www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13474-13483

Model for User's Trust in Cloud Service Providers in Cloud Environment

Kavita Rathi, Sudesh Kumari,
Assistant Professor, CSE Department,
Deenbandhu Chhotu Ram University of Science & Technology, Murthal.
Student, M.Tech(CSE),
Deenbandhu Chhotu Ram University of Science & Technology, Murthal.

ABSTRACT- Cloud computing is a current research area that provides elastic and flexible computing resources to best fit the today's business needs. In place of several advantages offered by cloud computing environments, it deals with the major roadblocks in its way of growth. The major roadblocks considered are found as security and secrecy of data along with the trust on cloud service providers (CSP). This paper tries to find out the trust parameters which could help in increasing trust of users on the service providers and helping to encourage the use of cloud computing among users at large. This paper proposes a new user trust model that finds out the trust parameters that make strong impact on users' trust in the cloud environment. The model helps the cloud service users (CSUs) to establish trust in the cloud service providers' (CSPs) for availing their services. Also the CSPs can refer the model to enhance their services for getting more trust among CSUs.

KEYWORDS- Defining trust, trust elements, users' trust model.

I. Introduction

Cloud computing is a new technology that helps in sharing of infrastructure that provides consumers with strong computational capabilities and availability of large memory spaces at very low costs. In comparison to various traditional technologies available, cloud provides consumers with many specific features, like ultra-large-scale and resources belong to each cloud providers are completely distributed, heterogeneous and totally virtualized [1]. Cloud computing provides provisioning of resources by the "pay-as-you-go" economic model [2].

Some Advantages of Cloud Computing:

1. The usage pricing model offers advantages like reduced capital expense, ability to scale up as demand arises [3].
2. Cloud computing can lower IT barriers to innovation, as can be witnessed from the many promising startups, from ubiquitous online applications such as face book and YouTube to the more focused like TripIt (for managing one's travel) or Mint for managing one's personal finances[4].
3. It can provide almost immediate access to hardware resources, with no upfront capital investments for users, leading to a faster time to market in many businesses [4].
4. It makes possible new classes of applications and delivers services that were not possible before [4].

Some Disadvantages of Cloud Computing:

1. Cloud services are often remote, hence they suffer latency and bandwidth related issues associated with any remote application [3].
2. Because hosted cloud services serve multiple customers, various issues related to multiple customers sharing same piece of hardware can arise [3].
3. Since data is accessible to third parties cloud services can present security, compliance, and regulatory issues [3].

The adoption of cloud computing services at large leads to various challenges that act as barrier in the use of these services. Trust and security are found to be the most eminent features in the cloud environment that lead to maximum impact on the consumers in adopting cloud services. Trusted computing is a field of trusted systems where a device is made to behave in a consistent and predictable manner using techniques like cryptography and authentication [4][5][6].

Trust is viewed as a measurable belief that utilizes experience to make trustworthy decisions [6][7]. Trust is considered as an essential substitute for forming security mechanism in distributed computing environments [6][7]. Trust has many security attributes like reliability,

dependability, confidence, belief, competence and suchlike [6][7]. Managing trust is fundamental part in cloud scenarios considering its characteristics such as dynamic in nature, scalability, resource pooling, on demand self service [8]. Distrust of cloud service users (CSUs) on the cloud service providers and vice versa is a major issue of concern in the adoption of cloud computing at large. Trusted cloud computing is seemingly the primary requirement in adopting cloud computing. Since the cloud service providers (CSPs) exist between the CSU and the data centers which provide cloud services, trust among both CSUs and CSPs is a critical factor which can never be ignored.

Trust is a social problem, not a purely technical issue [6][9]. The relationship of trust is established between the two parties which are stated as trustor and trustee. The trustor is the person or entity who holds confidence, belief, reliability, integrity and ability, etc. of another person or thing which is the object of trust, i.e. the trustee [6][10]. This paper proposes a new trust model that helps the CSUs to select the most trustworthy CSP from the available providers based on the various trust parameters that are being provided by the CSPs to the consumers. The rest of the paper is organized as follows. The first part presents the literature review regarding the existing trust models, followed by the parts presenting the proposed model with various trust parameters, then data analysis, results and simulation of the model. The last part is closed with conclusion.

II. Literature Review

Trust is the most complex relationship among entities, because it is subjective and difficult to be evaluated [6][11]. Trust models are considered as a methodology that helps to evaluate trust on the CSP's or the third party distributers that are providing the cloud services. Trust models in cloud computing are very diverse in a way that each model supports different features and evaluates cloud services on the basis of different parameters and requirements [12]. Some of the trust models are surveyed as under.

