Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2016 Proceedings

International Conference on Information Resources Management (CONF-IRM)

2016

Enhancing User Trust in Cloud Computing Applications

Roxanne Piderit
University of Fort Hare, rpiderit@ufh.ac.za

Tamsanqa Nyoni
University of Fort Hare, 200800344@ufh.ac.za

27. Enhancing User Trust in Cloud Computing Applications

Roxanne Piderit
University of Fort Hare,
rpiderit@ufh.ac.za

Tamsanqa Nyoni
University of Fort Hare,
200800344@ufh.ac.za

Abstract

Despite the surge in activity and interest in cloud computing, 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 foundation for this paper. The significant role that trust plays in use of cloud computing was considered in relation to various trust related models, theories and frameworks. The available trust models, frameworks and cloud computing adoption strategies focus on cost reduction and the various benefits that are associated with migrating to the cloud. This paper focused on the lack of user trust in cloud computing applications, and strategies of enhancing user trust with reference to the Proposed Trust Model by Mayer, Davis, and Schoorman, (1995) and the Confidentiality, Integrity, Availability (CIA) Triad. A questionnaire was used as the means of gathering data on trust related perceptions of the use of cloud computing. An initial cloud computing adoption model was proposed based on key portions of cloud computing literature that was explored, combined and expected to enhance trust in cloud computing. This initial model was an important foundation for the establishment of the Critical Success Factors (CSFs) and thereafter the framework to enhance user trust in cloud computing applications.

Keywords

Cloud Computing, Application, Adoption, Continued Use, User Trust

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 starting 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; Shaikh & Sasikumar, 2015).

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. Thus, by reducing the required computing resources, cloud computing is an innovative ICT option which drastically reduces operating costs for its users (Knode, 2009). The emergence and application of cloud computing has helped users gain access to various computing resources more conveniently (Nyoni & Piderit, 2013). 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 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 access various computing resources and services more conveniently. 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; Horvath & Agarwal, 2015). According to Zhang et al (2011), the volumes and type of data that can be stored and retrieved from the cloud through the use of the Internet threatens the perceived security and trustworthiness of cloud computing. 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.

This paper investigates 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 a framework for enhancing users' trust in the cloud computing applications was formulated. The framework should develop user understanding in cloud computing, enhance user trust and improve adoption rates of cloud computing applications. The development of an appropriate framework will be used to assist users to evaluate the different cloud computing options available.

2. The Research Problem and Objective

Despite the vast technical advantages of using cloud computing, potential cloud users are still reluctant to trust and migrate to the cloud (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. Thus, as the management of data and services in the cloud 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 act as an obstacle in the adoption and use of cloud computing (Horvath & Agarwal, 2015; Shaikh & Sasikumar, 2015). 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 the cloud, while the lack of trust results in inefficient and ineffective use of the services offered by the cloud (Bourne, 2010). Therefore, the research problem investigated in this research paper is the lack of user trust in cloud computing applications. Therefore, this study aimed to investigate a means of enhancing user trust in cloud computing to ensure successful adoption of cloud computing. 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.

3. Theoretical Background

The proposed Trust Model by Mayer, Davis, and Schoorman (1995), Diffusion of Innovations Theory proposed by Rogers (2003), and The Confidentiality, Integrity, Availability (CIA) triad provide a theoretical framework for this study. Challenges to the adoption of cloud computing are also described in this section.

3.1. Mayer, Davis, and Schoorman (1995) - The Proposed Trust Model

The model depicted in Figure 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.

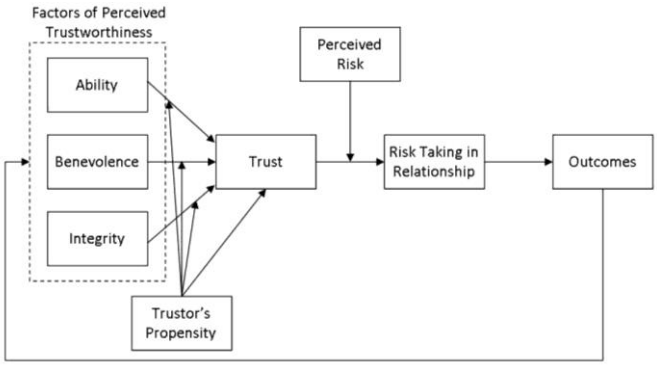

Figure 1: Proposed Trust Model
Source: (Mayer, Davis, & Schoorman, 1995)

