A Model for User Trust in Cloud Computing

Ahmad Rashidi and Naser Movahhedinia

University of Isfahan, Isfahan, Iran

ahd.rashidi@gmail.com
naserm@eng.ui.ac.ir

Abstract

Cloud has proved to be a suitable choice for providing computing and storage resources especially for small and medium sized businesses in recent years. The "pay per usage" cost model, on demand computing, large scale storage resource with easy access, and freeing users from managing and maintaining resources are among the important factors that have made cloud an attractive choice for such services. The issue of low trust on cloud computing is an obstacle, one of the major obstacle to its pervasive deployment, particularly in case of critical data storage on the provider's datacenter. This paper presents a model for trust in cloud computing, accounting for important elements which shape the users trust and a way of evaluating each element's importance.

Keywords

Cloud Computing, Service, Trust, Model.

1. Introduction

Cloud computing is introduced as one of the hottest and most promising issues in Information and Communication Technology (ICT) [1], However, the lack of trust in cloud computing is preventing it from being used widely among users. Having different definitions in computing literature "trust" is considered as followed in this paper: "the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective to the ability to monitor or control that other party" [2]. To employ cloud computing utilities, users have to place their resources (data, applications…) in the cloud provider's datacenter. Since users do not have direct control over their files on cloud provider's datacenter, the trust evaluation would be a critical issue for them. Since possible risks would threaten cloud resources, the need for trust arises as an important factor especially in vital data and transaction processing applications [3]. To address users concerns, cloud providers need to devise mechanisms to eliminate these risks. Elevating the importance of trust, recently "trust as a service" is emerged to cloud business model in which the trust may be offered at different levels with different prices so higher trust level would be achieved at a higher cost [4].

For users to distinct between cloud providers in terms of offered trust, there should be some mechanism to evaluate trust services by independent third parties. In this paper, first the main cloud risks would be recognized and then a model for evaluating user's trust based on these risks and their importance would be devised. In the first section of the paper, some of the works done

DOI : 10.5121/ijccsa.2012.2201

on identifying risks in cloud computing are reviewed. Then in the next section the most important risks from our point of view would be identified and hypothesizes about their importance would be made and a model explaining user's trust in cloud computing would be developed. In the third and forth sections the research methodology would be described and the statistical results would be discussed. Finally, the paper would conclude with a discussion of the managerial and research implications of the studies and directions for future research.

2. Literature Review

When user's critical resources aren't on the user's physical territory, they would have to devise mechanisms for ensuring that resource's security and integrity. When using cloud computing, users are putting their resources on provider's datacenters; hence, providers should implement the security and reliability mechanisms in behalf of the users. Furthermore, cloud computing model brings some new security threats such as resource sharing, fate sharing, and data lock in. These risks, are sources of concern for users and prevent them from using cloud computing. To mitigate these risks providers should identify main user's concerns and try to eliminate these concerns. Recognizing the importance of building users' trust, different researchers proceeded to identify and analyze the elements which are important in cloud computing trust model. Some of the main works in this area are surveyed below.

In [5] the authors introduced security, privacy, accountability, auditability as elements which impact user's trust in cloud computing. In [6] authors discussed security advantages and disadvantages of cloud computing environments. They have recognized investigation, data location, data segregation, long-term viability, compromised servers, regulatory compliance, and recovery as security disadvantages. Cloud Security Alliance (CSA) introduced cloud computing as a most important change in IT and identified ten most important threats against it [7]. These ten threats are abuse and nefarious use, insecure interfaces and APIs, malicious insiders, sharing technology issues, data loss or leakage, account or service hijacking, and unknown risk profile.
In [8], introducing some different models of cloud, concerns about cloud computing are identified by some questions. IDC's corporation website in a survey introduced the main concerns worrying cloud computing users [9].

Gartner Inc. also warned the cloud customer of seven security issues which they should ask before selecting a cloud vendor [10]. These concerns are privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability.

In [11], authors identified Service Level Agreement (SLA) as the only choice where cloud providers can use to make users trust them; hence it's critical to standardize it. In this article, after defining SLA and its content, the security concerns which SLA should contain are recounted similar to [10].

The main service models of cloud computing are introduced in [12] and the authors defined security problem as main obstacle which prevents cloud computing from being used widely. Then, the main security problems for each service model of cloud computing are discussed.

