TRUST MODEL FOR EFFECTIVE CLOUD COMPUTING USAGE: A QUANTITATIVE STUDY

HARFOUSHI, OSAMA
The University of Jordan, Department of Business Information Technology
E-mail: o.harfoushi@ju.edu.jo

ABSTRACT

Cloud computing is becoming more and more important for different types of organizations. However, one of the main challenges that face Cloud Computing is Trust. This study developed a User Trust Model to increase the usage of Cloud Computing. A self-administered questionnaire was distributed online to selected cloud user's groups and communities. The items used in this study model are Availability, Data location, Data protection and Confidentiality. The results obtained from the data analysis proved that the presence of availability, confidentiality, data location, and data protection affects users' trust levels of cloud services and in turn their willingness to move into the clod in a positive way.

Keywords: *Cloud Computing, User Trust Model, Availability, Confidentiallity, Data Location, Data Protection*

1. INTRODUCTION

All through PC history, various endeavors have been made to separate clients from PC equipment needs. This reflection is gradually turning into a reality as various scholastic and business pioneers are moving towards cloud computing. Cloud computing is creative data framework engineering, imagined as the eventual fate of registering, a main impetus requesting from its crowd to reconsider their comprehension of working frameworks, customer server design, and programs [1]. The boundless utilization of interconnected systems and distributed applications has empowered the selection of inescapable and universal cloud computing situations. These situations permit clients to buy computing power in light of need, flexibly adjusting to different performance needs while providing higher availability [2]. Although many organizations are using cloud computing, fear with respect to the utilization of cloud services is still an open issue. Different concerns that prevent the adoption of cloud computing are identified in the literature, however one of the significant issues is security [3] and [4]. According to a survey from IDCI in 2009, %74 of IT and CIOs believed that the primary challenge that hinders them from using cloud computing services is cloud computing security issues. Likewise, a study completed by Gartner in 2009 suggested that more than %70 of CTOs believed that the primary reason not to use cloud computing services is data security and protection concerns [5].

The highly distributed and non-transparent nature of cloud computing represents a considerable hurdle for the acceptance and market success of cloud services [6] since users do not have direct control over their files on the cloud provider's data centre [7]. Due to the loss of control felt by customers, trust issues emerge as an important aspect of security to take into consideration [8]. Finding a tool that assesses and evaluates these security concerns with respect to cloud services is necessary in the cloud environment [4]. Here we propose a trust model that is used to evaluate cloud service strength. Such trust can be evaluated by a list of parameters that cover important aspects of security. Thus, a trust model acts as a security strength evaluator and ranks services for cloud application and services. It can be utilized as a benchmark to setup cloud service security and to discover inadequacies and enhancements in cloud infrastructure [4]. By creating a cloud trust model to evaluate and screen, enhance and upgrade, and affirm and comply with cloud ecosystem, IT experts can transform fear of the cloud into a chance to address progressively complex security and protection issues [9].

2. LITERATURE REVIEW

2.1 Cloud Computing

Cloud computing has created so much noise in the world of technology by both researchers and practitioners. The emergence of this concept was attributed to the convergence between computing and telecommunication, ubiquitous mobile devices, and the downward trend of broadband costs [10]. Cloud computing had thus changed the way IT service are developed, deployed, used, maintained, and paid for [11].