Rizwana Shaikh and Dr. M. Sasikumar proposed a trust model in which they measured the security strength of a cloud computing service based on trust value. A trust value comprises of various parameters that are necessary dimensions along which security of cloud services can be measured [13]. The trust model focuses on evaluating the trust through security issues in a cloud computing environment. Various security issues are malicious insiders, data leakage, hijacking of services or accounts, issues relating to the shared environment and many other risks.

Significant barriers to cloud adoption are as stated in [14] are found to be security and privacy, connectivity and open access, reliability, interoperability, economic value, changes in IT organization, political issues due to global boundaries. Researchers in [4] present various mechanisms for trust evaluation in cloud environment. It determines reputation, QoS, SLA, Audit, Policy, Attribute certification, Evidence as the basis for trust evaluation in a cloud environment. In [15] the authors define security, accountability, and audit ability as the trust elements which make impact on users' trust in the cloud computing environments. The model proposed in [16] presents various security issues like data security, network security, data locality, integrity, data access, authentication, authorization, web security, backup, data non-readable at CSP and data non-editable by CSP, which if addressed by the CSP brings trust of the CSU in the provider. It proposes a method which helps the CSU to trust the third party providers to adopt the cloud services.

The models in [17], [18] and [19] provide various parameters that are used to identify the trust of the cloud service user (CSU) in the cloud service providers (CSPs). The various parameters identified are Data Location, Investigation, Data Segregation, Availability, Privileged User Access, Backup and Recovery, Regulatory Compliance, Long term viability, and Governance [6]. These are considered as the basic elements of user's trust establishment in cloud services. But these elements are meant only before the user starts using the cloud services. Then the question arises how the user could trust the cloud services after it starts using the services. This question again brings distrust. Trying to answer the question aroused, a trust model that incorporates some new parameters is proposed. This can be used for trust establishment on the CSP by the CSUs.

III. Proposed Trust Model

This model adds a few new trust parameters to the existing model as described in [18] so as to find the answer to the question that what after the services are being availed by the CSUs from the CSPs. If the CSP changes its policies or data locations after the agreements, then will the changes be acceptable to the CSUs and not affect the trust of the consumers? The main trust parameters that are identified are categorized into two parts:

I. Parameters establishing trust before the user starts availing the services of the CSP.

II. Parameters establishing trust after the user starts availing the services of the CSP.

I. Parameters establishing trust before the user starts availing the services of the CSP.

1. Transparency in Communication: It is believed that there must be a face that represents the services. If the communication for agreements and query for services by the user can be solved through transparent modes of communication like video conferencing and the cloud service providers represent a person or group of persons that are representing their firm and services. This is believed to bring confidence in the user for using the cloud services.

Hypothesis 1: Direct and transparent communication to the CSP relates directly to the CSUs' trust in the CSPs.

2. Providing Information about Location of Data: As explained in [18], data location deals with providing the full information about the data, where and how it is stored to which jurisdictional areas it follows and where it can be shared. It is also ensured by the CSP that the data is secure in the respective jurisdictions and full privacy of the data is maintained. From the fulfillment of this parameter, the following hypothesis can be derived.

Hypothesis 2: It is concluded that the information so provided regarding the data will bring confidence and trust in the users towards the services of the CSPs.

3. Data Safety through Investigation: Investigation refers to the handling of user queries regarding the data and assuring the user about the safety of their data in a shared environment. CSP must take the responsibility of any illegal or unauthorized action towards the users' data.

Hypothesis 3: If users' are allowed to investigate their data on data center of the CSP then it can be positively related to users' trust.

4. Distribution of Data: In a cloud computing environment, data is shared and stored across boundaries. This distribution of sharing the data must be regarding the users' concerns [20] and the CSP must have the proper mechanisms of encrypting the data to maintain the security of the data.

Hypothesis 4: Data distribution is directly related to the users' trust in the CSPs'.

5. Accessibility: It is the parameter which is of major importance for CSUs' in the cloud environment. For the pervasiveness of the services and access to data whenever required, it is important that the provider does not go down and user can get access to the resources and services anytime the user wants.

Hypothesis 5: All time availability and access to the services and resources is directly related to the trust of the CSUs'.

6. Assigning Data Access Privileges to Data Center Employees' of CSP: All the CSU data is stored on the data center of the CSP. This is the reason why the CSP must have a trustworthy criterion of selecting the employees' of the data center who will deal with all the data. The employees' of the CSP have full access to the data for maintaining and managing the data, hence they must be assigned with access privileges based on their work access to the data.

Hypothesis 6: This parameter is also directly related to the users' trust in the CSPs.