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. These are defined as:

- *Ability*: This is defined as the skills, competencies and characteristics that ensure the trustee has influence in the relationship (Mayer, Davis, & Schoorman, 1995).
- *Benevolence*: This is defined as the extent to which the trustee is believed to want to act in the trustor's best interests (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 best interests and not to take economic advantage of the cloud computing users.
- *Integrity*: This is defined as a perception that the trustee prescribes to the principles that the trustor finds acceptable (Mayer, Davis, & Schoorman, 1995). In the cloud computing scenario, integrity would be based on the cloud vendor's attitude towards honouring his commitments to all the cloud users.

3.2. The Confidentiality Integrity Availability (CIA) Triad

The Confidentiality, Integrity, Availability (CIA) Triad is an industry-accepted model for ensuring security (Steichen, 2010). It specifically focuses on the storage and management of data. The CIA triad is depicted in Figure 2 below.

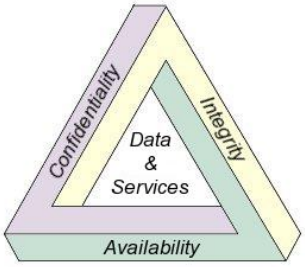

Figure 2: CIA Triad
Source: (Steichen, 2010)

- *Confidentiality*: This talks to the issue that user's information and data should only be disclosed to authorised parties (Johnson, 2010). 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 (Johnson, 2010).
- *Integrity*: Information, either in transmission or in storage, must not be changed or destroyed accidentally or 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 (Johnson, 2010).
- *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 (Johnson, 2010). This means that the cloud infrastructure, the security controls, and the networks connecting the clients and the cloud infrastructure should always be functioning correctly.

3.3. 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. Rogers' diffusion of innovations theory is the most appropriate for investigating the adoption and use of cloud computing by users. The Innovation-Decision Process (Figure 3) of the Diffusion of innovation Theory involves five steps: (1) Knowledge, (2) Persuasion, (3) Decision, (4) Implementation, and (5) Confirmation. The five steps are described in detail in Section 5.3.1 of this paper.

4. The Method

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 is 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). The questionnaire was constructed through the use of prior questionnaires related to the theories described above, and modified for a cloud computing context. As an iterative validation step is required in the Design Science Methodology, the artefact was validated through experts' reviews. The experts were selected for their knowledge and previous work in the cloud computing domain. 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.

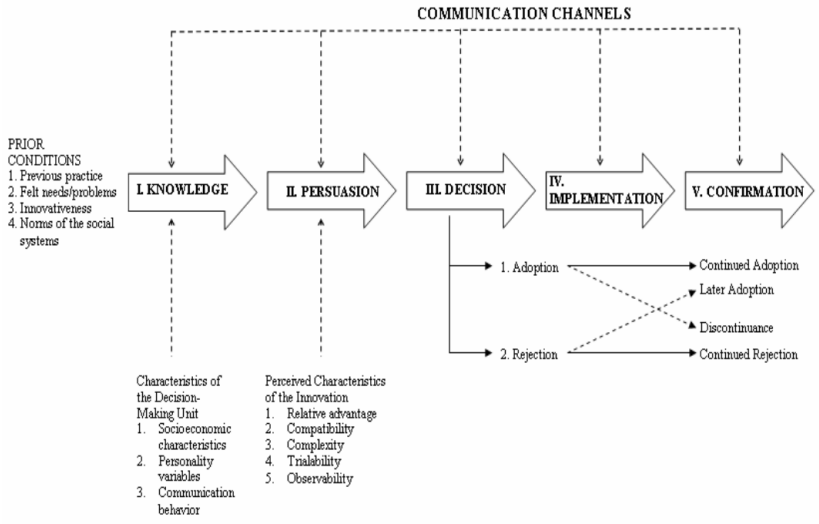

Figure 3: The Innovation Decision process
Source: (Rogers, 2003)

5. Development of the Research Framework

In this section the proposed research framework is presented. The initial literature reviewed lead to the construction of the Initial Cloud Computing Trust Model. The initial model was presented and published and tested by means of expert reviews, which led to a further refinement of the model and the need for more clearer strategies of enhancing trust in cloud computing. Thereafter, following the collection of questionnaire date, combined with the feedback from the experts review fed into the formulation of CSFs for enhancing user trust in cloud computing applications. These critical success factors were evaluated and tested by means of expert reviews. The comments and suggestions from the expert review process led to a further evaluation, refinement of the model and the need for clearer strategies of enhancing trust in cloud computing. This resulted in the proposal of 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 was presented to experts in the cloud computing industry for evaluation. 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 as presented below.