Cloud computing emphasizes the delivery of on demand computing services with minimal effort of interaction [12]. Researchers believed that attempts to introduce cloud computing began in 1997, however, it wasn't until 2007 when scholars and professionals started paying attention to cloud computing in terms of its adoption and promotion [13]. Given that cloud computing is still a new concept and affects many different aspects of IT technology, there is no single agreed upon definition of cloud computing [14]. Cloud computing was defined as kind of parallel and dispersed framework that includes a collection of virtual connected computers that are powerfully provisioned [15]. Moreover, [16] defined cloud computing as an arrangement of services enabled through a system that gives "scalable, QoS guaranteed, normally personalized, inexpensive computing platforms" on an on demand basis that can be accessed in a straightforward and pervasive manner. A standout amongst the most widely used definitions for cloud computing is the one provided by the National Institute of Standard Technology (NIST), where cloud computing is viewed as a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be accessed quickly with minimal efforts by management or interaction with service provider [17]. The NIST definition depicts five fundamental qualities of cloud computing; firstly, rapid elasticity which relates to the capacity to scale resources up or down as required. Secondly, measured service which relates to the way specific aspects of cloud services are controlled and maintained by the cloud provider. Third, on-demand self-service which implies that customers can use cloud services as needed without the need for human interaction with the cloud provider. Forth quality is ubiquitous network access which means that the capabilities provided by the cloud provider can be accessed through standard mechanisms by both thick and thin clients. Finally, resource pooling permits the cloud provider to serve its clients via a multitenant model [15]. Reference [1] identified a number of key features that are linked with cloud computing. These features are flexibility, scalability, broad network access, location independence, reliability, economies of scale and cost effectiveness, and sustainability.

2.2 Cloud Computing Layers

Cloud computing is comprised of various layers; each layer manages a specific part of making application resources available. Fundamentally, there are two primary layers: a lower and higher resource layer. The lower layer involves the physical infrastructure and computational resources while the higher layer provides services [2]; these services include software as a service, platform as a service, and infrastructure as a service [8]. Software as a service (SaaS) is the cloud model where an application facilitated by a service provider on the web is made accessible to users in a ready to use way. SaaS takes out the need to introduce and maintain applications on the user's local PC or server [18], therefore, it will be accessible from different clients PCs using unique interface [1]. Platform as a service (PaaS) offers users various software and services that do not need any downloads or installations [2]. PaaS allows developers to create and send applications without any cost especially acquiring and managing the software and hardware costs. In other words, PaaS provides all the important facilities for the building and delivering of web applications [18]. Infrastructure as a service (IaaS) is the part of the designing charge of providing the infrastructure required for PaaS and SaaS. The primary goal of IaaS is to make resources, for example, servers, storage, and network more promptly accessible by operating systems as well as applications [2]. Once the client has acquired an infrastructure from a service provider, he/she is allowed to install and run any operating system platform and application on it [18].

2.3 Cloud Computing Deployment Models

Considering the different access methods as well as cloud computing different environments, there are diverse models of deployment such as community cloud, hybrid cloud and public / private cloud. Private cloud, in this model the cloud infrastructure is only utilized by a particular organization [19]. The cloud might be overseen by the business or by third party [1]. Public cloud, in this model the infrastructure is available to the general population at large and can be accessed by any user that knows the service location [20]. This model is characterized by having no restrictions, authorization, or authentication techniques in place

[2]. Community model, in this model the cloud infrastructure is shared by several businesses and supports communities with similar interests. Such a model may be overseen by the organization or a third party, and may exist on premise or off premise [1]. Hybrid model, this model is consisted of two or more clouds (public, private, or community) that remain unique entities but are bound together by exclusive or standard innovation that enable data and application portability [20].

2.4 Security and Trust

Cloud computing has been reported to provide several advantages to businesses and customers that have switched to cloud based services, such as reliability, accessibility, cost reductions, the ability to scale services easily, flexibility, and the reduction of failure rates [21]. However, there are a number of concerns associated with cloud computing [22]. One of the most important challenges is related to security issues [8]. Recent studies have revealed that privacy, security, and trust issues arise as a result of handling computing resources by third parties that can be accessed via a network [10]. In this paper, security and trust will be investigated further in an attempt to develop a trust model that can be used by clients when choosing a service provider.

