MADZVAMUSE ……

2017/2018

DECLARATION

I, Najiyabanu Noormohmed Patala declare that this research titled, "Cybersecurity Framework for Cloud Computing Adoption in Rural Based Tertiary Institutions", is my own work and that all sources I have used or quoted have been indicated and acknowledged by means of complete references. I also declare that I have not previously submitted this work, or part of it, at UNIVEN for another qualification or at any other higher education institution.

Full name: PATALA NAJIYABANU NOORMOHMED

Signature: …… Date: ……

ACKNOWLEDGEMENTS

I would like to thank Almighty God for his unconditional blessings and giving me strength throughout the process leading up to the completion of my research. I would like to thank my supervisor, Prof. Armstrong Kadyamatimba and co-supervisor, Mr. Solomon Madzvamuse, for the supervision and help throughout the research project.

At most, I would like to show gratitude to my parents for their patience, continuous support, motivation and encouragement for completing this research. They were truly an inspiration and the reason for the completion of this research. Many thanks to all my friends specially Naziya, Sahir and Mohomed, who have directly and indirectly supported me and advised me during the study process and completion of the research.

I would further like to extend my gratitude to Mr. Donald Tutani, the Head of the BIS Department, for his ongoing support and encouragement. I would also like to thank my lecturers namely, Mr. Willard Munyoka and Mr. Francis Manzira for their continuous support and knowledge throughout the years.

DEDICATION

I dedicate this research to the Almighty God who was my pillar of strength throughout the completion of this study. I also dedicate this work to my family who was always there for encouraging and supporting me throughout the duration of this research study. Thank you for the love and motivation.

ABSTRACT

Although technology is being progressively used in supporting student learning and enhancing business processes within tertiary institutions, certain aspects are hindering the decisions of cloud usage. Among many challenges of utilizing cloud computing, cybersecurity has become a primary concern for the adoption. The main aim of the study was to investigate the effect of cloud cyber-security usage at rural based tertiary institutions in order to compare the usage with an urban-based institution and propose a cybersecurity framework for adoption of cloud computing cybersecurity. The research questions focused on determining the drivers for cloud cybersecurity usage; the current adoption issues; how cybersecurity challenges, benefits, and quality affects cloud usage; the adoption perceptions and awareness of key stakeholders and identifying a cloud cybersecurity adoption framework. A quantitative approach was applied with data collected from a simple random sample of students, lecturers, admin and IT staff within the tertiary institutions through structured questionnaires.

The results suggested compliance with legal law as a critical driver for cloud cybersecurity adoption. The study also found a lack of physical control of data and harmful activities executed on the internet as challenges hampering the adoption. Prevention of identity fraud and cheaper security costs were identified as benefits of adoption. Respondents found cloud cybersecurity to be accurate and effective, although most of the students and employees have not used it. However, respondents were aware of the value of cybersecurity adoption and perceive for it to be useful and convenient, hence have shown the intention of adopting it. There were no significant elements identified to differentiate the perceptions of usage at rural and urban-based tertiary institutions. The results of the study are to be used for clarifying the cybersecurity aspects of cloud computing and forecasting the suitability cloud cybersecurity within the tertiary institutions. Recommendations were made on how tertiary institutions and management can promote cloud cybersecurity adoption and how students, lecturers, and staff can effectively use cloud cybersecurity.

Keywords: cloud computing adoption, cloud computing security, cloud cyber-security framework.

Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CFA	Confirmatory Factor Analysis
DoS	Denial-of-Service
EFA	Exploratory Factor Analysis
F	Frequency
IaaS	Infrastructure as a Service
IP	Internet protocol
IS	Information Systems
ISS	Information Systems Success
KMO	Kaiser-Meyer-Olkin
N	Number
OS	Operating system
PaaS	Platform as a Service
R	Responses
SA	South Africa
SaaS	Software as a Service
SLA	Service Level Agreement
Univen	University of Venda
USA	United States of America
UTAUT	Unified Theory of Acceptance and Use of Technology
VM	Virtual Machine
VP	Valid Percentage

CHAPTER ONE: INTRODUCTION AND BACKGROUND

1.1. Introduction

Information technology has a significant impact on society (Lee and Chavannes, 2013). Large organizations had the means to afford, access and accommodate modern technologies previously, hence minor, and informal business would endeavor to adjust with similar technologies. However, cloud users within the business sector have recognized the enormous advantages of cloud computing and have adopted it in order to improve their business processes (Ragnet and Leach, 2010). In an effort to attain secure control over the lateest technologies, ICT users in South Africa are progressively discovering innovative information and communication technology services such as cloud computing (Nyoni, 2014). Tertiary institutions have familiarized the concept of cloud not only in their academic environment but in the business context as well. Adoption of the cloud may lead tertiary institutions towards growth, continuity, and agility (Salauddin, 2015).

As the level of cloud adoption increases, concerns regarding how safe the cloud environment have also increased. The essence of cloud computing technology is surrounded by various risks, threats, vulnerabilities, and challenges which requires significant attention by IT security experts in making adoption decisions. Security has been a critical concern which is believed to reduce the growth and acceptance of cloud computing. Cybersecurity is a challenge faced by the users, therefore how the migration towards cloud will affect cybersecurity of the business should be considered prior adoption. Cybersecurity has been broadly defined by (Dlamini, Taute and Radebe, 2011), as the selection of instruments, strategies, security perceptions, security defenses, procedures, risk administration processes, actions, education and training, optimum practices, security governance and assurance methods as well as technologies which supports the promotion of protection within the cyber environment including its users and organizational resources.

1.2. Background of the Study

The notion of cloud computing was primarily discovered in the 1950s represented by the term “utility computing” by John McCarthy in (Karamete, 2015). Cloud computing concept has advanced over time and it is more widely used currently than in the past. The concept is not completely new and thereby has evolved around numerous concepts of utility and grid computing and virtualization (Schubert and Jeffery, 2012). Large IT companies and research enterprises such

as IBM and Gartner have documented cloud computing concepts ambiguously built on its application areas in numerous industries (Sriram and Khajeh-Hosseini, 2010). Despite the existence of various debatable cloud computing definitions, the US National Institute of Standards and Technology (NIST) universally defined cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (which includes, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell and Grance, 2011).

1.2.1. Generations

The first generation of cloud computing was proposed for electronic business which progressed within the internet era (Dinh *et al.*, 2013). The current generation of cloud computing has developed to include IT as a service in the form of customized internet service. It is portrayed as the third wave of internet development after the internet and the web being the first and second (Delic & Walker, 2008). Cloud computing awareness spread in the early 2000s and became popular with the growth of the internet, the progression of mobile computing and recognition of the dot-com bubble (Laudon et al. 2011). Client-server computing has delivered applications that were apportioned to certain hardware mostly located in on-premise datacenters for a period of more than thirty years (Bond, 2015). Yet, the paradigm of on-demand cloud computing allows to conveniently access computing resources through any device connected to the internet at any time (Knorr and Gruman, 2017).

1.2.2. The Influence of Cloud Computing on the Education Industry

Cloud computing manifests an ability to retain a considerable influence on businesses within different industries because of its globalized elevations within the business environment (Pauline, 2014). Amongst African countries, the inclination of cloud computing in South Africa is at maximum with an urge by private sector demands (Sensinye, 2018). Cloud services are offered to different African markets by multinational companies such as SAP Africa and IBM for its Smart Cloud. The expansion of technology has impacted education as a system as it forms a basis for the growth and progress of all other systems (OECD, 2016). It is apparent that educational institutions around the world are dependent on information technology for managing and administrating their daily operations, thus making them amongst the key sectors using information technology for their activities. The South African national education information policy has mentioned that for a

broader education plan, supervision and distribution; it is necessary for the education system to successfully collect, disseminate and analyze information (Van Wyk, 2015).

Cloud computing has an effect on the academe enclosed by learners, lecturers, departmental and admin personnel allowing them to attain enormous amounts of diverse educational and research materials, applications and tools, thus making it beneficial (Cieplak and Malec, 2014). The goal of the Higher Education and Training Department, in the long run, is to execute the educational programs and courses by utilizing ICT (Meyer and Gent, 2016). Higher educational institutions are required to use their potential to enhance the quality of education by widening access to education utilizing online resources such as cloud-based e-learning systems (Pardeshi, 2014). Before the release of personal computers, tertiary institutions made provision of Dialup access for staff, lecturers and students to access mainframe computers on campus through a protocol called Kermit (Hayes, 2008). Although slow, it allowed the university members to connect home and office computers. In 2009, IBM released the publication of its cloud academy, which is a universal platform for the information technology workforce, educators and researchers aiming to develop associated skills and attain best practices for commencing cloud computing (IBM, 2009).

1.2.3. The Urge of Cloud Computing Adoption in Tertiary Institutions

Currently, educational institutions are under increasing pressure to sustain high teaching standards and improve their levels of service delivery to the users on or off campus (Chibaro, 2015). It may become challenging for educational institutions that avoid the adoption of cloud applications to survive in the competitive education industry (Johal, 2015). Tertiary institutions worldwide have given a rise in the demand for cloud computing use for improving their digital visibility. It is the obligation of students in the 21st century to adopt innovative technologies and systems for learning (Angeli and Valanides, 2009). The curriculum, therefore, changes to blended learning which is used to complement the traditional face-to-face teaching and learning system. Learning management systems such as multimedia facilities and video conferencing have been adopted by various Southern African tertiary institutions but still encountered challenges such as high bandwidth, ICT infrastructure costs and unavailability of adequate staff expertise (Unwin *et al.*, 2010; Lwoga, 2012). The manifestation of innovative technologies such as cloud computing enabled higher education institutions to reduce or alleviate these challenges by efficiently using the potential of the cloud services which aided in satisfying both staff and students (Chibaro, 2015).

1.2.4. Resistance to Cloud Computing Adoption at Tertiary Institutions

Despite the enormous benefits of cloud computing adoption such as broad network access, cost savings, and unlimited storage; this is accompanied by a diverse set of challenges and problems (Alshamaileh, 2013). The extensive application and usage of this technology have a significant resistance due to a number of security and trust related issues (Zhang, Liu, Li, Haiqiang, & Wu, 2011). Security has been referred to as the quality or state of being secure and to be free from danger (Whitman and Mattord, 2012). Various levels of security existed within cloud computing such as physical, network, data and information, applications, operations, communications, personnel, and systems security (Whitman and Mattord, 2012). There were generally six cloud computing security principles which included identification and authentication, authorization, confidentiality, integrity, non-repudiation, and availability (Ramgovind, Eloff and Smith, 2010). Since the operational functionality of cloud-based E-learning systems primarily depends on web-based sources, the possibility of attacks through the internet is becoming a threat for e-learners and influences their cloud adoption decisions (Kumar and Chelikani, 2011). Security management standards used by various tertiary institutions are (Kumar and Chelikani, 2011): International Organization for Standardization (ISO) 27001/27002, and IEEE P1484. There are three cloud computing models for delivering cloud services namely Software as a Service, Infrastructure as a Service and Platform as a Service with each requiring a unique level of security (Kandukuri, Ramakrishna and Rakshit, 2009).

A major trend in cybersecurity concerned IT personnel losing control of their technologies (Collin, 2014). It was indicated by (Loanzon, 2014a), that approximately 48 higher education institutions in the USA testified of substantial security breaches within their networks in 2011, where more than 175000 confidential records had been compromised. The occurrence of this incident became a major concern for tertiary institutions as cyber breaches pose a security risk to both information and computer security. According to the US government (2008), cybersecurity is regarded as the preclusion of harm to, safeties of, and reinstatement of computers with its equipment, digital communications services and systems, wired and wireless communications within which information is contained. Cybersecurity ought to secure the accessibility, integrity, validity, privacy, and non-repudiation of information (Moghaddasi, Sajjadi and Kamkarhaghighi, 2016).

1.2.5. The Need for Cloud-Cybersecurity Framework.

As different countries usually regulate their cyber environment using their own policies, it has been a challenge to resolve cross-border cyber issues due to an absence of global cyber laws, thereby hampering the cybersecurity efforts (Jaquire, 2015). Certain developing countries are familiarized with their cybersecurity initiatives, however, adequate cybersecurity frameworks for most of the developing countries necessitated a careful consideration due to a deficiency in infrastructure, resources and development capabilities of local technology. It was stated by (Roscorla, 2016), that higher education encountered cybersecurity challenges such as phishing, cloud security, identity and access management, unsecured personal devices and governance over data security which necessitates the adoption of a cloud cyber-security framework.

1.3. Research Problem Statement

Cloud computing is a valuable platform in both rural and urban-based educational institutions. It has provided institutions in developing countries with the opportunity to efficiently and cost-effectively access remote IT resources on a large scale (Trope, 2014). However, literature revealed that urban-based developed countries have more exposure and opportunities in adapting to the latest technologies compared to rural-based developing countries (Ganesh, 2016; Mbebe, 2017; Salemink, Strijker and Bosworth, 2017). Cloud adoption by tertiary institutions in developing countries is largely unknown (Muriithi and Kotze, 2012). Organizations ought to be conscious of the impending benefits and challenges of adopting this technology.

Security concerns continued to be a primary problem of cloud adoption in South African Universities (Schyff, 2014). Tertiary institutions seemed concerned about how their numerous functional departments will integrate with cloud security controls and at the same time, maintain the availability, confidentiality, and integrity of information (Tout, Sverdlik and Lawver, 2009). Currently, there is no one size fits all solutions to various levels to cloud computing security issues especially within the context of cloud-based cybersecurity.

The problem of the current research was that there were currently no solutions encountered in available literature meeting the specific cloud security requirements of rural tertiary institutions within the context of cybersecurity. Research on cloud cybersecurity adoption, issues, and solutions in higher educational institutions particular was minimal which encouraged this research.

Therefore, there was a need to understand cloud security from the perspective of students, lecturers and staff within tertiary institutions.

1.4. Research Aim and Objectives

The aim of this study was to investigate the effect of cybersecurity on cloud computing usage at rural based tertiary institutions (The University of Venda, and TVET) in order to compare the usage with an urban-based institution (Rosebank College) and propose a cyber-security framework for adoption of cloud computing cyber-security.

The objectives were as follows:

- To determine cyber-security drivers for cloud computing usage and adoption in tertiary institutions.
- To evaluate current cloud computing cyber-security adoption issues.
- To determine how cybersecurity challenges, benefits, and quality affects the cloud usage and adoption decisions within tertiary institutions.
- To determine the cloud cybersecurity adoption perceptions and level of awareness of key stakeholders within the tertiary institutions (UNIVEN and TVET, and Rosebank college).
- To propose a cyber-security framework for adoption of cloud computing in higher education institutions.

1.5. Research Questions

The following were the research questions:

R.Q.1 – What are the cyber-security drivers for cloud computing adoption in tertiary institutions? This question was significant in this study in order to gain an understanding of the role cybersecurity plays within cloud computing. It was also important to identify the factors (drivers) that influence the adoption of cloud-cybersecurity. It was to help in assessing if there was any relevant cybersecurity infrastructure for using cloud computing in tertiary institutions. Additionally, the question was also to aid in identifying and describing the current cybersecurity products and services that can be used within the cloud computing context.

R.Q.2 – What are the current cloud computing cybersecurity issues at UNIVEN, TVET, and Rosebank collage? The question was significant in terms of determining the cloud security issues currently present at UNIVEN, TVET and Rosebank college. It was to assist in determining if there

have been any security incidents in Univen's, TVET's and Rosebank's cloud environment. It aimed to determine if cloud computing enhances cybersecurity within tertiary institutions. It was also to help in describing any difficulties faced by students, lecturers or staff in securing their educational and administrative content.

R.Q.3 – How do cybersecurity challenges, benefits, and quality affect the cloud usage and adoption decisions within tertiary institutions? (are they satisfied with the current security?) The question was to assist the researcher in determining if cybersecurity was one of the reasons for the adoption of cloud computing at Univen, TVET and Rosebank college. The aim here was to determine quality perceptions of cloud-based cybersecurity based on the opinions of the stakeholders at Univen, TVET, and Rosebank. The question assisted in determining the possible challenges and benefits of using cloud-cybersecurity which could influence the adoption decisions within the tertiary institutions. It also intended to support the researcher in establishing if the usage of cloud cybersecurity has or will cause any difference in the business processes of tertiary institutions by establishing the importance of cloud-cybersecurity.

R.Q.4 – Are the stakeholders of UNIVEN, TVET, and Rosebank aware of the major cloud cybersecurity issues and How do they perceive the security aspects of cloud computing technology? This question was significant in terms of recognizing the views or perceptions of stakeholders with regards to cloud cyber-security. It was to assist in determining the level of awareness of stakeholders at UNIVEN, TVET and Rosebank college concerning the major security issues present in the cloud environment. It was also to aid in determining if the usage of cloud computing increases the value of cybersecurity for users within tertiary institutions. Lastly, it was to help the researcher in educating the stakeholders at tertiary institutions with major security threats in cloud technology.

***R.Q.5* – What cybersecurity framework can be suggested for the adoption of cloud computing in tertiary institutions?** This question was of vital importance in terms of identifying the best suitable cybersecurity framework that tertiary institutions can utilize to enhance the usage of cloud computing within their business environment. The question was to assist the researcher in describing the frameworks currently being used in industries and how they can be modified to suit the needs of tertiary institutions in specific.

1.6. The significance of The Study

The rationale of the study was to provide the management, lecturers, and students with a clear understanding of the cybersecurity aspects of the cloud technology enabling them to recognize the use of cloud computing in enhancing the education system. The study intended to contribute to understanding how cloud cyber-security was perceived by users in tertiary institutions. Through this information, it will be determined if cyber-security is a success factor for cloud adaptation in South African rural-based tertiary institutions. The research sought to address the literature gap of the role of security in cloud adoption in rural South African tertiary institutions. Whilst significant literature regarding cloud security prevailed, no research has ever been done regarding the security aspects of cloud computing at the University of Venda. The outcomes of this research would converse towards strengthening the developing literature on cloud security by provisioning information that would guide decision makers in tertiary institutions. The study was to furnish South African tertiary institutions like University of Venda, TVET and Rosebank college with enriched awareness on cloud security services by suggesting a cloud cyber-security framework. The findings of this study can be analyzed and used for future studies as well as provide a benefit to future researchers with similar research areas. The current research was to benefit the following stakeholders at Univen, TVET, and Rosebank:

Students: The current study was to help in identifying the security concerns of students using cloud computing services at Univen such as Blackboard, which is a cloud-based E-learning system. The study was also to provide students with knowledge on the importance of security in utilizing cloud technology for their learning experience.

Lecturers: The current study was significant to the lecturers of Univen, TVET, and Rosebank, as cloud computing has been a vital tool assisting them in their teaching process. The study would determine the level of awareness of lecturers regarding cybersecurity issues of cloud computing especially in the context of cloud-based E-learning systems and Email technology. It was also to aid in identifying the perceptions of lecturers regarding the significance of security in using cloud computing services.

Management and Support Staff: Tertiary institutions are found to make investments in technology for enhancing the overall education system. Therefore, the study was to investigate the security aspects of cloud computing by identifying the security risks, challenges, and benefits in order to provide a justification for their investment. The study was to suggest a cyber-security

framework that the management and IT staff can use to improve the usage of cloud computing both from a business and technical perspective. Using the information provided in the current study, IT managers can improve their service level agreements concerning cloud security with their service providers.

1.7. Scope of the Study

The scope of the current study was confined to tertiary institutions in South Africa specific to the University of Venda, Rosebank and TVET college. The University of Venda is a rural-based comprehensive University containing 8 schools and 58 departments. The target population of the study consisted of information technology users at the University of Venda, Rosebank and TVET college. The subjects were provided with the opportunity to decide whether or not to engage in the study and partake in the surveys. The research was not primarily focused on the subject's societal, racial, ethnic and technological background. However, the research was focused to examine cloud computing cybersecurity issues and how it impacts the adoption of cloud computing within this field.

1.8. Delimitations of The Study

The current study had a few inevitable restrictions in attaining the key aim of the investigation. Firstly, the time constraints contrived the selection of sample size. The nature of the research obligated the researcher to evaluate the respondent's responses and perceptions at a particular time. There was a possibility of some respondents not willing to participate in the study. There was also a possibility of some respondents being deceitful in answering the survey questionnaires which may lead to biases, over-reporting, and under-reporting to the study. Numerous expenses required in administrating the study such as communication, transportation, and costs of attaining appropriate literature positioned the researcher to utilize materials only easily accessible, and hence data accumulated in some instances could remain biased. The transcription of the study was restricted to English phraseology, therefore non-English readers were not to be catered for. The study focused only on security issues of cloud computing within the context of tertiary institutions in South Africa. However, the researcher chose to focus on rural-based universities because of the absence of relevant literature necessary for such universities aiding them in providing the essential insights associated with cloud computing security and increasing the overall computational benefits of such institutions. The urban-based institution which is Rosebank was included for the

purpose of comparisons. Since the research was limited to South African higher tertiary institutions; the literature review is presumed to be appropriate within the South African context.

1.9. Operational Definitions

Cloud computing: for this study, it was regarded as a medium of providing on-demand information technology resources and services adequately and proficiently whilst permitting rapid remote access to these large-scale hardware and software resources (Misra & Mondal, 2011).

Cloud adoption: in business terms**,** is considered as a strategic process of approving and continuously utilizing cloud computing capabilities in terms of lowering costs, alleviating risks, and attaining expanded database resources (HCL Technolgies, 2015).

Cybersecurity: it is a state in which a collection of activities and measures are taken with the aim to protect computers, computer networks, and its hardware and software devices containing information and communication data, from attacks, disruption, threats and unauthorized use of data (Fischer, 2016, pp. 1-2).

Cyber threats/crime: destructive activities, performed by an individual or a group of individuals using computers, internet and IT systems targeting the computers, IT infrastructure, IT systems and internet of another entity or individual in order to jeopardize the availability, integrity, and confidentiality of computer data and systems (IOSCO).

Framework: a basic structure (i.e. overview or outline) underlying a system or concept which supports a specific approach to meet a particular objective and acts as a guide that can be altered and adjusted (Business Dictionary, 2017).

1.10. Outline of the Study

The current research is comprised of six chapters in total and are briefed as follows:

Chapter 1: Introduction and Background: The primary concept of the research was discussed in this chapter. The chapter was essential as it explained the focus of the research in terms of determining the research problem and provided relevant cloud computing background literature. It also highlighted the aims and objectives of the study as it provided a clear research direction. Additionally, the research questions were also formulated to support the aim and objectives of the study which also formed a base for the research questionnaires. The delimitations and essential definitions within the study were also explained.

Chapter 2: Literature Review: This chapter involved presenting an in-depth knowledge of cloud computing, cloud security, and cybersecurity by reviewing existing published literature. The references within the chapter were primarily sourced from relevant textbooks, reports, journals, thesis, and published articles. This chapter was essential as it aided the researcher in identifying current literature gaps to support the foundation of the research. The researcher studied relevant literature on cloud computing usage and cybersecurity within tertiary institutions.

Chapter 3: Research Design and Methodology: This chapter explained the research methods and approaches used in the study. It justified the use of organized strategies for data collection and research instruments in this research as well as provided details on the suitable research design. The chapter also provided a description of the study population used in answering the research questions of the study. The processes used to record and transcribe data collected for data analysis were also discussed. The chapter was essential as it systematically accounted for the processes required in evaluating the use of cloud computing and cyber-security issues within Univen, TVET, and Rosebank college.

Chapter 4: Data Presentation and Interpretation of Results: This chapter demonstrated the research findings in detail which were established through data collected from research respondents and was aligned with the objectives of the study. Data collected was analyzed, interpreted and related to the literature review. The researcher used statistical and descriptive analysis for the data collected.

Chapter 5: Discussions of Findings and Proposed Cloud Cybersecurity Adoption Framework: This chapter discussed the implications of the findings of the study in coordination with the concepts of the study. It also determined if the objectives of the study were achieved and research questions were answered. The chapter also proposed a cyber-security framework that tertiary institutions can utilize based on the results obtained.

Chapter 6: Conclusion and recommendations: The chapter made concluding remarks of the overall research study based on the interpretation of the results. The limitations of the research were discussed and contributions to the knowledge body were highlighted. Finally, recommendations were presented in this chapter which supplemented ideas for future research that were beyond the limits of the current study.

1.11. Chapter Summary

In summary, the current chapter outlined the ustified reasoning of the study disclosing the fundamental concepts of the research. It gave a high-level overview of the research study. The chapter narrated the research problem and objectives to be accomplished. Other sub-sections in this chapter highlighted the background of the research study, research questions, research significance as well as the delimitations of the study. The next chapter covered a brief overview of literature in order to showcase the relationship that occurs between the current knowledge on key areas of the topic under study and provided a basic structure to the study.

CHAPTER TWO: LITERATURE REVIEW

2.1. Introduction

This chapter aims at delivering a critical assessment of the current research study. This includes former research discoveries on the prominence of cloud computing and cybersecurity within the cloud. The purpose of this chapter is to attain a thorough understanding of the research topic by recognizing developing themes with regards to cloud computing cybersecurity within the context of tertiary institutions. A brief overview of the cloud computing paradigm and related concepts are discussed. The characteristics of cloud computing, the cloud deployment and service delivery models for justifying its relevance in tertiary institutions are also discussed. Furthermore, a brief overview of cloud computing adoption in the context of tertiary institutions is presented. The chapter also provides discussions of cloud computing security within the context of tertiary institutions, highlighting the cloud adoption factors in the educational sectors. Lastly, various frameworks in the field of cloud cybersecurity are presented.

2.2. Cloud Computing Trends in Tertiary Institutions - Success Stories

University World News stated that a universal demand for tertiary education will double by 2025 (Tate, 2014). It predicted that the community is most likely to encounter an educational environment where services will be offered on the cloud. Hence, tertiary institutions can highly remain focused on teaching and research activities than managing IT (Shana and Abulibdeh, 2017). The following subsections identified the adoption of cloud computing in various tertiary institutions across the globe.

2.2.1. Adoption of Cloud Computing in Developed Tertiary Institutions

It is mentioned in a survey report by United States Campus Computing that, tertiary institutions in developed countries within the USA has shown above 89% interest in using and adopting the cloud technology. This included institutions such as the Eastern Washington University, Marist College and the University of Virginia among others (Olanrewaju *et al.*, 2017). In Canada, Lakehead University was the first institution to adopt cloud computing for its email and calendaring services in 2006 (Babin and Halilovic, 2017).

With regards to institutions in the United Kingdom (UK), learning management systems have been installed on cloud platforms providing accurate access to study materials on networks (Darus,

Ruziana Binti and Gaminan, 2015). Similarly, in Australia, tertiary institutions such as the University of Melbourne and Monash University have driven innovation through the utilization of cloud with the aim of enhancing critical business processes and investing in facilitating access to cloud capabilities for developing their own cloud resources (Hendrik, 2015). In Asia, India has a considerable interest in adopting cloud services for its educational sector with 44% of tertiary institutions already implementing the technology with an expectancy of reaching up to 61% by the end of 2020 (Vaishali Pardeshi, 2013).

The adoption of cloud technology within Southwestern Universities in Nigeria amounted to 90% due to the utilization of email and collaboration services (Akin, Matthew and Comfort, 2014). According to (Appiahene, Yaw and Bombie, 2016), the application of ICT in Ghanaian universities remained low within the academic context due to which a cloud computing model was proposed and adopted to govern an independent learning style and maintain data access over the internet.

2.2.2. Adoption of Cloud Computing in South African Tertiary Institutions

As stated by (Muriithi and Kotze, 2012), there are currently 23 civic tertiary institutions and 50 FET colleges in South Africa among which only 43% have adopted and used cloud technology. Above 92% have shown to be aware of the technology. In 2016, the University of Cape Town adopted a Cloud First Strategy and aims to migrate all its key ICT components to the cloud by 2020 (Rensburg, 2016). The University of Pretoria has been benefiting from cloud computing in the form of E-education within the field of medical research (Karim and Rampersad, 2017). Students from the University of Pretoria collaborated with the Computational Intelligence Research Group for conducting research on drug treatments explicitly for Africa-based illnesses (Kshetri, 2010).

2.2.3. Adoption of Cloud Computing in Rural Tertiary Institutions in South Africa.

Institutions across the globe with more focus on developing countries have encountered challenges of meeting educational requirements with technological advancements and its dependency (Okai *et al.*, 2014). However, rural-based tertiary institutions have shown efforts in utilizing cloud-based technologies for implementing e-learning, as it has provisioned future strategies for mitigating e-learning challenges enabling to maintain its sustainability and enhance its competitiveness (Odunaike, Olugbara and Ojo, 2012). Cloud adoption decisions at tertiary institutions in

developing countries have certainly inclined due to the awareness of cloud benefits (Sabi *et al.*, 2016).

Although with a rural background, the 2009-2016 strategic plan of the University of Fort Hare in South Africa has shown interest in embracing cloud technologies. The aim was to provide on-demand access to services such as publishing online exam results, processing online registration, performing online leave applications, availing electronics pay slips and conducting electronic payments (Univesity of Fort Hare, 2009).

2.2.3.1. University of Venda's Effort to Bridge the Digital Divide Via Cloud Computing

Univen's latest strategic plan document and a Microsoft report revealed the following information regarding the adoption of cloud computing (Microsoft, 2015; University of Venda, 2016):

Univen has boarded on a striving "smart campus" project for guiding future ICT functions and gaining a completive edge. The university did partner with Microsoft in rolling out ICT operations to the cloud using the Microsoft Azure platform and StoreSimple hybrid cloud storage solution. In order to retain its competitive advantage over other universities, the university took an innovative initiative in 2015 and became the first African university to distribute Windows-Tablets to each first-year undergraduate student for supporting his/her studies. Honors, Masters and Ph.D. students were provided with laptops for supporting their research. The university reformed its operations through the cloud by migrating administrative applications such as procurement and student registration to online platforms. Consequently, Univen has installed Wi-Fi networks with various connection points and increased its bandwidth from 8Mbps in 2008 to 10Gbps by the end of 2015 for reliably supporting the cloud-based activities on campus. Most notably, the university fully embraced cloud opportunities by transforming all teaching and learning back-office administrations towards the cloud-based infrastructure.

- **Notable Benefits Gained Through this Project:**

The productivity of IT staff increased by 14% as the need for fixing constant minor issues are eliminated. Remote upgrades are now performed without IT suppliers' time-consuming visits on Univen premises. Their hardware expenditure decreased by 30%. Access to applications for admin staff resulted to be 20% faster. Online setting and marking of assignments resulted to be quicker for lecturers. The number of incoming students increased by 1000 compared to the year prior to the project implementation. Enhanced e-learning through Windows-based tablets has been

achieved. Resilience and security increased for students and staff. Technology skills gained by students significantly makes them preferably suitable for the workforce, hence making them more productive to be employable. Univen is approached by other regional universities wanting to learn from them.

2.2.3.2. University of Limpopo's TV White Spaces Project – Bridging the Digital Divide

The University of Limpopo partnered with Microsoft, CSIR and the Department of Science and Technology in 2013 and launched the TV White Space Project with the aim of promoting rural economic developments (University of Limpopo, 2014). The goal was to make cost-effective wireless broadband access available for learners in an effort to create new online education opportunities with an improved internet speed (Armerding, 2014). The pilot project hoped to close the present digital divide between Africa and other developed regions by 2020 (Linington, 2014). The TV White Space networks implemented are accessed through smart, radio-enabled devices which then reports their location to a range of cloud-based databases and hence making room for an improved network capacity enabling larger numbers of users to connect simultaneously (Roberts, Garnett and Chandra, 2015).

2.2.4. Education-as-a-Service For Cloud-Based Rural Education

Cloud is seen to be capable of overcoming the sustainability challenges of e-learning implementation (Romiszowski, 2013). Within the concept of education-as-a-service, a cloud-based e-learning system architecture is proposed by measuring its effectiveness in terms of its social, operational, functional and economic benefit analysis (Chang, Walters and Wills, 2015; Masud and Huang, 2016). Chang et al. also developed a cloud-based m-learning architecture for tertiary institutions in Bangladesh (Hossain Masud and Huang, 2013).

The EduCloud framework was proposed for cloud adoption in Indian universities suggesting to deploy a cloud hybrid model for ensuring adequate security (Subramanian and Seshasaayee, 2014). The work of (Shahzad, Golamdin and Ismail, 2014) established a cloud strategy in higher education and highlighted the significance of aligning cloud migration with the organizational IT strategy. The strategy consists of five key components which are: to develop a cloud computing knowledge base, to assess the current stage of the University, to experiment the cloud computing solutions, to choose the optimum solution and to implement and manage the computing solution.

2.3. Cloud Significance in Tertiary Institutions

Approximately 70% of IT managers in tertiary institutions advocated for the use of cloud technology than traditional technology (Odeh, Garcia-Perez and Warwick, 2017). Tertiary institutions are required to create cloud-based IT governance to support decision making, balance opportunities and risks, achieve strategic goals and meet the needs of staff, lecturers and students (Babin and Halilovic, 2017). The significance of cloud computing in tertiary institutions was determined based on its attributes, service models and deployment models.

The NIST established five significant attributes of cloud computing which include: 1) The on-demand self-service, 2) broad network access, 3) Measured service, 4) Rapid elasticity and, 5) Resource pooling (Olive, 2011). With these capabilities, tertiary institutions can obtain cloud resources as required on a pay-per-use basis regardless of the time and location with built-in web browsers (Fehling *et al.*, 2014). Tertiary institutions would be able to acquire new computing resources immediately in an event of a breach. However, since clients with similar security requirements are categorized on a specific cloud offering, an attack towards one user may unintentionally affect other users utilizing the same shared resource (Kok, 2010; Carroll, 2012).

The various types of IT resources that could be offered to tertiary institutions are categorized into three service models which include: 1) Software-as-a-Service, 2) Platform-as-a-Service and 3) infrastructure-as-a-Service (Erl, 2013). With these services, tertiary institutions can access hardware and software which are developed, installed, run, updated and maintained over the internet (Iqbal *et al.*, 2016). Furthermore, central infrastructure assets such as networking and storage resources can be accessed on virtual platforms which save costs (Bamiah and Brohi, 2011). However, tertiary institutions are limited to have control over the operating systems and network storage servers of cloud services providers (Kok, 2010).

The regulation of how and which services can be accessed by tertiary institutions are based on four deployment models which include: 1) public cloud, 2) private cloud, 3) hybrid cloud and, 4) community cloud (Kavitha, 2014). Tertiary institutions could utilize the open-use cloud for serving the general public and multiple organizations off-premise through client access software (Diaby and Bashari Rad, 2017). Tertiary institutions could deploy private cloud for internal use by its employees (Karnwal, Sivakumar and Aghila, 2011). The hybrid cloud could be used for linking tools such as Business Intelligence to various software's requiring standard security and

accumulate sensitive user data through the private cloud (Mukundha and Vidyamadhuri, 2017). Tertiary institutions with comparative aims and central objectives could make use of the shared community infrastructure of the cloud (Manyando, 2013).

2.4. Security Challenges Within the Context of Cloud Computing

In available literature, security and privacy were ranked as major concerns of utilizing cloud systems accredited towards an absence of adequate security control policies, frameworks and substandard security protections (Andreassen and Blakstad, 2010; Muijnck-Hughes, 2011). The primary security challenges for cloud adoption were identified and discussed as follows:

a) **Service-Level Agreements (SLAs):** SLAs in most instances have not provisioned specific clauses for ensuring the level of security being offered by the cloud providers leading to an inadequate security handling process (Pearson, 2012). Therefore, the clients have been usually referred to be liable for the ownership of any security damage and its costs and may not account for any data being deleted, altered, corrupted or lost in a security incident (Mowbray, 2009). SLAs are not being tested by the laws, hence holding back public institutions from adopting the cloud (Charif, 2014). The security standards and metrics are not adequately established and benchmark information regarding security is found to be limited in SLAs which raised compliance issues especially when certifications are carried by a third-party (Hoehl, 2015).
b) **Identity, Authentication and Access Management:** Identity management did involve various security challenges such as identity theft, openness, high and least privileges with its controls (Habiba *et al.*, 2014). Cloud identity management is still developing and lacks well-established standards, hence requiring new identity and access management methods and models for ensuring end-to-end trust and privacy with appropriate authentication (Charif, 2014). Retaining track of numerous logins and identities maintained by employees during their tenancy has been challenging and a secure service configuration was said to be almost unattainable due to inadequate central management of credentials and authorizations (Kumari, 2016). A challenge of providing a single sign in for users exist as numerous cloud applications are not being integrated with identity access management.
c) **Trust Management and policy integration:** These security issues consisted security policy formulation for centralized security systems, formulation of security identification, federal control of trust relationships, stringency in supporting trust relationships on large-scale

networks, deferring trust to outsourced companies and establishing policy language heterogeneity (Noor *et al.*, 2013). The two main categories of trust management techniques concerned with security include the trust assessment layer, and the trust results distribution layer (Noor *et al.*, 2013). The service-oriented nature of cloud computing necessitates access control procedures integrated with requirements-driven trust negotiation practices enabling trust levels to be integrated with security service levels (Munir and Sellapan, 2013).

d) **Cloud Security Audits and Accounting:** A major challenge is concerned with auditors gaining adequate knowledge and familiarity in the cloud context (Ryoo *et al.*, 2014). Obtaining transparency is questioned in areas of data privacy and security, anonymity, accountability, and government controls (Seeburn, 2016). Cloud providers may be accountable for encrypting all the clients' data and relying solely on them may not be safe as they are reluctant or unable to fully disclose specific cryptographic information during the auditing process (Salazar, 2016). A lack of official standards dealing with the issue of standardizing the colocation structure and its security was identified (Chen and Yoon, 2010). Increased scope and scale have led to the complexity of the cloud system's auditing resulting in increased time and resource allocation throughout the process and compliance with international boundaries (Doelitzscher, 2014).

e) **Cross-Organizational security and service management:** The dependency on outsourced organizations raised issues concerning timely responses to security breaches and efficient implementation of disaster recovery and continuity plans (Ristov *et al.*, 2011). The challenge arises when organizations have to re-establish their security metrics and coordinate shared security governance for ensuring reliable and accurate risk measurements (Parekh and Sridaran, 2013). The providers have faced challenges of insufficiently complying with individual security requirements of several varied users and as such contradicts fulfilling security needs of a certain client during the implementation of security requirement of another (Thalmann *et al.*, 2012). Security concerns may also prevail in situations where cloud providers cannot review security contracts with subcontractors, hence unable to detect security violations (McGillivray, 2017).

2.5. Cloud Security according to the Software, Platform and Infrastructure Models

Each model unveiled its own unique characteristics, architecture concerns, and specific intrinsic security defects which may share certain security risks affecting all of them (Carroll, 2012; Hashizume, 2013; Iqbal *et al.*, 2016). Institutions can utilize a shared security model involving the service provider, the service model, the deployment model, and the cloud service features.

2.5.1.1. Security Issues Within the Software-as-a-Service Model

The utilization of the SaaS model has raised security concerns at an increasing level as the users have less control over security compared to other delivery models (Veeramachaneni, 2015). The following security issues were identified within the SaaS model:

a) **Application security:** since the cloud applications are delivered over the internet (Rittinghouse and Ransome, 2009), vulnerabilities may be created through defects in web applications. Attackers may execute malicious tasks from the web such as stealing confidential data and compromising client's computers (Owens, 2010). The traditional security solutions are not effective in firmly securing cloud from attacks (Subashini and Kavitha, 2011).
b) **Multi-tenancy:** since applications in the SaaS model are organized into maturity models determined by scalability, configurability and multi-tenancy features; it uses the same databases for storing data from multi-tenants (Ju *et al.*, 2010). Therefore security risk of data leakage among tenants has increased. There is a requirement for security policies which guarantees each client information to be kept separate from other clients (Bezemer and Zaidman, 2010).
c) **Data security:** a major security concern for SaaS clients has been their reliance on SaaS providers for the enforcement of adequate security controls of their data storages and processes (Viega, 2009). Despite data backup being a vital aspect in facilitating recovery, it also presented security concerns such as outsourcing disaster recovery services from other third-party service providers (Subashini and Kavitha, 2011).
d) **Accessibility:** cloud computing applications can be easily accessed through the internet on web browsers from any network device such as mobile device and Public computers. Therefore, the SaaS model has faced security risks such as mobile malware, information theft, unprotected networks, operating system vulnerabilities and proximity-based hacking (Cloud Security Alliance, 2012).

It was indicated by (Murtada, 2017) in her study that, the SaaS Model is challenged with security threats such as Privacy Breach, Exposure in network/network attack, Impersonation, Application and Interface Security attack, Data Interruption (deletion), Traffic Flow Analysis, Interception on Access Control, Session Hijacking and Modification of data at rest/transit.

2.5.1.2. Security Issues Within The Platform-as-a-Service Model

Application security of the PaaS model consisted of two software layers including the security of the platform itself and security of deployed client's applications on the PaaS platform (Mather, Kumaraswamy and Latif, 2009). The following security issues were identified within this model:

a) **Development lifecycle:** Security of applications would be promptly affected depending on the speed at which applications will change (Rittinghouse and Ransome, 2009). Developers are required to frequently upgrade the applications of PaaS so that the processes, techniques, and standards of application development are capable to adapt to changes (Ertaul, Singhal and Saldamli, 2010). Also, developers must recognize that the security of their applications can be compromised due to changes occurring in PaaS components (Bezemer and Zaidman, 2010).
b) **Third-party relationships:** whilst provisioning programming languages, the PaaS Model also offers web services components of third-party service providers for example mashups (Mather, Kumaraswamy and Latif, 2009). Hence, security issues related to these mashups (i.e. data and network security) while associating and integrating multiple source elements are inherited to the PaaS model (Ke *et al.*, 2009). Clients have expressed security concerns as they are subject to rely on the security of web-hosted developments tools and third-party services (Keene, 2009).
c) **Underlying infrastructure security:** the developers of applications generally have no access to the underlying layers; hence, the cloud providers are obligated to safeguard the underlying infrastructure (Chandramouli and Mell, 2010). Even if the application's security is controlled by its developers, they cannot provide security assurance of the provider's development tools.

Common threats prevailing within PaaS model included (Murtada, 2017): network exposures, analysis of traffic flows, communication disruptions, impersonation, distributed denial-of-service, session hijacking, and software manipulations (i.e. modification, interruption, deletion).

2.5.1.3. Security Issues Within The Infrastructure-as-a-Service Model

Despite the IaaS provider controlling the network and storage infrastructure, the users are accountable for adequately configuring security policies (Subashini and Kavitha, 2011). Extensive efforts are required by cloud providers necessary in securing their systems with the aim to reduce threats (Jaeger and Schiffman, 2010). The following security issues were identified in this model:

a) **Virtualization:** the isolation among virtual machines and hypervisor vulnerabilities presented new opportunities for attackers leading to various security issues such as data leaks and cross

VM-attacks as a result of shared hardware and software resources (Ristenpart *et al.*, 2009). It essential to understand the hypervisors being the main component of virtualization software, Virtual machine's lifecycle, and changes within (Messmer, 2011).

b) **Shared resource:** since the virtual machines are located on the same server, the CPU, memory and input/output devices are shared decreasing the security of each virtual machine (Ranjith, Priya and Shalini, 2012). An attacker (i.e. malicious VM) can gather information about other virtual machines without being noticed as well as leaving the hypervisor uncompromised (Hashizume, 2013).

c) **Network security:** security configuration requirements involve the alignment of protocols systems, firewall technologies, and prevailing solutions within the cloud environment for delivering the needed security and privacy while maintaining performance and efficiency (Hulme, 2011; Oleshchuk and Koien, 2011). The cloud service provider's network security should be offered as an extension of client's existing internal networks for enabling the adoption of local security strategies for protecting remote resources (Jensen *et al.*, 2012).

Additionally, (Murtada, 2017) stated that common threats identified within the IaaS layer include: theft of hardware, modification of hardware, interruption of hardware, abuse of infrastructure, network attacks, connection flooding, denial-of-service, attacks on storage devices, and Virtual Machine provisioning and Migration.

2.6. The Taxonomy of Cloud Computing Security Within Tertiary Institutions

This section identified security issues in tertiary institutions. Each category included several potential security issues leading in a classification with subdivisions as highlighted in several works of literature and presented in Table 2.1.

Table 2.1: Security Issues form Business and Technical perspective (Source: researcher's own)

Security Issues from a Business Perspective	Security Issues from a Technical perspective
Data location: since data can be accessed from anywhere, cloud service providers are required to provide assurance with regards to confidentiality, integrity, and availability of data; and ensure that the location of the data should be in compliance with the laws and regulations within which they operate (Heiser and Nicolett, 2008).	**Browser security**: since the user's devices are used for input/output, user authentication and authorization commands, the development of platform dependent client software is inefficient. It is required to establish a common platform-independency for input/output such as a standard web browser (Parekh and Sridaran, 2013).

Table 2.1. (*Continued*)

Regulatory and compliance: assessment of cloud service security is required by regulatory laws which include ensuring that requirements related to the availability of service, audit capabilities and security procedures are met through SLAs (Krutz and Vines, 2010).	**Lack of security awareness:** security awareness is often a disregarded security concern in the cloud environment. Users of cloud services are required to be educated with regards to various attacks as preventative measures (Khan and Al-Yasiri, 2015).
Web services security: improper configurations and operations of web server results in alteration and exposure of confidential information. The issue of Web server certificate of all web browsers is expected to be from a trusted authority. The SOAP (simple object access protocol) may encounter security challenges of message encryption during multiple sign-ins in the cloud (Jensen *et al.*, 2012; Grobkopf, 2015).	**Application programming interface security:** The architecture of cloud have exposure to attackers since service providers publish their APIs for marketing. Web security risks such as illegal redirects, interrupted authentication, security Misconfigurations, unprotected Direct Object References, Cross-Site Scripting, visible sensitive data, and cookie manipulation can be encountered by users (Veeramachaneni, 2015).
Security governance: includes issues regarding losing security controls within the cloud. Insufficient service level agreements result in security gaps that may or may not be identified in time. Loss of governance over security policies and mechanisms prohibits client-side assessment and tests with regards to security services.	**Investigative support:** Providers are required to make provision for tracking illegal activities. However, the utilization of log files to monitor activities of all cloud clients may be difficult as numerous processing and activities are present. Users may be sharing resources with hackers pretending to be cloud users (Sabahi, 2011).
Vendor lock-in: potential user's dependency on a service provider may become particularly vulnerable to service termination as they are bind with contractual agreements. Therefore, when security breaches occur, they will not be able to migrate to other platforms until the stipulated contractual period terminates (Chow *et al.*, 2009).	**Operating systems (OS) security:** Challenges of protecting the OS from known or unknown threats prevailed within the security design of the software itself. Complicated runtime layouts aid an attacker to exploit vulnerabilities for controlling the running of the OS. When an unprecedented exploit occurs, developers are required to release new software updates and during this process, the OS is left unprotected. (Ibrahim, 2014).

