Towards a Framework for Enhancing User Trust in Cloud Computing

by

Tamsanqa B Nyoni

Towards a Framework for Enhancing User Trust in Cloud Computing

by

Tamsanqa B Nyoni

200800344

Dissertation

submitted in fulfilment of the requirements for the degree

Master of Commerce

in

Information Systems

In the

Faculty of Management and Commerce

of the

University of Fort Hare

Supervisor: **Dr Roxanne Piderit**

January 2014

Abstract

Cloud computing is one of the latest appealing technological trends to emerge in the Information Technology (IT) industry. However, despite the surge in activity and interest, there are significant and persistent concerns about cloud computing, particularly with regard to trusting the platform in terms of confidentiality, integrity and availability of user data stored through these applications. These factors are significant in determining trust in cloud computing and thus provide the foundation for this study. The significant role that trust plays in the use of cloud computing was considered in relation to various trust models, theories and frameworks.

Cloud computing is still considered to be a new technology in the business world, therefore minimal work and academic research has been done on enhancing trust in cloud computing. Academic research which focuses on the adoption of cloud computing and, in particular, the building of user trust has been minimal. The available trust models, frameworks and cloud computing adoption strategies that exist mainly focus on cost reduction and the various benefits that are associated with migrating to a cloud computing platform. Available work on cloud computing does not provide clear guidelines for establishing user trust in a cloud computing application. The issue of establishing a reliable trust context for data and security within cloud computing is, up to this point, not well defined. This study investigates the impact that a lack of user trust has on the use of cloud computing. Strategies for enhancing user trust in cloud computing are required to overcome the data security concerns.

This study focused on establishing methods to enhance user trust in cloud computing applications through the theoretical contributions of the Proposed Trust Model by Mayer, Davis, and Schoorman (1995) and the Confidentiality, Integrity, Availability (CIA) Triad by Steichen (2010). A questionnaire was used as a means of gathering data on trust-related perceptions of the use of cloud computing. The findings of this questionnaire administered to users and potential users of cloud computing applications are reported in this study. The questionnaire primarily investigates key concerns which result in self-moderation of cloud computing use and factors which would improve trust in cloud computing. Additionally, results relating to user awareness of potential confidentiality, integrity and availability risks are described.

An initial cloud computing adoption model was proposed based on a content analysis of existing cloud computing literature. This initial model, empirically tested through the questionnaire, was an important foundation for the establishment of the Critical Success Factors (CSFs) and therefore the framework to enhance user trust in cloud computing applications. The framework proposed by this study aims to assist new cloud computing users to determine the appropriateness of a cloud computing service, thereby enhancing their trust in cloud computing applications.

Keywords: Adoption; Cloud Computing; User Trust

Declaration

I, Tamsanqa B Nyoni (200800344), hereby declare that:

- The work in this dissertation is my own work.
- All sources used or referred to have been documented and recognised.
- This dissertation has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institution.
- I am fully aware of the University of Fort Hare‘s policy on plagiarism and I have taken every precaution to comply with the regulations.
- I am fully aware of the University of Fort Hare‘s policy on research ethics and I have taken every precaution to comply with the regulations. I have obtained an ethical clearance certificate from the University of Fort Hare's Research Committee and my reference number is the following: **PID01 ISNYO01** (Attached as Appendix A).

____

14 January 2014

Acknowledgements

I wish to express my gratitude and appreciation to the following people for their support, guidance and advice during this research project:

- My supervisor, Dr. Roxanne Piderit, for the constructive feedback, advice, encouragement and the guidance which enabled me to complete this research project.

- The University of Fort Hare and the Department of Information Systems for the support it has provided me throughout the duration of my academic career. Special mention must be made to my fellow students for their continuous advice, support and encouragement.

- The University of Fort Hare and its associated research body, The Govan Mbeki Research and Development Centre, for the financial support that they provided to me throughout this research project.

- Lastly, my family and friends for their endless, valuable support, understanding and encouragement throughout this research project.

Table of Contents

Chapter 2: Cloud Computing and Its Benefits

Chapter 3: Cloud Computing Adoption Issues and Concerns

Chapter 6: Empirical Analysis and Discussion

Chapter 7: Towards a Framework for Enhancing User Trust in Cloud Computing Applications

List of Figures

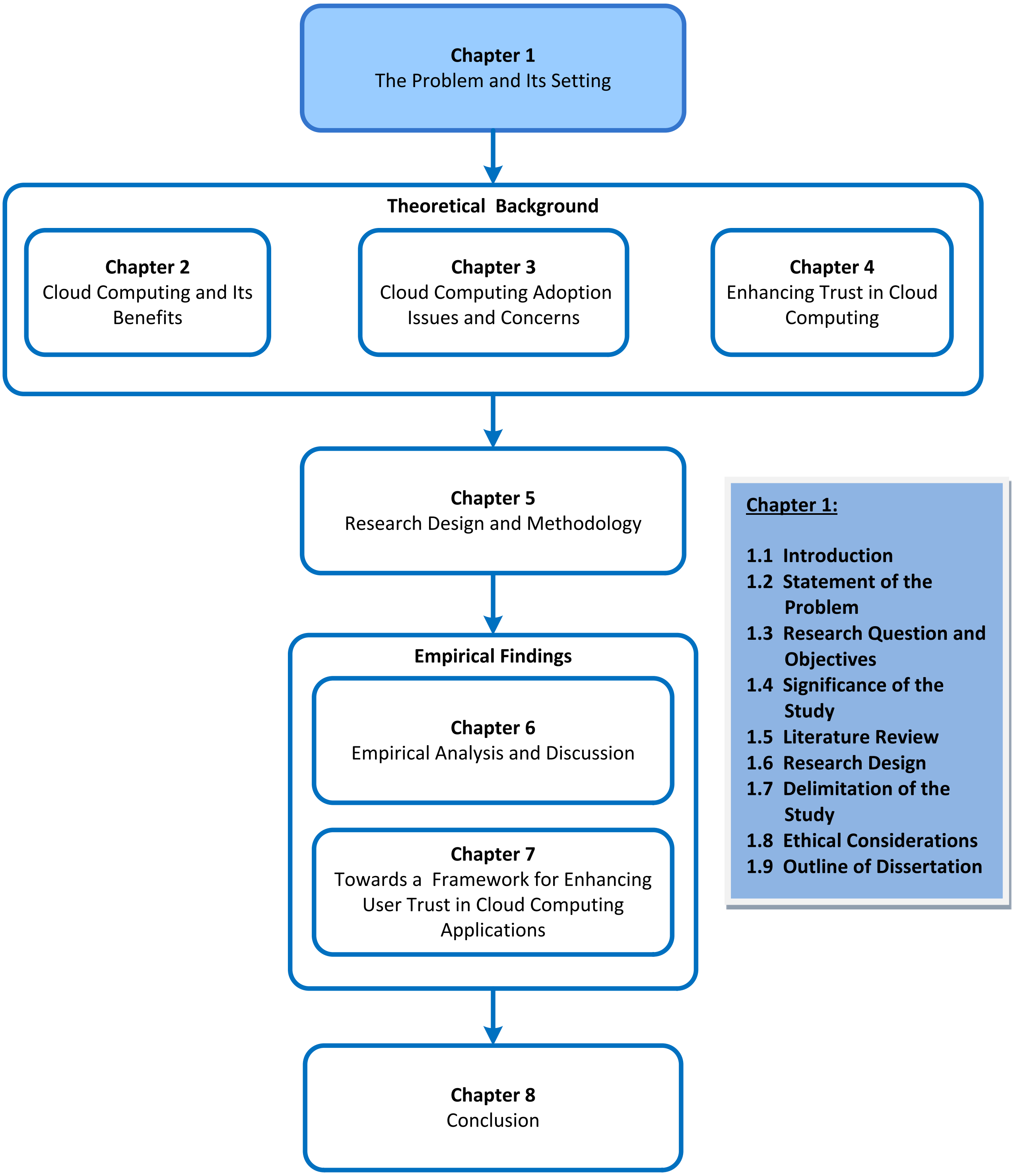
List of Tables

Abbreviations and Acronyms

API	Application Programming Interface
CIA	Confidentiality, Integrity, Availability
CRM	Customer Relationship Management
CSF	Critical Success Factor
DaaS	Data-as-a-Service
EC2	Elastic Compute Cloud
IaaS	Infrastructure-as-a-Service
ICT	Information and Communication Technology
IS	Information Systems
IT	Information Technology
PaaS	Platform-as-a-Service
PVI	Private Virtual Infrastructure
SaaS	Software-as-a-Service
SLA	Service Level Agreement
TAM	Technology Acceptance Model
TC	Trusted Coordinator
TCCP	Trusted Cloud Computing Platform
TVMM	Trusted Virtual Machine Monitor
UFH	University of Fort Hare
VM	Virtual Machines

Chapter 1:

The Problem and Its Setting


Chapter 1
The Problem and Its Setting
Theoretical Background
Chapter 2
Cloud Computing and Its Benefits
Chapter 3
Cloud Computing Adoption Issues and Concerns
Chapter 4
Enhancing Trust in Cloud Computing
Chapter 5
Research Design and Methodology
Empirical Findings
Chapter 6
Empirical Analysis and Discussion
Chapter 7
Towards a Framework for Enhancing User Trust in Cloud Computing Applications
Chapter 8
Conclusion

Chapter 1:

1.1 Introduction
1.2 Statement of the Problem
1.3 Research Question and Objectives
1.4 Significance of the Study
1.5 Literature Review
1.6 Research Design
1.7 Delimitation of the Study
1.8 Ethical Considerations
1.9 Outline of Dissertation

1.1. Introduction

Recent advances in the use of technology have pushed technological innovation to new frontiers. It has become a prerequisite for technology users to keep abreast of ever-evolving technology. In an attempt to gain a firm grip on new technologies, technology users in South Africa are increasingly exploring new innovative information and communication technologies (ICTs). This growing acceptance of innovative technologies amongst technology users has seen the popularity of cloud computing increase substantially (Lovell, 2010). Ragent and Leach (2010) concur with the above argument stating that cloud computing is fast becoming a dynamic force in the business world. Furthermore, cloud computing is both the most hyped and the most important trend in the modern day information technology (IT) industry (Taylor, 2012). However, the right approach and attitude to cloud computing is needed in order to create value for users (Ragent & Leach, 2010).

Cloud computing is a technology whereby data and applications are hosted in a secure environment (the cloud) and then provided as a service online, either by subscription or on a pay-on-demand basis. This is confirmed by Capers (2010) who states that cloud computing applications reside on network servers rather than on individual computers. Additionally, Ragent and Leach (2010) describe cloud computing as an Internet-based computing model which enables convenient, on-demand network access to shared resources, software and information which is provided to computers and other devices. It provides massive storage for data and faster ways of computing for users over the Internet. It essentially shifts the database and application software to the large data centres which provide the resources for cloud computing (Sood, 2012).

Thus, by reducing the required computing resources, cloud computing is an innovative ICT option which drastically reduces operating costs for its users (Knode, 2009). Cloud computing users in business sectors, such as banking, retail and communication, have realised the abundant benefits that come with cloud computing and have adopted it to enhance their business processes. Ragent and Leach (2010) concur with the above statement as they believe that cloud computing is fast becoming a dynamic force in the business world.

The emergence and application of cloud computing has helped users gain access to various computing resources more conveniently (Nyoni & Piderit, 2013). However, the widespread application and adoption of cloud computing has been met by considerable resistance because of various trust and security challenges associated with cloud computing (Zhang, Liu, Li, Haiqiang,

& Wu, 2011). According to Zhang, *et al.* (2011) the volumes and type of data that can be stored and retrieved from a cloud computing platform through the use of the Internet threatens the perceived security and trustworthiness of cloud computing.

The problem this study investigates is the low level of user trust in cloud computing which impacts on the adoption and use of these services. Shimba (2010) states that although the successful adoption of cloud computing promises various benefits to users, they need an understanding of the dynamics involved in its adoption and use. Most users traditionally view cloud computing to be a complex and insecure operation (Shimba, 2010). Thus, according to Ragent and Leach (2010), despite the potentially positive impact that the use of cloud computing has on efficiency and productivity, many organisations and users are still reluctant to fully embrace cloud computing. This confirms the views of Cofta (2007) who articulates that trust is increasingly becoming a necessity to ensure that new technologies are utilised for maximum benefit. Moreover, according to Ragent and Leach (2010) a lack of trust in cloud computing has caused the adoption and implementation process to become chaotic, haphazard and characterised by constant failure. This has also seen most users fail to utilise the vast advantages that come with migrating to cloud computing compared to traditional methods.

The study investigated the relationship between the lack of trust in cloud computing and the user's intentions to adopt and use cloud computing. The factors that influence the lack of trust in cloud computing were investigated, and because of the prevailing trust and security issues, an appropriate cloud computing adoption framework is needed. The framework should develop user understanding of cloud computing, enhance user trust and improve adoption rates of cloud computing applications. A framework for enhancing user trust in the cloud computing applications was formulated in this study in order to assist users to evaluate the different cloud computing options available.

The research problem is described in the next section, followed by the research question and the objectives of the study. Following this, the significance of the study will be briefly discussed, and a brief literature review of the concepts that are central to this research project namely trust and cloud computing is provided. Next, the research methodology and delimitation of the study are detailed, and the chapter outline for this dissertation is described.

1.2. Statement of the Problem

Despite the vast technical advantages of using cloud computing, potential cloud computing users are still reluctant to trust and migrate to the cloud computing platform (Chow, Golle, Jakobsson, Shi, Staddon, Masuoka, & Molina, 2009). This is largely due to the fact that the convenience and efficiency of cloud computing comes with a range of potential privacy and security related issues that pose a threat to a user's data. As the management of data and services on the cloud computing platform may not be completely trustworthy, users are reluctant to adopt and use cloud computing (Sood, 2012).

Security of data stored via cloud computing is noted as one of the major issues which acts as an obstacle in the adoption and use of cloud computing. Among these issues, the lack of trust in the cloud computing platform has proven to be a key barrier to the extensive adoption of cloud computing (Lockheed Martin Cyber Securty Alliance, 2010). Users often question cloud computing capabilities with regards to secure data storage, as well as the intentions of the cloud computing service providers (Kumar, Sehgal, Chauhan, Gupta, & Diwakar, 2011). The presence of trust would ensure the successful adoption of cloud computing, while the lack of trust results in inefficient and ineffective use of the services offered by the cloud computing platform (Bourne, 2010).

Therefore, the research problem investigated in this study is the low level of user trust in cloud computing applications which impacts on the adoption and use of these applications. This study aimed to investigate a means of enhancing user trust in cloud computing to ensure successful adoption of cloud computing. The following research questions were investigated in this regard:

1.3. Research Question and Objectives

1.3.1. Primary Research Question

How can user trust in cloud computing applications be enhanced to ensure adoption and use?

This primary research question was addressed through the following secondary research questions:

1.3.2. Secondary Research Questions

1.3.2.1. How can users benefit from using cloud computing applications?

Cloud computing allows for better IT resource optimisation, virtually unlimited scalability and greater flexibility, all at a contained cost (Callewaert & Luysterborg, 2011). Cloud computing is an attractive service offered for any individual looking to enhance IT resources while controlling costs (ISACA, 2009). Therefore, users should improve trust in cloud computing so as to maximise the benefits which include reduced cost and increased storage, flexibility and mobility (Callewaert & Luysterborg, 2011). Cloud computing also has the ability for users to access various computing resources remotely regardless of time and physical location.

1.3.2.2. What are the key concerns affecting user trust in cloud computing applications?

When considering the risks associated with cloud computing, the fundamental element that most users consider is how the cloud computing environment affects their trust boundary (Meade, 2009). According to Ko, Jagadpramana, Mowbray, Pearson, Kirchberg, Liang, and Lee (2011), the lack of trust is identified as the key barrier to widespread cloud computing adoption for most users (Ko, et al., 2011). The lack of trust clearly has a negative impact on the user's decision to adopt and use cloud computing. Users are concerned with their security and the privacy of their data stored via cloud computing. These, and the three confidentiality, integrity, availability (CIA) triad constructs are the paramount issues affecting user trust in cloud computing applications.

1.3.2.3. How can the trust barrier be overcome to enhance user trust in cloud computing applications?

In order to increase trust in cloud computing, there is a need for a strategy that also increases the level of transparency and accountability of data in the cloud computing environment for both enterprises and end-users (Ko, Jagadpramana, & Lee, 2011). The provision and assurance of total security and privacy when it comes to users and their data by service providers plays a pivotal role toward overcoming the trust barrier. The three determinants of trust, which are ability, integrity and benevolence as proposed by Mayer, Davis and Schoorman (1995), are also seen as vital factors that help overcome the trust barrier.

Complementary to the research questions outlined above, the following research objective is central to this research study.

1.3.3. Objectives of the Study

The objective of this study is to produce a framework that can be used to enhance the level of user trust in cloud computing by providing a decision making tool to influence user adoption. This framework is based on literature findings and empirical findings obtained from cloud computing users.

Having outlined the research questions and objectives of this study, the following section highlights the importance of this research project.

1.4. Significance of the Study

Cloud computing is still considered to be a new technology. Therefore minimal work and academic research has been done on enhancing trust in cloud computing (Vael, 2010). According to Shimba (2010) academic research which focuses on the adoption of cloud computing and, in particular, the building of customer trust has been minimal. Additionally, studies conducted on cloud computing as a new technology in the market mainly focus on the benefits to users. The key benefits identified are access to data from different devices anywhere, at any time. Thus, most of the available work and academic research on cloud computing does not provide clear trust enhancing strategies that will ensure the adoption of cloud computing.

As described previously, the use of cloud computing has numerous benefits for its users, including reduced cost and increased storage, flexibility and mobility (Callewaert & Luysterborg, 2011). Thus it is important to enhance trust in cloud computing services in order to ensure the services are adopted to maximise user benefits. Importantly, there is no existing framework which focuses on user concerns with cloud computing applications. Thus, the framework proposed in this study is important in so far as it provides a decision-making tool for users to assess the trustworthiness of a cloud computing application before making use of it. The following section will discuss the literature that was reviewed in order to gain an understanding of the identified problem.

1.5. Literature Review

This section provides a thorough investigation and discussion of various secondary literature sources relating to the research problem and a number of underlying theories. The Proposed Trust Model by Mayer, Davis and Schoorman (1995), Diffusion of Innovations Theory proposed by Rogers (2003), and The CIA triad by Steichen (2010) provide a theoretical framework for this study. Existing cloud computing models such as the Trusted Cloud Computing Platform (TCCP) and Private Virtual Infrastructure (PVI) are also described and evaluated in this section.

1.5.1. Underlying Theories

This research project will make reference to the Proposed Trust Model, The CIA Triad and the Diffusion of Innovations Theory throughout in order to underline the academic significance of the topic under discussion.

1.5.1.1. Mayer, Davis, and Schoorman's (1995) Proposed Trust Model

The model depicted in Figure 1.1 by Mayer, Davis, and Schoorman (1995) has been a predominant model for trust research. This model is based on literature research and developed within the management domain on issues relating to trust. The proposed model distinguishes between trustor and trustee characteristics that foster a trusting relationship between the two parties. In the cloud computing context, the user is the trustor and the service provider is the trustee. Thus, this model is appropriate for the context of user and service provider relationships in cloud computing.

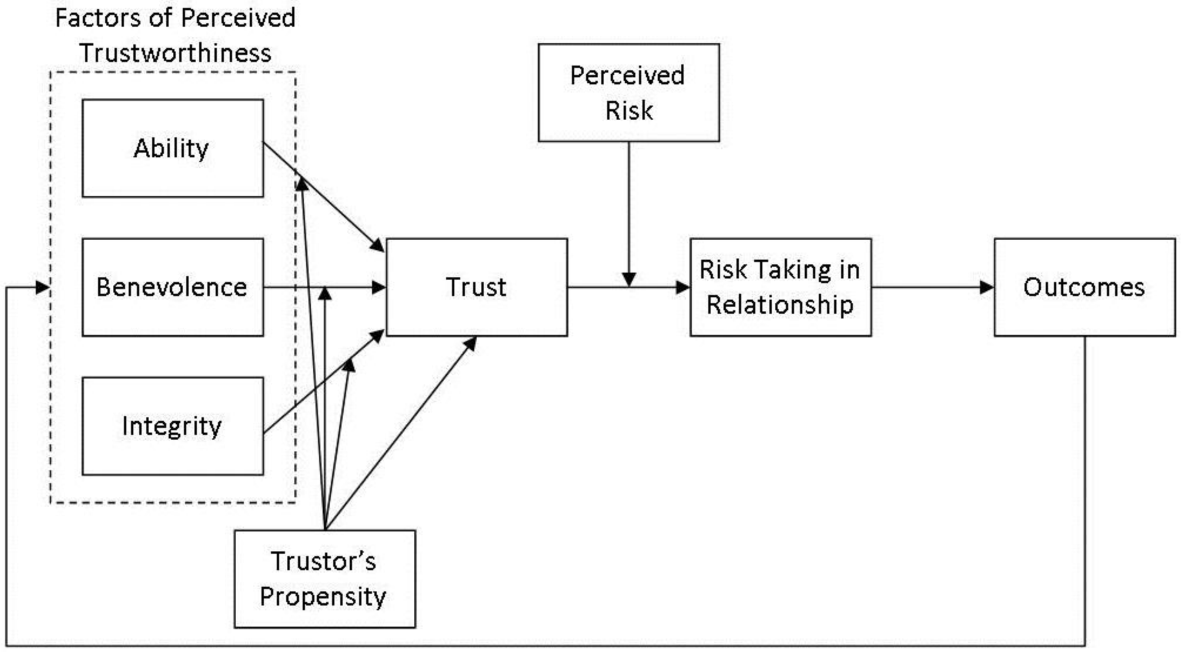


Figure 1.1: Proposed Trust Model (Source: Mayer, Davis, & Schoorman, 1995)

The model identifies ability, benevolence and integrity as key determinants of trust which need to be considered when evaluating the cloud computing service provider's trustworthiness. Thus, ability, benevolence and integrity were investigated through the questionnaire in order to develop a framework for cloud computing users. This theory is described in more detail in Chapter 4.

1.5.1.2. The Confidentiality Integrity Availability (CIA) Triad

The CIA Triad is an industry-accepted model for ensuring security in systems (Steichen, 2010). It specifically focuses on the storage and management of data. The CIA triad is depicted in Figure 1.2 and described in more detail in Chapter 3.

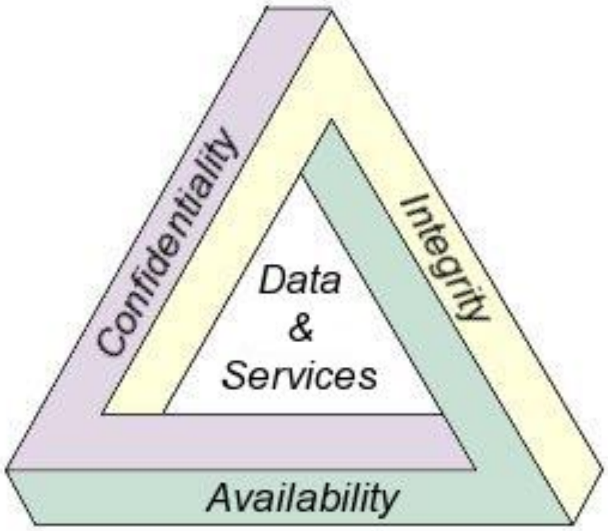


Figure 1.2: CIA Triad (Source: Steichen, 2010)

1.5.1.3. Rogers' (2003) Diffusion of Innovation Theory

According to Sahin (2006) the model by Rogers' (2003) is as a widely used theoretical framework in the area of new technology diffusion and adoption. The Innovation-Decision Process (Figure 1.3) of the Diffusion of Innovation Theory involves five steps: (1) Knowledge, (2) Persuasion, (3) Decision, (4) Implementation, and (5) Confirmation. These steps are relevant to this research project as they contribute to the decision-making process for adopting a cloud computing application and will be described in more detail in Chapter 4.

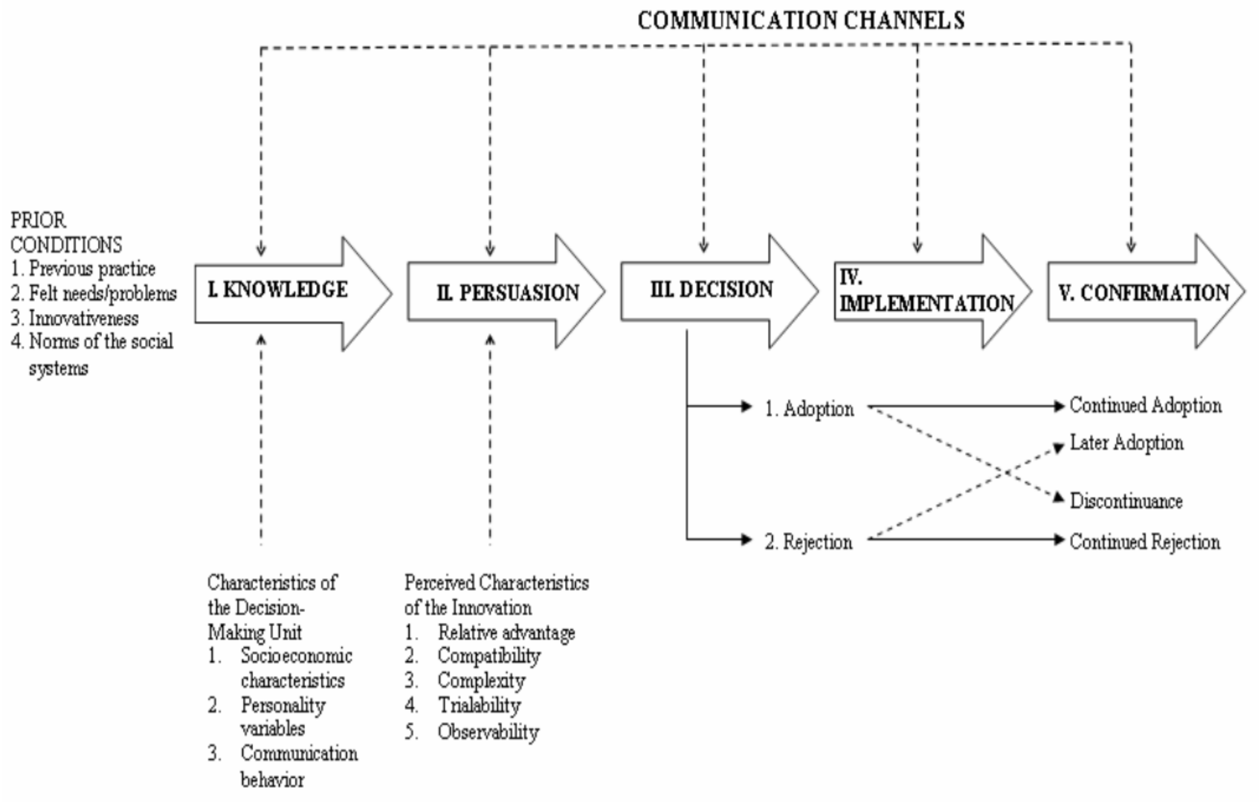


Figure 1.3: The Innovation Decision Process (Source: Rogers, 2003)

The section below describes some of the challenges that are affecting users when it comes to cloud computing adoption and use.

1.5.2. Cloud Computing Adoption Challenges

According to IBM (2009) cloud computing represents a key technological change in rapid deployment computing services. It is an innovation that builds on previous innovations that include grid, utility and on-demand computing, and offers users vast advantages and benefits (Bourne, 2010). Tyler (2010) states that cloud computing is changing how users invest in, and use, their IT infrastructure. Data and information security is a key concern for cloud computing as it affects user trust in using cloud computing applications. Thus, cloud computing encourages users to reconsider how they secure their data.

The adoption of cloud computing is faced with a number of challenges such as security, legal and compliance challenges (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2008). Khajeh-Hosseini, Sommerville and Sriram (2010) agree with this statement and add that cloud computing is not simply about a technological improvement of data centres, but a fundamental change in how IT is provisioned and used. Cloud computing is often coupled with challenges such as security concerns; and legal and privacy issues (Khajeh-Hosseini, *et al*, 2010).

Callewaert and Luysterborg (2011) further explain that as a result of the perceived open nature of cloud computing, adoption and use raises security, privacy and trust concerns.

Shimba (2010) points out an additional adoption challenge relating to the issue of trust that exists between users and service providers. This is because cloud computing as a new technology calls for users to trust service providers with the management of their data and IT resources. It therefore becomes clear that trust is an essential element in the cloud computing adoption process, as any unexpected behaviour by a service provider can lead to the disclosure of important and confidential user information.

Due to the existence of security and trust concerns, researchers have proposed trust models to reduce the impact of these challenges on cloud computing challenges. A description and critique of the existing trust models is provided in the next section.

1.5.3. Trust Models for Cloud Computing

Despite trust being an integral factor in the adoption process, most users still show low levels of trust when it comes to cloud computing adoption. Thus there is a need to enhance the trust levels that users have in cloud computing (Shimba, 2010). In an attempt to enhance the levels of trust that users have when faced with the decision to adopt and use cloud computing, a number of scholars have put forward models and theories that aim to promote trust amongst users, including the TCCP and PVI model which are described below.

1.5.3.1. Trusted Cloud Computing Platform (TCCP)

The TCCP proposed by Santos, Gummandi and Rodrigues (2009) suggests the improvement of user trust in cloud computing through a means of verifying the confidentiality and integrity of the data and computation. The TCCP enables cloud computing service providers to provide a closed box execution environment that guarantees total confidential execution of guest virtual machines (VMs) (Santos, Gummandi & Rodrigues, 2009).

Furthermore, according to Santos, Gummandi and Rodrigues (2009), the TCCP allows users to check and determine whether or not the service being offered by the cloud computing service provider is secure before they launch their VMs. The checking and verifying process also allows users to gain a certain level of trust toward the use of cloud computing. The confidential and closed nature of the TCCP tends to promote the levels of trust that the users have in using cloud computing.

1.5.3.2. Private Virtual Infrastructure (PVI) Model

Krautheim (2010) proposes the PVI model which suggests a synergistic relationship between the service provider and user of cloud computing services which will ensure privacy and security. According to Krautheim (2010), the relationship provides an increased security attitude while allowing both parties to set security controls required to protect the infrastructure and data within cloud computing (Krautheim, 2010). This in turn will improve trust in cloud computing.

Furthermore, according to Krautheim (2010), the synergistic relationship can be maintained and improved through trusted computing. Trusted computing provides mechanisms to control the behaviour of computer systems through the enforcement of security policies via hardware and software controls. By requiring service providers to use trusted computing technology, users can verify their security posture in the cloud computing platform and control their information and eventually increase trust in cloud computing (Krautheim, 2010).

1.5.3.3. Critique of the Cloud Computing Trust Models

Although the models described above attempt to build a certain level of trust in cloud computing, a more comprehensive solution is needed that will significantly enhance users' levels of trust and provide a decision making tool for the end users. An analysis of the above mentioned cloud computing trust models indicates that the TCCP solely concentrates on improving trust by providing a secure and confidential platform, and thus is focused solely on an infrastructure-as-a-service (IaaS) cloud computing delivery model. This excludes the platform-as-a-service (PaaS), software-as-a-service (SaaS) or data-as-a-service (DaaS) models which are relevant to this research project. These delivery models are discussed in detail in Chapter 2.

On the other hand, the PVI model is limited to improving the relationship between the cloud computing service provider and user as a way of improving trust levels in cloud computing. The PVI does not propose a means of improving transparency between parties to the cloud computing arrangement, and is thus inclined to lead to mistrust. These models do not provide clear guidelines that will enhance trust in cloud computing leading to successful adoption. Therefore the proposed solution, the framework from this research project will take into consideration the contribution of both the TCCP and PVI models towards enhancing trust in cloud computing. However, the main factors from these models will be further developed, refined and the presented as a framework which will provide clear guidelines towards enhancing trust in cloud computing adoption in various users.

The next section briefly outlines the research design that was employed to investigate the identified research problem.

1.6. Research Design

The Design Science methodology was used for this study. Design Science is a comprehensive problem solving process that is characterised by the detailed evaluation of a project with the end goal being the creation of an artefact (Hevner, March, Park, & Ram, 2004; Gasser, Majchrzak & Markus, 2002). For this study the artefact will be a proposed framework for enhancing user trust in cloud computing applications.

The study reviewed current and available literature on cloud computing including the analysis of frameworks, cloud computing guidelines and other related articles. This literature review informed the creation of the research instrument (questionnaire), and consequently, the proposal of the artefact (framework). As an iterative validation step is required in the Design Science Methodology, the artefact was validated through three rounds of expert reviews. Figure 1.3 below provides a diagrammatical representation of the research approach that will be employed for this research project.

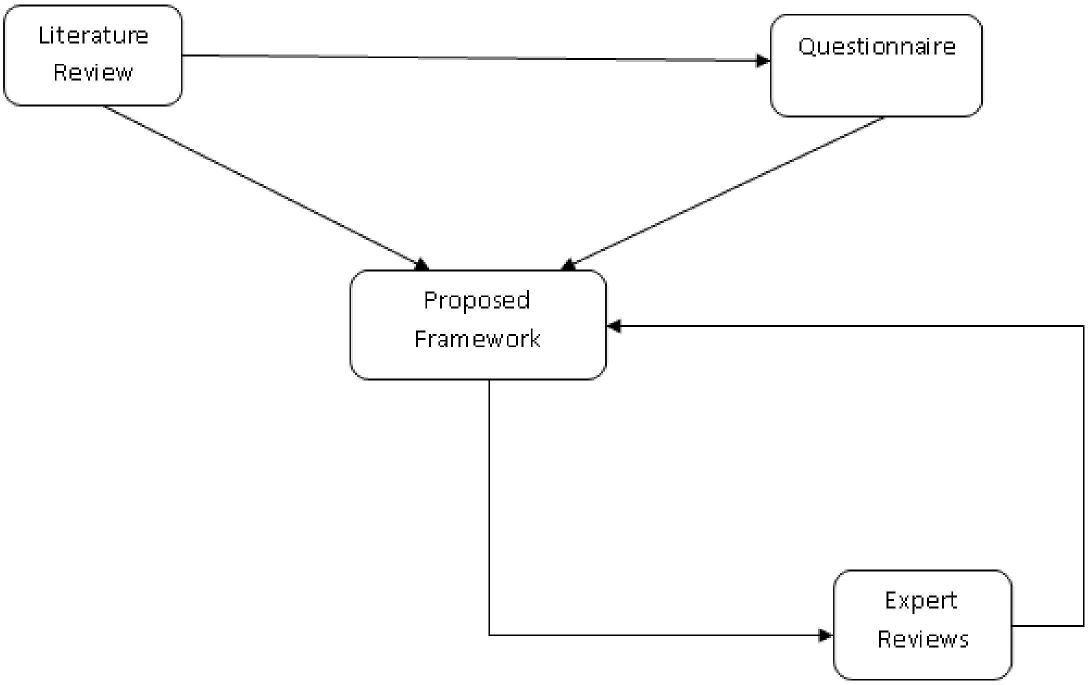


Figure 1.4: Research Strategy

This is the research strategy that was followed throughout this research project. A discussion of the choice of research paradigm, research methodology, data collection methods, data analysis methods and the sample and population for this study are described in the sections that follow.

1.6.1. Research Paradigm

A research paradigm is a framework of guidelines that explains how the research will be conducted. According to Hofstee (2006), academic research must have an underlying philosophical paradigm. This is defined as a pattern or shared way of thinking to which the research is aligned. A variety of philosophical paradigms are available because of the different ideas, views and perspectives of the world (Hofstee, 2006). This section discusses the research paradigm for this study. Figure 1.5 is used to illustrate the choice of paradigm for this research project.

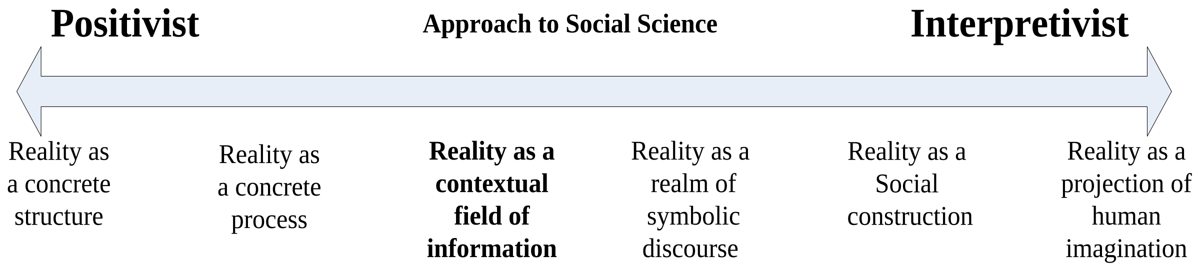

Positivist
Approach to Social Science
Interpretivist
Reality as a concrete structure
Reality as a concrete process
Reality as a contextual field of information
Reality as a realm of symbolic discourse
Reality as a Social construction
Reality as a projection of human imagination

Figure 1.5: Continuum of Core Ontological Assumptions (Source: Collis & Hussey, 2009)

As illustrated above, the positivist and interpretivist approaches are two extreme research paradigms, with several approaches combining elements from these two extremes along this continuum. Collis and Hussey (2009), explain that few people operate purely within either the positivist or interpretivist paradigms. Using a combination of the elements allows one to take a broader and often complementary view of the research problem or issue (Collis & Hussey, 2009).

This study will lean toward an interpretivist paradigm which is strongly linked to qualitative methods of data collection. The qualitative research method puts emphasis on understanding the setting of the phenomenon rather than the measurement of the phenomenon. According to Collis and Hussey (2009) this type of research involves an inductive process with a view to providing an interpretive understanding of social phenomena within a particular context (Collis & Hussey, 2009). In this case, the researcher begins with specific observations, or formulated research questions, from which patterns are identified. This leads to general conclusions or theories. In this study, the phenomena under investigation is user trust in cloud computing. Users of cloud computing provide the context, and the framework developed as the contribution of this study provides the conclusions.

The study will review current and available literature on cloud computing including the analysis of frameworks, cloud computing guidelines and other related articles. Current cloud computing trends and related studies will also be investigated.

1.6.2. Research Methodology

The research methodology is seen as the approach used in the research process. It also encompasses a body of methods that will be used in the research process (Collis & Hussey, 2009). Hofstee (2006) describes the research methodology as the blue print that explains how the researcher arrived at a conclusion and it should give a pictorial view of the steps followed.

This research project made use of the Design Science guidelines, leading towards the development of the proposed framework. Design Science is a problem solving paradigm which seeks to create innovations that define the ideas, practices, technical capabilities and products through which the analysis, design, implementation, management, and use of information systems (IS) can be effectively and efficiently accomplished (Hevner, *et al.*, 2004).

According to Hevner, *et al.* (2004) the Design Science paradigm consists of seven guidelines which must be considered to effectively utilise this research methodology. These guidelines are shown and briefly described in Table 1.1 below.

Table 1.1: Design Science Guidelines (Source: Hevner, March, Park, & Ram, 2004)

Design Science Guidelines	
Guideline	**Description**
Guideline 1: Design as an Artefact	Design Science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of Design Science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective Design Science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design Science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.
Guideline 6: Design as a Search Process	The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design Science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

For this study these guidelines where applied as described below:

1. *Design as an Artefact*: This study proposed a framework that can be used by users to assess the trustworthiness of cloud computing applications; and therefore enhance user trust in cloud computing applications.
2. *Problem Relevance*: The study identified a lack of user trust in cloud computing as the main problem of this research project. This study therefore focused particularly on proposing a framework to overcome this concern.
3. *Design Evaluation*: The research framework was evaluated using expert review. The experts were selected based on their expertise in cloud computing.
4. *Research Contributions*: The contribution of this project is the framework which provides users a means of assessing and evaluating the trustworthiness of cloud computing applications. This in turn leads to enhanced trust and improved adoption rates. This is an important contribution as no such framework exists at present.
5. *Research Rigor*: Valid data gathering and analysis techniques were used to investigate the research problem and propose the framework. These methods are described in detail in Chapter 5.
6. *Design as a Search Process*: The proposed framework was developed from related literature and empirical findings from the questionnaire. The comments and recommendations from the expert reviews on the proposed framework were used to refine the framework.
7. *Communication of Research*: This study has produced two publications in the form of peer reviewed conference papers. These papers are included in Appendix B and C.

1.6.2.1. Data Collection Methods

The data collection techniques that were used in this study include web-based questionnaires and expert reviews. The questionnaires were distributed electronically to selected cloud computing users and potential users. The research instrument was derived based on the literature reviewed and is included as Appendix D. This will be the primary data collection for this research project. A pilot study was conducted in order to test the adequacy of this research instrument, and where necessary changes were made.

Experts reviews were used to refine and verify the framework developed as a result of the literature review and questionnaire. Skulmoski, Hartman, and Krahn (2007) explain that the necessary information is gathered through a series of data collection and analysis techniques interspersed with feedback. The data collected for this study was analysed using the methods outlined below.

1.6.2.2. Data Analysis Methods

All fieldwork concludes in the analysis and interpretation of some set of data be it quantitative questionnaire data; experimental recordings; historical and literary texts; qualitative transcripts; or discursive data (Mouton, 2005). Mouton (2005) goes further to say that analysis involves breaking up data into manageable themes, patterns, trends and relationships. The aim of analysis is to understand the different constitutive elements of the data through an assessment of the relationships between concepts, constructs or variables, and to see whether there are any patterns or trends that can be identified or isolated, or to establish themes in the data.

The data may be gathered and thoroughly examined through deductive or inductive strategies. The approach for this research will be based on inductive reasoning. In this case, the researcher begins with specific observations, or formulated research questions, from which patterns are identified. This leads to general conclusions or theories. Analysis of the data collected from the questionnaires was done using descriptive statistics and pattern matching. Recommendations from the expert review were taken into consideration in the refinement of the proposed framework.

1.6.2.3. Sample and Population

The basic idea of sampling is that by selecting some of the elements in a population, conclusions may be drawn about the entire population (Cooper & Schindler, 2006). For this study the random sampling method was applied, whereby the population group was randomly selected to fit the purpose of this study.

A random sample of 100 commerce students from a higher education institution was selected for this study. The commerce students were considered to be appropriate as they are viewed as potential users of cloud computing services for personal and business use. They would therefore champion the widespread use of cloud computing. A total of 10 experts in cloud computing adoption and use participated in the refinement of the research framework.

1.7. Delimitation of the Study

For the purpose of this research project, the study of trust management has been narrowed and limited to the exploitation of user trust in the adoption and use of cloud computing applications. The effects of trust in cloud computing was considered only for the impact that it has on the user's intention to adopt and use cloud computing applications. The study was only limited to cloud computing users in South Africa. The next section describes the ethics that were considered for this study.

1.8. Ethical Considerations

An ethical clearance certificate for this research project was obtained from the University of Fort Hare (UFH) Ethics Committee (included in Appendix A). The other ethical considerations that the researcher followed in this study included informed consent, confidentiality, anonymity and no exploitation of respondents. The names of organisations and the individual respondents are not mentioned. The questionnaires were conducted with willing respondents and in all cases formal consent from the various individuals was obtained before the questionnaire was conducted.

1.9. Outline of Dissertation Chapters

The chapters of this dissertation will be arranged as shown in Figure 1.6.

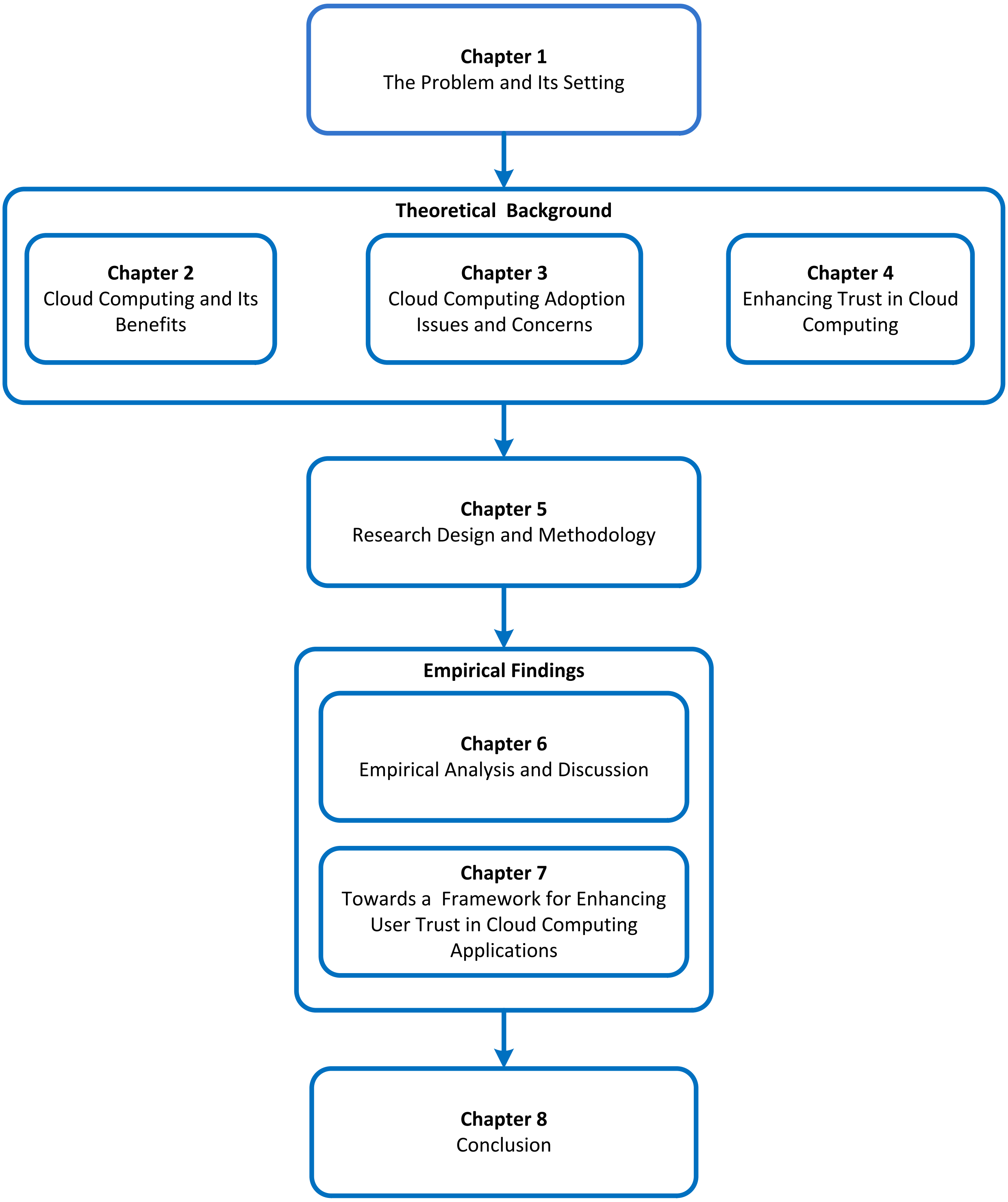
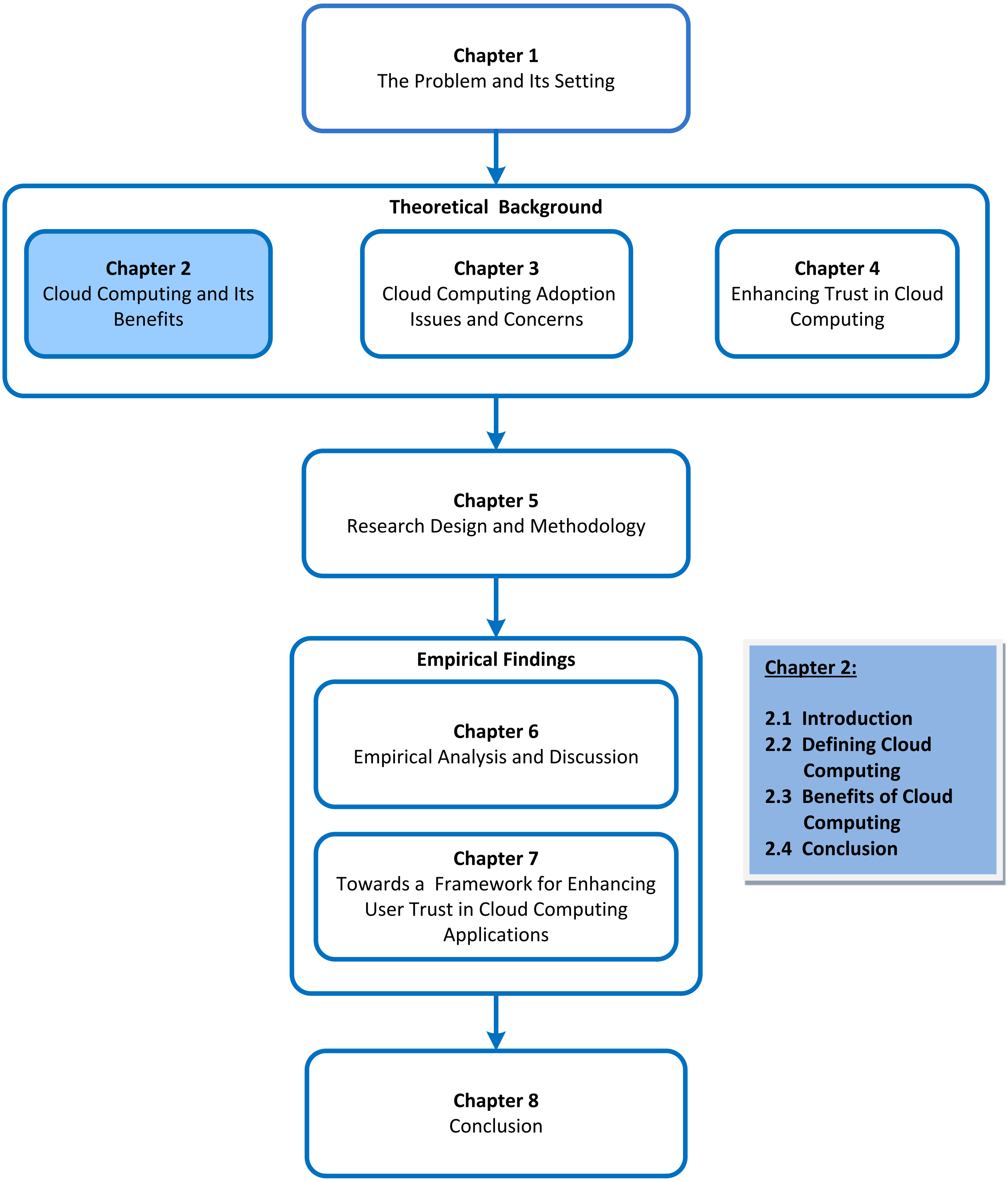

Chapter 1
The Problem and Its Setting
Theoretical Background
Chapter 2
Cloud Computing and Its Benefits
Chapter 3
Cloud Computing Adoption Issues and Concerns
Chapter 4
Enhancing Trust in Cloud Computing
Chapter 5
Research Design and Methodology
Empirical Findings
Chapter 6
Empirical Analysis and Discussion
Chapter 7
Towards a Framework for Enhancing User Trust in Cloud Computing Applications
Chapter 8
Conclusion

Figure 1.6: Dissertation Chapter Outline

Chapter 1 is the introduction chapter which presents the research problem and its setting. It is followed by the literature review in Chapter 2, Chapter 3 and Chapter 4, which provides a theoretical background of the key themes of this research, specifically trust, adoption and cloud computing. Chapter 5 describes the research design and methodology employed for this study. Chapter 6 of this research study details an analysis of the empirical findings. Chapter 7 outlines the contribution of this research project in the form of a proposed framework for enhancing user trust in cloud computing adoption. The study concludes with the summary, conclusions and recommendations for future research in Chapter 8.