Security is regarded by many as a make or break concern. Security in cloud computing relates to things other than authenticity, authorization, and responsibility; it also relates to data protection, disaster recovery, and business continuity [23]. The very nature of cloud computing makes security perspectives quite more complex [2] as cloud computing is concerned with relinquishing direct control over numerous aspects of security and privacy [24]. As a result, many Organizations are hesitant to host their internal data on computers that are external to theirs and that might be co-hosted with applications of other companies. Furthermore, service providers have access to all the data and could deliberately or accidentally use it for unapproved purposes [22] by doing so organizations are conferring a high level of trust into the cloud provider [24]. Trust is perceived as a key concern for end-user consumers, organizational customers, and regulators. Lack of trust is a major inhibitor to the adoption of cloud services, as people are suspicious about what happens to their data once it goes into the cloud. They are concerned about who can access their data how it will be copied, shared, and used, and they fell that they are losing control [25]. Mutual trust is needed in cloud computing between the users and the service providers, this trust is irreplaceable. Mistrust can occur due to risks of data leakage, storage position security, data being investigated, data damage, service disruption, and failure of the service provider [26].

Trust and security have been crucial aspects that guarantee the sound improvement of cloud platforms, providing solutions for concerns such as absence of privacy and protection, the assurance of security and author rights [2]. Assessing the security and trust associated with cloud services is accordingly viewed as a necessity for any organization moving towards the cloud. Therefore, we have identified a list of security parameters that are important to gauge security concerning cloud computing environment. These parameters are incorporated in our trust model and include: availability, confidentiality, data protection, and data location.

Availability: It is one of the most vital information security requirements in cloud computing [27]. Availability refers to the degree to which an organization's full set of computational resources is accessible and usable [24]. System availability includes a systems ability to carry on operations even when some authorities misbehave. It also refers to data, software, and hardware being available to authorized users upon request [1]. Availability can be influenced temporarily or permanently, and a loss can be partial or complete, dangers to availability may include denial of service attacks, equipment outages, and natural disasters. The concern here is that most downtime is unplanned and can affect the mission of the organization [24].

Confidentiality: It plays a major part in cloud computing especially in terms of maintaining control over organization's data located across multiple distributed databases. Maintaining confidentiality of users' profiles and protecting their data, allows for security protocols to be enforced at various different layers of cloud applications [27]. Confidentiality refers to protecting the secrecy of the communication between a cloud user and provider and all other actions performed in various activities [4]. It relates to having only authorized parties or systems access secured data. In the cloud the risk of data compromise is expanded since countless parties, devices, and applications are involved that lead to an increase in the number of access points [1].

Data protection: It is the most crucial asset for any user or organization moving on to the cloud is data, and protecting that data is of great concern while it moves to and from the cloud environment [4]. Protection of data in the cloud is best accomplished when we have a mixture of encryption, data loss prevention techniques, integrity protection, authentication, and authorization techniques [28].

Data Location: Another common compliance issues confronting an organization is data location. Depending on in-house computing centres allows organizations to structure its computing environment and know in detail where data is stored and how it's secured. Using cloud computing, on the other hand, does not disclose this information which makes it difficult to be sure whether sufficient safeguards set up and whether legal and regulatory requirements are being met [24].

3. RESEARCH METHODOLOGY

3.1 Research Model, Sample and Hypotheses

Testing the hypotheses developed to answer the research question requires the collection of data from individuals specific to the research undertaken. It may be possible on certain occasions to collect data from every possible individual; however, in many cases this is impossible due to restrictions of time, money, and access. Furthermore, the study can be severely harmed if the population is incorrectly chosen. Therefore, it is proposed that data should be collected from the people, events, or objects that can provide the correct answer to the problem and who are considered representatives of the population. The purpose of this study is to determine the relationship among Availability, Data Location, Confidentiality and Data Protection and User Trust. The population of this study consist people that apply Cloud Computing Servers in their businesses.

Once the population is determined, the next step is to select elements from this population in order to draw conclusions about the entire population. To develop an appropriate sample from the population selected for this study, convenience sampling was used, which is a form of non-probability sampling. Convenience sampling involves randomly selecting the cases that are easiest to obtain for the sample, and continuing this process until the required sample size is reached. This method represents the best way of obtaining needed information quickly and efficiently.