2.7. Cloud Computing Security Benefits

Despite various risks acknowledged in the cloud environment, cloud providers are constantly providing additional protection measures to be security driven in order to sustain their clients and maintain good reputations (Fumeaux, 2016). The benefits of scale enable security implementation measures to be inexpensive. Therefore, the costs of management of patches, sensitivity maintenance of VMs and hypervisors, provisioning of redundant hardware and software, and identity management are reduced. Security-as-a-Service resulted as a strong driver for improving security measures which can be utilized based on the reputation of the cloud providers'

confidentiality and integrity capabilities. Security-as-a-Service model has introduced readily available standardized interfaces for managed security services. The rapid scaling of resources improved the sustenance of defensive measures for an attack as resources can be vigorously relocated. The audit and evidence gathering accommodated the service providers with suitable risk management measures as the storage for logs is provisioned through offline forensic analysis. A different network is used for data backup-servers which reduces the traffic on the primary network (Haeberlen and Lionel Dupré, 2012).

2.8. Cloud Cybersecurity within the Context of Tertiary Institutions

Cyber-attacks reasonably keep transforming the risk landscape as tertiary institutions cannot determine exactly what type of cyber-attacks are to emerge within the next 5 to 10 years' time. Various cybersecurity trends prevailed within tertiary institutions in South Africa which shows that institutions are preparing to defeat cyber-attacks for limiting the risks and improving the reliance (Goodwin *et al.*, 2015)

2.8.1. Cyber-Security Initiatives by South African Tertiary Institutions

Tertiary institutions are becoming huge communities and therefore becoming targets for cybercriminals (Fishman, Clark and Grama, 2018). Various tertiary institutions have taken an initiative of promoting cybersecurity culture as part of their community engagement activities. Table 2.2 represents tertiary institutions identified in literature who have successfully engaged with cyber-security awareness programs in South Africa:

Table 2.2: South African Tertiary Cyber-Security Awareness Initiatives (Source: Researcher's Own)

SA CSA Initiatives	Objectives	Target Audience
Univen-CSIR	Addressing cyber-security challenges in South Africa through a cybersecurity self-defense programme	Non-technical student internet and computer users in Venda
University of Pretoria: ICSA-	Run PumaScope project every year as part of UP's cybersecurity awareness initiatives (Grobler *et al.*, 2011).	Rural schools
University of Fort Hare	To test personal information security competency level as students may be aware of the cyber issue but may not respond to the knowledge obtained (Grobler and Dlamini, 2012).	1st and 3rd-year University Students

Table 2.2 *(Continued)*

Nelson Mandela Metropolitan University (NMMU).	To address all aspects of information security management and create cybersecurity awareness, culture, and education (Dlamini and Modise, 2012)	General NMMU company end-users, entrepreneurs (public or private sectors), children, parents, tertiary and senior citizens.
University of South Africa (UNISA)	To contribute towards the creation of cyber awareness culture by educating individuals of their self-responsibility in securing their computers (Dlamini and Modise, 2012).	School Children

2.8.2. Cloud Cybersecurity Threats in the Software, Platform and Infrastructure Model

Cyber-security threats currently recognized in the cloud computing environment also highlighted in the studies by (Grobler *et al.*, 2011; Hashizume, 2013) are further discussed.

a) **Account or Service Hijacking**: Account thefts may occur through social engineering with the aim of performing malicious activities such as gaining access to sensitive data, manipulating data, and redirecting transactions to illegitimate sites (Cloud Security Alliance, 2016). Service hijacking such as phishing attacks leads to service theft which enables the use of cloud services without billing (Khalil, Khreishah and Azeem, 2014).

b) **Data Scavenging, Leakage, and manipulation**: A probability of data not being completely deleted from a storage area may prevail unless the storage devices are entirely destroyed, hence attackers may have capabilities of recovering the removed data through patching. (Chandna, Singh and Akhtar, 2014). Data is at a common risk of being stolen, exposed or lost due to weak encoding keys, unauthorized access, deletion or alteration without backups through SQL injections resulting in privacy violations (Duncan and Whittington, 2016). Also, attackers acquire the capability of obtaining tokens used by clients for accessing a service via the API and utilize it for data manipulation (Hashizume, 2013).

c) **Denial-of-Service (DOS)**: Occurs when a user is prevented from accessing resources of a specific service (i.e. data and applications) as a consequence of malicious user consuming all the available resources (i.e. network bandwidth, disk space, and memory) within the service. It causes a system to perform slowly making it unable to cater for any further requests from valid users and blocks resources (i.e. Flooding service attack) (Cloud Security Alliance, 2016).

d) **VM Escape and Hopping**: The virtual layer provides for a VM Escape from isolation, allowing the attacker to access the host OSs and various other VMs. Hypervisor vulnerabilities attribute to attack success since they have flexible VMs configurations and complicated hypervisors codes (Munir and Sellapan, 2013). Also, invaders are able to monitor target's resource procedures, manipulate and modify VM configuration and also delete data stored in the VMs to disrupt the integrity, confidentiality, and availability of VMs (Hashizume *et al.*, 2013).

e) **Malicious VM Creation and Insecure Migration**: the attack intends corrupting the cloud providers repositories without compromising the hypervisor layer by placing VM images in public repositories uncontrollably and spreading viruses such as Trojan horse via network or file systems (Khan and Al-Yasiri, 2016). Attackers can get control of incoming migration and move the target VM to the attacker's host server to code malicious information like advertising false resource availability and interrupt normal operations (Jamkhedkar *et al.*, 2013)

f) **Sniffing/Spoofing Virtual Networks**: A malicious VM is used by an attacker for tracking the virtual networks in the cloud. The address resolution protocols (APR) are spoofed for redirecting packets from or to other VMs linking MAC addresses with network IP. It occurs as a result of virtual network vulnerabilities where numerous virtual networks share IaaS virtual bridges.

2.8.3. Cloud-Cybersecurity Attacks Within Tertiary Institutions.

The cyber incidents encountered by tertiary institutions have been identified and summarised in Table 2.3 below (Raman *et al.*, 2016; Lester, 2017).

Table 2.3: Cyber-Security Attacks Faced by Tertiary Institutions *(Raman* et al.*, 2016; Lester, 2017)*

Boston University	WannaCry Ransomware attack encrypting files of the university
Rutgers University	Multiple DDoS
University of Alaska	Phishing scam breached 25000 students, staff and faculty records.
College of Southern Idaho	W-2 scam affected 3000 seasonal and auxiliary employees
Los Angeles Valley College	Ransomware attack taking over the campus email and computer network
Daytona State College	W- 2 Scam and breach of financial aid records.
University of Maryland	Network and database breach 287, 580 records of students, faculty, staff and affiliated personnel.

Table 2.3. *(continued)*

University of Delaware	Cyber-attack exposed identities such as name, addresses, social security numbers, and university IDs of more than 72000 people by exploiting a vulnerable web-based software.
King Saud University	Cyber-attack hacked the official website of the institute compromising records of 812 users dumping information such as email addresses, passwords and phone numbers on a file-sharing site.
Concordia University	Cyber-attack occurred on hardware devices which captured personal data and affected individuals who had utilized affected hardware prior to detecting the attack

2.8.4. Cyber-Security Drivers In Tertiary Institutions

In 2011, The Portland State University proposed a roadmap for its cyber-security within the cloud in order to evolve cybersecurity technology and practices (Loanzon, 2014). The study identified a set of cyber-security drivers to develop a secure cloud environment for tertiary institutions both in the short and long run. These drivers are graphically summarised in Figure 2.1.

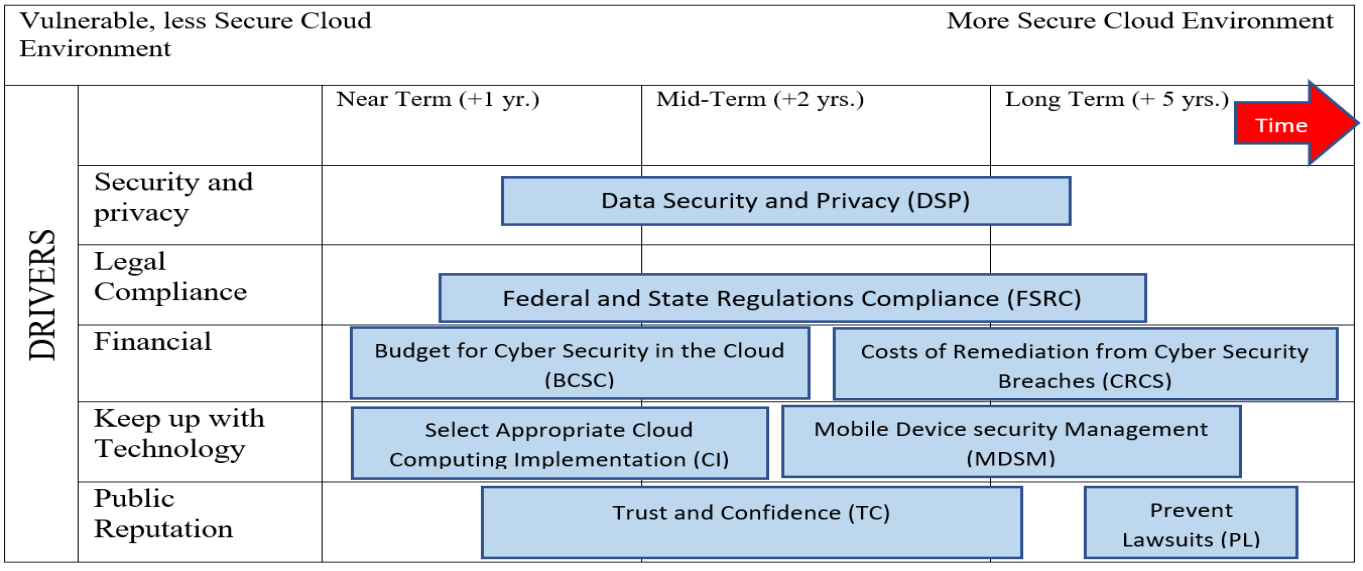

Figure 2.1: Cybersecurity Drivers for Cloud Computing in Higher Education (Loanzon, 2014).

2.8.5. Various Domains Prone To Cyber-Security Challenges In Tertiary Institutions.

After identifying numerous cloud cybersecurity issues from varied studies, the most common domains for cyber-attacks within tertiary institutions are in email, e-learning and library systems as further presented in the sections below:

2.8.5.1. Cybersecurity Issues within Cloud-Based Email and E-learning Systems

The cybersecurity issues specific to email and e-learning systems are presented in Table 2.4

Table 2.4: Cyber-security Issues in Cloud-Based E-learning and E-mail systems.

Cybersecurity Issues In Cloud-Based Email Systems	**Cybersecurity Issues In Cloud-Based E-learning Systems:**
Malware attacks: Attacker embeds malicious attachments in emails or malicious sites using a malicious software through which attacks such as worms and spyware are automatically launched enabling access to the systems and network servers for altering designated privileges (Rossi, 2015; Christin, 2017).	**Bring your own device and remote access:** It is a challenge to determine which personal data is allowed to be processed on personal devices of academics and students and which non-corporate information is being processed through those personal devices (Bandara, Ioras and Maher, 2014)
Spam and Phishing attacks: Phishing emails direct victims to a website that appears to be of a trusted business such as banks. Spams produces unwanted bulk emails as malware to disrupt productivity, unreasonably utilize IT resources, and block email servers and inbox messages (Woodard, 2017)	**Entry points:** Various users accessing e-learning servers from different remote locations resulting in multiple entry points raised the possibilities of attacks. A challenge occurs in implementing the approach of reducing entry points as there are large numbers of simultaneous users from various physical and geographical locations (Kumar and Chelikani, 2011; Zia *et al.*, 2013).
Unintentional acts by authorized users: Employees accidentally send the organization's sensitive information to outside entities through email; creating an opportunity for attackers in getting coverage by causing security incidents and face legal actions (Stine and Scholl, 2010).	**Non-repudiations:** it becomes a challenge when the e-learning systems lose the capability of recovering from data losses and virus infections such as a trojan horse. The system is required to ensure that data is modified during these attacks (Hashemi and Hashemi, 2013).
Malicious intent attack (internal or external): A malicious insider uses company's valuable data to leverage a new position within the company by giving unauthorized access of resources to malicious entities outside an organization's network (Bhardwaj and Goundar, 2018).	**Dynamic sessions security:** the dynamic nature of the e-learning systems enables any process to join or end a group session at any time without being noticed by others (Zia *et al.*, 2013). Numerous security credentials need to be verified for controlling the session levels and members site.

Table 2.4. (*Continued*)

Social engineering attacks: Baiting is used to extract usernames and passwords in exchange for free movies or music content, and Pretexting is used for performing social engineering attacks (Sweeney, 2015). Here, an email may pose to be from the institution's contractors, aiming to gain vital information from the contractor's social media in order to acquire the victim's trust.	**Protection against manipulations:** breach occurs when students uploads fake or incorrect materials (i.e. fake assessments and assignments, alters grading scales or intrude private conversations, submit and view examination before exam dates (Zia *et al.*, 2013). An attacker could also view, delete, and modify course materials on the e-learning platform (Assefa, 2009).
Security from flooding and blocking attacks: e-mail contents will be obtained from an external user hence, monitoring of IP addresses is required. A large amount of requests for accessing the e-mail services is sent leading to a blockage of the entire emails system. (Kumar and Chelikani, 2011).	**Social media aspects:** A possibility may occur where social media hosts and spread viruses such as malware. Blocking access to social media platforms within a university is close to impossible. Identifying devices with such as viruses for maintaining network security is also a challenge (Bandara, Ioras and Maher, 2014).
Cybersecurity Issues in Cloud-based Library Management Systems	
Content security: Challenges of maintaining digital watermarks, digital signatures, passwords, content encryptions, and copy detection systems are encountered by tertiary institutions.	User security: Digital credentials ought to be managed through a client/server model securing communication among the server on the local network of tertiary institutions
Functionality challenges: arise when cloud-based library management system adds new users to the library and search or browse the library for requested contents and encounters a DoS.	**Architecture:** An attack occurs at any architectural layer such as internet, transport or application layer and challenges acquiring security as the contents and operations are decentralized

2.9. Cloud Computing Security Standards

Security communities and initiatives such as ENISA, NIST, and CSA are striving to address security issues within the cloud and alleviating challenges of implementing risk-mitigating controls (Pearson and Yee, 2013). The following standards were identified to have a maximum direct effect on cloud computing security:

a) **Federal Information Security Management Act (FISMA):** Cloud providers accredited with FISMA would automatically be in compliance with the regulations that federal agencies need to follow to achieve data security. Federal institutions must develop, document and implement a program to ensure the security of information and related information systems (NIST, 2016).

b) **Payment Card Industry Data Security Standard (PCI-DSS):** offered cloud providers with a framework for hosting applications requiring a strong data security process for card payments. It is easier for developers to build applications requiring secure credit card payment systems without the need to approach commercial third-party account providers (Kajiyama, 2012).

c) **Health Insurance Portability and Accountability Act (HIPAA):** for ensuring the security of patients' privacy, every health care organization working with protected healthcare information must follow security guidelines of HIPAA (Kajiyama, 2012). The guidelines are not directly imposed on providers, but requires compliance with HIPAA and/or govern secure policies and infrastructure satisfying HIPAA standards for storing sensitive healthcare data in the cloud.

d) **ISO27000:** the International Organization for Standardization (ISO27000) is concerned with information security (Sikhosana, 2015). It contained general security standards which do not address all the security aspects of cloud. A need to provide strict guidelines for accommodating cloud security issues is needed While security needs for the cloud are distinctive, it is still vital for such security needs to be consistent with suitable security standards as the ISO27000.

e) **NIST Cloud Computing Standards Roadmap:** enclosed various aspects of cloud computing including security. As reported by NIST, traditional security processes and mechanisms can be used to address most of the cloud security issues, but where standards for specific security such as cloud cybersecurity does not exist, NIST and other US industry leaders are working on designing standards to accommodate those security needs (Annie and Michael, 2013).

f) **ISO/IEC 27017:** ISO together with the International Electrotechnical Commission (IEC) provisioned cloud providers and clients with implementation guidelines for information security controls. The gap of the standard is only catering for information security (i.e. integrity, confidentiality, and availability) leaving out issues as network and application security existed.

g) **Cloud Standards for Cloud Computing (CSCC):** The subject of the standards is client-focused and provides them with contents such as case studies, best practices, use cases and standards roadmap which can be utilized or reviewed in developing new cloud standards. It is concentrated on public cloud models and presents ten steps each containing various standards and certifications for ensuring security in the cloud.

h) **CSA Security Guidance for Critical Areas of Focus in Cloud:** strived to promote best practices of security within the cloud. It contained two sections: 1) governance of strategic and policy concerns and 2) operating tactical security and its implementation concerns. The identified gap was that the framework being designed is focused on the client-side wanting to migrate to the cloud and not cater to all the security requirements of cloud providers.

i) **ISACA Security Considerations for Cloud:** the independent international organization delivers concrete security guidance, present operative tools, approaches and benchmarks for

analyzing and measuring risks and threats in the cloud sector. The ISACA document identified and covered only four risks events namely unavailability, loss, theft, and disclosure.

j) **ENISA Cloud Computing Benefits, Risks, and Recommendations:** provided security guidelines, risks and advances for cloud users in the context of SMEs and e-health. However, the identified gap is that information security in the context of tertiary institutions is not covered such as the security of cloud-based e-learning systems.

2.10. Existing Cybersecurity Frameworks and Writings

To identify and understand the various elements required within a cybersecurity framework, it was significant to consider the existing cybersecurity policies, strategies, and frameworks employed by various developed and developing countries globally. Reviewing the cybersecurity documentation made by different regional bodies and expert organizations was also significant.

a) **International Telecommunications Union (ITU) Framework:** is a cybersecurity guide for developing countries. The elements consisted cybersecurity accountability, technical and procedural measures, organizational structures for crime units, legal measures, and capability building of skills, training, assurance, monitoring and international cooperation (ITU, 2009).

b) **Cybersecurity Risk Management and Threat Control Model:** is developed for enhancing the protection of information in the Namibian public sector. Issues of cybersecurity threat control, risk management, and security policy framework is covered. It also covers issues of vulnerable information assets, external security controls, internal security controls, uninterrupted service and residual risks (Uudhila, 2016).

c) **NIST Cybersecurity Framework:** consisted of simple and effective constructs of three elements namely: the core, the tiers and the profiles. It has a core structure of five risk management functions namely: identify, protect, detect, respond and recover. The tiers provide a baseline for managing cybersecurity risks. The profiles aim to regulate the organizations "as is" and "to be" risk posture (AWS, 2017).

d) **ENISA Guidelines on National Cybersecurity Strategies:** consisted of the following main elements: defining cybersecurity governance framework, identifying critical information infrastructure and providing an effort to diminish cyber-crime effects. It helps to define an integrated approach for national risk management aiming to improve training and education for security specialists with a focus on current and future security and reliance issues (Enisa, 2012).

e) **African Union on Cybersecurity and Personal Data Protection:** promotes cybersecurity and provides measures for combating cyber-crime present in e-commerce such as protection of personal data and security of electronic transactions. It highlighted the need for a national cybersecurity framework and its legislative measures. It is aimed at providing monitoring structures for national cybersecurity such as cybersecurity governance (African Union, 2014).

2.10.1. Existing Cyber-Security Policies and Strategies

This sub-section identified the national cyber-security policies as implemented in various countries and were explained as followed:

a) **National Cybersecurity Policy in India:** focused on two aspects: 1) the policy objectives to: generate adequate trust and confidence in cyberspace transactions, create an assurance framework, enhance the protection of national critical information structure and develop indigenous security technologies; 2) the strategies concerned with creating: a secure cyber-ecosystem, mechanisms for security threat warnings, cybersecurity awareness, and promoting cybersecurity culture (India Ministry of Communication and Information Technology, 2013).

b) **Malaysia Cybersecurity Policy:** is developed based on a national cyber-security framework including public-private cooperation, legislation, regulatory, technology, and international aspects with the aim of addressing the national information infrastructure containing the integrated information systems of ten sectors within Malaysia. The elements of the cyber-security policy include legislative and regulatory framework, governance, cyber-security technology framework, compliance and enforcement, cybersecurity emergency readiness and cooperation.

c) **Japan cybersecurity strategy:** is developed for social and economic development, crises management and safety and security of public by eliminating national cyber-attacks. It contains principles such as assurance of free flow information, strengthening the risk response measures, shared responsibility and innovative measures for cyber risks (Japan Information Security Council, 2013). It focuses on the construction of a resilient and hygienic cyberspace, strengthening information sharing in companies and educational institutions as well as strengthening capabilities of Japan state level cyber-attacks.

d) **Germany Cybersecurity Strategy:** included eleven elements such as: protection of critical national information infrastructure and services, securing IT in public administration, national cyber response centre and council, effective crime control of cyberspace, effective action for

ensuring cybersecurity in Europe and in global platforms, use of reliable and trusted Information technology, tools to respond to cyber-attacks, sustainable implementation and personal development in federal authorities (Germany Cyber Security Strategy, 2011).

e) **South African Cybersecurity Policy:** it includes six objectives or elements on a national level which are to: establish and facilitate structures for supporting cyber-security, ensure cyber-security threats and vulnerabilities are reduced, promote cooperation and coordination amongst the government and private sector, endorse and strengthen international cyber-security cooperation, build capacity and encourage cybersecurity culture, promote compliance with operational and technical cyber-security standards (Department of Basic Education, 2010).

2.11. Theoretical framework

A theoretical framework is known as a general theoretical system including assumptions, concepts and particular social theories (Alabi, 2016). The need for using theory as a conceptual basis in IS research is urged in various literature (Phillips, 2007; Costello, Donnellan and Curley, 2013). The underpinning theories of the current study were adapted from the Unified Theory of Acceptance and Use of Technology (UTAUT) model and the Information Systems Success (ISS) model within the context of IS security.

2.11.1. The Unified Theory of Acceptance and Use of Technology Model

The model has been proposed by (Venkatesh *et al.*, 2003) as one of the latest developments of general technology acceptance models which aimed to clarify the user's intention of using an information system and increasing usage behaviors. It was validated for providing a unified theoretical basis for facilitating research on ICT adoptions and diffusions (Alabi, 2016). The model presents a more comprehensive overview of the technology acceptance process than prior technology acceptance models (Chibaro, 2015). However, the theory of the UTAUT model identified four main constructs as direct determinants of behavioral intentions for technology adoption and use which consisted of the following:

Performance expectancy: is the extent to which a person believes that utilizing the information system will aid in attaining improvements in his or her job performance. Therefore, it is associated with a user believing that utilizing an innovative information system for performing a task will produce a positive outcome (Chibaro, 2015). **Effort expectancy**: is the extent of easiness or

difficulty associated in using the systems. It enables a user in evaluating the extent of efforts necessary in utilizing a technology (Nyembezi, 2014). **Social influence**: is the extent to which an individual perceives that it is vital for others (i.e. family and friends) to believe that they should utilize a specific innovative system or technology. The concept of this construct is to determine if an individual's behavior influences or is being influenced by believing how others will see them as an outcome of using a technology (Alotaibi and Wald, 2014). **Facilitating conditions:** is the extent to which a user believes that organizational resources and technical support and infrastructure exists for using a system and their perceptions regarding its availability when needed (Alabi, 2016). However, the model also takes into consideration the individual different variables such as age, gender, experience and voluntariness of use which can have an impact or influence on the four determinants of technology acceptance (Venkatesh *et al.*, 2003). Figure 2.2 is a systemic representation of the UTAUT theoretical framework.

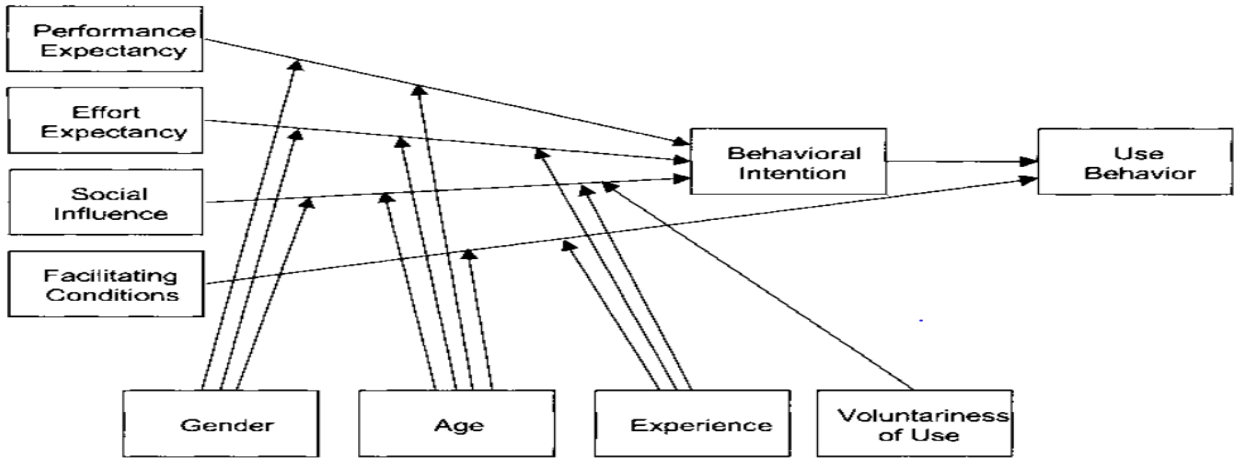

Figure 2.2: UTAUT Research Model adapted from (Venkatesh *et al.*, 2003)

2.11.2. Information Systems Success Model

This theoretical framework is most widely known as DeLone and McLean's IS Success Model. The model is developed for examining the use, user satisfaction and success of an information system or technology (DeLone and McLean, 2016). Information technology such as cloud computing consists of hardware and software utilized by individuals and institutions for gathering, processing, generating, distributing or transmitting information. Therefore, the ISS model was developed for reducing challenges related to defining IS success such as difficulties in handling

the complicated, reliant and multidimensional nature of IS success (Ayooluwa, 2016). Figure 2.4 presents a model with four constructs identified as determinants of information systems success and are explained as identified in a study by (Ayooluwa, 2016):

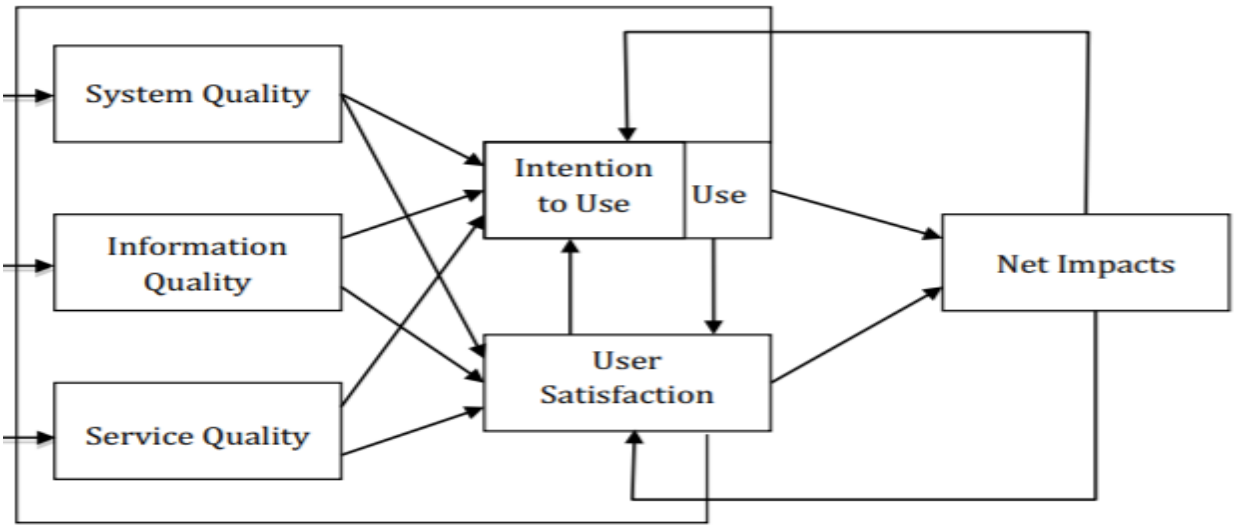

Figure 2.3: ISS Research Model adapted from (DeLone and McLean, 2016).

System quality consists of characteristics anticipated for a system in producing valid information for decision making and involves determining how good a system is with common measures including reliability, stability, ease of access and use, flexibility, user-interface, and response times. **Information quality** consists anticipated characteristics of the output of an IS influencing system use and user satisfaction with common measures including accuracy, usability, completeness, relevance, understandability, consistency, availability and format of information generated by an IS. **Service quality** consists the anticipated characteristics for measuring the quality of the support that is being received by system users from IS departments and IT support; with common measures including accuracy, reliability, responsiveness, and efficiency of a support team. **Use/intention to use**: use refers to the extent and method in which information system is used for a specific activity by customers and employees. The intention of use is commonly an individual level construct. General measures of this construct consist amount of use, number of access, nature of use, usage pattern, the purpose of use, the extent of use and time of use. **User satisfaction** refers to the extent of desire and happiness achieved from using an information system and technology with common measures including accuracy, relevancy, reliability, ease of use and quality of content. **Net impacts/benefits** are referred to as the extent to which an information system contributes to the success of individuals and institutions. The construct aids in determining

the positive and negative effects of information systems on its users through measures such as benefits, impacts, consequences, and outcomes of information system usage.

2.12. Gap Analysis

The major gap identified for the current research was that no other study has been done on cloud cybersecurity within tertiary institutions in Limpopo province from available literature with specific reference to University of Venda, TVET and Rosebank college in Vhembe district. Additionally, the concept of cybersecurity was not being well established within the cloud environment as most of the studies in literature focused on social, technical and economic aspects of cloud security. Furthermore, most of the frameworks were established for cloud computing with a focus on technology adoption without security considerations. Very limited frameworks were available in present literature regarding cloud adoption within the context of tertiary institutions. Very few studies are being conducted regarding cyber-security frameworks from available literature. Despite, no study has established a cybersecurity framework specifically for the cloud computing environment. The current study took all these elements into consideration for making an effort in reducing these gaps.

2.13. Summary

This chapter provided a transitory overview of the cloud computing paradigm and associated concepts. It discussed the characteristics of cloud computing, its deployment models and service delivery models infused within tertiary institutions. The chapter also explained various benefits and challenges of cloud computing security. It also classified numerous security issues within each cloud computing service delivery model with security requirements in each of these models. Cloud security issues in tertiary institutions were recognized from both the business and technical perspective. Furthermore, common security issues concerning email, e-learning, and library management systems within tertiary institutions were discussed. Additionally, cybersecurity concepts were discussed in the context of cloud computing. Various frameworks in available literature were highlighted regarding cloud computing and cybersecurity. A brief overview of theoretical frameworks to be adopted in the current study was presented. Lastly, the gaps in the study were discussed.

CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

3.1. Introduction

This chapter outlined the research design and methodology used in the current study. After identifying the research subject and questions, it was significant to align it with the research design and methodologies in order to formulate a research strategy and add meaning to the study (Kothari, 2016). The chapter also justified the theoretical models used and presented a conceptual framework guiding the study. The chapter aimed to detail the research approaches as well as the researcher's methods for data collection and analysis. Furthermore, it defended the selection of the population and sample of the study for examining the cloud cybersecurity issues faced by tertiary institutions. It also highlighted the internal validity, external validity and reliability issues in the study. Lastly, the researcher explained the ethical measures implemented in the study.

3.2. Conceptual Framework

The conceptual framework categorized and described the concepts related to the study and connected their relationship with the problem statement of the research (Rocco and Plakhotnik, 2009). It enabled to build a research foundation and provided support for the research design, methods, and instruments employed in the study (Maxwell, 2004). The underlying assumptions, expectations, beliefs, and theories from the theoretical framework were infused in the current study to provide a valid structure for informing the research. The identification of themes and constructs applied to the context of this study were important as there are multiple isolated studies identified in the previous chapter which determined the significance of cloud computing in education, however, it still lacked a unified conceptual framework with cases and examples of cyber-security considerations in practice.

The UTAUT in literature has been reflected as the most predictive framework and used as a standard in various technology acceptance researches (Alawadhi and Morris, 2009; Al-Shafi and Weerakkody, 2010). The researcher adopted the UTAUT model because it is comprehensive, reliable, rational and could be corroborated within the context of cloud computing cybersecurity adoption in tertiary institutions. The ISS model was adopted in this study because of its ability to enable the researcher in determining the effectiveness and success of cloud computing cyber-security adoption. As suggested by (George, 2015), the conceptual framework for this research is

presented in Figure 3.1 in a graphical format with narrations explaining the relevance of each construct to the current study.

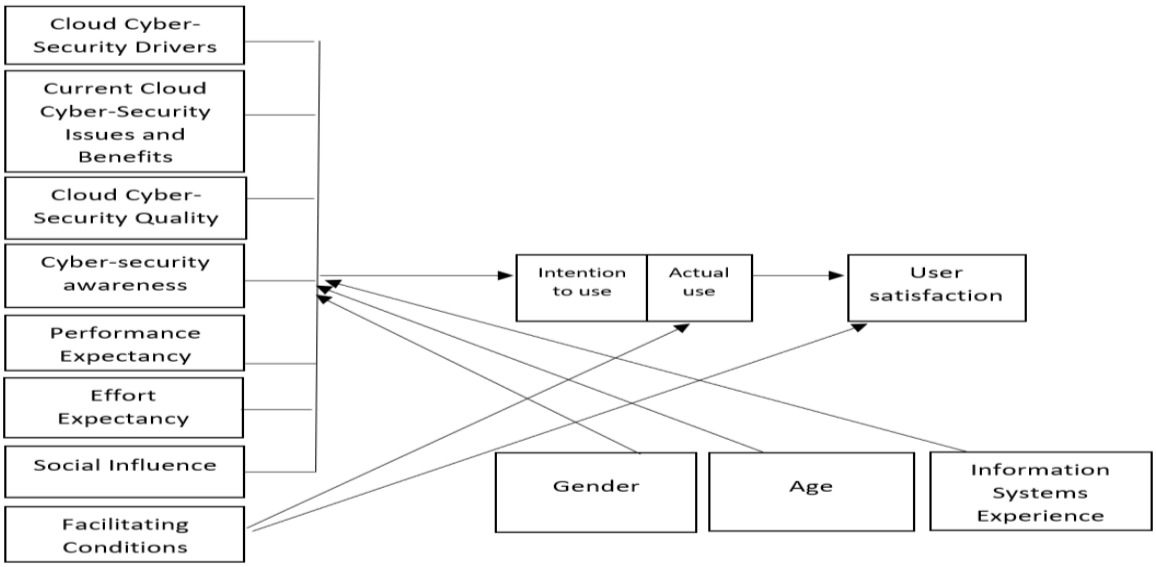

Figure 3.1: Conceptual Framework Derived from UTAUT and ISS Model

The proposed research model for this study also consisted of some modifiers added to meet the objectives of the study. The unified framework attempted to combine the quality dimensions from ISS model with the UTAUT model as antecedents for the intention of use with an effort to disclose the role of quality in using cloud computing cybersecurity in tertiary institutions. The acceptance of cloud computing cyber-security was clarified through the intention to use the cloud-based cyber-security services. The conceptual framework of this study hence consisted of eight direct intention to use and user satisfaction determinants with three moderators that could have an impact on adoption. Four constructs were adopted from the UTAUT model namely performance expectancy, effort expectancy, social influence and facilitating conditions, while three constructs (systems, information, and service quality) from the ISS model were merged into a single construct known as quality. Amongst the three moderators, two were adopted from the UTAUT model namely gender and age, while the information systems experience replaced the voluntariness of use construct to fit the research context. The three additional constructs added to the framework were cloud cyber-security drivers, cyber-security awareness and current cyber-security issues and benefits. Each construct of the framework is justified as follows:

a) **Performance expectancy** of cloud cyber-security was measured as the degree of usefulness that users perceived from using cloud cybersecurity services. The degree of usefulness in this study was achieved by measuring factors such as convenience, time-saving, efficiency, and process complication of securing contents using cloud cyber-security.

b) **Effort expectancy** of cloud cyber-security was measured as the degree of ease associated with University stakeholders' use of cloud cyber-security. The degree of ease of use in this study was achieved by measuring perceptions of ease of use of cloud cyber-security, ease of interacting and learning how to use cloud-cybersecurity system and services, and how easy it is to become skillful in the use of cloud cyber-security.

c) **Social influence** of cloud cyber-security was measured as the degree to which other people and lifestyle influence the use of cyber-security services. The degree of influence in this study was measured by the perception of how peers, colleagues, family members, and working environment affects the use of cyber-security services by members of the tertiary institution (i.e. student, staff and academics).

d) **Facilitating conditions** of cloud cyber-security were measured as the degree of required access available for using cloud cyber-security services. The degree of service access in this study was achieved by measuring perceptions of individual's ability in obtaining the resources and knowledge for using cybersecurity and the support available with assistance in any difficulties encountered while using the service.

e) **Quality** of cloud cyber-security was measured as the degree of information, system and service quality of using cloud-cybersecurity. The degree of information, system and service quality in this study was achieved by measuring the perceived accuracy, reliability, relevance, responsiveness and value of cloud cyber-security to members of the tertiary institutions.

f) **Cloud cyber-security drivers** were measured in terms of factors contributing to the adoption of cloud cybersecurity. The degree of factors contributing towards adoption was achieved by measuring perceived improved data and information security, financial reasons, the pace of keeping up with technology, maintaining the public reputation and legal law and regulatory compliance.

g) **Cyber-security issues and benefits** were measured in terms of perceived challenges and benefits of using cloud cyber-security.

h) **Cloud cyber-security awareness** was measured as the degree of awareness individuals in the tertiary institution has regarding cloud cyber-security. The degree of awareness in this study

was measured through perceptions regarding the risks and opportunities of cloud-cybersecurity, awareness and training programs.

i) **Age, Gender and Information systems experience** were moderators which enabled the researcher in determining their role and influence towards the adoption and usage of cloud-cybersecurity.

j) **Intention of use and User satisfaction** in this study were the factors determining the acceptance or rejection of the technology and the perceived satisfaction tertiary institutions cloud achieve from adopting the technology.

3.3. Philosophical Research Paradigm

A research paradigm is an approach that allows the researcher to explain the basic set of ideas, believes and assumptions that would shape the development of the research (e.g. what knowledge will be obtained from this research) and worked as a framework that is used to observe and understand the research phenomena (Babbie, 2010; Barbara, 2012). It is stated by (Chibaro, 2015) that, these have been informed through philosophical assumptions about ontology (i.e. the study of human being and nature of reality) and epistemology (i.e. the nature and forms of knowledge). In this study, the researcher and the researched are autonomous entities (Scotland, 2012).

The epistemological assumptions of the current study was objectivism, and ontological assumptions were based on realism with a positivist theoretical perspective and a deductive approach (Creswell, 2013). According to (Mubarak, 2014), it has been noted that most IS research studies have recognized positivism as a key epistemology in IS context and has been justified by many academics in the field such as by (Straub, Boudreau and Gefen, 2004; Yin, 2006; Galliers, Markus and Newell, 2007). The study adopted positivist epistemology to examine assumptions and gain insight towards an increased understanding regarding the challenges, benefits, quality, and drivers of cloud computing cyber-security acceptance and usage by conducting a study of knowledge in cloud-cybersecurity adoption within tertiary institutions (Patel, 2015). Research questions have been put forward as assumptions that could be empirically tested under controlled conditions (Jokonya, 2014). Realism ontology ruled out the conscience of the researcher from the research results which allowed the researcher to be neutral (Liya, 2014). The deductive approach aided in discovering casual relationships between cloud cyber-security constructs (i.e. effort and performance expectancy etc.) and its adoption or actual use in tertiary institutions (Neuman, 2009).

Positivism also enabled to generalize and determine common content as well as aided in predicting patterns of adoption behavior among key university stakeholders (Introna, 2015). For instance, knowledge could be obtained regarding the role of cyber-security awareness in the adoption of cloud-cyber-security services. Objectivism allowed to collect more factual information which can be described, measured and observed quantitatively (Alharbi, 2016).

3.4. Research Design

A research design is been defined by (Babbie, 2010) as a framework or plan on how the researcher anticipates administering the overall research. It focuses on the type of empirical evidence required to address the research problem by specifying the philosophical assumptions, research methods, data collection activities and analysis processes (Creswell, 2014). As detailed by (Gray, Grove and Sutherland, 2016), research design is a blueprint for regulating the methods and procedures for obtaining and analyzing the required information in a structured manner in order to answer the research questions as intended. In the current study, the research design was applied for ensuring the selection of suitable research sites and subjects as well as determining how, when, where and in which condition data is to be collected and analyzed (Liya, 2014). The research design of this study followed a logical approach to reduce or eliminate the factors which might have interfered with the validity of the research output and present credible results (McMillan and Schumacher, 2010). Various types of research design include exploratory, descriptive, explanatory, experimental, case study, survey and comparative (McMillan, 2014). The current study adopted a survey research design.

3.4.1. Survey Research Design

The survey design aimed at collecting information about one or more groups of subjects from a large population by studying the characteristics of the specific sample drawn (Fowler, 2009). The large sample size in the survey research distinguished it from other research designs and methods. A survey design was suitable for this study because of the large number of students, lecturers and staff involved and diversity of their location in three sperate institutions (i.e. Univen, TVET, and Rosebank). With this in mind, the given economic resources and time constraints made it difficult to reach all of them through a case-study design for conducting in-depth interviews or perform direct observations on the field (Beukman, 2005). In the current research, a survey design allowed the researcher to give the same status to all the respondents of the study (Jacob, 2007). Hence, the

same information could be obtained from each respondent in the same manner such as regarding the challenges and benefits of cloud cyber-security (Fellegi, 2010). By using this design, relationships occurring among various variables identified through research questions could be examined without any planned interference from the researcher (Ziehl, 2013).

Survey design has been proven to be a valuable source for statistically measuring beliefs, trends, values, demographics, opinions, and attitudes of a sample population which in this case was regarding cloud cyber-security adoption in tertiary institutions (McMillan, 2014). It is a powerful tool used in presenting a unique case in discovering new phenomena as it allows to collect information which is unavailable from other sources (Owens, 2002). Within the context of this study, the current rate of cloud-cybersecurity usage was unknown and hence could be established through surveys. According to (Creswell, 2014), implementing a survey design leads towards drawing valid conclusions providing a reference to generalize results to a population in a different setting such as other rural universities across South Africa. The current study employed a cross-sectional research design for collecting data at a single point in time using the questionnaire instrument by posing a set of questions to the respondents (Hall, 2011). This was a valid measurement design as the questionnaires would accurately measure the cloud security concepts the researcher intends and narrows the gap between what the researcher wants to measure and the actual results (Fink, 2016).

3.5. Research Methodology

Research methodology is the researcher's overall approach in conducting research (Leedy and Ormrod, 2013). IS research mainly follows quantitative, qualitative or mixed method research methodologies based on a particular research situation and its selection is dependent on the nature of the research together with the aim, assumptions and research questions of the study (Creswell, 2014).

3.5.1. Quantitative Approach

Quantitative approach has been most commonly adopted to study natural phenomena without changing or adjusting the research situation (Carroll, Van Der Merwe and Kotzé, 2011). As supported by (Trope, 2014), the research approach in this study was directed by the underpinning philosophical assumptions, hence, the positivist perspective with an objectivist ontological position suggested the use of quantitative research approach. The aim of using quantitative

approach was to determine facts, predict and explain the phenomena of cloud cyber-security adoption through numerical data collection which could be further analyzed based on computerized mathematical methods (Introna, 2015). This method allowed the researcher to generate quantifiable data regarding factors contributing to or hampering the use of cloud-based cyber-security services (Alharbi, 2016). Furthermore, mathematical data could be obtained through a formalized and systematic process of investigation (Perumal, 2014). Quantitative research yielded a better understanding of the relationships established amongst the measured research variables (Gray, Grove and Sutherland, 2016). Therefore, the researcher was able to make comparisons among the relationship between age, gender, and experience with behavioral intention and use of cyber-security for academic and non-academic purposes within Univen, TVET and Rosebank college.

However, not all data collected in this research naturally appeared to be in a quantitative form such as respondents attitudes and beliefs regarding cloud cyber-security (Muijs, 2011). Therefore, the designing of the research instrument accommodated for the conversion of such data into producing quantitative data by allocating numeric scales on a series of statements regarding the research phenomena (Nedev, 2014). The quantitative method was valuable for this study as it eliminated bias form the researchers' viewpoint (Bacon-Shone, 2015). Additionally, the quantitative approach enabled the researcher to developing knowledge through pre-determined instruments such as structured-questionnaires (Creswell, 2014).

3.6. Population and Sampling

The population, sampling size, sampling frame, and sampling procedures were further discussed.

3.6.1. Population

A population is regarded as the total number of elements which are of the researchers' interest from which data can be potentially sourced (Gray, Grove and Sutherland, 2016). It is indicated by (Muijs, 2011) that, a population consists of an entire set of individuals, entities, objects, data or events that share common characteristics to which findings can be generalized based on the conditions of the study. The target population is labelled as those elements that satisfy the eligibility criteria of actual inclusion in the study (Alabi, 2016). The inclusion criteria for participation in this study was for the respondent to be registered within the University of Venda, TVET and Rosebank college.

