Volume 7, Issue 5, May 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review of Security Challenges in Cloud Computing Adoption: A Conceptual Framework on Early Adopters of Cloud Computing as a Technology Model

Lufungula Osembe
Independent Institute of Education-Rosebank College
South Africa

DOI: 10.23956/ijarcsse/SV7I5/0176

Abstract- Cloud computing is developing as an efficient and viable model of delivering IT services. The challenges posed to-date by security are not to be underestimated with regard to cloud computing adoption. The study assesses the security challenges associated with cloud computing adoption and proposes a framework to assist early adopters of the technology model to address them. Various sections of the literature have indicated that security challenges are a great source of concern in the adoption and usage of cloud computing, and a comprehensive framework is vital to assess previous studies conducted in this area. This study would like to propose viable mechanisms to address these challenges. The study surveyed 380 participants in Gauteng, South Africa to assess the level of agreement and disagreement about the security challenges in cloud computing. The study used a quantitative method to analyse the findings.

Keywords: Security in cloud computing, privacy in cloud computing, authentication and validation, risks in cloud computing, availability in cloud computing, trust and transparency, data recovery and backup in cloud computing.

I. INTRODUCTION

Security in cloud computing is one of the most talked about topics in the literature and this study pays attention to security challenges associated with cloud computing adoption. With the current trends and advances in cloud computing, there seems to be a consensus in the literature that security in cloud computing is real and it needs to be addressed. The aim of this paper is to propose viable mechanisms in order to minimise the impact of security challenges in cloud computing.

While cloud computing is praised for its tremendous benefits that the technology model offers, decision-makers are faced with unpleasant challenges to minimise the impact of security aspects in cloud computing. Studies conducted in this regard indicate that users and organisations are considering adopting cloud computing technology in order to achieve their business goals. On one hand there is a need and excitement among users and organisations to adopt cloud computing, and on the other hand the potential for security challenges is real and mechanisms to address these challenges are critical for an effective adoption of the technology model.

The aim of this study is to propose guidelines and viable mechanisms on how to minimise the impact of security challenges associated with cloud computing adoption.

II. BACKGROUND TO THE STUDY

Cloud computing as a technology offers a real potential for expansion and other great benefits since its inception [2]. Users and organisations have shown a great interest in the technology and various benefits offered by the technology have proven to drive many users to adopt cloud computing as a viable technology solution [1].

The following are some of the benefits of cloud computing [2, 3]:

- Cost-efficiency
- Scalability
- Agility on computing platforms
- High performance and availability of computing resources
- Better IT resource management and business focus
- Improved security
- Saving on time and cost
- Sustainability
- Flexibility
- Rapid development
- Deployment and change management
- Better performance
- Greater mobility
- Improved automation

- Customisation
- Support management
- Green IT data centers.

"References [2, 3] argue that the list of cloud computing provided above is not exhaustive". Cloud computing benefits have paved the way for many users to save on massive cost associated with maintaining hardware and software in premise-based environments [4]. While cloud computing offers a number of benefits, security challenges and concerns are not negligible in the adoption of the technology model. This paper pays a particular attention to the security concerns associated with the adoption of the technology model by early adopters. The study would like to propose a conceptual framework in order to address these challenges.

III. LITERATURE REVIEW

III-A. CLOUD COMPUTING

Cloud computing is defined as a virtual pool of resources delivered over the Internet, offering on-demand systems software over the network with minimal human interaction [1]. In addition, "reference [5] provides a more technical and systematic definition to cloud computing as a compilation of existing techniques and technologies packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster start-up time, reduced management cost, and just-in time availability of resources".

The following are the characteristics about cloud computing [6]:

- On-demand self-service whereby the user has the ability to manage and perform computing tasks with minimal interaction from the service providers.
- Measured service whereby the user only pays for the service used.
- Resource pooling whereby the resources are made available through the network.
- Rapid elasticity and scalability whereby computing resources are delivered in a flexible manner and scaled based on users' requirements.

Services in cloud computing are presented at three levels, namely, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS). In addition to these three delivery models, other services generally referred to as the XaaS develop on regular basis [7]. "Reference [5] categorises the deployment models in cloud computing as follows:

- Public cloud whereby services are made available through the Internet;
- Private cloud whereby services are exclusively managed by one organization;
- Community cloud whereby computing resources are shared by organisations with similar policies or requirements; and
- Hybrid cloud whereby one, two or three of the above models are combined then deployed as a standard and single unit or entity".

III-B. SECURITY IN CLOUD COMPUTING

After discussing the background to the study, this section discusses aspects related to security in cloud computing. Security is one of the most important concerns reported in cloud computing adoption, thus the topic attracts a lot of attention [8, 9].

In many instances, the responsibility remains with the service provider to ensure security, protection of data from theft, malicious attacks and access [10]. One of the critical questions to be examined in this study is to assess how do security challenges affect the adoption of cloud computing.

1) SECURITY CONCERNS IN CLOUD COMPUTING: Security is considered as one of the major concerns in the implementation and adoption of any technology, and cloud computing is no exception. Security becomes an important factor since data used and shared by organisations should be protected, and unauthorised agents must not be allowed to have access [10]. The implication of security issues in the cloud leads to issues around privacy, confidentiality, authentication, encryption and decryption, data protection just to name a few [11].