7. Having effective backup and recovery mechanisms: CSP must ensure the user of having the most effective mechanisms to recover their data in case of any incident of disaster or damage to the data due to any other cause. Also proper backup plans for the data must exist at the providers' end.

Hypothesis 7: Providing effective backup and recovery for users' data directly relates to the trust of the CSU.

8. Compliance to Audits and Certifications: The CSP must have a history of undergoing the audits and certifications by the government officials on regularly basis for the authenticity of their services and resource availabilities. If any provider is ignoring or avoiding the audits and certifications, then it is assessed that it is not very trustworthy. If regular audits are being made then it means that the CSP have a feature that it will ensure to give healthy environment for the sharing and use of shared resources across multiple boundaries.

Hypothesis 8: Compliance to audits and certifications of the CSP is directly related to the trust of the CSUs'.

9. Workability for Long: This parameter deals with the fact that the services of the CSP are available to the CSUs' even in the non- working hours. Also if the CSP is taken over by any other organization or CSP, then it must ensure its users that they have access to their data without any restriction or problem.

Hypothesis 9: This parameter related to the trust of the CSUs' directly.

II. Parameters establishing trust after the user starts availing the services of the CSP.

10. User acceptance to timely changes/ updates: The cloud user must be informed to any changes to the CSP data center regarding the change of policies or storage of data. If any changes or updations are being made to the jurisdictional area of the CSP then it must have the acceptance of the user before sharing the cloud user data to that area. The data is very critical for the user and its work hence it must be kept in an area where the user wants it to and all the related information must be shared to the user on regular basis. If the CSP fails to do the same and any harm is found by the CSU to their data in any situation makes a heavy loss to the trustworthiness of the CSP in the cloud computing environment.

Hypothesis 10: User involvement in the tasks that could affect the CSU data directly relates to the trust of the CSUs' in the services of the CSP.

Figure 1 represents the trust model that provides ten most important parameters which are directly related in building trust of the CSUs in the CSPs in the cloud computing environment. The CSPs can also refer to the trust model to enhance their services for the users by gaining more trust and confidence by the users in their services.

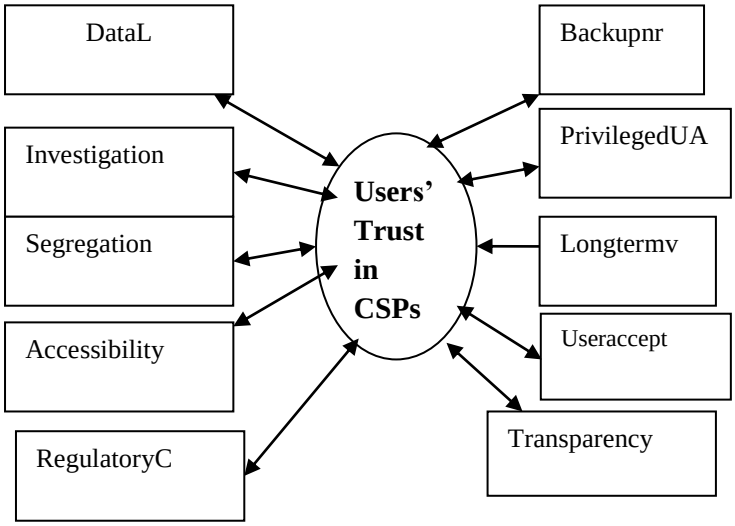

Figure 1. Model for Users' Trust in Cloud Service Providers

Table 1 gives the description of the parameters used in the model.

Sl No.	Name	
1.	Transparency	Transparency in Communication
2.	Datal	Providing Information about Location of Data
3.	Investigation	Data Safety through Investigation
4.	Segregation	Distribution of Data
5.	Accessibility	Accessibility
6.	PrivilegedUA	Assigning Data Access Privileges to Data Center Users' of CSP
7.	Backupnr	Having effective backup and recovery mechanisms
8.	RegulatoryC	Compliance to Audits and Certifications
9.	Longtermv	Workability for Long
10.	Useraccept	User acceptance to timely changes/ updates

3.1. Procedure to check the fitness of the model and to select the most trustworthy cloud service provider based on the parameters used in the model to measure trust.

The steps followed in the proceedings of the proposed model are as given under:-

Step 1: Create a self administered questionnaire based on 7 point Likert scale that takes the views of the cloud users about the various trust parameters.

Step 2: Extract the data from the questionnaires and make a data file with all the values.

Step 3: Analyze the data using MS Excel 2007 and IBM SPSS AMOS 22 and check for the fitness of the model against statistical and structural measures.

Step 4: Summarize the data analysis results and extract the path coefficient values for the trust parameters. The values represent the trustworthiness of the providers' based on the fact that the CSP provides those parameters which have higher values.