Chapter 2:

Cloud Computing and Its Benefits


Chapter 1
The Problem and Its Setting
Theoretical Background
Chapter 2
Cloud Computing and Its Benefits
Chapter 3
Cloud Computing Adoption Issues and Concerns
Chapter 4
Enhancing Trust in Cloud Computing
Chapter 5
Research Design and Methodology
Empirical Findings
Chapter 6
Empirical Analysis and Discussion
Chapter 7
Towards a Framework for Enhancing User Trust in Cloud Computing Applications
Chapter 8
Conclusion

Chapter 2:

2.1. Introduction

According to ISACA (2009), cloud computing offers the possibility of high reward to its users in terms of containment of costs, agility and provisioning of speed. This is due to the opportunity to decouple their information technology (IT) needs and infrastructure. It also offers users long-term IT savings by reducing infrastructure costs and using pay-for-service models (ISACA, 2009). Additionally, by moving IT services to cloud computing users have the advantage of using services in an on-demand model with less up-front capital expenditure required. This allows businesses to have increased flexibility with new IT services.

However, besides the various reasons and advantages it offers to users, cloud computing, as a new initiative, can also bring the potential for high risk. This is the reason why most users are still reluctant to trust cloud computing and switch from their traditional means of computing. Lovell (2010) states that many users that are considering adopting cloud computing raise concerns over security and the trust they have in data being stored and accessed via the Internet.

Chapter 1 of this research project identified the central problem for this study as a lack of user trust in cloud computing which is the main barrier to widespread adoption. Accordingly, in this research project the study of trust takes place within the context of cloud computing. Cloud computing has many definitions, each of which depends on the scope of what is being researched. Thus, to explain the context of this study, definitions of cloud computing from various sources have been compared in this chapter to provide the context for this study.

This chapter focuses on the definition and understanding of cloud computing in detail including its impact and the benefits of adopting cloud computing. This background information is necessary to provide insight into the context of this research project. In particular, the various types of cloud computing deployment and delivery models and the benefits of adopting and using cloud computing are described in this chapter. This chapter will begin by defining and explaining cloud computing. The different types of cloud computing will be discussed according to the different deployment and delivery models for cloud computing which users can adopt and use to their benefit. The various benefits of cloud computing are also discussed in this chapter.

2.2. Defining Cloud Computing

Cloud computing, which is the focus of this research project, is still considered to be a new technology in the business world, therefore minimal academic research has been done on enhancing trust in cloud computing (Nyoni & Piderit, 2012). Several scholars and researchers have put forward academic definitions of cloud computing which are relevant to this study. Some of these definitions will be briefly discussed in this section in order to gain a clear understating of cloud computing.

Ragent and Leach (2010) define cloud computing as an Internet-based computing model which enables convenient, on-demand network access to shared resources, software and information which is provided to computers and other devices. Thus, it is a type of IT business trend that allows for the sharing of technological resources, other sophisticated services and business process-like utilities via the Internet. In the way it works, cloud computing provides an entirely new computing model as it converts a fixed-cost structure to a transactional pay-as-you-go fee-based service. Cloud computing is a technology where data storage is outsourced and stored in a secure environment (the cloud) and then provided as a service online, either by subscription or on a pay-on-demand basis to customers. In cloud computing, applications reside on network servers rather than on individual computers (Capers, 2010).

According to Sriram and Khajeh-Hosseini (2010), cloud computing is the latest effort in delivering known computing resources as a service. It can be seen as a relatively new trend in business, but it deserves attention because of the potential it has to deliver a variety of innovative services such as the management of infrastructure, software applications and complex business processes effectively and efficiently. Cloud computing can also be seen as a shift from the traditional method of computing as a product that is purchased, to computing as a service that is delivered to customers over the Internet from large data centres called “clouds” (Sriram & Khajeh-Hosseini, 2010).

LuitBiz (2010) further defines cloud computing as Internet-based computing whereby virtually shared servers provide software, infrastructure, platform devices and hosting to customers on a pay-as-you-go basis. Customers can then access these services available on cloud computing without any previous know-how in dealing with the resources involved (LuitBiz, 2010). This means that cloud computing is a business trend that can help users to concentrate more on their main business process rather than spending valuable resources trying to gain the IT needed. For individual users this means that they will not have to worry about the need to purchase individual resources such as personal software as these will be made available by cloud computing service providers on a cloud computing platform.

In the way that cloud computing is used in the business world it can be concluded that it is a technology whereby data and applications are hosted in an environment (the cloud) and then provided as a service online, either by subscription or on a pay-on-demand basis. This is confirmed by Capers (2010) who states that cloud computing applications reside on network servers rather than on individual computers. Additionally, Ragent and Leach (2010) describe cloud computing as an Internet-based computing model which enables convenient, on-demand network access to shared resources, software and information which is provided to computers and other devices.

The resources involved in cloud computing can include various applications and services, as well as the infrastructure on which they operate. Cloud computing users can then purchase these resources, infrastructure and services over the Internet on an as-needed basis and avoid the capital costs of software and hardware. Figure 2.1 shows how data and other applications are hosted online in a secure environment (the cloud) and accessed by users through the Internet. Users can use various devices such as laptops, phones or tablets to access applications made available by cloud computing service providers. As shown in Figure 2.1 users can also use cloud computing as a platform for data storage which can be accessed via personal servers. Users can also use cloud computing as an infrastructure where they can compute or store data and information. At the same time cloud computing can be used for back up purposes. A good example of this is the use of Dropbox for off-site backups of important data and information.

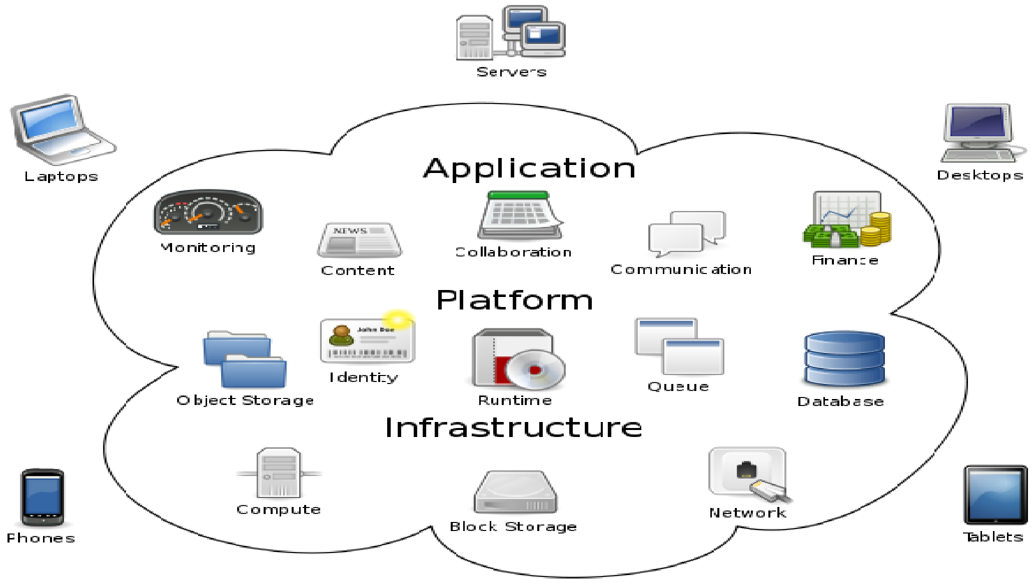


Figure 2.1: Cloud Computing (Source: Johnson, 2010)

In essence, cloud computing is a construct that allows users to access applications that actually reside at a secure location other than the user's computer or other Internet-connected device (Velte, Velte, & Elsenpeter, 2010). Additionally, LuitBiz (2010) explains that cloud computing users do not have to necessarily own the physical infrastructure; rather they rent the usage from a third party, namely the cloud computing service providers. This means the users consume the cloud computing resources as a service and only pay for the resources used.

In their definition and explanation of cloud computing Amrhein and Anderson (2009) point out that a definition of cloud computing is incomplete when there is no discussion or mention of the cloud computing models. Thus in their discussion of cloud computing they mention the various delivery and deployment models. These models help users to have a clearer understanding of cloud computing, how it works and the need for them to adopt it into their business processes (Amrhein & Anderson, 2009). The sections that follow describe the available deployment and delivery models and explain their relevancy to this study of user trust in cloud computing.

2.2.1. Deployment Models

In the IT industry there are four recognised deployment models for cloud computing, namely: Private, Public, Community and Hybrid (CSA, 2009). These are illustrated in Figure 2.2. Each deployment model is briefly described below. These clouds computing deployment infrastructures consist of services delivered through common centres and servers. Cloud computing applications often appear as single points of access for all a consumer's computing needs (IBM, 2010).

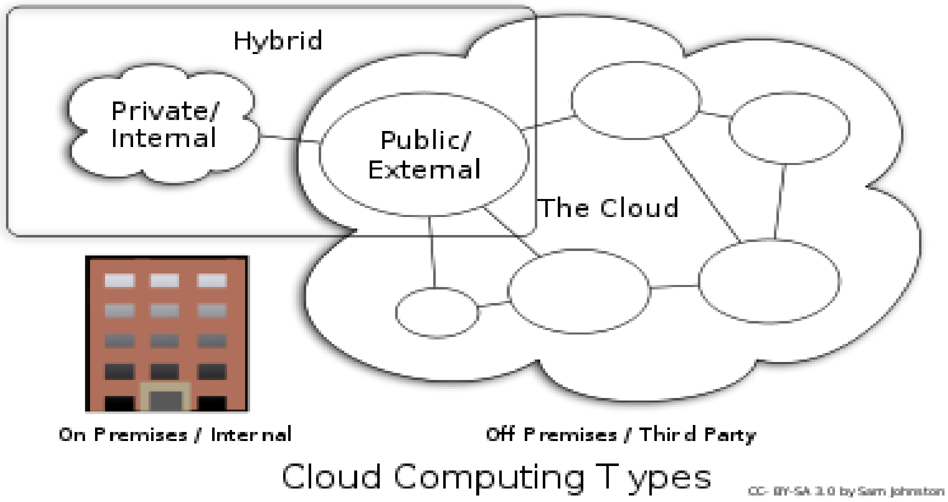


Figure 2.2: Cloud Computing Deployment Models (Source: Johnston, 2009)

2.2.1.1. Public/External Cloud

In a public cloud computing model, applications, storage and other resources are made available to the users by a service provider. The service providers own all infrastructure used in public cloud computing and the users can only access this type of cloud computing through the use of the Internet. A public cloud is also referred to as the external cloud, which refers to infrastructure made available to the general public through web browsers (Johnston, 2009).

These external, or public, clouds involve IT resources and services sold with cloud computing qualities such as self-service, pay-as-you-go billing, on-demand provisioning, and the appearance of unlimited scalability. They are accessed through web browsers or through Application Programming Interfaces (APIs) and offer nearly unlimited capacity on-demand at pay-per-use pricing, but with limited customer control (Cicso, 2009a).

According to LuitBiz (2010), a public cloud is traditional cloud computing in which resources are provided on a self-service basis over the Internet or from a third party off-site service provider. The public cloud refers primarily to third-party service providers who deliver services in a self-service model through the Internet. The third-party service provider divides up the resources and bills the users on a pay-as-you-use basis. Using the public cloud is fairly inexpensive for users as public cloud computing provides a flexible, cost-effective means to deploy solutions (Ahronovitz, Amrhein, Anderson, Arasan, Bartlett and Bruklis, 2010).

It should be noted, however, that the term “public” in cloud computing does not necessarily mean that services will be free. Additionally, public cloud computing does not mean that a user’s data is publicly visible to other users within the same cloud (Ahronovitz, et al., 2010). According to Ahronovitz, *et al.* (2010) public cloud computing service providers normally provide access and security mechanisms for their different users. The key concern for users of public cloud computing applications is the perceived loss of control over their data, which leads to trust concerns with the cloud computing application. This is the focus of this research project.

Public cloud computing occurs in an open environment as the architecture is built with the aim of creating an accessible business environment for the various users. Therefore there are concerns regarding security, privacy and service reliability that users should take into account before choosing a certain cloud computing deployment model (Ragent & Leach, 2010). Figure 2.3 shows a graphical representation of the public cloud, of which Amazon Elastic Compute Cloud (EC2), Google and Microsoft Azure are good examples. As shown in Figure 2.3, users can access public cloud computing services, such as database and storage services where they can store and retrieve their data and other services via the Internet.

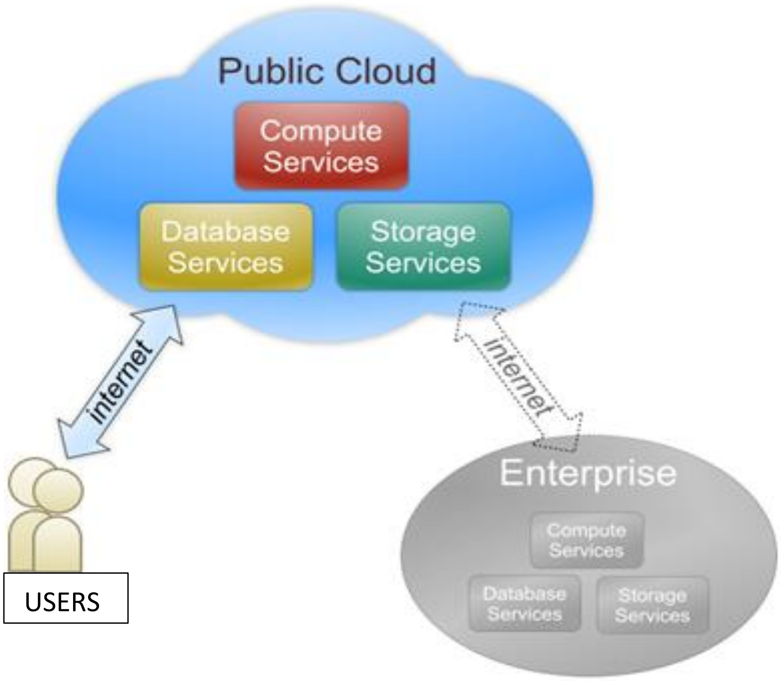


Figure 2.3: Public Cloud (Source: Ahronovitz, Amrhein, Anderson, Arasan, Bartlett and Bruklis, 2010)

2.2.1.2. Private/Internal Cloud

Private cloud computing is another deployment model for cloud computing services. It is also known as internal or corporate cloud computing as it is generally operated solely for a specified user or organisation. It can also be seen as a proprietary computing architecture that provides hosted services to a limited number of people behind a firewall. Thus, private cloud computing applications are perceived to be more secure than public cloud computing applications.

LuitBiz (2010) notes that private cloud computing involves deploying cloud computing services on private networks. According to Shimba (2010), the cloud computing resources in this model may be located within an organisation’s premises or offsite. Thus, in the private cloud computing model the user’s security and compliance requirements are not affected (Shimba, 2010). For many users this provides the ability to recover from failure and scalability.

Herzum (2006) explains private cloud computing as a term used to describe both a platform and a type of application that can be used for personal use. A private cloud computing platform dynamically provisions, configures, reconfigures, and de-provisions servers as needed and required by users (Herzum, 2006). Herzum (2006) also agrees with LuitBiz (2010) and maintains that in private cloud computing physical machines or virtual machines (VMs) are used as servers. Private clouds also include other computing resources such as storage network equipment, firewalls and other advanced security devices (Boss, Malladi, Quan, Legregni, & Hal, 2007).

Private cloud computing applications also use large data centres and servers that host Web applications and Web services. As with public cloud computing, the user has to have a reliable Internet connection and a standard browser to access and effectively utilise private cloud computing applications (Boss, *et al.*, 2007). Figure 2.4 shows the structural formation of the private cloud. In the example, the enterprise owns the private cloud as it is located within the organisation's premises.

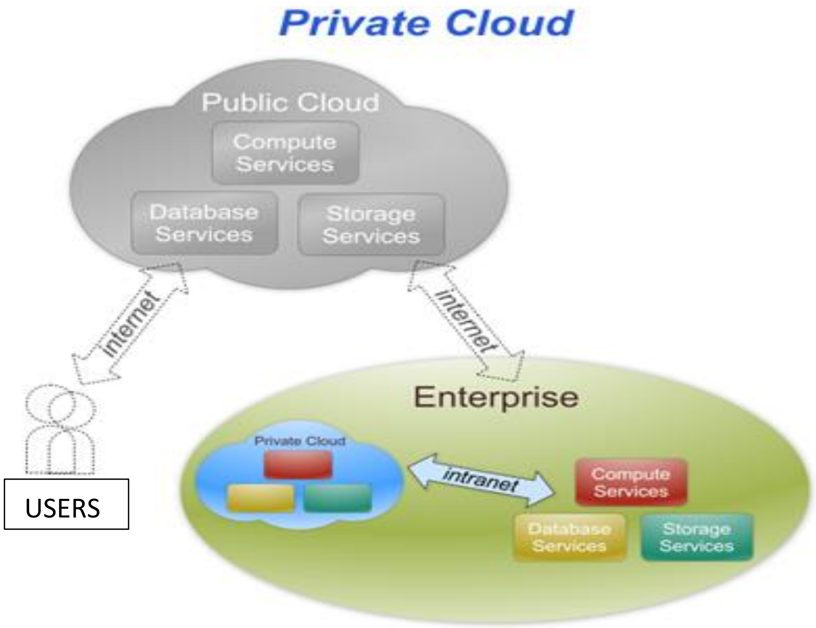


Figure 2.4: Private Cloud (Source: Ahronovitz, Amrhein, Anderson, Arasan, Bartlett and Bruklis, 2010)

The external user therefore has limited access in such a situation because the private cloud computing services are offered to a limited number of users behind the organisation's firewall. It should be noted however that the opposite is true if a specified user owns a private cloud for personal use. The individual user can set up a personal firewall and configure personal advanced security mechanisms to lock out unauthorised users.

2.2.1.3. Community Cloud

A community cloud is the model of cloud computing that has infrastructure shared among different users who share a common purpose. According to Ahronovitz, *et al.* (2010), a community cloud is the type of cloud that is controlled and used by a group of organisations or individuals that have shared interests such as specific security requirements or a common mission. This type of cloud computing may be managed by a third party and may be located on-premises or off-premises (Shimba, 2010). According to Shimba (2010), in this type of cloud computing both the public and the organisations or individual users in the community cloud have full access to the cloud computing services offered.

The community cloud is a more expensive option compared to public cloud computing as the operational costs are spread over fewer users than a public cloud computing application. However this comes with the benefit of offering higher levels of privacy, security and compliance (Baize, 2011). This is the type of cloud computing that most users are bound to invest more trust in and eventually adopt. However, due to the economic climate in South Africa few individuals are able to implement and use this type of cloud computing model. Figure 2.5 shows the community cloud.

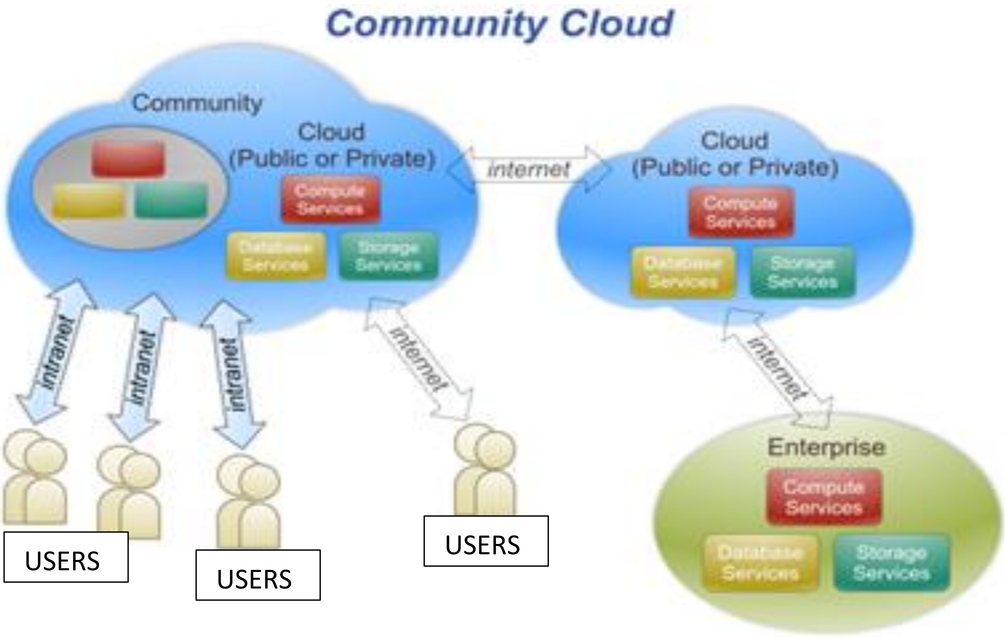


Figure 2.5: Community Cloud (Source: Ahronovitz, Amrhein, Anderson, Arasan, Bartlett and Bruklis, 2010)

As shown in Figure 2.5 the different individual users who are members of the community cloud share access to the data and applications in that particular cloud. Baize (2011) agrees with this as he further states that community cloud computing infrastructure is shared by several organisations or individuals and as such supports a specific community that has shared interests, requirements and concerns.

2.2.1.4. Hybrid Cloud

The hybrid cloud is the fourth deployment model that can be used to deliver cloud computing services. In this model, the cloud computing infrastructure is a composite of two or more types of cloud computing deployment models (private, community, or public) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability (Baize, 2011; CSA, 2009). LuitBiz (2010) describes the hybrid cloud as a combination of virtualised cloud computing servers used together with real physical hardware to provide a single common service to users. Figure 2.6 shows the structure of the Hybrid cloud.

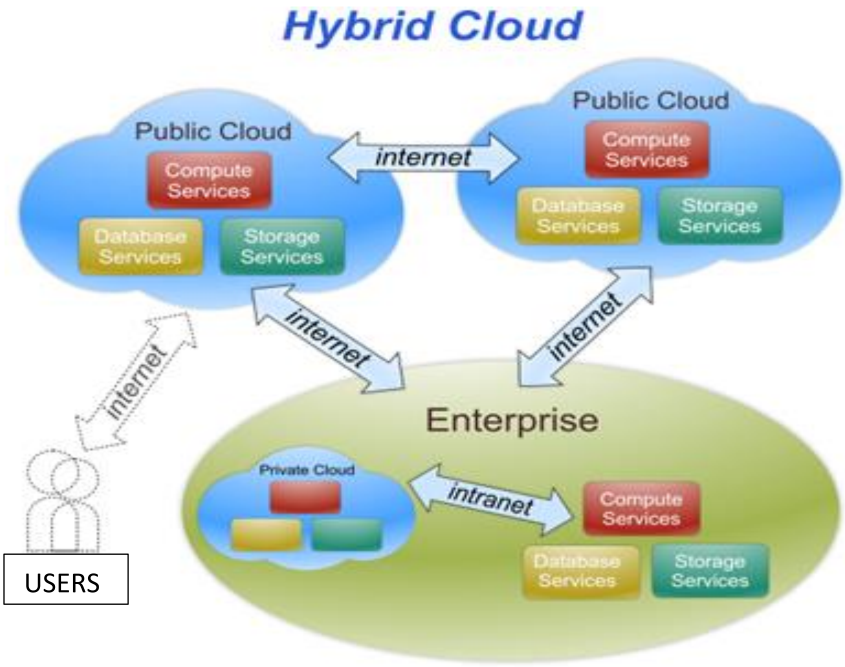


Figure 2.6: Hybrid Cloud (Source: Ahronovitz, Amrhein, Anderson, Arasan, Bartlett and Bruklis, 2010)

In this deployment model as shown in Figure 2.6, the service provider of the hybrid cloud manages all the cloud computing resources based on the consumer's terms, and the user has no knowledge as to what the service provider actually does in the cloud (Ahronovitz, et al., 2010). In this type of cloud the general public does not have access to the cloud, but the organisation uses infrastructure in both the public and private cloud (Shimba, 2010). It is important to note that the hybrid cloud should not be confused with the private cloud. A hybrid cloud uses both external (under the control of a service provider) and internal (under the control of the user) cloud computing capabilities. A private cloud on the other hand lets the enterprise choose and control the use of both types of resources (Cicso, 2009a).

2.2.1.5. Deployment Models Relevant To This Study

The above section describes the four cloud computing deployment model available for use by different users. It is important however to note that from these four deployment models only the public, private and the community models are relevant for this study. This is because these are the three deployment models in which end users (the general public) have direct access to these types of cloud models. The hybrid cloud deployment model as described by Shimba (2010) is mostly relevant for organisational use as in this type of cloud deployment model the general public does not have access to the cloud (Shimba, 2010). The aim of this study is to enhance user (general public) trust in cloud computing applications. Therefore the relevant deployment models are those in which users have access and can use. The next section below describes the different delivery models available in cloud computing namely; Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS) and the Data-as-a-Service (DaaS). The models will be described and explained briefly below.

2.2.2. Delivery Models

Through cloud computing the IT capacity of users can be adjusted quickly and easily to accommodate changes in demand, since users operate in a dynamic technological environment (LuitBiz, 2010). There are four common delivery models for offering cloud computing services. These models are: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS) and the Data-as-a-Service (DaaS) (CSA, 2009; Amrhein & Anderson, 2009). These four cloud computing delivery models will be briefly discussed below.

2.2.2.1. Software-as-a-Service (SaaS)

Amrhein and Anderson (2009) describe SaaS as the model in which the consumer uses an application, but does not control the operating system, hardware or network infrastructure on which it is running. The consumer in this particular service structure does not manage or control the underlying cloud computing infrastructure including network, servers, operating systems, storage, or even individual application capabilities. The only possible exception is when the user has limited control over user-specific application configuration settings (Muriithi & Kotzé, 2012).

Baize (2011) concurs with this and further explains that under this model a consumer uses the service provider’s software applications running on a cloud computing platform. The user uses the service provider’s applications and software through different client devices via a thin client interface such as a web browser. However, with the SaaS delivery model the users do not have control over the management of the infrastructure through which the applications are running (CSA, 2009). This therefore affects the levels of trust that the users have in the cloud computing applications that are delivered via this model, contributing to the existing lack of user trust in cloud computing.

In the SaaS model the service provider manages and controls the network, servers, operating systems, storage and even individual application capabilities (Baize, 2011). Shimba (2010) also states that in SaaS the user outsources all resources by renting remotely accessed services via the Internet. Popular examples of SaaS range from enterprise-level applications such as Salesforce.com's Customer Relationship Management (CRM) application; office productivity and collaboration tools such as Google Apps and Microsoft Office 365; and personal applications such as Gmail, Hotmail, TurboTax Online, Facebook and Twitter. Most of these are offered as free online services (Muriithi & Kotzé, 2012).

2.2.2.2. Platform-as-a-Service (PaaS)

According to CSA (2009) this model offers some control to the user which is related to the deployed applications but not to the cloud computing infrastructure. In this service offering the user has the ability to create applications or software using programming languages and tools supported by the service provider (Shimba, 2010). Baize (2011) further states that in the PaaS model the consumer has control over the deployed applications and possibly the application hosting environment configurations. According to Amrhein and Anderson (2009) and Muriithi and Kotze (2012), similar to PaaS, SaaS delivery is when the consumer controls the applications that run in the environment, but does not control the operating system, hardware or network infrastructure on which they are running. Typical examples of PaaS include Salesforce's Force.com development platform, Google Apps Engine, Amazon's Relational Database Services and Rackspace Cloud services.

The PaaS platform is typically an application framework (Ahronovitz, et al., 2010). This means that consumers use it as a hosting environment for their applications which offers some control to the user related to the deployed applications but not to the cloud computing infrastructure (CSA, 2009; Shimba, 2010). Even though this model offers some control to the users over deployd applications, it still raises security concerns as the users do not have control over the cloud computing infrastructure.

2.2.2.3. Infrastructure-as-a-Service (IaaS)

IaaS is the third delivery model for cloud computing. The IaaS model provides the consumer with the ability to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications (Baize, 2011). According to Shimba (2010) in this delivery model dedicated resources are offered to a single user and it does not allow sharing of dedicated resources to unknown third parties. This model provides the customer with the ability to deploy applications on the cloud computing infrastructure. Unlike the other models, in the IaaS model the consumer has control over operating systems, storage, deployed applications, and also has the control of select networking components such as the hosts' firewalls (Amrhein & Anderson, 2009). This model provides the users with the amount of control that is considered paramount to address the trust and security concerns that affect users when they are faced with the decision to adopt and use cloud computing applications.

However, according to Mell and Grance (2011) the customer does not have control over the infrastructure but may control the deployed applications and operating systems, storage and selected network components (Mell & Grance, 2011). According to Muriithi and Kotze (2012) the following provide good examples of cloud computing service providers that provide the IaaS service, namely: Amazon's EC2, Rackspace, Joyent, Terremark and RSAWeb. RSAWeb is an IaaS service provider operating in South Africa.

2.2.2.4. Data-as-a-Service (DaaS)

DaaS is fundamentally about the cloud computing services providers' ability to aggregate and manage user data and also allow the different users to have controlled access to their data sets through an API (Coporation, 2012). This is essentially a data management service offered by a service provider. This means that the database management services are made available to users through cloud computing applications deployed in any execution environment within the cloud computing platform.

According to DelphixCorp (2011), DaaS describes a cloud computing service provider's approach of making useful data available to users in a timely, secure and cost effective manner. Thus, the aim is to ensure that the users have broad, timely and self-service access to their data (DelphixCorp, 2011).

2.2.2.5. Delivery Models Relevant To This Study

Although all the delivery models do apply to cloud computing end users study will focus on the the SaaS and the Daas models which are more relevant to the study. These are the most relevant as they describe the delivery models that are mostly used by cloud computing end users in accessing various cloud computing applications. Examples of these were described in the discussions of these two relevant models above. The study focuses on enhancing user trust on cloud computing applications mostly used and delivered for end users. Now that cloud computing has been clearly defined, including deployment and delivery models, various advantages and benefits of using cloud computing will be described in the next section.

2.3. Benefits of Cloud Computing

There are numerous reasons why individual users are adopting cloud computing. Some users are pulled towards cloud computing by the obvious benefits it offers, while others are pushed to adopt it by the rapid change in technology and the need to use it. Cloud computing provides users with a way to increase capacity or add capabilities by investing in new infrastructure and new software (ISACA, 2009). Ultimately, cloud computing has revolutionised the way users access their various computing resources. Thus, the impact and potential benefits of using cloud computing services needs to be considered against the lack of trust in cloud computing. This is the central theme and the research problem investigated in this research project. However, the benefits offered by cloud computing are too significant to be ignored (Nyoni & Piderit, 2012).

According to ISACA (2009), cloud computing transforms business processes for users through means that were excessively expensive before the emergence of cloud computing. Through the adoption and use of cloud computing users can focus on the services they get, rather than being concerned about scalability of their IT infrastructure. Therefore, users should improve trust in cloud computing so as to maximise the benefits which include reduced cost and increased storage, flexibility and mobility (Callewaert & Luysterborg, 2011). The various benefits to individual users switching from traditional information and communication technologies (ICTs) and adopting cloud computing will be briefly discussed in the sections that follow. Figure 2.7 shows some of the most common cloud computing benefits.

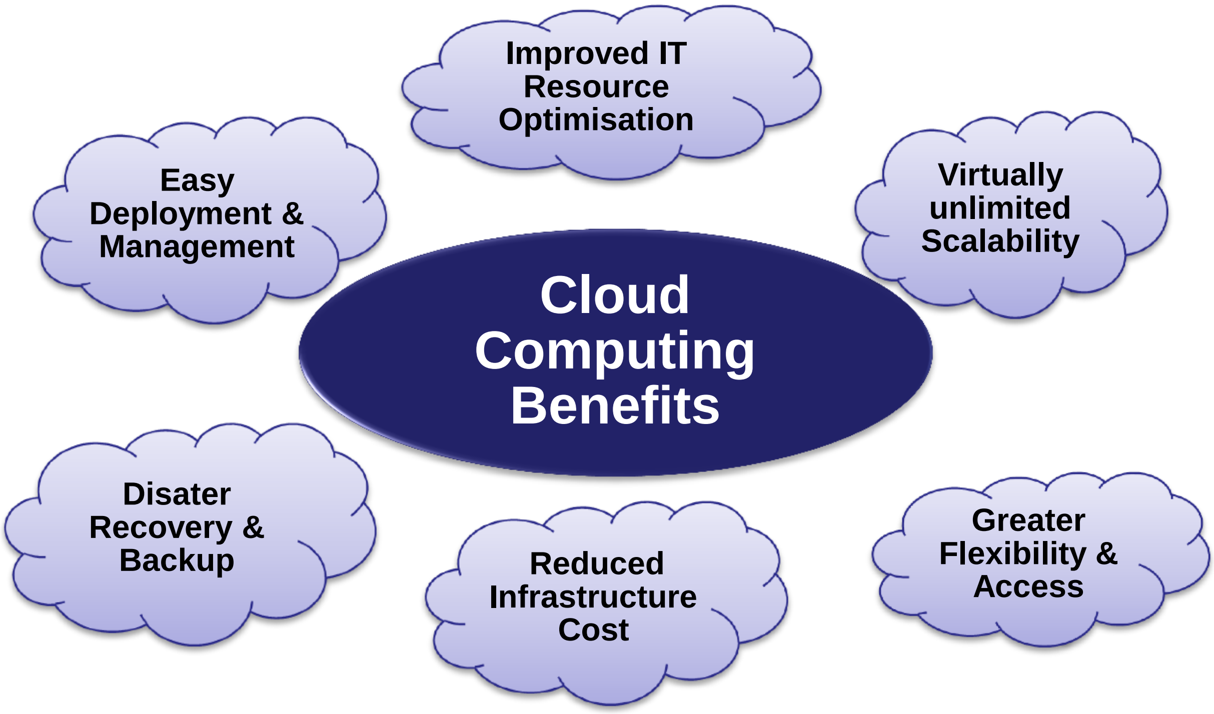

Improved IT Resource Optimisation
Easy Deployment & Management
Virtually unlimited Scalability
Cloud Computing Benefits
Disater Recovery & Backup
Reduced Infrastructure Cost
Greater Flexibility & Access

Figure 2.7: Cloud Computing Benefits

2.3.1. Improved Information Technology Resource Optimisation

Despite it being a relatively new technology, cloud computing allows for better IT resource optimisation, virtually unlimited scalability and greater flexibility (Callewaert & Luysterborg, 2011). According to Shimba (2010), cloud computing also offers users easier data monitoring, quick incident response and low costs to undertake various security measures. It also enables easier group collaboration and universal access to advanced computing resources. This is in accordance with Lovell (2010) who states that combining resources into large cloud computing platforms reduces costs and maximises utilisation by delivering resources only when they are needed.

Sharing computing power among multiple users can improve utilisation rates as servers are not left idle, which can reduce organisational and individual costs of accessing computing resources significantly while increasing the speed of application development (Lovell, 2010). By adopting cloud computing users will not have to be concerned about the over-provisioning for a service or under-provisioning of a service. This is because cloud computing offers users an option to only use the resources that they require at a particular point in time and only pay for what they use and need. This limits the underutilisation of computing resources.

2.3.2. Virtually Unlimited Scalability

ISACA (2009) states that cloud computing offers the option of scalability in terms of data storage without the severe financial commitments required for infrastructure purchase and maintenance. There is little to no upfront capital expenditure with cloud computing services such as Dropbox and Google Docs which offer users free storage as a service. Services and storage are available on-demand and are priced as a pay-as-you-go service (ISACA, 2009). Thus, scalability and flexibility are highly valuable advantages offered by cloud computing, allowing customers to react quickly to changing IT needs (Lovell, 2010). This involves adding or subtracting capacity as and when required and responding to real rather than projected requirements.

Another advantage is that cloud computing follows a utility model in which service costs are based on actual consumption. Customers benefit from greater elasticity of resources without paying a premium for large-scale usage (Lovell, 2010). LuitBiz (2010) agrees with Lovell (2010), pointing out that increased flexibility and market agility help as the quick deployment mode of cloud computing increases the ability to re-provision resources rapidly as needed.

Cloud computing users can benefit from the economies of scale enjoyed by service providers, who typically use very large-scale data centres operating at much higher efficiency levels, and multi-tenant architecture to share resources between many different users. In this model of IT provisioning, cloud computing then allows service providers to pass on savings to their customers (Lovell, 2010). By exploiting massive economies of scale, cloud computing service providers are able to offer some applications either at very low subscription rates or for free. For instance, Salesforce.com’s CRM subscriptions start from as low as R50 per user per month, while at the same time Gmail and Dropbox are offered as free online services (Muriithi & Kotzé, 2012).

2.3.3. Greater Flexibility and Access

Cloud computing services allow users to access applications and data securely from any location via an Internet connection (Lovell, 2010). This also means it is much easier to collaborate because both the application and data are stored in the cloud computing environment and multiple users can work together on the same project.

According to Lovell (2010), due to the anywhere-access nature of cloud computing, users can simply connect from different locations. Cloud computing also supports collaboration through the provision of an environment that supports global collaboration and knowledge sharing as well as group decision-making (Keane, 2011). Shared sites can be easily set up, replicated and removed as needed to meet the collaboration requirements of a given project. Additionally, flexible remote working amongst users can be enabled.

2.3.4. Reduced Infrastructure Costs

ISACA (2009) states that cloud computing carries with it the ability to offer users long-term IT savings, which includes reducing infrastructure costs and offering pay-for-service models as an option. According to Cisco (2009b), reduction in cost is a clear benefit of cloud computing. If users adopt cloud computing they can avoid spending large amounts of money on purchasing and installing new IT infrastructure, applications and software. Additionally, according to LuitBiz (2010) customers do not need to pay for excess resource capacity to meet fluctuating demand. Moreover, with cloud computing there is a reduction in upfront capital expenditure on hardware and software deployment. Keane (2011) also states that the cloud computing model provides users with infrastructure support and help desk services in case they encounter problems using the various cloud computing applications. This means that individual users will save on infrastructure costs as they will use those of the cloud computing service providers.

2.3.5. Easy Deployment and Management

As previously stated, by using cloud computing, users can take advantage of using services in an on-demand model. Cloud computing makes it relatively easy for IT solutions needed by the users to be deployed and quickly managed, maintained, patched and upgraded remotely by the service provider. Technical support on any cloud computing application can be provided to users around the clock by service providers for no extra charge (Lovell, 2010).

Cloud computing also eliminates the need to duplicate certain computer administrative skills related to setup, configuration and support for users. This puts the users at ease as the setup, configuration and management of cloud computing applications is done by the service providers. The users benefit from only using the application without having to be concerned about the technicalities behind the setup and use of such.

2.3.6. Disaster Recovery and Backup

Cloud computing service providers offer users an array of disaster recovery services which range from cloud computing backups, which allows the storage of important files from desktops and office networks within their data centres; to having ready-to-go desktops and services. It is essential for potential users to note that cloud computing service providers provide solutions that can be utilised in a disaster recovery scenario as well as for load-balancing of network traffic.

Whether it is a case of a natural disaster or heavy Internet traffic, cloud computing service providers have highlighted to users that they have the resiliency and capacity to ensure sustainability through an unexpected event (ISACA, 2009). This relates to the fact that all backup and recovery of user data in cloud computing becomes the responsibility of the service provider. This then gives users the confidence that they will recover their data and information from the cloud computing platform whenever they need it.

2.4. Conclusion

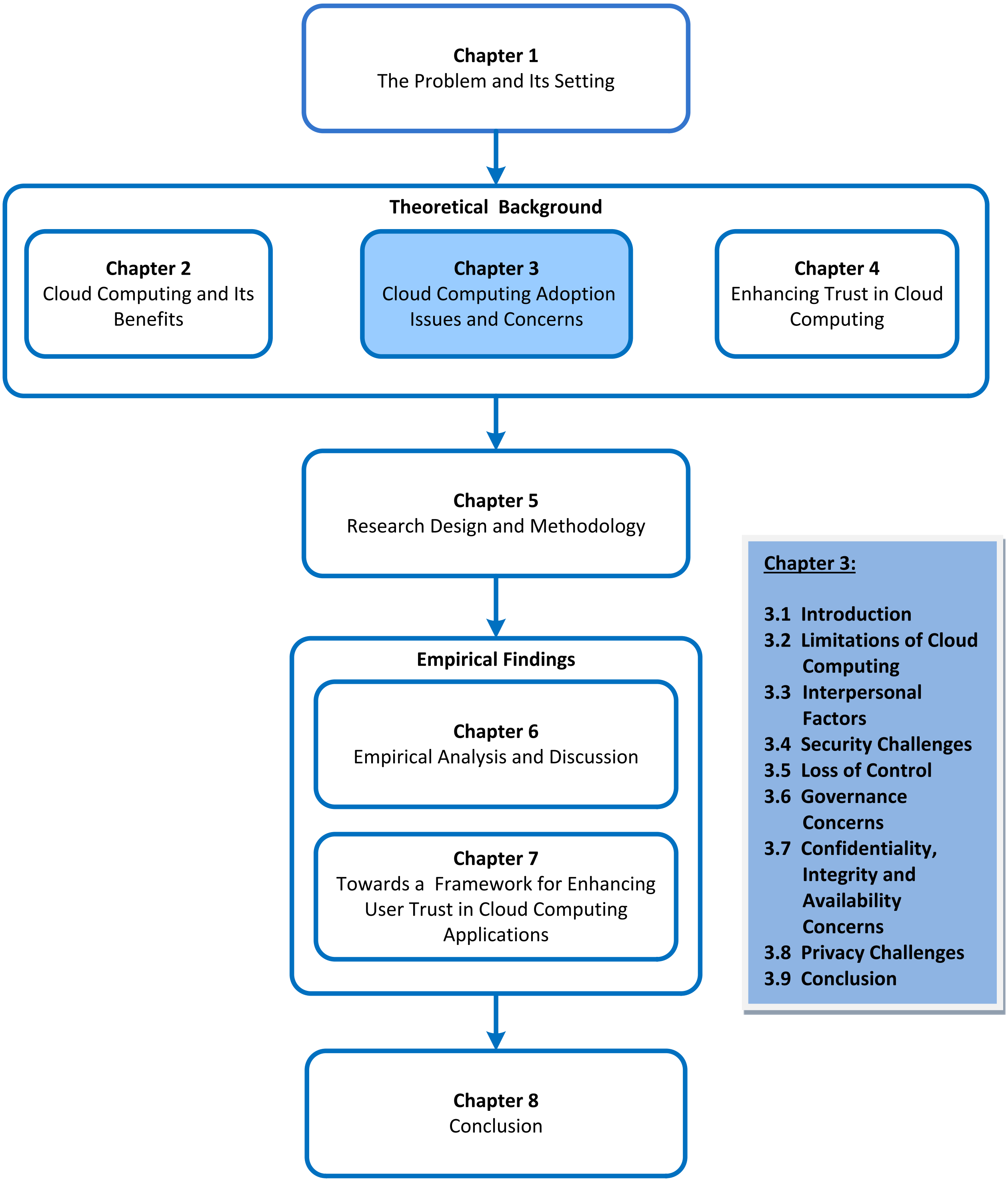
This chapter provided a clear definition of cloud computing and identified the different types of cloud computing deployment available for users to adopt and use namely: public, private, hybrid and community. The relevant delivery models for offering cloud computing services were also discussed in this chapter. These models are the SaaS, PaaS, IaaS and DaaS models.

It should be noted the successful adoption of cloud computing has the potential to provide users with the required modern day technologies and services. Cloud computing is a new technology which brings with it many benefits that might prove vital for users. This chapter identified the common benefits of cloud computing such as: IT resource optimisation, reduced infrastructural cost, easy deployment and management of applications and disaster recovery and backup to users of cloud computing applications.

However, the security risks of cloud computing that affect user trust should not be taken lightly as it has an adverse effect on the adoption process. This has resulted in the persistent lack of trust in cloud computing that inhibits users from the widespread adoption and use of cloud computing applications. The following section of this research project investigates different user trust issues and concerns surrounding cloud computing application adoption and widespread usage. These issues are central to the research project as they highlight the need to develop a cloud computing framework to assist users to evaluate a cloud computing service before they make use of it.

Chapter 3:

Cloud Computing Adoption Issues and Concerns



Chapter 1
The Problem and Its Setting

Theoretical Background

Chapter 2
Cloud Computing and Its Benefits

Chapter 3
Cloud Computing Adoption Issues and Concerns

Chapter 4
Enhancing Trust in Cloud Computing

Chapter 5
Research Design and Methodology

Empirical Findings

Chapter 6
Empirical Analysis and Discussion

Chapter 7
Towards a Framework for Enhancing User Trust in Cloud Computing Applications

Chapter 8
Conclusion

Chapter 3:

3.1. Introduction

As described previously, cloud computing is still considered an emerging computing service paradigm. Just like any other service of this scale, complexity and uniqueness in the information and communication technology (ICT) industry there are fears, uncertainties, issues and concerns about the technology's maturity (Sultan, 2011). The perceived open nature of cloud computing raises security, privacy and trust concerns (Kumar, Sehgal, Chauhan, Gupta, & Diwakar, 2011). According to Shimba (2010) these security, privacy, legal and compliance challenges affect the level of trust that users have in cloud computing. These issues have to be addressed in order to enhance the levels of trust, and consequently use of cloud computing. However, securing computer systems has not been an easy task, and it is even harder for cloud computing which has multi-tenancy which further complicates these security challenges (Shimba, 2010).

This chapter is relevant to the research problem and a starting point to solving the problem as it describes the cloud computing issues and concerns that affect and hinder user trust in cloud computing applications. The chapter begins with a brief discussion of the identified cloud computing limitations that users might face when using cloud computing applications. The following sections then explain the various user cloud computing issues and concerns.