With data in the cloud and data centres being controlled by a third party, there is no real guarantee for data security. This leaves the user with almost no power since the user is not in control of his data. The security concern affects both the user and the service provider. This constitutes a challenge in ensuring proper backup and recovery mechanisms for data and authentication of users, as well as data accessibility [12].

Given the current security threats in cloud computing, studies conducted in this regard indicate that clear measures are being taken to deal with security challenges in the cloud. Despite these clear measures, security challenges remain a big threat toward cloud adoption and implementation, with little room for users to make a choice other than to rely on the service provider [13]. There is a need in this study to establish the extent of security concerns with regard to the adoption of cloud computing.

***2) ORGANISATIONAL RISKS IN CLOUD COMPUTING*:** Security in cloud computing has direct implications on how the user wishes to handle its privacy and data security. There are also direct implications when affected by security threats and the manner in which the user intends to respond in order to protect his/her data.

"Reference [11] reiterates that data security and user's personal information remain a great concern in the cloud, and protecting these elements remains a great challenge for service providers". An effective information security governance

should be in place to protect organisation's data as agreed upon in the service level agreement. "Reference [11] adds that this type of information security governance should be replicable across the organisation". Thus, the security governance should be measurable, sustainable, repeatable and scalable.

***3) PROTECTION OF DATA FROM THEFT IN CLOUD COMPUTING*:** One of the most complex challenges identified in the literature is the protection of data in cloud computing [14]. Cloud computing service providers and users have no full control over application deployments and service delivery in the cloud, thus making data more vulnerable in various ways. "Reference [13] recalls the two spheres of data protection in cloud computing providing no geographic boundaries, where data protection can be provided as compared to in-house environments".

With cloud computing, data becomes the subject of breach and unauthorized access from internal or external quarters. The use of available methods such as encryption, draft of policies or security assurance mechanisms to regulate breaches can reinforce data protection. Protection of data in cloud computing will go a long way as long as there is a full commitment from both the service providers and users. Little has been done in the literature to create awareness for users in this regard. This study is about providing viable mechanisms to protect data from theft in the cloud.

***4) DATA ACCESS AND CONTROL IN CLOUD COMPUTING*:** While cloud computing provides data accessibility anywhere and anytime, there are various security risks to data stored outside the confinement of the organisation providing the service. "Reference [9] claims that despite the level of organisational security such as providing firewalls and other security controls, security remains a great challenge to deal with".

The complexity of organisational security is exacerbated by the fact that many insiders have access to organisational network systems on one hand and on the other hand, third parties are allowed to carry out or manage data operations. Data access and control in cloud computing seem to be difficult to administer [12]. The greatest challenge in the administration of data is exacerbated by the fact that even confidential data is illegally accessed because of the lenient access controls in the cloud.

"Reference [12] explains that the duration of data in the cloud can further increase the high possibility of risks for intruders to access data". At the same time, some of the increased risks associated with data access and control in the cloud emanate from both internal and external environments. Thus, data access poses a serious challenge to cloud computing adoption. The amplification of the accessibility risks in the cloud has become critical because IT services and users converge on one management domain with little transparency into the process and procedure [12].

The policy of compliance and granting access to users might not be fully explained or highlighted in the service level agreement with service providers, which can contribute to an attractive opportunity ranging for hobby hackers, organised crime to state-sponsored intrusion. Data access brings another dimension of trust in cloud computing. "Reference [15] claims that trust of data in cloud computing is critical to ensure a level of security in the provision of the service". The lack of trust often leads to issues of credibility, sensitivity and reputation, which have negative consequences. "Reference [15] further explains that the security of data in cloud should be trusted by users and the service provider through clauses established in the SLA". "Reference [15] also indicates that these established parameters in the SLA should protect the sensitivity or criticality of data, the quality of data, as well as other security parameters". This paper will further discuss aspects related to trust in this section of the literature.

These arguments contribute largely to the body of knowledge on data access and control in cloud computing and its impact on users.

5) AVAILABILITY ISSUES IN CLOUD COMPUTING: Availability is considered as an important characteristic in cloud computing [3]. "Reference [16] defines availability as a process of optimising the readiness of production systems by accurately measuring, analysing and reducing outages to the production systems".

The major goal of data availability in cloud computing is to ensure that users are able to access data anytime and anywhere [13]. With no room for doubt, the three main cloud services do the same function of providing the services anywhere when needed [12]. Service providers are said to do everything at their disposal to provide redundancy to make data accessible to a number of users.

The challenge though remains on the service providers to ensure availability of data anywhere and anytime [13]. When major operations or upgrades are undertaken by the service providers, serious risks of data unavailability and interruption are experienced by the user on one hand and on the other hand, the problem could even be exacerbated by the inefficiency of network or capacity of bandwidth to support upgrades.

The question of high availability of data in cloud computing constitutes one among other risks posed in cloud computing adoption. Little is done to ensure that data is available twenty-four hours a day, seven days a week, and three hundred and sixty five days a year. Users have little to do to protect their data; therefore, they are affected by the effect of availability of their data in the cloud.