Step 5: Select the most trustworthy CSP from a given set of providers by using a program module.

5.1. Algorithm for selecting the most trustworthy cloud service provider

Start

1. Define the limits for m=10 features for different cloud service providers (represented as servers in the program module).

1.1. limits= path coefficient values from AMOS path analysis for features (trust parameters)

2. Accept N [illegible] cept K

3. for i=1 to K

{

[Process all users]

if (requirement(User(i), Feature<limit(Feature))

{ Print "Not Acceptable"

}

else

{ Print "Acceptable"

}

}

5. for i=1 to N

{

[Process all servers]

if (High(Server(i), Feature)=High(limit(Feature)))

{ server(count)=server(count)+1;

}

} return server(count)

End

Step 6: Implement the algorithm of finding the most trustworthy CSP based on the requirements of the CSUs' using MATLAB 2009.

Step 7: Display the results.

IV. Data Collection, Analysis and Results

4.1. Data Collection

Data is collected with the use of a self-administered questionnaire approved by the guide. It was distributed to users of six IT companies in India using cloud services as private/ public. The questions are scaled using 7-point Likert scales, ranging from 1 for strongly agree to 7 for strongly disagree. 75 pieces of the questionnaires have been collected to evaluate the proposed parameters. The questionnaire is listed in Appendix 1 of this paper.

4.2. Data Analysis and Measurements

Statistical analysis is made using MS- Excel 2007 and the model fit testing is performed by using IBM SPSS AMOS Version 22. AMOS 22 is widely used for performing model fit testing for SEM (structural equation modeling) for analyzing data of survey for models.

4.2.1. Statistical Analysis

Table 2 provides a summary of the measurement model for the proposed model.

Sl. No.	Parameter Name	Mean	Standard Deviation	Composite Reliability
1.	Transparency	1.36	0.54	0.90
2.	Datal	1.87	0.62	0.82
3.	Investigation	2.73	0.92	0.72
4.	Segregation	2.92	0.88	0.70
5.	Accessibility	1.67	0.58	0.89
6.	PrivilegedUA	2.01	0.63	0.79
7.	Backupnr	1.68	0.68	0.90
8.	RegulatoryC	2.02	0.63	0.82
9.	Longtermv	3.14	1.16	0.76
10.	Useraccept	1.17	0.45	0.90

- A smaller standard deviation (SD) represents that data where results are very close in value to the mean. A smaller value of SD represents a lesser variance in the results. A variation of +-2SD from the mean is an acceptable limit to represent that the measurements are closer to the true value [21].
- The value of 0.7 or above is an acceptable limit for composite reliability and a variance in the values of composite reliability, greater than 0.50 indicates an acceptable reliability for the proposed model [22].

4.2.2. Structural Analysis

The model fit testing is done with the help of AMOS 22 by using the maximum likelihood method. The model fit summary results are stated in table 3. This table represents the values of various measures for the proposed model along with the recommended values that are acceptable for the measures. Figure 3 and Figure 4 represent the path analysis result for the model. Figure 5 and Figure 6 represent the model fit summary from the path analysis used for structural equation modeling of the data for the proposed model.

Table 3. Model fit summary along with the recommended values for the goodness-of-fit measures for a model.

Goodness-of-fit Measures	Recommended Values	Values for Measures for the proposed model
Comparative fit Index (CFI)	Between 0 and 1	0.635
Normed fit Index (NFI)	>=0.90	0.912
Root Mean Square Error of approximation (RMSEA)	<=0.08	0.040

The values found for the measures of CFI, NFI, RMSEA for the proposed model are close to the recommended values and the values are found to be acceptable. Hence the data provides a good fit to the model and proposed model is found to be good fit.

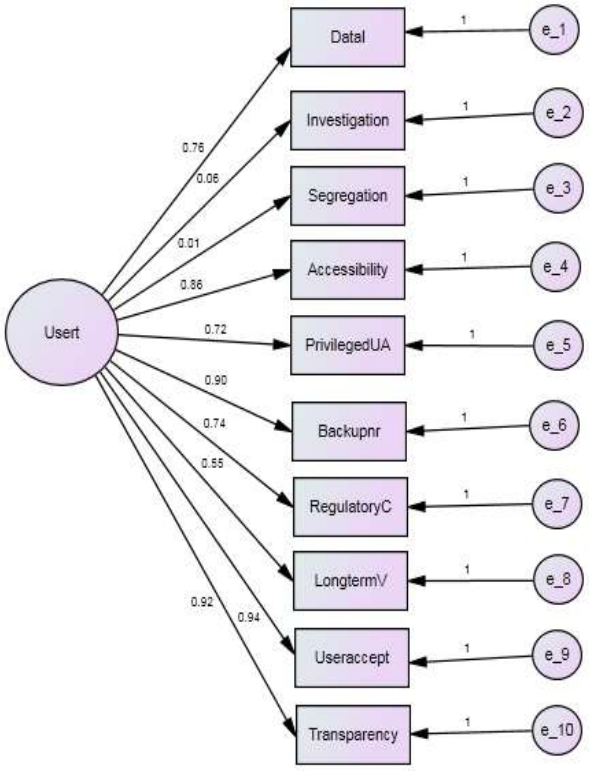

Figure 3. Path analysis diagram for the trust model.