A number of varied factors contribute to the lack of trust in, and therefore adoption and use of, cloud computing services. This chapter discusses the limitations of cloud computing which affect the adoption and use of these services. Other challenges described in this chapter include interpersonal factors; security challenges; loss of control; governance concerns; confidentiality, integrity and availability concerns; and privacy challenges.

3.2. Limitations of Cloud Computing

Despite the clear benefits of cloud computing described in Chapter 2, it should be noted many users are reluctant to adopt and use cloud computing applications available to them. This has been attributed to trust and security concerns. According to Schiffman, Moyer and Vijayakumar (2010), users with sensitive, security-critical data needs are beginning to push back strongly against using cloud computing because of the lack of trust that they have when it comes to dealing with such technologies. Cloud computing service providers run their computations upon cloud computing provided virtual machine (VM) systems, but users are still worried that such host systems may not be able to protect their data from attack, ensure isolation of customer processing and load customer processing correctly (Schiffman, Moyer, & Vijayakumar, 2010).

Baize (2011) agrees with Schiffman, Moyer and Vijayakumar (2010) as he points to the fact that while cloud computing offers tremendous benefits in cost and agility, it breaks down some of the traditional means of ensuring security, visibility and control of infrastructure and data. It is clear that where there is a perceived loss of security and control there is a lack of trust. The lack of trust in cloud computing is slowing broader adoption of cloud computing services (Baize, 2011). Similarly, Bourne (2010) identified the main issue with non-cloud computing adopters as the lack of trust cloud computing. Thus security of sensitive data, uncertainty regarding the value proposition of cloud computing, and security contribute to this lack of trust in cloud computing.

Cloud computing service providers, security service providers, integrators and consultants all have roles to play, both independently and jointly, to develop a culture of trust in the adoption of cloud computing (Penn, 2010). It is important to note that if users do not have trust in cloud computing they are not likely to use it. Trust as a priority concern for most organisations indeed plays a crucial role in the cloud computing adoption decision.

Luhmann (1988) further explains that the introduction of a new system requires trust as a vital input condition in order to stimulate supportive activities in situations of uncertainty or risk should they occur. The presence of trust improves and ensures the successful use of cloud computing applications, while the lack of it results in inefficient and ineffective performance and use of the services offered by the cloud computing. This points to the criticality of ensuring trust in cloud computing applications in order to ensure the efficient and effective use of these applications. This is the research problem under investigation in this study.

3.3. Interpersonal Factors

According to Moorman, Deshpande and Zaltman (1993) system users with lower levels of experience and exposure to ICT are usually not willing to trust new systems because of their limited knowledge of the ICT. Experienced users, in contrast, have more experience, knowledge and confidence in dealing with ICT and thus are able to trust the use of the ICT. The same goes for the different users when it comes to cloud computing. Those users who are exposed to cloud computing have the confidence to trust it as compared to those with limited knowledge and experience.

For experienced users Avgerou, Ganzaroli, Poulymenakou and Reinhard (2007) argue that in order for ICTs such as cloud computing to be successfully adopted they have to be perceived useful, easy to use and secure by the users. This argument was based on the Technology

Acceptance Model (TAM) by Davis (1989). If the users do not personally view cloud computing to be useful for their needs and secure they are bound not to trust it and this bears a negative impact on the adoption process.

Foley, Alfonso and Ghani (2002) found that another interpersonal factor that affects user trust in ICT is the level of education that the users have in terms of ICTs. Low levels of education affect the level of trust that users have on adopted ICTs and therefore their intention to adopt. This is because they develop the feeling of incompetence which turns into a psychological barrier that decreases the trust an individual has or will have on new ICTs (Foley, Alfonso, & Ghani, 2002). The combination of a low level of education and a lack of trust makes it difficult for an individual to undertake any kind of training on how to effectively use the adopted ICT (Foley, Alfonso, & Ghani, 2002). Similarly, Kabbar and Crump (2009) argue that poor ICT literacy, lack of basic ICT information, inadequate ICT skills and the user’s background are factors that affect their adoption of cloud computing.

3.4. Security Challenges

Security challenges leads users to have limited trust in cloud computing services. Cloud computing is still an evolving paradigm that has incredible momentum but the unique characteristics of the platform intensify security and privacy challenges that surround the use of the applications (Joshi, Joshi, & Ahn, 2010). Shimba (2010) also alludes to this as he points out that the security challenges, vulnerabilities and threats facing cloud computing raises a sense of fear in the potential users of cloud computing. This therefore creates distrust and hinders the adoption of cloud computing.

Cloud computing security requires total situational awareness of the threats to the network, infrastructure and data. One of the biggest advantages to the use of cloud computing, namely, abstraction, is also its biggest security weakness (Krautheim, 2010). This is because security in cloud computing is often intangible and less visible, which inevitably creates a false sense of security about what is actually secured and controlled. Most of the security and privacy issues in cloud computing are caused by users’ lack of control over the physical infrastructure where their data is stored (Khajeh-Hosseini, Sommerville, & Sriram, 2010). However, security concerns have always been at the top of an ICT user’s concerns, and this is no different for cloud computing (Technologies, 2011).

Kumar, *et al.* (2011) also point out that the off-premises computing paradigm which characterises cloud computing has resulted in several concerns about the security of data, specifically integrity and confidentiality of data. These concerns arise because cloud computing service providers have complete control on the computing infrastructure that underpins the services. Processing data with a cloud computing service provider followed by communication over the Internet, increases data and information vulnerability. It also leads to risks such as unauthorised modification or deletion of data. Cloud computing therefore brings new challenges when it comes to application security of data in cloud computing (Ernst & Young, 2011). It should therefore not come as a surprise that most cloud computing service providers view security as one of the challenges they feel they must overcome in order to make current and prospective users more comfortable with adopting cloud computing (Technologies, 2011).

A major concern with the use of cloud computing is that services provided by service providers are not as secure as services controlled by the individual user (Callewaert, Robinson, & Blatman, 2009). According to Kumar, *et al.* (2011), cloud computing is perceived as insecure by nature. An important reason for this is the lack of control the individual user has over the computing resources. This is discussed further in the next section.

3.5. Loss of Control

Cloud computing users typically have no control over the cloud computing resources used and how their data is stored. All technical control is given to the service provider and there is an inherent risk of data exposure to third parties via the cloud computing platform or the cloud computing service provider (Kumar, *et al.*, 2011). According to Holbl (2011), users are conscious of the risk of relinquishing control of their data and storing sensitive data with an external cloud computing service provider. Sultan (2011) further states that users are likely to be cautious of surrendering control of their information to cloud computing service providers who can alter or disclose it without their knowledge or consent.

Most users feel that their data could be compromised by the cloud computing service provider and other users who are also customers with the same cloud computing service provider, if they can access it due to the open nature of cloud computing (Holbl, 2011). In addition to the lack of transparency on where and how the data is stored, there is also concern about how data is processed in cloud computing (Holbl, 2011).

Cloud computing users and potential users also see the risk of losing control when it comes to how and when to access their data that is stored using cloud computing. Holbl (2011) points out that cloud computing is still a service that has to be accessed remotely and this presents a problem as the connection between the cloud computing service providers and users may not be adequately protected. Loss of control of user's data is also threatened by denial of service attacks and network down time (Holbl, 2011). As cloud computing is a service provided over the Internet, therefore there has to be a constant Internet connection between the users and the cloud computing service provider. Kumar, *et al.* (2011) further state that cloud computing depends largely on the reliability of a secure telecommunications networks which assures and guarantees undisrupted operations for a cloud computing service provider.

Additionally, concerns also exist with regards to the control and deletion of data in the cloud computing application. It has proven difficult to delete all available copies of electronic materials, thus it is impossible to guarantee complete deletion of all user's copies of important and sensitive data. Therefore it is difficult for users to have overall control over the deletion the data they have deleted in the cloud computing environment (Holbl, 2011).

3.6. Governance Concerns

According to Buyya (2009), when it comes to cloud computing the main concerns with reference to governance is whether the service providers can identify and implement appropriate structures, processes and controls to ensure that there is effective information security governance within cloud computing. Governance in cloud computing requires users to ensure that there are proper mechanisms and processes across the information supply chain that covers cloud computing service providers, customers, other stakeholders, and supporting third parties to service providers (CSA, 2009).

It is the users who should ensure governance, particularly, because it is them that are at risk of having their data exposed and manipulated. However, most users are not aware of the factors they should be confirming are in place, thus, the framework proposed in Chapter 7 of this study is relevant. By using cloud computing services the user passes control to the service provider. This passing of control to the service provider results in loss of control over a number of issues which were described in the previous section. This in turn may affect the security posture of the user data and applications. It is therefore difficult for users to trust cloud computing (Shimba, 2010).

3.7. Confidentiality, Integrity and Availability Concerns

Confidentiality, integrity and availability are key concerns affecting user trust when it comes to cloud computing. As shown in Figure 3.1 below and the explanation that follows, the three factors are important user concerns when it comes to cloud computing adoption. Thus, they are important factors for this study and they will be further investigated in order to enhance user trust in cloud computing applications.

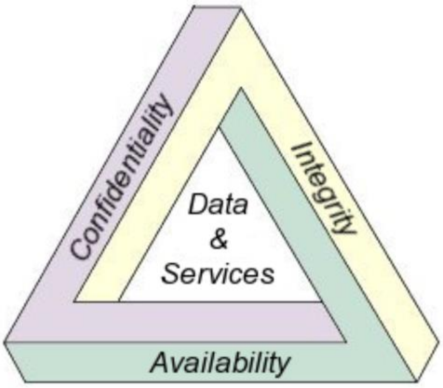


Figure 3.1: CIA Triad (Source: Steichen 2010)

3.7.1. Confidentiality

This refers to the issue of user's information and data which should only be disclosed to authorised parties. Confidentiality is the prevention of unauthorised disclosure of information. The service providers will have to make sure that user's data confidentiality is ensured by network security protocols, network authentication services and data encryption services (Johnson, 2010). Confidentiality is an important part of the trust relationship between the cloud computing service provider and users. The service provider's failure to ensure confidentiality will result in a loss of trust, damage to the service provider's reputation and legal implications (Wooley, 2011).

3.7.2. Intergrity

Information, either in transmission or in storage, must not be changed or destroyed accidentally or intentionally by unauthorised parties. It must remain in a consistent state. Therefore integrity is the guarantee by service providers that data received and data in transit will not be altered. This is ensured by firewall services, communication security and interference detection (Johnson, 2010).

3.7.3. Availability

This is the guarantee that information will be available to the consumer in a timely and uninterrupted manner when it is needed regardless of location of the data (Johnson, 2010). This means that the cloud computing infrastructure, the security controls, and the networks connecting the users and the cloud computing platform should always be functioning correctly.

3.8. Privacy Challenges

Privacy and security may represent the biggest risks to users when using cloud computing services (Li, Sedayao, Hahn-Steichen, Jimison, Spence, & Chahal, 2009). This is because these threaten some advantages of cloud computing such as flexibility, ease-of-use, service abstractions, and shared infrastructure. According to Li, *et al.* (2009), the issue of privacy introduces the concern that the use of cloud computing puts their information and intellectual property at risk.

Privacy is a core issue when it comes to the challenges that are currently threatening the widespread adoption of cloud computing. This includes the need to protect a user's identity information during integration, and all users' transaction histories when migrating to cloud computing (Takabi, Joshi, & Ahn, 2010). Many users are not yet comfortable storing their data in cloud computing applications on service provider infrastructure. According to Pearson (2009), privacy issues are central to users' concerns about the adoption of cloud computing, and unless mechanisms that develop user trust and address user concerns are implemented, the planned adoption processes will result in constant failure for cloud computing.

According to Takabi, Joshi and Ahn (2010), this might be the single greatest fear of potential cloud computing users. Migrating data to a shared infrastructure in the cloud computing environment means that private information faces increased risk of unauthorised access and exposure. Cloud computing service providers must assure their customers and provide a high degree of transparency into their operations and privacy assurance. Privacy-protection such as firewall and personalised access password mechanisms that limited unauthorised access must be implemented in all security solutions surrounding cloud computing.

Kumar, *et al.* (2011) state that the volumes of data that cloud computing service providers handle and the location of the cloud computing service providers makes it difficult for users to keep control of the information or data they entrust to service providers at all times. This is supplementary to the fact that privacy is an important issue for cloud computing user trust (Kumar, *et al.*, 2011).

Some users who deal with highly confidential and sensitive information do not trust the high volumes of data involved with cloud computing and are reluctant to use it in their everyday business. This is because entrusting this type of information to a cloud computing service provider increases the risk of uncontrolled dissemination of that information to unauthorised users using the same cloud computing platform.

Privacy and security are essential in all online computing environments, including cloud computing. Potential users are only willing to use cloud computing if the cloud computing service providers assure them that their data will remain private and secure. Therefore the ability of cloud computing service providers to provide a secure and private platform for its users is essential to develop trust amongst potential users (Microsoft, 2009).

According to Takabi, Joshi and Ahn (2010), this has proven to be a challenging task as cloud computing environments are multi-domain environments in which each domain can use different security and privacy mechanisms. For users to trust the privacy of such environments is not an easy task. This is because multi-tenancy and multi-domain environments result in the need for new solutions towards security and privacy in cloud computing (Khajeh-Hosseini, Sommerville, & Sriram, 2010).

Additionally, in a multi-tenant environment it may be very difficult for a cloud computing service provider to provide the level of isolation and associated guarantees that are possible with an environment dedicated to a single customer (Li, *et al.*, 2009). This then causes users not to trust and rely on the contractual controls provided by cloud computing service providers (Li, *et al*, 2009). In most cases these controls do not provide adequate protection when it comes to user data stored in cloud computing applications. It would therefore be difficult to use a public cloud for applications that handle controlled technologies due to the risk of potential compromises and concerns about privacy. It is essential to note that privacy is an important issue for cloud computing, both in terms of legal compliance and user trust, and needs to be considered at every phase of migrating to cloud computing (Pearson, 2009).

3.9. Conclusion

The adoption and use of new technology such as cloud computing for most users is still a delicate issue that is largely characterised by risk and uncertainty. This means high levels of user trust is needed to ensure the successful adoption of cloud computing and continued use thereafter. The introduction of a new system requires trust as a vital input condition in order to stimulate supportive activities in situations of uncertainty or risk should they occur.

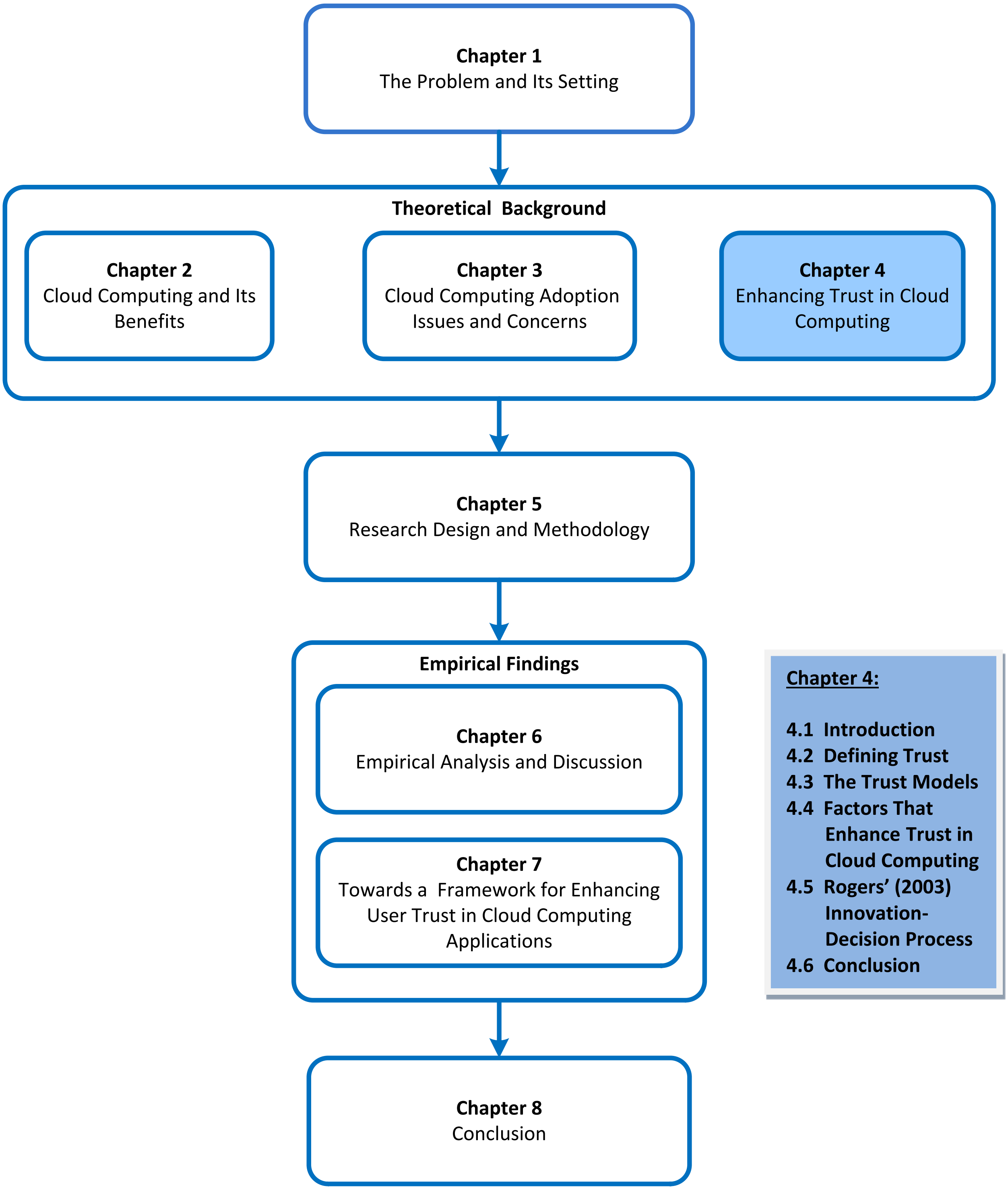
This chapter presented the main cloud computing adoption issues and concerns that affect user trust in cloud computing namely; interpersonal factors, security challenges, loss of control, governance concerns and privacy challenges. The presence of trust improves and ensures the successful adoption and use of cloud computing, while the lack of it results in inefficient and ineffective performance and use of the cloud computing services offered by the cloud computing service providers.

It is therefore important for users that before the adoption and use of cloud computing they consider the above mentioned factors as they have an impact in the cloud computing adoption process. These factors vary from individual, privacy and security factors. In addition, educational factors need to be considered to understand how they affect trust in cloud computing. It has been identified that the issues and concerns mentioned in this chapter have an impact on the lack of user trust in cloud computing applications which is the main problem being investigated in this research project.

Trust is therefore crucial as it plays a central role in helping users overcome perceptions of risk and insecurity (McKnight, Choudhury, & Kacmar, 2002). This is because trust in cloud computing will lead users to be more comfortable with cloud computing applications and use them. Therefore, trust is critical to both the users of cloud computing applications and the cloud computing service providers. Not only is trust critical, but it is also important as it aids users to overcome perceptions of uncertainty and risk and to engage in trust-related behaviours with cloud computing service providers (McKnight, Choudhury, & Kacmar, 2002). The next chapter (Chapter 4) will define and explain trust and the impact it has on the adoption and use of cloud computing applications.

Chapter 4:

Enhancing Trust in Cloud Computing



Chapter 1
The Problem and Its Setting

Theoretical Background

Chapter 2
Cloud Computing and Its Benefits

Chapter 3
Cloud Computing Adoption Issues and Concerns

Chapter 4
Enhancing Trust in Cloud Computing

Chapter 5
Research Design and Methodology

Empirical Findings

Chapter 6
Empirical Analysis and Discussion

Chapter 7
Towards a Framework for Enhancing User Trust in Cloud Computing Applications

Chapter 8
Conclusion

Chapter 4:

4.1 Introduction
4.2 Defining Trust
4.3 The Trust Models
4.4 Factors That Enhance Trust in Cloud Computing
4.5 Rogers' (2003) Innovation-Decision Process
4.6 Conclusion

4.1. Introduction

The perceived complex, unsecure nature of cloud computing applications, as highlighted in the previous chapter brings forth trust related issues and concerns amongst potential users. These users often hesitate to adopt and use cloud computing applications because of uncertainty and security issues that surround the use of the cloud computing. This hesitation is caused by the perceived risk of failing to effectively and efficiently use the various cloud computing services. Furthermore, there has been an increased interest in the pivotal role that user trust plays in facilitating widespread cloud computing adoption by potential users. This puts further emphasis on the importance of the study's objective into investigating the lack of user trust in cloud computing applications, moreover the significance of the study in attempting to enhance user trust in cloud computing to ensure adoption.

Related literature reviewed in previous chapters indicated that the lack of user trust in cloud computing applications hinders widespread adoption and at the same time leads to the inefficient and ineffective use of these applications in the post adoption phase. This then goes to show that the enhancement of user trust emerges as an essential element in cloud computing adoption and is too significant to be ignored. Therefore trust plays a central role in helping users overcome perceptions of risk and insecurity (McKnight, Choudhury, & Kacmar, 2002). This is because trust in cloud computing will lead users to be more comfortable with using cloud computing applications and services.

As highlighted in Chapter 1, the lack of trust in cloud computing hinders its successful adoption and widespread use. The previous chapters also highlighted the negative impact the lack of user trust in cloud computing has on their willingness to adopt and use cloud computing services. Therefore, trust proves to be critical to both the users and the cloud computing service providers. Trust is important as it aids users in overcoming perceptions of uncertainty and risk and in engaging in trust-related behaviours with cloud computing service providers (McKnight, Choudhury, & Kacmar, 2002).

Trust therefore plays an obviously role in the enhancement of user trust in cloud computing applications, and it is important to investigate it in more detail. Mayer, Davis and Schoorman (1995) point out that interest in investigating trust has increased, and research has established: a universal definition of trust, and an understanding of the relationship between trust, its determinants and its outcomes. These issues are examined in this chapter as a comprehensive understanding of these concerns is necessary for this study of enhancing user trust in cloud computing applications.

This chapter gives a brief definition of trust and the effect it has on the cloud computing adoption process. The relevance of trust models such as Mayer, Davis and Schoorman's (1995) Proposed Model of Trust and the Initial Trust Model by McKnight, Choudhury and Kacmar (2002) are then described in this chapter. A discussion of the factors that determine and enhance trust in cloud computing is also outlined in this chapter. In terms of establishing a framework for user decisions to adopt cloud computing, the innovation-decision process is then described for this purpose. This is further described in proceeding chapters.

4.2. Defining Trust

Trust has traditionally proven to be difficult to define and measure (Nyoni & Piderit, 2012). This has led to some researchers having to refer to the state of trust definitions as conceptual confusion (McKnight, Choudhury & Kacmar, 2002). Although some researchers have treated trust as a unitary concept, most however, agree that trust is more multidimensional than unitary and it takes various forms. Cofta (2007) agrees that trust escapes a clear definition; although it is essentially an important foundation to security. Furthermore, trust is the most important element of every transaction. Cofta (2007) further states that trust revolves around assurance and confidence that people, data, entities, information or processes will function and behave in expected ways. Trust is an important factor in new technology adoption, even though prior studies have paid little attention to its impact and role in the overall adoption process (Lee & Wan, 2010).

According to Lee and Wan (2010) previous studies reveal four different conceptualisations of trust. These conceptualisations view trust as:

1. a set of specific beliefs dealing primarily with the ability, benevolence, and integrity of another party;
2. a general belief that another party can be trusted;
3. an affect that reflects 'feelings'; or
4. a combination of these views.

On the other hand, Huang and Fox (2006) view trust as being a psychological state comprising of expectancy, belief and willingness to be vulnerable. Expectancy is when the trustor (in this case the cloud computing users) expect a specific behaviour of the trustee (cloud computing service providers) such as providing valid information or effectively performing cooperative actions. In terms of belief, the trustor, believes that expectation is true based on evidence of the trustee's competence and goodwill. In this case the belief expectancy applies to the cloud computing service provider. The trustor is willing to be vulnerable to that belief in a specific context where the information is used or the actions are applied (Huang & Fox, 2006).

Trust may be human to human, machine to machine, human to machine or machine to human. At a deeper level, trust might be regarded as a consequence of progress towards security or privacy objectives (Robinson, Lorenzo, Cave, & Starkey, 2010). According to Newell and Swan (2000), trust is viewed and defined in different ways, but there are two main issues about trust that seem to be central throughout the varied definitions of trust. These issues are that trust is about dealing with risk and uncertainty, and that trust is about accepting vulnerability. Similarly Luhmann (1988) asserts that trust tends to be needed in situations where there is risk and uncertainty.

Trust can also be defined as a feeling of being secure about an entity at a given time (Chen, Gillenson, & Sherrell, 2004). This refers to the users believing and trusting that a system or certain technology will perform according to its specifications. In the case of cloud computing it will mean that the users trust and believe that their data is secure with the service provider. This is the definition of trust that will be adopted for the purpose of this research project as it focuses on the trust that users have in cloud computing which is still a new technology. An additional concern central to this study is that technology trust is important because using technology especially new technology involves a number of risks (Lee & Wan, 2010).

According to Lee and Wan (2010), while most technology users take it for granted that technology will always function effectively and efficiently, there are others who view new technology with suspicion. These sets of users do not trust new technology and so they may not use it to complete work-related tasks. It is therefore essential to examine the importance of technology trust in the adoption of new technologies such as cloud computing. In order to establish a means of enhancing user trust in cloud computing, it is necessary to consider the various factors which affect trust. These factors are established in existing trust models as described in the next section.

4.3. The Trust Models

It is important to note that it is extremely difficult to establish and achieve at least a basic level of trust which is much needed when it comes to the use of cloud computing. The concerns discussed in Chapter 3, namely: interpersonal factors, security challenges, confidentiality, integrity, availability, loss of control, governance concerns and privacy challenges affect user trust in cloud computing in a negative manner. Several key trust models have emerged in literature in recent years which aim to ascertain trust enhancement strategies. The key trust models are discussed in this section, namely: Mayer, Davis and Schoorman’s (1995) Proposed Trust Model; McKnight, Choudhury and Kacmar’s (2002) Initial Trust Model; the Trusted Cloud Computing Platform (TCCP) proposed by Santos, Gummadi, and Rodrigues (2009); and the Private Virtual Infrastructure (PVI) proposed by Krautheim (2010).

4.3.1. Mayer, Davis and Schoorman’s (1995) Proposed Model of Trust

This trust model is based on literature research and developed within the management domain on issues relating to trust. Figure 4.1 shows this trust model that was proposed by Mayer, Davis and Schoorman (1995) to indicate the relationship between trust and trust behaviour. Mayer, Davis and Schoorman (1995) distinguish between trustor and trustee characteristics that foster a trusting relationship. In the cloud computing context, the user is the trustor and the service provider is the trustee. Thus, this model is appropriate for the context of user and service provider relationships in cloud computing.

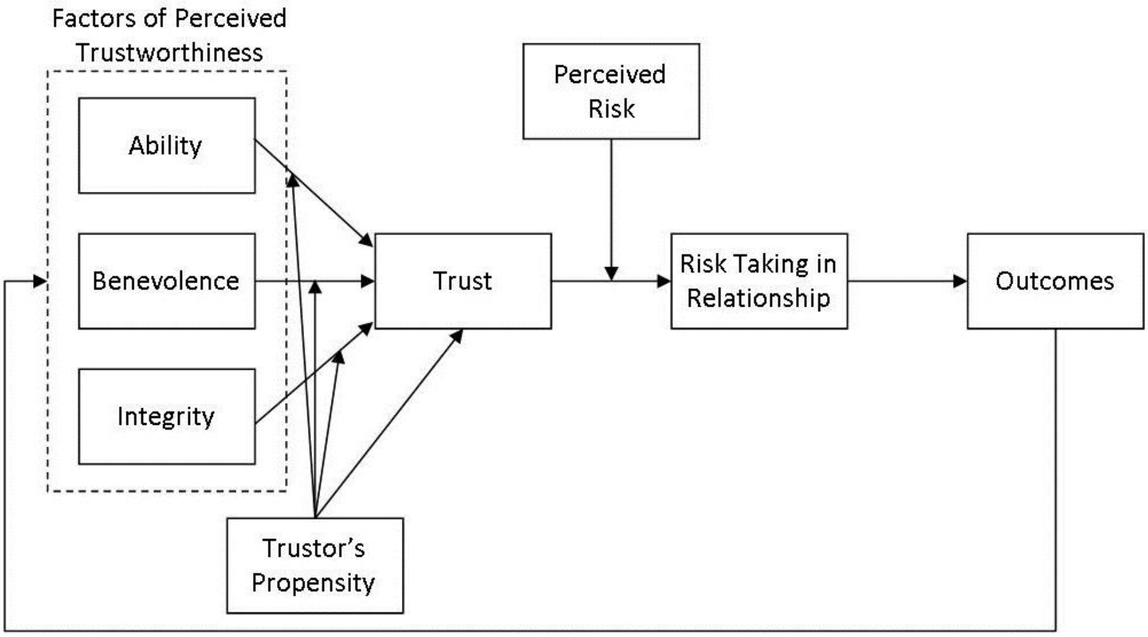


Figure 4.1: Proposed Model of Trust (Source: Mayer, Davis, & Schoorman, 1995)

Three determinants of a trustee's (the cloud computing service provider's) trustworthiness are proposed in this model, namely: ability, integrity and benevolence (Mayer, Davis, & Schoorman, 1995). These three characteristics form a foundation for the development of trust and are briefly explained below:

1. *Ability:* Ability is defined as the skills, competencies and characteristics that ensure the trustee has influence in the relationship (Mayer, Davis & Schoorman, 1995). It can be further defined as a collection of abilities, capabilities and characteristics that enable the trustee to have influence within a specific sphere (in this case in the cloud computing environment). A good example in the case of cloud computing service providers is the ability to provide its users with virtual data storage facilities such as Dropbox and Google Docs.

2. *Benevolence:* According to Mayer, Davis and Schoorman (1995) benevolence is defined as the extent to which the trustee is believed to want to act in the trustor's best interests. It refers to the extent to which one party or his proxy is believed to show some sensitivity to the needs of the other party and not take economic advantage of them (Mayer, Davis, & Schoorman, 1995). It relates more to the ethics and moral judgement of the cloud computing service providers that they will act in the trustor's (the users) best interests and not take economic advantage of the cloud computing users.

3. *Integrity:* Integrity is defined as a perception that the trustee prescribes to the principles that the trustor finds acceptable. It refers to a user's perception that the trustee adheres to a set of principles that the customer finds acceptable (Mayer, Davis, & Schoorman, 1995). In the cloud computing scenario, integrity would be based on the cloud computing service provider's attitude towards honouring his commitments to all the cloud computing users. That is to say the service provider will not tamper with the user's data in transit and storage, but will keep the data safe and secure.

The three characteristics complement each other in enhancing user trust and trustworthiness of cloud computing service provider, but perceptions of each tend to vary individually from one user to the other. It is important to note that a perceived deficiency of any of these characteristic has the potential to undermine trust in cloud computing applications (Mayer, Davis & Schoorman, 1995). The framework proposed in Chapter 7 of this study aims to address this phenomenon by providing a structured decision-making tool for all users.

The model also describes characteristics which apply to the trustor (in this case the cloud computing user). According to Mayer, Davis and Schoorman (1995) the trustor's (users) willingness to trust is referred to as the Trustor's Propensity. Some parties are more likely to be willing to trust than others. This personality trait can lead to a widespread expectation about the other party's trustworthiness in trusting relationships. Each individual user of cloud computing propensity to trust differs as it is based on an individual's willingness to trust others, in this case the cloud computing service provider.

The proposed model of trust by Mayer, Davis and Schoorman (1995) identifies the key determinants of trust which are significant for this research project. An important limitation to this proposed model is the fact that the model is largely based only on a literature survey and common sense (Rusman, Van Bruggen, & Valcke, 2009). However, these determinants have since been confirmed through empirical findings. Additionally, the proposed model of trust development developed by Mayer, Davis and Schoorman (1995) cannot be applicable in all scenarios that are related with the adoption and use of new technology. This is because different factors and determinants tend to affect individuals differently when they are faced with the decision to adopt new technologies like cloud computing.

4.3.2. McKnight, Choudhury and Kacmar's (2002) Initial Trust Model

The Initial Trust Model was proposed by McKnight, Choudhury and Kacmar (2002) in an electronic commerce (e-commerce) context to explain and predict customers' trust towards an e-vendor in an e-commerce context (Childerhouse, Hermiz, Mason-Jones, Popp, & Towill, 2003). This model deals with issues of trust and is fitting for this research project as it was proposed for an Information Technology (IT)-enabled trust relationship between two parties. This is similar to the user-service provider relationship in cloud computing.

According to Li, Valacich and Hess (2004) this trust model is one of the most cited models in literature that best explains initial trust. The McKnight, Choudhury and Kacmar (2002) Initial Trust Model is mentioned for this research project because it was derived from existing trust research in other disciplines and encompasses important constructs from other trust research models such as the Mayer, Davis and Schoorman (1995) trust model. The Initial Trust Model is shown in Figure 4.2.

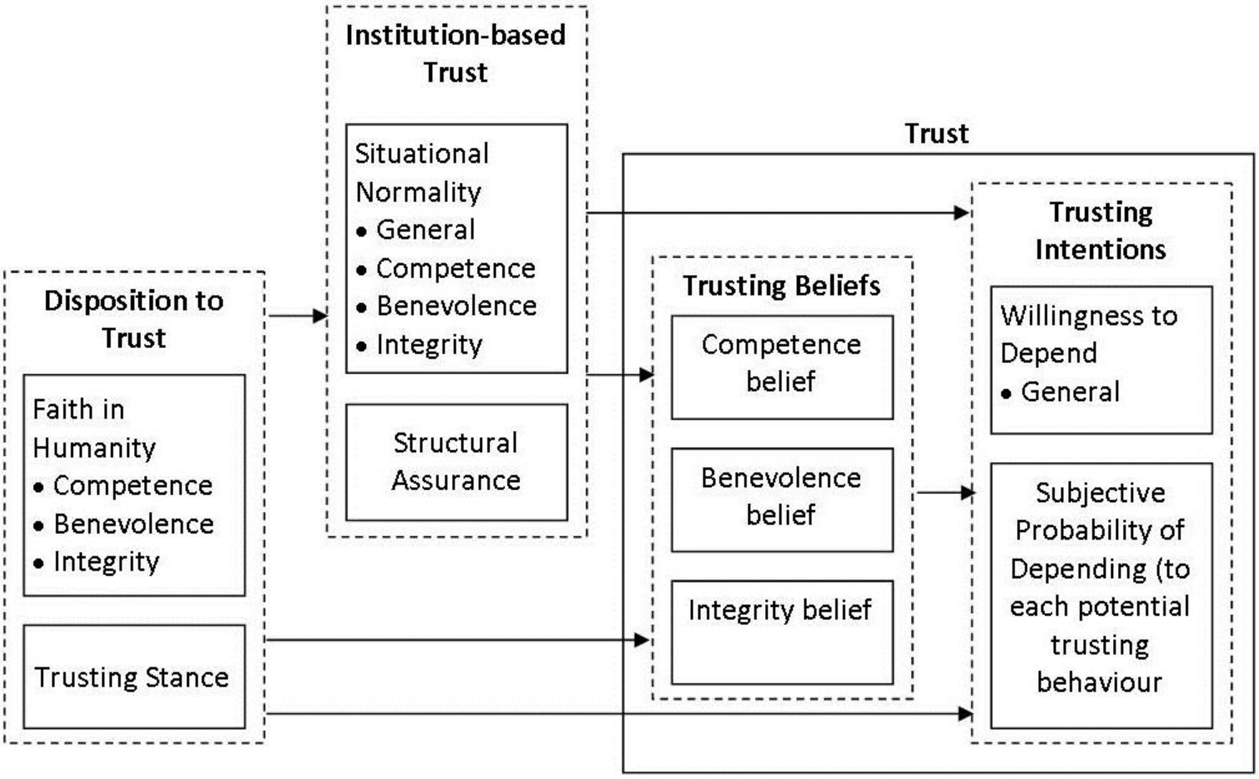


Figure 4.2: Initial Trust Model (Source: McKnight, Choudhury, & Kacmar, 2002)

According to Li, Valacich and Hess (2004), initial trust is defined as trust in an unfamiliar object, such as when dealing with a relationship in which the trusting subject does not have credible, meaningful experience, knowledge, or any affective bonds with, the trusting object. Thus, the initial trust referred to is the trust an individual user places in a system before ever using it. Thus, there are no historical interactions on which to make this decision. In the McKnight, Choudhury and Kacmar (2002) Initial Trust Model the concept of trust is divided in two components, namely Trusting Beliefs and Trusting Intention.

According to Li, Valacich and Hess (2004), the trusting beliefs component refers to the trustor's belief and perception that the trustee's object has attributes that are beneficial to the trustor's subject. This component is represented in the model by three categories of beliefs, namely:

1. *Competence*: Competence refers to the belief that the trustee has the power to fulfil transactional obligations (Shankar, Urban, & Sultan, 2002). This is the trustee's ability to do what the trustor needs (McKnight, Choudhury, & Kacmar, 2002). Shankar, Urban and Sultan (2002), go on to describe competence, as, "the belief in the sellers (trustee) expertise to do the job effectively." It is necessary that the cloud computing service provider displays these characteristics of competence, as these characteristics can be sufficient to generate trust. The *competence* construct mentioned in the Initial Trust Model by McKnight, Choudhury and Kacmar (2002) is equivalent to the *ability* construct of the Mayer, Davis and Schoorman (1995) Model of Trust. The cloud computing service provider has to prove to the users that he has the capability and the power to render all the cloud computing service that are meant to be provide by a particular cloud computing application.

2. *Benevolence*: Similarly to the Mayer, Davis and Schoorman (1995) Model of Trust, the Initial Trust Model by McKnight, Choudhury and Kacmar (2002) includes *benevolence* as a trust construct. According to Shankar, Urban and Sultan (2002), benevolence refers to the expectations or assumptions of the trustor that the trustee will consistently act fairly, care for the trustor, and act in their best interest. Thus they will not take advantage of the trustor even if the opportunity arises. Li, Valacich and Hess (2004) explains benevolence as the trustee's motivation to act in the trustor's interests. Thus the users expectation that the cloud computing service provide will not use the information provided and stored in cloud computing applications by users to his advantage. The users expect the service provider to actually care for them and their data stored in the cloud, also acting in their best interest all the time.

3. *Integrity*: Similarly to the Mayer, Davis and Schoorman (1995) Model of Trust, the Initial Trust Model by McKnight, Choudhury and Kacmar (2002) includes *integrity* as a trust construct. According to Li, Valacich and Hess (2004) integrity is the trustee's honesty. It can also be seen as the belief of the trustor that the trustee makes good faith agreements and fulfils promises (Chervany & McKnight, 2001).In the cloud computing context this refers to the honour and reliability of the cloud

computing service provider when it comes agreements and arrangements made between the two parties. This translates to the acceptance and confidence on the users' side that the service provider will act in good faith when it comes to handling and dealing with their data.

The other aspect of trust in this model is Trusting Intentions which is determined by the trusting beliefs described above. This is defined as the trustor's willingness to depend on the trustee (Li, Valacich, & Hess, 2004), which is similar to the trustor's propensity described in the Mayer, Davis and Schoorman (1995) model. This is represented by two subcomponents:

1. *Willingness to Depend:* This is the trustor's willingness to be vulnerable when interacting with the trustee. This subcomponent is the same as the Mayer, Davis and Schoorman (1995) Trustor's Propensity which is the trustor's (users) willingness to trust the trustee. Both models seem to agree that when it comes to trust some parties are more likely to be willing to trust than others.
2. *Subjective Probability of Depending:* The perceived likelihood that the trustor will depend on the trustee. This is equivalent to trustworthiness component of the Mayer, Davis and Schoorman (1995) model with reference to the trustor's willingness to trust the trustee. This is based on the components of the trusting belief described previously.

McKnight, Choudhury and Kacmar (2002) also describe the precursors to the trusting beliefs and intentions, namely:

1. *Disposition to Trust:* This is the trustor's willingness to trust based on:
    a. *Faith in Humanity*: which is an assumption that each party is honest and dependable; and
    b. *Trusting Stance*: which refers to the belief that better outcomes result from dealing with other parties as if they are honest and dependable, regardless of the trustor's perception of the trustee's attributes.
2. *Institution-based Trust:* which is the belief in structural conditions that need to exist to improve the probability of a successful outcome in the relationship based on:
    a. *Structural assurance*: which is a belief that structures such as guarantees, regulations, legal recourse or procedures promote success in the relationship; and

b. *Situational Normality*: which refers to a belief that the environment in which the interaction occurs is in the necessary state to ensure success.

In the Initial Trust Model, it is important to note that institution-based trust is determined by the disposition to trust. That is to say both of these components, the institution-based trust and disposition to trust, are believed to directly influence trusting beliefs and trusting intention between parties. This again points to the individual user's propensity to trust being an important factor in establishing a trusting relationship. McKnight, Choudhury and Kacmar's (2002) model furthermore identifies accompanying components that are relevant to this research project.

Structural assurance is the additional component that needs special mention, as it points to the need to achieve a balance between trust and controls as a way of building trusting relationships. In this case the controls are seen as the perceived behavioural control, which is the user's perception on internal and external resources and constraints that might result from trusting the service provider. Again control may occur in the sense that if the trustor cannot obtain sufficient direct knowledge about the trustee, their perception of their level of control in the relationship will affect their willingness to trust (Li, Valacich, & Hess, 2004). In this model components relating to Trustor's Propensity and controls have emerged. Additionally, this model recognises the trust determinants, as well as the need to consider potential outcomes of user/service provider trusting relationships. These components hold significant value for this research project.

4.3.3. Santos, Gummadi and Rodrigues' (2009) Trusted Cloud Computing Platform (TCCP)

Proposed by Santos, Gummadi and Rodrigues (2009), the TCCP suggests the improvement of user trust in cloud computing through a means of verifying the confidentiality and integrity of the data and computation. According to Shimba (2010), the TCCP model addresses the problem of root level access to the insider. It also addresses the problem of a perceived lack of confidentiality and integrity for the Infrastructure-as-a-service (IaaS) delivery model of cloud computing services. It assumes that there is a trusted third party that monitors the transactions in the cloud computing platform.

Santos, Gummadi and Rodrigues (2009) proposed the TCCP after realising a clear need for a technical solution that guarantees the confidentiality and integrity of computation in a way that is verifiable by the users (Santos, Gummadi, & Rodrigues, 2009). Therefore this allows the users to gain trust in the services that the service providers are offering, leading them to adopt and continue using these services. According to Santos, Gummadi and Rodrigues (2009), the TCCP enables cloud computing service providers to provide a closed-box execution environment that guarantees confidential execution of users virtual machines (VMs).

Additionally, the TCCP allows users to check and verify with the service provider and determine whether or not the services being offered are secure before they use of them. This therefore creates a sense of trust if the users find that the services are secure for use, as the TCCP guarantees confidentiality, integrity and security of user's data. It also grants the user the opportunity to determine upfront whether or not the cloud computing service provider enforces these properties (Santos, Gummadi, & Rodrigues, 2009).

As shown in Figure 4.3, the TCCP includes two components: a *trusted virtual machine monitor* (TVMM), and a *trusted coordinator* (TC). According to Santos, Gummadi and Rodrigues (2009), the TVMM hosts the users' VMs and data, and also prevents restricted users from inspecting and modifying them. Furthermore, the TVMM protects its own integrity over time, and complies with the TCCP protocols. The TC manages the set of nodes that can run user VMs securely and maintain data confidentiality at the same time. The nodes are located within the security perimeter, and run the TVMM. Users can then verify whether a service offered on this platform is secure by attesting to the TC.

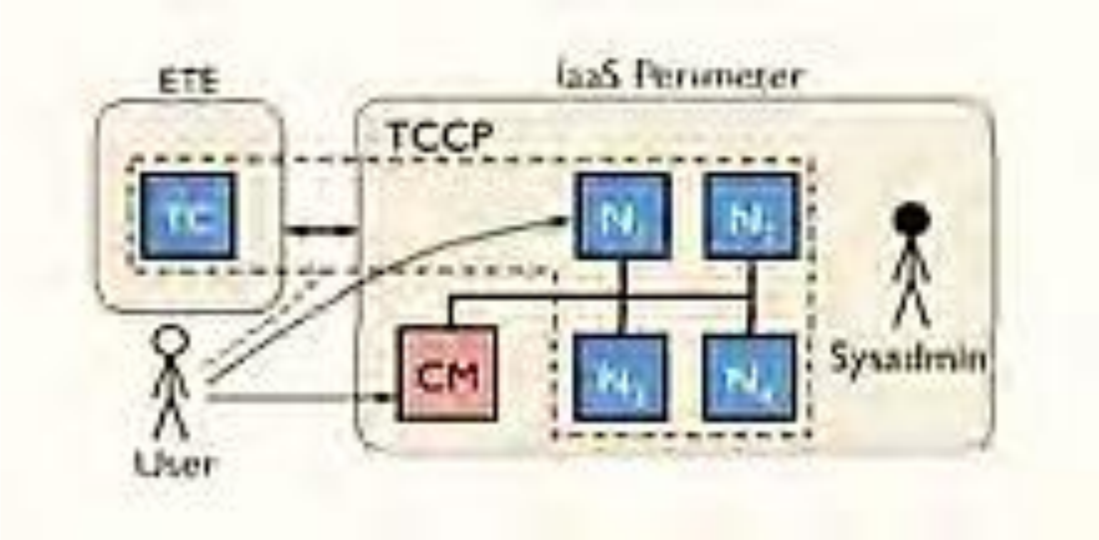


Figure 4.3: TCCP Architecture (Source: Santos, Gummadi & Rodrigues, 2009)

The limitation of this model, however, as identified by Shimba (2010), is that it only addresses one type of cloud computing delivery model, namely the IaaS. There is a possibility of single point of failure coupled with the possible increase in the attack surface. It also adds computation requirements and hence it may not be a cost effective method to be used (Shimba, 2010). The framework proposed in this study will improve on this aspect as it can be used to address the different types of cloud computing and the different delivery models used. The proposed framework in the study presents a cost effective, non-computation way that users can use to access the trustworthiness of cloud computing platforms.

4.3.4. Krautheim's (2010) Private Virtual Infrastructure (PVI)

According to Shimba (2010) this model addresses the problem of transparency whereby the service provider hides the internal security details from the customer. This hiding of the details results in mistrust. In order to enable the transparency collaboration between customer and service provider, a factory is used. The PVI model was proposed by Krautheim (2010) which suggests a synergistic relationship between the service provider and customer of cloud computing services which will ensure privacy and security.

Krautheim (2010) argues that this synergistic relationship provides an increased security attitude while allowing both parties to set security controls required to protect the infrastructure and data within the cloud computing platform (Krautheim, 2010). Shimba (2010) states that the aim of the PVI model is to enable effective cooperation between the cloud computing service provider and the customer to create a trusted system. This trusted system should enable separation of different users through their restricted PVI and give more control to the users as compared to the service providers. This in turn will improve trust in the use of cloud computing (Shimba, 2010).

Krautheim (2010) proposes the PVI as a new trust management and security model for cloud computing. The PVI shares the responsibility of security in cloud computing between the service provider and user, decreasing the risk of exposure to both. According to Krautheim (2010) the PVI datacentre is under the control of the information owner while the cloud computing material is under control of the service provider. In the setup a Locator Bot pre-measures the cloud computing platform for security properties, securely provisions the datacentre in the cloud computing environment, and provides situational awareness through continuous monitoring of the cloud computing platform security (Krautheim, 2010).

In this manner, according to Krautheim (2010), the PVI meets the goals of a shared security posture where all resources necessary for the virtual datacentre are securely isolated from the cloud computing platform (Krautheim, 2010). It provides secure provisioning of cloud computing resources by isolating the user's datacentre to operate in its own virtual domain. In this domain both parties must agree to share security information between them in the cloud computing environment to achieve situational awareness of the security at all times.

Krautheim (2010) states that each party has an active role to play to ensure the efficiency and effectiveness of the PVI as a way of enhancing trust in cloud computing. Thus, the service provider assumes responsibility for providing the physical security and the logical security of the service platform required for the PVI layer. While on the other hand the user is responsible for securely provisioning their virtual infrastructure with appropriate firewalls, interference detection systems, monitoring and logging to ensure that data is kept confidential (Krautheim, 2010). Therefore the PVI enables the user to successfully build a virtual infrastructure that meets these security requirements. It is under such an infrastructure that users are more willing to trust and make use of cloud computing.