6) DATA RECOVERY AND BACKUP IN CLOUD COMPUTING: Users have the obligation to ensure that they are aware of basic backup and recovery mechanisms to protect their data in the cloud. "Reference [17] claims that basic recovery and backup strategies are sometimes overlooked by users". "Reference [17] further explains that overlooking these aspects can bring an unrepairable damage to data stored in the cloud". The duration and time frame it should take to recover from outage and power failure in the cloud should be highlighted and accounted for in the service level agreement. Clear assurance mechanisms should also be provided by the service provider (SP) in the interest of recovering data in the cloud.

Consequences of not recovering data on time have immense financial and organisational implications for the user, who has invested in the technology [17]. As highlighted in the literature, implications of not assuring data recovery and backup raise issues around compliance and governance.

The issue of data recovery and backup in cloud computing has been one among other great concerns raised in cloud computing adoption. Little has been done in the literature to create awareness around data recovery and backup in the cloud for users. This paper would like to propose viable mechanisms to address these concerns.

7) STANDARD-BASED SECURITY ISSUES IN CLOUD COMPUTING: Security issues are considered as a nightmare by many users. Cloud computing technology has provided various alternatives to most and very complex security aspects as compared to in-house or on premise technologies [13, 18]. The challenges and concerns in the cloud though severe, "reference [3] indicates that security in the cloud can be tailored to suit the user's requirements". This is an important development where the user is able to focus on the core aspects of the business rather than spending a lot of effort to address complex mechanisms of securing data in the cloud.

This study has noted that though the customisation of security requirements seems to be an important development in cloud computing, users remain largely concerned about the implications of security issues, especially when they have little or not adequate understanding of the security standards offered by the technology model.

8) DATA PRIVACY IN CLOUD COMPUTING: The concept of data privacy in security has been consistently shaped by a number of factors depending on cultures and jurisdiction; thus making it not easy to define. "Reference [19] refers to privacy as being the accountability of the organisation to data, as well as its transparency with regard to personal information". The concept of privacy goes further and covers aspects of the use, retention and disclosure of personal information.

With this in mind, cloud computing makes it even harder for users to have a full control of their personal information since data is stored in data centres and servers located around the world. Though mechanisms might be provided by service providers, data privacy transcends beyond aspects of confidentiality and trust from users' perspective when it comes to the privacy of personal information.

Data in the cloud is either protected or not protected at all since vulnerability of data makes all aspects of privacy very complex. "Reference [14] further argues that a valuable amount of information can be accessed by hackers and even made available to third parties with no users' consent". Cloud computing technology model remains vulnerable to potential threats from accessibility of users' data and violation of users' privacy unless users are trained and fully made aware of potential risks associated with the adoption of the technology model.

9) TRUST AND TRANSPARENCY IN CLOUD COMPUTING: After discussing the privacy of data in cloud computing, trust and transparency are other two concepts very much aligned with privacy as resulting factors for the lack of security. Trust refers to when something or someone is reliable, honest, and effective [20]. "Reference [20] further argues that the reputation of the service provider is at stake due to its credibility for providing the so-called services in the cloud; therefore, reliability, guarantee and a high level of confidentiality are expected in the process".

With uncontrollable levels of security breaches in the cloud, a trust management model is critical. A trust management is useful in various decision-making situations and environments such as intrusion detection, authentication, access control, key management, as well as other related purposes [20]. "Reference [21] argues that a trust management model in cloud computing supports the notion of identification and trustworthiness, as well as reputation of the service provider".

How data is accessed and managed is vital for the users, who heavily rely on successful completions of transactions in the cloud. Nevertheless, trust and transparency in the cloud remain a concern since the building of a strong relationship between the user and the service provider is considered as a daunting task. This paper acknowledges the concerns with regard to trust and transparency of data in cloud computing. This paper would like to propose viable mechanisms to address them.

10) AUTHENTICATION AND VALIDATION IN CLOUD COMPUTING: Authentication in the cloud provides authorisation to users using their credentials through various context-aware information to access cloud services [22]. With key considerations to authentication, authorisation and validation services provide a medium and platform to control and manage what the user needs to access based on the decision of context for all constraints associated with the profile and role of the user.

Authentication is regarded as a great concern in cloud computing [22]. Users have an important responsibility to ensure that they authenticate themselves on organisational devices to access cloud services hosted outside the peripheries of own controlled firewalls. "Reference [23] argues that the concern is even greater since authentication puts a tremendous amount of pressure on users to manage active directories of databases, as well as their own credentials stored in the cloud". In addition, "reference [22] argues that authentication and validation of users' credentials have put a great amount of overhead on both IT management and users alike to self-manage and accurately assess the impact of not being in control of their own credentials".

11) RISKS OF CLOUD COMPUTING TECHNOLOGY: "Reference [24] explains that risks faced with by users in adopting cloud computing should be made known to them including hidden risks". Some of the risks of cloud computing technology highlighted in the literature include long-term sticker-shock, long-term viability, organisational risks just to name a few, which are in nature hidden to users [8, 13].

"Reference [25] notes that since cloud computing is no more a new concept; therefore, there is a great need to create awareness among users about the risks associated with the technology model, as well as its associated impacts". The debate on risks of cloud computing technology is still far from over, and a lot of awareness needs to be created especially for users willing to adopt the model as their preferred technology [8].