5.1. The Initial Cloud Computing Trust Model

The initial model was a combination of key portions of cloud computing literature that was explored and integrated 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 affecting trust in cloud computing. This model is presented in Figure 4 below.

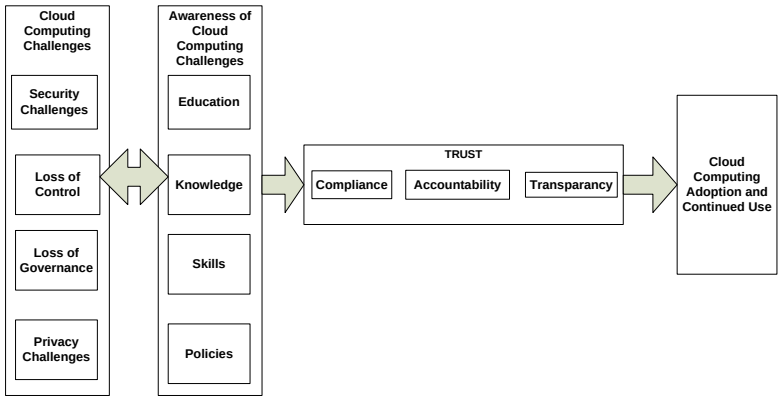

Figure 4: Initial Cloud Computing Trust Model
Source: Own creation

The model consists of the following sections, namely:

- *Cloud Computing Challenges*: The model identifies four major components that are viewed as the key issues that hinder user trust in cloud computing. The four major cloud computing challenges as identified by Kumar et al (2011) which are security, loss of control, loss of governance and privacy.
- *Awareness of Cloud Computing Challenges*: The second component of the model, talks to the awareness of the cloud computing challenges. The awareness of these challenges occurs through the education, skills, knowledge and policies that surround cloud computing, as also stated by Locke (2004).
- *Development of Trust and Adoption*: In order to develop user trust in cloud computing, the model includes Compliance, Accountability and Transparency to enhance the level of user trust in cloud computing, eventually leading to the successful adoption and continued use of the cloud. According to Robinson et al. (2010), these are the main issues that underlie and enhance user trust in cloud computing.

In order to determine the relevance of the Initial Cloud Computing Adoption Model in enhancing trust leading to cloud computing adoption and continued use it had to be evaluated by experts in the cloud computing fraternity. Three expert researchers recognised the relevancy of the model terms of a solution in web applications and its clarity in attempting to solve the problem of lack of trust in cloud computing adoption and use.

5.2. Critical Successes Factors for Enhancing User Trust

The Critical Success Factors that will be discussed in this section are based on both the results from the questionnaire and a content analysis that was carried out on the literature reviewed. The results in the form of comments and suggestions from the expert reviews were also valuable in the formulation of the CSFs. The content analysis showed that trust is a dominant concept in the

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 this paper focuses on these four concepts in the development of CSFs and in the overall development of the framework. The critical success factors are described in Table 2 below which includes a brief discussion of the empirical findings which were relevant.