Furthermore, according to Krautheim (2010) this synergistic relationship and security information sharing can be maintained and improved through trusted computing. Trusted computing provides mechanisms to control the behaviour of computer systems through the enforcement of security policies via hardware and software controls. This is in line with the McKnight, Choudhury and Kacmar (2002) Institution-based Trust construct which suggests that structural conditions need to exist to improve the probability of a trusting relationship. In the cloud computing scenario, the structural conditions can be seen as the enforcement of relevant security and legal policies. Additionally the structural assurance component of the McKnight, Choudhury and Kacmar's (2002) model is also relevant here as it suggests that structures such as guarantees, regulations, legal recourse or procedures, promote success in the relationship.

By requiring service providers to use trusted computing technology, users can verify their security in the cloud computing environment and control their information and eventually increase trust in cloud computing (Krautheim, 2010). However, the limitation according to Shimba (2010) is that the PVI leads to running overheads for both the cloud computing service provider and the customer.

In addition to the trust factors described in the models above, several factors relating to cloud computing have been identified in literature. These are described in the next section.

4.4. Factors That Enhance Trust in Cloud Computing

The lack of user trust in cloud computing presents an obstacle that needs to be overcome with regards to the adoption and widespread use of cloud computing applications. The trust models above described the conditions necessary for the development of trusting relationships between trustor and trustee. The trusting relationships between trustor (users) and the trustee (cloud computing service provider) is an essential foundation for the further development of user trust in cloud computing applications. The following section of this research project discusses additional factors that aid in the enhancement of user trust in cloud computing. Relevant factors such as knowledge, education and skill; awareness of perceived benefits; compliance; accountability and transparency are discussed below.

4.4.1. Knowledge, Education and Skill

According to Locke (2004), the relationship between information and communication technology (ICT) knowledge of users and their trust in ICT usage is significant. This is because the level of understanding of new ICT systems is highly likely to enhance the levels of trust in the use of new technologies. Similarly, the level of cloud computing understanding of potential users has a positive correlation with the levels of trust in cloud computing adoption and use. This is compared to when the users do not have the basic skill of how to use cloud computing applications. This often results in them avoiding the services offered by cloud computing service providers with the view that these services are complex processes and not easy to use (Locke, 2004).

Baize (2011) also argues that it is of great importance that potential users have a basic knowledge or skills of cloud computing before attempting to use the services offered by cloud computing service providers. More often than not, potential users with technological skill are more willing and can be easily encouraged to recognise, trust and use cloud computing more than the potential users without technological skills. This can be viewed as the principal internal motivating factor for users to adopt and use cloud computing (Baize, 2011). Those users with knowledge or previous experience may influence other users into using cloud computing applications and also enhance their level of trust.

The use of cloud computing by users who do not have prior knowledge and skill can therefore follow a similar trust enhancing path. The ability and understanding of users on how cloud computing operates has an impact on their levels of trust in cloud computing. An average potential cloud computing user is likely to trust the cloud computing platform’s sophisticated technologies if they do have the basic knowledge of how cloud computing operates. The lack of skill amongst users distorts their trust in the system, especially when the user believes that an ICT like cloud computing requires specialist skills (Locke, 2004).

4.4.2. Awareness of Perceived Benefits

Awareness of perceived benefits should be considered as one of the fundamental factors that could affect user trust in cloud computing. According to Locke (2004), existing literature and empirical evidence has proved that the greater the benefits perceived by users, the higher the possibility of new technology adoption and use. Users tend to invest trust in new technologies such as cloud computing because they have found that it offers them a wide range of feasible opportunities and specialised innovative services. The most common benefits were discussed in detail in Chapter 2, namely: IT resource optimisation, reduced infrastructural cost, easy deployment and management of applications and disaster recovery and backup to users of cloud computing applications.

4.4.3. Compliance

This refers to ensuring that a cloud computing deployment meets the requirements imposed by the applicable normative framework, including general legislation, sector-specific rules and contractual obligations. With compliance, the major issue will be ensuring the compliance of data protection rules (Robinson, Lorenzo, Cave, & Starkey, 2010). According to Holbl (2011), compliance can be seen as one of the important trust factors between a cloud computing service provider and their customers. Regulatory and legislative compliance by cloud computing service providers enhances the level of trust that users have in the cloud computing applications.

Cloud computing data centres can be geographically dispersed and hence different regulations have to be implemented in different locations to ensure compliance. Therefore, legislative compliance of cloud computing has to be adequately defined for different cloud computing service providers in different locations (Holbl, 2011).

4.4.4. Accountability

According to Baize (2011), accountability in cloud computing ensures that security or privacy breaches in a cloud computing deployment are correctly addressed. This is done through appropriate compensation mechanisms towards any victims, which in most cases are the users of cloud computing that might be affected. Cloud computing services can succeed when cloud computing services providers are able to provide these services in an efficient way and assure customers that they are fully accountable for hosting data and also that the users' data will remain private and secure (Microsoft, 2009). Potential users grow to have trust in cloud computing when accountability is achieved through the combination of law, regulation and technical enforcement mechanisms by the service providers.

4.4.5. Transparency

The general perception amongst cloud computing users is that cloud computing is less secure than traditional in-house systems. According to Gopalakrishnan (2009), security measures used in cloud computing must be made available to users for them to gain their trust in cloud computing. By nature the cloud computing infrastructure is secure according to the cloud computing requirements; however users are looking for a different set of security aspects within the cloud computing applications. The important aspect is to see that the cloud computing service provider meets the security requirements of the application and this can be achieved only through transparency in the offering and provisioning of cloud computing (Gopalakrishnan, 2009). Cloud computing service providers must demonstrate the existence of effective security controls that will assure users that their information is properly secured against unauthorised access, change and all forms of destruction in the cloud computing environment (Vael, 2010).

Transparency ensures that the operation of the cloud computing deployment is sufficiently clear to all stakeholders, including service providers and users. This can be witnessed, for example, in the difficulty of determining who or where a cloud computing service provider is, and where his responsibilities and liabilities end (Robinson, *et al*., 2010). Gopalakrishnan (2009) further states that transparency in cloud computing can be attained by a total and complete audit log and control measure in the cloud computing environment. According to Holbl (2011) in order to ensure transparency, the communication line that exists between the cloud computing service provider and the users has to be adequately protected all the time. This has to be done to ensure confidentiality, integrity, authentication control and to minimise the risk of denial of service occurrences. An open and clear specification of the measurements taken to ensure the security of the communication line should be mandatory for service providers and should be based on open and transparent standards and technologies.

With the cloud computing trust enhancing factors clearly defined and described above, the study also makes reference to the Diffusion of Innovations Theory proposed by Rogers (2003), specifically the innovation-decision process. This is used to structure the decision-making framework proposed to enhance trust in cloud computing which is described in Chapter 7. The innovation-decision process is described below.

4.5. Rogers' (2003) Innovation-Decision Process

The process of adopting and using new technological innovations, such as cloud computing has been the focus of many studies and research projects. Several models have been proposed and one of the most popular adoption models is the Diffusion of Innovations Theory by Rogers (2003). According to Sahin (2006) the model by Rogers (2003) is a widely used theoretical framework in the area of new technology diffusion and adoption. Rogers' (2003) Diffusion of Innovations theory is the most appropriate for investigating the adoption and use of cloud computing by users as it gives five relevant steps that users have to observe when faced with a decision to adopt a new innovation such as cloud computing.

It is these five stages of the Innovation-Decision Process that are relevant in the formulation of a framework aimed at enhancing trust in cloud computing applications which is the objective of this study. This is appropriate as the produced framework can then be used to enhance the level of trust in cloud computing by providing a decision making tool to influence user adoption. The Innovation-Decision Process involves five steps, namely Knowledge, Persuasion, Decision, Implementation, and Confirmation (Sahin, 2006). These stages typically follow each other in a sequential manner (Sahin, 2006). The Innovation-Decision Process is depicted Figure 4.4.

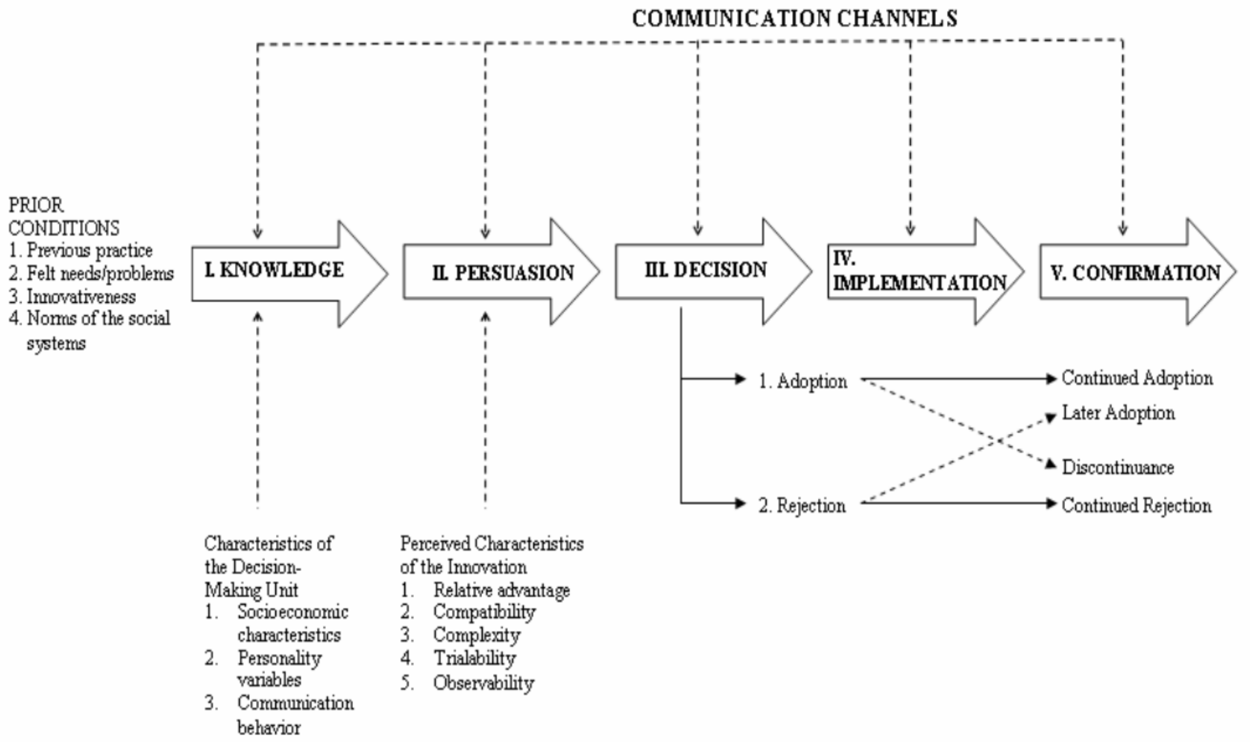


Figure 4.4: The Innovation-Decision Process (Source: Sahin, 2006)

The Innovation-Decision Process consists of the following components:

1. *Communication Channels*: These are the processes whereby respondents create and share information with one another in order to reach a mutual understanding (Sahin, 2006). This involves an innovation; two or more individuals or other units of adoption; and a communication channel. In the context of this study the respondents are the users and cloud computing service provider and the innovation involved is the cloud computing application. The communication channel will be the mass media and interpersonal communication systems that the users and service provider use to communicate with each other with regards to the cloud computing.

2. *The Knowledge Stage*: In this stage, an individual (the user) learns about the existence of an innovation (cloud computing application) and seeks information about the innovation. It involves questions from three types of knowledge, namely: awareness-knowledge, how-to-knowledge, and principles-knowledge (Sahin, 2006).

    a. *Awareness-knowledge* represents the knowledge of the existence of cloud computing applications. This type of knowledge, according to Sahin (2006) can motivate the individual to learn more about the innovation, which in this context is cloud computing and, eventually, to adopt it. It may also encourage users to fulfil their needs in terms of the other two types of knowledge (described below).

    b. *How-to-knowledge* contains information about how best to use an innovation such as cloud computing efficiently and effectively. This type of knowledge is an essential variable in the innovation-decision process (Sahin, 2006). To increase user trust in cloud computing applications and consequently the adoption process, users should have a sufficient levels of how-to-knowledge about cloud computing. Thus, this knowledge is critical for relatively complex innovations such as cloud computing.

    c. *Principles-knowledge* includes the functioning principles of the innovation (Sahin, 2006). In this case it would be the knowledge describing how and why cloud computing applications work. This type of knowledge equips the users with knowledge of how to integrate cloud computing into their everyday processes. It is an important type of knowledge when it comes to cloud computing adoption, as this type of knowledge guards against misuse of cloud computing applications. Thus, it also tends to enhance user trust ensuring continued use of cloud computing applications.

3. *The Persuasion Stage*: The persuasion step occurs when the individual has a negative or positive attitude toward the innovation. At this stage the individual is involved more sensitively with the innovation (Sahin, 2006). The persuasion stage is more affective or feeling centred. At this stage the degree of uncertainty that users have about cloud computing applications security, functionality and how other users perceive cloud computing affects the individual's opinions and beliefs about the innovation (Sahin, 2006). Thus, this stage is central to building trust in cloud computing and is the critical point in the user's decision to adopt and use cloud computing applications.

4. *The Decision Stage*: At this stage in the innovation-decision process, the individual chooses to adopt or reject the innovation (Sahin, 2006). If the user does not trust cloud computing and regard it as an unsafe process they are likely to reject it, thus abandoning the adoption. The opposite is true when users perceive cloud computing as a safe and secure innovation. This is based on the outcome of the persuasion stage.

5. *The Implementation Stage*: At the implementation stage, the innovation is adopted and put into practice (Sahin, 2006). At this stage the user chooses a cloud computing application for use. It is important to note that with the complex nature of cloud computing, uncertainty about the outcomes of using cloud computing applications might still persist. Thus, the user may need technical assistance from the cloud computing service provider in order to reduce the degree of uncertainty and enhance the levels of user trust. Thus, there may be a need for users to continuously re-evaluate previous stages in the process in order to reassess their implementation decision.

6. *The Confirmation Stage*: After the innovation adoption decision has been made, at the confirmation stage the individual looks for support for their decision of adopting the innovation (Sahin, 2006). The user needs to continuously re-evaluate the cloud computing platform to ensure it still meets their requirements.

4.6. Conclusion

This chapter of this research project reviewed the nature of trust and various definitions and attributes. This chapter also presented trust models and the limitations of these models in enhancing user trust in cloud computing. Four key trust models were discussed in this chapter, namely: Mayer, Davis and Schoorman's (1995) Proposed Trust Model, McKnight, Choudhury and Kacmar's (2002) Initial Trust Model, the TCCP proposed by Santos, Gummadi and Rodrigues (2009), and the PVI proposed by Krautheim (2010). The components suggested in these models were discussed and compared in this chapter. These components, namely competency, ability, benevolence and integrity are important for the enhancement of user trust and the development of the proposed framework to be discussed in Chapter 7 of this research project.

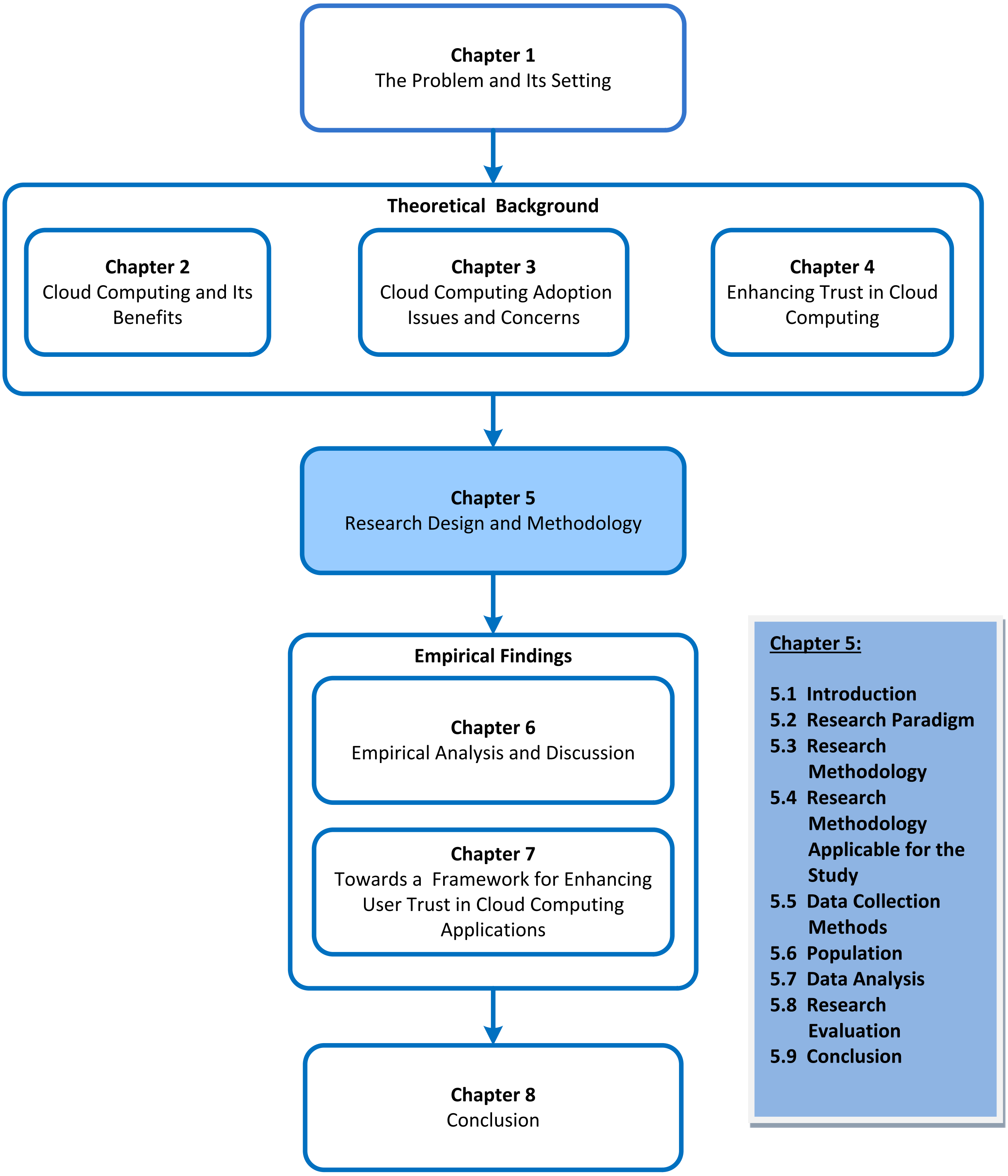
Furthermore, there are various components and factors that enhance trust in cloud computing which lead to effective and efficient use of cloud computing. The factors that are considered to be vital in enhancing trust in cloud computing are the knowledge, education and skill of users, awareness of perceived benefits, compliance, accountability and transparency. These factors are considered to be essential in addressing the main problem being investigated here, which is the lack of user trust in cloud computing applications.

In addition to the definition of trust, various trust models and trust enhancing factors, and the Rogers' (2003) Innovation-Decision Process was described. This process has been included as a means of structuring the decision-making process which is critical to the framework for enhancing user trust in cloud computing which is described on Chapter 7.

The preceding chapters of this research project established the theoretical base for this study. These chapters have dealt with the relevant elements of this research project, namely cloud computing and its benefits, the issues and concerns around the use of cloud computing that affect user trust in cloud computing applications and strategies to enhance trust in cloud computing. With this theoretical base as a starting point, empirical work needs to be conducted to further investigate the strategies of enhancing user trust in cloud computing applications. The approach for conducting this empirical work is described in the next chapter.

Chapter 5:

Research Design and Methodology


Chapter 1
The Problem and Its Setting
Theoretical Background
Chapter 2
Cloud Computing and Its Benefits
Chapter 3
Cloud Computing Adoption Issues and Concerns
Chapter 4
Enhancing Trust in Cloud Computing
Chapter 5
Research Design and Methodology
Empirical Findings
Chapter 6
Empirical Analysis and Discussion
Chapter 7
Towards a Framework for Enhancing User Trust in Cloud Computing Applications
Chapter 8
Conclusion

Chapter 5:

5.1. Introduction

A research methodology chapter provides the researcher with an opportunity to present the various methods that will be used to solve the identified research problem. Hofstee (2006) describes the research methodology as the blue print that explains how the researcher arrived at a conclusion and it should give a pictorial view of the steps followed. Moreover, it presents the researcher's motive behind the choice of each research method that is also presented in this chapter (Saunders, Lewis, & Thornhill, 2009).

According to Hofstee (2006) carefully choosing an appropriate method for a given research study is critical for the success of a research project. Therefore it is important that a researcher chooses the appropriate research method and design for a given research project. As the research methodology is seen as the approach used in the research process, it also encompasses a body of methods that will be used in the research process (Collis & Hussey, 2009).

The research method applied was influenced by the research project's objectives described in Chapter 1. By describing the theoretical aspects of the chosen method, the aim of this chapter is to illustrate how the study was conducted and how the results were derived. This chapter is important to show the link between the chosen method and how it enables the research objectives to be addressed.

The previous chapters presented and discussed the problem and the literature review relevant for this study, thereby, setting a solid theoretical base for the study. While these chapters help address the research questions, they also provide a theoretical lens that informed the theoretical and conceptual lens for identifying and developing a framework relevant for enhancing trust in cloud computing. Further, the insights gained from analysing the literature reviewed were instrumental in the identification and formulation of the framework that was developed to address the issue of a lack of trust in cloud computing applications.

This chapter therefore provides a detailed description of the research process that was followed in collecting, measuring and analysing data for this study. Careful consideration went into selecting the appropriate research methodology to achieve the objective of this study. The relevant research paradigm is described first which will be followed by the selected research methodology. Following this, a detailed discussion of the primary and secondary data collection methods will be provided as well as the population of the study and data analysis methods. The chapter concludes with an overview of how the credibility of the study can be evaluated.

5.2. Research Paradigm

A research paradigm is a framework of guidelines that explains how the research will be conducted. According to Hofstee (2006) academic research must have an underlying philosophical paradigm. This is defined as a pattern of a shared way of thinking to which the research is aligned. Maxwell (2005) refers to a paradigm as a set of general philosophical assumptions about the nature of the world (ontology) and how we understand it (epistemology) which is shared by researchers working in that area (Maxwell, 2005). Ontology is concerned with the form and nature of reality. This is a theory of what exists and how it exists. Epistemology is a philosophical assumption about what constitutes valid knowledge in the context of the relationship of the researcher to that being researched (Collis & Hussey, 2009). Therefore a paradigm is a perspective based on a set of assumptions, concepts and values that are held and practiced by a community of researchers.

A variety of philosophical paradigms are available because of the different ideas, views and perspectives of the world (Hofstee, 2006). These different paradigms can be differentiated from each other by the different philosophical assumptions and perspectives on which they are based. A certain research methodology is underpinned by a particular research philosophy. Therefore the researcher needs to carefully decide within which paradigm the research project will be conducted in order to determine the correct methodology to apply.

In research there are three general research paradigms that exist, namely: positivist, interpretivist and critical theory (Hofstee, 2006). These research paradigms identify specific data collection methods, observations and interpretation methods for both primary and secondary data that is relevant to what is being researched. The following sections briefly discuss the three key research paradigms.

5.2.1. Positivist Paradigm

According to Collis and Hussey (2009) positivist research focuses on and deals with facts associated with the occurrences of social phenomena. The positivist approach usually relies on experiments to look for evidence of cause and effect (Oates, 2006). Positivist research is objective and not influenced by the researcher. Therefore, with the positivist paradigm, logical reasoning is used to support assumptions made by the researcher. This means that reality can be analysed through measurable properties independent from the researcher (Myers, 2009). This ensures that research is conducted empirically and can be repeated.

Collis and Hussey (2009) describe the positivist approach as widely accepted in social science studies (including Information Systems (IS) research that considers environmental and behavioural aspects). According to Oates (2006), the positivist approach is largely based on two assumptions, namely:

1. The world is ordered and regular, not random.
2. The world can be investigated objectively.

Thus, social reality is singular and objective and is not affected by the act of investigating it (Collis & Hussey, 2009).

5.2.2. Interpretivist Paradigm

Interpretivist research tries to understand human behaviour in a specific context. Interpretivist research is therefore conducted in a subjective manner by focusing on the meaning of social phenomena rather than the measurement as suggested by the positivist paradigm. According to Oates (2006), this paradigm aims to understand IT as a practice constructed and developed by humans. Interpretivist research therefore identifies, explores and explains how the factors in a social setting are related and interdependent (Oates, 2006). Therefore, interpretivist research attempts to understand human behaviour in a specific context, in this case in the cloud computing context.

According to Collis and Hussey (2009), the interpretivist paradigm emerged in response to criticisms of positivism. Oates (2006), further explains that interpretivism does not aim to prove or disprove hypotheses as is done in positivist research, but rather to identify, explore and explain how the factors in a social setting are related and interdependent.

5.2.3. Critical Theory

According to Oates (2006) critical theory asserts that social reality is historically created and re-created by people in a consistent manner. Critical research goes beyond merely understanding IT practice; it goes on to challenge the power structures and assumptions about the development and implementation of IT artefacts (Oates, 2006). Critical researchers do not only seek to study and understand society, but they go on to critique and attempt to change society.

Researchers in this paradigm also view social reality as created by people with the addition of economic, political and cultural influences that shape this view of reality. According to Oates

(2006), critical researchers criticise interpretive research for failing to analyse the patterns of power and control that regulate views of reality.

5.2.4. Comparison of the Research Paradigms

According to Blanche, Durrheim and Painter (1999) the differences between these three research paradigms, ontology, epistemology and methodology can be summarised and illustrated as described in Table 5.1. Ontology refers to what is known about the nature of reality to be studied; epistemology refers to the relationship between the researcher and what can be researched; while methodology states how the research will be conducted (Blanche, Durrheim, & Painter, 1999).

Table 5.1: Research Paradigms (Source: Blanche, Durrheim & Painter, 1999)

	Ontology	**Epistemology**	**Methodology**
Positivist	• Stable external reality • Law-like	• Objective • Detached researcher	• Experimental • Quantitative • Hypotheses
Interpretivist	• Internal reality of subjective experience	• Empathetic • Interactively subjective researcher	• Interactional • Interpretative • Qualitative
Critical	• Socially constructed reality	• Suspicious • Political • Researcher constructs versions of reality	• Deconstruction • Textual analysis • Discourse analysis

It should be noted that although there are distinct differences between the three paradigms, researchers can combine certain characteristics from these research paradigms. However, this does not mean that a single study can have two paradigms. Thus, each study will be primarily positioned within a single paradigm, while another paradigm may influence certain aspects of the study.

5.2.5. Research Paradigm Applicable for this Study

This study is based on underlying theoretical paradigms which influence the reasoning and approach taken in this study. It should be noted that different philosophical paradigms have differing views about the nature of the world and the way in which unique knowledge about it can be acquired (Oates, 2006). The research paradigm is also an indication of which school of thought and principles the study is aligned to. A number of philosophical paradigms exist; but for the purposes of this study the philosophical framework was narrowed down to the choice between positivism and interpretivism, which are the two extremes on the continuum of ontological assumptions (Collis & Hussey, 2009). As illustrated in Figure 5.1, the positivist and interpretivist approaches are two extreme research paradigms, with several research paradigms combining elements from these two extremes along this continuum.

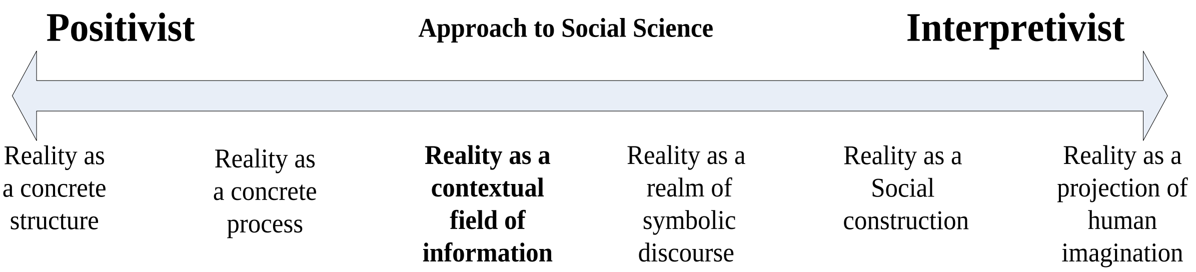

Positivist
Approach to Social Science
Interpretivist
Reality as a concrete structure
Reality as a concrete process
Reality as a contextual field of information
Reality as a realm of symbolic discourse
Reality as a Social construction
Reality as a projection of human imagination

Figure 5.1: Continuum of Core Ontological Assumptions (Source: Collis & Hussey, 2009)

Collis and Hussey (2009) explain that few people operate purely within any of these forms of research. Using a combination of the elements allows one to take a broader and often complementary view of the research problem or issue (Collis & Hussey, 2009). Due to the subjective nature of the methods that will be used in this study, an interpretivist influence will emerge in this study in line with the third stage (reality as a contextual field of information) of the continuum represented in Figure 5.1.

Despite the fact that these two paradigms can be used effectively with any research design, it is often argued that positivism is aligned with quantitative research and interpretivism is often linked with qualitative research. As this study will lean toward an interpretivist paradigm, it is strongly linked to qualitative methods of data collection. The qualitative research method puts emphasis on understanding the setting of phenomena rather than the measurement of the phenomena. According to Collis and Hussey (2009) this type of research involves an inductive process with a view to providing an interpretive understanding of social phenomena within a particular context (Collis & Hussey, 2009).

As mentioned above, the approach will be based on inductive reasoning. In this case, the researcher begins with specific observations, or formulated research questions from which patterns are identified. This leads to general conclusions or theories. For this research these conclusions will be recommendations based on the proposed framework for enhancing trust in cloud computing to ensure adoption. The next section discusses the research methodology used for this research project and the reason for its implementation in this study.

5.3. Research Methodology

The aim of this study is to develop a framework that will enhance trust in cloud computing. The framework will be derived from reviewing and analysing existing theories and models discussed in previous chapters of this study. The empirical evidence collected will be used to confirm and refine the framework. The method used to conduct this research is further described below.

A research methodology is an approach to the process of research and encompasses a body of methods (Collis & Hussey, 2009). The manner in which research is conducted is commonly divided into three categories: qualitative methods, quantitative methods and mixed methods (which comprises of both qualitative and quantitative methods). Therefore a researcher needs to choose a methodology that reflects the philosophical assumptions of the chosen paradigm. In this study the chosen paradigm is interpretivism.

Many researchers and authors refer to positivist research as quantitative research and interpretivist research as qualitative research, even though it can be argued that research may include characteristics of both positivist and interpretivist research approaches (Hofste, 2006). Therefore, it is necessary to make a clear distinction between qualitative and quantitative research indicating which research method will be adopted.

5.3.1. Qualitative and Quantitative Research Methods

Qualitative research is usually used in the social sciences context to understand behaviour and what causes such behaviour (cause and effect). It is a type of research method that focuses on a collection of qualitative data. Qualitative data can be characterised as low in volume and high in detail. Open-ended questions are commonly used that result in data being presented in a textual format. Research methods mostly commonly used in qualitative research are case studies, observations, in-depth interviews, experiments, literature review, action research, physical experiences, theories, social interaction, questionnaires and expert review.

Quantitative research, on the other hand, is commonly used in natural sciences research to observe and learn about occurrences of natural phenomena. Research conducted quantitatively carries the characteristic that it can be measured numerically by using closed-ended questions. Quantitative data can also be characterised as high in volume and low in detail. Research methods under quantitative research include written surveys, questionnaires, experiments and theories. Presentation of data under this method is usually statistical which includes graphs and tables formatted for analysis.

This research project, as previously outlined, makes use of the qualitative research methods to gather the empirical data. This is in line with the interpretive paradigm selected for this research project. As the study is aligned with the interpretivist approach, the selection of a qualitative approach respectively is appropriate for this research project, however elements of quantitative analysis were necessary for the questionnaire. The study also draws on expert review as a way analysing and evaluating the developed framework. The Design Science Methodology followed will be discussed in the section that follows.

5.3.2. Design Science Methodology

Design Science Methodology is a comprehensive problem solving process that is characterised by the detailed evaluation of a project with the end goal being the creation of an artefact (Hevner, March, Park & Ram, 2004; Gasser, Majchrzak & Markus, 2002). For this study, the artefact will be the proposed framework. This fulfils the purpose of this study is to develop a framework that can be used to enhance trust in cloud computing. According to Hevner, *et al.* (2004) this is a problem solving methodology which seeks to create innovations that define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, management and use of information systems (IS) can be effectively and efficiently accomplished.

Hevner, *et al.* (2004) further specify that the Design Science method consists of seven guidelines which must be considered to effectively utilise this research methodology. Hevner, *et al.*'s (2004) seven guidelines are the most widely cited set of guidelines for Design Science research and is thus relevant in this study. These guidelines provide a foundation for conducting Design Science research. It should be noted, however, that none of the guidelines are mandatory steps and it is up to each researcher to decide how and when to employ each of the seven guidelines in a specified research project (Hevner, March, Park, & Ram, 2004). These guidelines, a description to define the guideline and an explanation of how the guideline was applied in this research project are described in Table 5.2.

Table 5.2: Design Science Research Guidelines (Source: Hevner, March, Park & Ram, 2004)

Guideline	**Description**	**Application**
1. Design as an Artefact	Design Science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.	This study proposes a framework that can be used by users to assess the trustworthiness of cloud computing applications; and therefore enhance user trust in cloud computing applications.
2. Problem Relevance	The objective of Design Science research is to develop technology-based solutions to important and relevant business problems.	The study identified a lack of user trust in cloud computing as the main problem of this research project. This study therefore focused particularly on proposing a framework to overcome this concern.
3. Design Evaluation	The utility, quality and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.	The research framework was evaluated using expert review. The experts were selected based on their expertise on cloud computing.
4. Research Contributions	Effective Design Science research must provide clear and verifiable contributions in the areas of the design artefact, design foundation, and/or design methodologies.	The contribution of this project is the framework which provides users a means of assessing and evaluating the trustworthiness of cloud computing applications. This in turn leads to enhanced trust and improved adoption rates. This is an important contribution as no such framework exists at present.
5. Research Rigor	Design Science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.	Valid data gathering and analysis techniques were used to investigate the research problem and propose the framework. These methods are described in this chapter.
6. Design as a Search Process	The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.	The proposed framework was developed from related literature and empirical findings from the questionnaire. The comments and recommendations from the expert reviews on the proposed framework were used to refine the framework.
7. Communication of Research	Design Science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	This study has produced two publications in the form of peer reviewed conference papers. These papers are included in Appendix B and C.

If all seven of the Design Science guidelines as outlined by Hevner, *et al.* (2004) are effectively employed, they assert that valid conclusions in terms of producing a relevant framework will be achieved.

5.4. Research Methodogy Applicable for this Study

In this section the research methodology and process followed in developing the proposed research framework is described. This framework was developed in order to address the underlying research problem and the research objective in terms of enhancing user trust in cloud computing applications. The process of developing the framework is depicted in Figure 5.2.

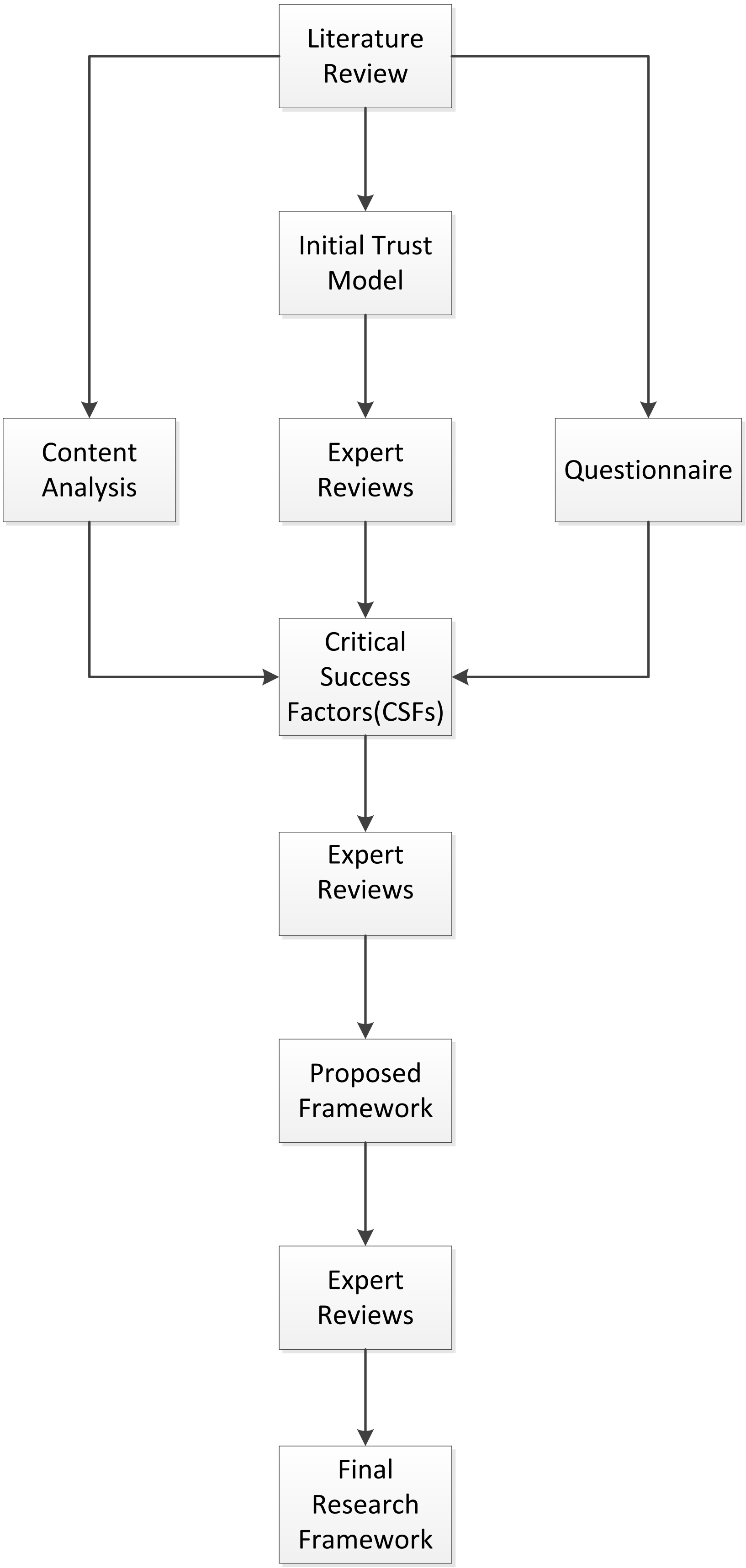


Figure 5.2: Development of the Research Framework

As indicated in Figure 5.2 above the initial literature reviewed as presented in Chapters 2, 3 and 4 led to the construction of the Initial Cloud Computing Trust Model. Prior to the expert review, this initial model was presented and published at a conference (see Appendix B). This paper was intended to confirm the applicability of the approach this research project was following. Following this, the initial model was evaluated by expert reviews. The expert reviews of the model are discussed in detail in Section 7.3.4 of this dissertation. The comments and suggestions from the expert review process led to further work towards the final framework.

Thus, relevant cloud computing literature was again reviewed and analysed in order to determine the most relevant factors. This was achieved through a content analysis described in Section 7.4. of this research project. These factors were then confirmed through a questionnaire distributed to cloud computing users to solicit from them the issues and concerns that affect user trust in cloud computing applications. This led to the proposal of CSFs for enhancing user trust in cloud computing applications. The CSFs were presented at an international conference (see Appendix C) and once again an expert review was carried out. The expert reviews of the CSFs are discussed in detail in Section 7.4.8 of this research project. The comments and suggestions from the expert review process led to a further evaluation and refinement.

From this second round of expert review, a framework that can be used to enhance the level of user trust in cloud computing by providing a decision making tool to influence user adoption was proposed. This framework was presented to experts in the cloud computing industry for evaluation in a final expert review. The feedback from the experts in the form of comments and suggestions was used to further refine the proposed framework into the final research framework which is presented in Section 7.5 of this research project. The next section of the research methodology refers to the data collection methods that were employed to gather both the primary and secondary data for this research project.

5.5. Data Collection Methods

In research there are numerous data and information collection techniques and methods relevant and available for researchers to use. There are diverse sources of data to choose from when one is conducting research, namely primary and secondary data. Most research projects require some combination of both in order to answer the research question and to meet the research objectives (Hofstee, 2006).

According to Collis and Hussey (2009), primary data is data collected from an original source such as the researcher's experiments, questionnaire and interviews. This is to say it is data that is unpublished and the researcher has gathered it directly from the respondents. Secondary data, on the other hand, is the data collected from existing sources of data such as publications, journals and records from databases (Collis & Hussey, 2009). Therefore, secondary data is any previously published materials such as books, articles and completed studies.

This study makes use of web-based questionnaires and expert reviews as primary data, and literature review as secondary data. Figure 5.2 shows the diagrammatical approach to using the mentioned data collection methods.

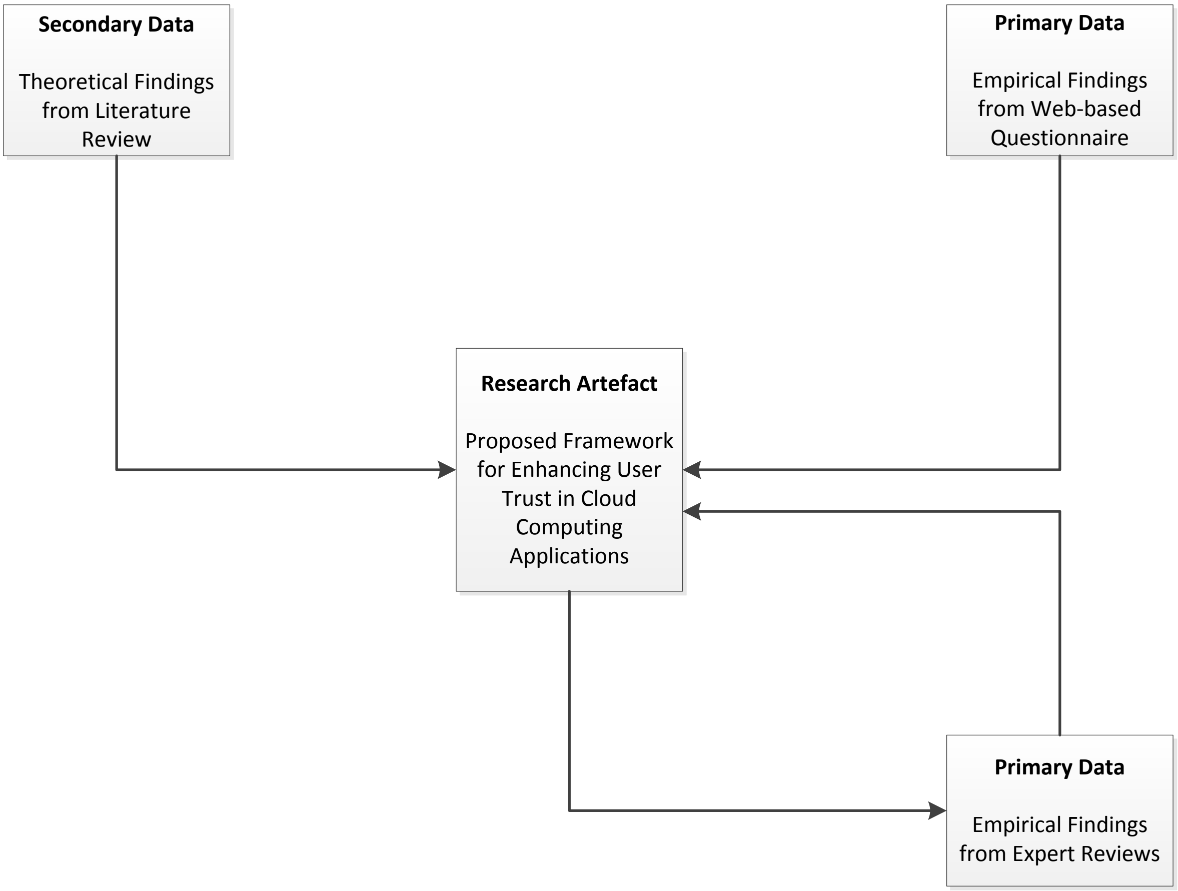

Secondary Data
Theoretical Findings from Literature Review
Primary Data
Empirical Findings from Web-based Questionnaire
Research Artefact
Proposed Framework for Enhancing User Trust in Cloud Computing Applications
Primary Data
Empirical Findings from Expert Reviews

Figure 5.3: Data Collection Process

As shown in Figure 5.2, the literature review was used to form the theoretical base for this research project. This theoretical base influenced the creation of the initial model and the web-based questionnaire which was then used to gather empirical data. Expert review of the initial model together with the questionnaire feedback led to the development of CSFs for enhancing user trust in cloud computing applications. The developed CSFs then went through another expert review process, which led to the formulation of the proposed framework. The framework which is the research artefact was formulated after careful analysis and consideration of the feedback from experts and empirical findings which were combined with the secondary data.

This research artefact is a framework for enhancing trust in cloud computing applications as described in Chapter 7. The framework was then further refined and evaluated using expert reviews. The primary and secondary data collection techniques employed by this study are discussed in the following sections.

5.5.1. Primary Data Collection Methods

The primary data sources for this research project are a web-based questionnaire and expert review. These are discussed in the sections that follow.

5.5.1.1. Web-based Questionnaire

According to Collis and Hussey (2009), in a research project the aim of the questionnaire is to elicit the respondent's opinion in order to address the research problem being investigated. The respondent's answers to the questions provide the researcher with essential data that can then be analysed and interpreted. A web-based questionnaire has the ability to reach a large number of respondents who are geographically dispersed and offers a much higher degree of freedom when completing the questionnaire compared to paper based questionnaires and interviews (Collis & Hussey, 2009).

However, the disadvantage of this data collection method is that it poses a risk of non-response, bias and respondents might incorrectly interpret and answer some of the questions. Questionnaire fatigue, which is the reluctance of people to respond to questionnaires, is another factor that affects the effectiveness of this data collection method (Collis & Hussey, 2009). It is therefore essential for the researcher to develop appropriate questions together which make use of a relevant response format. For this reason, a pilot study was conducted to test the suitability of the research instrument.

The web-based questionnaire for this study comprised both open-ended and closed-ended questions to gather information from the respondents (the research instrument is included as Appendix D). According to Collis and Hussey (2009), closed-ended questions allow respondents to choose from predetermined answers. In this case the Likert scale was used to ensure that analysis of the data is easier. Information gathered from open-ended questions, on the other hand, allows the researcher to explore certain aspects of the research problem as it allows users to respond in their own words. These responses are carefully analysed individually to identify keywords and themes across the responses. The findings of the questionnaire are described in detail in Chapter Seven.

5.5.1.2. Expert Review

After assessing a number of evaluation methods including those suggested by Hevner, *et al.* (2004), the expert review was found to be the most appropriate method to evaluate the artefact. The expert review is an evaluation approach which uses an expert group to criticise the research artefact (Molich & Jeffries, 2003). The expert group provides comments on the presented material, which is then used to refine the artefact.

Relevant experts must be chosen to ensure that the presented material is assessed effectively and valuable comments are provided. Experts used in an expert review process for a study should meet four criteria, namely: knowledge and experience relevant to the research; capacity and willingness to participate; sufficient time to participate; and effective communication skills (Skulmoski, Hartman, & Krahn, 2007). The experts used for this study met these criteria.

As a means of evaluating the proposed research model, expert reviews were conducted with 10 cloud computing experts. These experts were asked to comment on each stage of the development of the proposed framework. These stages of development are described in detail in Chapter 7 together with the expert review recommendations which led to the refined research framework. The recommendations were considered and the proposed framework was appropriately modified. The expert review ensured that the proposed framework was appropriately assessed and confidently presented as a valid and relevant solution in terms of enhancing user trust in cloud computing applications.

In addition to the primary data collection techniques described above, secondary data was used as a theoretical basis for this research project. The use of secondary data is described in the next section.

5.5.2. Secondary Data Collection Methods

The secondary data collected for this study involved an extensive and thorough literature survey of Internet sources, frameworks, methodologies, journal articles, past research, reports and books. Secondary data was used throughout the research process, including the creation of the research instrument, writing of the theoretical chapters and contributed to the formation of the proposed framework. All efforts were made to ensure that the content of the secondary research remained as current as possible.

5.6. Population

As described in the data collection methods in the previous section, questionnaires, expert review and secondary literature review were used in this research project. The population for each of these methods is described in the sections that follow.