"Reference [25] indicates that if users are aware of the risks of cloud computing technology; the effect of the risks might be lesser as compared to when they are not aware". "Reference [25] further argues that the awareness of a technology is largely associated with the knowledge level of the user, the competency and technology expertise to execute the

technology". Failures to account for these key developments put users at risk of losing their data resulting to losses and negative consequences. There is a need in this paper to emphasise on the level of awareness and create mechanisms to reduce the impact of hidden risks in the adoption of cloud computing.

12) REGULATORY AND LEGAL ISSUES IN CLOUD COMPUTING: Regulatory and legal uncertainties in cloud computing have raised many concerns in the adoption of cloud computing as a technology model [24]. These concerns are raised with regard to the manner in which data is managed, stored, accessed, controlled and regulated in the cloud.

The notion of data being stored in various locations around the globe and the type of laws that regulate breaches and complaints make it even difficult to protect the users' rights. The Business Software Alliance indicates that a well-balanced policy and involvement of foreign governments will play a significant role in addressing the users' concerns, as well as other related aspects such as privacy, information security, cybercrime and intellectual property in cloud computing. While a regulatory and legal framework well-designed with users' concerns in mind will be ideal to address the challenges and concerns associated with cloud computing adoption, a binding agreement is indispensable for a successful adoption process [26].

13) THE TWO CONTRASTING PARADIGMS OF SECURITY IN CLOUD COMPUTING: With immense implications that security brings in cloud computing adoption, the service provider finds itself under obligation to provide a number of security assurance mechanisms to users, who in turn are also responsible for reinforcing security controls. On one hand, "reference [27] explains that the manageability of security offerings by service providers in many instances takes away much responsibility from users of these security risks".

On the other hand, "reference [28] explains that security mechanisms in cloud computing present a number of complexities". "Reference [28] further argues that despite these security complexities in cloud computing, multi-domain interfaces of security present a number of benefits to users. Issues around technicalities, as well as complexities are left to the service provider to deal with.

Though security is still considered as one of the most challenging factors in cloud computing, some organisations are working toward reducing its complexities backed in service level agreements [17]. A security solution backed by a comprehensive service level agreement is a good way to provide peace of mind to businesses and users in order to concentrate on other areas of improvement and investment.

IV. CONCEPTUAL FRAMEWORK

The study uses the Technology Acceptance Model (TAM) as its conceptual framework. The proposed TAM model suggests that a system or technology use is a response that can be explained or predicted by a user motivation, which in turn can be directly influenced by an external stimulus consisting of the actual system or technology's features, capabilities, as well as characteristics [29, 30].

The diagram below represents the proposed TAM model [30]:

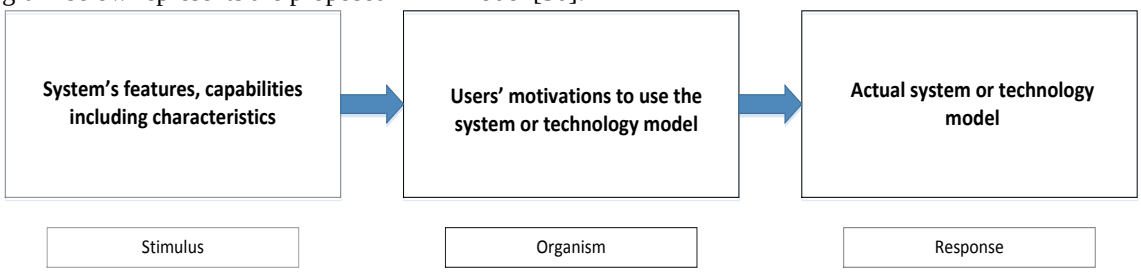

Fig. 1 The proposed TAM model [30]