Referring to the concerns discussed in the previous section, the research model and hypotheses for this study are:

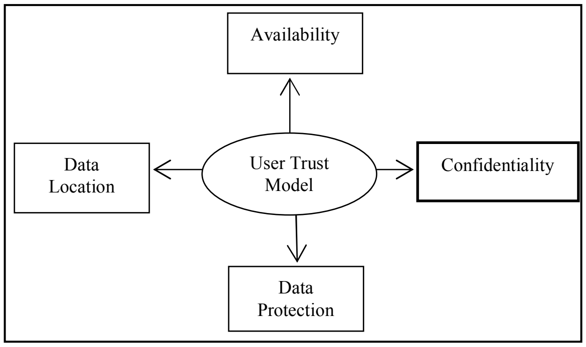

Figure 1: Research Model

Hypothesis 1: Availability is positively related to user's trust in cloud computing.

Hypothesis 2: Confidentiality of data is positively related to users' trust in cloud computing.

Hypothesis 3: Being aware of data location is positively related to the user's trust in cloud computing.

Hypothesis 4: Protection of data is positively related to users' trust in cloud computing.

3.2 Research Design

In order to assess how availability, confidentiality, data location, and data protection impact users' trust of cloud computing, a quantitative approach is carried out; in order to obtain clear understanding, researcher collected data through a questionnaire about how these components influence users' choice regarding which cloud computing provider to pick.

These data were obtained from participants working at different organizations through the use of a questionnaire. the use of questionnaire as a data collection method saves time and money, the answers obtained are not affected by the researcher, and is considered convenient for respondents. Another important feature of questionnaires is their ability to be administered to a large number of people simultaneously. The questionnaire designed for this study, is divided into five parts, beginning with a section regarding the personal data of the respondents (not used for the purpose of this study) and moving on to four sections, namely; Availability, Confidentiality, Data protection and Data Location . The questionnaire was administered by the researcher personally and by e-mail to participants working at different sectors in Jordan.

3.3 Data Collection Procedure

A self-administered questionnaire was distributed online to selected cloud user's groups and communities. The items used in this study to measure the selected variables were obtained from previous studies. Availability and data location were derived from the study conducted by [7], Data protection from [24], and confidentiality from [27] and [4].

4. DATA ANALYSIS AND RESULTS

The collected data aided the researcher in investigating the hypotheses associated with the proposed relationship between the variables of the study. Statistical Package for Social Sciences (SPSS) version 19 was used to analyse the data, where multiple regression was utilized to test the hypotheses. Thus, the results provided the basis for rejecting or accepting the hypotheses.

In order to examine the impact of availability, data collection, confidentiality, data location, data protection on users' decision to select a trusted cloud computing provider, in which these variables have been measured using 5-points Likert scale that varies between strongly disagree =1 and strongly agree =5; reliability and validity analyses were conducted.

4.1 Validity and Reliability

To determine whether the data collected is helpful and of good quality, validity and reliability should be measured. Validity is about accuracy and whether the instrument measures the right concept. Reliability, on the other hand, is more about precision as it is used to ensure stability as well as consistency questionnaire. The researchers of the current study relied on scales and items that were created beforehand and used by other researchers with comparative interests. In addition, a draft of the questionnaire was audited by five academic lecturers –who have sufficient knowledge and experience in this scope- to make sure that each item is measuring what is expected to measure, and to avoid any ambiguity or complexity in the phrasing of the questions. The reliability of the instrument was measured using the Cronbach's alpha coefficient. As suggested by [29] the values of all indicators or dimensional scales should be above the recommended value of 0.60. Table 1 presents the results of Cranach's alpha for the independent and dependent variables. It can be noticed that the Cronbach's alpha coefficients of all the tested variables were above 0.60 which demonstrates that the composite measure is reliable.