5.6.1. Respondents for the Questionnaire

A random sample of 100 commerce students from a higher education institution was selected for this study. The commerce students were considered to be appropriate as they are viewed as potential users of cloud computing services for personal and business use. They would therefore champion the widespread use of cloud computing. A link to the web-based questionnaire was emailed to the respondents with detailed instructions for the completion of the questions. 100 responses were received.

5.6.2. Respondents for the Expert Review

As the population of cloud computing experts in South Africa is unknown, the sample size of experts used for the expert review is relatively small. Ten cloud computing experts responded to the requests for participation and provided feedback on the proposed research framework.

5.7. Data Analysis

Data collected during the study has to be analysed and interpreted. Thus, the data collection process in every study concludes in the analysis and interpretation of some set of data, be it quantitative questionnaire data, experimental recordings, historical and literary texts, qualitative transcripts or discursive data (Mouton, 2005). Additionally, Mouton (2005) explains that the data analysis stage involves breaking up data into manageable themes, patterns, trends and relationships. The methods for analysing the primary and secondary data for this study are described in the sections that follow.

5.7.1. Secondary Data Analysis

The aim of analysis is to understand the different elements of the data through an assessment of the relationships between concepts, constructs or variables, and to see whether there are any patterns or trends that can be identified or isolated, or to establish themes in the data. For this reason the secondary data collected in this study was analysed through a content analysis of the most important concepts related to cloud computing. Thus, patterns were drawn from the content analysis which was relevant to the creation of the critical success factors (CSFs) described in Chapter 7.

5.7.2. Questionnaire Data Analysis

The primary data collected from the questionnaire was analysed using descriptive statistics and pattern matching. Data from the web-based questionnaire was used in order to inform the creation and development of the CSFs and the proposed framework.

5.7.3. Expert Review Data Analysis

The qualitative data from the expert reviews was summarised and changes were made according to the feedback they gave. The expert reviews contributed to the refinement of the initial research model, the CSFs and the proposed framework.

5.8. Research Evaluation

Research evaluation is a necessary step in order ensure the credibility and integrity of the research project. A set of equivalent criteria for positivist and interpretivist research is provided by Oates (2006). For this research the interpretivist criteria is applied, which involves trustworthiness, conformability, dependability, credibility and transferability. These are briefly defined below.

1. *Trustworthiness*: The information provided by the respondents was honest and hence contributes to this attribute of the study. Also, the trustworthiness of the expert reviews used to refine the proposed framework was evaluated.
2. *Conformability*: This criterion has been met through the use of the questionnaire undertaken to confirm the outcome of the research. The use of the questionnaire findings confirmed the theoretical findings. Additionally, the experts review was included which led to the development of the research framework.
3. *Dependability*: Dependability is established through the use of literature from recognised authors and the contributions from experts in the field of study. The use of established theories and models which have been previously used and tested in numerous research projects adds to the dependability of this project.

4. *Credibility*: Credibility has been achieved through the use of multiple data collection techniques and the use of expert review.
5. *Transferability*: Transferability has been achieved as the research framework can be applied to other users with similar characteristics, considering adopting and using a new technology.

The research project can therefore be considered credible through the application of these five criteria. For this reason these 5 factors are assessed in the final chapter of this research project.

5.9. Conclusion

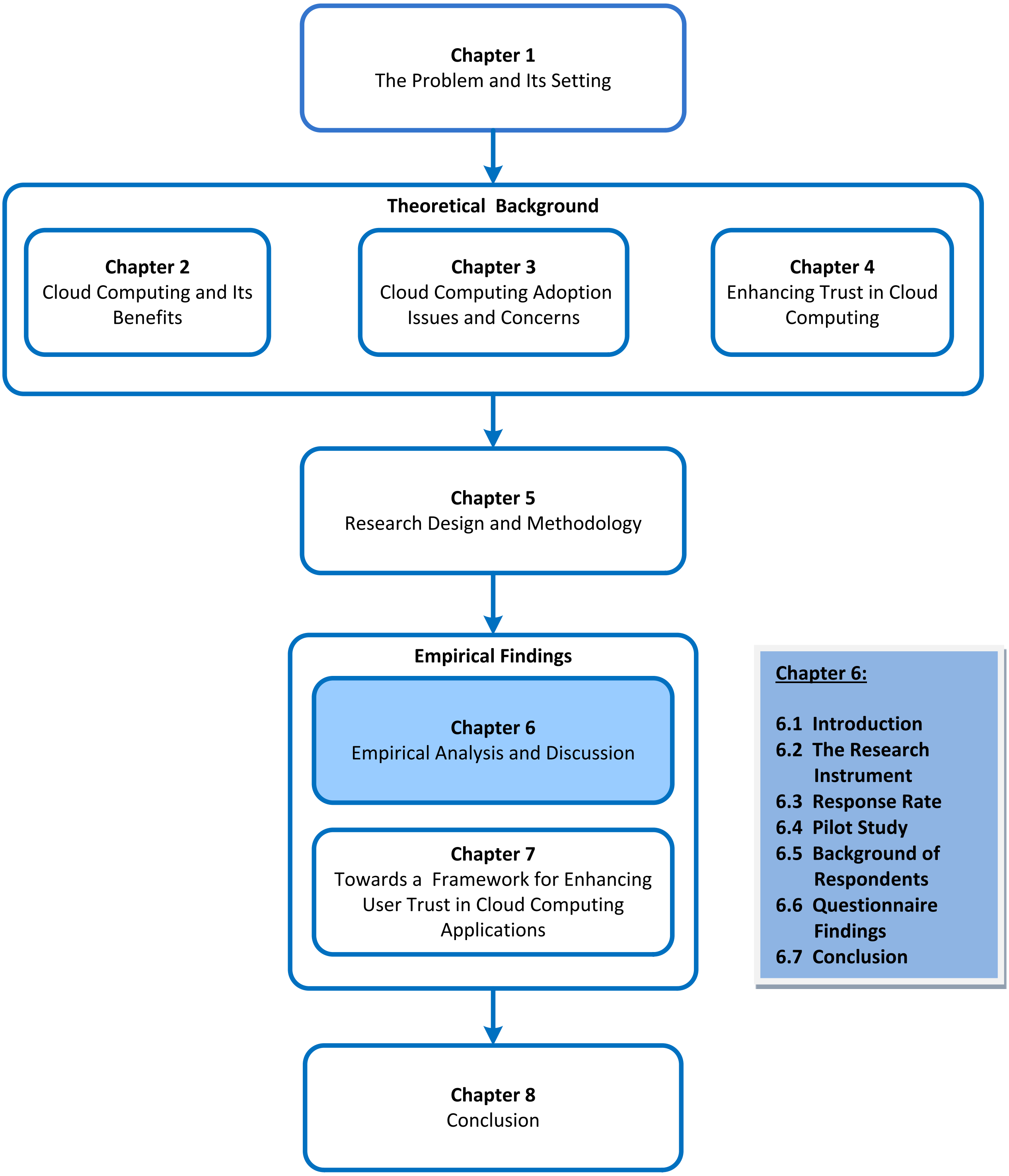
Chapter 5 provided a detailed description of the manner in which this research was conducted. A discussion of the available research paradigms, namely: positivist, interpretivist and critical theory was provided. This was followed by a comparison and supportive argument on the most appropriate research paradigm for this study. This study was conducted within an interpretivist paradigm and follows the qualitative approach consistent with this paradigm. The Design Science Methodology, which aims to create and evaluate IT artefacts, is followed in this research project. In this study the artefact is the research framework for enhancing user trust in cloud computing.

The methods used to collect the empirical data for this research project were a web-based questionnaire and expert reviews. The web-based questionnaires and expert reviews are the primary data collection methods that were used in this study and the secondary data came from the relevant literature that was reviewed. The population for collection of the data and the means of analysing the data are also outlined in this chapter. Expert reviews were used to evaluate and refine the artefact developed.

The chapter concluded with an evaluation of the integrity and credibility of this research project. All discussions mentioned here will allow this study to be conducted successfully, resulting in the formulation of the proposed framework. The next chapter describes the findings from the questionnaire.

Chapter 6:

Empirical Analysis and Discussion



Chapter 1
The Problem and Its Setting
Theoretical Background
Chapter 2
Cloud Computing and Its Benefits
Chapter 3
Cloud Computing Adoption Issues and Concerns
Chapter 4
Enhancing Trust in Cloud Computing
Chapter 5
Research Design and Methodology
Empirical Findings
Chapter 6
Empirical Analysis and Discussion
Chapter 7
Towards a Framework for Enhancing User Trust in Cloud Computing Applications
Chapter 8
Conclusion

Chapter 6:

6.1 Introduction
6.2 The Research Instrument
6.3 Response Rate
6.4 Pilot Study
6.5 Background of Respondents
6.6 Questionnaire Findings
6.7 Conclusion

6.1. Introduction

This research project aims to investigate the lack of user trust in cloud computing which impacts on adoption and use of the applications. For this reason, the literature chapters of this research project discussed issues and concerns that affect the widespread adoption and use of cloud computing applications. The research design and methodology used has also been outlined in the previous chapter. This chapter therefore presents a discussion of the results obtained from the web-based questionnaire described in Chapter 5.

The results obtained from the questionnaire are analysed and described using descriptive statistics. This questionnaire data is important as it is used to confirm the critical success factors (CSFs) described in the chapter that follows. These CSFs are an important component of the framework developed to solve the underlying the research problem. These CSFs and the framework are presented in the next chapter.

This chapter begins with a description of the research instrument and the response rate. Then the information about the pilot study and the background of the respondents is described. The specific, relevant findings from the questionnaires in relation to the research objectives are then discussed. The findings from the questionnaires are important as they are used to produce the model described in Chapter Seven.

6.2. The Research Instrument

The research instrument used for data collection in this study was a web-based questionnaire. The questionnaires were distributed electronically to selected cloud computing users and potential users. The research instrument was derived based on the literature reviewed and is included as Appendix D. A pilot study was conducted in order to test the adequacy of this research instrument, and where necessary changes were made to the initially developed questionnaire. The web-based questionnaire comprised of open-ended and closed questions around users knowledge and use of cloud computing and cloud computing applications. Some of the questions in the questionnaire focused in finding out the perceived user benefits of adopting and using cloud computing applications. The questionnaire also included questions around user's perceived barriers, issues and concerned surrounding the use of cloud computing applications

6.3. Response Rate

150 commerce students from a higher education institution were invited to complete the questionnaire for this study. The commerce students were considered to be appropriate as they are viewed as potential users of cloud computing services for personal and business use. These respondents are from various levels of study, ranging from first year undergraduate to Masters and Doctoral students.

100 questionnaires were completed. However 1 of the 100 respondents was screened out because the participant did not have access to a computer (a factor deemed instrumental in this research project and determining the CSFs). Without access to a computer, this respondent is deemed to have insufficient information and communication technology (ICT) knowledge to contribute to this study of cloud computing. The fact that the invited respondent did not have access to a computer meant that their responses would not be included in the results of the study. Thus 99 valid responses were received, representing a 66% response rate. According to (Oates, 2006), during a research study it is common to have a response rate of 10%, but a response rate of 30% or more is usually preferred. Therefore, a response rate of 66% can be considered adequate for analysis and reporting.

6.3. Pilot Study

The purpose of the pilot study is to ensure that the questionnaire was an adequate and refined research instrument to be used to attain relevant information from respondents (Hofstee, 2006). The pilot study made use of a number of colleagues from Information Systems (IS) and Information Technology (IT) sectors. The pilot study proved to be an essential step in refining the questionnaire to ensure the most appropriate and relevant responses were elicited with this research instrument.

Responses from the pilot study indicated that some of the questions were ambiguous and some used unfamiliar terminology. Feedback from the pilot study indicated that some initial questions required further explanation in order to gather the expected responses. The questionnaire was therefore adjusted accordingly in line with these suggestions and feedback obtained from the pilot study.

6.4. Background of Respondents

This section provides the background and demographic information about the questionnaire respondents. The respondents were asked to indicate their highest level of education achieved. The responses to this question are shown in Table 6.1 and indicate that the respondents are distributed across different levels of tertiary education. A fairly even representation of students at Undergraduate level (29% have completed high school), Honours level (26% have completed an undergraduate degree) and Masters and Doctoral level (24% have completed a postgraduate degree) was achieved. Additionally, 11% of the respondents have completed a Diploma and 9% have completed a Certficate.

In terms of these varied levels of education, the value is realised through the varied responses which will be gathered with regards to their use of cloud computing that can be attained due to their different knowledge base. The varied understanding, needs and use of cloud computing applications by respondents meant that richer responses were gathered from the respondents.

Table 6.1: Respondents Level of Education

Highest Level of Education	Number of Respondents	Percentage %
High School	29	29%
Bachelor's Degree	26	26%
Postgraduate Degree	24	24%
Diploma	11	11%
Certificate	9	9%
Totals	**99**	**100%**

As mentioned in section 6.3, 1 respondent was excluded from participation due to lack of computer access. Thus, the results shown in Table 6.1 exclude this respondent. Table 6.2 describes the number of respondents with access to a computer, which is a vital factor of this research project. It is important that all the respondents have access to at least one computer which is the primary method used to access cloud computing applications through the Internet.

As shown in Table 6.1, 99% of the total 100 respondents to the questionnaire have access to a computer. Only 1 respondent (1%) had no access to a computer. This meant that this particular respondent had to be screened out because the validity of the responses they would provide depend on having access to cloud computing applications through the use of a computer.

Table 6.2: Summary of Respondents with Access to a Computer

Response	Number of Respondents	Percentage %

Yes	99	99 %
No	1	1%
Totals	**100**	**100.%**

As defined in Chapter 2, cloud computing applications are services that are offered by service providers through various means such as computers over the Internet. It was therefore essential to establish how often the respondents access and use the Internet. Table 6.3 and Figure 6.1 indicate that most of the respondents use the Internet several times a day.

Table 6.3: Summary on How Often Respondents Use the Internet

	Number of Respondents	**Percentage %**
Several times a day	88	88%
Once a day	3	3%
2 - 4 times a week	8	8%
Once a week	0	0%
Less than once a week	0	0%
Never	0	0%
Totals	**99**	**100%**

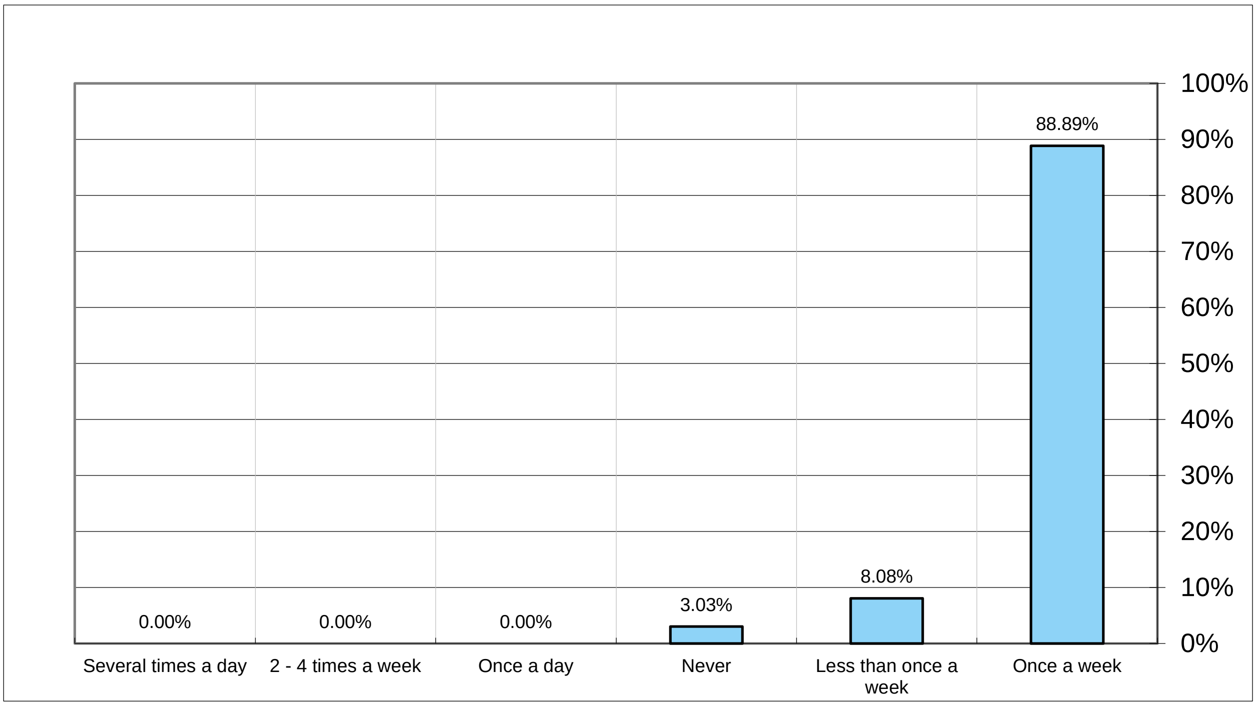


Figure 6.1: Frequency of Internet Usage

Results from the questionnaire reveal that 88% of the 99 respondents use the Internet several times a day. Only 11 (11%) of the respondents indicated that they access the Internet once a day to 2-4 times a week. As the clear majority of the respondents make use of the Internet several times a day, they are more likely to have accessed cloud computing applications at some point, although they may not necessarily be aware that they have. This is discussed further in section 6.5.1.

6.5. Questionnaire Findings

The objective of this study is to investigate the lack of user trust in cloud computing in order to develop a framework to enhance user trust in cloud computing applications. The following sections discuss the findings from the questionnaire relevant to the research questions which were stated in Chapter 1.

6.5.1. Questionnaire Findings: Knowledge of Cloud Computing

In order to explore levels of trust in cloud computing, it was essential to determine the initial knowledge they have in cloud computing. This provides an understanding of whether or not the respondents are able to suitably contribute to this research project. Respondents were asked to answer two open-ended questions about their knowledge of cloud computing.

Table 6.4 shows a summary of the responses to the first question: *What do you consider to be a Cloud Computing Application?.* These open-ended responses were matched to themes identified from the definitions of cloud computing described in Chapter 2.

Table 6.4: Summary of Responses on Cloud Computing Definition

Theme/Pattern	Number of Respondents	Percentages %
Cloud Computing is a data storage service with virtual servers	26	26%
Cloud Computing are applications hosted on the Internet and accessed via the web	24	24%
Cloud Computing is an application for storing and sharing data	15	15%
Cloud Computing is an online system for storing, processing and managing data safely	13	13%
I don’t know what Cloud Computing is/ Have no idea	11	11%
Cloud Computing is the delivery of services over the Internet	10	10%
Total	**99**	**100%**

As seen in Table 6.4, most of the respondents (26%) identified the ability to store and transmit data over virtual servers as their definition of cloud computing. A similar number of respondents (24%) mentioned that cloud computing is hosted on the Internet and accessed via the web. Of the 99 respondents, only 11 indicated that they had no knowledge of cloud computing.

Most of those respondents who indicated they had no knowledge of cloud computing had made use of cloud computing applications previously without being aware of it. This was ascertained through (amongst other questions) the open-ended question: *Please name any Cloud Computing applications or services you are aware of.* This question provides a complementary view of the respondent's understanding of cloud computing.

Table 6.5 lists the cloud computing applications mentioned by the respondents and the corresponding number of the respondents who had listed this application. It is important to note that the total number of respondents is more than 99 as each of the respondents may list more than one application. The most common applications identified were social networks and web-based email services and Dropbox.

Table 6.5: Summary of Unprompted Cloud Computing Applications Known by Respondents

Cloud Computing Application	Number of Respondents having knowledge of the Application	% of Responses
Web-Based email service and Social Networks	37	28.03%
DropBox	22	16.67%
Google Apps/Drive/Docs	18	13.64%
I do not know any Cloud Computing Applications	14	10.61%
Apple iCloud	12	9.09%
Microsoft Skydrive	7	5.30%
Amazon Web Services	6	4.52%
Microsoft Cloud OS	3	2.27%
Office 365	3	2.27%
Cloud Computing Landscape	1	0.76%
Cloud Assessment Tool	1	0.76%
BlackBoard	1	0.76%
CloudMe Application	1	0.76%
Oracle	1	0.76%
Share Point	1	0.76%
IceWeb Storage	1	0.76%
Evernote	1	0.76%
Sound Cloud	1	0.76%
Windows Azure	1	0.76%
TOTAL	**132**	**100.00%**

Furthermore, respondents were prompted to indicate which of the applications in a pre-defined list they considered to be cloud computing applications. The options provided for response in this list were determined through the literature review. These responses were reported as a percentage of the users that considered the listed application to be cloud computing applications, and are shown in Table 6.6 and Figure 6.2.

Table 6.6: Summary of Prompted Cloud Computing Applications Known by Respondents

	Number of	Percentage of

	Respondents	Respondents (%)
Web-based email (e.g. Hotmail, Gmail, Yahoo Mail)	62	62%
Google Apps (e.g. Google Docs)	62	62%
Apple iCloud	44	44%
Microsoft SkyDrive	40	40%
Skype	39	39%
Dropbox	36	36%
Amazon Elastic Compute Cloud (EC2)	24	24%
Microsoft 365	16	16%
Evernote	12	12%
Rackspace	8	8%
None of the Above	4	4%

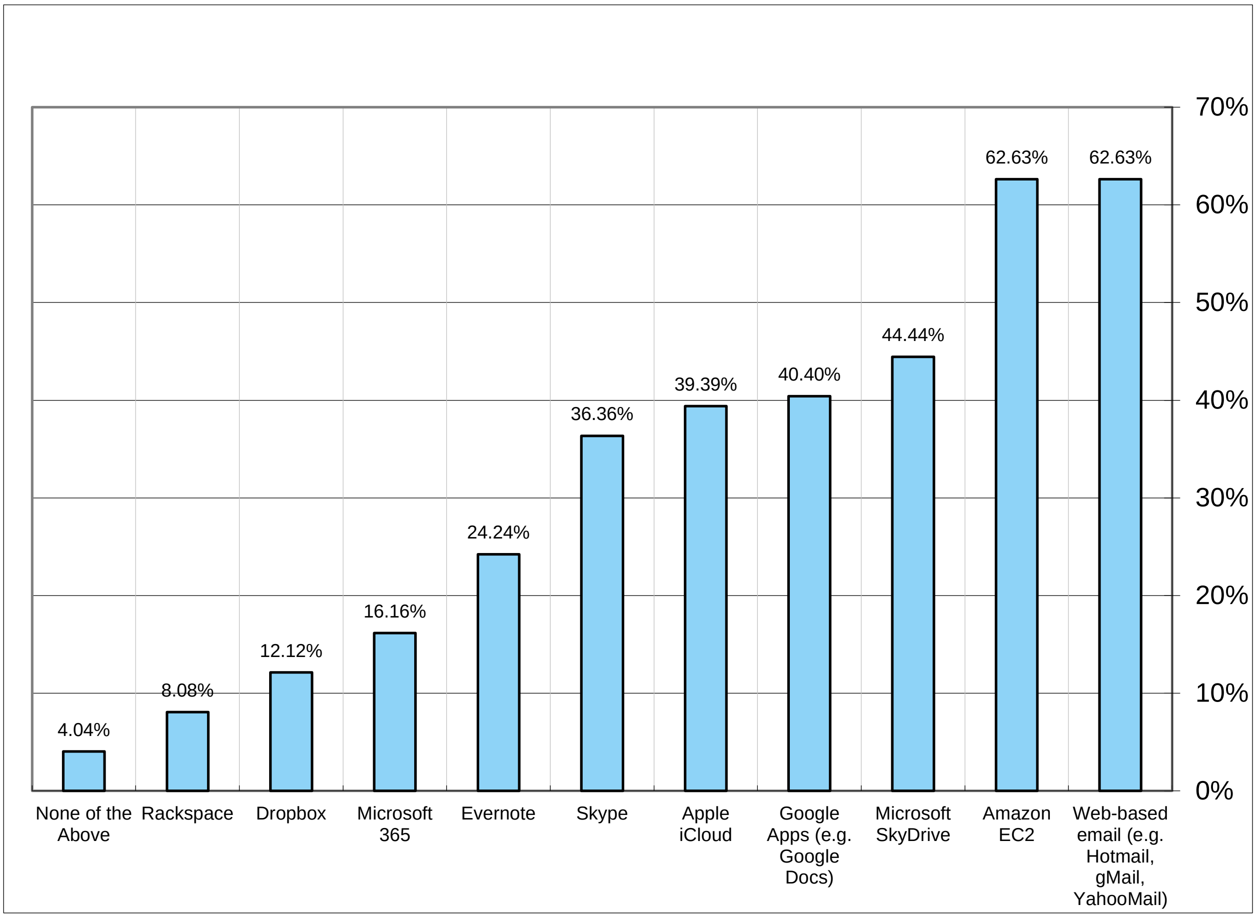


Figure 6.2: Knowledge of Cloud Computing

Again, web-based email was the most recognised cloud computing application with 62.63 respondents indicating they knew of it. An equivalent response was recorded for Google Apps. Other notable applications reported were Apple iCloud (44%), Microsoft SkyDrive (40%), Skype (39%) and DropBox (36%).

Further to ascertaining the awareness of the abovementioned cloud computing applications, the respondents were asked to indicate which of the applications they had actually used. These results are shown in Table 6.7 and Figure 6.3. It is important to note that respondents could select more than one application, thus the results are reported as a percentage of respondents.

Table 6.7: Summary of Cloud Computing Applications Used by Respondents

Cloud Computing Application	Number of Respondents to have used the Application	Percentage of Respondents (%)
Web-based email (e.g. Hotmail, Gmail, Yahoo Mail)	94	94%
Google Apps (e.g. Google Docs)	71	71%
Skype	59	59%
Dropbox	34	34%
Microsoft 365	27	27%
Microsoft SkyDrive	14	14%
Amazon EC2	12	12%
Apple iCloud	11	11%
Evernote	6	6%
Other	2	2%
I have not used any of these	1	1%
Rackspace	0	0%

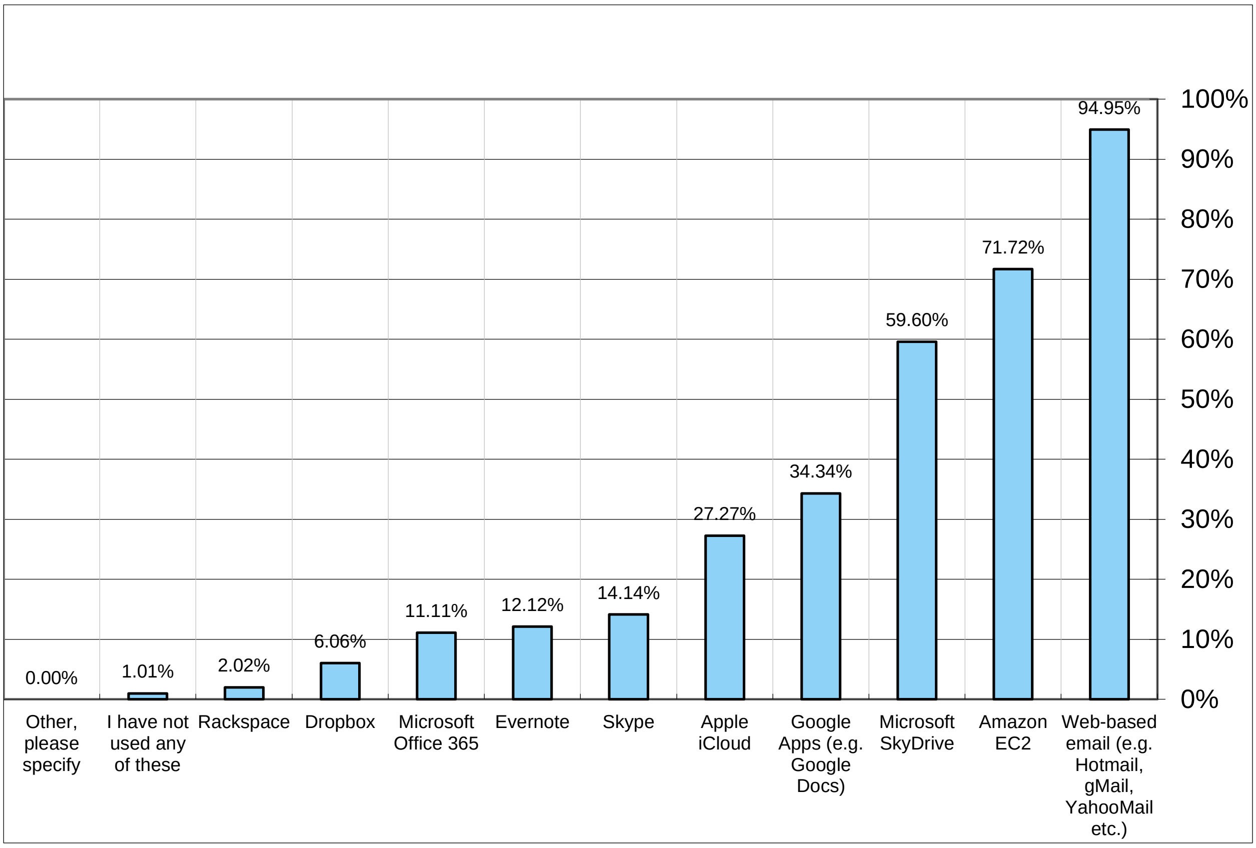


Figure 6.3: Cloud Computing Applications Used by Respondents

It is important to note that from the list of all cloud computing applications that respondents had to choose from, Web-based emails (94.95%), Google Apps (71.72%) and Skype (59.60%) are used by more than half of the respondents. Dropbox (34.34%) and Microsoft 365 (27.27%) were used by about a third of the respondents. Some respondents (2.02%) indicated that they had used other cloud computing applications than those listed in the questionnaire. The applications mentioned by these respondents were Sound Cloud, Windows Azure, Share Point, Oracle and Open Stack.

Notably, only 1 respondent indicated that they had not used any cloud computing applications. This is less than the 11 respondents who could not define cloud computing as reported earlier. Thus, this indicates that the 10 respondents were unaware that applications have used were in fact cloud computing applications. Thus, the respondents have the appropriate level of understanding to provide useful feedback for this survey.

The next section describes the responses to questions related to the benefits of cloud computing.

6.5.2. Questionnaire Findings: Benefits of Cloud Computing

This research project proposes a framework that can be used to enhance the level of user trust in cloud computing applications by providing a decision making tool to influence user adoption. This section describes responses related to the first secondary research question, namely: *How can users benefit from using cloud computing applications?* For this reason, several questions were asked of the respondents with regards to the perceived benefits of using cloud computing.

In order to determine the respondent's perception of the benefits of using cloud computing, they were asked to indicate how important they viewed the commonly reported cloud computing benefits. Respondents were presented with a list of five advantages of cloud computing that were derived from the literature reviewed. These benefits are: available on demand, easily accessible, secure, supported 24/7 and flexible and scalable. The questionnaire respondents were asked to indicate how important each of these benefits was to them as users of cloud computing application and services. The benefits were rated on a Likert Scale which ranged from 1 (Very Unimportant) to 5 (Very Important). Table 6.8 displays the results that were obtained from this question. The results are summarised into Important (which includes responses for Important and Very Important) and Unimportant (which includes Unimportant and Very Unimportant). Additionally, the middle scale (Neither Important Nor Unimportant) is not shown in the table, and thus explains the difference between the results shown and the expected 100%.

Table 6.8: Importance of Cloud Computing Benefits

	Mean	Median	Unimportant	Important
Secure	5 (Very Important)	4.35 (Very Important)	14%	82%

Supported 24/7	5 (Very Important)	4.17 (Very Important)	13%	77%
Available on demand	5 (Very Important)	4.16 (Very Important)	12%	80%
Easily Accessible	5 (Very Important)	4.15 (Very Important)	13%	79%
Flexible and Scalable	5 (Very Important)	4.11 (Very Important)	14%	76%

In terms of the cloud computing services being available on demand, the responses had a mean of 5 (Very Important) and a median of 4.16 (Very Important). A significant majority (80%) of the respondents indicated that this advantage was Important or Very Important. This benefit received the second highest responses on the positive side of the Likert scale.

The results from the questionnaire about the easily accessible benefit of cloud computing had a mean of 5 (Very Important) and a median of 4.15 (Very Important). The advantage was rated as Important or Very Important by 79% of the respondents. This benefit was rated as the third most important benefit by the respondents who value the ability to easily access their stored data when needed from the various cloud computing applications.

The questionnaire results show that security in cloud computing is viewed as the most important benefit by 82% of the respondents. The responses for this benefit have a mean of 5 (Very Important) and a median of 4.35 (Very Important). As described in the previous chapters, security and trust are intertwined. Thus as the respondents view security as an important benefit, they will be similarly concerned about trust issues.

Respondents indicated that 24/7 support as a benefit of cloud computing applications was less important than the first three benefits. The responses for 24/7 support had a mean of 5 (Very Important) and a median of 4.17 (Very Important). 77 % of the respondents indicated that this benefit was Important or Very Important.

The flexibility and scalability benefit of cloud computing was rated lowest in terms of importance. This however, does not mean that flexibility issue is any less important as 76% of the respondents indicated that they found it to be Important or Very Important. Responses for this benefit had a mean of 5 (Very Important) and a median of 4.11 (Very Important).

Responses from an open-ended question asking the respondents to relate an experience they have had with cloud computing revealed some benefits relevant to the categories described above.

These responses are quoted verbatim below and the relevant benefit is indicated in parenthesis after the response:

1. "The cloud applications are very convenient, the ability to have my data with me by a click of a button is very nice." *(Available on Demand; Easily Accessible)*

2. "Cloud computing has enabled me to access computing resources easily and cheaply, which would otherwise be too expensive to purchase." *(Easily Accessible)*

3. "Easily accessible from phone devices." *(Easily Accessible)*

4. "I could access my data anywhere without carrying my laptop around." *(Easily Accessible; Flexibility and Scalability)*

5. "It has helped me to keep my documents intact and ready for use by anyone anywhere there is internet services." *(Available on Demand; Flexibility and Scalability)*

6. "I enjoy the security of the applications." *(Security)*

7. "I have been able to access all information I needed." *(Easily Accessible)*

8. "I have only been using Dropbox and so far the experience has been good. The service has been reliable and is available every time I need to access it." *(Available on Demand)*

9. "I have only used dropbox. I have found it easy and trustworthy to use." *(Easily Accessible; Security)*

10. "I enjoy using it, it makes my life easy, and using Google Apps makes it easy for me I do not have to carry my laptop every day." *(Easily Accessible; Flexibility and Scalability)*

11. "I use dropbox to backup and store my files. It works well and enables me to share files with my friends. That is a very positive experience I had in that regard." *(Flexibility and Scalability)*

12. "It has been great for me. I can do assignments from different devices regardless of where in the country I am. It adds value to efficiency and productivity." *(Easily Accessible; Flexibility and Scalability)*

13. "I can access my documents anytime and anywhere." *(Available on Demand; Easily Accessible)*

14. “My documents and applications are accessible via the network 24 hours and are very secure.” *(Available on Demand; Easily Accessible; Security)*

15. “I recently started using dropbox, it is a great experience to be able to access my data anywhere where I can access internet.” *(Easily Accessible)*

The next section of the questionnaire focused on the key cloud computing barriers and concerns.

6.5.3. Questionnaire Findings: Cloud Computing Barriers and Concerns

As this study seeks to investigate the best ways of enhancing trust in cloud computing and the widespread use of its applications and services, it is important to verify the barriers which inhibit trust, and therefore adoption, of cloud computing. Respondents were asked to indicate barriers and key concerns to trust with regards to cloud computing. The barriers presented to the respondents are based on the most relevant barriers and key concerns to widespread cloud computing adoption which were drawn from the literature reviewed. The effect of the barriers was measured on a Likert Scale which ranged from 1 (Strongly Disagree) to 5 (Strongly Agree). It is important to note that in Table 6.9 the responses are aggregated into Disagree (which includes the Disagree and Strongly Disagree responses) and Agree (which includes the Agree and Strongly Agree responses). The Neither Disagree or Agree responses are not included in Table 6.9 and therefore account for the balance of responses shown.

Table 6.9: Relevant to Barriers to Cloud Computing

	Mean	**Median**	**Disagree**	**Agree**
Security concerns and breaches	4 (Agree)	4.25 (Agree)	4%	81%
Integration issues with existing systems and applications	4 (Agree)	3.74 (Neutral)	11%	65%
Loss of control over data and applications	4 (Agree)	3.96 (Neutral)	13%	72%
Availability and performance concerns	4 (Agree)	4.03 (Agree)	9%	73%
Regulatory, compliance and IT governance concerns	4 (Agree)	3.89 (Neutral)	11%	72%

In terms of security concerns and breaches related to cloud computing services, the responses had a mean of 4 (Agree) and a median of 4.25 (Agree). A significant majority (81%) of the respondents indicated that they agreed that this barrier contributes to trust issues in cloud computing. This barrier received the highest responses on the Agree side of the Likert scale.

The results from the questionnaire about the integration issues with existing systems and applications of cloud computing had a mean of 4 (Agree) and a median of 3.74 (Neither Agree nor Disagree). This barrier was rated as Agree or Strongly Agree by 65% of the respondents. This barrier was rated as the least important barrier by the respondents.

The questionnaire results show that the loss of control over data and applications is viewed as an important barrier by benefit by 72% of the respondents. The responses for this barrier have a mean of 4 (Agree) and a median of 3.96 (Neither Agree nor Disagree).

Respondents indicated that availability and performance concerns with cloud computing applications were the second most important barrier. The responses for this barrier had a mean of 4 (Agree) and a median of 4.03 (Agree). 73% of the respondents indicated that this was a relevant barrier.

The regulatory, compliance and IT governance concerns barrier of cloud computing was rated the same as the loss of control over data and applications. Thus, 72% of the respondents indicated that they found it to be a relevant barrier. The responses for this barrier have a mean of 4 (Agree) and a median of 3.89 (Neither Agree nor Disagree).

Cloud computing users have a number of concerns when it comes to the use of the various applications in cloud computing, as well as the manner in which their data is stored on the cloud computing platform. The main concerns revealed by the literature review include: confidentiality, integrity and availability; reputation of the service provider; Loss of control; privacy; and compliance.

In order to confirm the barriers, respondents were asked to identify which of the listed factors is a concern in relation to their use of cloud computing. Table 6.10 and Figure 6.4 depict the results that the respondents gave with regards to key cloud computing concerns. These responses were reported as a percentage of the users that considered the listed concern to be relevant.

Table 6.10: Summary of Respondents Key Cloud Computing Concerns

	Number of Respondents	**Percentage of Respondents (%)**
Confidentiality, integrity and availability	79	79%
Privacy challenges and concerns (privacy of data and that of users)	65	65%
Loss of control (all technical control being passed to the service provider)	45	45%
Reputation of the service provider or vendor	35	35%
Compliance (with industry regulations and contractual obligations)	22	22%
Other	3	3%

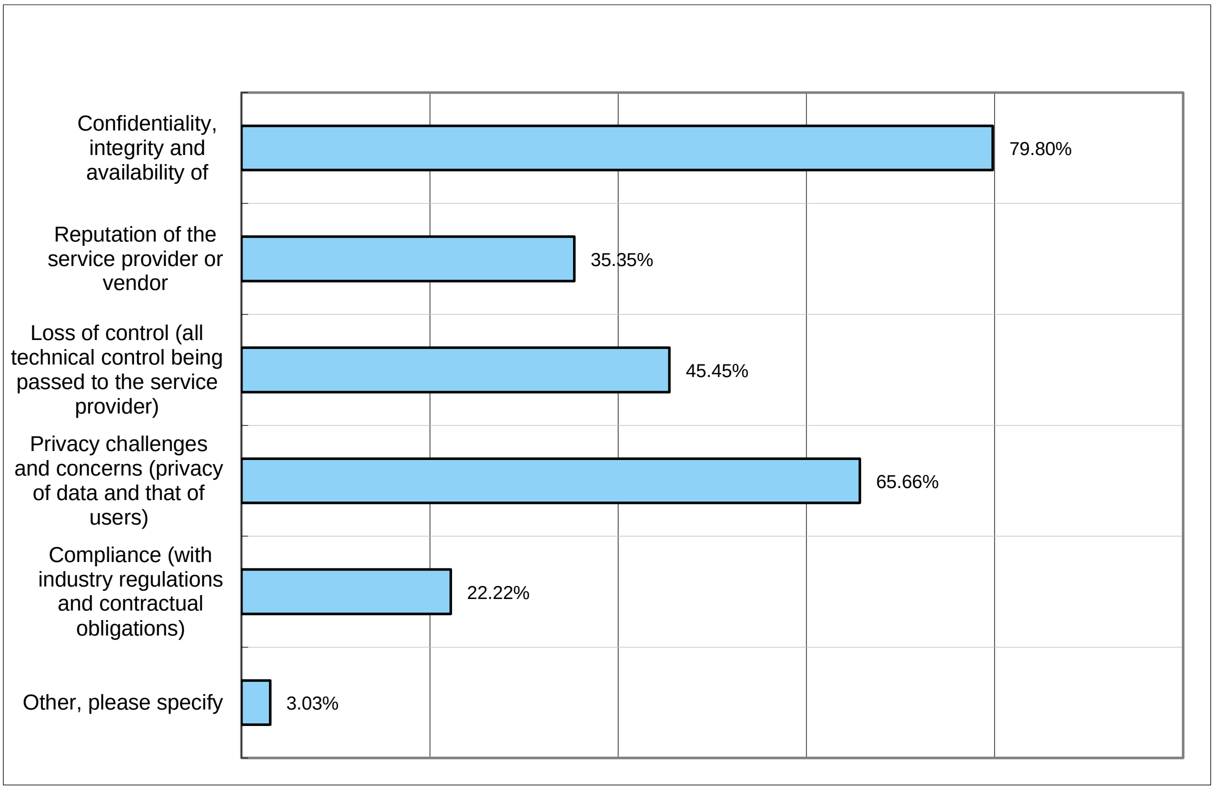


Figure 6.4: Cloud Computing Key Concerns

Results from the questionnaire with regards to the key concerns affecting user trust in cloud computing show that 79% of the respondents indicated confidentiality, integrity and availability issues as a concern. This confirms the concerns identified and mentioned by authors in the literature reviewed.

Privacy challenges and concerns with regards to privacy of data and that of users emerged as the second highest selected cloud computing concern. 65% of the respondents identified the privacy issue as key concern that hinders their level of trust when it came to adopting and continuously using cloud computing applications. The results from the questionnaire therefore indicate that for most users, before they can even consider adopting and using cloud computing applications, need to be assured on the confidentiality and privacy issues. Thus, cloud computing service providers need to provide measures that will ensure the privacy of users and that of their data.

Loss of control of data and applications was recognised as a relevant concern by 45% of the respondents. The reputation of the service providers (35%) and their compliance to regulations (22%) appeared to be less relevant to the respondents. 3% of the respondents identified other concerns as not being able to access the platform if the Internet or electricity is unavailable; and copyright issues regarding original work created or stored on a cloud computing platform.

Further to these barriers and concerns, responses from an open-ended question asking the respondents to relate an experience they have had with cloud computing revealed some barriers relevant to the categories described above. These responses are quoted verbatim below and the relevant benefit is indicated in parenthesis after the response:

1. "Concerned that personal information can leak." *(CIA; Privacy)*

2. "Doubts whether my data will be secured or not." *(Security)*

3. "If the Internet is down its hard to access the information." *(Availability and Performance)*

4. "Internet connection issues." *(Availability and Performance)*

5. "Lack of access to the information." *(CIA; Loss of Control)*

6. "Loss of control over data." *(Loss of Control)*

7. "Problems with ownership, who owns the data in the cloud." (*Compliance)*

8. "Retrieval of information tends to be slow or at times not available." *(CIA; Availability and Performance)*

9. "Security concerns need to be enhanced especially for the end user as security is only limited to general controls." (*Security)*

10. "Slow connections." *(Availability and Performance)*

11. "Sometime back someone once hacked into my account and I had to reset my password." *(Security)*

12. "The cloud applications use a lot of data, so for the mobile user it can be a challenge." *(Availability and Performance)*

These results from the questionnaires confirm that security breaches and concerns, cloud computing integration issues, loss of control, availability and performance factors together with regulatory, compliance and governance issues were key barriers to trust in cloud computing. Feedback from the questionnaire responses also confirmed confidentiality, integrity, availability, reputation of the cloud computing service provider, loss of control and privacy challenges to be the main concerns affecting use trust in cloud computing applications

The next section of the questionnaire focused on factors that would enhance trust in cloud computing.

6.5.4. Questionnaire Findings: Trust Enhancing Factors

The identification of measures to enhance trust in cloud computing adoption is the central theme of this research project. For this reason it was important to identify the factors that the respondents deemed important in order to build trust in a cloud computing application or service. Table 6.11 and Figure 6.5 show the respondent's choices on the factors they consider will enhance their trust in cloud computing applications. These responses were reported as a percentage of the users that considered the listed factor to be relevant.

Table 6.11: Summary of Trust Enhancing Factors

	Number of Respondents	Percentage of Respondents (%)
Security practices	79	79%
Disaster recovery, back up and business continuity plans	66	66%
Accountability (for security and privacy breaches)	65	65%
Reputation and consistency (of the Cloud Computing service provider)	63	63%
Transparency (audit and control measure for cloud computing)	56	56%
Compliance (with industry regulations and contractual obligations)	55	55%
Cloud Computing service provider size, location and number of users	36	36%
Other	3	3%

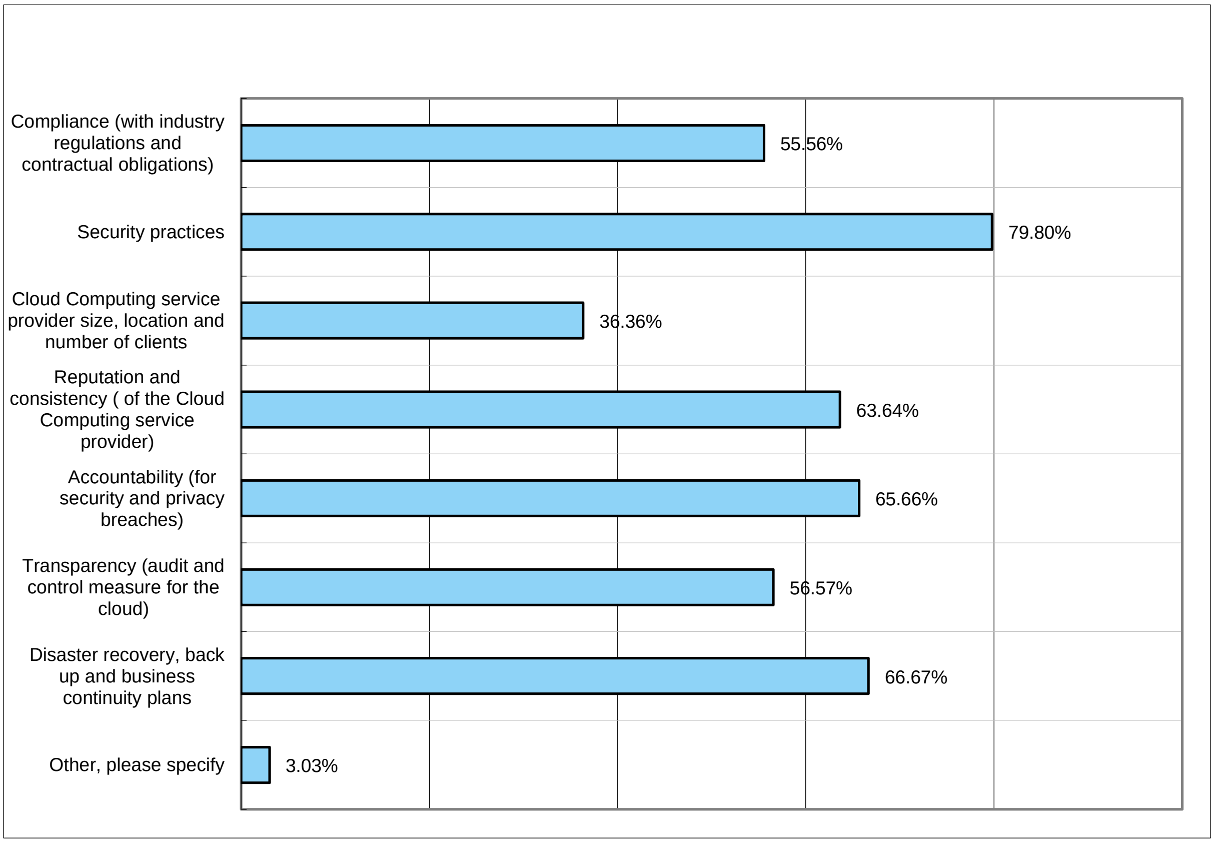


Figure 6.5: Trust Enhancing Factors

The results from the Table 6.11 and Figure 6.5 reveal that the most important factor in enhancing user trust are security related practices. According to the results for most of the respondents (79%) security is an important factor. These results were somehow expected as they are in line and consistent with most of the literature reviewed in this study so far. Thus, service providers would need to provide evidence of the security practices in place in order to enhance user trust.