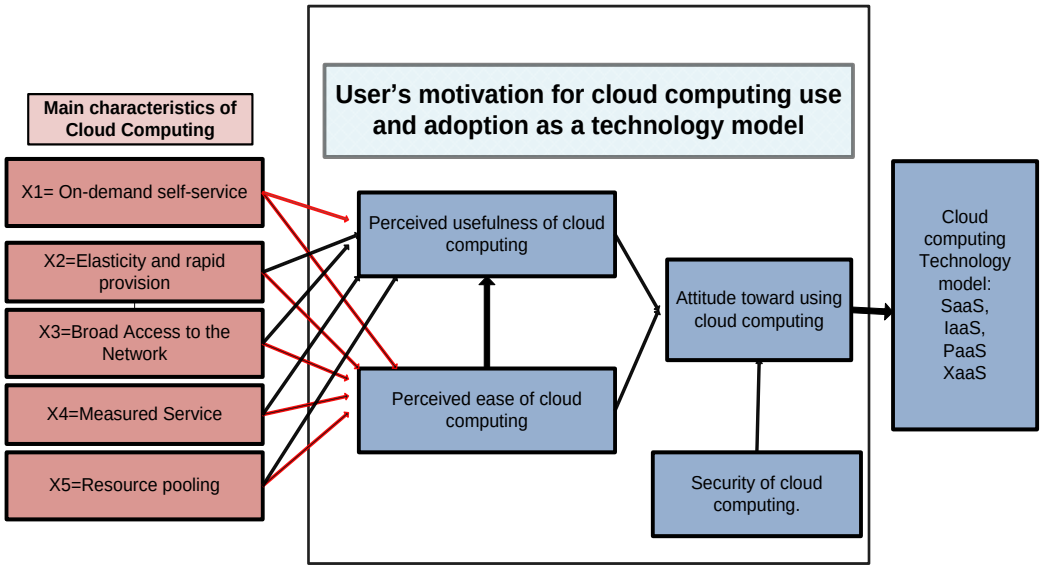

Fig. 2 Modified version of the TAM model

The framework can be applied to an information system or technology model to explain the computer usage and factors associated with the acceptance and technology adoption. The initial and proposed TAM model looks at the following three constructs, namely, perceived usefulness (PU), perceived ease of use (PEOU) and attitude towards usage (ATU) of the system [30]. With regard to this study, a fourth construct has been included to explain the phenomenon under investigation. The construct is referred to as security of cloud computing since it has an effect and an impact in the adoption and acceptance of cloud computing as a technology model. This study focuses primarily on the security of cloud computing construct since the first three constructs are not included in the scope of this research.
The following diagram represents the modified version of the initial TAM model:

V. RESEARCH METHODOLOGY AND ANALYSIS

The study used a single methodological approach. A research methodology is considered as a plan to determine the nature of the relationship between variables [32]. The methodology assists the researcher to gather participants and obtain their views.
The study used a survey-based strategy to analyse data. Usually associated with a deductive approach, the survey-based strategy is mostly used to answer who, what, where, how and why questions [33]. "Reference [33] further argues that the strategy is used for a number of reasons, namely:

- To allow the researcher to collect a wide range of data from a sizeable population;
- To allow data to be standardised for easy comparison;
- To ensure that generated data are easily understood and interpreted;
- To allow the researcher to establish possible reasons for relationships between variables and establish new models for these relationships; and
- To allow the researcher to generate findings that are representative of the whole population at a lower cost".

The study followed a descriptive-explanatory philosophy usually associated with a quantitative research where data are synthesised and analysed, and conclusions are drawn from descriptive data.
The study sampled 380 users of cloud computing in Gauteng, South Africa. These participants were among the early adopters of cloud computing. Services used in cloud computing by these early adopters include SaaS, IaaS, PaaS and XaaS. The main purpose of the research was to identify the level of security challenges among these early users of cloud computing.
Surveys in the form of online questionnaires were sent to all the participants. A Wilcoxon signed ranks test was used to test the validity and significance of results in the agreement and disagreement of findings provided by the participants.
The following diagram summarises the findings about the security challenges from the least cited to the most cited challenges by early adopters of cloud computing.