The population of this study was divided into four identifiable categories namely lecturers, students, admin staff and IT personnel. The accessible population in this study depending on their availability consisted of lecturers and students from eight schools in Univen, six schools from TVET college and four faculties from Rosebank as they were considered to be potential users and adopters of cloud computing technology. Therefore, it was important to understand their views regarding the use of cloud-computing cyber-security services within tertiary institutions. Admin staff was also considered as an appropriate population of the study because they were prone to performing certain routine activities using cloud computing technology. Therefore, it was vital to establish if they have encountered any cyber-security issues whilst using cloud technology. Furthermore, IT personnel were also relevant target population for this study because they are well-positioned to understand and manage cloud cyber-security services. They were the decision makers in the acquisition, installation, and deployment of cloud cyber-security; they interact with students, staff, and academics in assisting them with any cloud-cybersecurity issues. They could also provide important knowledge on current and future plans pertaining to the use of cloud cyber-security.

Without including all the groups mentioned above, the findings of this study would have been restricted to one viewpoint and would not draw a broad and inclusive picture about cloud cyber-security services in rural tertiary institutions in South Africa. However, given that the population specified is too broad, a sample was needed to be studied for this investigation.

3.6.2. Sampling

According to (Leedy and Ormrod, 2013), a sample is a sub-unit of elements or fraction of a whole population nominated to be studied for the purpose of analyzing their potential relevance to the research problem. Sampling is the procedure utilized in the selection of a subset or unit from a larger population as a foundation for appropriately representing the entire population (Polit and Beck, 2016). Sampling was important in this study as the population was too large and yielding information from the entire population of Univen, TVET and Rosebank might have been time-consuming, expensive and not easily reachable (Creswell, 2014). It is stated by (Goran, 2016) that, the higher the representativeness of the sample, the higher the quality of the study. Through sampling, greater precision of sample size was achieved and bias in sample selection was avoided enabling to draw valid conclusions about the entire population (Muijs, 2011).

3.6.3. Sampling Methods

The methods for gaining a representative sample is classified into two main types which are probability and non-probability sampling (Creswell, 2014). Probability sampling is referred as a method for selecting a sample randomly in which each element of the population has a known positive probability of being chosen, hence promoting its accuracy through the measurement of errors (Jacob, 2007). Non-probability sampling is implied as a method in which the unit of the population does not have an equal opportunity of being selected (Bacon-Shone, 2015). Due to the nature and objectives of the research, the researcher used both probability and non-probability sampling methods for providing more perspectives on the issue being investigated.

The study used probability sampling because it is most frequently associated with survey research strategies and therefore allowed the researcher to set parameters for ensuring that the lecturers, admin staff and students have a known non-zero probability of being selected (Chibaro, 2015; Fink, 2016). This method was ideal as it allowed the researcher to assume that the characteristics of the chosen sample for determining the adoption of cloud cyber-security are approximately equal to the characteristics of the entire population (Liya, 2014). Non-probability sampling was used to obtain data from IT personnel as the researcher believed them to have specific knowledge which could add value to the research study.

3.6.4. Sampling Techniques

The current study employed two sampling techniques derived from probability and non-probability sampling methods which are simple random sampling and purposive sampling.

3.6.4.1. Simple Random Sampling

In simple random sampling, the sample is extracted using a mathematical random procedure after developing a sampling frame enabling to locate a precise unit to be selected for inclusion (Babbie, 2010). This technique was vital for this study since each element of the population of interest is relatively homogenous (Alvi, 2016). This sampling technique was applied on students, lecturers and admin staff at Univen, TVET and Rosebank in order to give them an equal and independent chance of being selected (Bacon-Shone, 2015). The selection of one respondent did not affect the selection of another (Jacob, 2007). According to (Richardson and Gajewski, 2003), simple random sampling is a common design to be used when very less is known about the population beforehand.

Therefore, this technique enabled the researcher to study the perceptions of students, lecturers and admin staff regarding the usefulness of cloud cyber-security in tertiary institutions.

The sampling procedure: Depending on the willingness of participation, the selection of lecturers and students was based on the total number of students and lecturers in each of the schools at Univen, TVET and Rosebank whilst the selections of admin staff were based on the total number of staff in each department. The list of all these elements was requested from the IT department at Univen, TVET, and Rosebank college.

3.6.4.2. Purposive Sampling

In purposive sampling, the sample is extracted based on the researchers' knowledge and experience of the sample population (McMillan and Schumacher, 2010). It is asserted by (Gray, Grove and Sutherland, 2016) that, the sample size in this technique is relatively small. The purposive sampling was applied to IT personnel at Univen and TVET college because they are actively involved with matters regarding cloud cyber-security on behalf of their respective institutions. Since IT personnel has rich knowledge about cloud cyber-security services, through purposive sampling, the status and role of cloud-cybersecurity use at Univen, TVET and Rosebank college could be determined.

The sampling procedure: The researcher selected potential members from the IT department. The selected members were approached seeking their participation in the study. The researcher explained the purpose of the study and the value of their contribution.

3.6.5. Sample Size

The sample frame consisted of a list of all the respondents (i.e. students, lecturers, admin staff and IT personnel) from Univen, TVET and Rosebank college from which the population sample was chosen (McMillan, 2014). The University of Venda consisted of the following population: students (17105), staff (1180), and lecturers (418). TVET college consisted of 15000 students, while Rosebank college consisted of 1200 students and 121 lecturers. The sample size for the current study was the number of participants chosen for data collection (Creswell, 2014). A total of 255 questionnaires were distributed at Univen and 140 at TVET and 100 at Rosebank college due to time and cost constraints.

3.7. Data Collection

It was highlighted by (Gray, Grove and Sutherland, 2016) that data collection is a process of gathering data from selected participants of the study in order to answer the research questions. The researcher used both primary and secondary data collection sources for developing appropriate knowledge concerning the adoption of cloud cyber-security in tertiary institutions (Liya, 2014). The research instrument employed in this study was a structured questionnaire as a fact-finding strategy. The questionnaires were used to motivate students, lecturers, admin staff and IT personnel to easily communicate their views and opinions on the usage of cloud cyber-security and its effectiveness in various academic and non-academic purposes.

3.7.1. Data Collection Sources

Secondary data also known as literature review based data, was significant in this study in order to present knowledge regarding the concepts of cloud-cybersecurity and its relevance within tertiary institutions (Liya, 2014). Various theories were identified from previous studies through which the theocratical framework of this study was developed and used to conduct the empirical research (Peersman, 2014). Relevant cloud computing and cybersecurity related documents, books, articles, reports and journals were gathered and studied to gain an understanding regarding the challenges, benefits, and factors influencing the adoption of cloud-based cyber-security which then contributed towards the development of the questionnaires. Primary data is referred to as data which addresses a specific problem, it is collected for the first time and was previously unknown (AJAYI, 2017). The researcher used primary data as the main source of data collection enabling the researcher to significantly discover the reality pertaining towards the perceptions, behavior understanding, beliefs and satisfaction regarding the use of cloud cyber-security (Kumar, 2013).

3.7.2. Data Collection Instrument

According to (Nyembezi, 2014), data collection instrument is a tool used for collecting data required for the research. A structured questionnaire was used as a quantitative method of inquiry for addressing the research questions (Ayooluwa, 2016). It consisted of a series of pre-determined and related questions posed which were answered directly by the respondents for the purpose of obtaining useful information in establishing the acceptance and use of cloud cyber-security in a tertiary institution (Chibaro, 2015). The questions posed to the participants were close-ended in

nature because they were easier to code and analyze, allowed to standardize data and enabled the participants to quickly and easily complete the questionnaires (Alabi, 2016). Furthermore, the researcher did not adopt open-ended questions because respondents may not be able to accurately understand and interpret the questions. The current study implemented a self-administered questionnaire technique as it helped the researcher to extract satisfactory data from participants with a high response rate (Apulu, 2012). The questionnaires were used in this study because they are simple, cost-effective, quicker to simultaneously administer and enables to screen large numbers (Jacob, 2007). Additionally, questionnaires also enabled participants to react to the questions at their own convenience anonymously, hence promoting more honest answers (Muijs, 2011).

3.7.2.1. Questionnaire Design

Questionnaire design mainly relies on how it will be distributed, received and collected (Kumar, 2013). Its design follows three basic approaches which are: to adapt questions from prior studies, to adapt questions from relevant studies and develop own questions. The purpose of this approach was to ensure that the researcher collects suitable data, reduces bias in question formulation, makes data comparable and open for analysis and lastly to make questions engaging yet diverse.

In the current study, the questionnaire contents were guided by the literature review and the theoretical framework in alignment with the research questions and objectives. The researcher modified the UTAUT questions from previous studies to determine usage and adoption behaviors of cloud cyber-security. In order to ensure that the questionnaire covered all the research questions, various articles were studied from which related questions were formulated regarding the challenges, benefits, and drivers of cloud cyber-security adoption. The researcher kept caution of the following criteria in designing the questionnaire (McMillan and Schumacher, 2010):

- Use of clear and simple language to provoke the interest of the participants.
- The length of the questionnaire to be enough in getting the necessary information.
- The questions to be logical in order to avoid confusion about the questionnaire's purpose.
- The time it takes to complete the questionnaire to be enough for avoiding incomplete questionnaires.
- Distribution to a larger number to obtain a higher response rate.

There were four separate questionnaires designed for each sample sub-set. The format and content of the questionnaire were divided into various sections for easy reading and completion. The items of the questionnaire were rated based on a 5 point Likert scale ranging from strongly agree, agree, neutral, disagree to strongly disagree. It also included dichotomous questions with a yes or no response. Multiple response questions were included to obtain various probable answers to a specific question. The organization of the questionnaire was as follows: Cover letter: which explained the aim and purpose of the study, Section A: aimed to collect background information, Section B: covered the usage of cloud cyber-security and aimed to depict drivers for its adoption, Section C: covered the challenges, benefits and quality of cloud-based cyber-security, Section D: covered cloud cyber-security perceptions and awareness based on statements adapted from the UTAUT model.

3.7.2.2. Administration of The Questionnaires

The questionnaires were self-administered by the researcher with some aid from the research assistant. The questionnaires were pre-tested before distribution to the actual sample. The researcher engaged with one research assistant in collecting and distributing the questionnaires from respondents within Univen, TVET, and Rosebank college. The researcher or the research assistant explained the aim of the study and the significance of their contribution to the respondents. The respondents were expected to complete the questionnaire and return it within a period of five days to ensure a faster data collection process. However, if this in cases where that was not convenient, the researcher extended the days depending on the respondents' schedules but ensured overall data was collected within a period of one month. The researcher and research assistant personally collected the questionnaires from the respondents. However, if lecturers, staff and IT personnel were not available physically in their offices, a web survey link would be emailed to them. Once the data collection phase was completed, the data was being prepared for analysis. The following processes were followed in accurately representing the data collected (Nyembezi, 2014):

- Data editing: the questionnaires were verified by checking the accuracy of data, errors, and omissions. Any wrongly completed questionnaire was identified and eliminated from results. Any incomplete questionnaire was coded for data which was submitted.

- Data coding: the responses from the questionnaire were assigned with numeric values for easy identification and organization.
- Data classification: the data was categorized or grouped based on the response type for making data presentation easier for analysis.

3.7.2.3. Pilot Testing

According to (Leedy and Ormrod, 2013), it is significant and highly recommended to pre-test questionnaires on a smaller population before deploying to the actual sample. The purpose of pre-testing in this study was to detect any faults, weaknesses, ambiguities, and inadequacies in the instrument (Apulu, 2012). The researcher pre-tested the questionnaire with a small group of lecturers, students, admin, and IT staff in order to test the quality of the questionnaire. Pre-testing enabled the researcher to determine if the questions and instructions were clear and understandable, identify any errors, improve wording, eliminate unnecessary questions and make any modification suggested from the feedback (Chibaro, 2015). Any issues regarding the design, layout, grammar, sequence, and length of the questionnaire was also clarified (Goran, 2016).

3.8. Data Analysis

It has been mentioned by (Fink, 2016) that, data analysis remained essential for any research as it allowed to effectively organize, manage and understand the collected survey data. In this study, data analysis was necessary for presenting a clear picture of the current cyber-security trends and practices in tertiary institutions. According to (Alshehri, 2012; Maluleka, 2014), data analysis is the process used to examine, categorize, group, recombine and summarize raw data for obtaining valuable information in answering the research questions and bringing meaning to the study. The current study employed a quantitative approach for data analysis because it allowed for data interpretation through numerical calculations (Creswell, 2014).

Descriptive analysis method was used to analyze statistical data for establishing similarities and differences among characteristics of respondents and the relationship between various variables of the study (McMillan and Schumacher, 2010). Descriptive analysis was in the form of frequencies and percentages, which were used to describe the respondents profiles and factors which facilitated or impeded the adoption of cloud cyber-security from the perspectives of the lecturers, admin staff, students and IT personnel (Alshehri, 2012). The method also aided in determining the measures of

mean, median and mode as well as range, variance and standard deviation of the variables of the study (Apulu, 2012). The descriptive analysis was conducted using the Statistical Package for Social Sciences (SPSS) tool in order to capture, code and categorize data as well as identify patterns while MS Excel was used to create graphs, charts, and tables for visually presenting the data (Uudhila, 2016). The SPSS software was used because it allowed to code, retrieve and store data flexibly and provided various built-in tools to classify, sort, and arrange data effectively presenting accurate and automated results (Alarifi, 2013).

3.9. Validity and Reliability

It was significant to take into consideration the threats to validity and reliability for justifying the quality of the research. Validity and reliability were the two measurements considered for this quantitative research in determining the quality of the research instrument used for data collection.

3.9.1. Validity

Validity is referred to as the extent to which inferences drawn from data collected delivers an accurate description of what was intended to be measured (McMillan and Schumacher, 2010). The researcher considered a number of validity measurements for ensuring the validity of the research instrument which were as follows:

a) **Face validity** enabled to inspect if the questionnaire will adequately appear to measure the concept of the study (Nyembezi, 2014). In the current study, face validity was obtained by conducting a pilot-test to validate the significance of each item included in the questionnaire and eliminating irrelevant, unclear and ambiguous questions while determining if there was a logical link with the objectives of the study (Babbie, 2010).
b) **Content validity** enabled the researcher to inspect if there were sufficient questions included in the instrument to address all the objectives of the study (Neuman, 2009). It also allowed the researcher to check if the items were connected with existing theories. The scales used in the questionnaire were also pre-validated from literature and the test was based on the researcher's judgement as no objective technique existed (Trope, 2014; Mohajan, 2017). Therefore, the researcher submitted the questionnaires to the research supervisors who evaluated if appropriate content was covered regarding the concept of cloud cyber-security adoption.
c) **Construct validity** enabled the researcher to align underpinning assumptions with theoretical concepts (Kimberlin and Winterstein, 2008). To ensure construct validity, the researcher

developed questionnaire items by gaining insights from UTAUT and ISS theoretical frameworks as their validity is being tested by (Venkatesh *et al.*, 2003; DeLone and McLean, 2016) in their studies. Dimensions from the literature were also used as theoretical underpinnings for characterizing factors affecting the adoption of cloud cyber-security.

d) External validity refers to the extent of generalizing the results to the entire population. In the current study, external validity was achieved as the sampling technique was simple random whereby the population had an equal opportunity to participate.

e) Internal validity is referred to as the soundness of the research and is determined by the extent to which systematic error or bias is reduced (Stephanie, 2017). Internal validity may have been challenged as only one instrument for data collection was used and the researcher might not be able to assure if the responses were entirely honest. However, since the sample selection was random, the respondents were given an equal experience regarding the maturation and history effects and therefore, the internal validity might result in a strong causality.

3.9.2. Reliability

Reliability refers to extent of which findings of the study may be reproduced under the same condition yielding consistent results over a period of time (McMillan and Schumacher, 2010). According to (Polit and Beck, 2016), reliability in quantitative research is primarily focused on stability and consistency of the data collected. Stability refers to the extent to which repeatable results are emerged on administering the questionnaire twice (Creswell, 2014). In the current study, an inter-rater reliability approach was used for testing the stability of the questions asked and correlating its responses (Kimberlin and Winterstein, 2008). The researcher examined the consistency of the results by the Cronbach's alpha test (Nyembezi, 2014; Fink, 2016). The reliability analysis should have resulted in a coefficient value greater than 0.7 for indicating an adequate internal consistency of the questionnaires (Muijs, 2011).

3.10. Ethical Considerations

Ethical measures were significant aspects for any research design and were considered in the research planning (Neuman, 2009). The researcher obtained written permission for conducting the research from the university community and complied with the ethical policies and guidelines of the University of Venda in gaining approval from the research and ethics committee for collecting data. The data collected was strictly used for academic purposes of this investigation and adhered

to a non-disclosure procedure for information collected. The researcher briefed the participant on the nature and purpose of the study as well as explained matters regarding risks or benefits involved prior to their participation. A voluntary participation procedure was followed by gaining the participant's informed consent signed for proving their willingness towards participation. The researcher respected the participant's right to refuse to participate by not forcing them in any manner. The participants were informed about their rights to withdraw or discontinue at any stage from the survey towards an uncomfortable situation. The participants were informed about their right to not complete a particular question for the reasons of not revealing its details against their will and also to ask for clarity towards any uncertainty regarding the cloud cyber-security concepts covered in the questionnaire. The confidentiality of the respondents was maintained as the information collected was accessible by the researcher, the research assistant and was submitted to the respective supervisors only. Privacy and anonymity were guaranteed as no personal information such as names, addresses or contact details of respondents were collected. The respondents were not subjected to any form of harm, embarrassment, or violation during their participation in the survey. The researcher presented the research report in an honest manner and in no circumstance fabricated data, intentionally misinterpreted the results, or misled the nature of the study in supporting a specific conclusion. The researcher acknowledged information used from other sources to avoid plagiarism penalties.

3.11. Summary

This chapter justified the use of the selected research paradigm and design in answering the research questions. The underlying assumption for the study was a positivist paradigm based on the quantitative approach and survey research design for obtaining data. It addressed the population and sampling procedures followed for data collection. The researcher used simple random and purposive sampling techniques for selecting the appropriate sample size. A questionnaire was used as a data collection instrument as data can be collected easily and cost-effectively following a quantitative research approach. SPSS and Excel were used as tools for analyzing data. Reliability and validity measures were discussed for presenting accurate research results. Ethical measures were implemented for ensuring that the research is conducted rightfully without harming any respondent.

CHAPTER FOUR: DATA PRESENTATION, ANALYSIS, AND INTERPRETATION

4.1. Introduction

Chapter 3 described the research design and methodology used for data collection in this study. This chapter concentrates on the quantitative analysis of the main findings from the data collected. The questionnaires were administered to students, lecturers, admin staff and IT staff. However, permission for data collection at Rosebank college was only granted for student respondents. The results are illustrated through tables, pie charts, bar graphs figures (i.e. percentages and frequencies) in order to identify patterns, differences, and cross-tab analysis. The nature of the study is focused on determining the respondent's views on cloud-cybersecurity irrespective of their experience in using it, thus all the participants qualified in answering all sections of the questionnaire. However, the questions posed in each set of questionnaires varied to a certain degree (i.e. for students, lecturers, IT staff and admin staff). The data was collected within a period of 45 days from 15th August – 25th of September 2018.

The current chapter highlights the challenges encountered prior to and during the data collection process. It also outlines the data screening process for depicting missing data and determined the response rate. The overall data presented is divided into 5 sections. Section A discusses the demographic information of the respondents. Section B is followed consisting of information concerning the usage of cloud cyber-security as well as the drivers for its adoption. Section C depicts the current cyber-security challenges, benefits, and quality perceptions. Section D examines the respondent's perceptions of cloud-cybersecurity adoption decisions within tertiary institutions and presents information on their level of awareness of cloud-cybersecurity. Section E contains the reliability test, correlations and factor analysis of the results obtained.

4.2. Challenges Encountered in the Data Collection Process

Potential student respondents became reluctant in participating as no rewards were distributed to encourage participation which was a challenge. A number of targeted respondents showed no interest and refused to participate indicating that they were busy, and the survey may be time-consuming. Some respondents who were willing to participate withdrew from the survey due to a lack of understanding. A few questionnaires were incomplete, and a few were not returned which reduced the response rate of the study. Some academics were not readily available for participation

despite taking appointments, which delayed the data collection process. A few IT staff members refused to participate and those who agreed to participate despite their busy schedules required constant reminders in completing the survey. Regardless of all these challenges, the study produced a response rate higher than 50 %, thereby acquiring sufficient data credibility in achieving the research objectives.

4.3. Data Screening

A total of 495 possible respondents were recognized and communicated with from the targeted population for the distribution of questionnaires. A total of 441 questionnaires were returned and considered to be usable for data analysis. From a sample of 495, 22 students, 3 IT staff members, and 2 admin staff members refused to participate. The researcher substituted these respondents with other members who were willing to participate.

4.4. Response Rate

A total of 495 questionnaires were distributed to the three institutions. The average response rate constitutes 89% for the whole survey and was considered sufficient in being representative of the entire population. The high response rate was achieved with the support and effort of the three targeted institutions. However, a total of 46 questionnaires were not returned and 6 were received incomplete with no sufficient usable data. Therefore, a number of 54 questionnaires could not form part of the data analysis process. Table 4.1 illustrates the actual number of questionnaires distributed to each of the institutions and the number returned. It is reminded that 80.2% of the respondents were students, 10.9% were lecturers, 4.3% were IT staff and 4.5% were admin staff.

Table 4.1: Response Rate From The Survey (N=495)

Institution	**No of questionnaires Administered**					**No of questionnaires Returned**					**Response Rate (%)**			
	S	**L**	**ITS**	**AS**	**T**	**S**	**L**	**ITS**	**AS**	**T**	**S**	**L**	**ITS**	**AS**
Univen	200	30	15	10	255	179	28	11	10	228	89.5	93.3	73.3	100
TVET	100	20	10	10	140	81	20	8	10	119	81	100	80	100
Rosebank	100	-	-	-	100	94	-	-	-	94	94	-	-	-
Total	400	50	25	20	495	354	48	19	20	441	88.1 (avg.)	96.7 (avg.)	76.7 (avg.)	100 (avg.)

(S=students, L=Lecturers, ITS=IT Staff, AS=Admin staff, T=Total)*

4.5. Section A: Demographic Information

This section containes a description of the participants based on three questions inclusive of gender, age, and race for all the respondents. Information was also collected regarding the level of education for students. Additional information was acquired from lecturers regarding their teaching position, and level of teaching experience. Concerning IT and admin staff, information was acquired regarding their level of experience working with IT. This information is important as these demographic elements have an influence on the findings of the study and plays a significant part in determining the perceptions of respondents towards the use and adoption of cloud cybersecurity. The demographic results are presented in Table 4.2.

Table 4.2: Respondents' Demographics

Demographic Profile	Category	Univen		TVET		Rosebank		Total	
		F	%	F	%	F	%	F	%
1. Gender	Male	110	48%	60	50.4%	41	43.6	211	47.8%
	Female	118	52%	59	49.6%	53	56.4	230	52.2%
2. Age	15-25	127	55.7%	56	47%	63	67.0	246	55.9%
	26-35	57	25%	39	32.8%	29	30.9	125	28.3%
	36-45	28	12.2%	14	11.8%	2	2.1	44	9.9%
	46 and above	16	7.1%	10	8.4%	0	0	26	5.9%
3. Race	African/Black	209	91.6%	117	98.3%	57	60.6	383	86.9%
	Coloured	5	2.2%	2	1.7%	11	11.7	18	4.1%
	Asian/Indian	7	3.1%	0	0	11	11.7	18	4.1%
	White	7	3.1%	0	0	15	16.0	22	4.9%
4. Study Level	1st Year	47	26.3%	12	14.8%	23	24.5	82	23.2%
	2nd Year	37	20.7%	24	29.6%	29	30.9	90	25.4%
	3rd Year	50	27.9%	45	55.6%	42	44.7	137	38.7%
	4th Year	13	7.3%	0	0	0	0	13	3.7%
	Honors	16	8.9%	0	0	0	0	16	4.5%
	Masters	10	5.6%	0	0	0	0	10	2.8%
	PhD	6	3.4%	0	0	0	0	6	1.7%
5. Teaching Position	Junior Lecturer	3	10.7%	1	5%	0	0	4	8.3%
	Lecturer	19	67.9%	12	60%	0	0	31	64.6%
	Senior Lecturer	5	17.9%	5	25%	0	0	10	20.8%
	Professor	1	3.6%	2	10%	0	0	3	6.3%
6. Years of Experience In Teaching	Less than 1 Year	1	3.6%	1	5%	0	0	2%	4.2%
	Between 1 to 5 Years	11	39.3%	6	30%	0	0	17%	35.4%
	More than 5 Years	16	57.1%	13	65%	0	0	29%	60.4%
7. Experience Working With IT	Less Than One Year	3	14.3%	2	11%	0	0	5	12.8%
	2-5 Years	6	28.5%	4	22%	0	0	10	25.6%
	6-10 Years	6	28.5%	6	33.3%	0	0	12	30.8%
	More than 10 Years	6	28.5%	6	33.3%	0	0	12	30.8%

The gender status showed that from the 441 overall respondents, (211) thus 47.8% were males and (230) 52.2% were females. The findings indicates that the dominant gender for this study was females. The participants were also requested to indicate their age in years. The findings depicted that the largest age group of respondents (246) fell within the 15-20 year age classification contributing to 55.9%. The largest percentage was because most student participants were undergraduates. The second largest group was between the 26-35 age classification which contributed 28.3% towards the overall response rate. In terms of the racial demographics, the majority of the participants (383) were African/Black and contributed 86.9% of the total response rate. This was because the majority of the population enrolled within the three institutions in the year 2018 were African/Black. The remaining race categories contributed Coloured (4.1%), Indian/Asian (4.1%) and White (4.9%) to the total response rate.

The student participants were requested to indicate their level of study from the first-year level up to Ph.D. level. The study levels may cause a likely difference in the survey responses. The results indicated that out of 354 students, 38.7% thus 137 were enrolled in the third year level followed by second-year level with a number of 90 (25.4%). The postgraduates contributed 9% from Univen only as TVET and Rosebank does not offer any postgraduate degrees.

The lecturer participants were requested to indicate their teaching positions. The results in Table 4.2 depictes that 64.4% of academics held a lecturer position while 8.3% and 20.8% contributed towards junior lecturers and senior lecturers. Table 4.2 also showed that 60.4% of academics had more than five years of teaching experience, while 30.8% of staff had more than 10 years of experience in working with IT.

4.5.1. Section A Summary

This section revealed the respondents' personal characteristics. In terms of the gender demographics within students and staff, the majority of participants were female while lecturer participants were male-dominated. More student respondents fell within the age range of 15-25, while academics fell between 36-45 and staff between 26-35 years of age. The majority of participants were African/Black across all the three institutions. Specific to students' educational level, respondents were shown to be mainly within their 3-year level. The teaching positions of lecturers were shown to be the highest among other positions. The experience of years in teaching for most of the academics were more than 5 years, whilst in the IT department, most members had more than 10 years of experience working with information technology.

4.6. Section B: Cloud Computing Cyber-Security Usage and its Drivers

This section seeks to obtain information on achieving research *objective one* regarding the drivers for usage and adoption of cloud cybersecurity. Therefore, the section provides a report based on six relevant questions. The questions were inclusive of the respondent's knowledge of cloud computing cybersecurity and experience of using cloud computing cybersecurity. It also includes cloud computing cyber-security services and application used as well as the educational and administrative role cloud cyber-security plays within tertiary institutions. Furthermore, it included the drivers (i.e. factors) for cloud computing cybersecurity adoption, and the last question posed to IT staff members concerned the cybersecurity policies, frameworks, and audit implementation.

4.6.1. Knowledge and Experience Using of Cloud Cybersecurity

In order to determine the drivers of cloud computing cybersecurity adoption and usage, it was significant to establish if respondents were knowledgeable about cloud-cybersecurity. Thereafter, respondents were also requested to indicate if they had experience in using any of the cloud-cybersecurity services and applications. The findings revealed that an aggregate of 61.90% of respondents were knowledgeable compared to the 38.10% of respondents who indicated to have no knowledge. The results indicated that although some of the respondents are knowledgeable about, they are actually not using cloud cybersecurity. This may be because they may not have the necessary resources required to use cloud cybersecurity or they may have not yet established any need to use it.

4.6.2. Cloud Cybersecurity Applications and Services Usage

The respondents were expected to indicate the cloud-cybersecurity applications and services they have used. This question contributed to determining the usage of cloud-cybersecurity in tertiary institutions. It also assisted in determining the most preferred cloud-cybersecurity service and application used.. A large number of 267 respondents with 39% of overall responses indicated using Microsoft security applications and services in all the three tertiary institutions. This could be due to respondents being more known to or familiar with Microsoft services than Google or Amazon. Of the 441 respondents, 237 (132 from Univen, 53 from TVET and 52 from Rosebank) indicated using Google security applications and services. This could be a matter of preference whereby respondents feel more comfortable using Google security than Microsoft or Amazon. Approximately 12.4% of overall respondents indicated using Amazon security services and

applications, while 14% of respondents indicated not to have used any of the security services and applications. Amazon may not have higher level usage due to reasons such as respondents not having the access to, knowledge and preference of using their services, or the services may not be as user-friendly as Microsoft or Google.

4.6.3. Role of Cloud Cybersecurity within Tertiary Institutions

It was important to determine the role cloud cybersecurity plays in the educational context for increasing its usage and adoption levels within tertiary institutions. The role was determined based on the cybersecurity functionality of e-learning, e-mail and social network platforms hosted on the cloud. The results obtained from students and lecturers revealed that 81.8% of respondents believed that cloud platforms allow to securely upload/download assignments while 18.2% disagreed. 77.6% indicated that cloud platforms allow to securely upload/download lecture notes while 63% agreed that it enables to securely conduct online exams and tests. Approximately 67.7% indicated cloud platforms to be useful in securely carrying class and group discussions while 76.4% agreed that cloud-based e-learning, e-mail, and social network platforms are safe for posting and viewing marks. It can be assumed that respondents may have found cloud cybersecurity features to be useful, trustable and safe to work with in carrying out academic activities.

Additionally, the role of cloud cybersecurity was also determined by the IT and admin staff perspectives. The role was determined based on the cybersecurity functionality of ITS, e-mail and social network platforms hosted on the cloud. The findings revealed that 76.9% of respondents indicated that cloud platforms enable to securely send and receive messages to and from colleagues and stakeholders while 23.1% disagreed. Also, 71.8% indicated that cloud platforms enable to securely upload documents and files while 74.4% believed that cloud-based cybersecurity allows to securely conduct uninterrupted meetings online. Therefore, overall results depicted that majority of the respondents are keen towards trusting the cybersecurity features of cloud-based ITS, e-mail and social media platforms.

4.6.4. Drivers for Cloud Cybersecurity Adoption

The respondents were requested to rate their level of agreement or disagreement regarding their opinions about cloud cybersecurity drivers on a scale of 1-5 ranging from strongly agree to strongly disagree. This question assisted in determining the drivers that could influence respondents in adopting and using cloud cybersecurity. The researcher identified and used five cyber-security

adoption drivers from a study conducted by (Loanzon, 2014a) and presented a report in the subsequent Tables.

a) Improving data security and privacy information of students, lecturers, and staff.

This question presented the respondents' views on whether they perceive increased data security and privacy of students, staff, and lecturers as a driver of cloud cybersecurity adoption. The results in Table 4.3 indicate that an aggregate of 43.8% and 40.6% of respondents from the three institutions showed that they strongly agree and agree, making a total of 84.4% of respondents who agree. The higher level of agreement may be due to respondents' viewing cloud cybersecurity as an advanced technological opportunity for improving the security and privacy of their data. Of the 84.4% of respondents who are in agreement, 42.6% of respondents were from Univen, 23.8% were from TVET and 17.9% were from Rosebank. In contrast, an aggregate of 3.4% and 2.0% of respondents disagree and strongly disagree, making a respective total of 5.4% of respondents who disagreed. The respondents might have disagreed because they may be comfortable with the current security of their data or might not want to adapt to change and believe cloud cybersecurity services would not make any significant difference in securing their data.

Table 4.3: Increased Data Security and Privacy of Students, Staff, and Lecturers

Item	Univen		TVET		Rosebank		Total	
	F	%	F	%	F	%	F	%
Strongly Agree	113	49.6	49	41.2	31	33.0	**193**	**43.8**
Agree	75	32.9	56	47.1	48	51.1	**179**	**40.6**
Neutral	29	12.7	5	4.2	11	11.7	**45**	**10.2**
Disagree	7	3.1	5	4.2	3	3.2	**15**	**3.4**
Strongly Disagree	4	1.8	4	3.4	1	1.1	**9**	**2.0**
Total	228	100	119	100	94	100	**441**	**100**

b) Legal law and regulatory compliance

The respondents were required to rate their level of agreement or disagreement regarding compliance with legal law and regulatory bodies as a driver for adopting cloud cybersecurity. The findings in Table 4.4 depicts that, a large number of respondents agree (50.1%) and strongly agree (19.5%) that compliance with legal law and regulatory bodies could be a driver for adopting cloud cybersecurity. The respondents might have agreed because they may be knowledgeable about the role and significance of as well as the consequences of not complying with the laws and regulatory bodies within the tertiary institution environment. While an aggregate of 5.4% and 3.4% disagreed and strongly disagreed. The small number of respondents might have disagreed because they may

believe the engagement of laws and regulatory bodies are not strong enough to cause an influence towards the adoption of technology in tertiary institutions.

Table 4.4: Compliance with Legal Law and Regulatory Bodies

Item	Univen		TVET		Rosebank		Total	
	F	%	F	%	F	%	F	%
Strongly Agree	36	15.8	33	27.7	17	18.1	**86**	**19.5**
Agree	107	46.9	56	47.1	58	61.7	**221**	**50.1**
Neutral	66	28.9	17	14.3	12	12.8	**95**	**21.5**
Disagree	13	5.7	7	5.9	4	4.3	**24**	**5.4**
Strongly Disagree	6	2.6	6	5.0	3	3.2	**15**	**3.4**
Total	228	100.0	119	100.0	94	100.0	**441**	**100.0**

c) The pace of keeping up with the latest technology

This question sought to determine the respondents' opinion in terms of the pace of keeping up with the latest technology within tertiary institutions as a driver of cloud cybersecurity. Table 4.5 indicates that 44.3% and 32.7% of overall respondents agreed and strongly agreed, making a combined total of 77% of responses who are in agreement with the statement. The respondents might have agreed because they may believe keeping up with latest technologies would help them to progress faster. The findings also depicted that an aggregate of 16.4% of respondents were uncertain, while 3.9% and 2.7% of the respondents disagree and strongly disagree. Out of 77% of respondents who strongly agree and agree, 38.5% were from Univen, 22.5% were from TVET and 17% were from Rosebank. The results, therefore, indicate that the level of agreement at Univen is 16% higher than TVET and 21.4% higher than Rosebank. This might be because respondents at Univen may be having more exposure to the latest developments than TVET and Rosebank.

Table 4.5: Pace of Keeping up with Latest Technology

Item	Univen			TVET			Rosebank			Total		
	F	P	VP	F	P	VP	F	P	VP	F	P	VP
Strongly Agree	76	33.3	33.5	43	36.1	36.1	25	26.6	26.6	**144**	**32.7**	**32.7**
Agree	89	39.0	39.2	56	47.1	47.1	50	53.2	53.2	**195**	**44.2**	**44.3**
Neutral	47	20.6	20.7	14	11.8	11.8	11	11.7	11.7	**72**	**16.3**	**16.4**
Disagree	8	3.5	3.5	3	2.5	2.5	6	6.4	6.4	**17**	**3.9**	**3.9**
Strongly Disagree	7	3.1	3.1	3	2.5	2.5	2	2.1	2.1	**12**	**2.7**	**2.7**
Total	227	99.6	100	119	100	100	94	100	100	**440**	**99.8**	**100**
Missing	1	0.4		0	0		0	0		**1**	**0.2**	
Total	**228**	**100.0**		**119**	**100**		**94**	**100**		**441**	**100.0**	

d) Financial reasons such as reduced budgeting for the cost of cyber-breaches.

This part of the question assisted in determining the perceptions of respondents concerning financial reasons such as security cost reductions within tertiary institutions as a driver for cloud cybersecurity adoption. The responses based on Table 4.6 revealed that an aggregate of 42.4% and 27.8% of respondents agreed and strongly agreed making a total of 70.2% of respondents who agreed. It is assumed that respondents believe tertiary institutions could be more financially feasible and sound by using technologies with fewer costs, and hence cyber breaches could also be protected at a lesser cost. The results also depict that 9.1% and 4.8% of respondents disagreed and strongly disagreed, making a total of 13.9% of respondents who disagreed. It is assumed that respondents might have disagreed with a believe that technologies at a lesser cost would not be very productive and hence could be a risk if adopted. Out of the 70.2% who agreed, 34.4% were from Univen, 20.3% were from TVET and 15.9% were from Rosebank. The results indicate that the level of agreement at Univen is 14.1% higher than TVET and 18.5% higher than Rosebank.

Table 4.6: Financial Reasons as a Driver For Cloud-Cybersecurity Adoption.

Item	Univen			TVET			Rosebank			Total		
	F	P	VP	F	P	VP	F	P	VP	F	P	VP
Strongly Agree	62	27.2	27.4	32	26.9	26.9	28	29.8	29.8	**122**	**27.7**	**27.8**
Agree	89	39.0	39.4	57	47.9	47.9	40	42.6	42.6	**186**	**42.2**	**42.4**
Neutral	44	19.3	19.5	14	11.8	11.8	12	12.8	12.8	**70**	**15.9**	**15.9**
Disagree	24	10.5	10.6	7	5.9	5.9	9	9.6	9.6	**40**	**9.1**	**9.1**
Strongly Disagree	7	3.1	3.1	9	7.6	7.6	5	5.3	5.3	**21**	**4.8**	**4.8**
Total	226	99.1	100	119	100	100	94	100	100	**439**	**99.5**	**100**
Missing	2	0.9		0	0		0	0		**2**	**0.5**	
Total	**228**	**100**		**119**	**100**		**119**	**100**		**441**	**100**	

e) For maintaining public reputation.

This question sought to determine the respondents' views on maintaining a public reputation such as gaining trust and confidence of students and staff as a driver of adopting cloud cybersecurity. Table 4.7 depicts that an aggregate of 31.3% of and 41% of respondents indicated that they strongly agree and agree, making a total of 72.3% of respondents who agreed. It is assumed that the respondents believe using the most recent technologies in protecting students and staff data would create a positive image of the tertiary institutions and would gain the trust of students and staff. However, an aggregate of 15.6% of respondents remained uncertain while 4.8% and 7.3% of respondents disagreed and strongly disagreed, making a total of 12.1% of respondents who disagreed. It is assumed that respondents who disagreed might believe following technological

advances is not critical and does not change the reputation of an institution. Out of the 72.3% of respondents who were in agreement with the statement, 35.1% were from Univen, 20.6% were from TVET and 16.6% were from Rosebank.

Table 4.7: Maintaining Public Reputation

Item	Univen		TVET		Rosebank		Total	
	F	%	F	%	F	%	F	%
Strongly Agree	73	32.0	35	29.4	30	31.9	**138**	**31.3**
Agree	82	36.0	56	47.1	43	45.7	**181**	**41.0**
Neutral	43	18.9	16	13.4	10	10.6	**69**	**15.6**
Disagree	13	5.7	4	3.4	4	4.3	**21**	**4.8**
Strongly Disagree	17	7.5	8	6.7	7	7.4	**32**	**7.3**
Total	228	100	119	100	94	100	**441**	**100**

Overall, the results implies that most of the respondents are in agreement with the statements and perceives them as drivers of cloud cybersecurity. However, compliance with legal law and regulatory bodies turned out to be a dominating factor which received the highest level of agreement (50.1%) as compared to the other factors. Among this 50.1 % of respondents, 40% were students, 4.3% were lecturers, 1.8% were Admin staff and 2.9% were IT staff. Furthermore, the descriptive statistics with the mean and standard deviation values are presented in Table 4.8. The results indicated that data security and privacy was ranked as the most critical driver of cloud cybersecurity adoption according to the participants believes as the standard deviation is 0.905.

Table 4.8: The Mean and Standard Deviation Distributions of Cloud-Cybersecurity

Drivers	Mean	Std. Deviation	Rank of Agreement
Data security and privacy	1.79	.905	Strongly Agree
Legal Law and Regulatory Compliance	2.23	.940	Agree
The pace of Keeping up with technology	2.00	.945	Agree
Financial Reasons	2.21	1.092	Agree
Maintaining Public Reputation	2.16	1.136	Agree

4.6.5. Cybersecurity Policies, Frameworks and Audit Implementation

In order to achieve the objective of identifying and suggesting a suitable cloud cybersecurity framework for tertiary institutions, it was necessary to have knowledge on the current cybersecurity frameworks used by the tertiary institutions (if any). This information was obtained from the IT staff respondents within two institutions (i.e. Univen and TVET). 100% (19) of the respondents indicated that there was no cloud-cybersecurity framework currently used within their

tertiary institutions. It was also significant to determine if there were any established cyber-security policies for maintaining cyber-attacks within the institutions. The results displayed in Table 4.9 shows that 63.6% from Univen and 50% from TVET indicated not having any cybersecurity policies while 37.7% from TVET indicated having policies in place and none from Univen.

The findings also revealed, 45.4% from Univen and 12.5% from TVET indicated that their cloud service providers do not adhere to any established security framework involving cybersecurity controls. However, the majority of respondents (87.5%) from TVET indicated that their service providers adhere to established security frameworks. The results depicted that the majority of the respondents does not have knowledge of their service providers cybersecurity controls. Furthermore, 31.6% stated that their service providers experience regular third-party audits with established cybersecurity frameworks while 31.6% indicated not to be sure. However, 36.8% indicated that their service providers do not undergo any third-party audits. Lastly, 42.1% of respondents indicated that no cloud cybersecurity strategies were circulated to the employees for protecting against cyber-attacks. Therefore, the findings suggested that employees may easily encounter cyber-attacks within their systems if they are not aware of any institutional based strategies which could protect their systems from being attacked.

Table 4.9: Cloud-Cybersecurity Framework, Policies, Strategies and Audit Implementation

Institution	Category	Does your institution have cloud computing cyber-security policies in place for maintaining cyber-attacks?		Does your cloud service provider adhere to any established cloud security framework involving cyber-security controls?		Does your institution and cloud service provider undergo any regular 3rd party audits with established cloud cyber-security frameworks?		Are cybersecurity strategies circulated to the employees of your institutions to protect systems from cyber-attacks?	
		F	%	F	%	F	%	F	%
Univen	Yes	0	0	0	0	1	9.1	0	0
	No	7	63.6%	5	45.5%	4	36.4	5	45.5
	Not Sure	4	36.4%	6	54.5%	6	54.5	6	54.5
TVET	Yes	3	37.5%	7	87.5%	5	62.5	4	50.0
	No	4	50%	1	12.5%	3	37.5	3	37.5
	Not Sure	1	12.5%	0	0	0	0	1	12.5
Total	**Yes**	**3**	**15.8%**	**7**	**36.8%**	**6**	**31.6%**	**4**	**21.1%**
	No	**11**	**57.9%**	**6**	**31.6%**	**7**	**36.8%**	**8**	**42.1%**
	Not Sure	**5**	**26.3%**	**6**	**31.6%**	**6**	**31.6%**	**7**	**36.8%**
	Total	**19**	**100**	**19**	**100**	**19**	**100**	**19**	**100**

4.6.6. Section B Summary

According to the results presented in this section, the objective of determining cloud cybersecurity usage and its adoption drivers was achieved and subsequent research questions were answered. It is clear from the findings that, the majority of the students were knowledgeable about and experienced in using cloud cybersecurity as compared to academics and Admin staff across the three institutions. Majority of the respondents have indicated to have used Microsoft applications and services in all the three institutions. The lecturers and students believe that cloud cybersecurity would mainly enable them to securely upload, download assignments, while the staff believed it is relevant for securely sending and receiving messages. The respondents indicated compliance with legal law and regulatory bodies as a driver influencing the adoption of cloud-cybersecurity. The IT staff indicated having no cloud cybersecurity frameworks, policies and strategies in place for maintaining cyber-attacks.

4.7. Section C: Cloud Cybersecurity Challenges, Benefits, And Quality

This section sought to obtain information on achieving the objective of determining the cybersecurity issues encountered within the cloud as well as achieving the objective of determining the challenges, benefits and quality perceptions of cloud cybersecurity adoption. It includes eight relevant questions and the results are presented in the subsequent tables and graphs as follows.

4.7.1. Cybersecurity Incident (Attack) Encountered

The respondents were requested to indicate if they have ever encountered a cybersecurity incident or attack. The results depicted that 74.3% (263) of respondents have not experienced cyber-attacks, while 91 (25.7%) indicated to have encountered cyber-attacks. The respondents who have not encountered cyber-attacks may have their devices secured or may not be engaged with a high amount of online activities. Out of the 74.3%, 51.3% were from Univen, 22.4% were from TVET and 26.2% were from Rosebank. Out of the 25.7% who acknowledged to have experienced cyber-attacks, 48.4% were from Univen, 24.2% were from TVET and 27.5% were from Rosebank. The respondents might have encountered cybersecurity incidents if their devices and online activities are prone to attacks due to weak or no security mechanisms implemented.

4.7.2. Difficulties Faced in Securing Materials Online

The respondents were further requested to indicate if they have ever faced difficulties in securing their materials such as files, documents, videos, images or any other form of data online. The

findings depicted that 230 (57.2%) respondents have not faced any difficulties in securing their materials online, while an of 172 (42.6%) respondents have faced difficulties in securing their materials online. Of the 57.2% of respondents, 54.3% were from Univen, 22.2% were from TVET and 23.6% were from Rosebank. This may be because respondents were familiar with the security of the systems used within their tertiary institutions. Of the 42.6% of respondents, 47.7% were from Univen, 29.1% were from TVET and 23.3% were from Rosebank. This may be a result of respondents not being able to appropriately operate their devices and security features within or might not have the necessary skills required in using the technology.