Table 1: The study variables' Cronbach's alpha coefficients

Variables	Score (%)
Availability	0.846
Confidentiality	0.837
Data Location	0.779
Data Protection	0.725
Users' trust	0.816

4.2. Hypotheses Testing Results

The fundamental motivation behind this study is to develop a clients' trust model for adopting cloud computing. The model consisted of four factors: availability, confidentiality, data location, and data protection. Consequently, with a specific end goal to test the hypotheses created for this study, multiple regression technique was used. The decision rule followed in this study is the one recommended by [30]. As indicated by them, the probability value (p-value) obtained from the statistical hypotheses test is considered to be the decision rule for rejecting the null hypotheses. In the event that the p-value is less than or equal to 0.05 (α-level), then the null hypothesis will be rejected and the alternative hypothesis will be supported. However, if the p-value is greater than the α-level, the null hypothesis cannot be rejected and the alternative hypothesis will not be supported. The results of testing the main hypotheses are demonstrated in Table 2.

Table 2: Result of the study model

Variable	r	R^2	f	Sig	β	t	Sig (t)
Availability	0.590[a]	0.348	47.315	0.001[a]	0.282	5.833	0.001
Confidentiality					0.181	4.027	0.002
Data Location					0.126	2.851	0.005
Data Protection					0.107	2.401	0.016

a. Predictors: (Constant), Availability, confidentiality, data location, data protection
b. Dependent variable: Users' trust

As shown in Table 2, there is a positive relationship between the factors of the model and the capacity of users to trust providers of cloud computing since the multiple correlation coefficient r = 0.590. The adjusted R2 relates to the generalizability of the model. It allows us to generalize the results taken from the respondents to the whole population. In this case it equals 0.348. The results also showed that the F-ratio for this model is equal to 47.315, which is statistically significant at p<0.05. Therefore, it can be concluded that there is a statistically significant effect of the different factors of the model on users' trust.

Furthermore, the β indicates to the individual contribution of each predictor (independent variable) to the model, if other predictors are held constant. Table 2 shows the standardized coefficients for each of the four factors. The values of β for availability, confidentiality, data location, and data protection are 0.282, 0.181, 0.126, 0.107 respectively, which are all positive. The level of effect of these variables depends on the β value, the higher β value the higher the effect on the dependent variable. It can be concluded from the values of beta that the variable that has the highest contribution in the model is availability, followed by confidentiality, data location, and finally data protection.

5. DISCUSSION AND CONCLUSION

When organizations transition into cloud computing, decision-makers expect their corporate interests to be protected by cloud service providers, in addition to having internal mechanisms and processes in place that minimize exposure and remedies losses. These expectations depend on intellectual procedures and lead to the separation of trustworthy institutions from others [31]. Such attributes of trust in institutions are critical for organizations and thus will influence their decision to embrace cloud computing. Therefore, this study was undertaken to develop a trust model, composed of four factors, that affects users' decision to adopt cloud computing.