Two thirds of the respondents considered disaster recovery (66%), accountability (65%) and reputation (63%) as important to enhancing trust in cloud computing. In this regard, users would need to confirm that a cloud computing service has disaster recovery and backup features. In terms of accountability, it would be necessary to enquire or confirm how much responsibility the service provider takes in the event of a breach of user or data privacy. Related to most of the other factors, it is necessary to determine a service provider's reputation. The remaining factors were considered important by fewer respondents. These are: transparency (56%), compliance (55%) and size and location of the cloud computing service provider (36%).

6.6. Conclusion

This chapter presented the data that was collected for this research project by means of a web-based questionnaire. This chapter has dealt with the research findings and results by analysing the findings according to the three research sub-questions identified in this research project. These findings were described in terms of cloud computing knowledge, benefits of cloud computing, concerns and barriers related to cloud computing adoption, and trust-enhancing factors necessary to adopt cloud computing.

From the questionnaires findings it was clear that the respondents did have knowledge on what they termed a typical cloud computing application. The questionnaire also confirmed that some respondents had made use of certain cloud computing applications without them knowing that they were making use of such.

In terms of cloud computing benefits the questionnaires findings reveled that, according to the respondents, the availability of service and data on demand, the easily accessibility of services and data, security of data in cloud computing applications, 24/7 support services offered by the service providers, together with the flexibility and scalability in cloud computing were the most important benefits.

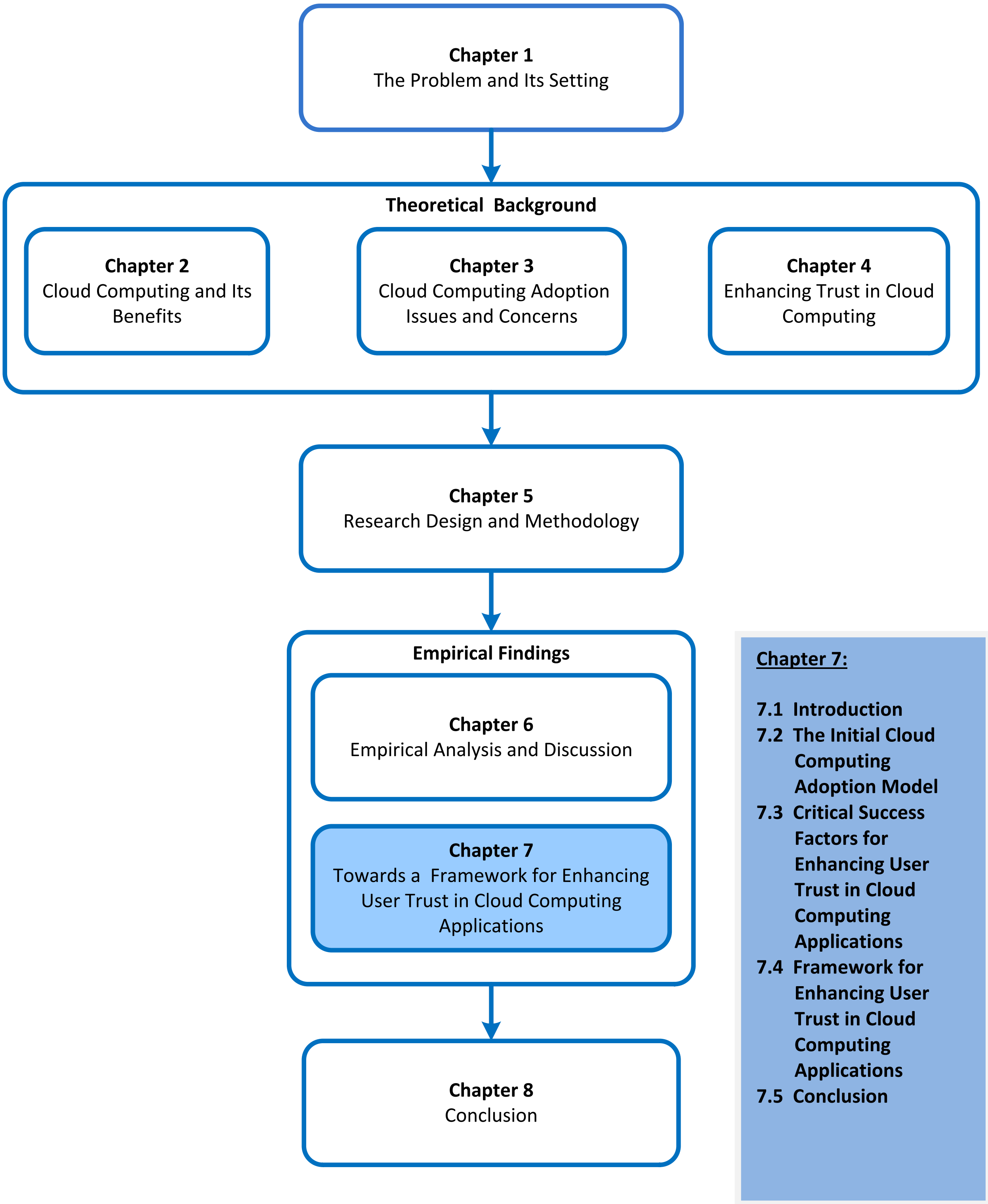
From the questionnaires findings it was found that security breaches and concerns, cloud computing integration issues, loss of control, availability and performance factors together with regulatory, compliance and governance issues were key barriers to trust in cloud computing. The questionnaire also confirmed confidentiality, integrity, availability, reputation of the cloud computing service provider, loss of control and privacy challenges to be the main concerns affecting use trust in cloud computing applications.

It is there clear from the questionnaires findings that security practices, accountability, reputation and consistency of the cloud computing service provider, transparency, services providers compliance with industry regulations and contractual obligations, disaster recovery, back up and business continuity plans, were key factors for enhancing user trust in cloud computing applications. The questionnaire also confirmed that cloud computing service provider size, location and number of users use that particular application played a role in enhancing user trust in cloud computing applications.

There is therefore a need to establish and formulate a framework that users can use to assess the trustworthiness of cloud computing applications before they can adopt and use them. The next chapter provides a detailed discussion of the development of the proposed framework for enhancing user trust in cloud computing applications which is the primary objective of this research project. The proposed framework was based on the literature reviewed and the questionnaire findings that were discussed in this chapter. The remaining primary data collected, in the form of expert reviews used to refine the model, is also provided in the next chapter.

Chapter 7:

Towards a Framework for Enhancing User Trust in Cloud Computing Applications



Chapter 1
The Problem and Its Setting
Theoretical Background
Chapter 2
Cloud Computing and Its Benefits
Chapter 3
Cloud Computing Adoption Issues and Concerns
Chapter 4
Enhancing Trust in Cloud Computing
Chapter 5
Research Design and Methodology
Empirical Findings
Chapter 6
Empirical Analysis and Discussion
Chapter 7
Towards a Framework for Enhancing User Trust in Cloud Computing Applications
Chapter 8
Conclusion

Chapter 7:

7.1. Introduction

Previously in this dissertation, the problem for this study was defined as a lack of user trust in cloud computing applications which impacts on the adoption and use of these applications. Theoretical and empirical literature related to this research problem was then evaluated in the literature chapters. These chapters covered the definitions and benefits of cloud computing, adoption issues and concerns, and strategies to enhance trust in cloud computing. The research design and methodology was described in terms of the relevant Design Science Methodology followed. This led to the discussion of the empirical findings from the questionnaire.

Based on the literature reviewed and the empirical findings from the questionnaire, this chapter describes the formulation of the framework for enhancing user trust in cloud computing. This is the research artefact for this dissertation which is required by the Design Science approach used in this study. Another requirement of Design Science is the use of an iterative process to refine the artefact. Three rounds of expert review were used in this regard.

This chapter begins by explaining the Initial Cloud Computing Trust Model. This model introduced and explained. This model was the initial research artefact based on literature findings. Based on expert reviews of the model and the questionnaire findings, Critical Success Factors (CSFs) for enhancing trust in cloud computing are then described. Further expert reviews led to the development of the final research artefact, namely: the framework for enhancing user trust in cloud computing applications.

7.2. The Initial Cloud Computing Trust Model

Initially, an extensive literature study on trust issues surrounding cloud computing was performed and it informed the construction of the initial cloud computing trust model. Analysis of the reviewed literature points out a number of challenges and factors that affect trust in cloud computing. A number of these trust issues were discussed in the previous chapters of this research project, specifically: security challenges, loss of control, governance issues and privacy challenges surrounding cloud computing. The model represented an assessment of cloud computing literature that was explored and integrated to offer a model to enhance trust in cloud computing. This model was presented at a conference (see Appendix B). Figure 7.2 presents the initial model.

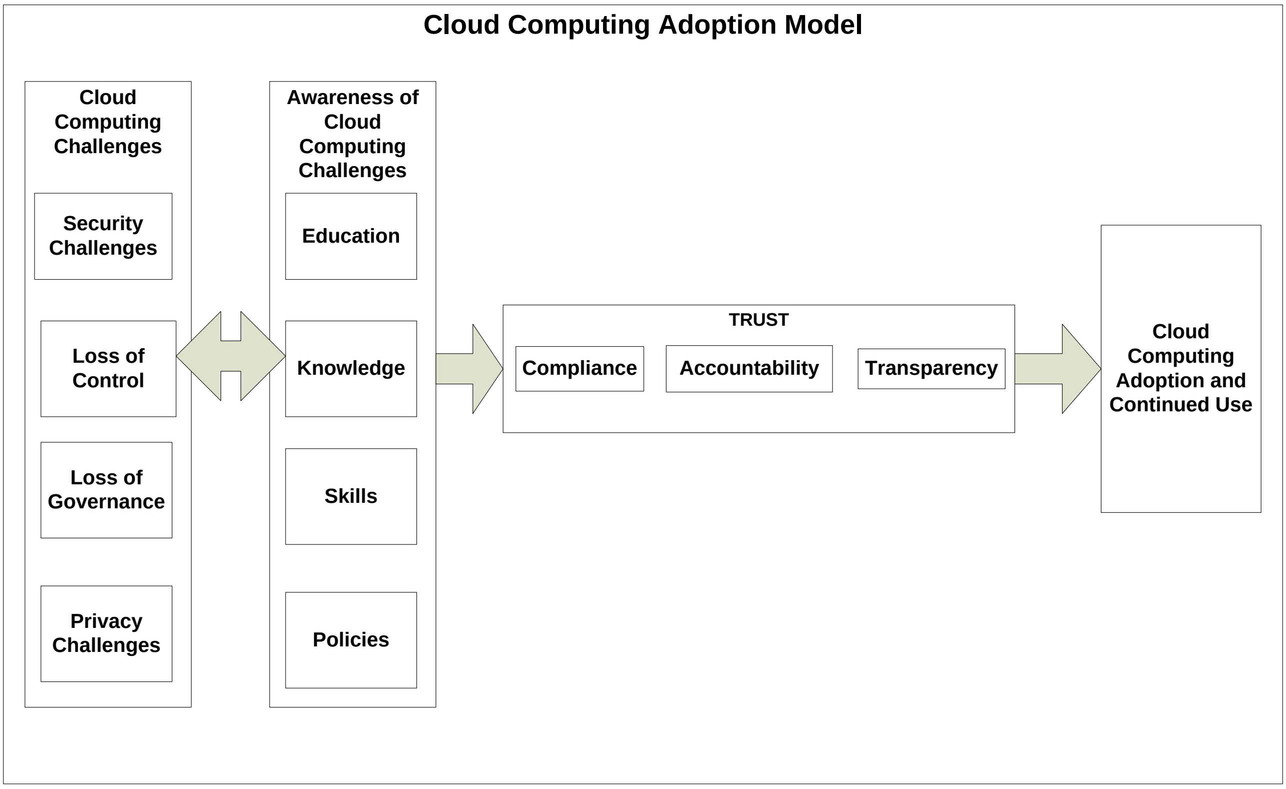


Figure 7.1: Initial Cloud Computing Trust Model

This model identified initial cloud computing challenges and corresponding methods to enhance awareness of these challenges. Once these challenges and the awareness concerns are addressed, trust, in terms of compliance, accountability and transparency can be enhanced. This trust would then lead to cloud computing adoption and continued use. The various phases of this model are discussed in the sections that follow.

7.2.1. Cloud Computing Challenges

The model identifies four major components that are viewed as the four cloud computing challenges which were also identified by Kumar, Sehgal, Chauhan, Gupta and Diwakar (2011). These are established as the main issues that hinder user trust in cloud computing. The model is informed by key portions of cloud computing literature. The four major cloud computing challenges identified by Kumar, *et al*. (2011) are security, loss of control, loss of governance and privacy challenges. These challenges have been described in further detail in Chapter 3.

7.2.2. Awareness of Cloud Computing Challenges

The next aspect of the model deals with awareness amongst the ordinary users of these challenges and the impact on their use of cloud computing. This awareness can be achieved through education, skills, knowledge and cloud computing policies (Nyoni & Piderit, 2012). These factors are discussed in Chapter 4 of this dissertation.

7.2.3. Development of Trust and Adoption of Cloud Computing

In order to develop user trust in cloud computing, the model includes three factors that have been identified to enhance trust in cloud computing adoption. A combination of Compliance, Accountability and Transparency will enhance the level of user trust in cloud computing, eventually leading to the successful adoption and continued use of cloud computing (Nyoni & Piderit, 2012). These factors can be achieved once the challenges and awareness aspects described in the previous section have been addressed.

According to Robinson, Lorenzo, Cave and Starkey (2010), Compliance, Accountability and Transparency are the main issues that underlie and enhance user trust in cloud computing. These are paramount components in ensuring and developing user trust. These trust issues are discussed in detail in Chapter 4. As described in Chapter 1, once trust in the cloud computing application is achieved, the user is willing to adopt and use the application.

7.2.4. Expert Review of the Initial Cloud Computing Trust Model

In order to determine the relevance of the Initial Cloud Computing Trust Model in enhancing trust leading to cloud computing adoption and continued use it was evaluated by three experts in the cloud computing fraternity. These experts recognised the relevance of the model in terms of proposing a solution for a recognised problem and its clarity in attempting to solve this problem of a lack of trust in cloud computing which negatively impacts on adoption and use.

The experts acknowledge that even though there are already a few theories and models that attempt to solve the lack trust in cloud computing most of them do not provide users with clear steps to follow. The proposed cloud computing adoption model was deemed relevant and appropriate to enhance user trust in cloud computing. A key criticism at this stage was that this model was not empirically tested. This was addressed through the questionnaire findings which led to the proposal of CSFs described in the next section.

7.3. Critical Success Factors for Enhancing User Trust in Cloud Computing Applications

These CSFs were developed as a result of the empirical work carried out based on the suggestions of the expert reviews of the initial cloud computing trust model. In order to determine the appropriate CSFs for enhancing user trust in cloud computing, a basic content analysis of key articles in the area of cloud computing was carried out. These content analysis findings were confirmed by the questionnaire findings from this study. This content analysis (Table 7.1) and the questionnaire results from Chapter 6 form the basis for the development of the CSFs, which are instrumental in the framework described later in this chapter.

Table 7.1: Context Analysis of Cloud Computing Concerns (Source: Nyoni & Piderit, 2013)

	Trust	Confidentiality	Integrity	Availability	Security	Adoption	Compliance	Privacy	Risk	Accountability
Mayer, Davis & Schooman (1995)	X		X		X	X			X	
McKnight, Choudhury & Kacmar (2002)	X					X				
Cofta (2007)										
Callewaert, Robinson & Blatman (2009)										
Chow, Golle, Jakobsson, Shi, Staddon, Masuoka & Molina (2009)		X			X			X		
CSA (2009)			X						X	
ISACA (2009)				X		X				
Jerico Forum (2009)	X									
Microsoft (2009)		X		X	X		X			
Pearson (2009)	X	X						X		
Santos, Gummadi & Rodrigues (2009)	X	X	X							
Farrell (2010)			X	X			X		X	
Khajeh-Hosseini, Sommerville & Sriram (2010)						X	X			
Krautheim (2010)	X	X								
Lee & Wan (2010)	X					X				
Lovell (2010)										
LuitBiz (2010)						X				
Ragent & Leach (2010)	X			X						
Robinson, Lorenzo, Cave & Starkey (2010)	X	X			X			X		
Schiffman, Moyer & Vijayakumar (2010)	X									
Shimba (2010)	X	X			X	X				
Callewaert & Luysterborg (2011)	X	X			X			X		
Ernst & Young (2011)			X	X					X	
Ko, Jagadpramana, Mowbray, Pearson, Kirchberg, Liang & Lee (2011)			X							X
Kumar, Sehgal, Chauhan, Gupta & Diwakar, (2011)		X	X	X			X	X		X
Zhang, Liu, Li, Haiqiang & Wu (2011)				X		X				

The content analysis shows trust emerges as the dominant concept in the analysis of research into cloud computing concerns. This, as the central theme of this research project, has been established as the research problem. The other notable factors are: confidentiality, integrity and availability; security; compliance; privacy and accountability. This suggests the importance of these issues, and thus this research project focuses on these concepts in the development of CSFs. Additional factors were found to be relevant upon analysis of the questionnaire findings.

These CSFs are expected to enhance user trust in cloud computing applications. These CSFs were published in a conference paper (see Appendix C). The CSFs described in Table 7.2 were derived from the content analysis and the questionnaire findings that were described in detail in Chapter 6. The CSFs aim to enhance the levels user trust on issues relating to security mechanisms, service level agreements, compliance, confidentiality, control, availability and accessibility. The CSFs proposed are to be considered by a user before adopting and using a new cloud computing platform (Rusman, Van Bruggen, & Valcke, 2009).

Table 7.2: Critical Success Factors for Enhancing User Trust in Cloud Computing

Critical Success Factor	Description
1. Security mechanisms in cloud computing applications must be adequate and operational.	The first CSF is in line with the Ability construct of the Proposed Model of Trust by Mayer, Davis, and Schoorman (1995). It states that in order to enhance user trust, cloud computing service providers must put in place adequate and fully operational security mechanisms. The existence of these security mechanisms must be evident to the user.
2. Service Level Agreements (SLAs) between users and cloud computing service providers must ensure service providers are accountable for inappropriate use of data.	SLAs should assure users that their data is safe and secure all the time. Service providers can enhance user trust by ensuring the users they will be liable and accountable for any inappropriate use of the user's data. This CSF is in line with the Benevolence construct of the Mayer, Davis and Schoorman (1995) Proposed Model of Trust.
3. Cloud Computing service providers must comply with industry regulations.	This factor is based on the Integrity construct from both the Proposed Model of Trust and the confidentiality, integrity, availability (CIA) Triad. It strongly suggests that for any users to trust cloud computing applications, the service provider needs to prove that they are compliant to the set industry regulations that govern the cloud computing community.
4. Cloud Computing Service Providers must ensure confidentiality of user data.	The fourth critical success factor which is based on the Confidentiality construct of the CIA Triad suggests the need of high levels of confidentiality. The CSFs suggests that for cloud computing service providers to enhance user trust, they must assure users that the confidentiality of the users and of their data will be treated with high regard all the time.
5. Users must remain in control of their data in cloud computing applications.	This CSF which is based on the CIA Triad's Availability construct focuses on the control of user data in cloud computing. It suggests that for users to develop and improve their levels of trust in cloud computing applications they need to be assured that

	they will always be in control of their data.
6. User data stored in cloud computing applications must be available for use at all times.	Based on the CIA Triad Availability construct, this CSF suggests that as a measure of enhancing user trust in cloud computing, service providers have to make sure that the users' data is available for use all the time.
7. Users should be able to easily access their data from cloud computing applications.	The last CSF is in line with the CIA Triad's Availability construct and is more concerned with the user's ability to access their data in the cloud computing environment. This CSF suggests that for users to have trust in cloud computing applications, the service providers have to ensure that the users are skilled in order to access their data through various devices.

Each of these CSFs are described in more detail in the following subsections. The underlying literature relevant to the CSF and the questionnaire findings which confirm the necessity of the CSF are also described.

7.3.1. CSF 1: Security Mechanisms

Security of data is one of the major issues that is still seen as an obstacle in the implementation and use of cloud computing (Sood, 2012). This is because the lack of security in cloud computing directly affects and limits the amount of trust users have in cloud computing applications in a negative manner. Therefore this highlights the significant need for service providers to provide visible, adequate and operational security measures in cloud computing applications.

In order for the presence of the security measure to enhance user trust in cloud computing, they must be effective, efficient and fully functional all the time. Sood (2012) suggests and discusses the provision of security through ensuring the presence of the three cryptographic parameters described in the CIA triad. Additionally, the presence of security mechanisms would satisfy the ability construct of the Mayer, Davis and Schoorman (1995) Proposed Trust Model, which is an important underlying theory for this research project. The existence of security measures improves the user's perceptions of the ability of the service provider to maintain the confidentiality, integrity and availability of the data stored through the cloud computing platform.

Empirical findings in Chapter 6 confirm the importance of security mechanisms in order to enhance user trust in cloud computing applications:

1. 82% of the respondents indicated that they considered a secure cloud computing environment as one of the important cloud computing benefits. Thus, ensuring that these mechanisms remain operational would ensure users continue to benefit from cloud computing applications.
2. 81% of the respondents agreed that security concerns and breaches were relevant barriers to cloud computing adoption and use. It is therefore important to implement adequate security mechanisms.
3. 79% of the respondents believed that security mechanisms are relevant for enhancing trust in cloud computing applications. Cloud computing service providers (service providers) can therefore enhance user trust by ensuring user's data security (Sood, 2012).
4. The responses to the open-ended question about cloud computing experiences also raised a number of security-related concerns. Some respondents had experienced security issues and require adequate security mechanisms in order to enhance trust in cloud computing.

Thus, both the literature and empirical evidence points to security mechanisms as an important factor for enhancing trust in cloud computing. It is important that the user is able to verify the existence and adequacy of the security mechanisms.

7.3.2. CSF 2: Service Level Agreements (SLAs)

According to Che, Duan, Zhang and Fan (2011), cloud computing service providers need to satisfy the user's demands on service level agreement (SLA) issues such as security, monitoring, compliance and duty expectations. Under the various SLAs, cloud computing service providers are responsible for the availability and security of elementary services such as infrastructure components and the underlying platform (Che, Duan, Zhang, & Fan, 2011).

The key purpose of the SLA is to reassure the user that the service provider is accountable for any negligent actions which compromise the user and their data. The users therefore need to ensure the SLA contains clauses necessary to protect their interests while using the cloud computing application. An appropriate SLA would therefore reinforce user trust in the cloud computing application.

This is in line with the benevolence construct in the Mayer, Davis and Schoorman (1995) Proposed Model of Trust. This is because the SLA provides reinforcement to the user's belief that the service provider will act in the user's best interests. The issue of accountability and benevolence have been described in Chapter 4.

Empirical evidence from Chapter 6 included findings from the questionnaire which indicate that accountability in the form of SLAs needs to be addressed:

1. Benefits identified by users as important, and thus should be guaranteed by the SLA include: 24/7 support which was identified by 77% of the respondents and the flexibility and scalability of the cloud computing platform which was identified by 76% of the respondents.
2. A notable concern with cloud computing use identified by the respondents was privacy challenges and concerns. This was noted by 65% of the respondents. Accountability of the service provider for ensuring data and user privacy is a key aspect of an SLA (as discussed previously).
3. One of the responses to the open-ended questions was concerned about the copyright of material created and stored on a cloud computing platform. Users should ensure necessary provision is made for this in a SLA.
4. 65% of the respondents indicated that accountability for security and privacy breaches on the cloud computing service provider side will enhance their trust in cloud computing applications.

Thus, the primary goal of the SLA is to ensure the accountability of service providers with regards to inappropriate use of user's data. Additionally, the SLA should include necessary provisions to hold the service provider accountable for technical support and providing consistent service availability.

7.3.3. CSF 3: Compliance With Industry Regulations

As described in Chapter 4, the compliance of cloud computing service providers to set industry regulations is an important trust enhancing factor. Evidence of regulatory and legislative compliance by cloud computing service providers enhances the level of trust that users have in cloud computing. It is important to note that cloud computing service providers and the users can be geographically dispersed. Therefore different regulations may be applicable in these different locations, depending on both the service provider and user locations. Consequently, legislative compliance of cloud computing has to be adequately defined for different service providers in different locations (Holbl, 2011).

This compliance factor is equivalent to the integrity construct of the CIA triad. In order to satisfy this factor, cloud computing service providers need to prove that they are compliant to the relevant regulations. Additionally, integrity is included in the Mayer, Davis and Schoorman (1995) Proposed Model of Trust. This refers to a user's perception that the service provider adheres to a set of principles that the customer finds acceptable. In this case the principles are the industry regulations. The integrity and compliance matters were discussed in Chapter 3 and Chapter 4 respectively.

Empirical findings from the questionnaire detailed in chapter 6 relevant to compliance are:

1. 72% of the respondents indicated that they considered it to be a relevant barrier to cloud computing adoption and use if the service provider did not address the Information Technology (IT) governance concerns and was not compliant with the industry regulations.
2. 22% of the respondents considered compliance to be an applicable concern when implementing cloud computing.
3. 55% of the respondents believe that evidence of a service providers' compliance to industry regulation is necessary to enhance trust in cloud computing.

Thus, cloud computing service provider compliance with necessary regulations is required in order to enhance the levels of user trust in cloud computing applications.

7.3.4. CSF 4: Data Confidentiality

In Chapter 3 some of the major issues in cloud computing such as privacy and confidentiality in cloud computing were discussed. Confidentiality is an important issue for the use of cloud computing applications, both in terms of legal compliance and user trust (Kumar, *et al.*, 2011). Cloud computing users who deal with highly confidential and sensitive information do not necessarily trust the high volumes of data and traffic involved with cloud computing and are therefore reluctant to use cloud computing application for storage of their sensitive data.

Confidentiality has been emphasised as a relevant requirement for cloud computing in Chapter 3. This construct is foremost in the CIA triad. Confidentiality is the prevention of unauthorised disclosure of information. In this regard, the service providers will have to make sure that user's data confidentiality is ensured as this is an important part of the trust relationship between the cloud computing service provider and users. Failure to ensure data confidentiality will have a negative impact on the user's trust in the cloud computing application.

The questionnaire findings validate the inclusion of this factor:

1. 79% of the respondents indicated that confidentiality of the user and their data was a concern.
2. Related to this, privacy of the user's data was also acknowledged as a concern in adopting cloud computing application by 65% of the respondents.

It can be concluded that users are likely to invest more trust in cloud computing applications if the service providers assure them that their data will remain confidential.

7.3.5. CSF 5: Data Control

Literature reviewed in Chapter 3 revealed that cloud computing users typically have no control over the cloud computing infrastructure and the various software applications used. It appears that all technical control is given to the service provider and as a result there is an inherent risk of data exposure to third parties (Kumar, *et al.*, 2011). However, users require complete control over their personal data stored in the cloud computing environment.

Data control matters were discussed in Chapter 3 of this dissertation. According to Holbl (2011), users are conscious of the danger of letting data control out of their hands and storing sensitive data with an outside cloud computing service provider. Issues about control are related to the availability construct of the CIA triad. By ensuring the user has consistent access to their data, the service provider ensures that the user has a perception of control over their data. If the users perceive that they are in control of their data, they are more likely to place trust in the cloud computing application and therefore adopt and use the application.

The questionnaire results discussed in Chapter 6 show that the users are aware of data control factor. The following empirical findings are relevant to data control:

1. 72% of the respondents agree that the loss of control over data and applications is a relevant cloud computing adoption barrier.

2. 45% of the respondents indicated that the loss of control, in terms of all technical control being passed to the service provider, was a key concern when it comes to their trust in cloud computing applications.

It is therefore important that users have control of their data which will in turn enhance their trust in using cloud computing applications for data storage.

7.3.6. CSF 6: Data Availability

Data stored electronically in the cloud computing environment is a valuable asset and should be protected against unauthorised disclosure, tampering or destruction and obstruction to availability to the owners (users) of that data (Wooley, 2011). In the cloud computing context, availability is seen as the guarantee that information will be available to the users in a timely and uninterrupted manner when it is needed regardless of location of the data (Johnson, 2010). This means that the cloud computing infrastructure, the security controls, and the networks connecting the users and the cloud computing infrastructure should always be functioning correctly.

Similar to the data control CSF, data availability relates to the Availability construct from the CIA triad. Thus in order to reduce the impact of user trust concerns on the adoption and use of cloud computing, service providers must aim to ensure constant availability of user data. This also references the ability construct of Mayer, Davis and Schoorman's (1995) Proposed Trust Model. In terms of ability, users trust the cloud computing service provider is capable of providing a consistent service that ensures access to their data. Availability issues were discussed in detail in Chapter 3.

Empirical findings from the questionnaire which are discussed in detail in Chapter 6 show that:

1. 80% of the respondents believe that the availability of their data is a relevant benefit for enhancing of cloud computing applications.
2. 73% of the respondents agree that availability and performance concerns are relevant barriers to cloud computing adoption and use.
3. 79% of the respondents indicated availability, confidentiality and integrity as key cloud computing adoption concerns.
4. Several of the responses to open-ended questions also indicated the criticality of this critical success factor.

Therefore, availability of user data whenever they need it is an important factor when it comes to enhancing trust in cloud computing.

7.3.7. CSF 7: Data Accessibility

According to Holbl (2011), cloud computing is still a service that has to be accessed remotely via the Internet and this might present a problem if the connection between the cloud computing service providers and users is not guaranteed and adequately protected. Accessibility of user data is threatened by downtime, denial of service attacks and network down time (Holbl, 2011). Kumar, *et al.* (2011) further state that cloud computing depends largely on the reliability of secure telecommunications networks. Therefore cloud computing service providers need to assure and guarantee their users undisrupted operations and offer alternative means of data access to user in the case of network or telecommunications failures.

As with the previous two CSFs, data accessibility is related to the availability construct of the CIA triad. Besides ensuring users are able to access the data via appropriate networks, this CSF also refers to the skilling of users to access their data via a cloud computing platform. In this regard, data accessibility issues were discussed in Chapter 4.

Empirical findings from the questionnaire which are discussed in detail in chapter 6 show that:

1. 79 % of the respondents indicated the relevance of the ease of access to their data as an important cloud computing benefit.
2. Related to accessibility, 65% of the respondents indicated that integration issues presented significant barriers to accessing information via cloud computing applications.
3. 63% of the respondents indicated the consistency of the cloud computing service provider is important for enhancing trust in cloud computing.

This means accessibility of user data with ease enhances user trust in cloud computing applications.

7.3.8. Expert Review of the Critical Success Factors (CSFs)

In order to determine the relevance of the CSFs in enhancing trust leading to cloud computing adoption and continued use, the CSFs were evaluated by experts in the cloud computing community. Three expert researchers in the cloud computing field acknowledged the relevancy of the suggested CSFs in solving the problem of a lack of trust in cloud computing applications.

A significant comment from the expert review related to the identification of the most important CSFs which could be considered indicators of trust or trustworthiness of cloud computing service providers. Evidence from the empirical findings indicates that the respondents are concerned about each of these factors to a similar extent.

One reviewer suggested that based on these findings from the questionnaire, and the CSFs identified, it would be useful to create a framework which could assist users in adoption issues. Thus, the framework described in the next section was developed to enhance user trust in cloud computing by providing a means of assessing the trustworthiness of cloud computing applications before they adopt and use the applications.

The issue of control also raised questions amongst the experts who queried how these CSFs would ensure that users have control of their data in the cloud computing environment. Based on the expert's comments on control, it is imperative to point out that for this study control is not viewed as the "physical" control but rather it is viewed as perceived control. As far as the user is concerned, a perception of control is sufficient for the establishment of trust in the cloud computing platform.

7.4. Framework for Enhancing User Trust in Cloud Computing Applications

Based on the expert reviews above, the CSFs are expanded into a framework to assist new cloud computing users to determine the appropriateness of a cloud computing service before adoption and use. In order to structure this decision-making process, the Rogers' (2003) Innovation-Decision Process was used. This process was discussed in Chapter 4.

Thus the CSFs and the 5 stages of the Innovation-Decision process are incorporated into the framework as a way of enhancing trust in cloud computing applications. The proposed framework provides cloud computing users with 5 structured and logical steps to assess and measure the trustworthiness of a cloud computing service provider and applications based on the above mentioned CSFs. The user will be able to use this framework to evaluate cloud computing options and to decide whether or not to use a certain cloud computing application.

7.4.1. Innovation-Decision Process Stages

These stages follow each other in an ordered manner and each of the 5 stages must be satisfied in terms of all seven CSFs before continuing to the next stage. The 5 stages were discussed in detail in Chapter 4, however a description specifically related to enhancing trust in the cloud computing environment is provided below:

1. *The Knowledge Stage*: This is the initial stage where the cloud computing users become aware of the different cloud computing options available for their needs. According to Sahin (2006), an individual at this stage learns about the existence of innovation (cloud computing applications) and seeks information about the innovation. Thus, in the knowledge stage the users must seek information relating to each of the CSFs. Through this process, users begin to develop a better understanding of its abilities, risks and what is expected for them to trust and adopt the innovation (Rogers, 2003). After the user has gathered and assessed the necessary information and understood it with regards to each of the CSFs, they then proceed to the persuasion stage.
2. *The Persuasion Stage*: The persuasion step occurs when the individual has a negative or positive attitude toward the innovation; at this stage the individual is involved more sensitively with the innovation (Sahin, 2006). According to Rogers (2003), here individuals will start developing either a favourable or unfavourable attitude towards the innovation (cloud computing application). The user is involved more sensitively with the cloud computing application with reference to the CSFs at this stage. Having acquired the necessary information in the previous stage, the users make use of the cloud computing application in order to assess the appropriateness of the application in terms of each of the CSFs. At this point, users are looking for practical validation that the application and service provider meet their requirements.
3. *The Decision Stage*: At this decision stage the individual chooses to adopt or reject the innovation (Rogers, 2003). According to the proposed framework, this will be the stage where the user decides to invest trust in cloud computing and the services offered by the service provider. At this point, the user is confident that the cloud computing application is trustworthy based on the knowledge acquired and their interaction with the application during the persuasion stage. Thus, the decision is made to adopt and fully implement the application.

4. *The Implementation Stage:* The implementation stage is when the innovation is adopted and put into practice (Sahin, 2006). This stage involves the actual full implementation and integration of the cloud computing application into the users work. This stage is a result of the outcome of the decision stage. Although the user has decided to adopt and use the cloud computing application, at this stage uncertainty about the use and outcomes of cloud computing still persist and can cause a negative impact on the overall enhancement of user trust at this stage.
5. *The Confirmation Stage*: According to Sahin (2006), at the confirmation stage the individual looks for support for their decision of adopting the innovation. This confirmation depends, to a large extent, on the performance of the cloud computing application and the level of support and help that the user receives from the service provider. Additionally, the user will need to continuously evaluate the cloud computing environment in terms of each of the CSFs.

7.4.2. Expert Review of the Proposed Framework

The experts were asked to analyse, comment and give suggestions on the validity of the proposed framework as a solution for enhancing user trust in cloud computing applications. As this was the final expert review, the reviewers were asked to comment on whether or not previous comments had been appropriately addressed. On a whole, consensus was reached that the proposed framework was an appropriate solution to the given research problem and that previous comments had been adequately addressed.

One relevant concern was raised as the experts felt that it was not clear how the framework should be used. This was taken into consideration as the aim was to produce a user friendly framework to be used as a tool to enhance the level of user trust in cloud computing. The proposed model was therefore refined to that effect, and an explanation as to how to make use of the framework was included in the description of the framework provided in the next section.

7.4.3. The Final Framework and Research Artefact

The refined final framework to enhance the level of user trust in cloud computing is shown in Table 7.3. This research artefact was refined through 3 rounds of expert review and provides a decision making tool to influence user adoption of cloud computing applications.

It is important to note that the proposed framework considers each of the 5 steps of the Innovation-Decision Process. The 5 stages must be assessed in the order shown in the proposed framework to effectively enhance user trust in cloud computing applications. The first column on the left hand side of the framework provides a list of the CSFs that were described in Section 7.4. The first row of the framework presents the stages of the Innovation-Decision Model, namely: Knowledge, Persuasion, Decision, Implementation, and Confirmation. A description of each of these stages was provided in Section 7.5.1.

The users need to assess the cloud computing platform in terms of each of the 7 CSFs in each of the stages. All 7 CSFs must be satisfied before continuing to the next stage. As the final confirmation stage requires a continuous evaluation of the CSFs, it is important to note that should an issue arise in the use of the cloud computing application relating to any of the CSFs, the user should reassess the cloud computing platform beginning again from the knowledge stage.

Table 7.3: Framework for Enhancing Trust in Cloud Computing Applications

Critical Success Factors	**Knowledge**	**Persuasion**	**Decision**	**Implementation**	**Confirmation**
Security Mechanisms	The user is able to locate information about security mechanisms.	The service provider has a reputation of adequate security mechanisms and is able to provide evidence to persuade the user of this.	The user decision to **trust** and Adopt the cloud computing application is made based on the service provider's Security Mechanisms.	The user adopts and uses the cloud computing application based on the outcomes of the Knowledge, Persuasion and Decision stages.	The user's decision to adopt and use the cloud computing application is validated as no security breach is apparent. Thus, the user will continue to use cloud computing and continuously re-evaluate the security mechanisms.
Service Level Agreements (SLAs)	The user is able to locate the relevant SLA.	The SLA should hold the service provider accountable for negligent actions which compromise the user's data.	The user decision to **trust** and Adopt the cloud computing application is made based on the service provider's SLA.	The user adopts and uses the cloud computing application based on the outcomes of the Knowledge, Persuasion and Decision stages.	The user's decision to adopt and use the cloud computing application is validated as the SLA ensures service provider accountability for breaches. Thus, the user will continue to use cloud computing and continuously re-evaluate the SLA.
Compliance with Industry Regulations	The user must investigate and understand the service provider's compliance with industry standards.	Evidence of compliance to industry regulations should be provided.	The user decision to **trust** and Adopt the cloud computing application is made based on the evidence of compliance.	The user adopts and uses the cloud computing application based on the outcomes of the Knowledge, Persuasion and Decision stages.	The user's decision to adopt and use the cloud computing application is validated as the service provider is compliant to industry regulations. Thus, the user will continue to use cloud computing and continuously re-evaluate the service provider's compliance in this regard.

Data Confidentiality	The user must investigate the service provider's data confidentiality policies and mechanisms to ensure confidentiality.	Evidence of confidentiality polices must be established. Accountability for breaches of confidentiality must also be described in the SLA (related to CSF 2).	The user decision to **trust** and Adopt the cloud computing application is made based on the service provider's confidentiality policy and/or SLA.	The user adopts and uses the cloud computing application based on the outcomes of the Knowledge, Persuasion and Decision stages.	The user's decision to adopt and use the cloud computing application is validated as no confidentiality breaches occur. Thus, the user will continue to use cloud computing and continuously re-evaluate the confidentiality policy.
Data Control	The user must investigate the limitations to complete control of their data stored on the cloud computing platform.	Initial use of the application must confirm the user's belief that they have complete control of the data stored on the cloud computing platform.	The user decision to **trust** and Adopt the cloud computing application is made based on the user's perception of control over their data.	The user adopts and uses the cloud computing application based on the outcomes of the Knowledge, Persuasion and Decision stages.	The user's decision to adopt and use the cloud computing application is validated as the user perceives that they are in control of the data. Thus, the user will continue to use cloud computing and continuously re-evaluate their perception of data control.
Data Availability	The service provider's reputation in terms of data availability must be investigated.	The user must be satisfied that the service provider can provide a consistent service, and that fail-safe measures are in place for any unexpected network faults.	The user decision to **trust** and Adopt the cloud computing application is made based on the service provider's service consistency.	The user adopts and uses the cloud computing application based on the outcomes of the Knowledge, Persuasion and Decision stages.	The user's decision to adopt and use the cloud computing application is validated as no availability issues exist. Thus, the user will continue to use cloud computing and continuously re-evaluate the availability of the data.
Data Accessibility	Factors which may lead to the inaccessibility of the user data must be investigated and understood.	The user must feel assured that they are able to easily access their data and that the cloud computing application is not overly-complicated in terms of their abilities.	The user decision to **trust** and Adopt the cloud computing application is made based on the user's ability to easily access their data on the application.	The user adopts and uses the cloud computing application based on the outcomes of the Knowledge, Persuasion and Decision stages.	The user's decision to adopt and use the cloud computing application is validated as no data accessibility issue is apparent. Thus, the user will continue to use cloud computing and continuously re-evaluate the accessibility of the data.

7.5. Conclusion

This study aimed to propose a framework that can be used to enhance the level of user trust in cloud computing by providing a decision making tool to influence user adoption. This framework aims to solve the underlying research problem of a lack of user trust which impacts on the adoption and use of cloud computing applications. In order to achieve this, the framework combined together two elements:

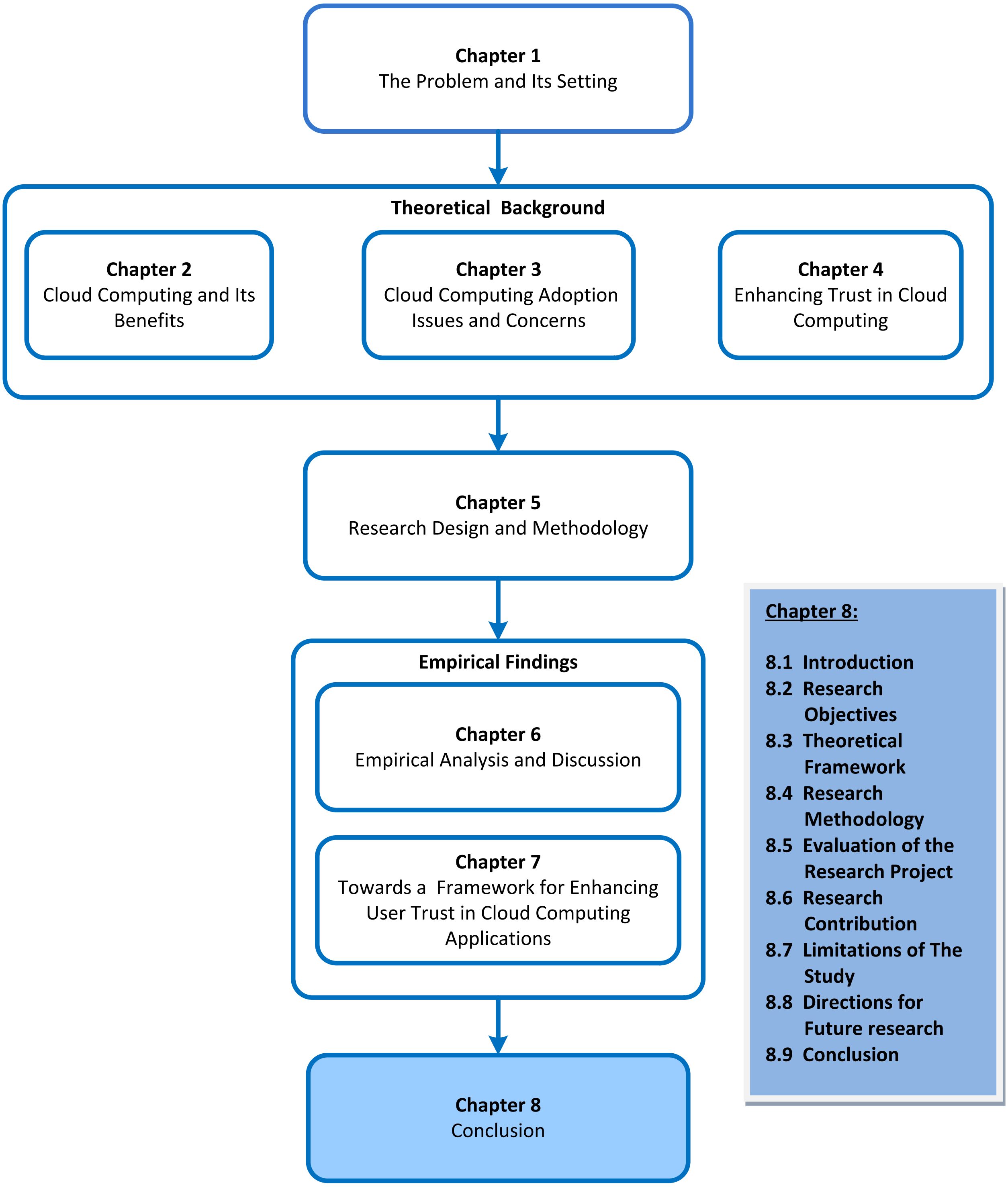
1. The CSFs for enhancing user trust in cloud computing application as described in Section 7.4; and
2. The Innovation-Decision Process adapted from Rogers' (2003) Diffusion of Innovations Theory.

This framework was developed based on an initial trust model and CSFs defined based on the findings from the questionnaire. This chapter provided a detailed explanation of both the initial model and the seven CSFs which are key components of the proposed framework. The seven CSFs were identified relating to security, accountability, compliance, confidentiality, control, availability and accessibility. The CSFs proposed here are to be considered by a user before adopting and using a new cloud computing platform.

The refinement of the initial proposed model and the CSFs through to the proposed framework by means of expert reviews are also detailed in this chapter. Following this refinement, the main contribution of this research project is the framework for enhancing user trust in cloud computing applications. The following chapter will provide a summative conclusion for this study.

Chapter 8:

Conclusion


Chapter 1
The Problem and Its Setting
Theoretical Background
Chapter 2
Cloud Computing and Its Benefits
Chapter 3
Cloud Computing Adoption Issues and Concerns
Chapter 4
Enhancing Trust in Cloud Computing
Chapter 5
Research Design and Methodology
Empirical Findings
Chapter 6
Empirical Analysis and Discussion
Chapter 7
Towards a Framework for Enhancing User Trust in Cloud Computing Applications
Chapter 8
Conclusion

Chapter 8:

- **8.1 Introduction**
- **8.2 Research Objectives**
- **8.3 Theoretical Framework**
- **8.4 Research Methodology**
- **8.5 Evaluation of the Research Project**
- **8.6 Research Contribution**
- **8.7 Limitations of The Study**
- **8.8 Directions for Future research**
- **8.9 Conclusion**

8.1. Introduction

The research problem to be investigated by this study was defined in Chapter 1 of this dissertation. Thus, the remaining chapters set out to propose a solution to this problem, namely: the lack of user trust in cloud computing applications which impacts on adoption and use of the applications. Following this, the theoretical background for this study was discussed in Chapters 2, 3 and 4. Chapter 5 highlighted the research design and methodology applied in the study, which resulted in the empirical findings which were provided in Chapter 6.

The previous chapter of this research project discussed the findings and recommendations of the study and proposed a framework that can be used to enhance user trust in cloud computing applications. The findings were presented in response to the research question and sub-questions, which constituted the framework within which the findings were discussed. The framework presented in this study was based on secondary data collected from a review of relevant literature and from primary data obtained through a web-based questionnaire. The elements of the framework were then refined through the use of expert reviews, which satisfied the Design Science Methodology requirement that the research artefact be evaluated.

This chapter provides a brief summative discussion and conclusion of the research project. In this regard, this final chapter reviews the research objects, theoretical framework, and research methodology. An evaluation of the credibility of the study is then described. The applicable contributions, limitations and directions for future research are then outlined.

8.2. Research Objectives

This research project aimed to investigate and solve the problem of a lack of user trust in cloud computing that hampers the widespread adoption and use of cloud computing applications. The research question that this study investigated was: *How can user trust in cloud computing applications be enhanced to ensure use?* Therefore, the primary objective of this research project was to formulate a framework that could be used to user trust in cloud computing applications to ensure adoption and continued use. This was achieved in the proposed framework described in Chapter 7.

In order to achieve the primary objective and answer the primary research question, the following secondary research questions were investigated:

1. *How can users benefit from using cloud computing applications?*

The literature survey in Chapter Two was used to answer this secondary research question. From the literature reviewed a clear definition of cloud computing was provided together with the various types of cloud computing deployment and delivery models. In addition, the definitions of the numerous benefits of cloud computing was outlined, namely: improved resource optimisation, greater flexibility and access, reduced cost, easy deployment and management of applications and disaster recovery and backup to users of cloud computing applications.