The variables e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9 and e_10 in the path analysis diagram represent the measurement errors in the analysis of the data supporting the model. The error value for the proposed model is 1 which is an acceptable limit for the model fitness.

Baseline Comparisons

Model	NFI Delta 1	RFI rho 1	IFI Delta 2	TLI rho 2	CFI
Default model	.513	.373	.666	.531	.635
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

Figure 4. Model Fit Summary

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.123	.83	.209	.000
Independence model	.179	.148	.211	.000

Figure 5. Model Fit Summary

Table 4 represents the regression weight estimates for the trust parameters of the model from the path analysis stated in Figure 3.

Parameters			Estimate	S.E.	C.R.	P	Label
Datal	<---	User	.760				
Investigation	<---	User	.060				
Segregation	<---	User	.010				
Accessibility	<---	User	.860				
PrivilegedUA	<---	User	.720				
Backupnr	<---	User	.900				
RegulatoryC	<---	User	.740				
LongtermV	<---	User	.550				
Useracceptt	<---	User	.940				
Transparency	<---	User	.920				

From table 4 stated above, it can be concluded that the service providers providing the parameters of user acceptance to timely changes/updates, transparency in communication, backup and recovery, and data location makes strongest impact on users' trust with data segregation and investigation making least impact.

Based on the values of the regression weight estimates for all the parameters, it can be concluded that the providers providing the services with an estimate value more than 0.74 are considered to be most trustworthy. For representing this fact, an algorithm representing the best providers from the given number of providers is proposed in the next section of the paper.

4.3. Selecting the Most Trustworthy Cloud Service Provider

4.3.1. Experimental Setup

The algorithm for selecting the best cloud service provider from the given set of providers is implemented by the use of MATLAB and results are plotted as graphs. For this experimental setup, the system requirements used are Windows 7Ultimate operating system, Intel core i3 processor with MATLAB 2009, win 32, version 7.8.0.387, 4 GB RAM for implementing the algorithm for selecting the most trustworthy cloud service providers from the available set of CSPs and displaying the results.

4.3.2. Results

The results are based on the requirements of 10 users and availabilities of the services provided by 10 cloud service providers. The values provided by the CSPs are mapped with the requirement values for each parameter of the user and then checked with the limit value required for the trustworthiness for the mentioned parameters of the services provided by the CSPs. The cloud service provider that is found to provide the maximum number of trust parameters with the limit value of more than 0.7 is considered to be the most trustworthy CSP.

Table 5 represents the parameter values for the ten parameters used in the model provided by 10 cloud service providers. The values mean the level of parameters that the services provided by the CSP fulfill.

Parameter No / Provider No	P1	P2 ↓	P3	P4	P5	P6	P7	P8	P9	P10
S1	0.8147	0.1576	0.6557	0.7060	0.4387	0.2760	0.7513	0.8407	0.3517	0.0759
S2	0.9058	0.9706	0.0357	0.0318	0.3816	0.6797	0.2551	0.2543	0.8308	0.0540
S3	0.1270	0.9572	0.8491	0.2769	0.7655	0.6551	0.5060	0.8143	0.5853	0.5308
S4	0.9134	0.4854	0.9340	0.0462	0.7952	0.1626	0.6991	0.2435	0.5497	0.7792
S5	0.6324	0.8003	0.6787	0.0971	0.1869	0.1190	0.8909	0.9293	0.9172	0.9340
S6	0.0975	0.1419	0.7577	0.8235	0.4898	0.4984	0.9593	0.3500	0.2858	0.1299
S7	0.2785	0.4218	0.7431	0.6948	0.4456	0.9597	0.5472	0.1966	0.7572	0.5688
S8	0.5469	0.9157	0.3922	0.3171	0.6463	0.3404	0.1386	0.2511	0.7537	0.4694
S9	0.9575	0.7922	0.6555	0.9502	0.7094	0.5853	0.1493	0.6160	0.3804	0.0119
S10	0.9649	0.9595	0.1712	0.0344	0.7547	0.2238	0.2575	0.4733	0.5678	0.3371

The graph in figure 6 represent the parameter values for the services provided by the cloud service provider named as S1 in the table 5. The red dots in the graphs in figures 6 and 7 represent the threshold values of the parameters that are found to be suitable for the mentioned parameters. If a provider provides the threshold value for the parameters as required by the user then it is considered to be trustworthy. These values are mapped with the user requirements as shown in table 6 and the graph in figure 7, to find the most trustworthy service provider of the given list of providers.