The results obtained from the data analysis proved that the presence of availability, confidentiality, data location, and data protection affects users' trust levels of cloud services and in turn their willingness to move into the clod in a positive way. Availability was found to have a strong impact on users' trust of cloud service providers which supports the findings of researchers such as [7] and [32]. Availability refers to the ability to ensure that data and resources are available at any time in a continuous manner when and where needed [21]; it should guarantee that amid a short or long disruption or a serious disaster, critical operations can be instantly continued and that all operations can be re-established in a timely and composed manner [24]. Providing this feature makes clod service providers more trustworthy in the eyes of users. With regards to confidentiality, it was found that confidentiality has a positive influence on users' trust of cloud computing providers and the ability to adopt cloud computing services. This conclusion was also reached by [1] and [28]. Confidentiality refers to the protection of personal privacy and proprietary information, which should not be accessed by others as unauthorized individuals, entities, or processes [21]. Hence, confidentiality is one of the most important security mechanisms for ensuring users' data in the cloud and keeping cloud service providers from modifying or reading the content stored in the cloud [28]. As a result, providers who include confidentiality into their systems gain thereby encouraging them to move their data into the cloud. Furthermore, data location is a vital issue in cloud computing. As suggested by this study it has a positive impact on users' trust of cloud service providers. The location of the data should be transparent to users and customers. However, not all providers reveal where the data is stored [33]. Therefore, providers who share the location of the data with their users are more likely to be trusted compared to other providers. Finally, data protection was also found to have a positive influence on the trust levels of users regarding the selection of cloud computing providers. Some organizations disclose sensitive corporate information that may be abused in some way during cloud transactions. Thus privacy considerations must be default in the design and provision of cloud computing services in relation to data collection, transmission, and storage, using data minimization and anonymity [34]; [35]. Such efforts will increase the abilities and integrity of cloud service providers and their systems when dealing with different users [10].

Despite the fact that this study observed that cloud computing has the capacity to minimize capital investment for computing resources and at the same time fulfil the computational needs of organizations, it is proposed that cloud computing is not completely seized by all organizations. The study models the concepts of security and trust to clarify why organizations have not exploited such cost-saving and efficient method of handling computing needs. The discussions of the findings and the inferences from the literature and theoretical framework have shown that availability, confidentiality, data location, and data protection are fundamental necessities to demonstrate attributes of trustworthiness. Even though past writings offered a range of elements for cloud computing adoption, use, or provision, this study brought trust into the forefront as an imperative for the selection of cloud service providers and the adoption of this service by different organizations.

REFRENCES:

[1] D. Zissis, and D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems, Vol 28, 2012, pp. 583-592.

[2] E.D. Canedo, R.T. Junior,and R. Albuquerque, "TRUST MODEL FOR RELIABLE FILE EXCHANGE IN CLOUD COMPUTING", International Journal of Computer Science & Information Technology (IJCSIT), Vol 4, No 1, 2012, pp. 1-18.

[3] O. Harfoushi, A. Akhorshaideh, N. Aqqad, M. Al Janini, and R. Obiedat, "Factors Affecting the Intention of Adopting Cloud Computing in Jordanian Hospitals", Journal of Communications and Network, Vol 8, 2016, pp. 88-101.

[4] R. Shaikh, and M. Sasikumar, "Trust Model for Measuring Security Strength of Cloud Computing Service", Procedia Computer Science, Vol 45, 2015, pp. 380-389.

[5] L.M Kaufman, "Data security in the world of cloud computing", IEEE Security and Privacy Magazine, Vol 7, 2009, pp. 61–64.

[6] S. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing", In: IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE Computer Society, Washington, DC, USA. 2011, pp. 933–939.

[7] A. Rashidi, and N. Movahhedinia, "A Model for User Trust in Cloud Computing", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol 2, No 2, 2012, pp. 1-8.

[8] O. Harfoushi, B. Alfawwaz, N. Ghatasheh, R. Obiedat, M. Abu-Faraj, and H. Faris, "Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review", Journal of Communications and Network. Vol 6, 2014, pp. 15-21.

[9] EY, "Building trust in the cloud: Creating confidence in your cloud ecosystem", Available from: http://www.ey.com/Publication/vwLUAssets/EY_-_Building_trust_in_the_cloud/$FILE/EY-grc-building-trust-in-the-cloud.pdf, 2014.

[10] J.K. Adjei, "Explaining the role of trust in cloud computing", Services Info, Vol 17, No 1, 2015, pp. 54 – 67.

[11] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing – the business perspective", Decision Support Systems, Vol 51, No 1, 2011, pp. 176-189.

[12] N. Sultan, "Cloud computing for education: A new dawn?", International Journal of Information Management, Vol 30, No 2, 2010, pp. 109-116.