Critical Success Factor	**Description**	**Relevant Empirical Findings**
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.	• 79.80% of the total survey respondents believed this to be relevant for enhancing their trust in cloud computing applications. • 82.83% of the respondents indicated that they considered a secure cloud environment as one of the important cloud computing benefit. • 81.81% of the respondents agreed that security concerns and breaches were relevant barriers to cloud computing adoption and use.
2. Service Level Agreements (SLA) between users and cloud computing service providers must ensure service providers are accountable for inappropriate use of data.	SLA should ensure 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 their (users) data. This CSF is in line with the Benevolence construct of the Mayer et al. (1995) Proposed Model of Trust.	• 66% of respondents believed this to be a concern that needs to be clearly addressed before they can trust and use cloud computing applications. • 65 of the 99 respondents indicated that accountability for security, private breaches and contractual obligations on the cloud service provider side will enhance their trust in cloud computing applications
3. Cloud Computing service providers must comply with industry regulations.	This factor is based on the Proposed Model of Trust and CIA Triad, Integrity construct. It strongly suggests that for any users to trust cloud computing applications, the service providers need to show and prove that they are compliant to all the set industry regulations that govern the cloud computing community.	• 55.56% of the respondents believe service providers' compliance to industry regulation is a concern that affects users trust in of cloud computing applications. • 72.72% of the respondents indicated that they considered it to be a relevant barrier to cloud computing if the service provider did not address the IT governance concerns and was not compliant with the industry regulations. • 22.22% respondents considered it to be a key cloud computing concern if the service provider did not comply with the industry regulations and contractual obligations.
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 ensure users that the confidentiality of the users and that of their data will be treated with high regard all the time.	• 79.80 % of the respondents indicated that confidentiality of the user and their data was a concern.
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 users data in the cloud. 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 in total control of their data all the time.	• 74% of them strongly believe that having control of their data while in the cloud is relevant for enhancing trust. • 72.72% of the respondents agree that the loss of control over data and applications is a relevant cloud computing applications adoption barrier. • 45.455% of the total 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.
6. Users' 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 always all the time. This is to say the data stored on the cloud by users should always be available for them to use it and anytime they need to use it.	• 80.81% of the respondents believe that the availability of their data for use all the times to be a relevant benefit for enhancing their trust in cloud computing applications. • 73.73 % of the respondents agree that the availability and performance concerns to be relevant barriers to cloud computing. • 79.80% of the total respondents indicated availability, confidentiality and integrity as cloud computing key concerns.
7. Users should be able to easily access their data from cloud computing applications.	The last of the seven CSF which is in line with the CIA Triad's Availability construct is more concerned with the user's ability in accessing their data in the cloud. This CSF suggests that for users to have trust in cloud computing applications, the service providers have to ensure that they (users) are in a position to easily access their data using various devices that the users might possess.	• 79.8 % of the respondents indicated the relevance of the ease of access to their data whenever needed as an important cloud computing benefit.

Table 2: Critical Success Factors for User Trust in Cloud Computing
Source: (Own Paper, 2013)

In order to determine the relevance of the Critical Success Factors in enhancing trust leading to cloud computing adoption and continued use, the CSFs had to be evaluated by experts in the cloud computing community. Three expert researchers in the cloud computing field acknowledged the relevancy of the suggested critical success factors in solving the problem of lack of trust in cloud computing applications. The three experts commented as to what the most important and relevant CSFs were for users to consider. They also wanted to know, according to the study and the empirical evidence collected what the single most important CSFs and indicators of trust or trustworthiness of cloud providers were. Evidence from the empirical evidence points to that there is no single CSF that will ensure the enhancement of trust, but instead indicate that a combination of the above mentioned CSFs enhance user trust in cloud computing application. These comments and feedback from the expert review prompted the development of the framework detailed in this paper for users to use as a means of assessing the trustworthiness of cloud computing service providers before they adopt and use their applications. The proposed CSFs will be further expanded into a framework to assist new cloud computing users to determine the appropriateness of a cloud computing service.

5.3. Framework for Enhancing User Trust in Cloud Computing Applications

The proposed framework shown below (Table 3) is a combination of the CSFs for enhancing trust in cloud computing applications that are merged together with the 5 stages of the Innovation-Decision Process discussed previously. Thus the CSFs and the 5 stages 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 sets of 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.

It is important to note that the proposed framework considers each of the 5 steps of the Innovation-Decision Process as individual but inter-linked stages. 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 side of the framework provides a list of the CSFs that were drawn from the literature review and the surveys empirical findings. The framework's first row presents the phases (stages) of the Innovation-Decision Model. These stages are briefly discussed below with reference to the proposed framework and in enhancing user trust in cloud computing applications:

- *The Knowledge Stage*: This is the initial stage where the cloud computing users become aware of the applications provided by the service provider and the subsequent CSFs for accessing the trustworthiness of the service provider. According to Sahin (2006), an individual at this stage learns about the existence of innovation (cloud computing applications) and seeks information about the innovation (relevant CSFs).
- *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 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. In this case the decision will be made based on the "persuasion" done by the service provider during the persuasion stage and the amount of information gathered at the knowledge stage with regards to cloud computing and the relevant CSFs.
- *The Implementation Stage*: The implementation stage is when the innovation is adopted and put into practice (Sahin, 2006). This is the stage where the users actually trust and adopt cloud computing applications for use. However, according to Rogers (2006) and Sahin (2006), at this stage the innovation still carries with it some degree of uncertainty
- *The Confirmation Stage*: According to Sahin (2006), after the innovation adoption decision has been made, at the confirmation stage the individual looks for support for their decision of adopting the innovation. At this stage the user looks for reasons to continue trusting the service provider together with the cloud adoption application.