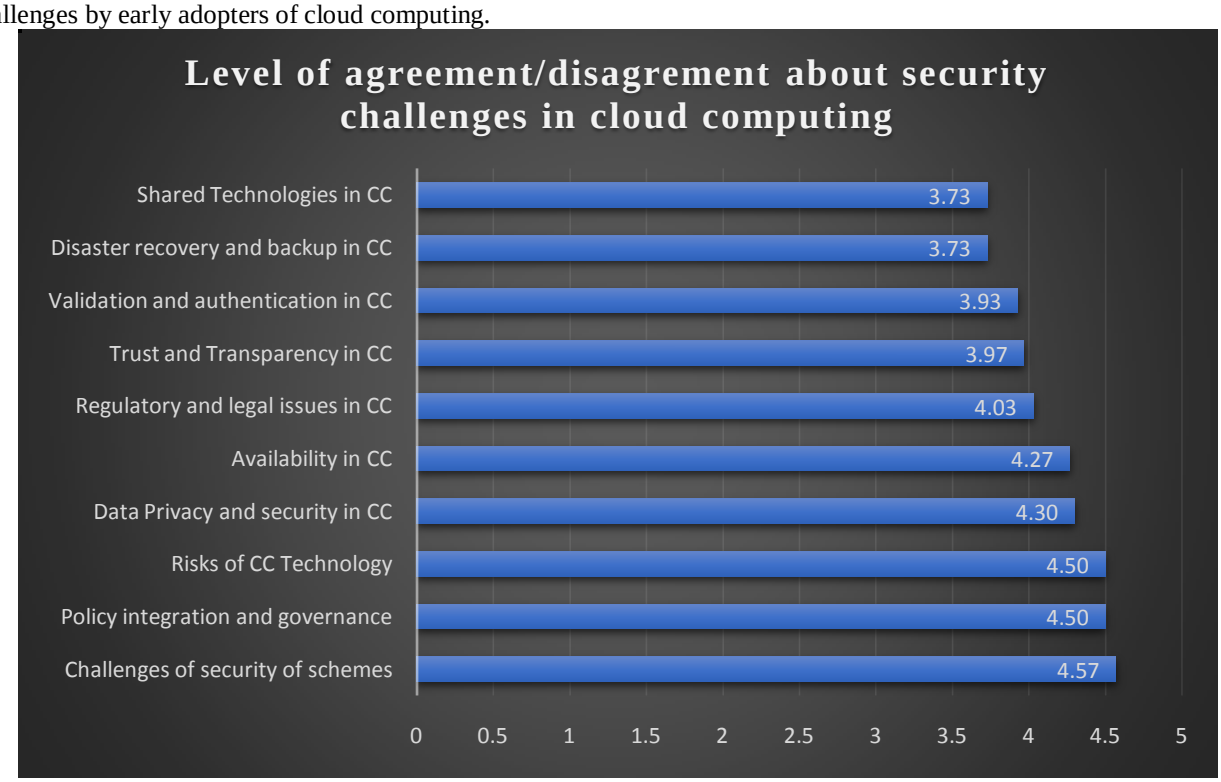

Fig. 3 Level of agreement/disagreement about security challenges in cloud computing

VI. RECOMMENDATIONS AND CONCLUSION

This section discusses the summary and provides recommendations with regard to a security framework in cloud computing adoption. The analyses of the research and discussion in the section of the literature indicate the need to address security challenges and concerns in cloud computing.

Various security platforms in cloud computing have been designed to provide guidelines to organisations and users in light of the adoption of the technology model. With security in cloud computing being one of the greatest challenges identified in the literature, proposed frameworks and mechanisms are perceived to play a vital role in minimising the risks and likelihood of seeing users incurring massive losses because of not being aware of the basic security mechanisms.

The study adapted a framework from reference [34] to support organisations and users. This framework can be further replicated across various platforms with users' perspective in mind. The framework suggests the following steps in ensuring that users and organisations are prepared to deal with aspects of security challenges with regard to the adoption of cloud computing:

- A review of business goals;
- Maintenance of a risk management programme;
- Creation of a security plan to support the business goals;
- Establishment of a corporate wide support;
- Creation of security policies, procedures, and standards;
- Audit and review plan; and
- Continuous improvement of the security plan.

The following diagram was adapted to represent the steps required in addressing security challenges in cloud computing:

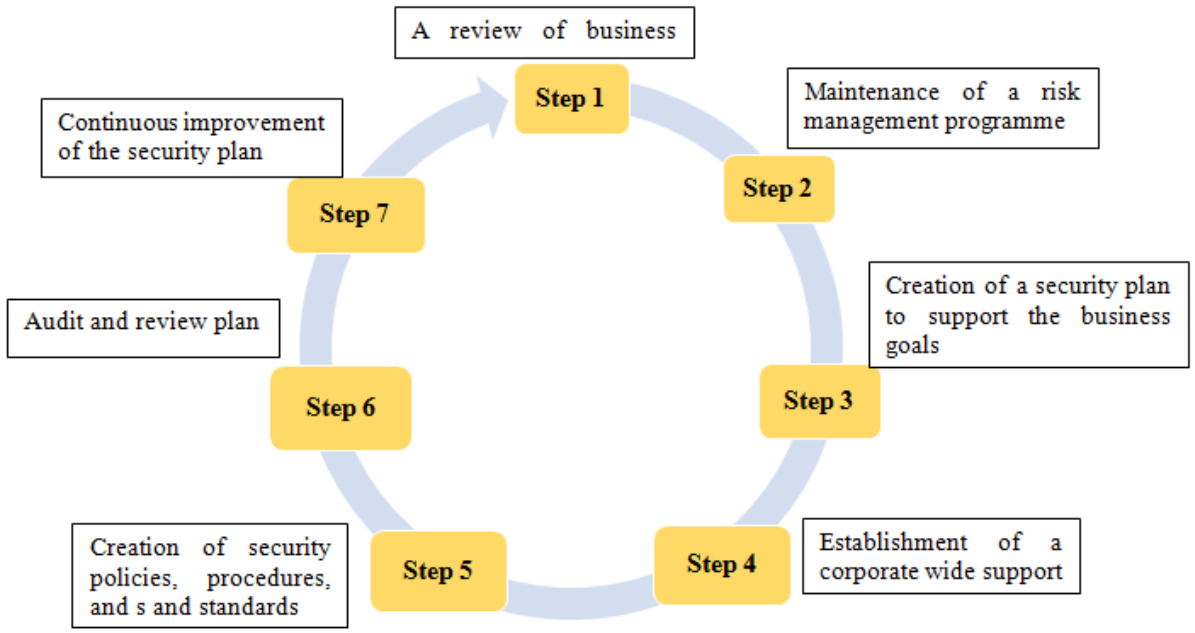

Fig. 4 Adapted security framework from reference [34]

Users are more exposed and more vulnerable given the fact that they are not aware of the risks associated with the adoption of cloud computing as a technology model. "Reference [25] explains that there is a relationship between awareness and adoption of a technology". "Reference [25] further explains that the non-adoption or lack thereof of a technology can be attributed to the lack of awareness".

Taking into consideration the seven steps proposed in creating awareness to users, the following section provides guidelines in applying the framework to meet the security requirements in cloud computing:

Step 1: A review of the business goals

Users and organisations alike need to be mindful of the type of activities and businesses they would like to move to the cloud. A clear understanding of the business goals is imperative in minimising the impact of losses or adverse risks. While users might not be sure of the type of data or businesses that need to be moved to the cloud, they need to be aware of the consequences of moving their data or activities to the cloud and assess the benefits associated with adopting cloud computing as a technology.