In a technical report containing the Berkeley University's view of cloud computing, availability of service, data lock-In, data confidentiality and auditability, data transfer bottlenecks, performance unpredictability, scalable storage, bugs in large-Scale distributed systems, quickly scaling, reputation fate sharing, and software licensing are stated as the main obstacles against cloud computing adoption.

3. Our Model and Hypothesizes

Considering the concerns reviewed in previous section, the main elements of user's trust in cloud computing are extracted as below:

Data Location: generally cloud user's aren't aware of where the cloud provider store their data and have no physical control over the data [6][10]. Indeed a lot of cloud providers store the data in different countries. So, it's important that the cloud provider considers user's concerns about different jurisdictions and keep the safety and privacy of user's data in behalf of them [10]. With respect to this topic, we made the following hypothesis.

Hypothesis 1: being aware of data location or being confident that the provider will respect their rights in different jurisdictions is positively related to the user's trust in cloud computing.

Investigation: investigating an illegal or inappropriate action is almost impossible in the cloud specially because different user's data are stored in a shared place or a user's data may be stored in different datacenters [11]. So the cloud provider should devise a mechanism which enables users to investigate their data or convince them that this would be done suitably by the cloud provider.

Hypothesis 2: cloud user's ability to investigate their data on provider's datacenter is positively related to user's trust in cloud computing.

Data segregation: user's data in cloud computing commonly would be stored on a shared physical environment. The shared environment is one of user's concerns about cloud computing [6 and 11]. The cloud provider should have an appropriate mechanism to guard user's data in the shared environment. The provider can use data encryption to gain users trust but would encryption be enough for eliminating this concern?

Hypothesis 3: data separation is positively related to user's trust in cloud computing.

Availability: one of most important advantage of cloud computing is it's service availability and user's pervasive and easy access to services and their data. So cloud providers availability is a parameter which if not met would destroy user's trust in cloud computing.

Hypothesis 4: availability is positively related to user's trust in cloud computing.

Long-term viability: often users would need their data to be viable for a long time, so they don't like their cloud provider goes down or any other bad thing happens to it. "Ideally, cloud computing provider should never go broke or get acquired by a larger company. But user must be assured about the data will remain available even after such an event [11]."

Hypothesis 5: long-term viability is positively related to user's trust in cloud computing.

Regulatory compliance: "Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are signaling that customers can only use them for the most trivial functions [6]." Regulatory compliance is a parameter which can ensures users that their cloud providers would act more trustworthy.

Hypothesis 6: provider's regulatory compliance is positively related to user's trust in cloud computing.
Backup and Recovery: user's data may get lost or damaged in case of a disaster. So the cloud provider should devise a mechanism for user's data backup and recovery in case of a disaster which may do harm to user's data.

Hypothesis 8: performing backup and recovery task by cloud provider is positively related to user's trust in cloud computing.

Privileged user access: when user's data are stored in provider's datacenter, the provider's staff would access, manage and maintain this data. So this staff should be trusty. "Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access [11]."

Hypothesis 8: privileged user access is positively related to user's trust in cloud computing.
Regarding this hypothesizes, the trust model in cloud computing can be shown as in Figure 1.

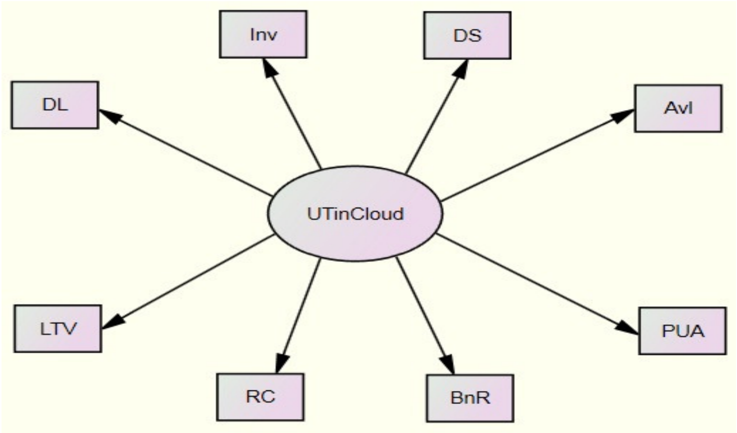

Figure 1: Model of user's trust in Cloud Computing

Table 1 describes the considered variables in our model.