4.7.3. Challenges of Using Cloud-Based Cybersecurity Services

The respondents were asked to highlight the challenges of using cloud-cybersecurity from the given twelve multiple response options. A total of 2376 responses were received from 441 respondents. Encountering challenges while using cloud cyber-security may influence the adoption and usage of cloud cybersecurity services. This subsection supported in answering the research question regarding how cybersecurity challenges affect the adoption decisions of cloud cybersecurity services. By identifying these challenges, the researcher can thereafter suggest solutions to overcome such challenges. The aggregate results collected from all the participants within 3 institutions are shown in Table 4.10.

Table 4.10: Aggregate Results of Cloud-Cybersecurity Challenges

Challenges	Responses		Percent of Cases	Mean	Std. Deviation
	Number	Percent			
Lack of physical control of data	226	9.5%	51.2%	1.49	.500
Harmful activities executed on the internet/network	225	9.5%	51.0%	1.49	.500
Data leakage to other cyber-security service users	185	7.8%	42.0%	1.58	.494
Denial of service Availability	219	9.2%	49.7%	1.50	.501
Monitoring and tracking activities compromising data privacy	181	7.6%	41.0%	1.59	.492
Files can be infected with Viruses	215	9.0%	48.8%	1.51	.500
Undesirable disclosure of data to law and regulatory bodies	153	6.4%	34.7%	1.65	.477
Lack of security awareness causing cyber-attacks	196	8.2%	44.4%	1.56	.497
Identity theft and Unauthorized access to my cloud applications	190	8.0%	43.1%	1.57	.496
Information can be lost, deleted, moved or changed.	197	8.3%	44.7%	1.55	.498
Sniffing/spoofing my cloud activities	178	7.5%	40.4%	1.60	.491
Hacking of my Files and Data	211	8.9%	47.8%	1.52	.500
Total	**2376**	**100.0%**	**538.8%**	1.49	.500

According to the findings, 226 (9.5%) indicated lack of physical control of data as a challenge of using cloud cybersecurity; followed by 225 responses which showed harmful activities executed on the network as a challenge which equally contributed 9.5% towards overall responses. Subsequently, 219 responses (9.2%) highlighted denial of service availability, then 215 (9%) responses highlighted virus infection as challenges. The least amount of responses (153) with 6.4% indicated undesirable disclosure of data to law and regulatory bodies as a challenge of cloud-cybersecurity usage. It can be seen from the findings that respondents are concerned about their data and information protection through cloud-cybersecurity platforms. However, the findings revealed that undesirable disclosure of data to law and regulatory bodies was indicated to be a critical factor in the adoption of cloud cybersecurity with a standard deviation of 0.477. It can be assumed that respondents believe laws and regulatory bodies might access and disclose information for legal purposes and therefore it could be a challenge towards adoption.

Furthermore, the findings obtained revealed that in Univen, the highest percentage (10%) of responses indicated harmful activities executed on the network or internet as a challenge of cloud cybersecurity usage. It is assumed that the respondents might believe using cloud cybersecurity may attract harmful activities being conducted on the internet through their profiles. In comparison, the highest percentage of respondents at TVET (9.8%) and Rosebank (9.7%) indicated a lack of physical control of data as a challenge. The respondents might have a belief that service providers could manipulate their data and mishandle it making it a challenge for adoption.

4.7.4. Benefits Of Cloud-Based Cyber-Security Services

The participants were requested to highlight all the benefits of cloud-cybersecurity based on their knowledge, experience, and opinions. This sub-section supports in answering the research question regarding how cybersecurity benefits affect the adoption decisions of cloud cybersecurity services. It also assisted in determining the level of satisfaction the respondents seem to have towards cloud cybersecurity. This was achieved by determining the benefits each respondent could attain by using cloud cybersecurity. The results are presented in Table 4.11.

Table 4.11: Benefits of Cloud Cybersecurity Adoption

Benefits	Total Responses	
	N	%
Educational and Administrative Benefits of Cloud Cybersecurity Adoption		
Prevents Forgery	269	21.7%
Prevents the Presenting of A False Identity	277	22.3%
Prevents Interference Upon Controlled or Private Conversations	225	18.1%
Prevents Altering Date Stamps on Submitted Work, files and documents	227	18.3%
Prevents Lecturers/ students/staff from Gaining Access to Personal Data of Students/lecturers/staff	214	17.2%
None	29	2.3%
Total	**1241**	**100%**
Technical Benefits of Cloud Cybersecurity Adoption		
Cheaper security costs as data are saved in multiple locations	16	26.2%
Standardized interfaces for managed cyber-security services	11	18%
Provisioning of cyber-security auditing	6	9.8%
Increased support for defensive measures when cyber-attack is taking place	16	26.2%
Efficient and effective capabilities of incident/attack response.	12	19.8%
Total	**61**	**100**

The findings revealed that 277 (22.3%) responses highlighted prevention of presenting false identities to university authorities as a benefit of cloud cybersecurity. Of the 277 responses, 136 were from Univen, 75 from TVET and 66 from Rosebank. It can be assumed that the majority of the respondents believe that cloud cybersecurity could be a solution for eliminating or reducing fraudulent individuals accessing the systems to study or work at their respective tertiary institutions. 21.7% responses highlighted prevention of forgery of course assessments and information on ITS, e-mail and social media as a benefit, while 18.3% indicated prevention of altering date stamps on files and documents. This result might be an indication of respondents' awareness and concerns regarding counterfeited documents circulated online for various illegal reasons within some institutions. 225 (18.1%) responses indicated prevention of interference upon controlled or private conversations among individuals, departments and schools as a benefit. The respondents might have a value for keeping the privacy of online communication and might know the importance of not disclosing confidential information, therefore this benefit could promote the adoption of cloud cybersecurity.

Furthermore, the IT staff were also requested to highlight the benefits of cloud cybersecurity. The findings revealed that at Univen, a greater percentage of 28.6% showed that cloud-based cybersecurity provides increased support for defensive measures when cyber-attack is taking place as a benefit, which was 5.5% higher than TVET. This can be because cloud-based activities are

under continuous surveillance which could detect the attack at earlier stages or while it is taking place. However, at TVET, a greater percentage of 30.8% showed cheaper costs of cloud-cybersecurity as a benefit since data can be saved in multiple locations, which is 7.9% higher than Univen. A percentage of 20% from Univen and 19.2% from TVET showed that cloud-based cybersecurity has efficient and effective capabilities of incident/attack response which is a benefit.

4.7.5. Quality Perceptions of Cloud Cyber-Security Services

This part serves to determine how quality affects the respondents' decision of adopting cloud cybersecurity. The quality measures such as reliability, flexibility, accuracy, effectiveness, consistency, relevancy, and responsiveness were adopted from the information systems success model (DeLone and McLean, 2016). The researcher also wanted to determine if cybersecurity quality increases the value of cloud and whether tertiary institutions have the necessary infrastructure for supporting system, information and service quality of cloud cybersecurity. The results were presented in the subsequent Tables and Figures.

4.7.5.1. Reliability and Flexibility of Cloud-Cybersecurity

The respondents were requested to determine their beliefs of whether cloud-based cybersecurity is reliable and flexible for securing contents on various platforms such as google drive, emails, Dropbox, blackboard etc. The results are presented in Figure 4.1.

Category	Univen		TVET		Rosebank	
	F	P	F	P	F	P
Strongly agree	91	39.9%	47	39.5%	30	31.9%
Agree	102	44.7%	56	47.1%	51	54.3%
Neutral	29	12.7%	11	9.2%	10	10.6%
Disagree	3	1.3%	1	0.8%	2	2.1%
Strongly Disagree	3	1.3%	4	3.4%	1	1.1%
Total	228	100%	119	100%	94	100%

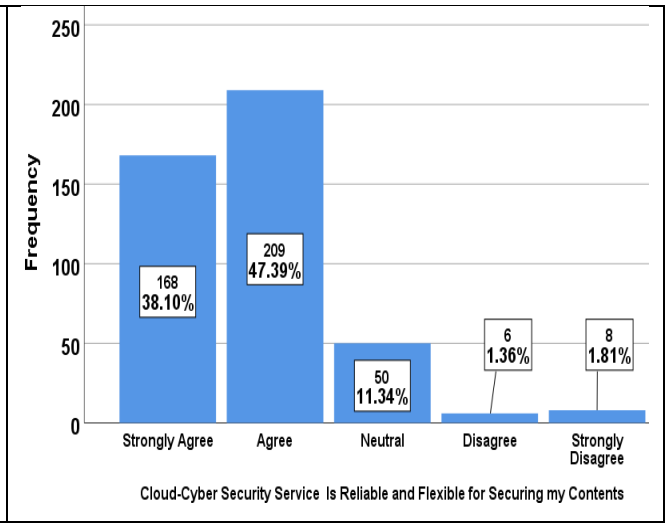

Figure 4.1: Reliability and Flexibility Perceptions for Cloud-Cybersecurity Quality

The results showed that an aggregate of 47.39% and 38.10% of respondents agreed and strongly agreed respectively, making a total of 85.49% of responses who agreed. The highest level of agreement was from respondents at TVET with a sum of 86.6%, followed by 86.2% from Rosebank, and 84.6% from Univen. It can be assumed that the respondents may have a belief that cloud cybersecurity would more reliably and flexibly support their security needs and that current security systems need to be changed or updated. An aggregate of 11.34% of respondents neither agreed nor disagreed, while an aggregate of 1.3% and 1.81% of respondents disagreed and strongly disagreed. The results indicated that most of the respondents agreed as compared to those who disagreed with a huge percentage gap of 82.85%. the respondents who disagreed are assumed to be satisfied with the current security systems or might not want to adapt to change.

4.7.5.2. Accuracy and Effectiveness of Cloud Cybersecurity

The respondents were requested to determine their beliefs of whether cloud-based cybersecurity is accurate and effective for protecting personal, educational and work-related contents. It should be noted that the question had two responses missing from TVET due to which the results were analyzed with the remaining 117 responses. The results presented in Figure 4.2 indicated that an aggregate of 51% and 25.7% agreed and strongly agreed, making a total of 76.7% of respondents who agreed. It can be assumed that the respondents may want a security service running for 24 hours continuously without any interruption which is what cloud cybersecurity offers. The participants might have encountered challenges and errors in protecting their educational and job-related contents hence would want to experience how operative cloud cybersecurity could be. Alternatively, a sum of 17.1% of respondents neither agreed nor disagreed, while an aggregate of 4.3% and 1.82% of respondents disagreed and strongly disagreed. The respondents might have disagreed as they may be satisfied with how their contents are currently secured and prefer to continue using it than any other technology. The results depicted that at Univen and TVET, the equal percent (26.3%) of respondents strongly agreed while Rosebank (23.4%) was 2.9% lower. It should be noted that none of the respondents strongly disagreed at Rosebank.

Category	Univen		TVET		Rosebank	
	F	P	F	P	F	P
Strongly agree	60	26.3%	31	26.5%	22	23.4%
Agree	111	48.7%	59	50.4%	54	57.4%
Neutral	45	19.7%	17	14.5%	13	13.8%
Disagree	10	4.4%	4	3.4%	5	5.3%
Strongly Disagree	2	0.9%	6	5.3%	-	-
Total	228	100%	117	100%	94	100%

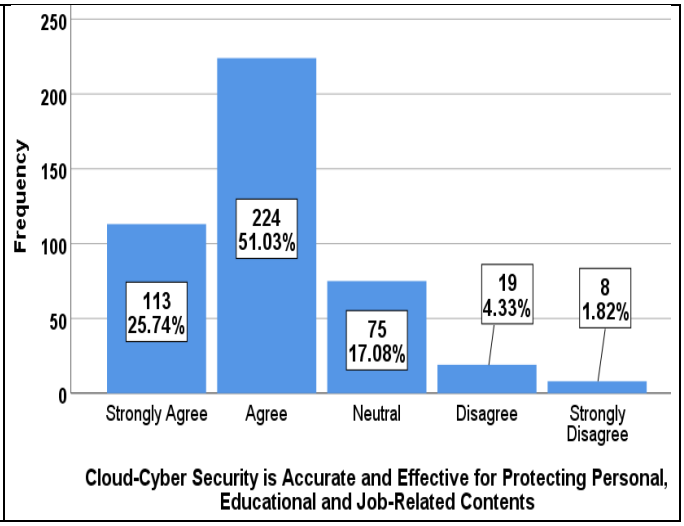

Figure 4.2: Accuracy and Effectiveness as Quality Perceptions for Cloud-Cybersecurity

4.7.5.3. Consistency and Relevancy of Cloud Cybersecurity

The respondents were requested to determine their beliefs of whether cloud-cybersecurity is consistent and relevant for securing personal, educational and work-related contents. It should be noted that a total of five responses were missing from Univen and TVET, therefore analysis was based on what was available. Figure 4.3 shows that an aggregate of 45.6% and 27% of respondents agreed and strongly agreed that cloud-cybersecurity is consistent and relevant for securing personal, educational and job-related contents, making a total of 72.7% of respondents who agreed. It can be assumed that respondents might not want to depend only on one security system for protecting their contents, hence they might have found cloud cybersecurity to be the most appropriate option. However, an aggregate of 5.9% and 2.5% of respondents disagreed and strongly disagreed, making a sum of 8.5% of respondents who were in disagreement, while an aggregate of 18.8% of respondents neither agreed nor disagreed. Out of the 72.7% of respondents who were in agreement, 36.7% of respondents were from Univen, 19.2% were from TVET and 16.7% were from Rosebank. It should be noted that none of the respondents at Rosebank strongly disagreed with the statement, while 2.2% from Univen and 5.2% from TVET strongly disagreed.

Category	Univen		TVET		Rosebank	
	F	P	F	P	F	P
Strongly agree	57	25.1%	35	30.4%	26	27.7%
Agree	103	45.4%	49	42.6%	47	50%
Neutral	48	21.1%	21	18.3%	13	13.8%
Disagree	14	6.2%	4	3.5%	8	8.5%
Strongly Disagree	5	2.2%	6	5.2%	-	-
Total	227	100%	115	100%	94	100%

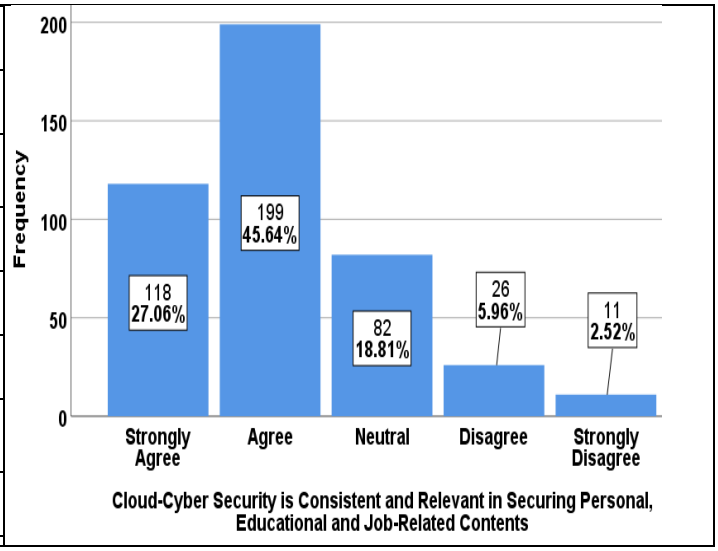

Figure 4.3: Consistency and Relevancy as Quality Perceptions for Cloud- Cybersecurity

4.7.5.4. Responsiveness of Cloud Cybersecurity

The respondents were asked about their views on whether cloud-cybersecurity is responsive in terms of the speed of notifying users during a cybersecurity attack. The results as shown in Figure 4.4 reveal that an aggregate highest percent (43.8%) of respondents agreed that cloud-cybersecurity is responsive, followed by 29.1% of respondents who strongly agreed, which makes a sum of 72.9% of respondents who agreed. The respondents might have agreed as they would want a security system which timely alerts security breaches and mishaps. Consequently, 6.4% and 3.2% of respondents disagreed and strongly disagreed, making a total of 9.6% of respondents who disagreed. The results implied that respondents who were in an agreement are 63.3% higher than the respondents who were disagreeing. However, 76 (17.4%) of respondents neither agreed nor disagreed. Out of the 72.9% of the respondents who agreed, 37.4% were from Univen, 19.7% were from TVET and 15.8% were from Rosebank.

Category	Univen		TVET		Rosebank	
	F	P	F	P	F	P
Strongly agree	60	26.7%	35	29.7%	32	34.4%
Agree	103	45.8%	51	43.2%	37	39.8%
Neutral	45	20%	18	15.3%	13	14%
Disagree	13	5.8%	6	5.1%	9	9.7%
Strongly Disagree	4	1.8%	8	6.8%	2	2.2%
Total	225	100%	118	100%	93	100%

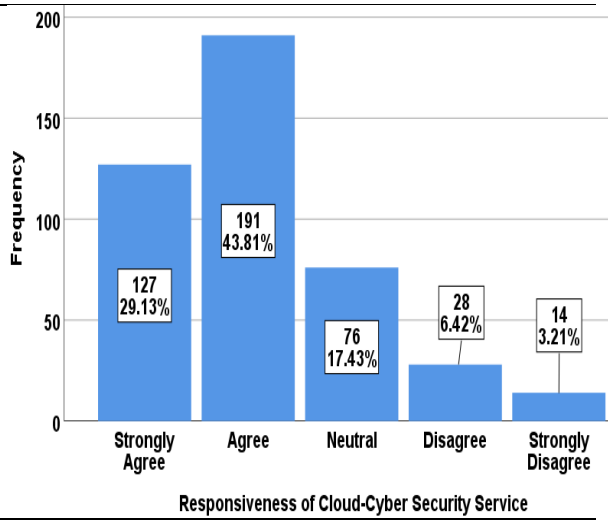

Figure 4.4: Responsiveness as a Quality Perception of Cloud Cybersecurity

4.7.5.5. Cloud Cybersecurity Increases Value and Adoption of Cloud Computing

The respondents were asked about their opinions on whether cloud-cybersecurity increases the value of cloud computing and promotes adoption.

Category	Univen		TVET		Rosebank	
	F	P	F	P	F	P
Strongly agree	53	23.2	37	31.1	20	21.3
Agree	102	44.7	50	42.0	48	51.1
Neutral	57	25.0	20	16.8	15	16.0
Disagree	12	5.3	5	4.2	9	9.6
Strongly Disagree	4	1.8	7	5.9	2	2.1
Total	228	100%	119	100%	94	100%

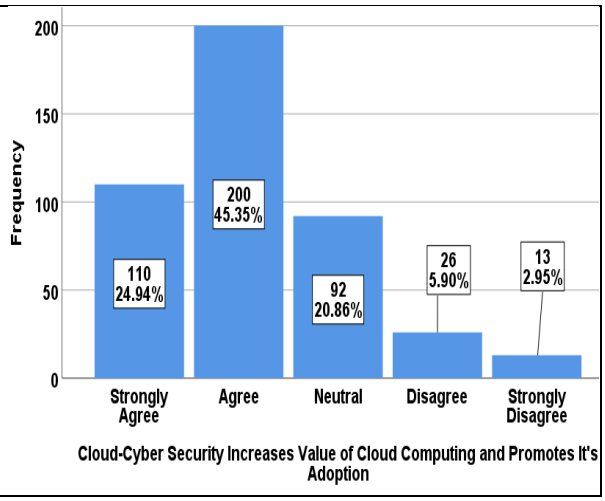

Figure 4.5: Cloud Cybersecurity Value of Cloud Computing

As shown in Figure 4.5, 23.2% respondents from Univen, 31.1% from TVET and 21.3% from Rosebank strongly agreed that cloud-cybersecurity increases the value of cloud computing, while an aggregate of 45.4% of respondents agreed with the statement. However, an aggregate of close to 21% of respondents neither agreed nor disagreed, while an aggregate of 5.9% and 2.9% of respondents disagreed and strongly disagreed, contributing a sum of 8.6% towards the respondents

who disagreed. The results implied that most of the respondents believe that cloud-cybersecurity increases the value of cloud computing which in turn could lead to an increase in its adoption.

4.7.5.6. Infrastructure Availability for Supporting Cybersecurity Quality

This question requested respondents to rate their level of agreement or disagreement in terms of the availability of infrastructure for supporting the quality of cloud cybersecurity information, services, and systems. The results in Figure 4.6 depict that majority of the respondents from Univen (36%), TVET (37.8%) and Rosebank (38.3%) agreed that infrastructure is available within their tertiary institutions and could be linked to cloud service providers for supporting the quality of cloud cybersecurity services, systems and information. The result is possibly due to the benefits that could be derived from the use of cloud cybersecurity using available infrastructure. While an aggregate of 26.1% of respondents strongly agreed, 9.8% and 7.3% disagreed and strongly disagreed. However, an aggregate of 19.6% of respondents remained neutral. The results implied that the majority of the respondents believed that adequate availability of infrastructure can improve the quality of the cloud cybersecurity and can increase its adoption and usage.

Category	Univen		TVET		Rosebank	
	F	P	F	P	F	P
Strongly agree	57	25%	32	26.9%	26	27.7%
Agree	82	36%	45	37.8%	36	38.3%
Neutral	51	22.4%	18	15.1%	19	20.2%
Disagree	22	9.6%	9	7.6%	12	12.8%
Strongly Disagree	16	7%	15	12.6%	1	1.1%
Total	228	100%	119	100%	94	100%

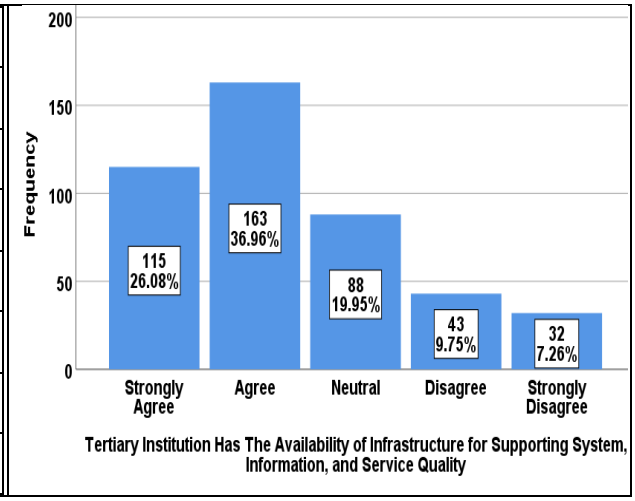

Figure 4.6: Quality of Available Cloud-Cybersecurity Infrastructure

The overall results implies that most of the respondents were in agreement with the various quality perceptions of cloud-cybersecurity. The accuracy and effectiveness of cloud cybersecurity was a dominating factor receiving the highest level of agreement (51%) compared to the other factors.

4.7.6. Section C Summary

This section achieved two objectives of the study namely, the objective of determining the security issues within the cloud and the objective of determining the challenges, benefits and quality perceptions of adopting cloud cybersecurity. Majority of the student respondents indicated to have not encountered any cybersecurity attack and did not face any difficulties securing materials online. The results showed that most respondents believed the lack of physical control of data and harmful activities executed on the network (internet) as challenges of using cloud cybersecurity. Majority of the student, lecturers, and admin staff have indicated prevention of presenting false identity as a benefit of using cloud cybersecurity, while IT staff have indicated cheaper security costs as a benefit. Most of the admin staff respondents have indicated that cloud-cybersecurity is important for protecting the faculty staff member's computer and mobile device applications, while IT staff indicated that it is important for preventing denial-of-service. In terms of quality, a large number of respondents believe cloud-cybersecurity is accurate and effective.

4.8. Section D: Perceptions And Awareness Of Cloud Cybersecurity Adoption

This section reports on the participants' perceptions of and attitude towards cloud cybersecurity usage and adoption. The respondents were required to rate their opinions on a scale of 1-5 ranging from strongly agree to strongly disagree. It includes perceptions of cloud cybersecurity performance expectancy, effort efficiency, social influence, facilitating conditions, intention of use, and awareness. The results are depicted in the subsequent subsections.

4.8.1. Perception of Performance Expectancy of Cloud Cybersecurity

This sub-section presented findings on the responses to question regarding the perceptions and attitudes towards the use of cloud-cybersecurity within tertiary institutions in terms of its performance. The measures of performance were based on usefulness and convenience, efficiency, and complexity as it can influence their willingness to adopt cloud-cybersecurity. The results in Table 4.12 showed that the majority of the respondents believed that the performance of cloud-cybersecurity is relatively good as most of the respondents agreed with the statements provided.

The results revealed that 42.4% and 41% of respondents strongly agreed and agreed respectively that cloud-cybersecurity will be useful and convenient in protecting materials on blackboard, social media and ITS Systems, making a total of 83.4% of respondents who agreed. From the respondents

who agreed, 82.5% were from Univen, 87.4% from TVET and 80.9% from Rosebank. However, 4.3% and 1.45% of respondents disagreed and strongly disagreed with a total of 5.4% who disagreed, while an aggregate of 10.9% of respondents neither agreed nor disagreed.

Table 4.12 also depicted that a greater number of 216 (49%) respondents agreed and 125 (28.3%) respondents strongly agreed that cloud-cybersecurity can enable to track security breaches quickly and efficiently, which would in turn, save time that one could spend in managing the security and applications of their data. From the 77.3% of respondents who were in an agreement, a sum of 78.1% were from Univen, 82.4% from TVET and 69.2% from Rosebank, which showed that level of agreement at TVET was the highest. 27 (6.1%) respondents disagreed and 6 (1.4%) respondents strongly disagreed, while a considerate amount of 67 (15.2%) respondents remained neutral.

In terms of the complexity of cloud-cybersecurity processes, an aggregate of 21.8% and 41.5% of respondents strongly agreed and agreed that cloud-cybersecurity processes are less complicated, which makes a total of 63.3% of respondents who agreed. From the respondents who were in an agreement, 57.5% were from Univen, 73.6% were from TVET and 63.9% were from Rosebank. The results revealed that the level of agreement at TVET was 16.1% higher than Univen and 9.7% higher than Rosebank. A sum of only 8.8% and 3.6% of respondents disagreed and strongly disagreed, making a total of 12.4% who disagreed. However, an aggregate of 24.3% of respondents remained neutral with the statement, which is 2.5% higher than those who have strongly agreed.

Table 4.12: Perceptions on Performance Expectancy of Cloud Cybersecurity

Category	Item	Univen		TVET		Rosebank		Total	
I believe Cloud-cybersecurity:		**F**	**%**	**F**	**%**	**F**	**%**	**F**	**%**
Will be useful and convenient in protecting materials on e-learning platform and other learning applications such as emails and social media as well as on ITS systems	Strongly Agree	98	43%	55	46.2%	34	36.2%	**187**	**42.4%**
	Agree	90	39.5%	49	41.2 %	42	44.7%	**181**	**41%**
	Neutral	29	12.7%	6	5.0%	13	13.8%	**48**	**10.9%**
	Disagree	9	3.9%	6	5.0%	4	4.3%	**19**	**4.3%**
	Strongly Disagree	2	0.9%	3	2.5%	1	1.1%	**6**	**1.4%**
can enable me to track any security breaches quickly and efficiently saving my time in managing the security of my applications and data	Strongly Agree	59	25.9%	37	31.1%	29	30.9%	**125**	**28.3%**
	Agree	119	52.2%	61	51.3%	36	38.3%	**216**	**49%**
	Neutral	38	16.7%	10	8.4%	19	20.2%	**67**	**15.2%**
	Disagree	9	3.9%	8	6.7%	10	10.6%	**27**	**6.1%**
	Strongly Disagree	3	1.3%	3	2.5%	29	30.9%	**6**	**1.4%**
processes are less complicated	Strongly Agree	40	17.5%	36	30.3%	20	21.3%	**96**	**21.8%**
	Agree	91	40.0%	52	43.7%	40	42.6%	**183**	**41.5%**
	Neutral	67	29.4%	17	14.3%	23	24.5%	**107**	**24.3%**
	Disagree	19	8.3%	11	9.2%	9	9.6%	**39**	**8.8%**
	Strongly Disagree	11	4.8%	3	2.5%	2	2.1%	**16**	**3.6%**
	Total	**228**	**100%**	**119**	**100%**	**94**	**100%**	**441**	**100%**

Although the majority of respondent agreed with the statements, the usefulness and convenience of cloud cybersecurity received the most attention as it dominated with 83.4% of the level of agreement compared to the other measures, therefore having a positive effect on the willingness of adoption.

4.8.2. Perception of Effort Expectancy of Cloud-Cybersecurity

This part presented results on the responses to question regarding the perceptions and attitudes towards the use of cloud cybersecurity within tertiary institutions in terms of its effort expectancy. The measures of performance were based on understandability, easiness of use and easiness of skills development. The respondents believed that using cloud cybersecurity is relatively easy and understandable as most of the respondents agreed with the statements provided.

The findings in Table 4.13 revealed that a greater percentage of 46.5% of respondents agreed and 21.5% strongly agreed that cloud cybersecurity service interactions would be clear and understandable, making a sum of 68% of respondents who agreed. This result is possibly due to the respondents believe in cloud cybersecurity being user-friendly. From the respondents who agreed, a sum of 63.2% were from Univen, 77.3% were from TVET, and 68.1% were from Rosebank. The results implied that the level of agreement in TVET was 14.1% higher than Univen and 9.2% higher than Rosebank. It can be assumed that respondents at TVET are more exposed and familiar to latest technologies than Univen and Rosebank. However, a sum of 10.6% disagreed. The respondents might have disagreed with a believe that technologies are complex and may be difficult to interact with. 21.3% of respondents remained neutral. This result is a challenge as respondents would remain inconclusive about their choice towards adoption.

Table 4.13: Perceptions on Effort Expectancy of Cloud Cybersecurity

Category	Item	Univen		TVET		Rosebank		Total	
		F	%	F	%	F	%	F	%
Cloud computing cybersecurity service interactions would be clear and understandable	Strongly Agree	39	17.1%	34	28.6%	22	23.4%	**95**	**21.5%**
	Agree	105	46.1%	58	48.7%	42	44.7%	**205**	**46.5%**
	Neutral	58	25.4%	16	13.4%	20	21.3%	**94**	**21.3%**
	Disagree	18	7.9%	7	5.9%	9	9.6%	**34**	**7.7%**
	Strongly Disagree	8	3.5%	4	3.4%	1	1.1%	**13**	**2.9%**
It would be easier for me to learn and develop the skills to use cloud computing cybersecurity features.	Strongly Agree	72	31.6%	32	26.9%	29	30.9%	**133**	**30.2%**
	Agree	101	44.3%	71	59.6%	41	43.6%	**213**	**48.3%**
	Neutral	41	18%	7	5.9%	16	17%	**64**	**14.5%**
	Disagree	9	3.9%	4	3.4%	8	8.5%	**21**	**4.8%**

Table 4.13 (*Continued*)

	Strongly Disagree	5	2.2%	5	4.2%	29	0	**10**	**2.3%**
It is easy to use cloud computing cyber-security services	Strongly Agree	60	26.3%	32	26.9%	26	27.7%	**118**	**26.8%**
	Agree	80	35.1%	56	47.1%	37	39.4%	**173**	**39.2%**
	Neutral	65	28.5%	20	16.8%	19	20.2%	**104**	**23.6%**
	Disagree	**18**	7.9%	7	5.9%	11	11.7%	**36**	**8.2%**
	Strongly Disagree	5	2.2%	4	3.4%	1	1.1%	**10**	**2.3%**
	Total	**228**	**100%**	**119**	**100%**	**94**	**100%**	**441**	**100%**

Table 4.13 also indicates that a majority of 48.3% of respondents agreed and 30.2% strongly agreed that learning and developing the skills to use cloud cybersecurity features would be easier, making a total of 78.5% of respondents who agreed. It includes learning and developing skills such as setting up passwords, usernames, and verifying personal details etc. on the cloud system. The respondents might have agreed with certainty to educate themselves with the features of the latest technology and believe that acquiring the skills to use the cloud cybersecurity might not be challenging. The results show that the level of agreement at TVET was 10.6% higher than Univen and 12% higher than Rosebank. This result might be due to respondents at TVET being more approached towards the latest technology. 4.8% and 2.3% of respondents disagreed and strongly disagreed, making a total of 7.1% of respondents who are in a disagreement which is 71.4% lower than those who agreed. However, 14.5% of respondents remained neutral towards the statement.

In terms of ease of use of cloud cybersecurity services, Table 4.13 showed that the highest percentage of 39.2% and 26.8% of respondents agreed and strongly agreed, making a sum of 66% of respondents who agreed. The respondents might be aware that learning how to use a certain system or technology could be easy with the aid of vast information available on the internet. From those respondents who agreed, a sum of 61.4% were from Univen, 74% were from TVET and 61.1% were from Rosebank. The results implied that while the level of agreement at Univen and Rosebank only had a difference of 0.3%, the level of agreement at TVET was 12.4% higher than Univen and 12.9% higher than Rosebank. It can be assumed that the respondents at TVET could be more equipped with facilities of using cloud cybersecurity. An aggregate of 8.2% and 2.3% of respondents disagreed and strongly disagreed, making a sum of 10.5% who are in a disagreement. In contrast, a considerate figure of 23.6% of respondents neither agreed nor disagreed.

Note that although a majority of respondents agreed with the statements, the measure of easily learning and developing skills to use cloud-cybersecurity received the most attention as it dominated with 78.4% of the level of agreement compared to the other statements.

4.8.3. Perception of Social Influence of Cloud-Cybersecurity

This section presented findings on the responses to question regarding the perceptions and attitudes towards the use of cloud-cybersecurity within tertiary institutions based on social influence. The measures were based on influence from important people, influence from family/friends and colleagues as well as support from tertiary institutions. The results showed that majority of the respondents believed that usage and adoption of cloud cybersecurity can be socially influenced.

The statistics in Table 4.14 shows that 18.1% and 38.8% of respondents strongly agreed and agreed that important people who influence their behavior think they should use cloud cybersecurity. The respondent's influence could be from people connected on social media, people from the same community or simply their neighbors. From the respondents who agreed, 52.6% were from Univen, 57.1% were from TVET and 67% were from Univen. The statistics showed that the level of agreement in Rosebank is 14.4% higher than Univen and 9.9% higher than TVET. However, an aggregate of 12.2% and 5.7% of respondent disagreed and strongly disagreed, making a total of 17.9% who disagreed. However, 25.2% of respondents gave neutral responses.

Table 4.14: Perceptions on Social Influence of Cloud Cybersecurity

Category	Item	Univen		TVET		Rosebank		Total	
		F	%	F	%	F	%	F	%
People who are important to me and influence my behavior think I should use cloud computing cyber-security	Strongly Agree	40	17.5%	26	21.8%	14	14.9%	**80**	**18.1%**
	Agree	80	35.1%	42	35.3%	49	52.1%	**171**	**38.8%**
	Neutral	61	26.8%	29	24.4%	21	22.3%	**111**	**25.2%**
	Disagree	33	14.7%	14	11.8%	7	7.4%	**54**	**12.2%**
	Strongly Disagree	14	6.1%	8	6.7%	3	3.2%	**25**	**5.7%**
I would use cloud computing cyber-security if my friends, family or colleagues use it	Strongly Agree	49	21.5%	27	22.7%	16	17%	**92**	**20.9%**
	Agree	77	33.7%	51	42.9%	46	48.9%	**174**	**39.5%**
	Neutral	56	24.6%	28	23.5%	21	22.3%	**105**	**23.8%**
	Disagree	30	13.2%	9	7.6%	7	7.5%	**46**	**10.4%**

Table 4.14 (*Continued*)

	Strongly Disagree	16	7%	4	3.4%	4	4.3%	**24**	**5.4%**
My tertiary institution encourages/ supports students to use cloud computing cyber-security	Strongly Agree	50	21.9%	23	19.3%	20	21.3%	**93**	**21.1%**
	Agree	67	29.4%	31	26.1%	34	36.2%	**132**	**29.9%**
	Neutral	67	29.4%	37	31.1%	21	22.3%	**125**	**28.3%**
	Disagree	28	12.3%	16	13.5%	12	12.8%	**56**	**12.7%**
	Strongly Disagree	16	7%	12	10.1%	7	7.5%	**35**	**7.9%**
	Total	**228**	**100%**	**119**	**100%**	**94**	**100%**	**441**	**100%**

Also, 39.5% of respondents agreed and 20.9% strongly agreed to use cloud-cybersecurity if their friends, family or colleagues use it. It can be assumed that the respondents are influenced by the people within their surrounding environment and might be engaged in discussions about the latest technology trends like cloud cybersecurity. From the respondents who agreed, a total of 55.2% were from Univen, 65.6% were from TVET and 65.9% were from Rosebank. The results implied that the level of agreement at Univen was 10.7% lower than Rosebank, while there was only a difference of 0.3% between TVET and Rosebank. However, 10.4% and 5.4% of respondents disagreed and strongly disagreed with a sum of 15.8% who disagreed.

In terms of encouragement and support from tertiary institutions, 29.9% of respondents agreed and 21.1% strongly agreed that their tertiary institutions support the use of cloud cybersecurity, making a sum of 51% of respondents who agreed. An assumption can be made that tertiary institutions are to some extent getting involved in promoting advanced technologies for securing their environments. The results implied that the highest level of support from tertiary institutions in using cloud cybersecurity was indicated by Rosebank, which was 6.2% higher than Univen and 12.1% higher than TVET. A reason could be a well-established availability of infrastructure and facilities since Rosebank is an urban-based institution. However, 12.1% and 7.9% of respondents disagreed and strongly disagreed. 28.3% of respondents remained neutral with their response.

The findings in Table 4.14 showed that majority of respondents gave a significant level of agreement (60.4%) towards the statement of using cloud cybersecurity if family, friends, and colleagues use it as opposed to other statements.

4.8.4. Perceptions on Facilitating Conditions of Cloud Cybersecurity

This section presented findings on the responses to question regarding the perceptions and attitudes towards the use of cloud cybersecurity within tertiary institutions based on the facilitating conditions. The measures were based on accessibility, knowledge, and availability of IT support/assistance. Majority of the respondents believed that facilitating conditions of cloud cybersecurity could have a significant positive influence on adoption.

The findings in Table 4.15 reveals that 24.8% and 42.7% of respondents strongly agreed and agreed to have access to the resources necessary to use cloud cybersecurity, making a total of 67.5% who agreed. It can be assumed that the respondents could be familiar with and have access to the resources required for the use of cloud cybersecurity like computers, smartphones, network connectivity, hardware equipment, and software. Of the responses who agreed, 65.6% of responses were from Univen, 68.1% from TVET and 71.8% from Rosebank. The results showed that the level of agreement from Rosebank was 6.2% higher than Univen and 3.7% higher than TVET.

Table 4.15 also illustrates that a greater amount of 44% agreed and 22.6% strongly agreed to have the knowledge necessary to use cloud cybersecurity services, making a total of 66.6% of respondents who agreed. It can be assumed that the respondents might be familiar with cloud computing and therefore might have the knowledge to use cloud cybersecurity. Of the respondents who agreed, 60.3% were from Univen, 73.8% from TVET, and 72.3% from Rosebank. While 10.5% of respondents disagreed, only 4.3% of respondents strongly disagreed on having any knowledge, making a total of 14.8% who disagreed. 18.7% of respondents gave a neutral response.

Table 4.15: Perceptions on Facilitating Conditions of Cloud Cybersecurity

Category	Item	Univen			TVET			Rosebank			Total	
		F	P	VP	F	P	VP	F	P	VP	F	VP
I have access to the resources necessary to use cloud-based cybersecurity	Strongly Agree	57	25%	25.1%	29	24.4%	24.4%	23	24.5%	24.5%	**109**	**24.8%**
	Agree	92	40.4%	40.5%	52	43.7%	43.7%	44	46.8%	46.8	**188**	**42.7%**
	Neutral	40	17.5%	17.6%	21	17.6%	17.6%	15	16%	16.0	**76**	**17.3%**
	Disagree	26	11.4%	11.5%	11	9.2%	9.2%	10	10.6%	10.6	**47**	**10.7%**
	Strongly Disagree	12	5.3%	5.3%	6	5%	5%	2	2.1%	2.1	**20**	**4.5%**

Table 4.15 (*continued)*

	Total	**227**	**99.6%**	**100%**	**119**	**100%**	**100%**	**94**	**100%**	**100%**	**440**	**100%**
I have the knowledge necessary to use cloud-based cybersecurity	Strongly Agree	45	19.7%	19.8%	33	27.7%	28%	21	22.3%	22.3%	**99**	**22.6%**
	Agree	92	40.4%	40.5%	54	45.4%	45.8%	47	50%	50%	**193**	**44%**
	Neutral	52	22.8%	22.9%	14	11.8%	11.9%	16	17%	17.0	**82**	**18.7%**
	Disagree	26	11.4%	11.5%	13	10.9%	11%	7	7.4%	7.4	**46**	**10.5%**
	Strongly Disagree	12	5.3%	5.3%	4	3.4%	3.4%	3	3.2%	3.2	**19**	**4.3%**
	Total	**227**	**99.6%**	**100%**	**118**	**99.2%**	**100%**	**94**	**100%**	**100.0**	**439**	**100%**
IT Support people will be available for assistance with any difficulties I might encounter while using cloud cybersecurity.	Strongly Agree	50	21.9%	21.9%	36	30.3%	30.3%	24	25.5%	25.5	**110**	**24.9%**
	Agree	90	39.5%	39.5%	53	44.5%	44.5%	44	46.8%	46.8	**187**	**42.4%**
	Neutral	63	27.6%	27.6%	21	17.6%	17.6%	17	18.1%	18.1	**101**	**22.9%**
	Disagree	17	7.5%	7.5%	4	3.4%	3.4%	6	6.4%	6.4	**27**	**6.1%**
	Strongly Disagree	8	3.5%	3.5%	5	4.2%	4.2%	3	3.2%	3.2	**16**	**3.6%**
	Total	**228**	**100%**	**100%**	**119**	**100%**	**100%**	**94**	**100%**	**100.0**	**441**	**100%**

In terms of availability of support and assistance, 42.4% agreed and 24.9% strongly agreed that support and assistance can be received from IT people if any difficulties or challenges are encountered while using cloud cybersecurity. It is assumed that the respondents believe that the IT department is familiar with cloud cybersecurity and could help with problems faced through their help desk services. Out of the respondents who agreed, 61.4% were from Univen, 74.8% from TVET and 72.3% from Rosebank. The results showed that respondents' level of agreement at TVET is 13.4% higher than Univen and 2.5% higher than Rosebank. However, 6.1% and 3.6% of respondents disagreed and strongly disagreed, while 14% of respondents gave a neutral response.

Although the majority of respondents agreed with all the statements, the highest level of agreement (67.5%) catered towards having the resources necessary to use cloud-cybersecurity as opposed to having the knowledge and availability of IT support people.

4.8.5. Intention of Use

This section examined the perceptions of students, lecturers, Admin staff and IT personnel's intention of cloud cybersecurity adoption within tertiary institutions. Figure 4.7 shows that a greater number of 42% of respondents agreed while 38% of respondents strongly agreed, making a total of 80% of respondents who intend to adopt and use cloud cybersecurity. However, from the

respondents who agreed to adopt, a sum of 65.6% were from Univen, 85.6% were from TVET, and 78.7% were from Rosebank. The results showed significant variations amongst the three institutions as the highest level of agreement regarding the intention of adoption was from respondents at TVET which was 20% higher than Univen and 6.9% higher than Rosebank. However, a small percentage of 4.3% and 1.6% of respondents disagreed and strongly disagreed to adopt and use cloud cybersecurity in future, making a sum of 5.9% of respondents who did not intend to adopt. While only 14% of respondents neither agreed nor disagreed remaining neutral.

Item	UNIVEN		TVET		Rosebank	
	F	VP	F	VP	F	VP
Strongly Agree	57	25.1%	50	42.4%	30	31.9%
Agree	92	40.5%	51	43.2%	44	46.8%
Neutral	40	17.6%	9	7.6%	17	18.1%
Disagree	26	11.5%	6	5.1%	3	3.2%
Strongly Disagree	12	5.3%	2%	1.7%	0	0
Total	227	100%	118	100%	94	100%

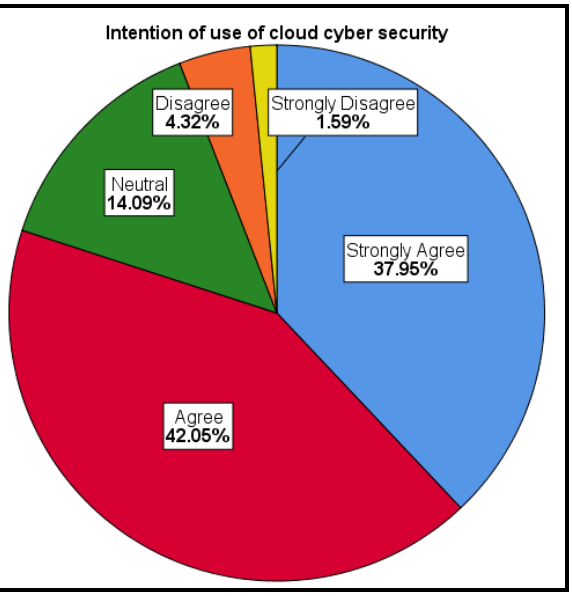

Figure 4.7: Intention of Use of Cloud Cybersecurity Within Tertiary Institutions.

4.8.6. Perceptions of Awareness of Cloud Cybersecurity

This part presents a report on the respondent's perceptions and attitude towards the awareness of cloud cybersecurity. Detailed statistics are presented in Appendix C. A number of 9 elements were measured which are discussed as follows.