[13] L. Mei, W.K. Chan, and T.H. Tse, "A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues", In IEEE Asia-Pacific Services Computing Conference, APSCC '08, Presented at the IEEE Asia-Pacific Services Computing Conference, 2008, pp. 464–469.

[14] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges", Journal of Internet Services and Applications, Vol 1, No 1, 2010, pp. 7-18.

[15] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility", Future Generation computer systems, Vol 25, No 6, 2009, pp. 599–616.

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing", in INFOCOM, 2010 Proceedings IEEE, pp. 1–9.

[17] NIST, "Evaluation Plan", 2009, available online on: http://www.itl.nist.gov/iad/mig/tests/lre/2009/LRE09_EvalPla n_v6.pdf.

[18] M. Firdhous, O. Ghazali, and S. Hassan, "Trust Management in Cloud Computing: A Critical Review", International Journal on Advances in ICT for Emerging Regions, Vol 4, No 2, 2011, pp. 24-36.

[19] A. Tweel, "Examining the relationship between technological, organizational, and environmental factors and cloud computing adoption (Doctoral dissertation)", Retrieved from ProQuest Dissertations and Theses. 2012.

[20] M. Amini, "The Factors That Influence on Adoption of Cloud Computing for Small and Medium Enterprises", Masters Dissertation, UniversitiTeknologi Malaysia, Johor. 2014.

[21] S. Benabied, A. Zitouni, and M. Djoudi, "A Cloud Security Framework Based on Trust Model and Mobile Agent" Cloud Technologies and Applications (CloudTech) International Conference, 2015.

[22] H. Gangwar, H. Date, and R. Ramaswamy, "Understanding determinants of cloud computing adoption using an integrated TAM-TOE model", Journal of Enterprise Information Management, Vol 28, No 1, 2015, pp. 107 – 130.

[23] H. Katzan, "On the privacy of cloud computing", International Journal of Management and Information Systems, Vol 14, No 2, 2010, pp. 1-12.

[24] W. Jansen, and T. Grance, "Guidelines on security and privacy in public cloud computing", National Institute of Standards and Technology (NIST) Special Publication 800–144, 2011.

[25] S. Pearson, "Privacy, Security and Trust in Cloud Computing", Privacy and Security for Cloud ComputingPart of the series Computer Communications and Networks, 2012, pp 3-42.

[26] Y. Bendale, S. Shah, "User Level Trust Evaluation in Cloud Computing", International Journal of Computer Applications, Vol 69, No 24, 2013, pp. 31-35.

[27] S. Ramgovind, M.M. Eloff, and E. Smith, "The Management of Security in Cloud Computing", IEEE Computer Society, 2010.

[28] K. Jakimoski, "Security Techniques for Data Protection in Cloud Computing", International Journal of Grid and Distributed Computing, Vol 9, No 1, pp. 49-56.

[29] J. Hair, R. Anderson, R. Tatham, W. Black, "Multivariate Data Analysis", 5th ed. Prentice Hall International, 1998 London.

[30] U. Sekaran, and R. Bougie, "Research Methods for Business", United Kingdom: John Wiley & Sons Ltd, 6th edition, UK 2013.

[31] J.D Lewis, and A. Weigert, "Trust as a social reality", Social Forces, Vol 63, No 4, 1985, pp.967-985.

[32] W. Jing, "A Brief Survey on the Security Model of Cloud Computing", Distributed Computing and Applications to Business Engineering and Science (DCABES), IEEE Computer Society, 2010.

[33] P. Jain, "Security Issues and their Solution in Cloud Computing" International Journal of Computing & Business Research, 2012.

[34] K. Cameron, "Identity blog-digital identity, privacy, and the internet's missing identity layer", Available at: www.identityblog.com/?p_1142, 2010.

[35] A. Cavoukian, "Privacy in the clouds", Identity in the Information Society, Vol 1, No 1, 2008, pp. 89-108.