Table 1: Variables Description

Variable	Description
DL	Data Location
Inv	Investigation
DS	Data Segregation
Avl	Availability
PUA	Privileged User Access
BnR	Backup and Recovery
RC	Regulatory Compliance
LTV	Long-Term Viability

4. Data collection, analysis and results

4.1 Data Collection Procedure

A self-administered questionnaire was distributed online to cloud user's groups and communities. The questions are scaled using 7-point Likert scale, from 1= strongly disagree to 7= strongly agree. The questionnaire is listed in Appendix A. To evaluate the extracted parameters 72 pieces of credible questionnaires have been collected.

4.2 Data Analysis

Statistical analyses were performed using SPSS 19 and model testing and fit examined with AMOS 18. AMOS is one of the most widely used Structural Equation Modeling (SEM) techniques in Information Systems.

4.3 The Measurement Model

A composite reliability of 0.70 or above and an average variance extracted of more than 0.50 are deemed acceptable. Table 4 summarizes composite reliability, mean and standard deviation of the measures of this research model.

Table 2: Summary statistics and reliability estimates for the model construct

Items	Mean	Standard Deviation	Composite Reliability
DL	4.7	1.1	0.82
Inv	4.6	0.9	0.71
DS	4.9	0.75	0.75
Avl	5.2	1.1	0.79
LTV	5.2	1.1	0.76
RC	3.9	1.2	0.92
BnR	4.5	1.0	0.79
PUA	4.7	1.0	0.81

4.4 The Structural Model

The model was estimated using maximum likelihood method. Figure 2 depicts model analysis result with AMOS. The statistics in Figure 2 indicate that the research model provides a good fit to the data (Chi-square=27.9, p= 0.1; CFI= 0.95; NFI=0.87; RMSEA=0.07). Table 3 lists the recommended values and this research model's values of various measures of the model.

Table 3: Recommended values of goodness-of-fit measures.

Goodness of Fit measure	Recommended value	Fit indexes In current study
Comparative fit index (CFI)	>= 0.90	0.95
Normed fit index (NFI)	>= 0.90	0.87
Root mean square error of approximation (RMSEA)	<= 0.08	0.07

Table 3 shows acceptable fitness of the introduced model and figure 2 depicts results of AMOS analysis of the model.

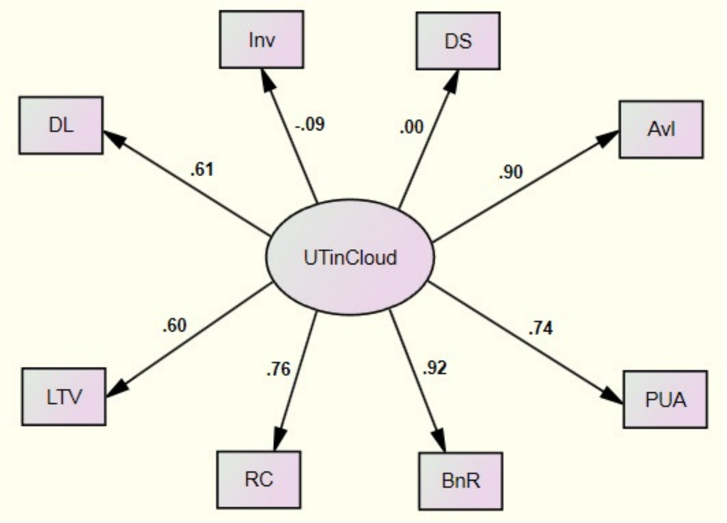

Figure 2: Results of AMOS analysis

As figure 2 shows, backup and recovery (BnR) produces strongest impact (0.91) on user's trust in cloud computing followed by availability (Avl, 0.78), Privileged User Access (PUA, 0.74), Regulatory Compliance (RC, 0.63), Long-Term Viability (LTV, 0.57) and Data Location (DL, 0.56). this survey showed that data segregation (DS) and investigation (Inv) have weak impact on user's trust on cloud computing.

5. Conclusion

Motivated by the need to better understanding the incentives of the user's trust in cloud computing, eight parameters which are believed to be most important have been extracted in this paper. Regarding this elements eight theoretical perspectives of trust have been synthesized and a model for consumer trust in cloud computing is developed. Analyzing this model, the effect of each of these eight elements trust is investigated and described. The outcomes of this paper could be a clue to better recognizing the main parameters affecting users trust and characterizing each parameter's importance.