Firstly, the respondents were requested to rate their level of agreement regarding their perception of awareness of cloud-based backup and recovery of data stored in cloud systems. The results indicated that an aggregate of 31.7% and 42.4% of respondents strongly agreed and agreed, making a total of 74.1% of respondents who were aware that cloud systems maintain an up-to-date back and recovery of data stored within. It can be assumed that respondents believe backup and recovery ought to be a basic facility of a security system since smartphones have also introduced cloud backup as a built-in feature. Next, the respondents were requested to rate their level of agreement

regarding their awareness of the prevention of unauthorized access to files and data when using cloud cybersecurity. In response, 26.8% of respondents strongly believed that cloud-cybersecurity prevents unauthorized access to files and data, while a greater number (46.1%) of respondents agreed. It can be assumed that respondents might know how to prevent unauthorized access to files through various specialized applications and software developed for smartphones and computers and that cloud cybersecurity could be added as an extra layer of security. Thereafter, perceptions about their level of awareness regarding the security threats and negative consequences of using cloud cybersecurity were determined. In response, the results indicated that a greater percentage of 41.7% of respondents agreed and 28.2% of respondents strongly agreed while 9.1% were in disagreement. The respondents might have agreed with an awareness that security systems have some definite loopholes which could be beyond the respondent's control and thus poses security risks. Of the respondents who agreed, a sum of 65.9% were from Univen, 69.8% were from TVET and 79.7% were from Rosebank.

Furthermore, findings on the respondents' perception of their level of awareness of security training and awareness programs for promoting the efficient use of cloud cybersecurity were determined. If respondents are aware of the training and awareness programs, they will be able to effectively secure their materials on cloud-based e-learning, e-mail, social media, and ITS systems. The results revealed that (35.4%) of respondents agreed and 18.4% of respondents strongly agreed to be aware of the cloud-cybersecurity training and awareness programs. The respondents might have agreed as a result of their interactions with social media and the internet, whereby training programs are advertised or searched for. Subsequently, the respondent's opinions concerning the awareness of the value that cybersecurity adds towards the adoption of cloud were determined. The results revealed that 56% agreed to be aware of the value of cloud cybersecurity. It can be assumed that the respondents are knowledgeable about the advantages cybersecurity could add within the cloud and may have a positive influence on its adoption. The results also revealed that 19.9% and 31.3% of respondents agreed and strongly agreed to be aware of who to contact during a cyber-security attack. It can be assumed that the respondents are knowledgeable about the IT support services offered within their tertiary institutions as well as the help desk support offered by various cloud service providers.

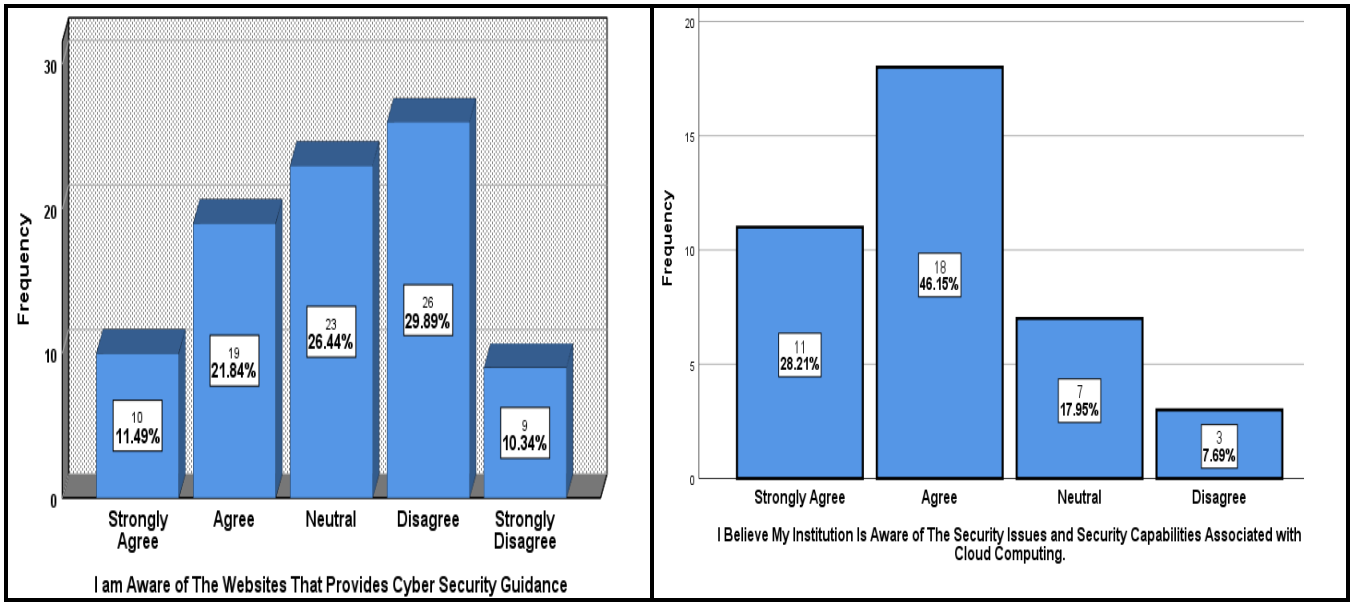

Figure 4.8: Awareness of Cloud Cybersecurity websites and Capabilities

However, the results in Figure 4.8 revealed that 29.9% of respondents disagreed and 10.3% strongly disagreed to be aware of any websites that provide cybersecurity guidance. It can be assumed that there might be a lack of dissemination of appropriate information within the institutions which lead towards respondents failing to acquire cybersecurity guidance. On the other hand, 46.2% of respondents agreed and 28.2% strongly believed that their institutions are aware of the cybersecurity issues and capabilities associated with cloud computing. The overall findings on awareness perceptions revealed that although the majority of respondents agreed with all the other statements, the highest level of agreement (92.3%) catered towards awareness of staff members being notified while data is collected on cloud systems as represented in Figure 4.9 In contrast, the highest level of disagreement (40.8) catered towards awareness of websites providing cyber-security guidance compared to other statements.

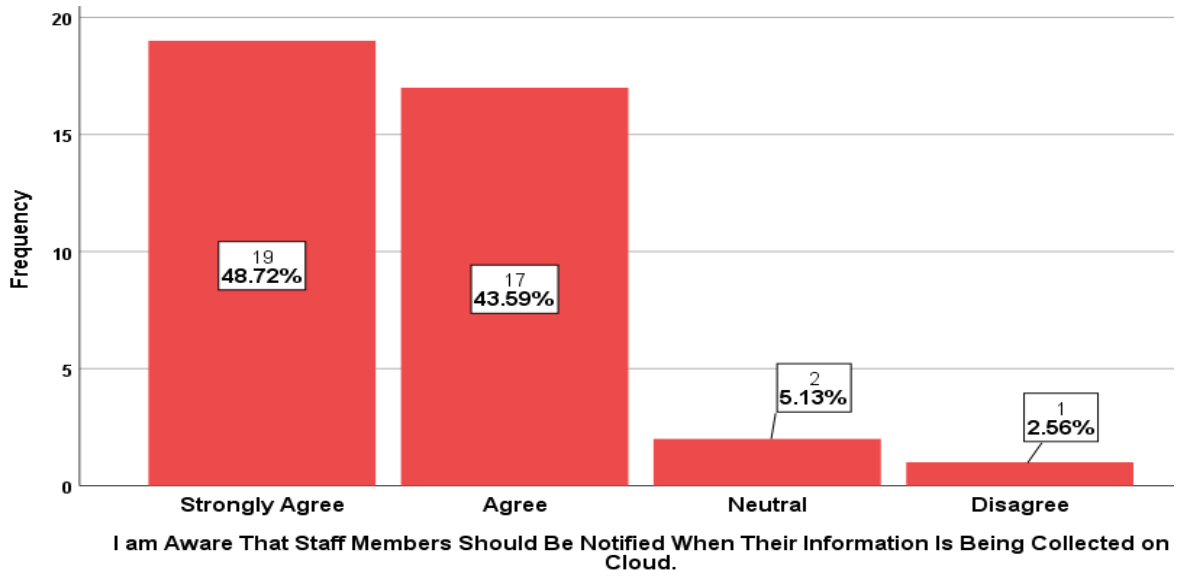

Figure 4.9: Awareness of Staff Members Being Notified While Data is Collected on Cloud Systems

4.8.7. Section D Summary

The objective of determining the cloud-cybersecurity perceptions and its awareness perceptions were achieved. It can be summarized that most of the respondents believed that cloud-cybersecurity is useful and convenient. The participants also indicated that learning and developing skills to use cloud-cybersecurity is easy. Majority of the respondents have shown interest in using cloud-cybersecurity if family, friends, and colleagues use it. The participants also believed to have the necessary resources for using cloud-cybersecurity. Many respondents have shown an intention to adopt and use cloud-cybersecurity. The respondents have indicated to be aware of being notified when their data is captured on the cloud-systems.

4.9. Section E: Reliability, Factor Analysis, and Correlations.

This section started with the analysis of the reliability test conducted through SPSS. It then presented the factor analysis and correlations analysis between the various variables of the study.

4.9.1. Reliability Test

The reliability test in this study measured the consistency of responses of items within a set of constructs in order to determine the degree to which the outcome of the research would remain constant over a certain period of time (Polit & Hungler 1997:296). The research instrument is regarded as reliable if the findings of the research can be imitable and reproducible using a similar methodology. Reliability enabled to purify data and determined the extent to which the test was

free from measurement errors and prevented misleading results (McMillan and Schumacher, 2010). The inter-rater reliability test was used as a measure to assess the degree of agreement of different observers in the assessment decisions and proved to be useful as different observers have different interpretations (Ramagoffu, 2012).

In order to measure the internal consistency, the Cronbach's alpha method/tool was used to assess the degree of reliability which was based on the mean inter-correlations between all the single items within a test (Jain and Angural, 2017). It varied from 0 and 01, whereby 0 specifies no significant relationship between the items on a specified scale, while 01 specifies an absolute significant relationship. According to (Taber, 2017), some scholars stated that generally, a rule of thumb, alpha values above 0.7 are considered good, above 0.8 are very good and above 0.9 are excellent internal consistency. However, values from .6 to < .7 are considered to be a moderate level of reliability taking into consideration the number of items in a scale being less than 10 (Ursachi, Horodnic and Zait, 2015; Hair *et al.*, 2016). The reliability test was performed on seven constructs and analysis are presented in Table 4.16. The findings depicted that the measurements obtained for the seven sections of the instrument were reliable and consistent which were as follows: $\alpha = 0.787$ (awareness), $\alpha = 0.786$ (intention of use), $\alpha = 0.784$ (Quality), $\alpha = 0.705$ (facilitating conditions) $\alpha = 0.668$ (social influence), $\alpha = 0.661$ (performance expectancy), and $\alpha = 0.647$ (effort expectancy). Therefore, all these constructs were used for any further analysis.

Table 4.16: A Reliability Test Analysis For key Constructs of the Research Instrument

Item statistics based on Cronbach's alpha reliability test				
Construct	**Indicator**	**Mean**	**Std. Deviation**	**Alpha (α)**
Quality	Q1	1.83	.829	.784
	Q2	2.05	.878	
	Q3	2.12	.957	
	Q4	2.12	1.002	
	Q5	2.17	.966	
	Q6	2.38	1.179	
Performance Expectancy	PE1	1.81	.891	.661
	PE2	2.03	.896	
	PE3	2.31	1.023	
Effort Expectancy	EE1	2.24	.973	.647
	EE2	2.01	.918	

Table 4.16 (*Continued*)

	EE3	2.20	.998	
Social Influence	S1	2.49	1.096	.668
	S12	2.40	1.093	
	S13	2.56	1.184	
Facilitating Conditions	FC1	2.27	1.082	.705
	FC2	2.30	1.066	
	FC3	2.21	1.005	
Intention of Use	IU1	1.90	.910	.786
	IU2	1.99	.957	
Awareness	A1	2.03	.925	.787
	A2	2.11	.964	
	A3	2.14	1.006	
	A4	2.55	1.149	
	A5	2.42	1.132	

4.9.2. Factor Analysis

Factor analysis enabled to condense information into a small set of dimensions by identifying the smallest number of common factors that account for maximum correlation among indicators (Ramagoffu, 2012). In order to test the structure of the factors of cloud cybersecurity adoption, Confirmatory Factor Analysis (CFA) was performed (Gie Yong and Pearce, 2013). The Exploratory Factor Analysis (EFA) technique in terms of principal component analysis was conducted to discover the new factor structure of the multi-items scale and scrutinize the construct validity (Trope, 2014). The factor analysis was helpful in placing variables of cloud security adoption into meaningful categories. The dimensionality of 25 items was analyzed using principal component analysis and rotated by varimax rotation.

Prior to conducting the EFA, the Kaiser-Meyer-Olkin (KMO) test and Bartlett's Test of Sphericity were performed to examine the factorability. In other words, it was used as a measure of sampling adequacy for testing the eligibility of data. The measures for this test varies from 0 and 01, wherein values nearer to 01 are more adequate. According to (Kaiser, 1974), the acceptable values for KMO is equal to or above 0.60. The KMO measures of sampling adequacy was 0.879, which indicated to be meritorious in terms of its acceptance. The significance of Bartlett's Test of Sphericity ought to be less than 0.05, hence the test results of this dataset were 0.000 which means that EFA is applicable to the data obtained.

After conducting the KMO and Sphericity tests, commonality analysis was performed to determine the degree to which a variable correlates with all the other variables. Communalities for a variable between 0.0 and 0.4 are considered low and specifies that the variable does not correlate well with other variables and therefore items below 0.4 are suggested to be removed (Ul Hadia, Abdullah and Sentosa, 2016). It is suggested by (Nunnally and Bernstein, 1994) that, for a sample size greater than 250, extraction value greater than 0.3 is fairly acceptable. The commonalities presented in Table 4.17 illustrates that all variable extractions were greater than 0.3 which indicated that each variable had some commonality with other variables. The 25 items as examined ranged from 0.393 to 0.746.

Table 4.17: Factor Analysis Communalities

	Survey Item	Initial	Extraction
QP1	Cloud computing cyber-security is reliable and flexible	1.000	.566
QP2	Cloud computing cyber-security is accurate and effective	1.000	.553
QP3	Cloud computing cybersecurity is consistent and relevant	1.000	.549
QP4	Cloud computing cybersecurity services are responsive as I will be informed about security breaches timeously	1.000	.622
QP5	Cloud cyber-security increases the value of cloud computing	1.000	.541
QP6	Necessary infrastructure is available at my institution for supporting system, information and service quality of cloud-cybersecurity	1.000	.593
PE1	Cloud computing cybersecurity will be useful and convenient in protecting my contents on a cloud platform	1.000	.455
PE2	Using cloud computing cyber-security will enable me to track any security breaches quickly and efficiently	1.000	.433
PE3	Cloud computing cybersecurity processes are less complicated	1.000	.484
EE1	Cloud computing cyber-security service interactions would be clear and understandable	1.000	.652
EE2	It would be easier for me to learn and develop the skills to use cloud computing cybersecurity features.	1.000	.592
EE3	It is easy to use cloud computing cyber-security services	1.000	.500
SI1	People who are important to me and influence my behavior think I should use cloud computing cyber-security	1.000	.623
SI2	I would use cloud computing cyber-security if my friends, family or colleagues use it	1.000	.649
SI3	My tertiary institution encourages/supports students to use cloud computing cyber-security	1.000	.639
FC1	I have access to the resources necessary to use cloud-based cybersecurity services	1.000	.746
FC2	I have the knowledge necessary to use cloud-based cybersecurity	1.000	.706
FC3	IT Support people will be available for assistance with any difficulties in using cloud cybersecurity.	1.000	.393

IU1	Assuming I have access to cloud-cybersecurity services, I intend to use it	1.000	.647
IU2	Given that I have access to the cloud-cybersecurity services, I plan to use it.	1.000	.723
A1	I am aware that my data stored in cloud systems maintains an up-to-date back-up and recovery facility	1.000	.607
A2	I am aware that cloud computing cyber-security will prevent unauthorized access to my files	1.000	.522
A3	I am aware of the potential security threats and the negative consequences of using cloud cybersecurity services.	1.000	.585
A4	I am aware of the security training and awareness programs that are provided by various institutions in order to efficiently use cloud-based cybersecurity	1.000	.609
A5	I am aware of the value that cybersecurity adds towards the adoption of cloud computing	1.000	.561
Extraction Method: Principal Component Analysis.			

After the commonality analysis, the total variance was explained by means of extracting eigenvalues in order to determine the numbers of factors to extract from the UTAUT and ISS theory on cloud cybersecurity. The eigenvalues ideally determined which factors are to be retained after extraction. As rule of thumb, it is suggested that factors greater than or equals to eigenvalue with variance equal to 1.0 should be retained and therefore all factors with eigenvalue of less than one were to be cut-off in this study (Gie Yong and Pearce, 2013). This was because a factor of one and above depicts that the factor is relevant and appropriate for analysis. The results in Table 4.18 presented a summary of the total variance explained by each factor. A number of 6 factors were extracted to have an eigenvalue of 1.0 and above. The initial eigenvalues showed that component 1 to 6 explained a respective of 30.9%, 7.3%, 5.8%, 5.1%, 4.5%, and 4.5% of the variance. However, after rotation, the variance per component was changed to 12%, 10.9%, 10.7%, 9%, 8%, and 7.7%. All the 6 components cumulatively described a total of 58% of the total variance.

Table 4.18: Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	**Total**	**% of Variance**	**Cumulative %**	**Total**	**% of Variance**	**Cumulative %**	**Total**	**% of Variance**	**Cumulative %**
1	7.735	30.938	30.938	7.735	30.938	30.938	2.990	11.959	11.959
2	1.824	7.294	38.232	1.824	7.294	38.232	2.725	10.900	22.859
3	1.459	5.837	44.069	1.459	5.837	44.069	2.665	10.658	33.518
4	1.284	5.136	49.205	1.284	5.136	49.205	2.244	8.978	42.496

Table 4.18 (*Continued*)

5	1.131	4.523	53.728	1.131	4.523	53.728	2.008	8.032	50.528
6	1.117	4.468	58.196	1.117	4.468	58.196	1.917	7.669	**58.196**
7	.942	3.768	61.964						
Extraction Method: Principal Component Analysis									

As seen in Table 4.19, the rotated component matrix captured components with correlations of 0.55 and above using principal component analysis. Although the results showed reasonable factors loaded per component, the variables were not grouped into any categories and hence the output generation did not depict any consistent pattern of the loading as the factors were not clustered.

Table 4.19: Component Matrix

Items	Component					
	1	2	3	4	5	6
Cloud Computing cybersecurity service is reliable and flexible	.667					
Cloud Computing cybersecurity service is accurate and effective	.613					
Cloud Computing cybersecurity service is consistent and relevant	.619					
Cloud Computing cybersecurity service is responsive	.621					
Cloud computing cybersecurity will be useful and convenient in protecting my contents on a cloud platform	.635					
Using cloud cybersecurity will enable me to track data breaches quickly and efficiently	.585					
My tertiary institutions encourage/supports students to use cloud cybersecurity				.580		
IT support people will be available for assistance with any difficulties in using cloud cybersecurity services	.597					
Assuming that I have access to cloud cybersecurity services I intend to use it	.565					
Given that I have access to the cloud security services I plan to use it	.558					
I would use cloud cybersecurity if my friends and family or colleagues use it			-.576			
I am aware that my data stored in cloud systems maintains an up to date back-up and recovery facility	.606					
I am aware that cloud computing cybersecurity service will prevent unauthorized access	.585					
I am aware of the security training and awareness programs that are provided by various institutions in order to efficiently use cloud-based cybersecurity	.570					
I am aware of the value that cybersecurity adds towards the adoption of cloud	.638					
Extraction Method: Principal Component Analysis. a. 6 components extracted.						

However, for improving the relationships amongst the factors per component, the rotation needs to be performed. A varimax rotation process was followed. The rotated component matrix indicated that 19 items were extracted to be of significance from the overall dataset of 25 items on cloud cybersecurity adoption perceptions. The strongest factor value of 0.814 was from component 6 and the least strong was 0.557 from component 4 but was still considered for further analysis as it exceeded the factor loading value of 0.55 (acceptable level).

Furthermore, Table 4.20 presents the final loadings with the new labels. It also showed an overview of all the questions per components extracted and the questions which were encompassed in each component. The information in Table 4.20 was used for correlation analysis. However, for ensuring validity and consistency with the theory, the components were categorized as follows: 1 – Quality Perceptions (QP), Component 2 – Awareness (A), Component 3 – Intention of Use (IU), Component 4 – Effort Expectancy (EE), Component 5 – Social Influence (SI), and Component 6 – Facilitating Conditions..

Table 4.20: Final Component Loading

Items	**Component**					
	QP	**A**	**IU**	**EE**	**SI**	**FC**
Cloud Computing cybersecurity service is accurate and effective	.578					
Cloud Computing cybersecurity service is responsive	.633					
Cloud Computing cybersecurity service increases the value of cloud computing	.684					
has cloud computing infrastructure for supporting system, information and service quality of cybersecurity	.701					
I am aware that my data stored in cloud systems maintains an up to date back-up and recovery facility		.635				
I am aware of potential security threats and the negative consequences of using cloud cybersecurity services		.684				
I am aware of the security training and awareness programs that are provided by various institutions in order to efficiently use cloud-based cybersecurity		.698				
I am aware of the value that cybersecurity adds towards the adoption of cloud computing		.719				
Assuming that I have access to cloud cybersecurity services I intend to use it			.752			
Given that I have access to the cloud security services I plan to use it			.812			
Cloud computing cybersecurity processes are less complicated				.557		
Cloud computing cybersecurity service interactions will be clear and understandable				.596		
It will be easier to learn and develop skills to use cloud cybersecurity features				.706		
It is easy to use cloud cybersecurity services				.746		

Table 4.20 (*continued*)

people who are important to me and influence my behavior thinks I should use cloud-cybersecurity					.646	
I would use cloud computing cybersecurity if my friends and family or colleagues use it					.747	
My tertiary institutions encourage/supports students to use cloud computing cybersecurity					.775	
I have access to the resources necessary to use cloud cybersecurity services						.722
I have the knowledge necessary to use cloud cybersecurity						.814
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization. a. Rotation converged in 9 iterations.						

Overall, the factor analysis adequately enabled to deduct variables which were not reliable from the entire data set of the selected constructs, and the results conceived a total of 19 usable variables.

4.9.3. Correlations Analysis.

The correlations test was performed using bivariate correlations in order to determine the relationship among the components (constructs) extracted from the factor analysis (Gogtay and Thatte, 2017). The relationship can be positive, negative or unrelated/weak. The constructs included Quality, Awareness, Intention of Use, Effort Expectancy, Social Influence and facilitating Conditions. The correlations measured enabled to test the strength and direction which existed among the constructs. Pearson's product-moment correlation method was used to evaluate the correlations between the constructs. The values of r, either ±1 depicts that a perfect positive or negative relationship exists between two contrasts, while r=0 indicates no relationship among the constructs. As a general rule of thumb, any r-value that ranges from ± 0.10 to ± 0.29 indicates a weak positive or negative correlation, and any value ranging from 0.30 to 0.49 indicates a moderate relationship, while any value ranging from 0.50 to 1 indicates a strong relationship. Table 4.21 illustrates the output of correlation analysis and the subsequent sections explained the output.

Table 4.21: Correlation Coefficients between the Constructs of the Study

		Q1	A2	I3	EE4	SI4	FC6
Quality = 1	Pearson Correlation	1					
	Sig. (2-tailed)						
Awareness=2	Pearson Correlation	**.445****	1				
	Sig. (2-tailed)	.000					
Intention of Use =3	Pearson Correlation	**.336****	**.355****	1			

Table 4.21 (*Continued*)

	Sig. (2-tailed)	.000	.000				
Effort Expectancy = 4	Pearson Correlation	**.485****	**.430****	**.304****	1		
	Sig. (2-tailed)	.000	.000	.000			
Social Influence = 5	Pearson Correlation	**.301****	**.410****	**.175****	**.315****	1	
	Sig. (2-tailed)	.000	.000	.000	.000		
Facilitating Conditions = 6	Pearson Correlation	**.360****	**.470****	**.321****	**.374****	**.329****	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	
**. Correlation is significant at the 0.01 level (2-tailed).							

a) The relationship between quality and awareness of cloud cybersecurity

The relationship between quality of cloud cybersecurity and awareness was investigated. The analysis depicted that there was a significant moderate correlation between quality and awareness of cloud cybersecurity ($r = .445^{**}$, $p<0.01$). With a significance of (.000), the likelihood that this occurred coincidentally was low. The results indicated that with the increase in quality of cloud-cybersecurity in terms of its accuracy, effectiveness, responsiveness and convenience with the availability of infrastructure in tertiary institutions, the stakeholders (i.e. Staff, lecturers and students) will become more aware of the security threats and its negative consequences which will have a positive influence on adoption of cloud cybersecurity.

b) The relationship between quality and intention of use of cloud-cybersecurity

The relationship between quality and intention of use of cloud cybersecurity was also discovered as presented in Table 4.21. The correlation output demonstrates that the quality of cloud cybersecurity has a moderate positive relationship on the intention of use ($r = .336^{**}$, $p<0.01$) of cloud cybersecurity in tertiary institutions. The probability that this happened by chance was low with a significance of (.000). The results showed that an increase of quality of cloud cybersecurity within tertiary institutions impacted positively on intention of use. A greater quality of cloud cybersecurity may encourage the students, staff, and lecturers to increase usage of cloud cybersecurity for reasons such as securely posting assignments, marks and receiving/ sending messages through cloud-hosted platforms. If increased access to cloud cybersecurity is provided within tertiary institutions, the quality of cloud cybersecurity may improve as feedback from users may increase.

c) The relationship between awareness and intention of use of cloud cybersecurity

The relationship between the awareness construct and intention of use construct was investigated. The analysis output from Table 4.21 confirmed that a moderate positive relationship seems to exist between awareness and intention of use ($r = .355^{**}$, $p<0.01$). The P-value test reported being of (.000) which gives strong evidence to accept that there was a significant positive correlation between the two constructs. The results of the correlation mean that more awareness of cloud cybersecurity has a more positive influence on the intention of use. This also indicated that an increase of awareness of cloud cybersecurity would lead to more students, lecturers and staff members in using cloud cybersecurity and may successively promote the adoption.

d) The relationship between awareness and effort expectancy of cloud cybersecurity

The relationship between awareness and effort expectancy construct was being investigated. The Pearson correlation value of ($r = .430^{**}$, $p<0.01$) approved that there was a moderate correlation between awareness (of cybersecurity features, challenges, benefits, training programs etc.) and effort expectancy. The significance value of (.000) proved that there was a significant positive relationship between the two constructs as there is no evidence of the correlation occurring by accident. The results implied that the more aware students, lecturers, and staff members become about cloud-cybersecurity, the better understanding they will have on using cloud-cybersecurity, and more skills will be developed which will the make it less complex for them to use it.

e) The relationship between the intention of use and effort expectancy of cloud cybersecurity

The relationship between intention of use and effort expectancy constructs was investigated of which the analysis was shown in Table 4.21. The outcome of the Pearson's product moment correlations indicated a reasonable positive relationship between the two constructs ($r = .304^{**}$, $p<0.01$). The significance coefficient of (.000) validated that there was a low probability that the correlations occurred by chance. The analysis showed that an increase in the values of intention of use may lead to an increase in the values of effort expectancy. The results implied that as more lecturers, staff, and students plan to use cloud cybersecurity, the more clear and less complicated cloud cybersecurity processes an interaction will become, and the easier it becomes for them to learn and develop skills of using cloud cybersecurity.

f) The relationship between intention of use and social influence of using cloud cybersecurity

The correlation between intention of use and social influence was investigated. The results have shown a weak strength relationship between the two constructs ($r = .175^{**}$, $p<0.01$). There was no enough to evidence to prove that this correlation might have occurred by coincidence as the significance coefficient was (.000). The results showed that although there was a low positive

correlation, the social influence value will increase to some extent when the intention of use value increases. This indicated that as more people intend to use cloud cybersecurity, the more they will socially influence others for its usage. This means that intention of use may result in a positive impact on the adoption of cloud cybersecurity.

g) Relationship between intension-of-use and facilitating conditions of cloud cybersecurity

The relationship between intention of use and facilitating condition of cloud cybersecurity was examined. The outcome showed a moderate strength correlation between the two constructs ($r = .175^{**}$, $p<0.01$) with a significance of (.000). The analysis implied that as the intention of use of cloud-cybersecurity increase, the facilitating conditions of cloud-cybersecurity will also increase. This means that as more people are willing to use cloud-cybersecurity, more cloud-cybersecurity resources may be accessed, and more knowledge may be gained among the students, staff, and lecturers within the tertiary institutions, hence a significant impact on adoption.

We can easily say that each construct had a moderate strength relationship with each other. Moreover, there was a significant impact amongst each of the constructs, which may to some extent positively influence the adoption of cloud cybersecurity services.

4.9.4. Regression analysis

Regression is a method used for investigating the effect of predictor variables on a specific outcome variable enabling to produce a report on how effectively one or more independent constructs will forecast the value of a dependent construct. The current research utilized a regression model for determining the extent to which quality, awareness, effort expectancy, social influence and facilitating conditions of cloud-cybersecurity impacts the intention of use of cloud-cybersecurity. The analysis results are shown in Table 4.22.

Table 4.22: The Regression Analysis Model

Model	Unstandardized Coefficients		Standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
(Constant)	.603	.151		3.999	.000
Quality	.186	.060	.161	3.084	.002
Awareness	.190	.057	.181	3.322	.001
Effort Expectancy	.123	.063	.102	1.949	.052
Social Influence	-.028	.047	-.029	-.592	.554
Facilitating Conditions	.132	.045	.149	2.939	.003

a. Dependent Variable: Intention of Use				
R-Square	.192		F. Change	20.686
Adjusted R-Square	.183		Sig.	.000[b]

The regression analysis output depicted that the predictor variables for the current study justified 19.2% of the variance in the intention of use of cloud-cybersecurity (adjusted R^2 = .183). The results indicated that quality (Beta =.186, Sig. =.002), awareness (Beta =.190, Sig. =.001) and facilitating conditions (Beta =.132, Sig. =.003) were the main predictors of using cloud-cybersecurity as the significance values were less than 0.05 ($p<0.05$). The results also indicated that effort expectancy (Beta =.123, Sig. =.052) and social influence (Beta = -.028, Sig. =.554) are not significant predictors of using cloud cybersecurity within the tertiary institution. These findings mean that quality contributes to (.161), awareness contribute (.181), and facilitating conditions contribute (.132) positive changes in the intention of use of cloud-cybersecurity within tertiary institutions. Thus, tertiary institutions should give more importance to the quality of cloud cybersecurity and focus on awareness and facilitating conditions in promoting the use and adoption of cloud- cybersecurity.

4.9.5. Chapter Summary

In summary, this chapter presented the analysis of data collected from respondents within three institutions and the results were examined. This chapter conducted the reliability test using Cronbach's alpha method. One construct had a value above 0.7. additionally, the correlation analysis was also conducted to determine the relationship between the significant constructs of the current study. The correlation analysis was performed after conducting the factor analysis which extracted a total of six significant factors. The construct of performance expectancy as originally included in the conceptual framework of this study was ruled out through factor analysis as it was insignificant. Lastly, the regression analysis was conducted to determine the degree of important prediction to the intention of the use of cybersecurity within tertiary institutions. It was found from the regression analysis that quality and awareness can play an important part in influencing the adoption of cloud cybersecurity. The next chapter presents the main findings aligned with research questions and the proposed framework.

CHAPTER FIVE: DISCUSSIONS OF FINDINGS AND PROPOSED CLOUD-CYBERSECURITY ADOPTION FRAMEWORK

5.1. Introduction

The previous chapter provided the analysis, presentation, and interpretation of the collected data from the respondents. This chapter provides a discussion of the main research findings as analyzed in the previous chapter. The chapter seeks to determine if the research questions as outlined in chapter one were answered. A framework for adoption of cloud cybersecurity is proposed based on the results obtained.

5.2. Discussions Based on the Results Obtained.

The key objective of this study was to investigate the effect of cyber-security on cloud usage at Rural based tertiary institutions (The University of Venda, and TVET) in comparison with the urban-based institution (Rosebank), and propose a framework for adoption of cloud computing cybersecurity. The discussions below are based on answering the research questions of the study.

5.2.1. Cloud Cybersecurity Drivers.

The drivers influencing the adoption of cloud cybersecurity in tertiary institutions were discovered by answering the research question: *What are the cyber-security drivers for cloud computing adoption in tertiary institutions?* In order to answer this research question, some background information such as knowledge and experience of using cloud-cybersecurity, the role of cloud-cybersecurity, as well as the cloud-cybersecurity applications and services used was acquired.

5.2.1.1. Knowledge and Experience of Cloud Cybersecurity

According to a research study by (Patala, 2017), the majority of the sampled population were found to be knowledgeable about cloud computing technology at the University of Venda, where most of the students and staff and lecturers were using various cloud-based applications such as email, social networks, and e-learning systems. However, in the current study with reference to the findings, although most of the respondents were knowledgeable (61.9%) about cloud-cybersecurity, a small percentage of only 38.1% indicated to have used it. It was also discovered that although some respondents have indicated not being knowledgeable about cloud cybersecurity, they were found to be using it. The findings also showed that a large number of respondents were familiar with and were using cloud-cybersecurity applications and services from

providers such as Google, Microsoft, and Amazon for products such as Microsoft office, google email, google drive and drop-box. The results have shown that respondents from all the three institutions have indicated having used Microsoft security services as compared to Google and Amazon. This might be due to the fact that their availability of resources may be higher compared to the other two institutions. In contrast, Amazon services were rarely used by the respondents.

5.2.1.2. Role of Cloud Cybersecurity

Furthermore, the respondents highlighted the role cloud cybersecurity could play within their respective tertiary institutions. The findings revealed that within the educational context, a large number of 81.8% of respondents believed that cloud-cybersecurity plays a role of securely uploading, downloading and posting assignments on cloud-based e-learning, email and social media platforms like Facebook and WhatsApp. It should be noted that from the 81.8%, the majority of students (90.1%) were from TVET and the majority of the lecturers were from (78.6%) were from Univen. The results indicated that more lecturers were supportive of the statement from Univen compared to TVET while more students were supportive of the statement at TVET than of Univen. Within the administrative context, most of the IT and admin staff respondents (76.9%) indicated that cloud-cybersecurity plays a role of securely sending and receiving messages to and from colleagues and other stakeholders on cloud-based ITS, email and social media platforms.

5.2.1.3. Drivers Influencing Cybersecurity Adoption

Lastly, the following were revealed as the drivers of cloud-cybersecurity adoption within tertiary institutions: (1) Data security and privacy, (2) Legal law and regulatory compliance, (3) pace of keeping up with the latest technology, (4) financial benefits, and (5) maintaining public reputation and gaining trust from students, lecturers and staff. Although all the five drivers were selected by various respondents based on their knowledge and opinions, data security and privacy of students, staff and lecturer information was highlighted as a major influencing factor (84.4%) to be considered in the adoption of cloud-cybersecurity. From the results, it can be concluded that this research question was fully answered, and it assisted in achieving objective number one of the research study.

5.2.2. Cloud Cybersecurity Issues

The issues of cloud cybersecurity adoption in tertiary institutions were discovered by answering the research question: *What are the current cybersecurity issues at Univen, TVET and Rosebank college?*

The findings revealed that respondents from all three institutions are faced with cloud-cybersecurity issues to some extent. Approximately a total of 25.7% of respondents indicated to have encountered a cybersecurity incident (attack) within the cloud environment. However, the highest percentage of respondents who encountered cyber-attacks were from TVET college (26.6%). Furthermore, it was also revealed that 42.7% of respondents faced difficulties in securing their data and information on the cloud platforms. The highest percentage of respondents who faced difficulties were from TVET (49.5%) compared to Univen and Rosebank. A reason could be that those respondents might be lacking the necessary knowledge required to protect their materials online. Therefore, tertiary institutions should promote knowledge in this area. It can be concluded that this research question was fully answered and objective number two was achieved.

5.2.3. Cybersecurity Challenges, Benefits, and Quality

The challenges, benefits and quality of cloud cybersecurity adoption in tertiary institutions were discovered by answering the research question: *How does cybersecurity challenges, benefits and quality affect the cloud usage and adoption decisions within tertiary institutions?*

5.2.3.1. Challenges of Cloud Cybersecurity

The third research question sought to determine how the adoption decisions of cloud cybersecurity can be influenced based on the three parameters: challenges, benefits and quality perceptions of cloud-cybersecurity. Vulnerability to cybersecurity breaches may become a challenge when adapting the cloud computing technology. The results showed that cybersecurity is a major element contributing towards the adoption of cloud-cybersecurity services. The analysis of results revealed that a wide variety of challenges were highlighted by students, staff, and lecturers. The challenges included: (1) Lack of physical control of data; (2) Harmful activities executed on the internet/network; (3) Data leakage to other cyber-security service users; (4) Denial of service Availability; (5) Monitoring and tracking activities compromising data privacy; (6) Virus infection; (7) Undesirable disclosure of data to law and regulatory bodies; (8) Lack of security awareness causing cyber-attacks; (9) Identity theft and Unauthorized access to cloud applications;

(10) data manipulation (Information can be lost, deleted, moved or changed); (11) Sniffing/spoofing cloud activities; and (12) Hacking of files and data. Based on the evidence presented in chapter 4, most of the respondents indicated lack of physical control of data (9.5%), and harmful activities executed on the internet (9.5%) as challenges of cloud-cybersecurity adoption. It can be implied from this result that most of the respondents' adoption decisions will be significantly based on these two challenges and the cloud providers capacity in protecting users from the two challenges. However, in terms of comparison, lack of physical control of data received the highest percentage at TVET (9.8%), followed by Rosebank (9.7%), then Univen (9.2%), while, harmful activities on the internet received the highest percentage at Univen (10%), followed by Rosebank (9.2%), then TVET (8.7%). However, the study does not imply that other challenges highlighted were of least importance as the challenges highlighted were based on individual opinions of respondents of the study.

5.2.3.2. Benefits of Cloud Cybersecurity

The benefits of using cloud cybersecurity were investigated based on two contexts, namely educational/administrative and technical contexts. In terms of the educational and administrative benefits, the following were identified: (1) prevention of forgery; (2) prevention of presenting a false identity; (3) prevention of interference upon controlled and private conversations; (4) prevention of altering date stamps on submitted work, files and documents such as examination scripts, assignments, financial statements, or admission records; (5) prevention from gaining access to personal data of other students/lecturers/staff. However, most of the students, lecturers and admin staff indicated prevention of presenting a false identity to the institution as a benefit of cloud cybersecurity. It means that the adoption of cloud cybersecurity among students, lecturers and admin staff can be majorly influenced by this benefit. The highest percentage was received by respondents from Rosebank (23.7%) as compared to respondents from Univen (22.1%) and TVET (21.6%). In contrast, the following benefits were identified from the IT staff perspective: (1) cheaper cybersecurity costs; (2) standardized interfaces for managing various cyber-security services; (3) provisioning of cyber-security auditing; (4) increased support for defensive measures during cyber-attack(s); and (5) efficient/effective capabilities of incident response. However, most of the IT staff members indicated increased support for defensive measures during a cyber-attack as a benefit of using cloud cybersecurity. Thus, this is a highly influencing beneficial element that IT staff within tertiary institutions would consider in the adoption of cloud cybersecurity.

5.2.3.3. Quality of Cloud Cybersecurity

In terms of the quality perceptions, the following quality measures of cloud-cybersecurity were identified: (1) reliability and flexibility; (2) accuracy and effectiveness; (3) consistency and relevancy; (4) responsiveness; (5) increased value; and (6) availability of infrastructure. However, most of the respondents have indicated to agree with accuracy and effectiveness of cloud-cybersecurity as a highly influencing quality measure in the adoption of cloud-cybersecurity within tertiary institutions. The highest level of agreement in this regard was from Rosebank (80.8%) as compared with Univen (75%), and TVET (76.9%). This means that when making adoption decisions, most of the respondents will consider how accurate cloud-cybersecurity is depending on their individual needs and will also consider how effective cloud-cybersecurity could be in protecting their data and information on cloud platforms.

5.2.3.4. Importance of Cloud Cybersecurity

Furthermore, the admin staff members have revealed that cloud-cybersecurity is important within tertiary institutions for protecting their business processes and systems. This includes protecting: (1) central administrative systems such as finance and human resource systems; (2) research systems and databases as it contains intellectual research properties; (3) departmental systems such as ITS integrator and MyAccess; (4) web applications such as office 365; and (5) computer and mobile devices applications and files of staff members. Despite the various reasons given indicating the importance of cloud-cybersecurity, most of the respondents (24.5%) have shown that protecting their computers and mobiles devices from attacks is of utmost importance as most of their work-related activities are conducted online. The highest percentage was received by respondents from Univen (27%) as compared to TVET (21.9%). In contrast, the IT staff respondents have revealed that adoption of cloud-cybersecurity is also important from a technical perspective. This includes: (1) preventing denial-of-service; (2) protecting against data breaches; (3) eliminating internal and external malicious threats; (4) protecting web applications; (5) protecting user identities as cloud-cybersecurity has multiple authentication processes; (6) ensuring privacy of communication; and (7) preserving the integrity of the institutional databases. Despite the several reasons discovered, prevention of denial-of-service (16.7%) turned out to be a highly influencing factor to be considered in the adoption decision of cloud-cybersecurity. Form the data collected, it can be said that the business processes within the tertiary institutions can be more securely protected through cloud-cybersecurity. The positive responses of respondents also indicate that they will be more satisfied in using cloud-cybersecurity services for protecting their

contents than traditional systems. Based on the findings, it can be concluded that this research question was fully answered and objective number three was achieved.

5.2.4. Perceptions and Awareness of Cloud Cybersecurity

The perceptions and awareness of cloud cybersecurity adoption in tertiary institutions were discovered by answering the research questions: *Are the stakeholders at Univen, TVET and Rosebank college aware of the major cloud-cybersecurity issues? and how do they perceive the cyber-security aspects of cloud computing?*

5.2.4.1. Awareness of Cloud Cybersecurity

The fourth research question sought to determine if the students, lecturers, and staff at Univen, TVET and Rosebank were aware of the major cybersecurity issues. The results revealed that respondents were aware of the backup and recovery facility of data and information within the cloud environment. The students, lecturers, and staff also indicated to be aware of the fact that cloud-cybersecurity has the capability of preventing unauthorized access to their files. However, only a few respondents agreed to be aware of the threats and negative consequences of using cloud cybersecurity services. Additionally, some respondents have specified not to be aware of any cybersecurity training and awareness programs which could negatively influence the adoption. Most of the respondents were aware that cybersecurity adds greater value to the cloud computing environment which could positively influence the adoption of cloud computing. The results obtained also revealed that a large number of the respondents were aware of who to contact within their institutions when they encounter a cyber-security attack. Furthermore, majority of the respondents were not aware of the websites that provisions cyber-security guidance for efficiently using cloud-cybersecurity. However, the respondents believe that their respective institutions are aware of the cybersecurity issues and capabilities associated with cloud computing and its usage. In contrast, staff members have indicated to be aware of getting notified while their information is collected on the cloud systems such as their personal details.

5.2.4.2. Perceptions of Cloud Cybersecurity

In addition, the respondents were also required to indicate how they perceive the cyber-security aspects of cloud computing. The perceptions of the possible adopters have shown to influence the use and adoption of cloud-cybersecurity within tertiary institutions. The results obtained revealed that there is an opportunity for students, staff and lecturers in South African tertiary institutions to

start utilizing cloud cybersecurity for securing their everyday tasks and activities performed online. The perceptions of cloud-cybersecurity are categorized based on five constructs namely: (1) performance expectancy; (2) effort expectancy; (3) social influence; (4) facilitating conditions; and (5) intention of adoption. With regards to perceptions of performance expectancy, most of the respondents believe that cloud-cybersecurity is useful; convenient; efficient; and less complex. With regards to the perceptions of effort expectancy, most of the respondents believe that cloud-cybersecurity is clear and understandable; easy to use; and easier to learn and develop skills to use cloud-cybersecurity. With regards to perceptions of social influence, the respondents believe that important people in their lives influence them in using cloud-cybersecurity. The majority of the respondents indicated to use cloud-cybersecurity if friends, family, and colleagues use it. They have also indicated to believe that their tertiary institution encourages and supports students, lecturers, and staff in using cloud-cybersecurity. With regards to perceptions of facilitating conditions, a large number of respondents indicated to believe that they have access to the necessary resources; knowledge; and availability of support from IT department required in using cloud-cybersecurity. Lastly, with regards to intention of use, a greater number of respondents have shown to plan and intend using cloud-cybersecurity if access is provisioned by their tertiary institutions. Based on the findings, it can be concluded that this research question was fully answered and objective number four was achieved.

5.2.5. Suggested Framework for Cloud Cybersecurity Adoption

The framework of cloud cybersecurity adoption in tertiary institutions was proposed based on the results of the study and answered the research question: *What framework can be suggested for cloud-cybersecurity adoption in tertiary institutions?*

This question sought to propose a cloud-cybersecurity adoption framework for South African tertiary institutions. However, some background information concerning cybersecurity policies, frameworks, audits, and strategies was collected. The findings revealed that the IT staff respondents from Univen and TVET indicated that their institution does have any cloud-based cyber-security policies implemented for maintaining cyber-attacks. They also highlighted that there are currently no cyber-security frameworks established within their cloud environments. Furthermore, their institutions do not undergo any regular third-party audits with the cloud service providers concerning cloud-cybersecurity, meaning that there are no cyber-security controls in place. Lastly, the management and IT department have not circulated any cloud-cybersecurity

strategies to the employees within the tertiary institutions which could protect the systems from cyber-attacks. It was also discovered during the research process that there are currently no cloud-cybersecurity adoption frameworks established and implemented in other industries based on available literature. Therefore, a suitable cloud-cybersecurity adoption framework is developed in this study to assist in its successful adoption and usage within tertiary institutions in South Africa. Thus, it could be implemented to enhance the usage of cloud computing cybersecurity within the tertiary institution's business environment surrounded by students, staff, and lecturers. The framework is critically explained in the next section.