Step 2: Maintenance of a risk management programme

Organisations might be well vested in having a risk management plan in place to deal with any eventualities. Users instead need to establish a mechanism to address the likelihood of anything to happen in the event of loss or disaster to appease their concerns in cloud computing. This goes a long way since it requires a level of awareness and exposure to the technology to ensure that users are familiar with associated risks.

Step 3: Creation of a security plan to support the business goals

The creation of a security plan is one of the most challenging tasks in any organisations. The purpose should be to ensure that users are able to comply with the guidelines in executing the instructions to address all the security challenges in cloud computing. A security plan needs to be measurable and consistent throughout in order to bring the much-needed level of stability in the running of the organisation and take full control of data in the cloud.

In order to be effective, the security plan should include the following aspects such as monitoring mechanisms, change management, problem management, backup control strategies, physical and environmental safeguards, as well as logical and physical access.

Step 4: Establishment of a corporate wide support

While it is imperative to have a security plan in place to tackle security challenges in cloud computing, there is a need for a wide support and alignment of objectives and organisational goals to gather support from everyone in the organisation. This goes back to the issue of trust and transparency in establishing a high level of acceptance and integrity in the use and manipulation of data in cloud computing.

To start with, the level of support required by users should be aligned to security priorities to be addressed in order to ensure that there is a great level of balance between the required objectives and policies to eliminate any underlying and conflicting issues.

Step 5: Creation of security policies, procedures, and standards

As much as organisations would like to address security challenges, users should be made aware of the security policies, procedures and standards in order to achieve required goals. Users should be assisted in the design of these policies, procedures and standards to allow for a seamless integration and interpretation that eliminate possible constraints in meeting security requirements in cloud computing.

Since the aim of this paper is not to develop security policies, procedures and standards, users making use of cloud computing should pay attention to compliance to meet their security requirements. One thing to note in the development of security policies, procedures and standards is that there is a need to ensure that they are realistic, acceptable and measurable.

Step 6: Audit and review plan

The creation of a security plan for compliance does not address all the challenges and security loopholes in cloud computing. There is a need to review the security plan on a regular basis. An internal or external audit exercise will go a long way in reinforcing compliance and meeting organisational best practices.

Step 7: Continuous improvement of the security plan

It is imperative that users understand the need for an improved security plan. Once a security plan has been developed, there should be mechanisms in place to review, revise and edit where possible in order to meet the current security needs. The number of times one will decide to review or revise a security plan in the best interest of improving it, will largely dependent on what aspects of the security plan need to be addressed to meet the security requirements in cloud computing.

In conclusion, as indicated in the sections of the literature, security challenges in cloud computing constitute an important topic for discussion and users need to be made aware of mechanisms on how to address these challenges. The proposed framework only provides guidelines that can be further developed in order to reinforce compliance and minimise the impact of security challenges in cloud computing.

Users of cloud computing need to look beyond the proposed framework in order to develop a more secure and comprehensive plan that meets their security needs.

REFERENCES

[1] C. EROL, S. GULSECEN, E. KARATAS and Z. OZEN, Cloud Computing and Some Scenarios for its Applications in Universities. European Researcher, 30(9-3), pp.1515-1526, 2012.

[2] P. COWHEY and M. KLEEMAN (2013), Unlocking the Benefits of Cloud Computing for Emerging Economies - A Policy Review. [Online]. Available: http://wwww.wto.org/english/tratop-e/serv_e/wkshop-june13_e/unlocking benefits_e.pdf.

[3] A.E. YOUSSEF, Exploring Cloud Computing Services and Applications, Journal of Emerging Trends in Computing and Information Sciences, 3(6), 2012.

[4] F. ETRO, The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe: An Application of Endogenous Market structures- Approach to a GPT innovation, Review of Business and Economics, 2009.

[5] T. GLANCE and P. MELL, The National Institute of Standard and Technology - Definition of Cloud Computing, Computer Security 800-145, 2011.

[6] A. JOSHUA and N. OGWUELELA, Cloud Computing with Related Enabling Technologies, International Journal of Cloud Computing and Services Sciences, 2(1), pp. 40-49, 2013.

[7] M. MUJINGA, Developing Economies and Cloud Services: A Study of Africa, Journal of Emerging Trends in Computing and Information Sciences, 3(8), pp. 2079-8407, 2012.

[8] R. LOUW, Six Steps to taking the complexity out of moving to the cloud, TechSmart, Pretoria, 2013.

[9] I. ROTARIU and R. SERBU, Privacy Versus Authentication in the Internet Era, 22nd International Economic Conference-IECS 2015 "Economic Prospects in the Context of Growing Global and Regional Interdependencies, Procedia and Finance, 27(2015), pp. 73-76, 2015.

[10] C. CHANDRAVATHY, V. KUMAR and G. MURUGABOOPATHI, Study on Cloud Computing and Security Approaches, International Journal of Soft Computing and Engineering, 3(1), pp. 2231-2307, 2013.