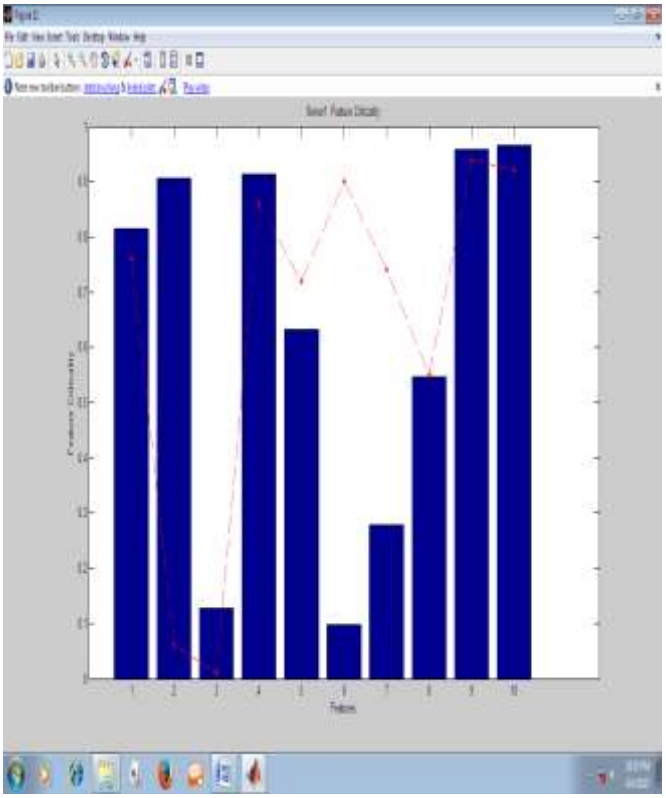

Figure 6: Representing the values of the parameters provided by the cloud service provider S1.

Table 6 represents the requirements of each parameter required by 10 users.

Parameter No / User No	P1	P2 ↓	P3	P4	P5	P6	P7	P8	P9	P10
U1	0.1622	0.4505	0.1067	0.4314	0.8530	0.4173	0.7803	0.2348	0.5470	0.9294
U2	0.7943	0.0838	0.9619	0.9106	0.6221	0.0497	0.3897	0.3532	0.2963	0.7757
U3	0.3112	0.2290	0.0046	0.1818	0.3510	0.9027	0.2417	0.8212	0.7447	0.4868
U4	0.5285	0.9133	0.7749	0.2638	0.5132	0.9448	0.4039	0.0154	0.1890	0.4359
U5	0.1656	0.1524	0.8173	0.1455	0.4018	0.4909	0.0965	0.0430	0.6868	0.4468
U6	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.

	60	82	86	13	07	48	13	16	18	30
	20	58	87	61	60	93	20	90	35	63
	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
	26	53	08	86	23	33	94	64	36	50
	30	83	44	93	99	77	21	91	85	85
	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
	65	99	39	57	12	90	95	73	62	51
	41	61	98	97	33	01	61	17	56	08
	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
	68	07	25	54	18	36	57	64	78	81
	92	82	99	99	39	92	52	77	02	76
	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
	74	44	80	14	24	11	05	45	08	79
	82	27	01	50	00	12	98	09	11	48