5.3. Cloud Cybersecurity Adoption Framework for Tertiary Institutions

The proposed framework entails the critical success factors for adoption of cloud cybersecurity. The framework and the significant elements within each critical success factor were illustrated in Figure 5.1 Each of these factors are discussed in the subsequent sub-sections as follows:

5.3.1. Cloud Cybersecurity Drivers

The framework proposed specific cybersecurity drivers that have an influence on the adoption from the data collected. The analysis revealed that the drivers are critical factors in the adoption as they will enable to determine what promotes the use of cloud-cybersecurity within tertiary institutions. The first driver which is improving data security and privacy was shown to affect the adoption of cloud cybersecurity with 84.4%. The legal law and regulatory compliance were also a critical driver influencing the adoption of cloud cybersecurity with 50.1%. Therefore, it is proposed that the government of South Africa in alignment with authorities from various tertiary institutions develop appropriate cybersecurity laws and regulations for protecting critical information. The pace of keeping up with the latest technology was identified as an influencing factor with 77%. Tertiary institutions require a roadmap of short- and long-term goals for cloud cybersecurity adoption. The reduced financial burden driver was shown to affect the adoption with 70.2%, as cloud cybersecurity costs are cheaper than in-built security systems. Maintaining public reputation was also identified as an influencing factor with 72.3%. Therefore, by implementing cloud cybersecurity, tertiary institutions systems and databases can be efficiently protected and chances of attacks such as ransomware can be reduced. The results are constant with the study of (Loanzon, 2014a), which identified these drivers as factors for cloud cybersecurity adoption.

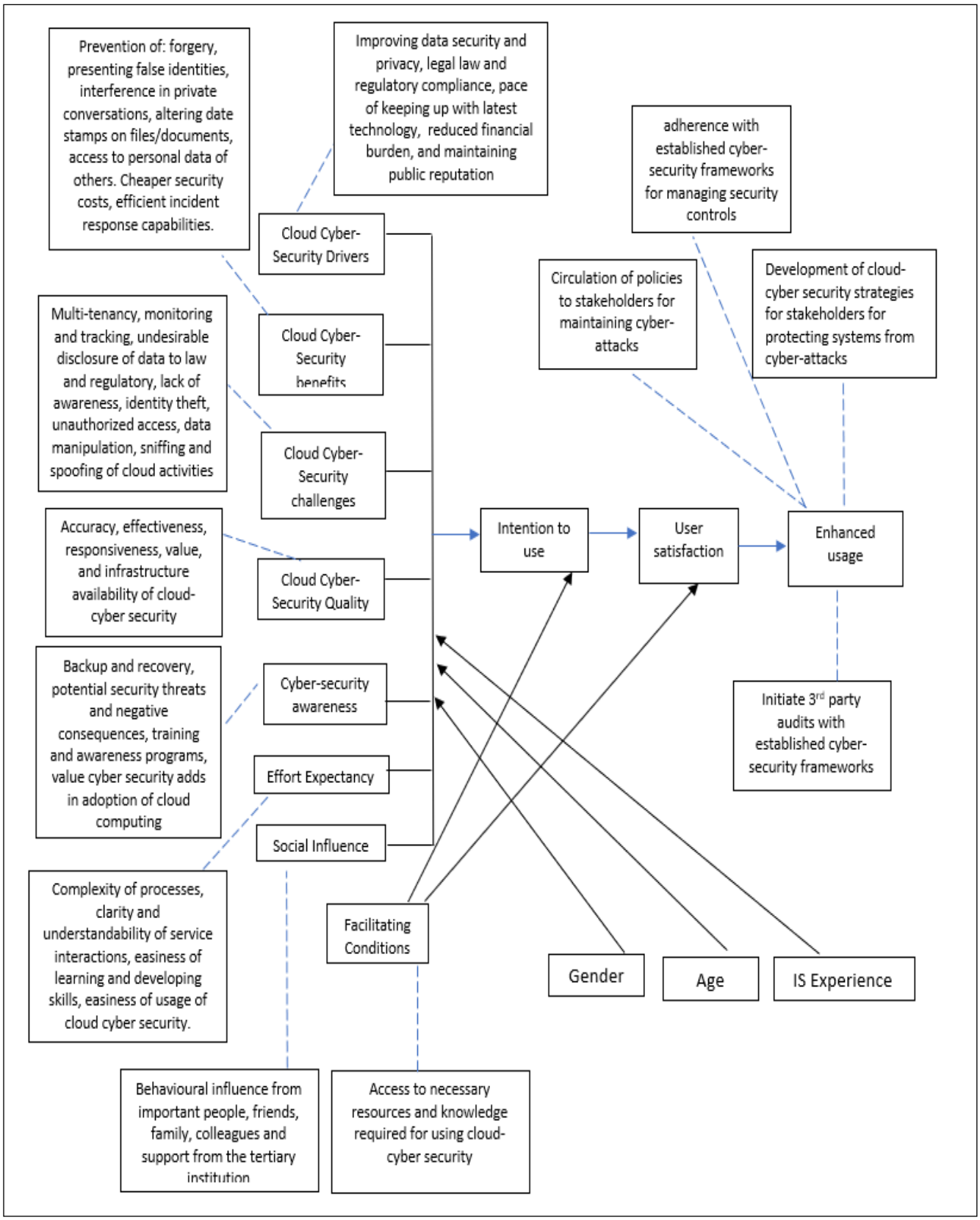

Figure 5.1: Cloud Cybersecurity Adoption Framework for Tertiary Institutions

5.3.2. Benefits of Cloud Cybersecurity Adoption

The findings revealed that the benefits affect the intention of adoption of cloud cybersecurity within the South African tertiary institutions. This variable was supported as a possible predictor of adoption due to the fact that most respondents, especially the students, were aware of and clear about the benefits of using cloud cybersecurity. The benefits of using cloud cybersecurity were realized because most of the students have used cloud computing technology and it's readily available applications such as Google apps, Microsoft office, and Dropbox. According to (Alshamaileh, 2013), when firms and institutions perceive that latest technology offers a relative benefit, then it is more likely that they will adopt that innovation. However, these benefits have to be clear for and understood by tertiary institutions in the adoption decision. Therefore security benefits such as prevention of identity fraud, interference in private communications, manipulation of date stamps on files and documents, and unauthorized access to data play a pivotal role in facilitating the adoption and use of cloud cybersecurity. The results vary from the studies conducted by (IBM, 2012; Vaishali Pardeshi, 2013; Nyembezi, 2014; Chibaro, 2015) which were concerning the benefits of cloud computing adoption within higher education institutions.

5.3.3. Challenges of Cloud Cybersecurity Adoption

It has been shown in this research that the challenges of cloud cybersecurity negatively affect the adoption of cloud computing. The challenges may limit the tertiary institutions to adopt cloud cybersecurity because respondents have shown to be aware of drawbacks such as lack of physical control of data, multi-tenancy, identity theft, sniffing/spoofing, and unauthorized access. Tertiary institutions may feel restricted by their capabilities to perform some tasks of running cybersecurity systems. Therefore, some sort of assurance is required from cloud service providers on the handling of these challenges with proper plans, designs, implementations, and management of cybersecurity systems specifically geared towards a tertiary institutions' internal and external operational environment. Although the perception is that cloud cybersecurity poses a threat to the users of tertiary institutions, recent developments show that the cloud environment may provide improved security for tertiary institutions. The cloud security challenges identified in this study are similar to the studies of (Subashini and Kavitha, 2011; Ramagoffu, 2012; Zissis and Lekkas, 2012; Parekh and Sridaran, 2013; Akin, Matthew and Comfort, 2014).

5.3.4. Cloud Cybersecurity Quality

The findings suggested that quality affects the cloud cybersecurity adoption decisions of students, lecturers, and staff within tertiary institutions. The quality of cloud cybersecurity considered three dimensions namely system, information and service quality. The respondents have shown to believe cloud cybersecurity to be reliable, flexible, accurate, effective, consistent, relevant, responsive and valuable. These attributes are important towards adoption, since the higher the quality, the higher the security effects, then the greater the likelihood of attracting positive user intentions and successful user satisfaction among tertiary institutions in South Africa (DeLone and McLean, 2016). The study also reported a significant ($p<0.01$) influence between quality and intention of adoption and use. As the relationship was moderately positive ($r = .445$), quality accounted for 11.9% of the total variance on the respondents' perception towards the adoption of cloud cybersecurity within tertiary institutions. Although the scope is not the same, the results concur with the study conducted by (Ayooluwa, 2016), which highlighted that quality plays an important role in the adoption of latest technologies in teaching and learning at universities. However, other IS and cloud-based studies have expressed features such as convenience of access, adaptability, integration, content, support, and availability to have played a vital role in showing competence to its users and forecasting the behavior of use (Flack, 2016; Lian, 2017; Rammutloa, 2017; Adya and Wang, 2018). Therefore, these features together with the quality features identified in this study should be considered as metrics for measuring the quality of cloud-cybersecurity adoption within South African tertiary institutions.

5.3.5. Cloud Cybersecurity Awareness

The results suggested that awareness affects the adoption of cloud cybersecurity within tertiary institutions. The study also reported a moderate significant ($r = .355^{**}$, $p<0.01$) influence between quality and intention of adoption and use of cloud cybersecurity in South African tertiary institutions. Improved awareness may result in tertiary institutions to understand the potential cloud cybersecurity can provide in the areas of teaching, learning, research, and finances. The results have shown that respondents were aware of the basic cybersecurity features such as prevention of unauthorized access and back-up and recovery. The study of (Apulu, 2012) suggested that lack of awareness has delayed the adoption technologies because users are not confident about it. Most respondents have indicated to be aware of the value of cloud

cybersecurity. However, respondents who were not aware required resources such as guides, websites and help desk support for identifying the capabilities and issues of cloud cybersecurity adoption and reducing the level of uncertainty. As awareness is an important predictor of influencing adoption of cloud cybersecurity, the results concur with the study of (Kajiyama, 2012; Siyaboni, 2012; Chibaro, 2015; Introna, 2015; Ayooluwa, 2016).

5.3.6. Effort Expectancy

The results have shown that effort expectancy significantly predicts the adoption of cloud cybersecurity within tertiary institutions in South Africa ($r = .304^{**}$, $p<0.01$). For cloud cybersecurity services to be diffused successfully, they must be convenient, easy to use, efficient and less complex. The overall perception of students, lecturers, and staff was that cloud cybersecurity would be easy to use and understand. The respondents agreed that the interactions with cloud cybersecurity would be clear and skills would be easy to develop. The perceptions were based on the fact that most of the respondents were using cloud applications such as Gmail, Microsoft office and YouTube. The simplicity of cloud cybersecurity in terms of understanding how to use it would be an important influencing factor especially for those with fewer computer skills. The results concur with the studies of (Suman, Mathur and Dhulla, 2014; Chibaro, 2015; Hashim and Hassan, 2015), which stated that effort expectancy has a positive influence on innovative technology adoption decisions.

5.3.7. Social Influence

The role of social influence on the adoption of technology has been complex, whereby impact is created through compliance, internalization and identification (Venkatesh *et al.*, 2003). The findings revealed that social influence positively ($p<0.01$) affects the adoption of cloud cybersecurity within tertiary institutions. Social influence depends on the environment in which the users are situated, social influence could be a non-existent factor for users coming from a disadvantaged background. The respondents agreed to have had an influence from important people, friends, family and support from tertiary institutions. The findings coincide with the studies of (Suman, Mathur and Dhulla, 2014; Chibaro, 2015), which stated that social influence has a significant positive impact on the intention of adoption. However, the results vary from the study of (Nyembezi, 2014), where social influence had no positive influence on the intention of adoption.

5.3.8. Facilitating Conditions

The study found the effect of facilitating conditions to be significant ($p<0.01$) towards cloud cybersecurity adoption and use. The also study also revealed that facilitating conditions have a positive role in the adoption of cloud cybersecurity. The respondents have agreed to have access to the resources, infrastructure, and IT support within their tertiary institutions required for using cloud cybersecurity services. Tertiary institutions ought to include factors such as training, management and IT support in the implementation context of cloud cybersecurity for those users who have disagreed to have access to resources and support. The assessment of the availability or absence of the factors facilitating the cloud cybersecurity adoption ought to be in relation to the existing practice of cloud computing usage within the context of tertiary institutions. The results concur with the study of (de Oliveira *et al.*, 2013; Cao, Bi and Wang, 2014; Yaokumah and Amponsah, 2017), which indicated that facilitating conditions have a significant influence towards the adoption of cloud-based technologies. However, the study of (Suhendra, Hermana and Sugiharto, 2009) found that facilitating conditions mostly had an impact on actual use but not on the intention of adoption. Nevertheless, the results vary from the study of (Nyembezi, 2014), where facilitating conditions had no positive influence on the intention of adoption.

Overall, the framework suggests that tertiary institutions should take into consideration the elements detailed within each critical factor of cloud cybersecurity adoption. The framework is significant as it is uniquely designed for rural tertiary institutions and it strives to initiate a stable and secure standard for cloud operations and aimed to provide a secure roadmap for safely adopting cloud cybersecurity. As alluded in chapter 2 (section 2.12) of this study, the framework bridges the gap identified of a lack of cloud cybersecurity framework for rural tertiary institutions in South Africa. The framework provides clarity on benefits, challenges, and awareness of cybersecurity for rural tertiary institutions. The framework also suggests that for enhanced usage, tertiary institutions should initiate third-party audits in line with other established cloud security frameworks.

5.4. Chapter Summary

This chapter discussed the main research findings of the research. All the research questions aligned with the objectives were answered. The drivers, benefits, challenges and quality factors were discussed. Also, the effort expectancy, facilitating conditions and social influence as

predictors of intention of use were outlined. The significance of awareness towards the adoption of cloud cybersecurity was highlighted as well. A framework for adoption of cloud cybersecurity was proposed based on the findings obtained. The performance expectancy factor was not included in the framework because it was insignificant in this context according to the results obtained.

CHAPTER SIX: CONCLUSIONS AND RECOMMENDATIONS

6.1. Introduction

The results presented in chapter four and discussions from chapter 5 enabled the researcher to draw conclusions on the research study. The contributions of the research towards the knowledge body are highlighted in this chapter. Furthermore, the limitations to the research study are outlined. The chapter seeks to highlight recommendations as well as the suggestions for future research. Lastly, the concluding remarks of the study are provided.

6.2. Key Findings of the Research Study

The study has found that cloud cybersecurity provides tertiary institutions with a cost-effective solution to implement security systems in South Africa as a developing country. The study also found that the urban and rural-based privilege of tertiary institutions did not make any significant difference towards the intention of adoption and use of cloud cybersecurity. Hence it could be suggested that cloud cybersecurity is fit for use for both urban and rural based institutions. Cloud computing proved to be a valuable platform in both rural and urban-based tertiary institutions and therefore can reap the benefits of cloud cybersecurity with consciousness regarding the associated challenges. General conclusions on the key findings are as follows:

- The study found that most of the respondents were knowledgeable of cloud cybersecurity although had less experience of using it.
- The findings found that most respondents (students, lecturers, and staff) were aware of cloud cybersecurity drivers.
- The results showed that respondents were aware of the benefits that cloud cybersecurity has for tertiary institutions in improving their security environment within the teaching and learning context as well as the technical context.
- The findings also showed that respondents were aware of the challenges and threats of adopting cloud cybersecurity. These challenges could possibly slow down the adoption level of cloud cybersecurity within tertiary institutions.
- The findings indicated that quality plays an important role in respondents' adoption decisions of cloud cybersecurity.

- The results indicated that there is some sort of awareness of cloud cybersecurity amongst students within the tertiary institutions, however, staff and lecturers do not have enough awareness of using it.
- Factors such as effort expectancy, social influence and facilitating conditions were found to have an important influence on the adoption of cloud cybersecurity. However, performance expectancy was not an important influencing factor.
- The results found that the tertiary institutions were not in adherence with established security frameworks, neither initiated any third-party audits with cloud services providers.
- The results found that no strategies were developed and circulated to the staff and students for maintaining cyber-attacks and protecting security systems from cloud cyber-attacks

6.3. Contributions of the Research Study

This research added value to the current body of knowledge as it contributed to the theory of UTUAT and ISS by laying a foundation in the field of information systems and cloud computing cybersecurity, particular to South African tertiary institutions. Key factors affecting the adoption and use of cloud-cybersecurity were identified. In terms of practical contribution, an implementation framework for cloud computing cybersecurity adoption was developed. The framework can aid tertiary institutions chosen in this study, as well as the Department of Higher Education and Training in South Africa to understand the factors to be considered for guiding the adoption of cloud-cybersecurity. The framework will generally support the decision makers to establish a strategic action plan for overall development in the security environment of the higher education sector. The study also bridges the gap of the digital divide in the adoption of cloud-cybersecurity. The empirical findings revealed that there were no significant differences in the adoption perceptions of subjects from rural institutions and the urban-institution.

6.4. Limitations to the Study

The data collected depended on the level of access provided to the researcher. Therefore, the study was limited to a sample size of 441 participants in total. Moreover, the number of lecturers and staff participating were relatively lower than the student participants. The challenge was to look for willing and committed participants as participation was entirely voluntary. Also, the inclusion of other South African universities would have made the results more valid with regards to the adoption of cloud computing cybersecurity in tertiary institutions. Additionally, due to time and

resource constraints, international tertiary institutions were excluded from the scope of this study, which could have improved the results of the study and the researcher's knowledge. Furthermore, the suggested framework was only reviewed for context applicability by the project supervisors and was not practically tested within any of the tertiary institution's environment. The study did not include data collection through the interviews but only questionnaires including closed-ended questions. The external validity can be compromised due to the several errors which may contain the respondent's desire to impress the researcher and results may become biased. The participants may have decided not to participate in the survey for reasons such as lack of interest, motivation and time. This could be for a number of reasons such as question not being relevant to the respondents' situation, the respondents' lack of understanding regarding the question asked, options not suitable to represent the participant's true opinions and completing the question may be of discomfort to the respondents (Erdos, 1970; Mangione, 1995). Incomplete data is a result of unanswered questions that can have an impact on the reliability of the results. The survey of this study had some missing responses. Despite the above-mentioned facts, the findings can be used to justify the subjects' preference, attitude, and experience with cloud computing cybersecurity which will aid in determining the overall impacts of cloud computing cybersecurity adoption within tertiary institutions.

6.5. Recommendations

The recommendations below can be used as strategies to promote the effective use of cloud cybersecurity within tertiary institutions.

a) Recommendations For Tertiary Institutions:

The results established that a cloud cybersecurity system is required to be implemented within tertiary institutions investigated in this study. Therefore, a project life cycle is required to be followed as suggested below.

- It is recommended that each department of the tertiary institutions should adopt cloud computing cybersecurity services by analyzing requirements specific to their department. This includes considering the innovation that the cloud technology offers and measure the competency of the environment of the department. A cost-benefit and risk analysis could be carried out. The benefits and challenges should also be discussed with the cloud services

providers before committing to their services. For clarifying issues, service level agreements must be drawn up.

- It is suggested that a suitable selection of cloud service providers should be made for securing the software as a service, infrastructure as service and platform as a service based on the requirements analyzed. The selection should be made based on the criteria suggested in the adoption framework (relate to Figure 5.1).
- It is suggested that the implementation of the chosen cloud cybersecurity solution should be done on a trial basis as a pilot phase prior to the entire adoption.
- It is recommended that change management should be taken into consideration. The prospective users should be communicated with in terms of the various characteristics of the cloud cybersecurity systems. The top management should in collaboration with the IT management develop plans and strategies that are sufficient to provide for any changes needed by the adoption of cloud cybersecurity.
- It is recommended that tertiary institutions should establish a suitable team for the management of the cloud cybersecurity adoption project. The team would be required to follow the entire cycle of the project management and methodology including the initiation of the project, followed by the planning, execution, monitoring and controlling of the project.
- It is also recommended that the process of managing cloud cybersecurity systems should be monitored and directed by an authorized person equally influencing the users to utilize the cloud cybersecurity.
- Lastly, it is suggested that tertiary institutions should continuously strive to improve the cloud cybersecurity systems employed. This will ensure that the technology addresses the most current requirements of the institution and hence, ensures sustainability. This can be accomplished by ensuring that all the resources required are available to meet the demands of the technology.

b) Recommendations For Management

The results depict that management within the tertiary institutions investigated does not seem to have a clear understanding of the cybersecurity aspects of the cloud technology. This may become a reason for the low usage of cloud cybersecurity as established in the study. Therefore,

recognizing the use of cloud computing in enhancing the education system is a challenge. Hence, the following recommendations are proposed:

- The management should acquire the necessary information from cloud-based companies in collaboration with the IT personnel, that will guide them as decision-makers, on the implementation of the cloud cybersecurity.
- The framework proposed in this study could assist the managers in evaluating the possibility of adoption and enhance their awareness of the factors that influence the adoption.
- It is suggested that the management should provide an equal opportunity for all the stakeholders to meet and discuss the initiative of adopting cloud cybersecurity with adequate planning.
- The management should consider providing suitable educational opportunities for students, staff, and lecturers to gain the technical skills required to use cloud-cybersecurity systems appropriately. Trained librarians should be employed to provide students, lecturers and staff with all the required information on cloud cybersecurity use. Furthermore, capacity building programmes should be set up for equipping students, staff, and lecturers with necessary skills. According to (Alabi, 2016), factors such as age, gender and experience with technology should be taken into consideration when developing the capacity building programmes for improving the adoption and use of cloud cybersecurity.
- Necessary support should be in place for students, lecturers and staff through a help desk centre. It is important that lecturers should be given full support through appropriate pre-service preparation and an on-going state-of-the-art in-service activities and establish links to other universities for additional support. Needs assessments should be conducted for identifying the skills gap and types of training required.
- The management should ensure that individual departments conduct evaluation activities throughout implementation process of cloud cybersecurity programs.
- For new processes of cloud cybersecurity to be successfully introduced and implemented, the management should ensure suitable courses and a methodological training framework be developed for students, staff and lecturers as part of their training and practice program.
- It is suggested that management should make an investment on the necessary infrastructure required to efficiently host the cloud cybersecurity systems within the tertiary institutions.

- The findings discovered a lack of policies on cloud cybersecurity usage. Thus, it is suggested that an institutional policy be established by the management for integrating cloud cybersecurity with day-to-day activities of students, lecturers and staff. The policies should also be integrated with the ICT policies. The policies should contain guidelines to administer the deployment and ethical use of cloud cybersecurity by students, lecturers and staff. The policies should be clear in terms of the standards, strategies, and practices for adoption and use of cloud cybersecurity.
- The management should also consider developing a number of governance and compliance rules for managing the use of cloud cybersecurity. The students, staff, lecturers and IT department should know how, to whom and where to report cybersecurity incidents and share information correctly.

c) Recommendations for Students, Lecturers and Staff

The findings of this study established that there is some awareness regarding cybersecurity among students, staff and lecturers. However, a higher level of awareness was depicted among students than staff and lecturers.

- An awareness should be created for the stakeholders on the importance of adopting cloud cybersecurity. Exposure on the different types of cloud-cybersecurity breaches and attacks should be gained, as the stakeholders does not have an in-depth understanding of the technical aspects of cybersecurity. The awareness can be raised by attending continuous workshops arranged by the respective tertiary institutions.
- There should be a communication and collaboration established between the students and lecturers so they cloud identify and select the cybersecurity tools suitable for tasks related to academic activities.
- The students, staff and lecturers are advised to part take in continuous trainings related to cloud cybersecurity. The trainings are essential for ensuring that technological skills are developed among the students, staff and lecturers and would keep them well-informed. IT staff should be specifically given work shop training in order to take advantage of the technical developments with regard to the cloud cybersecurity system.

- The students, staff and lecturers should familiarise themselves with the challenges and benefits of adopting cloud cybersecurity. This will provide them with an opportunity to evaluate the relative advantages and possibly reduce the level of uncertainty of adoption.
- It is recommended that students, staff and lecturers should secure all their devices including smart phones through cloud cybersecurity as these devices are used as significant tools for teaching, learning and conducting routine activities.
- The lecturers are requested to promote cloud cybersecurity to students through lectures as part of the implementation process. The students are requested to research more about the technology through social media and websites of the respective institutions.
- The staff, lecturers and students are recommended to report any security incident encountered within the network of the tertiary institution to the IT department which is responsible for further investigation.
- It is recommended that students and employees back up all their necessary data to the cloud services provided by the tertiary institutions so that important data can be recovered in case of a cyber-attack.
- Once cloud cybersecurity is implemented on a pilot basis, the students and employees are recommended to give user feedback and reviews about their experiences with the cloud cybersecurity services provisioned.

d) Recommendations for IT Personnel

The findings of the study discovered that IT members have not yet made any efforts in supporting the use of cloud cybersecurity. However, the IT staff members have shown interest towards adopting cloud cybersecurity. The following recommendations are proposed for the adoption and sustainable use of cloud cybersecurity:

- Establish a risk-based method – the IT personnel is recommended to assess the risks of using cloud cybersecurity by identifying its threats, vulnerabilities, and consequences. Thereafter, relevant mitigations, controls and measures should be developed for managing the threats and vulnerabilities at a cost.
- Set priorities – IT department should consider following a graduated approach. Here, the most critical areas should be identified for cloud cybersecurity usage. Critical areas must

be identified based on the level of sensitivity and value it holds to the institution. It should also be recognized that disruption or failure varies between critical departments and assets.

- Build incident response capabilities – incident response capabilities should be established for critical and vital cybersecurity attacks.
- Invest in research on cloud cybersecurity – it is critically recommended that an agenda for promoting advances in cloud cybersecurity and related fields must be developed. This will aid in developing a knowledgeable cybersecurity work force within tertiary institutions.
- Think out of the box – it is recommended that international cybersecurity standards must be integrated to the fullest to keep up with global trends.
- Stipulate penalties for violating polices and standards – an acceptable use policy should be enforced and require staff and students to acknowledge and sign those polices.

6.6. Further Research Suggestions

The current study expands knowledge on the adoption of cloud-cybersecurity within South African tertiary institutions based on three selected institutions. Although this research has fulfilled its aim and objectives, there are several other areas for further research, given the limitations of the current research. Future research can be conducted based on this study by examining cloud-cybersecurity adoption in different sectors and industries which could provide data for comparison, as it is identified through literature review that a lack of studies in this field prevailed.

However looking at the context of the current study from a geographical dimension, since only three institutions were selected for this study, it may not be suitable to generalise the results to the entire population of the tertiary institutions in South Africa or any other country. Therefore, it can be justified that empirical studies in other tertiary institutions in South Africa and other countries are required, of which the results could also be compared. Another interesting area is to consider the methodological aspects of the current study. The methodology of the current study was limited to only one method for data collection (i.e. structured questionnaires) with a quantitative approach. Therefore, future study can be built on this research by examining cloud-cybersecurity adoption in tertiary institutions through a qualitative approach or mixed method approach. For instance focus groups and interviews can be arranged with managers, lecturers, students and staff in which issues concerning the adoption of cloud-cybersecurity can be discussed and case studies can be

formed. The results from quantitative and qualitative studies can be compared to determine the level of significance each contributes towards the knowledge gap.

Furthermore, it should not be ignored that the factors which influences the adoption of cloud-cybersecurity at a specific phase may change over a period of time. Therefore, the cloud-cybersecurity adoption drivers, challenges, benefits and quality perceptions of the sampled population may also change over time. Thus, it would be of interest to conduct a longitudinal research to address this concern.

A study could also be conducted to determine the success levels of adoption of cloud-cybersecurity within tertiary institutions. This could be based on the same institutions used in this study, or any other institutions which have already adopted the technology. The reason for this is to evaluate the institutions performance post adoption.

It is also a matter of concern that the research model of this study was more focused on the relationships recognized among the constructs of this study. Therefore, the variables contained within are not meant to be comprehensive. This is because they were selected to represent the critical factors possibly influencing the adoption of cloud-cybersecurity in tertiary institutions. This gives room for testing the research study with different theories, such as TOE or DOI frameworks. In this way, the cultural inferences of cloud-cybersecurity adoption, an organisational assessment of the acceptance of cloud-cybersecurity adoption, and governmental role and support towards the cloud-cybersecurity implementation within tertiary institutions could be investigated. This is an interesting area for future research because different countries have different cultural beliefs, different point of views, and laws and relations regarding a specific technology adoption (in this case, cloud-cybersecurity), which could be debated.

The researcher also bears in mind that the current framework developed for cloud-cybersecurity adoption has not been implemented and tested. Therefore, a study could be conducted based on the testing and implementation of the framework within the very same tertiary institutions (i.e. Univen, TVET and Rosebank). In this way, it can be determined how reliable and significant the framework proves to be in the adoption process or how significantly it could enhance the adoption.

A cloud-cybersecurity framework can be developed by merging the NIST cloud computing security framework, NIST cybersecurity framework, and ENISA guidelines. Focus on how

security policies, strategies, and governance influence the adoption of cloud-cybersecurity within tertiary institutions can be investigated.

Lastly, a comparison can be provided between the institutions which are cloud-cybersecurity adopters and non-adopters. It can be determined if the adoption of cloud-cybersecurity causes any significant difference within their operational environment. An investigation can also be conducted to determine the delay of cloud-cybersecurity adoption in South Africa tertiary institutions. Similarly, a comparison of cloud cybersecurity adoption can be made between public and private South African tertiary institutions.

6.7. Concluding Remarks

The study focused on the adoption and use of cloud cybersecurity within the South African tertiary institutions. Although students, staff and lecturers were familiar with cloud cybersecurity, it was not used to a high extent by the students and lecturers in protecting their resources such as lecture notes, examination question papers, marks on e-learning systems, Gmail and social media. The admin and IT staff members at Univen and TVET have not used cloud cybersecurity for securing contents on platforms like ITS. Using cloud cybersecurity as a tool for securing the tertiary institutions operational environment is reasonable since it is designed with cost, resources and effort constraints whereby no in-built infrastructure is required to be set up. The literature reviewed showed that the challenges associated with adopting latest technologies makes it difficult for students, staff and lecturers to interact with the technology. The information gathered using the quantitative method was sufficient enough to answer all the five research questions and address the research gaps pertaining to cybersecurity within tertiary institutions. This study enabled to identify the drivers, challenges and benefits of cloud cybersecurity adoption within Univen, TVET and Rosebank which were previously unidentified. The effects of quality and awareness on adoption of cloud cybersecurity services were considered. Perceptions of the students, lecturers and staff were discussed. It was shown that the students, lecturers, and staff intend to use cloud cybersecurity systems for teaching and learning and work activities which will also improve their security experiences. Effort expectancy, social influence and facilitating conditions were shown to an influence towards adoption decisions. Recommendations were proposed for enhancing the use and adoption of cloud cybersecurity. Limitations of the study were stated, and future research suggestions were also highlighted.

REFERENCES

Adya, M. and Wang, W. (2018) 'A Cloud Update of the DeLone and McLean Model of Information Systems Success', *Journal of Information Technology Management*, 29(3), pp. 23–34.

African Union (2014) *African Union Convention On Cybersecurity And Personal Data Protection*, *Arican Union*. Available at: http://pages.au.int/sites/default/files/en_AU Convention on CyberSecurity Pers Data Protec AUCyC adopted Malabo.pdf (Accessed: 1 February 2018).

AJAYI, V. O. O. (2017) *Primary Sources of Data and Secondary Sources of Data*. Makurdi. doi: 10.13140/RG.2.2.24292.68481.

Akin, O. C., Matthew, F. T. and Comfort, D. (2014) 'The Impact and Challenges of Cloud Computing Adoption on Public Universities in Southwestern Nigeria', *International Journal of Advanced Computer Science and Applications*, 5(8), pp. 13–19. Available at: www.ijacsa.thesai.org (Accessed: 2 March 2018).

Al-Shafi, S. and Weerakkody, V. (2010) 'Factors Affecting E-Governemnt Adoption In The State Of Qatar', in *European and Mediterranean Conference on Information Systems*. Abu Dhabi, UAE, pp. 1–23. doi: 10.1179/204264411X12961227987886.

Alabi, A. O. (2016) *Adoption And Use of Electronic Instructural Media Among Academics In Selected Universities In South West Nigeria*. University of kwaZulu-Natal.

Alarifi, A. (2013) *Assessing and Mitigating Information Security Risk In Saudi Arabia*. University of Wollongon.

Alawadhi, S. and Morris, A. (2009) 'Factors Influencing The Adoption of E-Commerce', *Journal of Softwareoftware*, 4(6), pp. 584–590. doi: 10.4304/jsw.4.6.584-590.

Alharbi, N. (2016) *The role of security and its antecedents in e-government adoption*. Plymouth University.

Alotaibi, S. J. and Wald, M. (2014) 'Discussion and Evaluation of the Updated UTAUT Model in IAMSs', *Journal of Intelligent Computing Research*, 5(1/2), pp. 1–10. Available at: https://eprints.soton.ac.uk/363442/ (Accessed: 4 April 2018).

Alshamaileh, Y. Y. (2013) *An Empirical Investigation of Factors Affecting Cloud Computing Adoption Among SMES in the North East of England*. Newcastle University Business School. Available at: https://theses.ncl.ac.uk/dspace/bitstream/10443/2080/1/Alshamaila 13.pdf.

Alshehri, M. A. (2012) *Using the UTAUT Model to Determine Factors Affecting Acceptance and Use of E-government Services in the Kingdom of Saudi Arabia*. Griffith University. Available at: http://hdl.handle.net/10072/368130 (Accessed: 28 May 2018).

Alvi, M. H. (2016) *A Manual For Selecting sampling Techniques in Research*. Karachi. Available at: https://mpra.ub.uni-muenchen.de/70218/1/MPRA_paper_70218.pdf.

Andreassen, M. and Blakstad, K. M. (2010) *Security in Cloud Computing: A Security Assessment of Cloud Computing Providers for an Online Receipt Storage*. Norwegian University of Science and Technology.

Annie, S. and Michael, H. (2013) *NIST Cloud Computing Standards Roadmap*, *NIST Cloud Computing Standards*. USA. doi: 10.6028/NIST.SP.500-291r2.

Appiahene, P., Yaw, B. and Bombie, C. (2016) 'Cloud Computing Technology Model for Teaching and Learning of ICT', *International Journal of Computer Applications*, 143(5), pp. 22–26. doi: 10.5120/ijca2016910183.

Apulu, I. (2012) 'Developing a Framework for Successful Adoption and Effective Utilisation of ICT by SMEs in Developing Countries: a Case Study of Nigeria', (February), pp. 3–369. Available at: http://wlv.openrepository.com/wlv/handle/2436/249899.

Armerding, P. T. (2014) *Emerging Technology Trends and Policy implications.* Limpopo.

Assefa, S. (2009) *An Information Security Reference Framework E-Learning Management Systems*. University of Johanessburg.

AWS (2017) *Amazon Web Services – NIST Cybersecurity Framework*. Available at: https://d0.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf.

Ayooluwa, P. K. (2016) *Use of Web 2 . 0 Technologies for Teaching and Learning in Selected Federal Universities in Southwest Nigeria*, *University of KwaZulu-Natal*. University of KwaZulu Natal.

Babbie, E. R. (2010) *The practice of social research*. Wadsworth Cengage. Available at: https://openlibrary.org/books/OL24486897M/The_practice_of_social_research (Accessed: 28 May 2018).

Babin, R. and Halilovic, B. (2017) 'Cloud Computing e-Communication Services in the University Environment', *Information Systems Education Journal*, 15(1), pp. 55–67. Available at: http://iscap.info (Accessed: 8 March 2018).

Bacon-Shone, J. (2015) *Introduction to Quantitative Research Methods*, *Graduate School, The University of Hong Kong*. doi: 10.13140/2.1.4466.3040.

Bamiah, M. A. and Brohi, S. N. (2011) 'Exploring the Cloud Deployment and Service Delivery Models', *International Journal of Research and Reviews in Information Sciences*, 1(3), pp. 2046–6439.

Bandara, I., Ioras, F. and Maher, K. (2014) 'Cybersecurity Concerns in E-Learning Education', in *Proceedings of ICERI2014 Conference*. Seville, Spain, pp. 728–734.

Barbara, K. (2012) 'Selecting a Research Approach:Paradigm, Methodology, and Methods', *Doing Social Research A Global Context*, (October), pp. 51–61. Available at: https://www.researchgate.net/profile/Barbara_Kawulich/publication/257944787_Selecting_a_research_approach_Paradigm_methodology_and_methods/links/56166fc308ae37cfe40910fc/Selecting-a-research-approach-Paradigm-methodology-and-methods.pdf (Accessed: 4 June 2018).

Beukman, T. (2005) *Chapter 8 Research Design and Methodology*. University of Pretoria. Available at: https://repository.up.ac.za/bitstream/handle/2263/29307/08chapter8.pdf?sequence=9 (Accessed: 6 June 2018).

Bezemer, C. P. and Zaidman, A. (2010) 'Multi-Tenant SaaS Applications: Maintenance Dream or Nightmare?', in *Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE) on - IWPSE-EVOL '10*. The Netherlands: Software Engineerin Research Group, p. 88. doi: 10.1145/1862372.1862393.

Bhardwaj, A. and Goundar, S. (2018) 'Security Challenges For Cloud-Based Email Infrastructure', *Network Security*, 17(11), pp. 8–15. doi: 10.1016/S1353-4858(17)30094-6.

Bond, J. (2015) *The Evolution To Cloud Computing (How Did We Get Here?)*, *The Enterprise Cloud Blog*. Available at: https://mycloudblog7.wordpress.com/2015/05/29/the-evolution-to-cloud-computing-how-did-we-get-here/ (Accessed: 26 June 2018).

Cao, Y., Bi, X. and Wang, L. (2014) 'A study on user adoption of cloud storage service in china: A revised

unified theory of acceptance and use of technology model', in *Proceedings - 2013 International Conference on Information Science and Cloud Computing Companion, ISCC-C 2013*. IEEE, pp. 287–293. doi: 10.1109/ISCC-C.2013.32.

Carroll, M. (2012) *A Risk and Control Framework for Cloud Computing and Virtualization*. University of South Africa. Available at: http://hufee.meraka.org.za/Hufeesite/staff/the-hufee-group/paula-kotze-1/mariana-carroll-phd-thesis.

Carroll, M., Van Der Merwe, A. and Kotzé, P. (2011) 'Secure Cloud Computing: Benefits, Risks and Controls', in *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*. South Africa: IEEE, pp. 1–9. doi: 10.1109/ISSA.2011.6027519.

Chandna, S., Singh, R. and Akhtar, F. (2014) 'Data Scavenging Threat in Cloud Computing', *International Journal of Advances In Computer Science and Cloud Computing*, 2(2), pp. 17–22.

Chandramouli, R. and Mell, P. (2010) 'State of Security Readiness', *Crossroads*, 16(3), pp. 23–25. doi: 10.1145/1734160.1734168.

Chang, V., Walters, R. J. and Wills, G. (2015) *Delivery and Adoption of Cloud Computing Services in Contemporary Organizations*, *ASASEHPC - Information science Reference*. Available at: https://books.google.co.za/books?id=AWfCCAAAQBAJ&pg=PA190&lpg=PA190&dq=cloud+computing+trends+in+rural+universities+across+the+world&source=bl&ots=n5Qn3ctAqV&sig=segvsidX_dPhRk1uNUBYxEHMMxI&hl=en&sa=X&ved=0ahUKEwjApf-StfPbAhWGL8AKHRhtDF0Q6AEIbTAJ#v=onepag (Accessed: 28 June 2018).

Charif, B. (2014) *Security Concerns on Adoption of Cloud Computing*. Luleå University of Technology.

Chen, Z. and Yoon, J. (2010) 'IT Auditing to Assure a Secure Cloud Computing', in *Proceedings - 2010 6th World Congress on Services,*. IEEE, pp. 253–259. doi: 10.1109/SERVICES.2010.118.

Chibaro, N. (2015) *Adoption of Cloud Pedagogy by Higher Learning Institutions in Southern Africa*. Cape Peninsula University of Technology.

Chow, R. *et al.* (2009) 'Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control', *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 85–90. doi: 10.1145/1655008.1655020.

Christin (2017) *5 Facts on Email Security Threats - Mailbird*, *MailBird*. Available at: https://www.getmailbird.com/5-facts-email-security/ (Accessed: 27 March 2018).

Cieplak, T. and Malec, M. (2014) 'Applications of Cloud Computing Services in Education – Case Study', *Advances in Science and Technology Research Journal*, 8(24), pp. 55–60. doi: 10.12913/22998624/568.

Cloud Security Alliance (2016) 'The Treacherous 12 Cloud Computing Top Threats in 2016', *Security*, (February), pp. 1–34. Available at: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf (Accessed: 26 March 2018).

Collin, W. (2014) *The Importance of Cybersecurity in the Age of the Cloud and Internet of Things*, *Government Technology*. Available at: http://www.govtech.com/security/The-Importance-of-Cybersecurity-in-the-Age-of-the-Cloud-and-Internet-of-Things.html (Accessed: 15 February 2018).

Costello, G., Donnellan, B. and Curley, M. (2013) 'A Theoretical Framework to Develop a Research Agenda for Information Systems Innovation', *Communications of the Association of Information Systems*, 33(33), pp. 443–462. Available at: http://aisel.aisnet.org/cais (Accessed: 3 April 2018).

Creswell, J. W. (2013) *Research Design- Qualitative, Quantitative, and Mixed Methods Approaches*. 3rd editio, *SAGE*. 3rd editio. Lincoln: university of Nebraska. Available at: http://www.ceil-conicet.gov.ar/wp-content/uploads/2015/10/Creswell-Cap-10.pdf (Accessed: 4 June 2018).

Creswell, J. W. (2014) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Fourth edi, *Research Design Qualitative, Quantitative and Mixed Methods Approaches*. Fourth edi. Edited by K. Vicki et al. USA: SAGE Publications Ltd. doi: 10.1007/s13398-014-0173-7.2.

Darus, P., Ruziana Binti, M. R. and Gaminan, N. Z. (2015) 'A Review on Cloud Computing Implementation in Higher Educational Institutions', *International Journal of Scientific Engineering and Applied Science (IJSEAS)*, 1(8), pp. 459–465. Available at: www.ijseas.com (Accessed: 4 March 2018).

DeLone, W. H. and McLean, E. R. (2016) 'Information Systems Success Measurement', *Foundation and Trends in Information Systems*. Boston, 2(1), pp. 1–32. doi: http://dx.doi.org/10.1561/2900000005 Information.

Department of Basic Education (2010) 'Government Gazette Staatskoerant', *Government Gazette*, 583(32963), pp. 1–16. doi: http://dx.doi.org/9771682584003-32963.

Diaby, T. and Bashari Rad, B. (2017) 'Cloud Computing: A Review Of The Concepts and Deployment Models', *I.J. Information Technology and Computer Science Information Technology and Computer Science*, 6(6), pp. 50–58. doi: 10.5815/ijitcs.2017.06.07.

Dinh, H. T. *et al.* (2013) 'A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches', *Wireless Communications and Mobile Computing*, 13(18), pp. 1587–1611. doi: 10.1002/wcm.1203.

Dlamini, I. Z., Taute, B. and Radebe, J. (2011) 'Framework for an African Policy Towards Creating Cybersecurity Awareness', in *proceedings of Southern African Cybersecurity Awareness Workshop*. Gaborone, Botswana: Defence, Peace, Safety and Security Council for Scientific and Industrial Research, pp. 15–31. Available at: https://researchspace.csir.co.za/dspace/handle/10204/5163 (Accessed: 15 February 2018).

Dlamini, Z. and Modise, M. (2012) 'Cybersecurity Awareness Initiatives in South Africa: A Synergy Approach', *7th International Conference on Information Warfare and Security*, p. 10. doi: 10.1007/978-3-8349-4134-3_3.

Doelitzscher, F. H.-U. (2014) *Security Audit Compliance for Cloud Computing*. University of Applied Sciences Furtwangen, Germany. Available at: https://pdfs.semanticscholar.org/260f/5b83e3722981067df648a8fba2ee9e73243f.pdf (Accessed: 20 March 2018).

Duncan, B. and Whittington, M. (2016) 'Cloud Cyber-Security: Empowering the Audit Trail', *International Journal on Advances in Security*, 9(3 & 4), pp. 169–183.

Enisa (2012) 'National Cybersecurity Strategies', *ENISA*, (May), p. 15. doi: 10.2824/3903.

Erl, T. (2013) *Cloud Computing: Concepts, Technology, and Architecture*. Prentice Hall/PearsonPTR. Available at: http://whatiscloud.com/cloud_delivery_models/index (Accessed: 27 January 2018).

Ertaul, L., Singhal, S. and Saldamli, G. (2010) 'Security Challenges in Cloud Computing', in *Security and Management*. Las Vegas, pp. 36–42. doi: 10.1109/CloudCom.2014.171.

Fehling, C. *et al.* (2014) 'Cloud Computing Fundamentals', in *Cloud Computing Patterns*, pp. 21–78. doi: 10.1007/978-3-7091-1568-8_2.

Fellegi, I. (2010) *Survey Methods and Practices*, *Statistics Canada*. Edited by S. Franklin and C. Walker. Canada: Statistic Canada. doi: 12-587-X.

Fink, A. (2016) 'How to Conduct Surveys.', in Tricia, C. K. (ed.) *In How to Conduct Surveys. A Step by Step Guide*. 6th edn. Los Angeles: SAGE Publications Ltd., pp. 67–91. Available at: https://jerosystems.com/2016/rskills4.pdf (Accessed: 6 June 2018).

Fishman, T. D., Clark, C. and Grama, J. L. (2018) *Elevating CyberSecurity on The Higher Education Leadership Agenda*, *Deloitte Insights*. Available at: https://www2.deloitte.com/insights/us/en/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html (Accessed: 19 September 2018).

Flack, C. K. (2016) *IS Success Model for Evaluating Cloud Computing for Small Business Benefit : A Quantitative Study*. Coles College of Business. Available at: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1020&context=dba_etd.