[11] A. AL-YASIRI and N. KHAN, Identifying Cloud_Security threats to Strengthen Cloud Computing Adoption Framework, The 2nd International Workshop on Internet of Thing: networking Applications and Technologies (IoTNAT' 2016), Procedia Computer Science, 94 (2016), pp. 485-490, 2016.

[12] L.A. NIVEDITA and K. SRAVANI, Effective Service Security Schemes in Cloud Computing, International Journal of Computational Engineering Research, 3(2), pp. 2250-3005, 2012.

[13] K. GOYAL and SUPRIYA, Security Concerns in the World of Cloud Computing, International Journal of Advanced Research in Computer Science, 4(4), pp. 0976-5697, 2013.

[14] E.S. HAJJI and T. MAHA, From Single to Multi-Clouds Computing Privacy and Fault Tolerance, International Conference on Future Information Engineering, IERI Procedia, 10 (2014), pp. 112-118, 2014.

[15] N. BENNANI, K. BOUKADI and C. GUEGAN, A Trust Management Solution in the Context of Hybrid Clouds, IEEE 23rd International WETICE Conference, 978(1), pp. 4799-4249, 2014.

[16] R. SCHISSER, Information Technology Systems Management, City: Prentice Hall, ISBN 13:978-137 02506-0, 2010.

[17] G. TUDOR, The Importance of backup and recovery for mid-sized businesses, TechSmart Business, 2, SmartPublishing, Pretoria, 2013.

[18] S. CARLIN and K. CURRAN, Cloud Computing Technologies. International Journal of Cloud Computing and Services Science, 1(2), pp. 59-65, 2012.

[19] S. LATIF, S. KUMARASWAMY and T. MATHER, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, 1st ed., O'Reilly Media, Inc., CA, United States of America, 2009.

[20] G. SAROJINI, K.SELVAMANI and A. VIJAYAKUMAR, Trusted and Reputed Services using Enhanced Mutual Trusted and Reputed Access Control Algorithm in Cloud, 2nd International Conference on Intelligent Computing, Communication and Convergence (ICCC), Procedia Computer Science, 92(2016), pp. 506-512, 2016.

[21] M. AHMAD, M. CHONG and A. HAMID, Enhancing Trust Management in Cloud Environment, International Conference on Innovation, Management and Technology Research, Procedia Social and Behavioral Sciences, 129 (2014), pp. 314-321, 2014.

[22] E. CHOI and H. JEONG, User Authentication using Profiling in Mobile Cloud Computing, 2012 AASRI Conference on Power and Energy Systems, AASRI Procedia, 2(2012), pp. 262-267, 2012.

[23] M. SASIKUMAR and R. SHAIKH, Trust Model for Measuring Security Strength of Cloud Computing Service, International Conference on Advanced Computing Technologies and Applications (ICACTA-2015), Procedia Computer Science, 45(2015), pp. 380-389, 2014.

[24] I. WALDEN (2012), Demystifying Regulation in the Cloud: Opportunities and Challenges for Cloud Computing, International Telecommunication Union. [Online]. Available: http://www.itu.int/ITUD/treg/Events/Seminars/GSR/GSR12/documents/GSR12_CloudWald.pdf.

[25] H. AWA, O. UKOHA and B. EMECHETA, Integrating TAM and TOE Frameworks and Expanding their characteristic constructs for E-commerce Adoption by SMES, Proceedings of Information Science & Education Conference (Insite), 2012.

[26] M. HEYINK, An Introduction to Cloud Computing: Legal Implications for South African Law Firms, Law Society of South Africa (120425), 2014.

[27] I. KOUATLI, Managing Cloud Computing Environment: Gaining Customer Trust with Security and Ethical Management, Information Technology and Quantitative Management (ITQM), Procedia Computer Science, 91 (2016), pp. 412-421, 2016.

[28] L. JANCZEWSKI and A. HERRERA, Issues in the study of organisational resilience in cloud computing environments, Conference on ENTERprise Information Systems – International Conference on Project MANagement – International Conference on Health and Social Care Information Systems and Technologies, Procedia Technology, 16 (2014), pp. 32-41, 2014.

[29] M.Y. CHUTTER, "Overview of the technology Acceptance Model: Origins, Developments and Future Directions", Spouts: Working Papers on Information Systems, 9(37), 2009.

[30] F.D. DAVIS, Perceived usefulness, perceived ease of use, and user acceptance of information Technology, MIS Quarterly, 13(3), pp. 319-340, 1989. [Online]. Available: http://www.jstor.org/pss/249008.

[31] F.D. DAVIS, A Technology Acceptance Model for empirically testing new end user information systems: Theory and results, Unpublished Doctoral dissertation, MIT Slon School of Management, Cambridge, MA, 1985.

[32] S. L. JACKSON, Research Methods: A Modular Approach, 2nd ed., CA, Cengage Learning, 2010.

[33] V. VENKATECH, M.G. MORRIS, M.G. DAVIS and F.D. DAVIS, User Acceptance of Information Technology: Toward A Unified View, MIS Quarterly, 27(3), pp. 425-478, 2013.

[34] D. SALAZAR (2016), Cloud Security Framework Audit Methods, The SANS Institute. [Online]. Available: https://www.sans.org/reading-room/whitepapers/cloud/cloud-security-framework-audit-methods-36922.