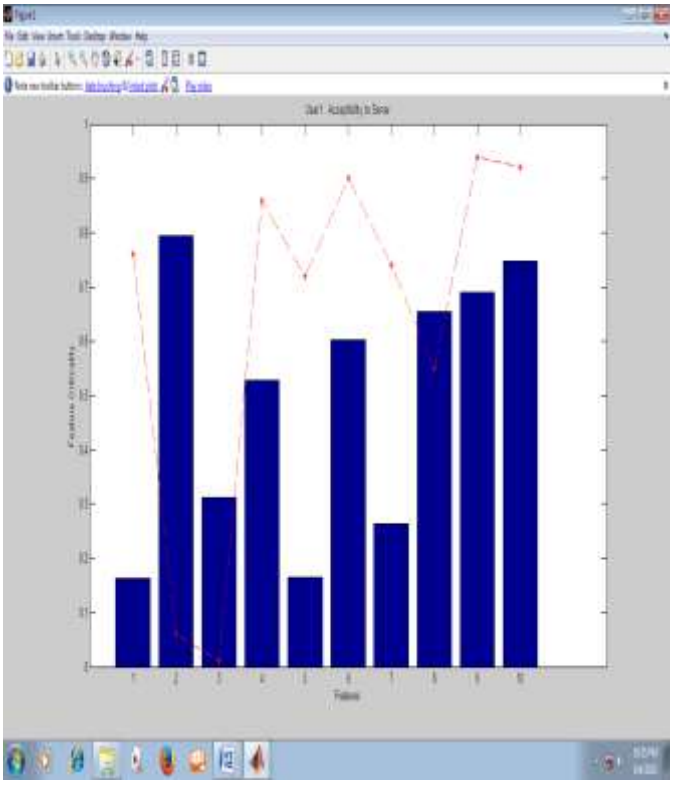

Figure 7: Representing the values of the parameters required by the cloud service user U1.

The graph below represents the most trustworthy cloud service provider for the asked service requirements supported by maximum number of users.

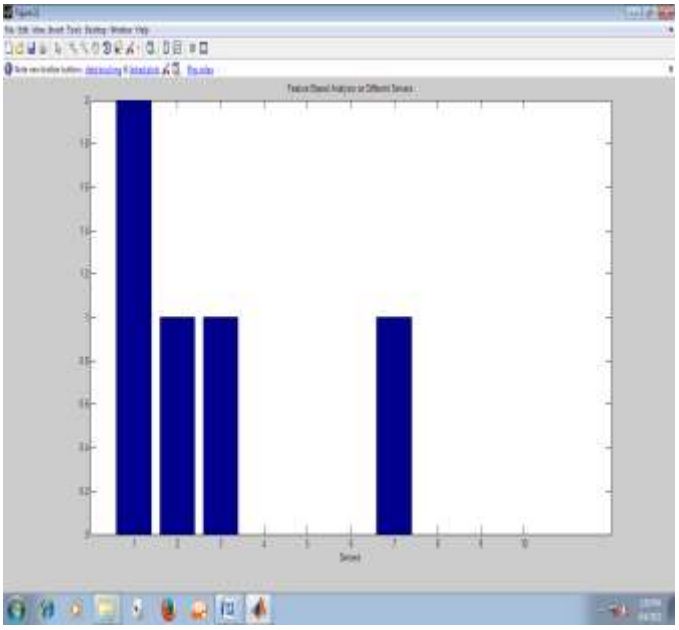

Figure 8 shows that the cloud service provider S1 is found to be most trustworthy among majority of users.

V. Conclusion and Future Work

In the cloud computing environment, security and trust are considered to be the most important aspects in promoting and expansion of cloud services at large. This paper focuses on trust and a new trust model is proposed. The most important trust parameters are extracted and surveyed among the cloud users for establishment of trust in the CSPs by the CSUs. Ten important trust parameters are stated and the model is described and analyzed. The results of the data analysis are used as a basis to select the most trustworthy CSP from a given set of providers. The results lead to the establishment of trust in the cloud service users for the service providers. The model can also be referred by the service providers to enhance their services and achieve trust among CSUs for increasing the adoption of cloud services at a large scale. The algorithm for selecting the most trustworthy cloud service provider can be improved in its functionality by making it more flexible and introduction of user interface to give the inputs as required in place of the system generated values.

REFERENCES

[1] Ali. Mohsenzadeh, "Trust Model to Enhance Security of Cloud Computing", Journal of mathematics and Computer science, page 315-325, January 16, 2015.

[2] Marios D. Dikaiakos and George Pallis, et al., "Cloud Computing Distributed Internet Computing for IT and Scientific Research", IEEE Internet Computing, 2009.

[3] Robert L. Grossman, "The Case of Cloud Computing", IT Pro, Published by IEEE Society, 2009.

[4] Maricela-Georgiana Avram(Olaru), "Advantages and Challenges of adopting Cloud Computing from an enterprise perspective", The 7th International Conference Interdisciplinarity in Engineering, Procedia Technology 12, Page. 529-534, 2013.

[5] Kavita Rathi, Sudesh Kumari, "A Survey on Trust in Cloud Computing", International Journal of Engineering Technology, Management and Applied Sciences, Volume 3 Issue 1, ISSN 2349-4476, January 2015.

[6] Kavita Rathi, Sudesh Kumari, "Analyzing and Surveying Trust In Cloud Computing Environment", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. 1 (May – Jun. 2015), PP 66-70.