The refined final 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 is presented in Table 3 below.

Critical Success Factors	Knowledge	Persuasion	Decision	Implementation	Confirmation
Security Mechanism	User Awareness of all Security Threats affecting Cloud Computing Applications.	Evidence of Effective Information Systems Management Programme(ISMP) & Data Loss Prevention Measures	User Decision to trust and Adopt or Reject is made based on the Service provider's available Security Mechanisms	Implementation of Effective and Efficient Security Mechanisms	Continuous Assessment and Control of Implemented Security Mechanisms
Accountable Service Level Agreements (SLA)	Service Level Agreements must be understood by both parties	Evidence of an Incident Response & Resolution Times Plan that Complies With Industry Standards	User Decision to trust and Adopt or Reject is made based on the Service provider's accountability to the SLA	Implementation of Industry accepted SLA	Continuous Assessment of the Implemented Service Level Agreements
Compliance with Industry Regulations	Service provider's compliance with Industry Standards must be investigated and understood	Compliance with the Protection of Personal Information (POPI) Act & availability of a Cloud Computing Assurance and Audit Program	User Decision to trust and Adopt or Reject is made based on the Service provider's compliance with Industry Regulations	Implementation of the correct Industry Regulations	Continuous Assessment of Service provider's compliance with the Implemented Industry Regulations
Data Confidentiality	Service providers Data Retention Polices must be investigated and be in line with the Data Protection Laws	Availability of Effective Data Retention Policies and the Right to Audit the Provider's management and Storage System	User Decision to trust and Adopt or Reject is made based on the Confidentiality of user data provided and assured by the Service provider	Implementation of Effective Data Protection, Data Retention Policies and Laws	Continuous Assessment of Implemented Data Protection, Data Retention Laws and Policies
Data Control	User Awareness of the need to maintain control and Ownership of Data	Policies that maintain that the ownership of Data remains with the user and the ability to provide the physical location of storage data upon request	User Decision to trust and Adopt or Reject is made based on the availability of policies that ensure, maintain that data ownership and control remains with the user	Implementation of Data loss Liability Clause and Data Control Policies	Continuous Assessment of Implemented Data Control Policies

Availability of Data	Availability of user Data in transit/ stored by the Service provider must be investigated and understood	Evidence of multi (fail-safe) Internet connections, options on the back up and restoration processes with disaster recovery Plans	User Decision to trust and Adopt or Reject is made based Availability of user Data regardless of Geographical Location	Implementation of Infrastructure and Environment that assures the Availability of Data all the time	Continuous Assessment of the Implemented Infrastructure and Environment
Accessibility of Data	Accessibility of user Data in transit/ stored by the Service provider must be investigated and understood	Guaranteed round the clock accessibility to user data, Defined Response and Downtime resolution Times regardless of time zones	User Decision to trust and Adopt or Reject is made based Accessibility of user data regardless of time zones	Implementation of various mediums and devices for easy access to user data	Continuous Assessment and Regular updates of providers devices and mediums to be in line with users technology and infrastructure used to access data

Table 3: Framework for Enhancing Trust in Cloud Computing Applications

6. Conclusion

This research paper presented a study of trust in cloud computing, in particular the lack of user trust in cloud computing applications that hinders adoption and widespread 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 widespread adoption and continued use.

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. This study can also be repeated on other new technologies. It would also be interesting to investigate relative perceptions of alternatives to cloud computing, such as self-hosting, or the impact of educating users on risks of use of cloud computing or its alternatives.

References

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 .

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.

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

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

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

Horvath, A. S., & Agrawal, R. (2015). Trust in cloud computing. In SoutheastCon 2015 (pp. 1-8). IEEE.

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

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

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 .

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.

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 .

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

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

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.

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

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.

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.

Shaikh, R., & Sasikumar, M. (2015). Trust Model for Measuring Security Strength of Cloud Computing Service. Procedia Computer Science, 45, 380-389.

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

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

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

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

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.