Fowler, F. J. J. (2009) *Survey Research Methods*. 5th edn. USA: SAGE Publications Ltd. Available at: https://books.google.co.za/books?hl=en&lr=&id=CR-MAQAAQBAJ&oi=fnd&pg=PP1&dq=survey+research+design+pdf&ots=KOriIXRTKU&sig=EBlLN6Mofwdy6d1xPpEW4YbqUmg#v=onepage&q&f=false (Accessed: 6 June 2018).

Fumeaux, G. (2016) *Thesis Project Public Software as a Servic- A Business Driven Risk Control*. Linnaeus University.

Galliers, R., Markus, M. L. and Newell, S. (2007) *Exploring Information Systems Research Apporaches: Readings and Reflections*. 1st edn. Edited by R. Galliers. Routledge. Available at: https://books.google.co.za/books/about/Exploring_Information_Systems_Research_A.html?id=9FDuAAAAMAAJ&redir_esc=y (Accessed: 4 June 2018).

Ganesh, E. N. (2016) 'Evaluation of ICT Technology in India between', *IJARIIE*, 2(5), pp. 2395–439. Available at: https://www.researchgate.net/publication/309039700 (Accessed: 26 June 2018).

George, A. . (2015) *Conceptual Framework For The Study of Factors Affecting Teachers' Use of Technology*, *Applied Cognitive Psychology*. University of the Witwatersrand. Available at: http://wiredspace.wits.ac.za/jspui/bitstream/10539/16919/4/04.pdf.

Gie Yong, A. and Pearce, S. (2013) *A Beginner's Guide to Factor Analysis: Focusing on Exploratory Factor Analysis*, *Tutorials in Quantitative Methods for Psychology*. Available at: http://www.tqmp.org/RegularArticles/vol09-2/p079/p079.pdf (Accessed: 19 September 2018).

Gogtay, N. J. and Thatte, U. M. (2017) 'Statistics for Researchers Principles of Correlation Analysis', *Journal of The Association of Physicians of India*, 65(03), pp. 78–81. Available at: http://www.japi.org/march_2017/12_sfr_principles_of_correlation.pdf (Accessed: 21 November 2018).

Goodwin, C. *et al.* (2015) *A Framework for CyberSecurity Information Sharing and Risk reduction*. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVoNh (Accessed: 1 March 2018).

Goran, O. H. (2016) *Cloud Computing Adoption In Unversities: Instrucor's Perceptions*. Near East University.

Gray, J., Grove, S. K. and Sutherland, S. (2016) *Burns and Grove's the Practice of Nursing TResearch : Appraisal, Synthesis, and Generation of Evidence*. 8th edn. Elsevier. Available at:

https://books.google.co.za/books/about/Burns_and_Grove_s_The_Practice_of_Nursin.html?id=oD_UDAAAQBAJ&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=false (Accessed: 28 May 2018).

Grobkopf, H. (2015) *Challenges of Service Interchange in a Cross Cloud SOA Environment*. Linnaeus University.

Grobler *et al.* (2011) 'Cyber Awareness Initiatives in South Africa: A National Perspective', *Proceedings of Southern African Cybersecurity Awareness Workshop (SACSAW)*, 32, pp. 32–41. Available at: https://researchspace.csir.co.za/dspace/bitstream/handle/10204/5164/Grobler2_2011.pdf?sequence=1&isAllowed=y (Accessed: 29 June 2018).

Grobler, M. and Dlamini, Z. (2012) 'Global Cyber Trends a South African Reality', in Paul, C. and Miriam, C. (eds) *IST-Africa Conference 2012*. IIMC International Information Management Corporation, pp. 1–8. Available at: http://researchspace.csir.co.za/dspace/handle/10204/5989.

Habiba, U. *et al.* (2014) 'Cloud Identity Management Security Issues and Solutions: A Taxonomy', *Complex Adaptive Systems Modeling- a springer open journal*, 2(1), pp. 1–37. doi: 10.1186/s40294-014-0005-9.

Haeberlen, T. and Lionel Dupré (2012) *Cloud Computing - Benefits, Risks and Recommendations for Information Security*. Heraklion. Available at: http://www.enisa.europa.eu (Accessed: 29 January 2018).

Hair, J. F. *et al.* (2016) *The Essentials of Business Research Methods*. 3rd edn. New York: Routledge.

Hall, J. (2011) 'Encyclopedia of Survey Research Methods Cross-Sectional Survey Design', *Encyclopedia of Survey Research Methods*. SAGE Publications Ltd. Available at: http://methods.sagepub.com/base/download/ReferenceEntry/encyclopedia-of-survey-research-methods/n120.xml.

Hashemi, S. and Hashemi, S. Y. (2013) 'Cloud Computing for E-Learning with More Emphasis on Security Issues', *international of Computer, Electrical, Automation, Control and Information Engineering*, 7(9), pp. 1023–1028.

Hashim, H. S. and Hassan, Z. Bin (2015) 'Factors That Influence The Users ' Adoption Of Cloud Computing Services At Iraqi Universities : An Empirical Study', 9(August), pp. 379–390.

Hashizume, K. (2013) *A Reference Architecture for Cloud Computing and Its Security Applications*. Florida Atlantic University. Available at: http://gradworks.umi.com/35/71/3571426.html.

Hashizume, K. *et al.* (2013) 'An Analysis of Security Issues For Cloud Computing', *Journal of Internet Services and Applications*, 4(1), pp. 1–13. doi: 10.1186/1869-0238-4-5.

Hayes, B. (2008) 'Cloud computing', *Communications of the ACM*, 51(7), p. 9. doi: 10.1145/1364782.1364786.

HCL Technolgies (2015) 'What is Cloud Adoption?', *HCL Technolgies Q&A*, May. Available at: https://www.hcltech.com/search/apachesolr_search/what is cloud adoption (Accessed: 25 February 2018).

Heiser, J. and Nicolett, M. (2008) 'Assessing the Security Risks of Cloud Computing', *Gartner Inc*, (June), pp. 1–6. doi: G00157782.

Hendrik, K. (2015) *Australian Universities Driving Innovation with the Cloud*, *Crucial Broadcast*. Available at: https://www.crucial.com.au/blog/2015/01/22/australian-universities-driving-innovation-with-the-

cloud/ (Accessed: 4 March 2018).

Hoehl, M. (2015) *Proposal for Standard Cloud Computing Security SLAs - Key Metrics for Safeguarding Confidential Data in the Cloud*.

Hossain Masud, A. and Huang, X. (2013) 'M-learning Architecture for Cloud-based Higher Education System of Bangladesh', *www.mc-journal.org Mobile Computing*, 2(4). Available at: https://researchoutput.csu.edu.au/ws/portalfiles/portal/8874184 (Accessed: 28 June 2018).

Hulme, G. V (2011) *Cloud Passage Aims To Ease Cloud Server Security Management*, *CSO*. Available at: https://www.csoonline.com/article/2126687/data-protection/cloudpassage-aims-to-ease-cloud-server-security-management.html (Accessed: 29 January 2018).

IBM (2009) *IBM News room - 2009-11-04 IBM Advances Cloud Computing in Education; Unveils IBM Cloud Academy - United States*. United states. Available at: https://www-03.ibm.com/press/us/en/pressrelease/28749.wss (Accessed: 15 February 2018).

IBM (2012) *Applying The Cloud in Education- An Innovative Approach to IT*. Netherlands.

Ibrahim, A. S. (2014) *Securing the Virtual Infrastructure in the IaaS Cloud Computing Model*. Swineburne University of Technolgy.

Introna, N. (2015) *A Cloud Computing Adoption Framework for Financial Service Institutions in South Africa*. University of Fort Hare. Available at: http://libdspace.ufh.ac.za/bitstream/handle/20.500.11837/801/NicoletteIntrona_Masters_Complete_v5_Corrections_FINAL_Leather Binding.pdf?sequence=1&isAllowed=y (Accessed: 28 May 2018).

Iqbal, S. *et al.* (2016) 'Service Delivery Models of Cloud Computing: Security Issues and Open Challenges', *Security and Communication Networks*, 9(17), pp. 4726–4750. doi: 10.1002/sec.1585.

Jacob, A. T. T. (2007) *An Approach For The Implementation Of Technology Education In Schools In The North West province*. North-West University. Available at: http://dspace.nwu.ac.za/bitstream/handle/10394/13476/Tholo_Jacob Adam Thabo Chapter 4.pdf?sequence=5 (Accessed: 6 June 2018).

Jaeger, T. and Schiffman, J. (2010) 'Outlook: Cloudy With a Chance of Security Challenges and Improvements', *IEEE Security and Privacy*, 8(1), pp. 77–80. doi: 10.1109/MSP.2010.45.

Jain, S. and Angural, V. (2017) 'Use of Cronbach's Alpha in Dental Research', *Medico Research Chronicles*. Available at: http://www.medrech.com/sites/default/files/articles/321 USE OF CRONBACH%27S ALPHA .pdf (Accessed: 17 November 2018).

Jamkhedkar, P. *et al.* (2013) 'A Framework for Realizing Security on Demand in Cloud Computing', in *Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom*. USA: Princeton, pp. 371–378. doi: 10.1109/CloudCom.2013.55.

Jaquire, V. J. (2015) *A Best Practice Strategy Framework for Developing Countries to Secure Cyberspace*. University of Johannesburg.

Jensen, M. *et al.* (2012) 'On Technical Security Issues in Cloud Computing', in *CLOUD 2009 - 2009 IEEE International Conference on Cloud Computing*. Banglore, India: IEEE, pp. 109–116. doi: 10.1109/CLOUD.2009.60.

Johal, N. (2015) *Higher Education Won ' t Be Able To Resist The Cloud Much Longer*, *The Evolllution*. Available at: https://evolllution.com/revenue-streams/market_opportunities/higher-education-wont-

be-able-to-resist-the-cloud-much-longer/ (Accessed: 15 February 2018).

Jokonya, O. (2014) *A Framework to Assist Organisations With Information Technology Adoption Governance*, *CloudCom*. University of South Africa.

Ju, J. *et al.* (2010) 'Research on Key Technology in SaaS', in *2010 International Conference on Intelligent Computing and Cognitive Informatics*. IEEE, pp. 384–387. doi: 10.1109/ICICCI.2010.120.

Kaiser, H. . (1974) 'An Index of Factorial Simplicity', *Psychometrika*, 39, pp. 31–36.

Kajiyama, T. (2012) *Cloud Computing Security: How Risks and Threats are Affecting Cloud Adoption Decisions*. San Diego State University. Available at: http://sdsu-dspace.calstate.edu/handle/10211.10/3522.

Kandukuri, B. R., Ramakrishna, P. and Rakshit, A. (2009) 'Cloud Security Issues', in *2009 IEEE International Conference on Services Computing*. IEEE, pp. 517–520. doi: 10.1109/SCC.2009.84.

Karamete, A. (2015) 'Computer education and instructional technology teacher trainees ' opinions about cloud computing technology', *Educational Research and Reviews*, 10(14), pp. 2043–2050. doi: 10.5897/ERR2015.2297.

Karim, F. and Rampersad, G. (2017) 'Cloud Computing in Education in Developing Countries', *Computer and Information Science*, 10(2), pp. 87–96. doi: 10.5539/cis.v10n2p87.

Karnwal, T., Sivakumar, T. and Aghila, G. (2011) 'Cloud Services in Different Cloud Deployment Models: An Overview', *International Journal of Computer Applications*, 34(8), pp. 975–8887. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.259.1377&rep=rep1&type=pdf (Accessed: 23 January 2018).

Kavitha, K. (2014) 'Study on Cloud Computing Model and its Benefits, Challenges', *International Journal of Innovative Research in Computer and Communication Engineering*, 2(1), pp. 2423–2431. Available at: www.ijircce.com (Accessed: 23 January 2018).

Ke, X. *et al.* (2009) 'Mobile Mashup: Architecture, Challenges and Suggestions', in *Proceedings - International Conference on Management and Service Science*. IEEE, pp. 1–4. doi: 10.1109/ICMSS.2009.5301595.

Keene, C. (2009) *The Keene View on Cloud Computing*. Available at: http://www.keeneview.com/2009/ (Accessed: 28 January 2018).

Khalil, I., Khreishah, A. and Azeem, M. (2014) 'Cloud Computing Security: A Survey', *Computers*, 3(1), pp. 1–35. doi: 10.3390/computers3010001.

Khan, N. and Al-Yasiri, A. (2015) 'Framework for Cloud Computing Adoption: A Roadmap for Smes to Cloud Migration', *International Journal on Cloud Computing: Services and Architecture*, 5(5/6), pp. 01-15. doi: 10.5121/ijccsa.2015.5601.

Khan, N. and Al-Yasiri, A. (2016) 'Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework', in *Procedia Computer Science*, pp. 485–490. doi: 10.1016/j.procs.2016.08.075.

Kimberlin, C. L. and Winterstein, A. G. (2008) 'Validity and Reliability of Measurement Instruments Used in Research', *American Journal of Health-System Pharmacy*, 65(23), pp. 2276–2284. doi: 10.2146/ajhp070364.

Knorr, E. and Gruman, G. (2017) *What Is Cloud Computing? Everything You Need To Know Now*,

Inforworld. Available at: https://www.infoworld.com/article/2683784/cloud-computing/what-is-cloud-computing.html (Accessed: 15 February 2018).

Kok, G. (2010) 'Cloud Computing & Confidentiality', *Capegemini: University og Twente*, p. 11.

Krutz, R. L. and Vines, R. D. (2010) *Cloud security: A Comprehensive Guide To Secure Cloud Computing*. 2nd edn. Indianapolis: Wiley Pub. doi: 10.1017/CBO9781107415324.004.

Kshetri, N. K. (2010) *Cloud Computing in Developing Economies*, *IEEE Computer*. Available at: http://www.ieee.org/ (Accessed: 21 August 2018).

Kumar, G. and Chelikani, A. (2011) 'Analysis of Security Issues in Cloud Based E-Learning', *Security Management*, pp. 1–74.

Kumar, M. (2013) *Source of Data in Research*, *slideshare*. Available at: https://www.slideshare.net/manukumarkm/source-of-data-in-research (Accessed: 14 June 2018).

Kumari, S. (2016) *Challenges of Identity and Access Management in the Cloud*, *Sysfore Blog*. Available at: http://blog.sysfore.com/challenges-of-identity-and-access-management-in-the-cloud/ (Accessed: 14 March 2018).

Lee, K. R. and Chavannes, R. de (2013) *Impacts of Information Technology on Society in the New Century*, *StudyMode Research*. Available at: https://www.zurich.ibm.com/pdf/news/Konsbruck.pdf (Accessed: 15 February 2018).

Leedy, P. D. and Ormrod, J. E. (2013) *Practical Research: Planning and Design*. 10nth edn. Emerita: Pearson. Available at: https://books.google.co.za/books/about/Practical_Research.html?id=YWckygAACAAJ (Accessed: 13 June 2018).

Lester, C. M. (2017) *Be Prepared: Cybersecurity for Higher Education*, *Mimecast*. Available at: https://www.mimecast.com/blog/2017/11/be-prepared-cyber-security-for-higher-education/ (Accessed: 31 March 2018).

Lian, J. (2017) 'Establishing a Cloud Computing Success Model for Hospitals in Taiwan', *Journal of Health care*, 54, pp. 1–6. doi: 10.1177/0046958016685836.

Linington, D. (2014) *Microsoft Brings Tech to the Classroom With TV White Space*, *IT News Africa*. Available at: http://www.itnewsafrica.com/2014/06/microsoft-brings-tech-to-the-classroom-with-tv-white-space/ (Accessed: 28 June 2018).

Liya, X. (2014) *Readiness Assessment of Cloud-Computing Adoption within a Provincial Government of South Africa*, *4th International Conference on Design, Development & Research*. University of Western Cape.

Loanzon, E. (2014a) 'A Proposed Road Map for Cybersecurity in Cloud Computing at Portland State University', in *Planning and Roadmapping Technological Innovations: Cases and Tools*. Springer, Cham, pp. 177–213. doi: 10.1007/978-3-319-02973-3.

Loanzon, E. (2014b) *Planning and Roadmapping Technological Innovations*. Edited by R. T. Tugrul U. Daim, Melinda Pizarro. USA: Springer Science+Business Media. doi: 10.1007/978-3-319-02973-3.

Lwoga, E. (2012) 'Making Learning and Web 2.0 Technologies Work for Higher Learning Institutions in Africa', *Campus-Wide Information Systems*, 29(2), pp. 90–107. doi: 10.1108/10650741211212359.

Maluleka, S. M. (2014) *A Framework for Cloud Computing Adoption in South African Public Sector: A Case of Department of Social Development*. Tshawane University of Technology.

Manyando, O. (2013) *Technologies and Business Value of Cloud Computing : Strategy for the Department of Information Processing*. Kemi-Tornio University of applied sciences. Available at: http://www.theseus.fi/bitstream/handle/10024/68177/Manyando_Obyster.pdf;jsessionid=D3BC6AD5F42FF8493B429ABA7C0C30BB?sequence=1.

Masud, A. H. and Huang, X. (2016) 'Strategies and Practice of Cloud-Based Learning Environment Implementation', in Chao, L. (ed.) *Handbook of Research on Cloud-Based STEM Education for Improved Learning Outcomes*. Hershey: PA:IGI Global, pp. 42–63. doi: 10.4018/978-1-4666-9924-3.ch004.

Mather, T., Kumaraswamy, S. and Latif, S. (2009) *Cloud Security and Privacy*. 1st edn. Edited by Loukides Mike. Sebastopol: O'Reilly Inc. doi: 978-0596802769.

Mbebe, T. M. (2017) *Analysing The Developmental Role of ICT In The Case of Bakgoma Community Library*. Univerity of Stellenbosch.

McGillivray, K. (2017) 'A Right Too Far? Requiring Cloud Service Providers To Deliver Adequate Data Security To Consumers', *International Journal of Law and Information Technology*, 25(1), pp. 1–25. doi: 10.1093/ijlit/eaw011.

McMillan, J. H. and Schumacher, S. (2010) *Research in Education : Evidence-Based Inquiry*. 7th edn. USA: Pearson. Available at: https://www.amazon.com/Research-Education-Evidence-Based-Inquiry-7th/dp/0137152396 (Accessed: 28 May 2018).

McMillan, S. (2014) *Research in Education.* Available at: https://www.scribd.com/document/356284977/2010-McMillan-Schumacher-Research-in-Education (Accessed: 28 May 2018).

Mell, P. and Grance, T. (2011) 'The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology', *Nist Special Publication*, 145, p. 7. doi: 10.1136/emj.2010.096966.

Messmer, E. (2011) *Gartner: New security Demands Arising For Virtualization, Cloud Computing*, *Network World*. Available at: https://www.networkworld.com/article/2178628/virtualization/gartner--new-security-demands-arising-for-virtualization--cloud-computing.html (Accessed: 29 January 2018).

Meyer, I. and Gent, P. (2016) *The Status of ICT in South Africa and The Way Forward*. Available at: http://nect.org.za/publications/technical-reports/the-state-of-ict-in-education-in-south-africa/ (Accessed: 26 June 2018).

Microsoft (2015) *South African University Transforms Education Through Move to Cloud and Tablet.*, *Microsoft publication*. Available at: https://www.microsoft.com/empowering-countries/pt-pt/quality-education/south-african-university-transforms-education-through-move-to-cloud-and-tablet/ (Accessed: 28 June 2018).

Moghaddasi, H., Sajjadi, S. and Kamkarhaghighi, M. (2016) 'Reasons in Support of Data Security and Data Security Management as Two Independent Concepts:A New Model.', *The open medical informatics journal*. Bentham Science Publishers, 10, pp. 4–10. doi: 10.2174/1874431101610010004.

Mohajan, H. K. (2017) 'Two Criteria for Good Measurements in Research: Validity and Reliability', *Munich Personal RePEc Archive*, 17(3), pp. 58–82. doi: 10.26458/1746.

Mowbray, M. (2009) 'The Fog over the Grimpen Mire: Cloud Computing and the Law', *SCRIPT-ed*, 6(1),

pp. 1–16. doi: 10.2966/scrip.060109.132.

Mubarak, A. (2014) *Factors that Influence the Adoption of e-Learning An Empirical Study in Kuwait*. Brunel University. Available at: https://bura.brunel.ac.uk/bitstream/2438/11447/1/FulltextThesis.pdf (Accessed: 28 May 2018).

Muijnck-Hughes, J. de (2011) *Data Protection in the Cloud:*, *The Netherlands*. Radbound University Nijmegan. Available at: http://www.ru.nl/ds.

Muijs, D. (2011) *Doing Quantitative Research in Education with SPSS*. 2nd edn. London: Sage Publications. doi: 10.1080/09500790.2011.596379.

Mukundha, C. and Vidyamadhuri, K. (2017) 'Cloud Computing Models : A Survey', *Advances In Computational sciences and technology*, 10(5), pp. 747–761. Available at: http://www.ripublication.com (Accessed: 23 January 2018).

Munir, K. and Sellapan, P. (2013) 'Framework for Secure Cloud Computing', *International Journal on Cloud Computing: Service and Architecture*, 3(2), pp. 21–35. doi: 10.5121/ijccsa.2013.3202.

Muriithi, G. and Kotze, J. (2012) 'Computing in Higher Education: Implications for South African Public Universities', in Koch, A. and Brakel, V. P. . (eds) *14 th Annual Conference on World Wide Wed Applications*. Durban, South Africa: Cape Peninsula University of Technology, pp. 1–25. Available at: http://www.zaw3.co.za.

Murtada, N. A. (2017) *A Design of an Econometric Model for Evaluating the Security in Cloud Computing Environment*. Sudan University of Science and Technology. Available at: http://repository.sustech.edu/bitstream/handle/123456789/18256/A Design of an Econometric model ....pdf?sequence=1 (Accessed: 8 March 2018).

Nedev, S. (2014) *Exploring The Factors Influencing The Adoption of Cloud Computing and The Challenges Faced By The Business*. Sheffield Hallam University.

Neuman, W. L. (2009) *Social Research Methods: Qualitative and Quantitative Approaches*. 7nth edn. Pearson. Available at: https://www.pearson.com/us/higher-education/program/Neuman-Social-Research-Methods-Qualitative-and-Quantitative-Approaches-7th-Edition/PGM74573.html (Accessed: 4 June 2018).

NIST (2016) *Federal Information Security Management Act*. Available at: https://www.nist.gov/programs-projects/federal-information-security-management-act-fisma-implementation-project (Accessed: 29 January 2018).

Noor, T. H. *et al.* (2013) 'Trust Management of Services in Cloud Environments: Obstacles and Solutions', *ACM Computing Surveys*, 0(0), pp. 1–35. doi: 10.1145/2522968.2522980.

Nunnally, J. and Bernstein, I. (1994) *Psychometric Theory*, *McGraw-Hill, New York*. McGraw-Hill. doi: 10.1007/978-1-4020-9173-5_8.

Nyembezi, N. (2014) *Determinants Of Cloud Computing: Adoption And Application By High School Learners*. University of Fort Hare.

Nyoni, T. B. (2014) 'Towards a Framework for Enhancing User Trust in Cloud Computing'.

Odeh, M., Garcia-Perez, A. and Warwick, K. (2017) 'Cloud Computing Adoption at Higher Education Institutions in Developing Countries: A Qualitative Investigation of Main Enablers and Barriers', *International Journal of Information and Education Technology*, 7(12), pp. 921–927. doi:

10.18178/ijiet.2017.7.12.996.

Odunaike, S., Olugbara, O. and Ojo, S. (2012) 'Using Cloud Computing to Mitigate Rural E-Learning Sustainability and Challenges', *Proceedings of the World Congress on Engineering and Computer Science*, 1(10), pp. 24–26.

OECD (2016) *Innovating Education and Educating for Innovation - The Power of Digital Technologies and Skills*, *Educational Research and Innovation*. Paris: OECD Publishing. doi: http://dx.doi.org/10.1787/9789264265097-en.

Okai, S. *et al.* (2014) 'Cloud Computing Adoption Model for Universities To Increase ICT Proficiency', *SAGE Open*, 4(3), pp. 1–10. doi: 10.1177/2158244014546461.

Olanrewaju, R. F. *et al.* (2017) 'Adoption of Cloud Computing in Higher Learning Institutions: A Systematic Review', *Indian Journal of Science and Technology*, 10(9), p. 19. Available at: http://www.indjst.org/index.php/indjst/article/view/117641/82024 (Accessed: 4 March 2018).

Oleshchuk, V. A. and Koien, G. M. (2011) 'Security and Privacy In The Cloud a Long-Term View', in *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011*. Chennai, India: IEEE, pp. 1–5. doi: 10.1109/WIRELESSVITAE.2011.5940876.

Olive, C. (2011) 'Cloud Computing Characteristics Are Key', *General Physics Corporation*. Available at: www.gpworldwide.com (Accessed: 15 January 2018).

de Oliveira, L. R. *et al.* (2013) 'Adoption Analysis of Cloud Computing Services', *African Journal of …*, 7(24), pp. 2362–2374. doi: 10.5897/AJBM12.1333.

Owens, D. (2010) 'Securing Elasticity in the Cloud', *Communications of the ACM*. ACM, 53(6), p. 46. doi: 10.1145/1743546.1743565.

Owens, L. K. (2002) *Survey Research Design*. Chicago. Available at: https://www.researchgate.net/publication/253282490_INTRODUCTION_TO_SURVEY_RESEARCH_DESIGN?enrichId=rgreq-44fd4517c66c8e0318983ca7dc6c1d48-XXX&enrichSource=Y292ZXJQYWdlOzI1MzI4MjQ5MDtBUzoxNjAyMTAxMTkzMDcyNjRAMTQxNTIwODQ3NzAzNg%3D%3D&el=1_x_2&_esc=publicati.

Pardeshi, V. H. (2014) 'Cloud Computing for Higher Education Institutes: Architecture, Strategy and Recommendations for Effective Adaptation', *Procedia Economics and Finance*. Elsevier B.V., 11(14), pp. 589–599. doi: 10.1016/S2212-5671(14)00224-X.

Parekh, D. H. and Sridaran, R. (2013) 'An Analysis of Security Challenges in Cloud Computing', *IJACSA-International Journal of Advanced Computer Science and Applications*, 4(1), pp. 38–46. Available at: www.ijacsa.thesai.org (Accessed: 14 March 2018).

Patala, N. N. (2017) *The Impact of Cloud Computing Usage On Educational Institutions: a Case Study on University of Venda*. Thohoyandou.

Patel, S. (2015) 'The Research Paradigm - Methodology, Epistomology and Ontology - Explained in Simple Language', *salmapatel.co.uk*. Available at: http://salmapatel.co.uk/academia/the-research-paradigm-methodology-epistemology-and-ontology-explained-in-simple-language (Accessed: 4 June 2018).

Pauline, W. W. (2014) *Adoption of Cloud Computing In Medium and High Tech Industries in Kenya*. University of Nairobi.

Pearson, S. (2012) 'Privacy, Security and Trust in Cloud Computing', *Springer*, (6), pp. 1–58. doi: 10.1007/978-1-4471-4189-1.

Pearson, S. and Yee, G. (2013) *Privacy and Security for Cloud Computing*. Edited by S. Pearson and G. Yee. London: Springer London (Computer Communications and Networks). doi: 10.1007/978-1-4471-4189-1.

Peersman, G. (2014) *Overview: Data Collection and Analysis Methods in Impact Evaluation*, *Methodological Briefs: Impact Evaluation 10*. Florence. Available at: https://www.unicef-irc.org/publications/pdf/brief_10_data_collection_analysis_eng.pdf (Accessed: 14 June 2018).

Perumal, T. (2014) 'Research Methodology', *Course Material*, Chapter 8(Leedy 1993), pp. 87–104. doi: http://dx.doi.org/10.5210/fm.v8i1.1023.

Phillips, B. (2007) 'A Theoretical Framework for Information Systems Portfolio Management A Theoretical Framework for Information Systems Portfolio Management', in *Americas Conference on Information Systems (AMCIS)*. Association for Information Systems AIS Electronic Library (AISeL), pp. 1–7. Available at: http://aisel.aisnet.org/amcis2007 (Accessed: 3 April 2018).

Polit, D. F. and Beck, C. T. (2016) *Resource Manual for Nursing Research: Generating and Assessing Evidence for Nursing Practice*. 10nth edn, *Journal of Chemical Information and Modeling*. 10nth edn. LWW. doi: 10.1017/CBO9781107415324.004.

Ragnet, F. and Leach, C. (2010) *Can You Trust the Cloud ? A Practical Guide to the Opportunities and Challenges of the Document 3 . 0 Era*, *Cloud Computing White Paper, Xerox*. Available at: http://www.officeproductnews.net/sites/default/files/XeroxWP_3.pdf (Accessed: 15 February 2018).

Ramagoffu, M. (2012) *The Impact of Network Related Factors on Internet Based Technology in South Africa: A Cloud Computing Perspective*, *Univerity of Pretoria*. University of Pretoria. Available at: https://scholar.google.com.br/scholar?start=440&q=%22Cloud+Computing%22+%22Cloud+Services%22+%22Cloud+Interoperability%22+%22Cloud+Migration%22+OR+%22legacy-to-cloud+migration%22+OR+%22Cost%22+OR+%22Return+of+investiment%22+OR+%22ROI%22+OR+%22Cost-benefit.

Raman, A. *et al.* (2016) *CyberSecurity in Higher Education: The Changing Threat Landscape - EY Consulting*, *EY technologies blog*. Available at: https://consulting.ey.com/cybersecurity-in-higher-education-the-changing-threat-landscape/ (Accessed: 31 March 2018).

Ramgovind, S., Eloff, M. and Smith, E. (2010) 'The Management of Security in Cloud Computing', *Information Security for South Africa (ISSA), 2010*, pp. 1–7. doi: 10.1109/ISSA.2010.5588290.

Rammutloa, M. W. (2017) *Application of the Delone and McLean's Model To Asses the Effectives of an Intranet In and Open Distance Learning Library*. Stellenbosch University.

Ranjith, P., Priya, C. and Shalini, K. (2012) 'On Covert Channels Between Virtual Machines', *Journal in Computer Virology*. Springer-Verlag, 8(3), pp. 85–97. doi: 10.1007/s11416-012-0168-x.

Rensburg, S. J. Van (2016) *The Year Information and Communication and Technology Services Got Flipped- 2016 Annual Report*. Cape Town. Available at: http://www.icts.uct.ac.za/sites/default/files/image_tool/images/286/UCT - ICTS Report 2016 - SJvR.PDF (Accessed: 27 June 2018).

Richardson, M. and Gajewski, B. (2003) 'Archaeological Sampling Strategies', *Journal of Statistics Education*, 11(1). doi: 10.1080/10691898.2003.11910693.

Ristenpart, T. *et al.* (2009) 'Hey, You, Get Off of My Cloud: Exploring Information Leakage In Third-Party Compute Clouds', in *Proceedings of the 16th ACM conference on Computer and communications security*. New York, USA: ACM Press, pp. 199–212. doi: 10.1145/1653662.1653687.

Ristov, S. *et al.* (2011) 'Business Continuity Challenges in Cloud Computing', *ICT Innovations 2011 Web Proceedings*, pp. 149–157. Available at: http://proceedings.ictinnovations.org/attachment/paper/238/business-continuity-challenges-in-cloud-computing.pdf (Accessed: 22 March 2018).

Rittinghouse, J. and Ransome, J. (2009) *Cloud computing Implementation, Management, and Security*. 1st edn, *CRC Press*. 1st edn. Taylor and Francis Group. Available at: http://books.google.com/books?hl=en&lr=&id=YRIeASgVUJoC&oi=fnd&pg=PP1&dq=Cloud+Computing.+Implementation+,+Management+and+Security&ots=z6vLsbjo0O&sig=2K3Bdu6dM3NLaEMYNAXXfsxDPyQ.

Roberts, S., Garnett, P. and Chandra, R. (2015) *Connecting Africa Using the TV White Spaces : From Research to Real World Deployments*, *Lanman*. Redmond, WA, USA. doi: 10.1109/LANMAN.2015.7114729.

Romiszowski, A. (2013) *Implementing Cloud-Based e-Learning Systems: Potential Benefits and Practical Results*. USA. Available at: http://oasis.col.org/bitstream/handle/11599/1931/2013_Romiszowski_Cloudbased.pdf?sequence=1 (Accessed: 11 August 2018).

Roscorla, T. (2016) *8 Cybersecurity Challenges Facing Higher Education*, *Center for Digital Education*. Available at: http://www.centerdigitaled.com/higher-ed/8-Cybersecurity-Challenges-Facing-Higher-Education.html (Accessed: 15 February 2018).

Rossi, B. (2015) *How To Solve The Five Biggest Email Security Problems*, *Information Age*. Available at: http://www.information-age.com/how-solve-five-biggest-email-security-problems-123460017/ (Accessed: 27 March 2018).

Ryoo, J. *et al.* (2014) 'Cloud Security Auditing: Challenges and Emerging Approaches', *IEEE Security and Privacy*, 12(6), pp. 68–74. doi: 10.1109/MSP.2013.132.

Sabahi, F. (2011) 'Cloud Computing Security Threats and Responses', in *2011 IEEE 3rd International Conference on Communication Software and Networks*. Xi'an, China: IEEE, pp. 245–249. doi: 10.1109/ICCSN.2011.6014715.

Sabi, H. M. *et al.* (2016) 'Conceptualizing a model for adoption of cloud computing in education', *International Journal of Information Management*. Pergamon, 36(2), pp. 183–191. doi: 10.1016/j.ijinfomgt.2015.11.010.

Salauddin, D. (2015) *A study on Cloud Computing Adopton in Small and Medium Enterprises*. Malmo, Hogskola. Available at: https://dspace.mah.se/handle/2043/19738.

Salazar, D. (2016) *Cloud Security Framework Audit Methods*, *SANS Institute InfoSec Reading Room*. Available at: https://www.sans.org/reading-room/whitepapers/cloud/cloud-security-framework-audit-methods-36922 (Accessed: 18 March 2018).

Salemink, K., Strijker, D. and Bosworth, G. (2017) 'Rural Development In The Digital Age: A systematic Literature Review on Unequal ICT Availability, Adoption, and Use in Rural Areas', *Journal of Rural Studies*, 54, pp. 360–371. doi: 10.1016/j.jrurstud.2015.09.001.

Schubert, L. and Jeffery, K. (2012) 'Advances in Clouds Research in Future Cloud Computing', *European Commission, the Cloud Expert Group*, p. 84. doi: http://cordis.europa.eu/fp7/ict/ssai/docs/future-cc-2may-finalreport-experts.pdf.

Schyff, K. van Der (2014) *Cloud Information Security : A Higher Education Perspective*. Rhodes University.

Scotland, J. (2012) 'Exploring the Philosophical Underpinnings of Research: Relating Ontology and Epistemology To The Methodology and Methods of The Scientific, Interpretive, and Critical Research Paradigms', *English Language Teaching*, 5(9), pp. 9–16. doi: 10.5539/elt.v5n9p9.

Seeburn, kris (2016) *Auditing Cloud Security: Challenges and Ideas*, *LinkedIn*. Available at: https://www.linkedin.com/pulse/auditing-cloud-security-challenges-ideas-kris-seeburn (Accessed: 20 March 2018).

Sensinye, N. (2018) *Understanding the Cloud's Value for South Africa*, *IT News Africa*. Available at: http://www.itnewsafrica.com/2018/05/understanding-the-clouds-value-for-south-africa/ (Accessed: 26 June 2018).

Shahzad, A., Golamdin, A. G. and Ismail, N. A. (2014) 'Opportunity and Challenges Using The Cloud Computing In The Case Of Malaysian Higher Education Institutions', in *Proceedings of 6th Annual American Business Research Conference*. New York, USA: ResearchGate, pp. 9–19.

Shana, Z. and Abulibdeh, E. (2017) 'Cloud Computing Issues For Higher Education: Theory of Acceptance Model', *International Journal of Emerging Technologies in Learning (iJET)*, 12(11), pp. 168–184. doi: 10.3991/ijet.v12.i11.7473.

Siyaboni, J. L. (2012) *Factors Influencing Cloud Computing Readiness In Small and Medium Enterprises*. Tshwane University of Technology.

Sriram, I. and Khajeh-Hosseini, A. (2010) 'Research Agenda in Cloud Technologies', *1st ACM Symposium on Cloud Computing, SOCC*, cs.DC, pp. 1–11. doi: 10.1016/j.dss.2010.12.006.

Stephanie (2017) *Internal Validity: Definition and Examples*, *Statistics How To*. Available at: http://www.statisticshowto.com/internal-validity/ (Accessed: 23 June 2018).

Stine, K. and Scholl, M. (2010) 'E-mail Security. An overview of Threats And Safeguards', *Journal of AHIMA*. American Health Information Management Association, 81(4), p. 28–30; quiz 31.

Straub, D., Boudreau, M.-C. and Gefen, D. (2004) 'Validation Guidelines for IS Positivist', *Communications of the Association for Information Systems*, 13(24), pp. 380–427. doi: Article.

Subashini, S. and Kavitha, V. (2011) 'A Survey On Security Issues In Service Delivery Models Of Cloud Computing', *Journal of Network and Computer Applications*, pp. 1–11. doi: 10.1016/j.jnca.2010.07.006.

Subramanian, S. and Seshasaayee, A. (2014) 'Review & Proposal for a Cloud based Framework for Indian Higher Education', *International Journal of Engineering and Computer Science*, 3(1), pp. 3689–3694.

Suhendra, E. S., Hermana, B. and Sugiharto, T. (2009) 'Behavioral Analysis of Information Technology Acceptance in Indonesia Small Entreprises', *Framework*, (May 2014), pp. 1–13.

Suman, A., Mathur, K. and Dhulla, T. V (2014) 'Factors Influencing Professionals ' Decision for Cloud Computing Adoption', 2(4), pp. 397–401.

Sweeney, B. (2015) *Social Engineering: How an Email Becomes a Cyber Threat | SecurityWeek.Com*, *Security Week - internet and enterprise security news, insights and analysis.* Available at:

https://www.securityweek.com/social-engineering-how-email-becomes-cyber-threat (Accessed: 28 March 2018).

Taber, K. S. (2017) 'The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education', *Research in Science Education*, pp. 1–24. doi: 10.1007/s11165-016-9602-2.

Tate, A. R. (2014) *Five Ways Cloud is Enhancing Higher Education - Cloud Computing News*, *IBM*. Available at: https://www.ibm.com/blogs/cloud-computing/2014/08/five-ways-cloud-is-enhancing-higher-education/ (Accessed: 2 March 2018).

Thalmann, S. *et al.* (2012) 'Challenges In Cross-Organizational Security Management', in *Proceedings of the Annual Hawaii International Conference on System Sciences*. Innsbruck, pp. 5480–5489. doi: 10.1109/HICSS.2012.148.

Tout, S., Sverdlik, W. and Lawver, G. (2009) 'Cloud Computing and its Security in Higher Education', in *The Proceedings of the Information Systems Education Conference*. Washington DC; USA: Eastern Michigan University, pp. 1–5. doi: 10.5176/978-981-08-5837-7_201.

Trope, J. (2014) *Adoption of Cloud Computing By South African Firms : an Institutional Theory and Diffusion of Innovation Theory Perspective*. University of Witwatersrand. Available at: http://wiredspace.wits.ac.za/bitstream/handle/10539/15208/J TROPE_Research Report_ v5 0_FINAL.pdf?sequence=1 (Accessed: 15 February 2018).

Ul Hadia, N., Abdullah, N. and Sentosa, I. (2016) 'An Easy Approach to Exploratory Factor Analysis: Marketing Perspective', *Journal of Educational and Social Research*. doi: 10.5901/jesr.2016.v6n1p215.

University of Limpopo (2014) *The Power of Technology: Unveil of TVWS in Limpopo*, *University of Limpopo Punlication* . Available at: https://www.ul.ac.za/index.php?Entity=c_news&TheS=150 (Accessed: 28 June 2018).

University of Venda (2016) *Univen Strategic Plan 2016-20020*. Thohoyandou. Available at: http://www.univen.ac.za/wp-content/uploads/docs/StrategicPlan2016_2020lowres.pdf (Accessed: 28 June 2018).

Univesity of Fort Hare (2009) *Stragetic Plan 2009-2016: University of Fort Hare*. Available at: http://wvw.ufh.ac.za/files/Strategic Plan 2009_Final_Nov 2009.pdf.

Unwin, T. *et al.* (2010) 'Digital Learning Management Systems in Africa: Myths and Realities', *Open Learning*, 25(1), pp. 5–23. doi: 10.1080/02680510903482033.

Ursachi, G., Horodnic, I. A. and Zait, A. (2015) 'How Reliable are Measurement Scales? External Factors with Indirect Influence on Reliability Estimators', *Procedia Economics and Finance*, 20, pp. 679–686. doi: 10.1016/S2212-5671(15)00123-9.

Uudhila, J. M. (2016) *Cybersecurity Risk Management and Threat Control Model*. The University of Namibia. Available at: https://repository.unam.edu.na/bitstream/handle/11070/1688/Uudhila_2016.pdf?sequence=1.

Vaishali Pardeshi (2013) 'Architecture and Adoption Model for Cloud in Higher Education: Indian Perspective', in *Proceedings of National Conference on New Horizons in IT*. NCNHIT, pp. 30–34. Available at: http://www.conference.bonfring.org/papers/met_ncnhit2013/ncnhit51.pdf (Accessed: 5 March 2018).

Veeramachaneni, V. K. (2015) 'Security Threat Issues and Countermeasures in Cloud Computing', *International Journal of Engineering Science and Innovative Technology (IJESIT)*, 4(5), pp. 82–93.

Venkatesh, V. *et al.* (2003) 'User Acceptance of Information Technology: Toward a Unified View', *Source: MIS Quarterly*, 27(3), pp. 425–478. doi: 10.2307/30036540.

Viega, J. (2009) 'Cloud Computing And The Common Man', *Computer*. IEEE Computer Society Press, 42(8), pp. 106–108. doi: 10.1109/MC.2009.252.

Whitman, M. R. and Mattord, H. H. (2012) *Principles of Information Security*. Course Technology.

Woodard, P. (2017) *Cybersecurity and Online Privacy Issues for Employee Benefit Plans*, *Butterfiled Schechter*. Available at: https://www.bsllp.com/cyber-security-and-online-privacy-issues-for-employee-benefit-plans (Accessed: 27 March 2018).

Van Wyk, C. (2015) *An Overview of Education Data in South Africa: An Inventory Approach*, *Working Papers*. 19/15. South Africa. Available at: http://0-search.ebscohost.com.wam.seals.ac.za/login.aspx?direct=true&db=edsrep&AN=edsrep.p.sza.wpaper.wpapers252&site=eds-live.

Yaokumah, W. and Amponsah, R. A. (2017) 'Examining the Contributing Factors for Cloud Computing Adoption in a Developing Country', *International Journal of Enterprise Information Systems*. IGI Global, 13(1), pp. 17–37. doi: 10.4018/IJEIS.2017010102.

Yin, R. K. (2006) 'Case Study Reserach - Design and Methods', *Clinical Research*, 2, pp. 8–13. doi: 10.1016/j.jada.2010.09.005.

Zia, T. *et al.* (2013) *Security and Privacy in Communication Networks*. Edited by A. Ozgur and B. et. a. Paolo. Sydney, Australia: Springer. doi: 10.1007/978-3-319-04283-1.

Ziehl, S. (2013) *Social Research Methodology*. Available at: http://splshortcourses.co.za/available-courses/advertised-short-courses-2013/social-research-methodology-generating-information-for-programme-design-evaluation/course-outline-5-days (Accessed: 6 June 2018).

Zissis, D. and Lekkas, D. (2012) 'Addressing cloud computing security issues', *Future Generation Computer Systems*. Elsevier B.V., 28(3), pp. 583–592. doi: 10.1016/j.future.2010.12.006.

ANNEXURE A: ETHICAL CLEARANCE

RESEARCH AND INNOVATION
OFFICE OF THE DIRECTOR

NAME OF RESEARCHER/INVESTIGATOR:
Ms NN Patala

Student No:
11634215

PROJECT TITLE: **Cyber security framework for cloud computing adoption in rural based tertiary institutions.**

PROJECT NO: SMS/18/BIS/01/1403

SUPERVISORS/ CO-RESEARCHERS/ CO-INVESTIGATORS

NAME	INSTITUTION & DEPARTMENT	ROLE
Prof A Kadyamatimba	University of Venda	Supervisor
Mr S Madzvamuse	University of Venda	Co - Supervisor
Ms NN Patala	University of Venda	Investigator – Student

ISSUED BY:
UNIVERSITY OF VENDA, RESEARCH ETHICS COMMITTEE

Date Considered: March 2018
Decision by Ethical Clearance Committee Granted
Signature of Chairperson of the Committee: .....
Name of the Chairperson of the Committee: Senior Prof. G.E. Ekosse

UNIVERSITY OF VENDA
DIRECTOR
RESEARCH AND INNOVATION
2018 -03- 16
Private Bag X5050
Thohoyandou 0950

University of Venda
PRIVATE BAG X5050, THOHOYANDOU, 0950, LIMPOPO PROVINCE, SOUTH AFRICA
TELEPHONE (015) 962 8504/8313 FAX (015) 962 9060
"A quality driven financially sustainable, rural-based Comprehensive University"

ANNEXURE B: INFORMED CONSENT FORM

RESEARCH ETHICS COMMITTEE

UNIVEN Informed Consent

Appendix B

LETTER OF INFORMATION

Title of the Research Study : Cyber Security Framework For Cloud Computing Adoption In Rural Based Tertiary Institutions.

Principal Investigator/s/ researcher : *Patala Najiyabanu Noormohmed, BCOM Honours - Business Information systems.*

Co-Investigator/s/supervisor/s : *Prof A. Kadyamatimba, PHD.*
: Mr S. Madvamuse, Masters.

Brief Introduction and Purpose of the Study : The main purpose of the current research is to investigate the effects of security on cloud computing usage at University of Venda and TVET college and also suggest a cyber security framework for adoption of cloud computing in tertiary institutions.