From the empirical findings, the key cloud computing benefits were confirmed. These findings were obtained through the web-based questionnaire. In particular, respondents agreed that availability of their data in the cloud computing environment on demand, its accessibility and security were the relevant and important benefits for enhancing trust in cloud computing applications. This led to the inclusion of the elements of availability, accessibility and security amongst the critical success factors (CSFs) for enhancing user trust in cloud computing applications.

2. What are the key concerns affecting user trust in cloud computing applications?

The theory of this secondary research question was addressed in Chapter Three. From the literature review the limitations of cloud computing in terms of user trust were described. The key concerns evident from the literature included: interpersonal factors, security challenges, loss of control, governance concerns, and privacy challenges. In terms of theoretical contributions, the Confidentiality, Integrity, Availability (CIA) triad provided a relevant basis for this aspect of the study.

From the empirical findings, aspects relating to the key concerns were confirmed. From the questionnaire findings, factors relating to the security challenges, loss of control, and privacy were confirmed. In particular, respondents agreed that integrity coupled with availability and confidentiality were relevant key concerns that affected their trust in cloud computing applications.

3. How can the trust barrier be overcome to enhance trust in cloud computing applications?

The theory of this research objective was addressed in Chapter Four. In this chapter, an applicable definition of trust was provided and several trust models were evaluated. The Mayer, Davis and Schoorman (1995) Proposed Trust Model was determined to be the most relevant for this study. From the literature survey it has been noted that knowledge, education and skill;

awareness of perceived benefits; compliance; accountability and transparency are useful for enhancing user trust in cloud computing. In terms of assisting the decision making process of cloud computing adoption, the Rogers (2003) Innovation-Decision process was discussed.

The empirical findings show that to enhance user trust in cloud computing, security, accountability, reputation and consistency, transparency and compliance need to be addressed. The service providers have to ensure that these factors are adequately dealt with.

Based on these theoretical and empirical findings the framework for enhancing user trust in cloud computing was proposed. This was then refined through expert reviews. The refined model which fulfils the primary objective of this research project was then presented. The study objective has thus been addressed through collectively addressing the research sub-questions.

8.3. Theoretical Framework

In order to develop the proposed framework for enhancing trust in cloud computing applications, a number of frameworks were used, namely: the Proposed Trust Model by Mayer, Davis and Schoorman (1995), Confidentiality, Integrity, Availability (CIA) Triad by Steichen (2010), the Diffusion of Innovations Theory proposed by Rogers (2003) (specifically the Innovation-Decision Process).

Mayer, Davis and Schoorman’s (1995) Proposed Model of Trust distinguishes between trustor and trustee characteristics that foster a trusting relationship between the two parties. Thus, this model is appropriate for the context of user and service provider relationships in cloud computing. The trustor characteristics provide a frame of reference for evaluating a cloud computing service provider, and the trustee characteristics describe the end-user. Mayer, Davis and Schoorman (1995) propose three characteristics that form a foundation for the perception of trustworthiness relevant to this study, namely: ability, benevolence and integrity.

The CIA Triad is an industry-accepted model for ensuring security in systems in order to further enhance trust in the systems. It specifically focuses on the storage and management of data. The CIA Triad focuses on the confidentiality, integrity and availability (Steichen, 2010).

The model by Rogers (2003) is a widely used theoretical framework in the area of new technology diffusion and adoption. Rogers’s Diffusion of Innovations Theory is the most appropriate for investigating the adoption and use of cloud computing by users. However, it is the 5 stages of Innovation-Decision Process that are relevant in the formulation of a framework aimed at enhancing trust in cloud computing applications by providing an aid to their decision making process. The Innovation-Decision Process involves five steps which are knowledge, persuasion, decision, implementation, and confirmation. These steps provide the structure for the decision-making process in the framework.

8.4. Research Methodology

This study was conducted within an interpretivist paradigm. The research methodology applicable was the qualitative approach as this is consistent with the interpretivist paradigm adopted for the study. The Design Science Methodology was used in this study. With regards to Design Science research, this research project adopted and used Hevner, March, Park and Ram's (2004) seven guidelines. These are the most appropriate set of guidelines for Design Science research and are thus relevant in this study. The seven steps were adopted in this research project as shown in Table 8.1 below:

Table 8.1: Relevance of the Design Science Guidelines

Design Science Research Guideline	Description and Relevance in the Study
1. Design as an Artefact	This study produced a framework for enhancing user trust in cloud computing applications.
2. Problem Relevance	For this study the problem under investigation is the lack of trust in the use of cloud computing applications. A solution in the form of the proposed framework was provided for end-users to adopt and use.
3. Design Evaluation	The research model is evaluated through applicable data gathering and analysis techniques that were discussed in detail in the previous chapters.
4. Research Contributions	The contribution of this study is the proposed framework, which is considered to enhance user trust in cloud computing applications.
5. Research Rigor	In terms of rigor, the research project employed valid data gathering and analysis techniques and the components of the framework were evaluated using expert review.
6. Design as a Search Process	This guideline was satisfied through the collection of related primary data and secondary data .
7. Communication of Research	This guideline is satisfied by the publishing of two publications included as Appendix B and C. A third publication is currently under review for the final framework from this study.

This research project made use of a web-based questionnaires and expert reviews as primary data collection methods, and literature review for secondary data collection. The literature survey formed the theoretical base for this study. This theoretical base and the empirical findings from the questionnaire led to the development of the proposed framework. The proposed framework was then evaluated using the expert reviews.

8.5. Evaluation of the Research Project

Evaluation of the research project ensures that the research is credible and trustworthy. The evaluation and validation of this study complies with the Design Science Methodology as shown in Table 8.1. Research evaluation is a necessary step in order to ensure the credibility and integrity of the research project. Oates's (2006) evaluation criteria for interpretivist research were adopted for this study. These are described briefly below.

1. *Trustworthiness*: The trustworthiness of the experts used to refine the proposed framework was evaluated. The experts used in this process are respected in the new technology adoption field. Thus, the recommendations made by these experts can be considered trustworthy.
2. *Confirmability*: The use of the questionnaire findings confirmed the theoretical findings. This led to the development of the research framework which was then confirmed through expert reviews.
3. *Dependability*: Dependability is established through the use of literature from recognised authors and the contribution from experts in the field of study in the form of the expert review. The use of established theories and models that have been tested in numerous research projects add to the dependability of this project. The theories and models used in this study include the Proposed Trust Model by Mayer, Davis and Schoorman (1995), CIA Triad by Steichen (2010), and the Diffusion of Innovations Theory proposed by Rogers (2003).
4. *Credibility*: Credibility has been achieved through the use of multiple data collection techniques, the use of expert review and the publication of two articles.
5. *Transferability*: Transferability has been achieved as the research framework can be applied by users on other new technologies with similar characteristics.

Through the application of these five criteria, the research project can therefore be considered credible.

8.6. Research Contribution

Previous studies have focused their contribution mostly on establishing the vast advantages and benefits of using cloud computing, however, very few focus on strategies that enhance user trust in cloud computing applications (Shimba, 2010). Thus, considering these previous studies, this research project suggested a framework that aims to enhance user and potential user trust in cloud computing by providing a means of evaluating the cloud computing application. This will ensure adoption and widespread use of cloud computing applications.

This research project contributes to the body of information systems (IS) knowledge regarding the enhancement of user trust in cloud computing applications. This study set out to develop a framework to enhance user trust in cloud computing applications, thereby improving the adoption and the widespread use of cloud computing.

The framework developed, proposed and discussed in Chapter Seven is the primary contribution of this research study. The developed framework is the extension of a previously proposed Cloud Computing Trust Model and CSFs suggested in the published papers attached here as Appendix B and Appendix C and described in Chapter 7.

The specific contribution made through the development of this framework was the proposal of an evaluation framework that users and potential cloud computing users can use to evaluate the trustworthiness of cloud computing applications provided by service providers.

8.7. Limitations of the Study

This study addresses the lack of user trust in cloud computing. A specific focus of this research project was to enhance user trust in cloud computing applications. The enhancement of trust in cloud computing was restricted to end-users view. The enhancement of trust in cloud computing was not investigated from the service provider point of view. This limitation of the study is acknowledged and also provides a direction for future research as described below.

8.8. Directions for Future Research

Further research can be undertaken to explore more factors and issues that impact on trust in cloud computing applications. In addition, researchers might also explore trust enhancing factors from the cloud computing service provider’s perspective as described in the limitations above.

8.9. Conclusion

This research project presented a study of user trust in cloud computing, in particular the lack of user trust in cloud computing applications that hinders adoption and use. The outcome of this study was the development of a framework for enhancing user trust in cloud computing applications. The significance of this study will be the enhancement of end-user trust in cloud computing, that will be seen through the improvement in cloud computing application adoption and continued use.

This conclusion chapter provided a summary of the research objective followed by that of the theoretical framework used to direct this study. The next section summarised the research methodology. The evaluation of the research project and the research contribution of this study were described. This chapter concluded with a description of the limitations of the study and direction for future research.

Reference List

Ahronovitz, M., Amrhein, D., Anderson, P., Arasan, E., Bartlett, J., Bruklis, R., (2010). Cloud Computing Uses . *Cloud Computing Use Case Discussion Group. Version 4.0*. 1-63.

Alam, S., & Noor, M. (2009). ICT Adoption in Small and Medium Enterprise: An Emprical Evidence of Seervice Sectors in Malaysia. *International Journal of Business and Management Vol.4.No 2* , 112-125.

Alliance, L. C. (2009). Awareness, Trust and Security to Shape Government Cloud Adoption. *Emerging Technology Markets in the U.S. Federal Government, 2009-2014* .

Amrhein, D., & Anderson, P. (2009). Cloud Computing Use Cases. *Cloud Computing Use Case Discussion Group*.

Avgerou, C., Ganzaroli, A., Poulymenakou, A., & Reinhard, N. (2007). ICT and citizens' trust in government: lessons from electronic voting in Brazil. *Information Communications Technologies and Regional Integration*.

Baize, E. (2011). In Cloud We Trust.

Blanche, M. T., Durrheim, K., & Painter, D. (1999). Research in Practice: Applied Methods for the Social Sciences. Cape Town: University of Cape Town Press.

Boss, G., Malladi, P., Quan, D., Legregni, L., & Hal, H. (2007). Cloud Computing. *IBM Corporation 2007 Version 1.0* , 1-17.

Bourne, V. (2010). Rising to the Challenge. *2010 Global IT Leadership Report* .

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2008). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems 25 (2009)* .

Callewaert, P., & Luysterborg, E. (2011). Security,Trust and Risk. *Cloud Computing Forecasting* .

Callewaert, P., Robinson, P. A., & Blatman, P. (2009). Cloud computing Forecasting change. *Deloitte Consulting Cloud computing Market overview and perspective* , 1-63.

Capers, J. (2010). *Software Engineering Best Practices.* USA: Mc Graw- Hill Companies.

Catteddu, D., & Hogben, G. (2009). Benefits, risks and recommendations for information security. *Enisa 09* .

Che, J., Duan, Y., Zhang, T., & Fan, J. (2011). Study on the security models and strategies of cloud computing. *2011 International Conference on Power Electronics and Engineering Application* (pp. 586 – 593). Elsevier Ltd.

Chen, L., Gillenson, L. M., & Sherrell, D. L. (2004). *Consumer acceptance of virtual stores: a theoretical model and critical success factors for virtual stores.* New York: AGM.

Chervany, N. L., & McKnight, D. H. (2001). Conceptualising trust: A typology and e-commerce customer relationships model. *Proceedings of the thirty-fourth Hawaii International Conference on System Sciences*, (pp. 883-888).

Childerhouse, P., Hermiz, R., Mason-Jones, R., Popp, A., & Towill, D. (2003). Information flow in automotive supply chains - identifying and learning to overcome barriers to change. *Industrial Management and Data Systems , 103* (7), pp. 491-502.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., et al. (2009). Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. *CCSW'09* , 1-10.

Cicso. (2009a). Private Cloud Computing for Enterprises: Meet the Demands of High Utilization and Rapid Change. *Cisco C11-543729-00 06/09* , 1-13.

Cisco. (2009b). Cisco Cloud Computing - Data Center Strategy, Architecture, and Solutions. 1 -16.

Cofta, P. (2007). *Trust, Complexity adn Control.Confidence in a Convergent World*. Ontiario: John Wiley.

Collis, J., & Hussey, R. (2009). *Bussiness Research A Practical Guide For Undergraduate and Postgraduate Students.* New York: Palgrave Macmillan.

Cooper, D., & Schindler, P. (2003). *Business research methods* (8th ed.). New York: McGraw-Hill/Irwin.

CSA. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. 1-76.

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, And User Acceptance of Information Quality. *MIS Quarterly* , 318-340.

Ernst, & Young. (2011). Into the cloud, out of the fog. *Global Information Security Survey* , 1-36.

Farrell, R. G., Rajput, N., Das, R., Danis, C., & Dhanesha, K. (2010). Social navigation for the spoken web. Proceedings of the fourth ACM conference on Recommender systems (RecSys '10) (pp. 333-336). New York: ACM.

Foley, P., Alfonso, X., & Ghani, S. (2002). The digital divide in a world city.

Gasser, L., Majchrzak, A., & Markus, M. (2002). Design theory for systems that support emergent knowledge processes. *MIS Quarterly, 26*(3), pp. 179-212.

Gopalakrishnan, A. (2009). Cloud Computing Identity Management. *SETLabs Briefings Vol 7 No 7* , 45-58.

Herzum, D. (2006). Web Service and Service Orinted Architectures. *Computers and Security* , 200-204.

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

Hofstee, E. (2006). *Constructing a Good Dissertation A Practical Guide to Finishing a Master's, MBA or PhD on Schedule.* Sandton: EPE.

Holbl, M. (2011). Cloud Computing Security and Privacy Issues. *CEPIS LSI SIN (10) 02* , 1-4.

Huang, J., & Fox, M. (2006). An ontology of trust - formal semantics and transitivity. . *ICEC* , 256-259.

IBM Research. (2010). Benefits of Cloud Computing. *IBM* .

ISACA. (2009). Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives. *ISACA Emerging Technology White Paper* , 1-10.

Jayathilake, H. A., Jayaweera, B. A., & Waidyasekera, E. C. (2006). ICT Adoption and It's Implications for Agriculture in Sri Lanka. 54-62.

JERICHO (2009) Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration

V1.0 (Position Paper). Jericho Forum

Johnson, B. C. (2010). Information Security Basics. *ISSAJ vol 8 no 7* , 28-32.

Johnston, S. (2009). *Cloud Computing Types: Public Cloud, Hybrid Cloud, Private Cloud.*

Joshi, T., Joshi, B. D., & Ahn, G. (2010). Security and Privacy Challenges in Cloud Computing Environmemnts. *Cloud Computing* .

Kabbar, E. F., & Crump, B. J. (2009). The Factors that Influence Adoption of ICTs by Recent Refugee Immigrants to New Zealand. *Informing Science Journal Volume 9*, 112-121.

Keane. (2011). Cloud Computing. *Application and Infrastructure Solutions: Keane White Paper* , 1-15.

Khajeh-Hosseini, A., Sommerville, I., & Sriram, I. (2010). Research Challenges for Enterprise Cloud Computing. *Computer-Communication Networks C.2.4* , 1-11.

Knode, R. (2009). Exploring Security and Trust in the Cloud. *Business Solutions Technology* .

Ko, R. K., Jagadpramana, P., & Lee, B. S. (2011). Flogger: A File-centric Logger for Monitoring File Access and Transfers within Cloud Computing Environments. *HP Laboratories HPL-2011-119* , 1-8.

Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., et al. (2011). TrustCloud: A Framework for Accountability and Trust in Cloud Computing. *Cloud & Security Lab* , 1-5.

Krautheim, F. J. (2010). Private Virtual Infrastructure for Cloud Computing. 1-5.

Kumar, P., Sehgal, K. V., Chauhan, D. S., Gupta, P. K., & Diwakar, M. (2011). Effective Ways of Secure, Private and Trusted Cloud Computing. *IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3,* , 412-422.

Lee, C. P., & Wan, G. (2010). Including Subjective Norm and Technology Trust in the Technology Acceptance Model:A Case of E-Ticketing in China. *The DATA BASE for Advances in Information Systems Volume 41, Number 4* , 40-51.

Li, H., Sedayao, J., Hahn-Steichen, J., Jimison, E., Spence, C., & Chahal, S. (2009). Developing an Enterprise Cloud Computing Strategy. *Developing an Enterprise Cloud Computing Strategy IT@Intel White Paper* . United States of America: Intel Corporation.

Li, X., Valacich, J., & Hess, T. (2004). Predicting user trust in information systems: A comparison of competing trust models. *37th Hawaii International Conference on System Science*, (pp. 1-10).

Lin , S. W., & Fu, P. H. (2012). Uncovering Critical Succcess Factors for Business-to-Customer Electronic Commerce in Travel Agencies. *Journal of Travel & Tourism Marketing, 29(6)* , 566-584.

Locke, S. (2004). ICT Adoption and SME Growth in New Zealand. *The Journal of American Academy of Business, Cambridge* , 93-102.

Lovell, R. (2010). Business IT on Demand. *ThinkGrid* .

Luhmann, N. (1988). *Trust and power*. Chichester: Wiley.

LuitBiz. (2010). What is Cloud Computing. *Luit Infotech* .

Maxwell, J. (2005). *Qualitative Research Design: An Interactive Approach*. California: SAGE Publications.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review 20(3)* , 709-734.

Myers, M. D. (2009). *Qualitative Research in Business & Management*. London: Sage Publications.

McKnight, D. H., Choudhury, V., & Kacmar, M. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research* , 334-359.

McKnight, H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *Journal of Strategic Information Systems , 11,* pp. 297-323.

Meade, F. (2009). Cloud Computing-Overview of Information Assurance Overview of Information Assurance. *JAD* , 1-8.

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. *NIST Special Publication 800-145* , 1-7.

Microsoft. (2009). Privacy in the Cloud Computing Era A Microsoft Perspective. *Microsoft* .

Moorman, C., Deshpande, ,. R., & Zaltman, G. (1993). Factors Affecting Trust in Market Research Relationships. *The Journal of Marketing, Vol. 57, No. 1* , 81-101.

Mouton, J. (2005). *How to succeed in your Masters and Doctoral Studies.* Pretoria: Van Schaik Publishers.

Muriithi, G. M., & Kotzé, J. E. (2012). Cloud computing in higher education: implications for South African public universities and FET colleges. *PROCEEDINGS OF THE 14th ANNUAL CONFERENCE ON WORLD WIDE WEB APPLICATIONS* (pp. 1-24). Cape Town: Cape Peninsula University of Technology.

Nyoni, T. B., & Piderit, R. (2012). Enhancing trust in cloud computing. *PROCEEDINGS OF THE 14th ANNUAL CONFERENCE ON WORLD WIDE WEB APPLICATIONS* (pp. 1-16). Cape Town: Cape Peninsula University of Technology.

Nyoni, T., & Piderit, R. (2013). Towards a model for enchancing user trust in cloud computing applications. *Joint International Conference on Engineering Education and Research and International Conference on Information Technology* (pp. 59-67). Cape Town: Cape Peninsula University of Technology.

Oates, B. (2006). *Researching Information Systems and Computing.* London: SAGE Publications.

Pearson, S. (2009). Taking Account of Privacy when Designing Cloud Computing Services. *ICSE'09 Workshop* , 44-52.

Penn, J. (2010). Protecting your brand in the cloud:Transparency and trust through enhanced reporting. *Forrester Research*, 1-7.

Ragent, F., & Leach, C. (2010). Can You Trust the Cloud? A Practical Guide to the Opportunities and Challenges Involved in Cloud Computing. *Cloud Computing Whitepaper*, 1-12.

Robinson, N., Lorenzo, V., Cave, J., & Starkey, T. (2010). The Cloud: Understanding the Security, Privacy and Trust Challenges. *Information Society and Media TR-933-EC* .

Rogers, E. M. (2003). *Diffusion of Innovations, 5th Edition.* Simon and Schuster.

Rusman, E., Van Bruggen, J., & Valcke, M. (2009). Emprical testing of a conceptual model and measurement instrument for assesment of trustworthines of project team members. *8th AAMAS.* Budapest.

Sahin, I. (2006). DETAILED REVIEW OF ROGERS’ DIFFUSION OF INNOVATIONS THEORY AND EDUCATIONAL TECHNOLOGY-RELATED STUDIES BASED ON ROGERS' THEORY. *The Turkish Online Journal of Educational Technology – TOJET April 2006 ISSN: 1303-6521 volume 5 Issue 2 Article 3* , 14-23.

Santos, N., Gummadi, K. P., & Rodrigues, R. (2009). Towards Trusted Cloud Computing. *MPI-SWS*, 1-5 .

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods forBusiness Students (5th ed).* England: Prentice Hall.

Schiffman, J., Moyer, T., & Vijayakumar, H. (2010). Seeding Clouds with Trust Anchors. *Systems and Internet Infrastructure Security Laboratory* .

Shankar, V., Urban, G. L., & Sultan, F. (2002). Online trust: a stakeholder perspective, concepts, implications, and future directions. *Strategic Information Systems 11* , 325–344.

Shimba, F. (2010). Cloud Computing:Strategies for Cloud Computing Adoption. *ARROW@DIT* , 1-134.

Sin Tan, K., Eze, U., & Chong, S. (2011). Effects of Industry Type on ICT Adoption among Malaysian SMEs. *Journal of Supply Chain and Customer Relationship Management Vol. 2011 (2011), Article ID 113797, 13 pages* .

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi Method for Graduate Research. *Journal of Information Technology Education* , *6*, 1-21.

Sood, S. K. (2012). A combinedapproachtoensuredatasecurityincloudcomputing. *Journal of Network and Computer Applications 35 (2012)* , 1831–1838.

Sriram, I., & Khajeh-Hosseini, A. (2010). Research Agenda in Cloud Technologies. *Computer Science*, 1-11.

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

Takabi, H., Joshi, J. B., & Ahn, G. (2010). Security and Privacy Challenges in Cloud Computing Environments. *IEEE SECURITY & PRIVACY* , 24 -39.

Taylor, P. (2012). The Business Impact of Cloud Computing. In D. Plummer, *The Business Landscape of Cloud Computing* (pp. 1-7). Finacial Times, Gartner.

Technologies, C. (2011). *Rising Above the Competition as a Cloud Services Provider: Five Effective Steps for Claiming Your Share of the Pie*. New York: TechTarget Custom Media.

Tyler, G. (2010). Establishing Trust in Cloud Computing. *IATAC* , 3-7.

Vael, M. (2010). Cloud Computing An insight in the Governance & security aspect. *ISAC Belgium* .

Velte, A. T., Velte, T. J., & Elsenpeter, R. (2010). *Cloud Computing: A Practical Approach.* New York: McGraw-Hill Companies.

Wooley, P. (2011). *Identifying Cloud Computing Security Risks*. University of Oregon.

Wu, M., & Kuo, F. (2008). An Empirical Investigation of Habitual Usage and Past Usage on Technology Acceptance Evaluations and Continuance Intention. *The DATA BASE for Advances in Information Systems Volume 39, Number 4* , 48-73.

Zhang, X., Liu, H., Li, B., Haiqiang, W., & Wu, S. (2011). Application-Oriented Remote Verification Trust Model in Cloud Computing. *Cloud Computing Technology and Science (CloudCom)* , 405 - 408.

Appendices

A Ethical Clearance Certificate

B Nyoni, T. B., & Piderit, R. (2012). Enhancing trust in cloud computing. *Proceedings of the 14th Annual Comference on World Wide Web Applivations* (pp. 1-16). Cape Town: Cape Peninsula University of Technology.

C Nyoni, T. B., & Piderit, R. (2013). Towards a model for enhancing user trust in cloud computing applications. *Joint International Conference on Engineering Education and Research and International Conference on Information Technology* (pp. 59-67). Cape Town: Cape Peninsula University of Technology.

D Research Instrument: Cloud Computing Questionnaire

Appendix A

University of Fort Hare
Together in Excellence

ETHICAL CLEARANCE CERTIFICATE

Certificate Reference Number:	PID01 ISNYO01
Project title:	Enhancing trust in cloud computing to ensure adoption and continued use.
Nature of Project:	Masters
Principal Researcher:	Tamsanqa Nyoni
Supervisor:	Dr Roxanne Piderit
Co-supervisor:	

On behalf of the University of Fort Hare's Research Ethics Committee (UREC) I hereby give ethical approval in respect of the undertakings contained in the above-mentioned project and research instrument(s). Should any other instruments be used, these require separate authorization. The Researcher may therefore commence with the research as from the date of this certificate, using the reference number indicated above.

Please note that the UREC must be informed immediately of

 Any material change in the conditions or undertakings mentioned in the document

 Any material breaches of ethical undertakings or events that impact upon the ethical conduct of the research

The Principal Research must report to the UREC in the prescribed format, where applicable, annually, and at the end of the project, in respect of ethical compliance.

The UREC retains the right to

 Withdraw or amend this Ethical Clearance Certificate if o Any unethical principal or practices are revealed or suspected

o Relevant information has been withheld or misrepresented

o Regulatory changes of whatsoever nature so require

o The conditions contained in the Certificate have not been adhered to

 Request access to any information or data at any time during the course or after completion of the project.

The Ethics Committee wished you well in your research.

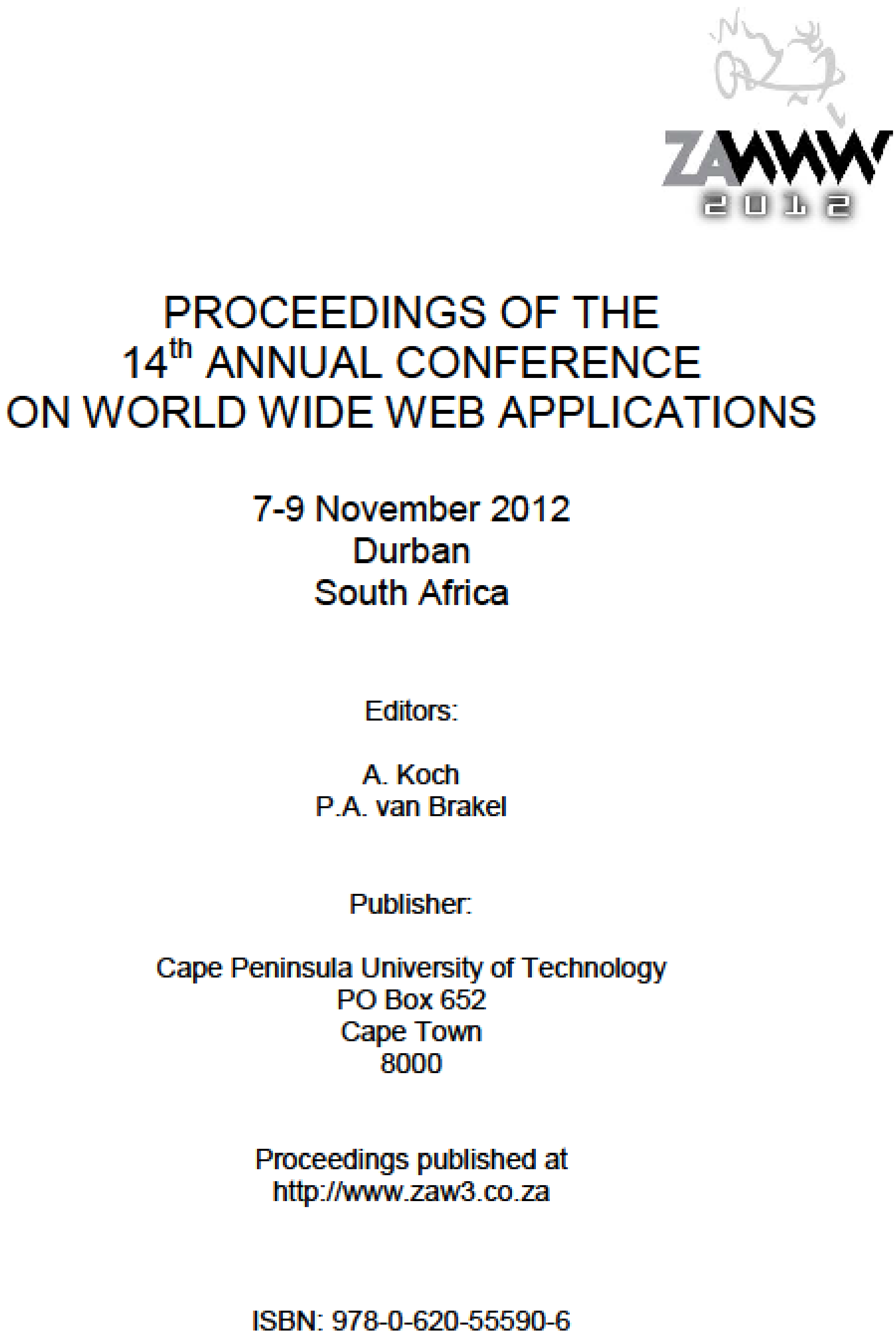
Yours sincerely

Professor Gideon de Wet

Dean of Research

31 May 2013

Appendix B



PROCEEDINGS OF THE
14th ANNUAL CONFERENCE
ON WORLD WIDE WEB APPLICATIONS

7-9 November 2012
Durban
South Africa

Editors:

A. Koch
P.A. van Brakel

Publisher:

Cape Peninsula University of Technology
PO Box 652
Cape Town
8000

Proceedings published at
http://www.zaw3.co.za

ISBN: 978-0-620-55590-6

TO WHOM IT MAY CONCERN

The full papers were refereed by a double-blind reviewing process according to South Africa's Department of Higher Education and Training (DHET) refereeing standards. Before accepting a paper, authors were to include the corrections as stated by the peer-reviewers. Of the 72 full papers received, 64 were accepted for the Proceedings (acceptance rate: 89%).

Papers were reviewed according to the following criteria:

- Relevancy of the paper to Web-based applications
- Explanation of the research problem & investigative questions
- Quality of the literature analysis
- Appropriateness of the research method(s)
- Adequacy of the evidence (findings) presented in the paper
- Technical (e.g. language editing; reference style).

The following reviewers took part in the process of evaluating the full papers of the 14th Annual Conference on World Wide Web Applications:
Prof RA Botha
Department of Business Informatics
Nelson Mandela Metropolitan University
Port Elizabeth

Mr AA Buitendag
Department of Business Informatics
Tshwane University of Technology
Pretoria

Prof AJ Bytheway
Faculty of Informatics and Design
Cape Peninsula University of Technology
Cape Town

Mr A El-Sobky
Consultant
22 Sebwih El-Masry Street
Nasr City, Cairo

Prof M Herselman
Meraka Institute, CSIR
Pretoria

Mr EL Howe
Institute of Development Management

Swaziland

Dr A Koch
Department of Cooperative Education
Faculty of Business
Cape Peninsula University of Technology
Cape Town

Dr DI Raitt
Editor: The Electronic Library (Emerald)
London

Mr PK Ramdeyal
Department of Information and Communication Technology
Mangosuthu University of Technology
Durban

Prof CW Rensleigh
Department of Information and Knowledge Management
University of Johannesburg
Johannesburg

Prof A Singh
Business School
University of KwaZulu-Natal
Durban

Prof JS van der Walt
Department of Business Informatics
Tshwane University of Technology
Pretoria

Prof D van Greunen
School of ICT
Nelson Mandela Metropolitan University
Port Elizabeth

Further enquiries:
Prof PA van Brakel Conference Chair: Annual Conference on WWW Applications
Cape Town
+27 21 469 1015 (landline)

+27 82 966 0789 (mobile)

Enhancing trust in cloud computing

TB Nyoni
University of Fort Hare
East London South Africa
thamsanqa.nyoni@yahoo.com
R Piderit
University of Fort Hare
East London South Africa rpiderit@ufh.ac.za

Abstract

The use of the cloud is without a doubt the latest appealing technological trend to emerge in the IT industry. As a promising approach for delivering ICT services, cloud computing improves the utilisation of data center resources. However, despite the surge in activity and interest, there are significant and persistent concerns about cloud computing that are impeding momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. Cloud computing is characterised by problems that impact on adoption and continued use of the cloud. The significant lack of trust in cloud computing adoption provides the framework of this study. The significant role that trust plays in new technology acceptance, adoption and continued use was considered in relation with the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) models. Cloud computing is still considered to be a new technology in the business world. Therefore minimal work and academic research has been done on enhancing trust in cloud computing. Academic research which focuses on the adoption of cloud computing and in particular the building of customer trust over the years has been minimal. Although a number of trust models and cloud computing adoption strategies have been produced, their main focus has been on the security aspects of the cloud. Again, studies conducted on cloud computing as a new technology in the market mainly focus on cost reduction and the various benefits that organisations will realise by migrating to the cloud. Most available work on cloud does not provide clear trust enhancing strategies for organisations, that will ensure trust in the adoption and successful continued use of cloud computing. The issue of establishing a reliable trust context for data and security within the cloud is, up to this point, not well defined. This paper investigates the negative impact that a lack of trust has on the successful adoption and continued use of cloud computing. It suggests and maps a successful strategy to enhance organisational trust in cloud computing. In addition this will lead to its adoption and continued use. This study therefore proposes a Cloud Computing Adoption Model that will enhance organisations' trust in the cloud, leading to a successful strategy for cloud computing adoption. The model highlights the major challenges that hinder trust in cloud computing and also raises awareness of these challenges through education, skills, knowledge and cloud computing policies. Compliance, accountability and transparency are the three factors identified to enhance trust in cloud computing adoption, leading to successful adoption and continued use.

Keywords: Cloud computing, trust, adoption, continued use

Proceedings of the 14th Annual Conference on World Wide Web Applications Durban,

7-9 November 2012 (http://www.zaw3.co.za)

ISBN: 978-0-620-55590-6

1. Introduction

Recent advances in the use of technology have pushed technological innovation to new frontiers and cloud computing has emerged as one of these recent web-based innovations. The growing acceptance of innovative technologies in the business world has seen the popularity of cloud computing increase substantially. Cloud computing is a technology whereby data is outsourced and stored in a secure environment (the cloud) and then provided as a service online, either by subscription or on a pay-on-demand basis to customers. It adds value to organisations by improving business efficiency and effectiveness. Additionally cloud computing enables increased productivity and transforms business processes through means that were considered very expensive before the emergence of cloud computing (ISACA, 2009:6). It is important to note that in this paper cloud computing is seen as a new web-based ICT that organisations can adopt and use to their advantage. The emergence and application of cloud computing has helped users gain access to various computing resources, more conveniently and it is fast becoming a dynamic force in the business world (Ragent & Leach, 2010:4). Business sectors, such as banking, retail and communication have realised the abundant benefits that come with cloud computing and have adopted it, implementing it to their business process.

Unfortunately, the volumes and type of data that can be stored and retrieved from the cloud through the use of the Internet threatens the security and trustworthiness of the cloud. This also brings forth security and trust challenges (Zhang, Liu, Li, Haiqiang, & Wu, 2011:406). Therefore, the correct approach to cloud computing is needed in order to create a competitive advantage for organisations (Ragent & Leach, 2010:10). Shimba (2010:ii) is in agreement with the above statement as he further states that although the adoption of cloud computing promises various benefits to an organisation, successful adoption of cloud computing in an organisation requires an understanding of different dynamics that are involved with cloud computing adoption.

The lack of trust is seen to have a negative impact on the successful adoption, implementation and continued use of cloud computing. Organisations view investing trust in cloud computing it to be a complex and unsecure operation (Shimba, 2010:2). According to Ragent and Leach (2010:8), despite the potentially positive impact that the cloud has on efficiency and productivity, many organisations lack trust and are reluctant to fully embrace cloud computing. This confirms the views of Cofta (2007:94) who articulates that trust is increasingly becoming a necessity in most modern organisations. There is a growing need for organisations to apply a great deal of trust in order to eventually achieve greater organisational flexibility with new technology. Moreover, according to Ragent and Leach (2010:8), an organisations' lack of trust in cloud computing has caused the adoption and implementation process to become a chaotic and haphazard process, characterised by constant failure. This has also seen organisations failing to utilise the vast advantages that come with migrating to cloud computing compared to traditional methods. The implementation of effective trust strategies in organisations could reduce the lack of trust in cloud computing.

The increasing lack of trust in cloud computing that hinders successful adoption is widely recognised and highlights the significance of this research. This study sets out to explore

ISBN: 978-0-620-55590-6

the most important strategic trust issues around cloud computing adoption in organisations. It will investigate and consider strategies that can be used to enhance the levels of user trust in cloud computing, thereby influencing its acceptance, widespread adoption and continued use in organisations. Accountability, compliance and compatibility will be further examined as some of the factors that will enhance organisations trust in the cloud leading to a successful strategy for cloud computing adoption.

Cloud computing adoption by organisations is a delicate process that requires high levels of trust. The enhancement of organisational trust that will lead to successful cloud computing and continued used is an essential concern for this study. Following this introduction, the underlying problem hindering successful cloud computing adoption and continued use is discussed. An examination of the role of trust in the adoption process and the factors that enhance trust in the cloud are included in this paper. The relationship between organisational trust and migrating to the cloud is investigated in the context of cloud adoption and continued used. A proposed cloud computing adoption model is presented in this paper as a solution to enhance trust.

2. The problem: lack of trust in the cloud

Despite the vast business and technical advantages of using cloud computing, many organisations who are potential cloud users are still reluctant to trust and migrate to the cloud (Chow, et al., 2009:8). This is largely due to the fact that the convenience and efficiency of cloud computing comes with a range of potential privacy and security related issues that pose a threat to organisational data. Among these issues, the lack of trust has proven to be a key barrier to the extensive adoption of cloud computing by potential users (Alliance, 2009:7). The issue of trusting cloud computing and storing valuable data on it is a paramount concern for most organisations. Most organisations question cloud computing capabilities and the services provider’s intentions (Kumar, Sehgal, Chauhan, Gupta, & Diwakar, 2011:413). The presence of trust improves and ensures the successful adoption and continued use of the cloud, while the lack of it results in inefficient and ineffective performance and use of the services offered by the cloud (Bourne, 2010:6). Therefore, a lack of trust hampers the successful adoption of cloud computing and its continued use in organisations.

Again when considering the adoption issues associated with cloud computing, the most fundamental element that most organisations consider is how the cloud environment affects the trust boundary of the organisation (Meade, 2009:2). According to Ko, Jagadpramana, Mowbray, Pearson, Kirchberg, Liang and Lee (2011:1), the lack of trust is identified as the key barrier to widespread cloud computing adoption and continued use in most organisations. Lack of trust clearly has a negative impact on the organisation’s decision to adopt, implement and continue using cloud computing. According to Monsuwe, Dellaert and Ruyter (2004:114), a lack of trust distorts the user’s perception on using the new technology. The lack of trust also distorts the users view on the systems ‘usefulness’, ‘ease of use’ and ‘enjoyment’ which, according to Monsuwe (2004:107), are fundamental factors in determining the acceptance and continued use of new ICTs - in this case, cloud computing.

3. The method

Cloud computing is still considered to be a new technology in the business world. Therefore, minimal work and academic research has been done on enhancing trust in cloud computing (Vael, 2010:9). According to Shimba (2010:2), academic research which focuses on the adoption of cloud computing and in particular the building of customer trust over the years has been minimal. Although a number of trust models and cloud computing adoption strategies have been produced, their main focus has been on the security aspects of the cloud. In cloud computing adoption research, security is the topic that has been receiving increased attention (Shimba, 2010:2).

Available work on cloud does not provide clear trust enhancing strategies for organisation's, that will ensure trust in the adoption and successful continued use of cloud computing. This study therefore reviewed the recent and available literature, academic and professional perspectives from various media on trust in cloud computing. The media reviewed included printed media (such as books and journals) and online media in the form of electronic journals and industry white papers. Through this review, the effects of trust on cloud computing adoption and continued use was investigated, and a proposed model developed. This proposed model is described in a later section.

4. Benefits of cloud computing

The impact and potential benefits of migrating organisational services to the cloud needs to be considered against the lack of trust in cloud computing. The benefits offered by the cloud to organisations are too significant to be ignored. Despite it being a relatively new technology, cloud computing allows for better IT resource optimisation, virtually unlimited scalability and greater flexibility, all at a contained cost (Callewaert & Luysterborg, 2011:8). ISACA (2009:7) state that cloud computing carries with it the ability to offer organisations long-term IT savings, which includes reducing infrastructure costs and offering pay-for-service models as an option to the enterprise. By moving IT services to the cloud, enterprises can take advantage of using services in an on-demand model. Migrating to the cloud makes it relatively easy for IT solutions to be deployed and be quickly managed, maintained, patched and upgraded remotely by the service provider. Technical support for the organisations can be provided round the clock by service providers for no extra charge, thus reducing the burden on the internal IT staff (Lovell, 2010:7).

Therefore cloud computing is an attractive potential service offering for any business looking to enhance IT resources while controlling costs (ISACA, 2009:6). This has led to the rapid spreading of cloud adoption and therefore presents various new opportunities for companies that should not be ignored; given cloud computing's profound impact in the IT industry. Therefore, organisations should improve trust in cloud computing so as to maximise on benefits which include reduced cost and increased storage, flexibility and mobility (Callewaert & Luysterborg, 2011:8).

5. Trust in cloud computing adoption

Organisations often hesitate to adopt and shift to using the cloud because of uncertainty and security issues that surround use of cloud computing. Most often than not, the hesitation is caused by the perceived risk by the organisation failing to effectively use the cloud in its production and business processes. Trust therefore plays a central role in helping consumers overcome perceptions of risk and insecurity (McKnight, Choudhury, & Kacmar, 2002:334). This is because trust in the cloud will lead organisations to be more comfortable with cloud computing adoption and continued use. Therefore, trust is critical to both the organisations and the cloud computing vendors. Not only is trust critical, but it is also important as it aids organisations in overcoming perceptions of uncertainty and risk and in engaging in "trust-related behaviours" with cloud vendors (McKnight, Choudhury, & Kacmar, 2002:335). This section of the paper gives a brief description of trust and the effect it has on the cloud computing adoption process.

5.1 Defining *trust*

Trust has traditionally proved to be difficult to define and measure. Some researchers have treated trust as a unitary concept, however, seem to now agree that trust is more multidimensional and it takes various forms (Cofta, 2007:123). Cofta (2007:127) explains trust as a foundation to security and recognises trust to be the most important element of every transaction. He further states that trust revolves around 'assurance' and confidence that people, data, entities, information or processes will function and behave in expected ways.

Trust may be human to human, machine to machine, human to machine or machine to human. At a deeper level, trust might be regarded as a consequence of progress towards security or privacy objectives (Robinson, Lorenzo, Cave, & Starkey, 2010:14). According to Luhmann (1988:18), trust tends to be needed in situations where there is risk and uncertainty. On the other hand, according to Newell and Swan (2000:1293), trust is viewed and defined in different ways, but there are two main issues about trust that seem to be central throughout the varied definitions of it. These issues are that trust is about dealing with risk and uncertainty, and that trust is about accepting vulnerability. Trust can also be defined as a feeling of being secure about an entity at a given time (Chen, Gillenson, & Sherrell, 2004: 7). This is the definition of trust that will be adopted for the purposes of this paper as it focuses on the trust that organisations have in cloud computing.

Cloud computing adoption in most organisations is still seen as a delicate issue that is largely characterised by risk and uncertainty. This then means high levels of organisational trust are needed to ensure its successful adoption and continued use. The introduction of a new system requires trust as a vital input condition in order to stimulate supportive activities in situations of uncertainty or risk should they occur (Luhmann, 1998). Evidence from the reviewed literature indicates that the presence of trust improves and ensures the successful adoption and continued use of cloud computing, while the lack of it results in organisations being reluctant to adopt and use the services offered by cloud computing.

5.2 Factors that affect trust in cloud computing

Lack of trust within an organisation usually tends to influence a number of organisational processes which affect the extent to which new systems such as cloud computing can be accepted and then used within that organisation. The levels of trust in new systems that an organisation has tend to also affect users perceptions of the new system and its ability to perform. A number of varied factors contribute to the lack of trust when it comes to cloud computing adoption in organisations. It is important to note that cloud computing has unlocked a new frontier of challenges by introducing a different type of trust scenario (Kumar, Sehgal, Chauhan, Gupta, & Diwakar, 2011:412). The problem of trusting cloud computing is a paramount concern for most organisations, as most of them question cloud computing capabilities and the service provider's intentions for hosting the cloud. Some of the major factors that affect trust in cloud computing will be discussed next.

5.2.1 Security challenges

According to Kumar et al. (2011:413), cloud computing is seen as insecure by nature. This is because security in the cloud is often intangible and less visible, which inevitably creates a false sense of security about what is actually secured and controlled. Kumar et al. (2011:413) also point out that the off-premises computing paradigm that comes with cloud computing has incurred great concerns on the security of data, especially the integrity and confidentiality of data, as cloud service providers may have complete control on the computing infrastructure that underpins the services. This security challenge leads users (customers) to have limited trust in the whole cloud computing process. Cloud computing is still an evolving paradigm that has incredible momentum, but its unique aspects intensify security and privacy challenges that surround its use (Hassan, Joshi, & Ahn, 2010:24). This therefore hampers the levels of trust that the organisations and potential cloud users have in cloud computing, depriving the organisations of the many benefits of cloud computing.

5.2.2 Loss of control

Cloud users typically have no control over the cloud resources used. All technical control is given to the provider and there is an inherent risk of data exposure to third parties on the cloud or the cloud provider itself (Kumar, Sehgal, Chauhan, Gupta, & Diwakar, 2011:413). According to Holbl (2011:2), organisations are conscious of the danger of letting data control out of their hands and storing sensitive data with an outside cloud computing provider. This is because organisations' private data could be compromised by the cloud computing provider and other competitive enterprises which are also customers with the same cloud computing provider. There is a lack of transparency in the cloud on where and how data is stored; there is also the question of how data is processed in cloud computing (Holbl, 2011:2).

Organisations also see the risk of losing control when it comes to how and when to access their data that is stored in the cloud. Holbl (2011:2) points out that cloud computing is still a service that has to be accessed remotely and this presents a problem as the connection between the cloud providers and organisation is not adequately protected. Loss of control on organisational data is threatened by denial of service attacks and network down time (Holbl, 2011:2). Kumar et al. (2011:418) further state that cloud computing depends largely on the reliability of secure telecommunications network that assures and guarantees the operations of undisrupted operations by the cloud computing providers.

Telecommunication networks are often provided separately from the cloud computing services and so it's beyond the organisations control (Holbl, 2011:2). Again with the loss of control, concerns also exist with regards to the control and deletion of data in the cloud. It has proven difficult to delete all available copies of electronic materials, thus it is impossible to guarantee complete deletion of all organisation's copies of important data. Therefore it is difficult for organisations to have control over the deletion of the data they have stored in the cloud.

5.2.3 Loss of governance

By using cloud services the client passes control to the provider. This passing off of control to the provider results in loss of control over a number of issues. This in turn may affect the security posture of the client data and applications. It is therefore difficult for organisations to trust cloud computing (Shimba, 2010:35). The loss of governance in cloud computing has a severe impact on the organisation's strategy and therefore on their capacity to meet set goals and objectives. The loss of governance could lead to things like impossibility of complying with the security requirements, lack of confidentiality, integrity and availability of data, and a deterioration of performance and quality of service, not to mention the introduction of compliance challenges (Catteddu & Hogben, 2009:29).

5.2.4 Privacy concerns

Kumar et al. (2011:414) state that the location of the cloud computing providers makes it difficult for companies and private users to keep control of the information or data they entrust to cloud suppliers at all times. This is against the fact that privacy is an important issue for cloud computing, both in terms of legal compliance and user trust (Kumar, Sehgal, Chauhan, Gupta, & Diwakar, 2011:419). Some organisations who deal with highly confidential and sensitive information do not trust the high volumes involved with cloud computing and are reluctant to adopt and use it in their everyday business. This is because entrusting this type of information to a cloud increases the risk of uncontrolled dissemination of that information to competitors who also use the same cloud platform.

According to Microsoft (2009:2), privacy and security are essential in all online computing environments such as cloud computing. Organisations are only willing to use cloud computing if the cloud providers assure them that their data will remain private and secure. Therefore, the ability of cloud computing providers to provide a secure and private platform for its users is essential to develop trust within the organisations (Microsoft, 2009:5).

6. Factors that enhance trust in cloud computing

The above mentioned are the factors that contribute to the widespread lack of trust in cloud computing. The following section of this paper will discuss the essential factors that are important for enhanced trust in cloud computing.