REFERENCES

[1] Trong Duong Quoc1 , Heiko Perkuhn2, Daniel Catrein2, Uwe Naumann3 and Toni Anwar, (2011) "Optimization and Evaluation of a Multimedia Streaming Service on Hybrid TELCO Cloud", International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.1, No.2, August 2011.

[2] R. C. Mayer, J. H. Davis, and F. D. Schoorman, (1995) "An integrative model of organizational trust", The Academy of Management Review, vol. 20, no. 3, pp. 709–734.

[3] Zainab M. Aljazzaf, Mark Perry, Miriam A. M. Capretz, (2010) "Online Trust: Definition and Principles", 2010 Fifth International Multi-conference on Computing in the Global Information Technology, IEEE.

[4] http://www.opentrust.com/en/saas

[5] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee, (2011) "TrustCloud: A Framework for Accountability and Trust in Cloud Computing", 2nd IEEE Cloud Forum for Practitioners, IEEE.

[6] Amit Sangroya, Saurabh Kumar, Jaideep Dhok, Vasudeva Varma, "Towards Analyzing Data Security Risks in Cloud Computing Environments", International Conference on Information Systems, Technology, and Management (ICISTM 2010), Bangkok, Thailand.

[7] Jerry Archer, Alan Boehme, Dave Cullinane, Paul Kurtz, Nils Puhlmann, Jim Reavis, (2010) "Top Threats to Cloud Computing V1.0" , Cloud Security Alliance (CSA) , March 2010.[8] Michael Gregg et al, "10 Security Concerns for Cloud Computing", (2010) Global Knowledge Training LLC.

[9] http://blogs.idc.com/ie/?p=730, December 15th, 2009, 2011, By Frank Gens.

[10] http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853, July 02 2008, 2010, By Jon Brodkin.

[11] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing, IEEE, 2009.

[12] S. Subashini n, V.Kavitha , " A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Elsevier, 2010.

[13] Michael Armbrust and others, "Above the Clouds: A Berkeley View of Cloud Computing", February 10, 2009, Berkeley university, 2009.

Appendix A. Measures

Data Location (DL)

DL1: It's important for me to know where the cloud provider stores my data.

DL2: The provider would obey local privacy requirements on behalf of me.

DL3: The provider will store my data in jurisdictions which are consistent with my data privacy and security requirements.

Investigation (Inv)

Inv1: It's important to me to be able to investigate my stored data on the cloud.

Inv2: Even if I wouldn't be able to investigate my stored data on the cloud, the cloud provider would investigate my data and don't let malicious operation on my data.

Data segregation (DS)

DS1: I'm worried about my data being stored on a shared environment on the cloud

DS2: The provider would protects my data on the shared environment by encryption

DS3: Encryption would solve data shared environment problems.

Availability (Avl)

Avl1: The provider would have a acceptable availability

Avl2: The provider devises mechanism to keep availability if one server or datacenter went down

Long-term viability (LTV)

LTV1: The cloud provider would have long-term viability
LTV2: If the cloud provider goes broke or get acquired by other company or anything else happens to it, my data will remain available.
LTV3: The cloud provider stores my data in such format that it would be possible to get my data back on my own datacenter or change my cloud provider.

Regulatory compliance (RC)

RC1: There are adequate external audits and security certifications to confirm cloud provider’s qualifications.
RC2: External audits are doing a good job in confirming cloud provider’s qualifications.
RC3: If the cloud provider violates any agreements with me or if it does any illegal thing against my data, there are enough authorities to investigate it.

Backup and Recovery (BnR)

BnR1: The cloud provider devises an adequate mechanism for back up my data.
BnR2: Any incident that led to the loss of my data on the provider’s data center will not happen.
BnR3: If anything goes wrong and my data corrupt on a datacenter, it would be adequate mechanism to recover it from backed up data.

Privileged user access (PUA)

PUA1: The cloud provider hires trusty people for managing and accessing my data.
PUA2: The provider gives adequate teaching to its personnel whom access and manage my data.
PUA3: Provider’s hired personnel who access and manage my data would keep privacy of my data and do no harm to my data.