Outline of the Procedures : The participant is required to read all the questions mentioned in the survey very carefully and if there is any lack of understanding, he or she may consult the researcher with regards. The participant is required to answer each question honestly to the best of his or her ability and understanding. The participant will require an approximate time of 20 minutes to fully complete the survey questionnaire. The questionnaire is expected to be completed individually and no group allotments will be made. The participation in this study is completely voluntary and no individual may be forced.

Risks or Discomforts to the Participant : The current study does not have any present or foreseeable risk that might lead to participant's discomfort. However the participant can withdraw anytime in an occurrence of any discomfort.

Benefits : The researcher is interested in publishing the research which will benefit tertiary institutions including its students, staff and lecturers.

Reason/s why the Participant May Be Withdrawn from the Study: The participant may be withdrawn in terms of non-compliance by not fully completing the questionnaire and not answering all the questions in the survey.

Remuneration : Remuneration of any sort (i.e. monetary or incentives) will not be awarded to the participant.

Costs of the Study : The participant will not be required to cover any costs towards the study.

Confidentiality : The privacy of the participant will be maintained while conducting the study, as no identity information will be collected such as cell phone numbers, ID, student, or staff numbers. The access to questionnaires are only available for use by the researcher and supervisor, therefore no access will be granted to any other third party, unless legally required. All information collected from participants will saved in a file which will be in possession of the researcher only and all the data will be transferred in to the researcher's computer device.

Research-related Injury : I do not take any responsibility of any research-related injury during the course of the completion of survey questionnaires. The researcher will report the issue to the relevant research office. There will be no compensation from the researchers side.

Persons to Contact in the Event of Any Problems or Queries:

(Supervisor and details) Please contact the researcher (tel no.), my supervisor (tel no.) or the University Research Ethics Committee Secretariat on 015 962 9068. Complaints can be reported to the Director: Research and Innovation, Prof GE Ekosse on 015 962 8313 or Georges Ivo.Ekosse@univen.ac.za

General:

Potential participants must be assured that participation is voluntary and the approximate number of participants to be included should be disclosed. A copy of the information letter should be issued to participants. The information letter and consent form must be translated and provided in the primary spoken language of the research population

CONSENT

Statement of Agreement to Participate in the Research Study:

- I hereby confirm that I have been informed by the researcher, (*Patala Najiyabanu Noor Mohmed*), about the nature, conduct, benefits and risks of this study - Research Ethics Clearance Number: _
- I have also received, read and understood the above written information (*Participant Letter of Information*) regarding the study.
- I am aware that the results of the study, including personal details regarding my sex, age, date of birth, initials and diagnosis will be anonymously processed into a study report.
- In view of the requirements of research, I agree that the data collected during this study can be processed in a computerized system by the researcher.
- I may, at any stage, without prejudice, withdraw my consent and participation in the study.
- I have had sufficient opportunity to ask questions and (of my own free will) declare myself prepared to participate in the study.
- I understand that significant new findings developed during the course of this research which may relate to my participation will be made available to me.

Full Name of Participant	Date	Time	Signature
I, ...	.....	.....	.....

(*Patala Najiyabanu Noormohmed*), herewith confirm that the above participant has been fully

Informed about the nature, conduct and risks of the above study.

Full Name of Researcher	Date	Signature
Patala Najiyabanu Noormohmed	August 2018	.....

Full Name of Witness (If applicable)

..... Date ..... Signature.....

ANNEXURE C: QUESTIONNAIRES

STUDENT QUESTIONNAIRE

CYBERSECURITY FRAMEWORK CLOUD COMPUTING FOR ADOPTION IN RURAL BASED TERTIARY INSTITUTIONS

SECTION A: Background Information

For each item below, Please indicate your answer by putting a clear cross (X) in the relevant block (please choose only one response in each question).

1. What is your gender ?	2. What is your age group?
○ Male ○ Female	○ 15-25 ○ 26-35 ○ 36-45 ○ 46 and above
3. What is your race ?	**4. What is your current level of study ?**
○ African/Black ○ Coloured ○ Asian/Indian ○ White ○ Other……, please specify	○ 1st Year ○ 2nd Year ○ 3rd Year ○ 4th Year ○ Honours ○ Masters ○ PhD

SECTION B: Cloud Computing Cyber-Security Usage and Its Drivers

5. Are you knowledgeable of cloud-based cybersecurity services?

○ Yes ○ No

6. Do you have experience of using cloud-based cybersecurity services?

○ Yes ○ No

7. Which cloud computing cybersecurity services and application do you use? (select all that apply)

☐ Microsoft Security (i.e. for Windows and Microsoft Office 365)

☐ Google Apps Security Services (i.e. for Google Drive, G-mail, Google Docs, calendar)

☐ Amazon Web Service for online storage protection (i.e. for Dropbox)

8. In terms of educational contents,

Do you think using cloud cybersecurity features will allow you to:	Yes	No
Securely upload/download assignments from e-learning, email, or social network platforms	○	○
Securely upload/download lecture notes from e-learning, email, or social network platforms	○	○
Securely conduct online tests and exams on e-learning, email, or social network platforms	○	○
Securely carryout class/group discussions on e-learning, email, or social network platforms	○	○
Securely view marks on e-learning, email, or social network platforms	○	○

9. Please rate the following statements that best represents your opinion regarding the usefulness of cloud-cybersecurity in tertiary institutions by putting a Cross (X) on it.

SA=strongly, Agree A=Agree, N-Neutral, D=Disagree, SD=Strongly Disagree.						
	Drivers for cloud computing cybersecurity adoption:- I believe:	SA	A	N	D	SD

D1	Tertiary institutions shall use cloud-based cyber-security services for improving data security and privacy information of students.					
D2	Legal law and regulatory compliance encourages tertiary institutions in using cloud-based cybersecurity services					
D3	The pace of keeping up with latest technology motivates tertiary institutions in using cloud-based cybersecurity services					
D4	Tertiary institutions may use cloud cybersecurity for financial reasons such as reduced budgeting for cost of cyber-breaches					
D5	Tertiary institutions may use cloud cybersecurity for maintaining public reputation such as gaining trust and confidence of students					

SECTION C: Cloud Computing Cyber-Security Issues, Benefits and Quality

10. What according to you are or could be the challenges of using cloud-based cybersecurity services from the items below? (Select all that applies)

CYBERSECURITY CHALLENGES			
☐	Lack of physical control of data and information	☐	Undesirable disclosure of information to law and regulatory bodies.
☐	Harmful activities executed on the network (web/internet)	☐	Lack of security awareness causing cyber-attacks
☐	Information leakage to other cloud cybersecurity service users (Multi-tenancy)	☐	Identity theft and Unauthorized access to my cloud-based applications and study materials
☐	Denial-of-service availability preventing access to my information applications	☐	Information can be lost, deleted, moved or changed.
☐	Compromise of data and information privacy due to its monitoring and tracking by security service providers	☐	Monitoring and tracking of my cloud activities by attackers (Sniffing/spoofing)
☐	My files can be infected with viruses using cloud-based cybersecurity	☐	My device can be hacked while using cloud-based cybersecurity (hacking)

11. What according to you are the benefits of using cloud computing cybersecurity services from the items below? (Select all that applies)

	Benefits of cloud cybersecurity usage for E-learning, email and social network systems: I believe cybersecurity:		
☐	prevents falsification of course assessments	☐	prevents the presenting of a false identity to others
☐	prevents intrusion upon controlled or private conversations	☐	prevents the alteration of date stamps on submitted work
☐	prevents lecturers from gaining access to personal data of students	☐	None

12. Rate the following statements according to the response most suitable to your beliefs regarding the quality of cloud cybersecurity.

SA=strongly, Agree A=Agree, N-Neutral, D=Disagree, SD=Strongly Disagree.

	Quality perceptions of cyber-security services :- I believe:	SA	A	N	D	SD
QP1	Cloud cyber-security is accurate for securing my contents on various platforms such as google drive, emails, dropbox , blackboard (e-learning) etc.					
QP2	Cloud cyber-security is reliable for protecting my personal and educational contents					
QP3	Cloud cybersecurity is relevant for securing my personal and educational contents					

QP4	Cloud cybersecurity services is responsive as I will be informed about security breaches timeously					
QP5	Overall, cloud cyber-security is a success as it increases the value of cloud computing and promotes the adoption of cloud computing					

SECTION D: Cloud-Computing Cybersecurity Perceptions and Awareness

13. Rate the following statements according to the response most suitable to your beliefs regarding the perceptions and level of awareness of cloud cybersecurity.

SA=strongly, Agree A=Agree, N-Neutral, D=Disagree, SD=Strongly Disagree.						
	Performance Expectancy:- I believe:	SA	A	N	D	SD
PE1	Cloud cybersecurity will be useful and convenient in protecting my learning material on blackboard e-learning platform and other learning applications such as emails and social media					
PE2	Using cloud cyber-security will enable me to track any security breaches quickly and efficiently saving my time in managing security of my applications and data					
PE3	Cloud computing cybersecurity processes are less complicated					
	Effort Expectancy:- I believe:					
EE1	Cloud cyber-security service interactions would be clear and understandable					
EE2	It would be easier for me to learn and develop the skills to use cloud cybersecurity features. (i.e. setting passwords and usernames, verifying personal details etc. on the cloud system)					
EE3	It is easy to use cloud cyber-security services					
	Social influence:- I believe					
SS1	People who are important to me and influence my behavior think I should use cloud cyber-security					
SS2	I would use cloud cyber-security if my friends, family or colleagues use it					
SS3	My tertiary institution encourages/supports students to use cloud cyber-security					
	Facilitating conditions:- I believe					
FC1	I have access to the resources necessary to use cloud-based cybersecurity					
FC2	I have the knowledge necessary to use cloud-based cybersecurity					
FC3	Support people will be available for assistance with any difficulties I might encounter while using cloud cybersecurity.					
	Intention of Use					
IU1	Assuming I have access to cloud-cybersecurity services, I intent to use it					
IU	Given that I have access to the cloud-cybersecurity services, I plan to use it.					
	Awareness :					
A1	I am aware that my data stored in cloud-based e-learning systems maintains an up-to-date back-up and recovery facility					
A2	I am aware that cloud cyber-security will prevent unauthorized access to my files					
A3	Overall, I am aware of the potential security threats and their negative consequences of using cloud cybersecurity services.					
A4	Security training and awareness programs should be provided by the institution in order to efficiently use cloud-based cybersecurity for E-learning systems					

LECTURER QUESTIONNAIRE

CYBERSECURITY FRAMEWORK FOR CLOUD COMPUTING ADOPTION IN RURAL BASED TERTIARY INSTITUTIONS

SECTION A: Background Information

For each item below, Please indicate your answer by putting a clear cross (X) in the relevant block (please choose only one response in each question).

1. What is your gender ?	2. What is your age group?
○ Male ○ Female	○ 18-25 ○ 26-35 ○ 36-45 ○ 46 and above
3. What is your race ?	4. What is your teaching position ?
○ African/Black ○ Coloured ○ Asian/Indian ○ White ○ Other……, please specify	○ Teaching Assistant ○ Lecturer ○ Senior lecturer ○ Professor
5. For how long have you been teaching in this field?	6. What faculty or school do you belong to ?
○ Less than 1 year. ○ Between 1 to 5 years. ○ More than 5 years	○ Agriculture ○ Law ○ Education ○ Health ○ Management ○ Mathematical & Natural sciences ○ Human & Social Sciences ○ Environmental sciences

SECTION B: Cloud Computing Cyber-Security Usage and Its Drivers

7. Are you knowledgeable of cloud-based cybersecurity services?

○ Yes ○ No

8. Do you have experience of using cloud-based cybersecurity services?

○ Yes ○ No

9. Which cloud computing cybersecurity services and application do you use? (select all that apply)

☐ Microsoft Security (i.e. for Windows and Microsoft Office 365)
☐ Google Apps Security Services (i.e. for Google Drive, G-mail, Google Docs, calendar)
☐ Amazon Web Service for online storage protection (i.e. for Dropbox)

10. In terms of educational contents,

Do you think using cloud-based cyber-security features will allow you to:	Yes	No
Securely post assignments on e-learning, email, or social network platforms	○	○
Securely post lecture notes from e-learning, email, or social network platforms	○	○
Securely conduct online tests and exams on e-learning, email, or social network platforms	○	○
Securely carry out class and group discussions with students on e-learning, email, or social network platforms	○	○
Securely post marks on e-learning, email, or social network platforms	○	○

11. Please rate the following statements that best represents your opinion regarding the usefulness of cloud-cybersecurity in tertiary institutions by putting a Cross (X) on it.

SA=strongly, Agree A=Agree, N-Neutral, D=Disagree, SD=Strongly Disagree.						
	Drivers for cloud computing cybersecurity adoption:- I believe:	SA	A	N	D	SD
D1	Tertiary institutions shall use cloud-based cyber-security services for improving data security and privacy information of students and lecturers.					
D2	Legal law and regulatory compliance encourages tertiary institutions in using cloud-based cybersecurity services.					
D3	The pace of keeping up with latest technology motivates tertiary institutions in using cloud-based cybersecurity services.					
D4	Tertiary institutions may use cloud cybersecurity for financial reasons such as reduced budgeting for cost of cyber-breaches.					
D5	Tertiary institutions may use cloud cybersecurity for maintaining public reputation such as gaining trust and confidence of students.					

SECTION C: Cloud Computing Cyber-Security Issues, Benefits and Quality

12. Have you ever encountered a cyber-security incident (attack) within your institution?

○ Yes ○ No

13. Have you ever faced any difficulties in securing you educational materials online?

○ Yes ○ No

14. What according to you are or could be the challenges of using cloud-based cybersecurity services from the items below? (Select all that applies)

CYBERSECURITY CHALLENGES			
☐	Lack of physical control of data and information	☐	Undesirable disclosure of information to law and regulatory bodies by my institution.
☐	Harmful activities executed on the network (web/internet)	☐	Lack of security awareness causing cyber-attacks
☐	Information leakage to other cloud cybersecurity service users (Multi-tenancy)	☐	Identity theft and Unauthorized access to my cloud-based applications and teaching materials
☐	Denial-of-service availability preventing access to my information on Blackboard and other applications	☐	Information can be misused, lost, deleted, moved or changed.
☐	Compromise of data and information privacy due to its monitoring and tracking by security service providers	☐	Monitoring and tracking of my cloud activities by attackers (Sniffing/spoofing)
☐	Files can be infected with viruses using cloud-based cybersecurity	☐	Device can be hacked while using cloud-based cybersecurity (hacking)

15. What according to you are the benefits of using cloud computing cybersecurity services from the items below? (Select all that applies)

	Benefits of cloud cybersecurity usage for E-learning, email and social network systems: I believe cybersecurity:		
☐	prevents falsification of course assessments	☐	prevents the presenting of a convincing false identity to others
☐	prevents intrusion upon controlled or private conversations	☐	prevents the alteration of date stamps on submitted work
☐	prevents students from gaining access to personal data of lecturers	☐	None

16. Rate the following statements according to the response most suitable to your beliefs regarding the quality of cloud cybersecurity.

SA=strongly, Agree A=Agree, N-Neutral, D=Disagree, SD=Strongly Disagree.						
	Quality perceptions of cyber-security services :- I believe:	SA	A	N	D	SD
QP1	Cloud cyber-security is reliable and flexible for securing my contents on various platforms such as google drive, emails, dropbox , blackboard (e-learning) etc.					
QP2	Cloud cyber-security is accurate and effective for protecting my personal and educational contents.					
QP3	Cloud cybersecurity is consistent and relevant for securing my personal and educational contents.					
QP4	Cloud cybersecurity services is responsive as I will be informed about security breaches timeously.					
QP5	Overall, cloud cyber-security is a success as it increases the value of cloud computing and promotes the adoption of cloud computing.					
QP6	My tertiary institution has the necessary infrastructure for supporting the system, information and service quality of cyber-security					

SECTION D: Cloud-Computing Cybersecurity Adoption Perceptions and Awareness

17. Rate the following statements according to the response most suitable to your beliefs regarding the perceptions and level of awareness of cloud cybersecurity.

SA=strongly, Agree A=Agree, N-Neutral, D=Disagree, SD=Strongly Disagree.						
	Performance Expectancy:- I believe:	SA	A	N	D	SD
PE1	Cloud cybersecurity will be useful and convenient in protecting teaching material on blackboard e-learning platform and other applications such as emails and social media					
PE2	Using cloud cyber-security will enable me to track any security breaches quickly, efficiently and save my time in managing security of my applications and data					
PE3	Cloud computing cybersecurity processes are less complicated					
	Effort Expectancy:- I believe:					
EE1	Cloud cyber-security service interactions would be clear and understandable					
EE2	It would be easier for me to learn and develop the skills to use cloud cybersecurity features. (i.e. setting passwords and usernames, verifying personal details etc. on the cloud system)					
EE3	It is easy to use cloud cyber-security services					
	Social influence:- I believe					
SS1	People who are important to me and influence my behavior think I should use cloud cyber-security					
SS2	I would use cloud computing cyber-security if my friends and colleagues use it					
SS3	My tertiary institution encourages/supports students to use cloud cyber-security					
	Facilitating conditions:- I believe					
FC1	I have access to the resources necessary to use cloud-based cybersecurity					
FC2	I have the knowledge necessary to use cloud-based cybersecurity					
FC3	IT Support people will be available for assistance with any difficulties I might encounter while using cloud cybersecurity.					
	Intention of Use					

IU1	Assuming I have access to cloud-cybersecurity services, I intent to use it					
IU	Given that I have access to the cloud-cybersecurity services, I plan to use it.					
	Awareness :					
A1	I am aware that my data stored in cloud-based e-learning systems maintains an up-to-date back-up and recovery facility					
A2	I am aware that cloud cyber-security will prevent unauthorized access to my files					
A3	Overall, I am aware of the potential security threats and their negative consequences of using cloud cybersecurity services.					
A4	I am aware of the security training and awareness programs that are provided by various institutions in order to efficiently use cloud-based cybersecurity for E-learning systems					
A5	I am aware of who to contact if I encounter a cyber-security attack within my institution					
A6	I am aware of the websites that provides cyber-security guidance					
A7	I am aware of the value that cybersecurity adds towards adoption of cloud computing					

IT STAFF QUESTIONNAIRE

CYBERSECURITY FRAMEWORK FOR CLOUD COMPUTING ADOPTION IN RURAL BASED TERTIARY INSTITUTIONS

SECTION A: Background Information

For each item below, Please indicate your answer by putting a clear cross (X) in the relevant block (please choose only one response in each question).

1. What is your gender ?	2. What is your age group?
○ Male ○ Female	○ 18-25 ○ 26-35 ○ 36-45 ○ 46 and above
3. What is your race ?	4. What is your experience level working with information technology?
○ African/Black ○ Coloured ○ Asian/Indian ○ White ○ Other……, please specify	○ Less than 1 Year ○ 2-5 Years ○ 6-10 Years ○ More than 10 Years

SECTION B: Cloud Computing Cyber-Security Usage and Its Drivers

5. For each item in this question, please indicate your answer by putting a clear cross (X) on the relevant block

		YES	NO	NOT SURE
5A	Are you knowledgeable of cloud-based cybersecurity services?	○	○	○
5B	Do you have experience of using cloud-based cybersecurity services?	○	○	○
5C	Does your institution have cloud computing cyber-security policies in place for maintaining cyber-attacks?	○	○	○

5D	Does your cloud service provider adhere to any established cloud security framework involving cyber-security controls?	○	○	○
5E	Does your institution and cloud service provider undergo any regular 3rd party audits with established cloud cyber-security frameworks?	○	○	○
5F	Are cyber-security strategies circulated to the employees of your institutions to protect systems from cyber-attacks?	○	○	○

6. Which cloud computing cyber-security services and application do you use? (Select all that apply)

☐ Microsoft Security (i.e. for Windows and Microsoft Office 365)

☐ Google Apps Security Services (i.e. for Google Drive, G-mail, Google Docs, calendar)

☐ Amazon Web Service for online storage protection (i.e. for Dropbox)

☐ None of the Above

7. In terms of your job-related contents,

	Do you think using cloud-based cybersecurity features will allow you to:	YES	NO
7A	Securely send documents and messages through email, or social network platforms	○	○
7B	Securely receive documents and messages through email, or social network platforms	○	○
7C	Securely upload documents and other contents on ITS	○	○
7D	Securely download documents and other contents from ITS	○	○
7E	Securely conduct uninterrupted meetings on online platforms (i.e. video conferencing on skype)	○	○

8. Please rate the following statements that best represents your opinion regarding the usefulness of cloud-cybersecurity in tertiary institutions by putting a Cross (X) on it.

SA=strongly, Agree A=Agree, N-Neutral, D=Disagree, SD=Strongly Disagree.

	Drivers for cloud computing cybersecurity adoption:- I believe:	SA	A	N	D	SD
D1	Tertiary institutions shall use cloud-based cyber-security services for improving data security and privacy information of students, academics and staff.					
D2	Legal law and regulatory compliance encourages tertiary institutions in using cloud-based cybersecurity services.					
D3	The pace of keeping up with latest technology motivates tertiary institutions in using cloud-based cybersecurity services.					
D4	Tertiary institutions may use cloud cybersecurity for financial reasons such as reduced budgeting for cost of cyber-breaches.					
D5	Tertiary institutions may use cloud cybersecurity for maintaining public reputation such as gaining trust and confidence of students, academics and staff.					

SECTION C: Cloud Computing Cyber-Security Issues, Benefits and Quality

9. What according to you are or could be the challenges of using cloud-based cybersecurity services from the items below? (Select all that applies)

CYBERSECURITY CHALLENGES			
☐	Lack of physical control of data and information	☐	Undesirable disclosure of information to law and regulatory bodies.

☐	Harmful activities executed on the network (web/internet)	☐	Lack of security awareness causing cyber-attacks
☐	Information leakage to other cloud cybersecurity service users (Multi-tenancy)	☐	Identity theft and Unauthorized access to my cloud-based applications and study materials
☐	Denial-of-service availability preventing access to my information applications	☐	Information can be lost, deleted, moved or changed.
☐	Compromise of data and information privacy due to its monitoring and tracking by security service providers	☐	Monitoring and tracking of my cloud activities by attackers (Sniffing/spoofing)
☐	Communication security on multiple cloud platforms	☐	Application security on various cloud systems
☐	Files can be infected with malware and viruses using cloud-based cybersecurity	☐	Device can be hacked while using cloud-based cybersecurity (hacking)

10. What according to you are the benefits of using cloud computing cybersecurity services from the items below? (Select all that applies)

	Benefits of cloud cybersecurity usage: I believe cybersecurity:		
☐	Cheaper security costs as data is saved in multiple locations	☐	Standardized interfaces for managed cyber-security services
☐	Provisioning of cyber-security auditing	☐	Increased support for defensive measures when cyber-attack is taking place
☐	Efficient and effective capabilities of incident/attack response.	☐	None of the Above

11. Why do you think cloud computing cyber-security is important in tertiary institutions? (select all that applies).

☐	To prevent Denial-of-service.	☐	To protect against data breaches and data loss.
☐	To eliminate or reduce internal and external malicious threats.	☐	To protect web applications (i.e. office 365)
☐	To preserve integrity of university databases	☐	To ensure privacy of communication
☐	To provide multiple authentication processes which will protect user identity		

12. Rate the following statements according to the response most suitable to your beliefs regarding the quality of cloud cybersecurity.

SA=strongly, Agree A=Agree, N-Neutral, D=Disagree, SD=Strongly Disagree.

	Quality perceptions of cyber-security services :- I believe:	SA	A	N	D	SD
QP1	Cloud computing cyber-security is reliable and flexible for securing my contents on various platforms such as google drive, emails, dropbox , ITS, Library Systems etc.					
QP2	Cloud computing cyber-security is accurate and effective for protecting my personal and job related contents					
QP3	Cloud computing cybersecurity is consistent and relevant for securing my personal and job related contents					
QP4	Cloud computing cybersecurity services is responsive as I will be informed about security breaches timeously					
QP5	Overall, cloud cyber-security is a success as it increases the value of cloud computing and promotes the adoption of cloud computing					

QP6	My tertiary institution has the necessary infrastructure for supporting the system, information and service quality of cyber-security					

13.My institution uses (Select all that applies):

☐	The NIST Cyber-Security Framework	☐	ENISA Cyber-Security Guidelines
☐	Other Cyber-Security Guidelines	☐	Does Not Use any Cyber-Security Framework

SECTION D: Cloud-Computing Cybersecurity Perceptions and Awareness

14. Rate the following statements according to the response most suitable to your beliefs regarding the perceptions and level of awareness of cloud cybersecurity.

SA=strongly, Agree A=Agree, N-Neutral, D=Disagree, SD=Strongly Disagree.

	Performance Expectancy:- I believe:	SA	A	N	D	SD
PE1	Cloud cybersecurity will be useful and convenient in protecting Job-related contents on various cloud-based systems and applications.					
PE2	Using cloud cyber-security will enable to track any security breaches quickly and efficiently saving my time in managing security of my applications and data					
PE3	Cloud cybersecurity processes are less complicated					
	Effort Expectancy:- I believe:					
EE1	Cloud cyber-security service interactions would be clear and understandable.					
EE2	It would be easier for me to learn and develop the skills to use cloud cybersecurity features. (i.e. setting passwords and usernames, verifying personal details etc. on the cloud system)					
EE3	It is easy to use cloud cyber-security services					
EE4	It is easier for my institution to adopt the cloud service provider's cyber-security model					
	Social influence:- I believe					
SS1	People who are important to me and influence my behavior think I should use cloud computing cyber-security					
SS2	I would use cloud cyber-security if my friends and colleagues use it					
SS3	My institution encourages/supports the staff to use cloud cyber-security					
	Facilitating conditions:- I believe					
FC1	I have access to the resources necessary to use cloud-based cybersecurity					
FC2	I have the knowledge necessary to use cloud-based cybersecurity					
FC3	IT Support people will be available for assistance with any difficulties I might encounter while using cloud cybersecurity.					
	Intention of Use					
IU1	Assuming I have access to cloud-cybersecurity services, I intent to use it					
IU	Given that I have access to the cloud-cybersecurity services, I plan to use it.					
	Awareness :					
A1	I am aware that data stored in cloud-based systems maintains an up-to-date back-up and recovery facility					
A2	I am aware that cloud cyber-security will prevent unauthorized access to my files					

A3	Overall, I am aware of the potential security threats and their negative consequences of using cloud cybersecurity services.					
A4	I believe my institution is aware of the security issues and security capabilities associated with cloud computing.					
A5	I am aware that staff members should be notified when their information is being collected on cloud.					
A6	I am aware of the security training and awareness programs provided by various institutions in order to efficiently use cloud-based cybersecurity systems					
A7	I am aware of the websites that provides cyber-security guidance					
A8	I am aware of the value that cybersecurity adds towards adoption of cloud computing					

ADMIN STAFF QUESTIONNAIRE

CYBERSECURITY FRAMEWORK FOR CLOUD COMPUTING ADOPTION IN RURAL BASED TERTIARY INSTITUTIONS

SECTION A: Background Information

For each item below, Please indicate your answer by putting a clear cross (X) in the relevant block (please choose only one response in each question).

1. What is your gender ?	2. What is your age group?
○ Male ○ Female	○ 18-25 ○ 26-35 ○ 36-45 ○ 46 and above
3. What is your race ?	4. What is your experience level working with information technology?
○ African/Black ○ Coloured ○ Asian/Indian ○ White ○ Other……, please specify	○ Less than 1 Year ○ 2-5 Years ○ 6-10 Years ○ 6-10 Years

SECTION B: Cloud Computing Cyber-Security Usage and Its Drivers

5. Are you knowledgeable of cloud-based cybersecurity services?

○ Yes ○ No

6. Do you have experience of using cloud-based cybersecurity services?

○ Yes ○ No

7. Which cloud computing cybersecurity services and application do you use? (select all that apply)

☐ Microsoft Security (i.e. for Windows and Microsoft Office 365)

☐ Google Apps Security Services (i.e. for Google Drive, G-mail, Google Docs, calendar)

☐ Amazon Web Service for online storage protection (i.e. for Dropbox)

8. In terms of your job-related contents,

Do you think using cloud-based cybersecurity features will allow you to:	YES	NO
Securely send documents and messages through email, or social network platforms	○	○
Securely receive documents and messages through email, or social network platforms	○	○

Securely upload documents and other contents on ITS	○	○
Securely download documents and other contents from ITS	○	○
Securely conduct uninterrupted meetings on online platforms (i.e. video conferencing on skype)	○	○

9. Please rate the following statements that best represents your opinion regarding the usefulness of cloud-cybersecurity in tertiary institutions by putting a Cross (X) on it.

SA=strongly, Agree A=Agree, N-Neutral, D=Disagree, SD=Strongly Disagree.

	Drivers for cloud computing cybersecurity adoption:- I believe:	SA	A	N	D	SD
D1	Tertiary institutions shall use cloud-based cyber-security services for improving data security and privacy information of students, academics and staff.					
D2	Legal law and regulatory compliance encourages tertiary institutions in using cloud-based cybersecurity services.					
D3	The pace of keeping up with latest technology motivates tertiary institutions in using cloud-based cybersecurity services.					
D4	Tertiary institutions may use cloud cybersecurity for financial reasons such as reduced budgeting for cost of cyber-breaches.					
D5	Tertiary institutions may use cloud cybersecurity for maintaining public reputation such as gaining trust and confidence of students, academics and staff.					

SECTION C: Cloud Computing Cyber-Security Issues, Benefits and Quality

10. What according to you are or could be the challenges of using cloud-based cybersecurity services from the items below? (Select all that applies)

CYBERSECURITY CHALLENGES			
☐	Lack of physical control of data and information	☐	Undesirable disclosure of information to law and regulatory bodies.
☐	Harmful activities executed on the network (web/internet)	☐	Lack of security awareness causing cyber-attacks
☐	Information leakage to other cloud cybersecurity service users (Multi-tenancy)	☐	Identity theft and Unauthorized access to my cloud-based applications and study materials
☐	Denial-of-service availability preventing access to my information applications	☐	Information can be lost, deleted, moved or changed.
☐	Compromise of data and information privacy due to its monitoring and tracking by security service providers	☐	Monitoring and tracking of my cloud activities by attackers (Sniffing/spoofing)
☐	My files can be infected with viruses using cloud-based cybersecurity	☐	My device can be hacked while using cloud-based cybersecurity (hacking)

11. What according to you are the benefits of using cloud computing cybersecurity services from the items below? (Select all that applies)

	Benefits of cloud cybersecurity usage: I believe cybersecurity:
☐	Prevents falsification of information on ITS, Email, social media, finance, library, IT, Customer relationship management systems and supply chain management systems of the university.
☐	Prevents individuals from presenting a false identity to University authorities

☐	Ensures privacy of communication and Prevents intrusion upon controlled or private conversations among individuals, departments and schools of the University.
☐	Prevents the alteration of date stamps on files and documents (such as application forms, results, transcripts, research outputs and other contents on MyAccess)
☐	Prevents individuals from stealing and gaining access to personal data of students, academics and staff members.

12. Why do you think cloud computing cyber-security is important in tertiary institutions? (select all that applies).

☐ To protect central administrative systems (i.e. student records, financial systems)

☐ To protect research systems and databases (i.e. intellectual research properties)

☐ To protect departmental systems (i.e. ITS Integrator)

☐ To protect web applications (i.e. office 365)

☐ To protect faculty staff member's computer and mobile device applications and files

☐ None of the Above

13. Rate the following statements according to the response most suitable to your beliefs regarding the quality of cloud cybersecurity.

SA=strongly, Agree A=Agree, N-Neutral, D=Disagree, SD=Strongly Disagree.

	Quality perceptions of cyber-security services :- I believe:	SA	A	N	D	SD
QP1	Cloud cyber-security is reliable and flexible for securing my contents on various platforms such as google drive, emails, dropbox , ITS, Library Systems etc.					
QP2	Cloud cyber-security is accurate and effective for protecting my personal and job related contents.					
QP3	Cloud cybersecurity is consistent and relevant for securing my personal and job related contents					
QP4	Cloud cybersecurity services is responsive as I will be informed about security breaches timeously					
QP5	Overall, cloud cyber-security is a success as it increases the value of cloud computing and promotes the adoption of cloud computing					
QP6	My tertiary institution has the necessary infrastructure for supporting the system, information and service quality of cyber-security					

SECTION D: Cloud-Computing Cybersecurity Perceptions and Awareness

14. Rate the following statements according to the response most suitable to your beliefs regarding the perceptions and level of awareness of cloud cybersecurity.

SA=strongly, Agree A=Agree, N-Neutral, D=Disagree, SD=Strongly Disagree.

	Performance Expectancy:- I believe:	SA	A	N	D	SD
PE1	Cloud cybersecurity will be useful and convenient in protecting Job-related contents on various cloud-based systems and applications.					
PE2	Using cloud cyber-security will enable me to track any security breaches quickly and efficiently saving my time in managing security of my applications and data					

PE3	Cloud cybersecurity processes are less complicated					
	Effort Expectancy:- I believe:					
EE1	Cloud cyber-security service interactions would be clear and understandable					
EE2	It would be easier for me to learn and develop the skills to use cloud cybersecurity features. (i.e. setting passwords and usernames, verifying personal details etc. on the cloud system)					
EE3	It is easy to use cloud cyber-security services					
	Social influence:- I believe					
SS1	People who are important to me and influence my behavior think I should use cloud cyber-security					
SS2	I would use cloud cyber-security if my friends and colleagues use it					
SS3	My institution encourages/supports the staff to use cloud cyber-security					
	Facilitating conditions:- I believe					
FC1	I have access to the resources necessary to use cloud-based cybersecurity					
FC2	I have the knowledge necessary to use cloud-based cybersecurity					
FC3	IT Support people will be available for assistance with any difficulties I might encounter while using cloud cybersecurity.					
	Intention of Use					
IU1	Assuming I have access to cloud-cybersecurity services, I intent to use it					
IU	Given that I have access to the cloud-cybersecurity services, I plan to use it.					
	Awareness :					
A1	I am aware that data stored in cloud-based systems maintains an up-to-date back-up and recovery facility.					
A2	I am aware that cloud-computing cyber-security will prevent unauthorized access to my files.					
A3	Overall, I am aware of the potential security threats and their negative consequences of using cloud cybersecurity services.					
A4	I believe my institution is aware of the security issues and security capabilities associated with cloud computing.					
A4	I am aware that staff members should notified when their information is being collected on cloud.					
A6	I am aware of the security training and awareness programs provided by various institutions in order to efficiently use cloud-based cybersecurity systems					
A7	I am aware of the websites that provides cyber-security guidance					

ANNEXURE D: AWARENESS PERCEPTIONS

Item	UNIVEN		TVET		Rosebank	
	F	VP	F	VP	F	VP
Strongly Agree	74	32.5%	35	29.4%	31	33%
Agree	88	38.6%	58	48.7%	41	43.6%
Neutral	49	21.5%	20	16.8%	16	17%
Disagree	14	6.1%	2	1.7%	6	6.4%
Strongly Disagree	3	1.3%	4	3.4%	0	0
Total	**228**	**100%**	**119**	**100%**	**94**	**100%**

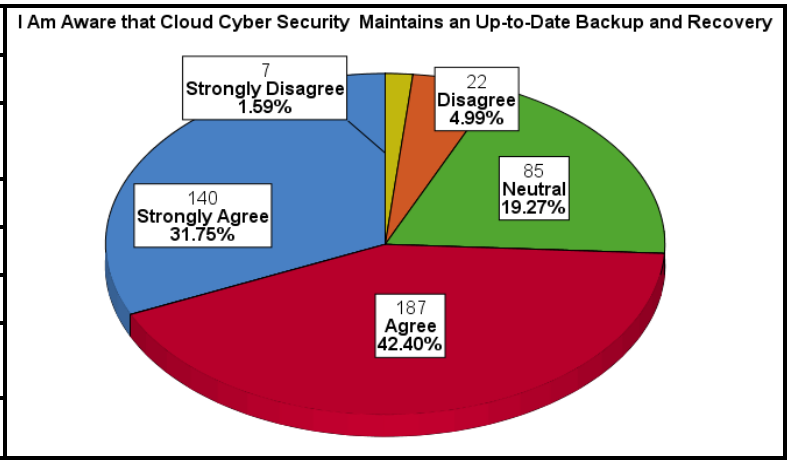

Figure 4a. Awareness Perception on Cloud-Based Backup and Recovery Facility

Item	UNIVEN		TVET		Rosebank	
	F	VP	F	VP	F	VP
Strongly Agree	63	27.8%	30	25.2%	25	26.6%
Agree	95	41.9%	62	52.1%	46	48.9%
Neutral	44	19.4%	20	16.8%	18	19.1%
Disagree	14	6.2%	5	4.2%	5	5.3%
Strongly Disagree	11	4.8%	2	1.7%	0	0
Total	**227**	**100%**	**119**	**100%**	**94**	**100%**

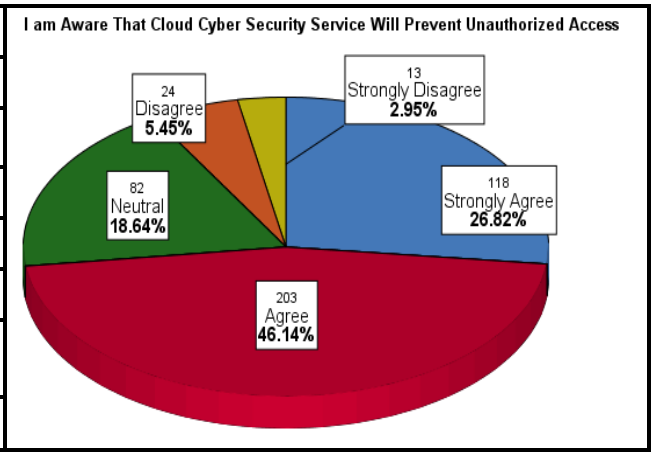

Figure 4b. Awareness on Prevention of Unauthorized Access to Files when Using Cloud-Cybersecurity

Item	UNIVEN		TVET		Rosebank	
	F	VP	F	VP	F	VP
Strongly Agree	61	27%	31	26.1%	32	34%
Agree	88	38.9%	52	43.7%	43	45.7%
Neutral	54	23.9%	24	20.2%	14	14.9%
Disagree	14	6.2%	7	5.9%	4	4.3%
Strongly Disagree	9	4%	5	4.2%	1	1.1%
Total	226	100%	119	100%	94	100%

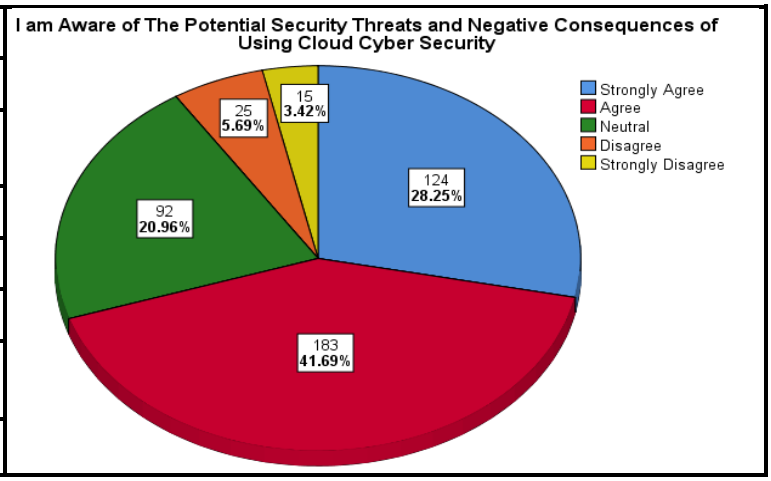

Figure 4c. Awareness Perception on Security Threats and Consequences of Using Cloud-Cybersecurity

Item	UNIVEN	TVET	Rosebank	

	F	VP	F	VP	F	VP
Strongly Agree	40	17.5%	25	21%	16	17%
Agree	74	32.5%	42	35.3%	40	42.6%
Neutral	65	28.5%	29	24.4%	24	25.5%
Disagree	26	11.4%	18	15.1%	8	8.5%
Strongly Disagree	23	10.1%	5	4.2%	6	6.4%
Total	**228**	**100%**	**119**	**100%**	**94**	**100%**

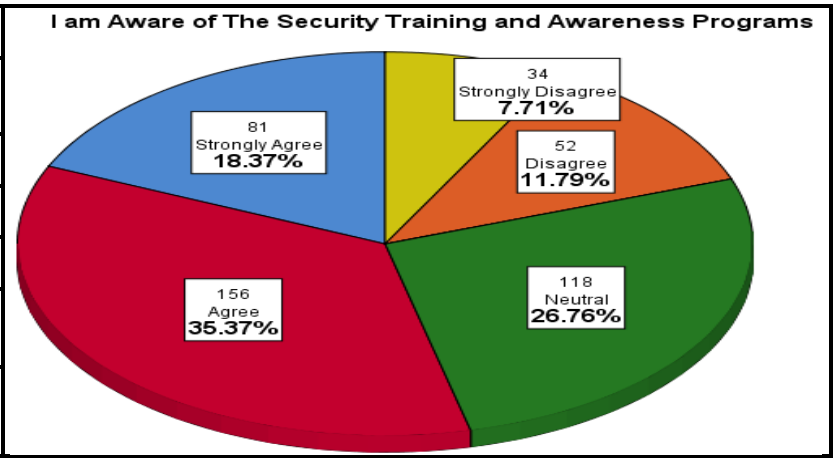

Figure 4d. Awareness Perception on the Security Training and Awareness Programs by Various Institutions

Item	UNIVEN		TVET		Rosebank	
	F	VP	F	VP	F	VP
Strongly Agree	55	24.1%	28	23.5%	25	26.6%
Agree	69	30.3%	37	31.1%	33	35.1%
Neutral	67	29.4%	28	23.5%	20	21.3%
Disagree	26	11.4%	17	14.3%	15	16.0%
Strongly Disagree	11	4.8%	9	7.6%	1	1.1%
Total	**228**	**100%**	**119**	**100%**	**94**	**100%**

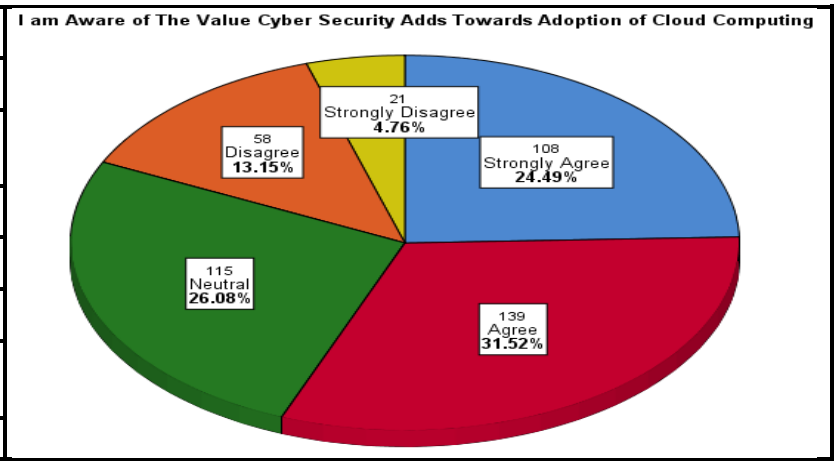

Figure 4e. Awareness of the Value Cyber-Security Adds Towards the Adoption of Cloud Computing

Item	UNIVEN		TVET		Rosebank	
	F	VP	F	VP	F	VP
Strongly Agree	38	18.4%	22	21.8%	20	21.3%
Agree	56	27%	34	33.7%	36	38.3%
Neutral	64	30.9%	28	27.7%	15	16%
Disagree	29	14%	11	10.9%	18	19.1%
Strongly Disagree	20	9.7%	6	5.9%	5	5.3%
Total	**207**	**100%**	**101**	**100%**	**94**	**100%**

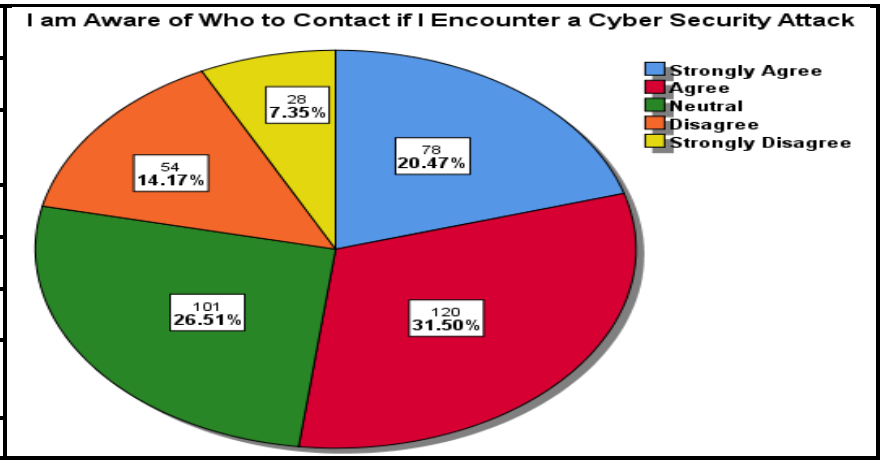

Figure 4f. Awareness Perceptions on Who To Contact During a Cyber-Security Attack

ANNEXURE E: PROOF READING LETTER

SCHOOL OF HUMAN AND SOCIAL SCIENCES

Department of English
University of Venda
Thohoyandou
0950

14 February 2019

Dear Sir/Madam

This serves to notify that I proof-read a dissertation titled "**Cybersecurity Framework For Cloud Computing Adoption in Rural Based Tertiary Institutions**" by Patala Najiyabanu Noor Mohmed., Student Number: 11634215

The proof-reading entailed editing some parts from it; for example, to avoid wordiness, redundancy; sub-dividing sentences, and so on, to make the document more understandable. However, I have not tempered with the content of the document, except where there are language errors.

Sincerely

.....

Robert Moyo
0736702487
robbiemoyo1@yahoo.co.za

University of Venda