6.1 Compliance

This refers to ensuring that a cloud deployment meets the requirements imposed by the applicable normative framework, including general legislation, sector-specific rules and contractual obligations. In compliance, the major issue will be assuring the compliance of data protection rules (Robinson, Lorenzo, Cave, & Starkey, 2010:108). According to Holbl (2011:3), compliance can be seen as one of the important trust factors between the cloud computing provider and their customer. Regulatory and legislative compliance by cloud computing providers enhances the level of trust that organisations have in the cloud. Cloud data centres can be geographically dispersed and hence different regulation have to be implemented in different locations to ensure compliance. Therefore, legislative compliance of cloud computing has to be adequately defined for different providers in different locations (Holbl, 2011:3).

6.2 Accountability

Accountability in cloud computing ensures that security and privacy breaches in the cloud deployment are correctly addressed, through appropriate compensation mechanisms towards any victims (organisations) that might be affected. Cloud services can succeed when cloud providers are able to provide these services in an efficient way and assure customers that they are fully accountable for hosting data, and also that the organisational data will remain private and secure (Microsoft, 2009:5). Organizations grow to have trust in cloud computing when accountability in the cloud is achieved through the combination of law, regulation and technical enforcement mechanisms by the providers.

6.3 Transparency

The general perception within most organisations is that cloud computing is less secure than their traditional in-house systems. According to Gopalakrishnan (2009:50), security measures assumed in the cloud must be made available to organisations for them to gain their trust in cloud computing. By nature the cloud infrastructure is secure according to the cloud computing requirements, but organisations are looking for a different set of security aspects within the cloud. The important aspect is to see that the cloud provider meets the security requirements of the application and this can be achieved only through transparency (Gopalakrishnan, 2009:50). Cloud computing providers must demonstrate the existence of effective and strong security controls that will assure organisations their information is properly secured against unauthorized access, change and all forms of destruction in the cloud (Vael, 2010:8).

Transparency is there to ensure that the operation of the cloud deployment is sufficiently clear to all stakeholders, including service providers and users, both professional businesses and private consumers. This can be witnessed, for example, in the difficulty of determining who/where a cloud service provider is, and where his responsibilities/liabilities end (Robinson, Lorenzo, Cave, & Starkey, 2010:110). Gopalakrishnan (2009:50) further states that transparency in cloud computing can be attained by a total and complete audit logging and control measure in the cloud. According to Holbl (2011:3), in order to ensure transparency, the communication line that exists between the cloud computing provider and the organisation has to be adequately protected all the time. This has to be done to ensure confidentiality, integrity, authentication control and to further minimise the risk of denial of service occurrences. An open and clear specification of the measurements taken to ensure the security of the communication line should be mandatory for providers and should be based on open and transparent standards and technologies.

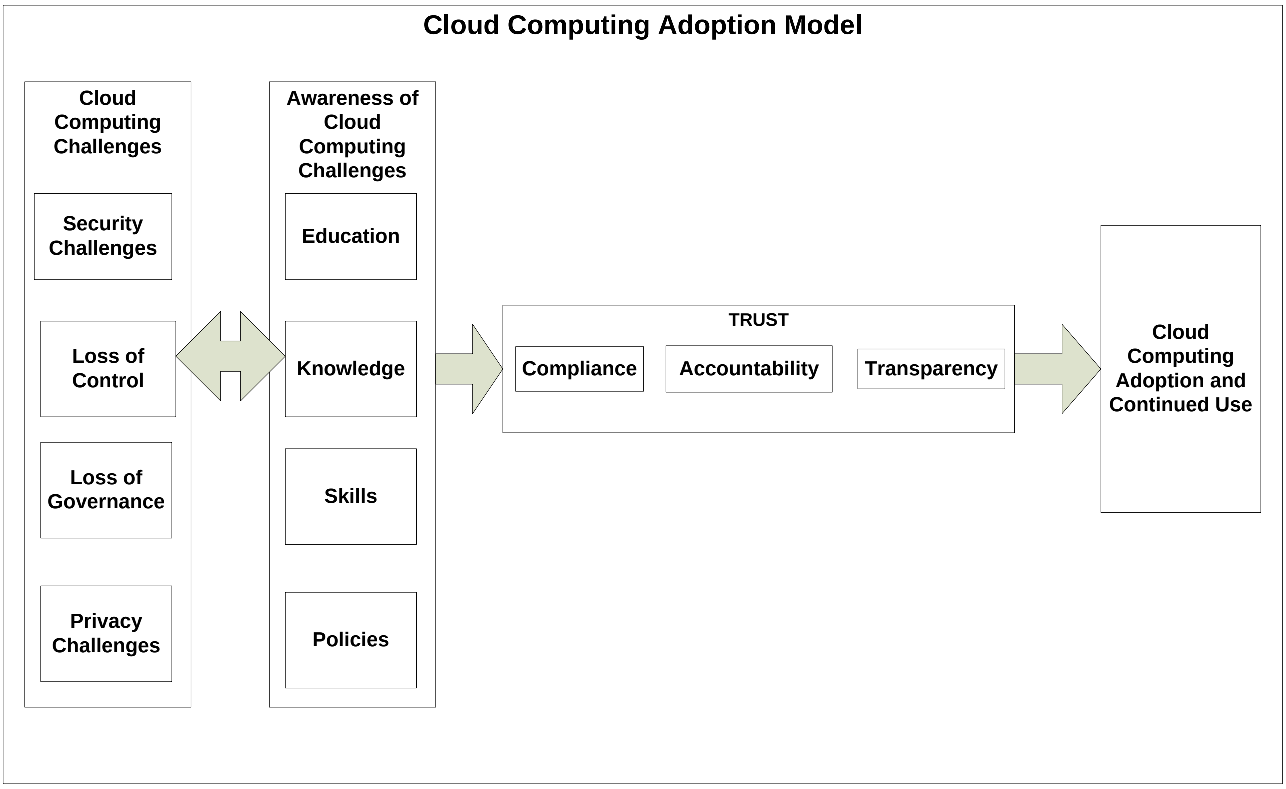
There are various components and factors that enhance trust in the cloud computing which eventually lead to its successful adoption by organisations. The factors that are considered to be vital in enhancing trust in cloud computing are compliance, accountability and transparency. However, the role of people in the cloud computing adoption process cannot be overlooked. People in organisations need to be educated and trained on how best to use cloud computing and what they stand to benefit. This will equip employees with the much needed cloud computing skill and how to use the new technology. This is an important part of enhancing trust in the cloud adoption process as people and technology need to be used effectively together for the successful cloud computing adoption and continued use thereafter. It is from these various factors that the base of the proposed adoption model is drawn from.

7. Towards enhancing trust in cloud computing

An extensive literature study was completed, which points out a number of challenges and factors that affect trust in cloud computing. A number of trust issues were also discussed. The model proposed in this paper is a combination of key portions of the literature explored and combined to offer a model expected to enhance trust in cloud computing, eventually leading to its successful adoption. The model has been developed through discussions, reasoning and a critical analysis of issues discussed above. Figure 1 below presents the proposed model followed by a brief discussion of its logical flow. A number of theoretical models have been proposed to facilitate the understanding of factors impacting the acceptance, adoption and trust in new information technologies (Marchewka, Liu, & Kostiwa, 2007:94). The proposed model is based upon and also draws components and some its elements from the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT).

The first four major components in the model are the four cloud computing challenges. These form the initiating phase of the model and establish the main issues that hinder trust in cloud computing. The second component included in the model is the awareness of the cloud computing challenges brought about by education, skills, knowledge and cloud computing policies as discussed in the reviewed literature. In order to develop the trust in cloud computing, the model includes the next three major components that have been identified to enhance trust in cloud computing adoption. The combination of these three will enhance the level of trust that organisations have in cloud computing, eventually leading to the successful adoption and continued use of the cloud.

Figure 1: Proposed cloud computing adoption model



The first phase of the model starts off with a clear identification of the main cloud computing challenges as identified by Kumar et al. (2011:413), which are security, loss of control, loss of governance and privacy challenges. The second phase of the model is the organisation's awareness of the cloud computing challenges. The awareness of the challenges can be made or occurs through the education, knowledge, skill and policies that surround cloud computing (Locke, 2004:94). Awareness of the challenges leads to the organisation realising the benefits that lie with adoption of cloud computing, eventually leading to increased trust in the cloud. There is a repetitive iteration between the first and second phases; this is because the awareness of the challenges is never a one way, smooth flowing process. It takes time for the organisation to be fully aware of these challenges. The education, knowledge and the acquiring of the correct skills is a process that has to be fully understood.

A positive outcome from the second phase should eventually lead to the enhancement of trust in cloud computing and ultimately in adoption. According to Robinson et al. (2010:108), cloud compliance, accountability and transparency are the main issues that underlie and enhance organisational trust in the cloud. These are paramount components in ensuring trust. Trust in cloud computing leads to the last phase of the model which is the adoption and continued use phase.

8. Conclusion

This paper has shown how several works have highlighted the importance of trust in cloud computing adoption and the effects of low levels of trust in cloud computing. The studies suggest that enhancing the level of trust in the cloud computing is required. This leads to the formulation of the proposed model as a way forward in enhancing organisations trust in cloud computing, leading its adoption and continued use.

The paper presents a model which details a combination of components extracted from existing technology adoption models. The components discussed in the model were the result of an analysis of relevant literature. The various components identified were modified and fused together to form the integral part of a cloud computing adoption model that organisations can use in the adoption process.

In conclusion, it is important to note that the process of adopting cloud computing is a process that requires trust from the organisation and the end users. Trust in cloud computing should be enhanced and closely managed to ensure successful adoption and continued use. This research paper, therefore, sought to identify trust enhancing measures aimed at ensuring that organisations gain confidence in the cloud. Relevant literature on the cloud and cloud computing was reviewed in order to gain a thorough understanding of the reasons behind organisations lack of trust in cloud computing.

9. References

Bourne, V. (2010). Rising to the Challenge. *2010 Global IT Leadership Report* . Available at http:// networkworld.com (accessed 13 July 2012).

Callewaert, P., & Luysterborg, E. (2011). Security,Trust and Risk. *Cloud Computing Forecasting* . Available at http:// deloitte.com (accessed 8 June 2012).

Catteddu, D., & Hogben, G. (2009). Benefits, risks and recommendations for information security. *Enisa 09* . Available at http:// ibimapublishing.com (accessed 8 June 2012).

Chen, L., Gillenson, L. M., & Sherrell, D. L. (2004). *Consumer acceptance of virtual stores: a theoretical model and critical success factors for virtual stores.* New York: AGM. Available at http:// portal.acm.org (accessed 19 July 2012).

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., et al. (2009). Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. *CCSW'09* , 1-10. Available at http://dl.amc.org (accessed 9 July 2012).

Cofta, P. (2007). *Trust, Complexity adn Control.Confidence in a Convergent World.* Ontiario: John Wiley.

Gopalakrishnan, A. (2009). Cloud Computing Identity Management. *SETLabs Briefings Vol 7 No 7* , 45-58. Available at http:// cis.cau.edu (accessed 9 July 2012).

Holbl, M. (2011). Cloud Computing Security and Privacy Issues. *CEPIS LSI SIN (10) 02* , 1-4. Available at http://dl.amc.org (accessed 7 July 2012).

ISACA. (2009). Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives. *ISACA Emerging Technology White Paper* , 1-10. Available at http://www.ibimapublishing.com/journals (accessed 19 July 2012).

Hassan, T., Joshi, B. D., & Ahn, G. (2010). Security and Privacy Challenges in Cloud Computing Environmemnts. *Cloud Computing* . Available at http://dl.amc.org (accessed 9 July 2012).

Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., et al. (2011). TrustCloud: A Framework for Accountability and Trust in Cloud Computing. *Cloud & Security Lab* , 1-5. Available at http://dl.amc.org (accessed 7 July 2012).

Kumar, P., Sehgal, V. K., Chauhan, D. S., Gupta, P. K., & Diwakar, M. (2011). Effective Ways of Secure, Private and Trusted Cloud Computing. *IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2,* , 412-422. Available at www.IJCSI.org (accessed 10 July 2012).

Lovell, R. (2010). Business IT on Demand. *ThinkGrid* . Available at www.thinkgrid.co.uk/docs/ (accessed 7 July 2012).

Marchewka, J. T., Liu, C., & Kostiwa, K. (2007). An Application of the UTAUT Model for Understanding Student Perceptions Using Course Management Software. *Operations Management and Information Systems Vol 7 Issue 2*, 93-104. Available at http:// pdfcloud.org (accessed 16 July 2012).

Monsuwe´, T. P., Dellaert, B. G., & de Ruyter, K. (2004). What drives consumers to shop online? A literature review. *International Journal of Service Industry Management Vol 15*, 102-121. . Available at http://www.emeraldinsight.com/journals. (accessed 26 July 2012).

McKnight, D. H., Choudhury, V., & Kacmar, M. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research* , 334-359. Available at http:// www.bus.iastate.edu (accessed 20 June 2012).

Meade, F. (2009). Cloud Computing-Overview of Information Assurance Overview of Information Assurance. *JAD* , 1-8. Available at http:// www.nsa.gov/ia/ (accessed 20 June 2012).

Microsoft. (2009). Privacy in the Cloud Computing Era A Microsoft Perspective. *Microsoft* . Available at http://www.sciencedirect.com/science/article (accessed 12 June 2012).

Ragent, F., & Leach, C. (2010). Can You Trust the Cloud? A Practical Guide to the Opportunities and Challenges Involved in Cloud Computing. *Cloud Computing* . Available at www.xerox.com/thoughtleadership (accessed 9 July).

Robinson, N., Lorenzo, V., Cave, J., & Starkey, T. (2010). The Cloud: Understanding the Security, Privacy and Trust Challenges. *Information Society and Media TR-933-EC* . Available at http://dl.amc.org (accessed 8 July 2012).

Shimba, F. (2010). Cloud Computing:Strategies for Cloud Computing Adoption. *ARROW@DIT* , 1-134. Available at http://arrow.dit.ie/scschcomdis/29/ (accessed 20 June 2012).

Vael, M. (2010). Cloud Computing An insight in the Governance & security aspect. *ISAC Belgium* . Available at http:// pdfcloud.org (accessed 16 July 2012).

Zhang , X., Liu, H., Li, B., Haiqiang, W., & Wu, S. (2011). Application-Oriented Remote Verification Trust Model in Cloud Computing. *Cloud Computing Technology and Science (CloudCom)* , 405 - 408 . Available at http://dl.amc.org (accessed 6 July 2012).

Appendix C

ICEE/ICIT-2013

CONFERNCE

Joint International Conference on Engineering Education and Research and International Conference Information Technology

8 -12 DECEMBER

CAPE TOWN

Cape
Peninsula
University
of Technology

PROCEEDINGS

of the

ICEE ICIT 2013 Conference

9 – 11 December 2013

Organised by

Cape Peninsula University of Technology

In association with

iNEER

HEICTA

Published by

Cape Peninsula University of Technology, Cape Town, South Africa

ISBN 978-0-9922041-3-6

WELCOMING MESSAGE FROM THE VICE-CHANCELLOR

Delegates, visitors and friends, welcome to an official iNEER Conference, the “2013 Joint International Conference on Engineering Education and Research & International Conference on Information Technology” or “ICEE/ICIT-2013 Cape Town” in short. A big thank you to the Conference Organisers and the Editorial Committee, who have worked hard to organise this conference. We are all challenged to research and improve engineering education and to equip our respective countries with well skilled information technology manpower so that we can compete successfully on local and international markets. This conference focuses the attention on educational research and information technology. At the Cape Peninsula University of Technology, the Department of Information Technology’s involvement with HEICTA and iNEER continues to address these issues of national and international importance.

The programme and the impressive conference proceedings, which you already received at the registration desk, are indicative of yet another important conference. All delegates and visitors, especially those from overseas and other African States, are most welcome to enjoy what our campus has to offer and please enjoy your stay in greater Cape Town, where our university has five campuses.

Prof L V Mazwi-Tanga

VICE-CHANCELLOR

CONFERENCE

ORGANISING COMMITTEE

Conference Chairs**:**

Anthony Staak	CPUT
Chris Nhlapo	CPUT
Bennett Alexander	CPUT

Organising Committee:

Deon Kallis	CPUT
Ilyas Omar	CPUT
Nico Beute	CPUT
Rosetta Ziegler	CPUT
Tom van Breda	CPUT
Wilfred Fritz	CPUT
Anneke de Klerk	CPUT
Nadia Cassiem	CPUT

International Advisory Committee:

Anthony Staak	CPUT
Bennett Alexander	CPUT
Chris Nhlapo	CPUT
Hamadou Saliah-Hassane	University of Quebec
James Uomoibhi	Ulster University
Mohamed Essaaidi	IEEE
Nico Beute	CPUT
Olga Dolinina	Yury Gagarin State Technical University of Saratov
Win Aung	iNEER

ICEE / ICIT 2013 EDITORIAL POLICY

The Editorial Committee of the *2013 Joint International Conference on Engineering Education and Research & International Conference on Information Technology* or *ICEE/ICIT-2013 Cape Town* in short, has been upholding the following principles and editorial procedures:

- The Editorial Committee consists of invited senior subject specialists from a broad spectrum of local and international universities and research institutions
- In order to ensure a high standard, all abstracts of proposed conference papers are sent for evaluation to those members of the Editorial Committee, who are specialists in a particular topic
- Upon acceptance of the abstract, authors are invited to submit their papers
- Upon receipt of the paper, at least 3 reviewers are asked to blind review the paper on the web based EasyChair review system.. The Evaluation Form is completed, reflecting the rating of the quality and contents of the intended paper; how well it would fit into the forthcoming conference; the standing of the presenter; and his/her ability to present a paper, together with additional recommendations for the author(s) to consider to enhance the value of the presentation
- Each evaluator informs the relevant Track Chair of the Editorial Committee, recommending that the manuscript be either accepted; accepted with amendments; or rejected.
- The Track Chair informs each author of the outcome timeously. In some cases authors are invited to resubmit the paper based on comments made by the reviewers and the review process is repeated
- In total 169 papers have been submitted and after the review process 104 were accepted for publication in the proceedings, but 91 of them had authors attending the conference to present their paper. So 91 papers are included in the proceedings.

The peer-evaluated and refereed papers are included in a memory stick carrying an ISBN number. The conference proceedings are then distributed to all delegates upon registration.

EDITORIAL COMMITTEE

Janardan Choubey	Eastern Regional Institute of Science and Technology
Janne Roslöf	Turku University of Applied Sciences
Jarka Glassey	CEAM, Newcastle University
Jekaterina Bule	Riga Technical University
Jerzy Moscinsk	i Silesian University of Technology
John Prados	The University of Tennessee
Karmela Aleksic-Maslac	Zagreb School of Economics and Management
Larisa Zaitseva	Riga Technical University
Loren Schwieber	t Wayne State University
Luis Manuel Sanchez Ruiz	Universitat Politècnica de València
Maria Braz	ICIST, Instituto Superior Técnico, TULisbon
Maria Jose Marcelino	University of Coimbra
Maria Lúcia Pereira Da Silva	Escola Politécnica da USP
Mariana Ruiz	Universidad Iberoamericana
Mohd Fairuz Shiratuddin	Murdoch University
Morteza Biglari-Abhari	University of Auckland
Nhlahla Mlitwa	CPUT
Nobert Jere	Walter Sisulu University
Olga Dolinina Yury	Gagarin State Technical University of Saratov
Oner Yurtseven	EarthSolar Technologies
Patricia Fox	IUPUI
Paula Postelnicescu	University "Politehnica" of Bucharest
Pradesh Ramdeyal	Mangosuthu University of Technology
Raija Tuohi	Turku University of Applied Sciences
Richard C Kavanagh	University College Cork
Richard Millham	Durban University of Technology
Rosetta Ziegler	CPUT
Sameer Naik	Purdue University

Suama Hamunyela	Polytechnic of Namibia
Syed Mahfuzul Aziz	University of South Australia
Taurai Chikotie	AFDA
Wilfred Fritz	CPUT, Department of Energy

These Proceedings are a collection of original selected papers, which were accepted after the abstracts and full papers submitted were refereed by a panel of local and international peer evaluators, each a specialist in his or her own field. Every effort has been made to include only those papers that are original and of a high, scientific standard. The organizers and publishers do, however not accept any responsibility for any claims made by the authors.

Table of Contents

Engineering, Design & Technology

Embedded Systems

Telecommunications

Design in ICT and/or Engineering Practice

Innovative ICT and/or Engineering Approaches

Towards Critical Success Factors for Enhancing User Trust in Cloud Computing Applications

Tamsanqa Nyoni[1] and Roxanne Piderit[2]

[1] *University of Fort Hare, East London, South Africa,* tybex07@yahoo.com

[2] *University of Fort Hare, East London, South Africa,* rpiderit@ufh.ac.za

Abstract

The use of the cloud is without a doubt the latest appealing technological trend to emerge in the IT industry. However, despite the surge in activity and interest, there are significant and persistent concerns about cloud computing, particularly with regard to trusting the cloud platform in terms of confidentiality, integrity and availability of user data stored through these applications. These factors are significant in determining trust in cloud computing and thus provide the framework for this paper. The significant role that trust plays in adoption and continued use of cloud computing was considered in relation to the Proposed Model of Trust [1] and the Confidentiality-Integrity-Availability (CIA) Triad [2].

Although a number of trust models and cloud computing adoption strategies have been produced, their main focus has been on cost reduction and the various benefits that organisations and users will realise by migrating to the cloud. Most available work on cloud does not provide clear trust enhancing strategies for cloud computing service providers that will ensure user trust in the adoption and successful continued use of cloud computing applications.

This paper reports on findings of a questionnaire administered to users (and potential users) of cloud computing applications. The questionnaire primarily investigates key concerns which result in selfmoderation of cloud computing use and factors which would improve trust in cloud computing.

Additionally, results relating to user awareness of potential confidentiality, integrity and availability risks are included. Based on the results of this questionnaire, Critical Success Factors (CSFs) to enhance user trust in cloud computing applications are proposed. These CSFs are an enhancement of a previous model suggested by the authors.

Keywords: *Adoption; Availability; Cloud Computing; Confidentiality; Continued Use; Integrity; User Trust*

1. Introduction

Recent advances in the use of technology have pushed technological innovation to new frontiers and cloud computing has emerged as one of these recent web-based innovations. The growing acceptance of innovative technologies in the business world has seen the popularity of cloud computing increase substantially. Cloud computing enables increased productivity and transforms business processes through means that were considered very expensive before [3]. The emergence and application of cloud computing has helped users gain access to various computing resources, more conveniently and it is fast becoming a dynamic force in the business world [4].

However, the volumes and type of data that can be stored and retrieved from the cloud through the use of the Internet threatens the security and trustworthiness of the cloud [5]. Although the use of cloud computing promises various benefits to end-users, successful adoption of cloud computing requires an understanding of the different dynamics that are involved with cloud computing adoption. The lack of trust in the cloud computing platform is seen to have a negative impact on the successful adoption, implementation and continued use of cloud computing.

The increasing lack of trust in cloud computing that hinders successful adoption is widely recognised and highlights the significance of this research. With the proliferation of cloud computing applications for general computer users, a number of security and trust concerns have arisen [5]. For this reason, cloud computing users require a means of assessing whether or not the platform is trustworthy before adopting and using it. This study sets out to explore the most important trust issues, including confidentiality, integrity and availability, around cloud computing adoption for end-users.

A survey based on the constructs of the Proposed Trust Model [1] and the Confidentiality Integrity Availability triad [2] was administered to a convenient sample at an educational institution. The respondents identified perceived barriers to the use of cloud computing applications, specifically with regards to trust, confidentiality, integrity and availability. The results from the survey were analysed making use of descriptive statistical analysis. The results indicate that accountability, security, access, accountability and transparency are key factors to assure end-users of a cloud computing platforms trustworthiness.

Following this introduction, the theoretical background for this paper is provided which highlights the relevance of cloud computing applications, the underlying trust theory for this paper, and the Confidentiality Integrity Availability triad. The methodology, which includes the construction of the survey instrument, is described next. This is followed by an analysis of the survey results in order to identify the Critical Success Factors for enhancing end-user trust in cloud computing. The conclusion, which highlights the contribution made by this paper, is the last section of this paper.

2. Theoretical Background

Despite the vast business and technical advantages of using cloud computing, many potential cloud users are still reluctant to trust and migrate to the cloud [6]. This is largely due to the fact that the convenience and efficiency of cloud computing comes with a range of potential privacy and security related issues that pose a threat to the user‟s data. The presence of trust improves and ensures the successful adoption and continued use of the cloud, while the lack of it results in inefficient and ineffective performance and use of the services offered by the cloud [7]. Therefore, a lack of trust hampers the successful adoption of cloud computing and its continued use.

In order to determine the appropriate factors to focus on for this study, a basic content analysis of key articles in the area of cloud computing was discussed. This content analysis (Table 1) forms the basis for the development of the survey described later in this paper.

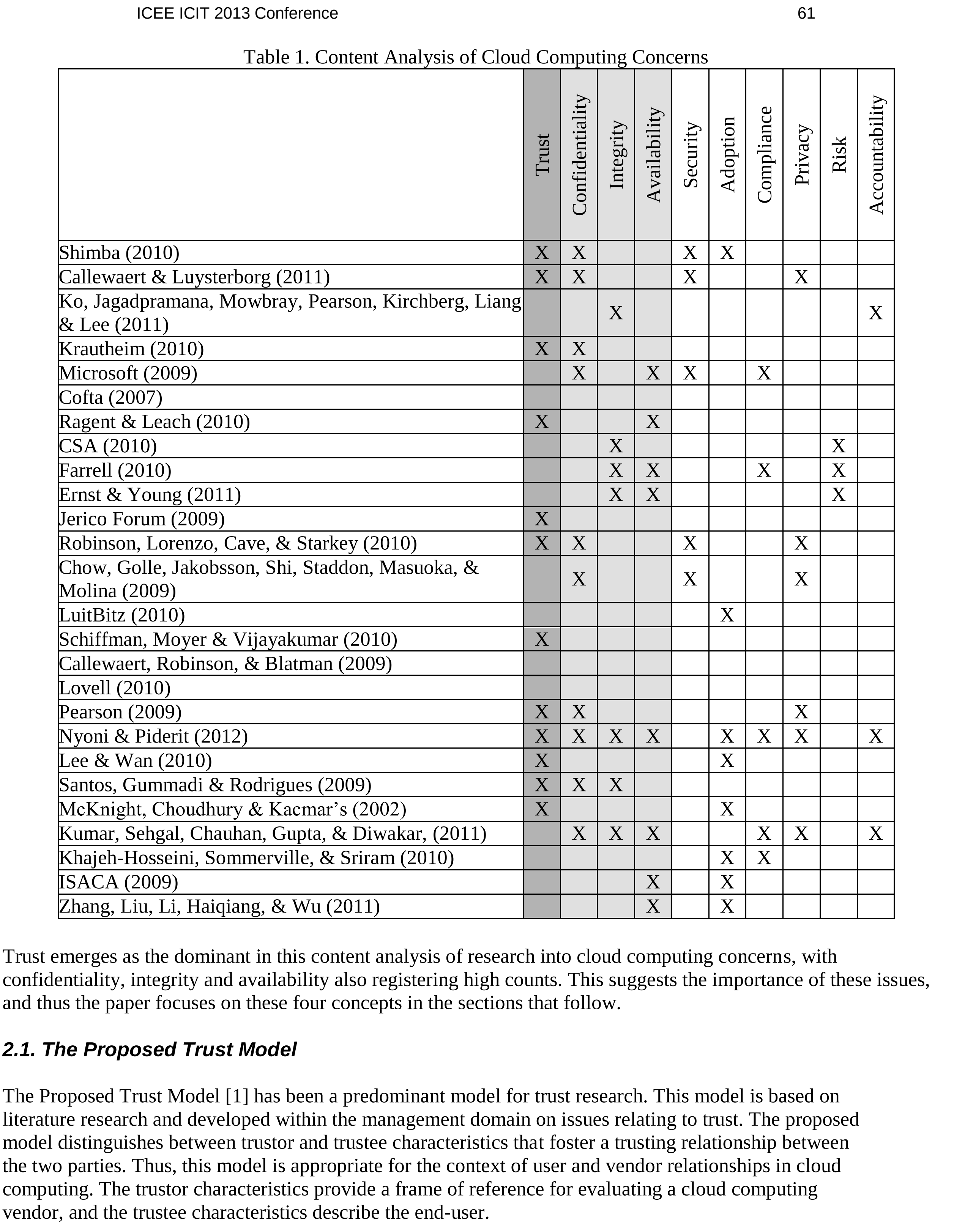


Table 1. Content Analysis of Cloud Computing Concerns

	Trust	Confidentiality	Integrity	Availability	Security	Adoption	Compliance	Privacy	Risk	Accountability
Shimba (2010)	X	X			X	X				
Callewaert & Luysterborg (2011)	X	X			X			X		
Ko, Jagadpramana, Mowbray, Pearson, Kirchberg, Liang & Lee (2011)			X							X
Krautheim (2010)	X	X								
Microsoft (2009)		X		X	X		X			
Cofta (2007)										
Ragent & Leach (2010)	X			X						
CSA (2010)			X						X	
Farrell (2010)			X	X			X		X	
Ernst & Young (2011)			X	X					X	
Jerico Forum (2009)	X									
Robinson, Lorenzo, Cave, & Starkey (2010)	X	X			X			X		
Chow, Golle, Jakobsson, Shi, Staddon, Masuoka, & Molina (2009)		X			X			X		
LuitBitz (2010)						X				
Schiffman, Moyer & Vijayakumar (2010)	X									
Callewaert, Robinson, & Blatman (2009)										
Lovell (2010)										
Pearson (2009)	X	X						X		
Nyoni & Piderit (2012)	X	X	X	X		X	X	X		X
Lee & Wan (2010)	X					X				
Santos, Gummadi & Rodrigues (2009)	X	X	X							
McKnight, Choudhury & Kacmar's (2002)	X					X				
Kumar, Sehgal, Chauhan, Gupta, & Diwakar, (2011)		X	X	X			X	X		X
Khajeh-Hosseini, Sommerville, & Sriram (2010)						X	X			
ISACA (2009)				X		X				
Zhang, Liu, Li, Haiqiang, & Wu (2011)				X		X				

Trust emerges as the dominant in this content analysis of research into cloud computing concerns, with confidentiality, integrity and availability also registering high counts. This suggests the importance of these issues, and thus the paper focuses on these four concepts in the sections that follow.

2.1. The Proposed Trust Model

The Proposed Trust Model [1] has been a predominant model for trust research. This model is based on literature research and developed within the management domain on issues relating to trust. The proposed model distinguishes between trustor and trustee characteristics that foster a trusting relationship between the two parties. Thus, this model is appropriate for the context of user and vendor relationships in cloud computing. The trustor characteristics provide a frame of reference for evaluating a cloud computing vendor, and the trustee characteristics describe the end-user.

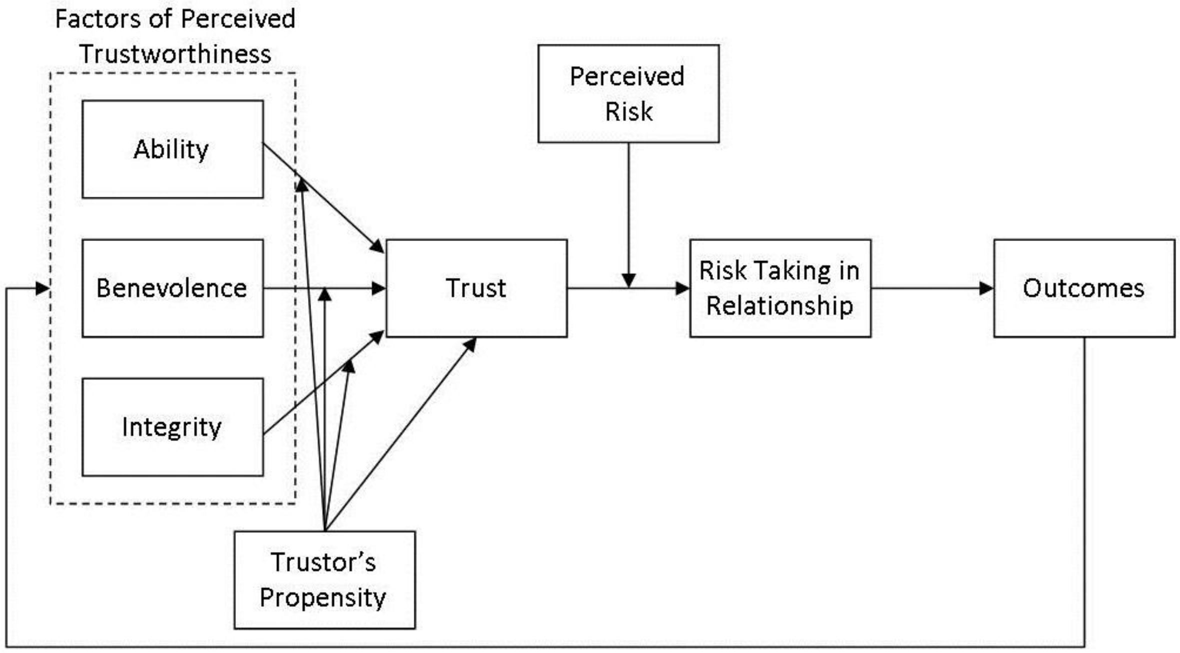


Figure 1 Proposed Model of Trust (Mayer,

In this model (Figure 1) three determinants of a trustee's trustworthiness are proposed, which are ability, integrity and benevolence [1].

1. *Ability*: This is defined as the skills, competencies and characteristics that ensure the trustee has influence in the relationship [1]. It can be further defined as collection of abilities, capabilities and characteristics that enable the trustee to have influence within a specific sphere in this case in the cloud.
2. *Benevolence*: This is defined as the extent to which the trustee is believed to want to act in the trustor's best interests [1]. It relates more to the ethics and moral judgement of the cloud computing service providers that they will act in the trustor's best interests and not to take economic advantage of the cloud computing users.
3. *Integrity*: This is defined as a perception that the trustee prescribes to the principles that the trustor finds acceptable [1]. In the cloud computing scenario, integrity would be based on the cloud vendor's attitude towards honouring his commitments to all the cloud users. It refers to a user's perception that the trustee adheres to a set of principles that the customer finds acceptable.

These key determinants of trust need to be considered when evaluating the cloud computing vendor‘s trustworthiness. Thus, ability, benevolence and integrity were investigated through the survey in order to identify the related critical success factors for cloud computing users. Further to the trust considerations, the confidentiality, integrity and availability concerns recognised in the content analysis are described in the next section.

2.2. The Confidentiality Integrity Availability (CIA) Triad

Data stored electronically in computers is a valuable asset and should be protected against unauthorized disclosure, tampering or destruction and obstruction to availability [8]. The Confidentiality, Integrity, Availability (CIA) Triad is an industry-accepted model for ensuring security in systems in order to further enhance trust in the systems. It specifically focuses on the storage and management of data. This theory was investigated through the survey administered to cloud computing users.

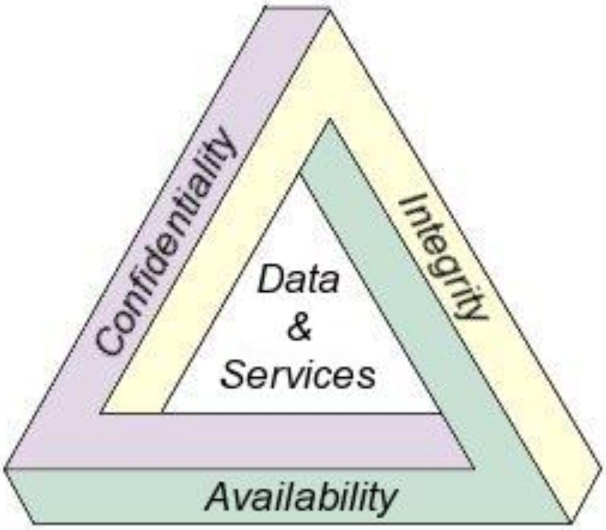


Figure 7: The CIA Triad [2]

As identified by the content analysis earlier, confidentiality, integrity and availability are key concerns with cloud computing. Thus, they require further investigation in order to enhance user trust in the cloud computing applications.

Confidentiality: This talks to the issue that user's information and data should only be disclosed to authorised parties [9]. Confidentiality is the prevention of unauthorized disclosure of information. The vendors will have to make sure that user's data confidentiality is ensured by network security protocols, network authentication service and data encryption services [9]. Confidentiality is an important part of the trust relationship between the cloud vendor and users.

1. The vendor's failure to ensure confidentiality will result in a loss of trust, damage to vendor's reputation and legal implications [8].
2. *Integrity*: Information, either in transmission or in storage, must not be changed or destroyed accidentally or worse, intentionally, by unauthorized parties. It must remain in a consistent state. Integrity therefore is the guarantee by vendors that data received and data in transit will not be altered. This is ensured by firewall services, communication security and interference detection [9].
3. *Availability* is the guarantee that information will be available to the consumer in a timely and uninterrupted manner when it is needed regardless of location of the data [9]. This means that the cloud infrastructure, the security controls, and the networks connecting the clients and the cloud infrastructure should always be functioning correctly. Availability is ensured by: fault tolerance, authentication and network security.

Based on the Trust and CIA constructs above, a survey was constructed to investigate user's perceptions of trustworthiness of cloud computing applications. The section that follows describes the methodology followed in this study.

3. Methodology

This study focused on identifying the trust, confidentiality, integrity and availability concerns relevant for user adoption of cloud computing application. Due to the nature of the surveys used in this study, a positivistic influence emerges, namely "reality as a contextual field of information" [10].

The research instrument was a formal, web based survey investigating user's perceptions of the trust, confidentiality, integrity and availability issues when adopting cloud computing. The quantitative data from the web-based survey was analysed and the responses summarised to be meaningful and to identify trends through the use of charts and graphs. These findings provide the basis for the recommendations, namely Critical Success Factors (CSFs) to enhance user trust in cloud computing applications are proposed.

The survey administered to participants was based on the constructs of the Proposed Trust Model [1]and the CIA Triad [2] as follows:

1. *Ability*: Respondents were asked to comment on the degree to which the cloud computing service provider's security practices affected use of the services. Additionally, they were asked about the effect which transparency and data recovery practices impact their assessment of the platform.
2. *Benevolence*: Respondents were asked to comment on the degree to which the cloud computing service provider's reputation affected use of the services. Additionally, they were asked about the effect which consistency and accountability practices impact their assessment of the platform.
3. *Integrity*: Respondents were asked to comment on the degree to which the cloud computing service provider's compliance practices affected use of the services.
4. *Confidentiality:* Respondents were asked to comment on the degree to which the cloud computing service provider's privacy practices affected use of the services. Additionally, they were asked about the effect confidentiality practices impact their assessment of the platform.
5. *Availability:* Respondents were asked to comment on the degree to which the cloud computing service provider's control practices affected use of the services. Additionally, they were asked about the effect which availability on demand and ease of access impact their assessment of the platform.

The results for these five constructs are described below.

4. A Survey of Cloud Computing Users

The factors affecting user trust in cloud computing applications were investigated according to the constructs of the Proposed Model of Trust [1] and CIA Triad [2], namely: Ability, Benevolence, Integrity, Confidentiality and Availability. The findings from the survey relating to these constructs are provided in the sections that follows.

4.1. Ability

Three questions in the survey focused on the effect of ability on user trust in cloud computing applications. Respondents were asked to acknowledge whether or not the attributes described would improve trust in a cloud computing platform. The results of these three questions are shown in Table 2.

Table 2: Ability Results

Attribute	% Response
Security Practices	82%
Transparency	54%
Disaster Recovery Practices	66%

The results indicate that the participants found that security practices were the most relevant mechanism to assure users of the ability of a cloud computing service provides.

4.2. Benevolence

Three questions in the survey focused on the effect of benevolence on user trust in cloud computing applications. Respondents were asked to acknowledge whether or not the attributes described were a cause of concern when using a cloud computing platform. The results of these three questions are shown in Table 3.

Table 3: Benevolence Results

Attribute	% Response
Reputation	36%
Consistency	62%
Accountability	66%

The results indicate that the participants found that Consistency and Accountability were the most relevant concerns which need to be addressed to assure users of the platform’s trustworthiness.

4.3. Integrity

Two questions in the survey focused on the effect of integrity on user trust in cloud computing applications. Respondents were asked to acknowledge whether or not the attributes described would improve trust in a cloud computing platform. The results of these three questions are shown in Table 4.

Table 4: Integrity Results

Attribute	% Response
Legal Compliance	24%
Industry Regulatory Compliance	54%

The results indicate that the participants found that compliance to industry standards were the most relevant mechanism to assure users of the ability of a cloud computing service provides.

4.4. Confidentiality

Two questions in the survey focused on the effect of confidentiality on user trust in cloud computing applications. Respondents were asked to acknowledge whether or not the attributes described were a cause of concern when using a cloud computing platform. The results of these three questions are shown in Table 5.

Table 5: Confidentiality Results

Attribute	% Response
Confidentiality of Data	76%
Privacy of Data	66%

The results indicate that the participants found that Confidentiality of the data is the most relevant concern which needs to be addressed to assure users of the platform's trustworthiness.

4.5. Availability

Three questions in the survey focused on the effect of availability on user trust in cloud computing applications. The first question, "Was the loss of control over your data a concern when using cloud computing applications?", focused on the control concerns of using cloud computing. The second question, "How important is it that your data is available on demand?", focused on the availability concerns of using cloud computing. The third question, "How important is it that your data is easily accessible?", focused on the accessibility concerns of using cloud computing. The results of these three questions are shown in Table 6.

Table 6: Availability Results

Question	Median	Mean	Agree	Disagree
Was the loss of control over your data a concern when using cloud computing applications?	1 (Strongly Agree)	1.88 (Strongly Agree)	74%	26%
How important is it that your data is available on demand?	2 (Agree)	1.86 (Strongly Agree)	80%	20%
How important is it that your data is easily accessible?	1 (Strongly Agree)	2.08 (Agree)	74%	26%

The results indicate that control of the data, availability and ease of access are important factors in determining trust in a cloud computing platform.

From the results described in the preceding sections, Critical Success Factors for enhancing user trust in cloud computing are proposed in the section that follows.

5. Critical Success Factors for Enhancing User Trust in Cloud Computing

The table below describes the Critical Success Factors (CSF) proposed based on the empirical findings described above. Each CSF is stated and then linked to the theoretical and empirical findings which led to its inclusion.

Table 7: Critical Success Factors for Enhancing User Trust in Cloud Computing

Critical Success Factor	Theoretical Findings	Empirical Findings
Security mechanisms must be adequate and operational.	Proposed Model of Trust – Ability construct	82% of respondents believed this to be relevant for enhancing trust.
Service Level Agreements between users and service providers must ensure service providers are accountable for inappropriate use of data.	Proposed Model of Trust – Benevolence construct	66% of respondents believed this to be a concern for users of cloud computing services.
Cloud Computing service providers must comply with industry regulations.	Proposed Model of Trust and CIA Triad – Integrity construct	54% of respondents believed this to be a concern for users of cloud computing services.
Cloud Computing Service Providers must ensure confidentiality of user data.	CIA triad – Confidentiality construct	76% of respondents believed this to be a concern for users of cloud computing services.
Users must remain in control of their data.	CIA triad – Availability construct	74% of respondents believed this to be relevant for enhancing trust.
Users' data must be available for use at all times.	CIA triad – Availability construct	80% of respondents believed this to be relevant for enhancing trust.

Users should be able to easily access their data.	CIA triad – Availability construct	74% of respondents believed this to be relevant for enhancing trust.

6. Conclusion

This paper tested the constructs of the Proposed Trust model and the CIA Triad in order to determine the critical success factors (CSFs) for enhancing user trust in cloud computing. From the findings of the survey distributed to participants in an educational institution, seven CSFs were identified relating to security, accountability, compliance, confidentiality, control, availability and access.

These findings confirm the relevance of the constructs of the Proposed Trust model and the CIA Triad in this context. The CSFs proposed are to be considered by a user before adopting and using a new cloud computing platform. This is the key contribution of this paper.

Further research conducted into enhancing user trust in cloud computing should propose CSFs from a service provider point of view. The CSFs suggested in this paper can also be expanded into a framework to assist new cloud computing users to determine the appropriateness of a cloud computing service.

References

[1] R. C. Mayer, J. H. Davis, and F. D. Schoorman, “An integrative model of organizational trust,” Acad. Manage. Rev., pp. 709–734, 1995.

[2] P. Steichen, “Principles and fundamentals of security methodologies of information systems - Introduction.” 2010.

[3] ISACA, “Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives.” 2009.

[4] F. Ragent and C. Leach, “Can You Trust the Cloud? A Practical Guide to the Opportunities and Challenges Involved in Cloud Computing.” 2010.

[5] X. Zhang, H. Liu, B. Li, X. Wang, H. Chen, and S. Wu, “Application-Oriented Remote Verification Trust Model in Cloud Computing,” Cloud Comput. Technol. Sci. CloudCom 2010 IEEE Second Int. Conf., pp. 405–408, 2010.

[6] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, “Authentication in the clouds: a framework and its application to mobile users,” in Proceedings of the 2010 ACM workshop on Cloud computing security workshop, 2010, pp. 1–6.

[7] V. Bourne, “Rising to the Challenge. 2010 Global IT Leadership Report.” 2010.

[8] P. Wooley, “Identifying Cloud Computing Security Risks.” University of Oregon, 2011.

[9] B. C. Johnson, “Information Security Basics,” ISSA J., vol. 8, no. 7, pp. 28–32, 2010.

[10] J. Collis and R. Hussey, Business Research: A Practical Guide for Undergraduate and Postgraduate Students. Palgrave Macmillan, 2009.

Appendix D

Questionnaire

Part 1: Participant Profile

1. Please indicate your Gender.

○ Male

○ Female

2. Please indicate your age group.

○ Less than 16 years

○ 16-21

○ 22-31

○ 32-51

○ 52-61

○ 62 years and over

3. Are you employed?

○ Full Time

○ Part Time

○ Retired

○ Unemployed

○ Student

4. Which sector are you employed in?

□

6. Please indicate your highest level of education.

High School
Bachelor's Degree
Postgraduate Degree
Diploma
Certificate
Other, please specify

Part 2: Computer Access and Knowledge

7. Do you have access to a computer?

● Yes

○ No

8. Where do you have access to this computer?

9. Have you ever had formal training on using computers?

○ Yes

○ No

10. How often do you use the Internet? Please select one

○ Several times a day

○ Once a day

○ 2-4 times a week

○ Once a week

○ Less than once a week

○ Never

11. What is your main purpose for using the Internet?

Part 3: Cloud Computing Knowledge

12. Which of the following have you used or do you use? Select all that apply

□ Web based email (Hotmail, GMail, Yahoo Mail etc)

□ Amazon EC2

□ Microsoft Skydrive

□ Google Apps (Google Docs)

□ Apple iCloud

□ Skype

□ Evernote

□ Microsoft Office 365

□ Dropbox

□ Rackspace

□ I have not used any of these services

13. Please name any Cloud Computing applications or services you are aware of.

14. Which of the following do you consider to be cloud computing applications? Select all that apply

□ Web based email (Hotmail, GMail, Yahoo Mail etc)

□ Amazon EC2

□ Microsoft Skydrive

□ Google Apps (Google Docs)

□ Apple iCloud

□ Skype

□ Evernote

□ Microsoft Office 365

□ Dropbox

□ Rackspace

Part 4: Usage Concerns

(Please Mark (**X** *) Relevant Response)*

15. What are,or would be, your key concerns about using Cloud Computing applications or services?

	Security challenges and practices
	Reputation of provider
	Loss of Control
	Privacy policy/policy statement/challenges
	Compliance with industry standards and
	Regulations
	Loss Governance
	Other (please specify)

16. What factors related to a service provider would encourage you to trust the service provider and use the Cloud Computing application or service? Select all that apply.

	Compliance - with industry standards
	Security practices
	Vendor size, location and number of clients
	Reputation
	Accountability
	Transparency
	Disaster recovery and business continuity plans
	Other (please specify)

17**.** How important is it for Cloud Computing Services to be;

Question Number		Not Important	Neutral	Important	Very Important
3.1	**Available** on demand				
3.2	**Accessible** on demand				
3.3	**Secure** all the time				
3.4	Have **24/7 Technical Support**				
3.5	**Flexible** and **Scalable**				

18. Are the following factors relevant barriers to widespread Cloud Computing adoption?

	Strongly Disagree	Disagree	Agree	Strongly Agree

Security concerns				
Integration issues with existing systems and applications				
Loss of control over data and applications				
Availability and performance concerns				
Regulatory, Compliance and IT governance issues				

19. Please relate any experience you have had (positive or negative) while using any cloud computing application or service.