[7] M. Makay, T. Baker, A. Al-Yasiri, "Security-Oriented cloud computing platform for Critical infrastructures", SciVerse ScienceDirect, Computer Law and Security Review, 2012.

[8] Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", Advanced in Control Engineering and Information Science, Procedia Engineering 15, page. 2852-2856, 2011.

[9] Chaitali Uikey, Dr. D. S. Bhilare, "A Broker Based Trust Model for Cloud Computing Environment", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 11, November 2013.

[10] Kai Hwang, Deyi Li, "Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE Internet Computing, 2010.

[11] Yashashree Bendale, Seema Shah, "Feasibility of User Level Trust in Cloud Computing", UACEE International Journal of Computer Science and its Applications, vol.2 : issue2[ISSN 2250-3765], 2013.

[12] Qiang Guo, Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, "Modeling and Evaluation of Trust in Cloud Computing Environments", 3rd International Conference on Advanced Computer Control (ICACC), 2011.

[13] Xiaoyong Li, Junping Du, "Adaptive and Attribute based Trust model for service-level agreement guarantee in cloud computing", IET Information Security, 2012.

[14] Rizwana Shaikha, Dr. M. Sasikumarb, "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) 380 – 389, Published by Elsevier B.V., 2015.

[15] Jingwei Huang and David M.Nicol, "Trust Mechanisms in cloud computing", Journal of Cloud Computing: Advances, Systems and Applications, a Springer Open Journal, 2013.

[16] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing", 2nd IEEE Cloud Forum for Practitioners (IEEE ICFP 2011), Washington DC, USA, July 7-8, 2011.

[17] Shakeel Ahmad, Basir Ahmad, Sheikh Muhammad Saqib and Rashid Muhammad Khattak, "Trust Model: Cloud's Provider and Cloud's User", International Journal of Advanced Science and Technology, Vol. 44, July 2012.

[18] Ahmad Rashidi and Naser Movahhedinia, "A Model for User Trust in Cloud Computing", International Journal on Cloud Computing: Services and Architecture(IJCCSA), Vol.2, No.2, April 2012.

[19] EY Building trust in the Cloud, Insights on governance, risk and compliance, June 2014.

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

[21] www.medialabinc.net/spg49741/acceptable_standard_deviation_sd.aspx, June 3, 2015.

[22] https://books.google.co.in/books?id=4e-nbzuL8L8C&pg=PA100&lpg=PA100/McGill,Klobas&Hobbs, June 3, 2015.

Appendix 1. Measures used in the Questionnaire

1. Transparency in Communication: It is believed that a face must represent any communication. If the communication for agreements and query for services by the user can be solved through transparent modes of communication like video conferencing and the cloud service providers represent a person or group of persons that are representing their firm and services. This is believed to bring confidence in the user for using the cloud services.

2. Providing Information about Location of Data (Data Location): It allows the users to know where their data is stored and legal as well as the privacy requirements will be considered and obeyed regarding the data.

3. Data Safety through Investigation (Investigation): It allows users to check the consistency of their data stored on the cloud. In case the cloud user is not able to investigate its data it is the responsibility of the cloud service provider (CSP) to do the same.

4. Distribution of Data (Data Segregation): It provides information to the cloud user regarding the encryption techniques required to guard the data in a shared environment that are being used by the cloud service provider.

5. Accessibility (Availability): The CSP have proper mechanisms to ensure the availability of data to the cloud user whenever required.

6. Assigning Data Access Privileges to Data Center Employees' of CSP (Privileged User Access): The personnel hired must be trustworthy and there must be regular monitoring of the employees to judge that they are not doing any harm to the data. There must be a secure mechanism to distribute their access permissions.

7. Having effective backup and recovery mechanism (Backup and Recovery): In case of any incident that leads to the loss of data, the CSP must have proper backup and recovery techniques to retrieve back cloud users' data from any losses. There must be transparency in the selection of plans devised to deal with the incidents. The CSP must provide information to the user for any changes to the jurisdictional changes and update contacts of lawful authorities.

8. Compliance to Audits and Certifications (Regulatory Compliance): The CSP must inform the user for the external audits and security certifications to ensure that it is qualified to meet the standards and also if it does anything wrong to the cloud user data then there are enough authorities to investigate the matter and take necessary action.

9. Workability for long (Long term viability): The data must be stored in such a way that the user can get back the data on its own data center and can change its CSP. The data must be available to the cloud user in case of any break down on the CSP side or it gets acquired by other firm/company.

10. User acceptance to timely changes /updates to data location and policies: The cloud user must be informed to any changes to the CSP data center regarding the change of policies or storage of data. If any changes/ updation had been made to the jurisdictional area of the CSP then it must have the acceptance of the user before sharing the cloud user data to that area.