International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June-2018 www.irjet.net p-ISSN: 2395-0072

Survey on Trust Management and Consumer Trust in Cloud Environment

M. Shanmukha Satya Narayana[1], Dr. L. Venkateswara Reddy[2]

[1]Student, Dept. of Information Technology, Sree Vidyanikethan Engineering College, Tirupati-517102, AP, India.
[2]Professor, Dept. of Information Technology, Sree Vidyanikethan Engineering College, Tirupati-517102, AP, India.

Abstract - *Cloud computing is a developing innovation. Every single association required to interface with the distributed computing condition. A couple of associations deny interfacing because of the trust administration and security issues. Many security factors had been raised. Few of them are the third party auditor which used for solving security issues.*

Another critical factor will be factor is trust on the cloud specialist co-op's i.e., at up to certain level would organization be able to confide in the cloud specialist organization for dealing with the endeavor's information. It speaks to the current work on reliability which is characterized as a level of satisfaction of a CSP's (Cloud Service Provider's) to the guaranteed QoS parameters as characterized in SLA.

Keywords:Cloud computing, Trust, Trustworthiness, SLA, Cloud service provider, Quality Of Service.

1. INTRODUCTION

Cloud computing is the growing technology. It gives on request administrations to client and furthermore gives access to the common assets.

The cloud model comprises of 5 fundamental attributes, 4 sending models and 3 administrations, for example, IaaS, PaaS, SaaS as appeared in Figure1. These can be deployed in different levels like community, hybrid, private and public clouds.

As the quick development in innovation and administrations the new security issues emerges. The information which put away on cloud is kept up at different physical machines which are obscure to the cloud clients. Along these lines their information is in danger measures should be taken to ensure client's information. We additionally utilize the outsider examining for information assurance.

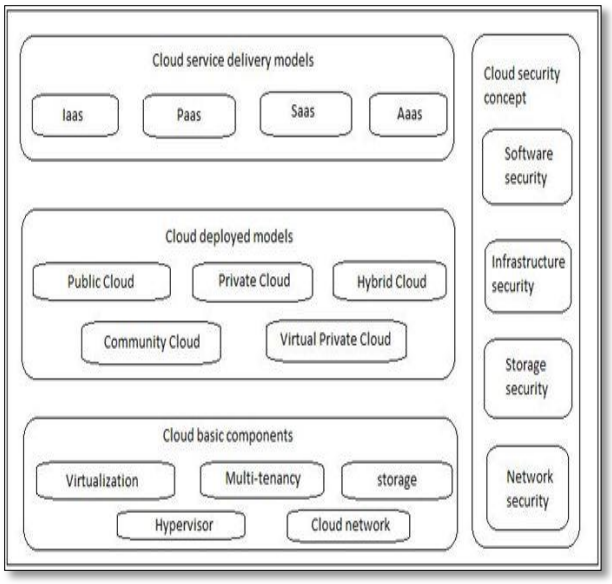

Fig1. Cloud computing Model.

As there is rapid expanding and man vendors are coming with more and similar functionalities. The clients are concerned with their information stockpiling area and by whom their information can be gotten to. They can't without much of a stretch trust the cloud specialist co-op so in this manner the trust administration is the critical variables which emerge in this situation.

Concept of Trust: Trust may speak to various things to various individuals which defines in different domains like law, psychology, philosophy, economics, computing….etc and trust may represent distinctive things to various people and can vary from person to person, system to system.

The same number of terms is utilized with marginally unique implications in the writing, first we define those used here to avoid ambiguity.

Trust Factors (TFs) are criteria and considered when evaluating trust in CSPs. Examples of high-level trust factors can be security, privacy, and data management.

Trust Indicators (TIs) are ways of representing trust factors. For instance, score (e.g. 95 percent), or rating are

trust indicators used for representing the trust factor reputation. The leaf/Service Level Objects (SLO).

Trustor: A trustor is an agent that trusts another entity. In our framework, a trustor is spoken to by a consumer. Inside the setting of this assessment we additionally allude to the trustor as client.

Trustee: A trustee is an element that the trustor trusts. In our model CSP's represent the trustee entity.

Trustworthiness: Trustworthiness is the arrangement of all relevant trust factors.

2. CHALLENGES AND EXISTING SOLUTIONS

In this we talk about the challenges related to trust between consumers or users and CSP's. It represents a comparative overall view of existing models or frameworks that assess the dependability of CSP's. It ended with open problems and potential values for consideration in future.

Based on the several issues on trust frameworks the comparison is done using five criteria which brings aspects of service providers and consumers together, and give a far reaching picture in a flexible manner.

Deutsch[1] characterized trust as "certainty that an individual will discover, what is wanted from another instead of what is dreaded ".

Diego Gambetta[2] characterized trust as "a specific level of the subjective likelihood with which specialist surveys that another operator or gathering of specialists will play out a specific activity, both before that which can screen such activity and in a setting in which it influences his own particular activity".

Gradison[3] characterized Trust as "the firm confidence in the fitness of an element to act constantly, safely and dependably with in specified context".

The concept of trust has been linked to the compliance provided by CSP's as according to set SLA(Service Level Agreement).An SLA is a formal contract signed between the CSP (Cloud Service Provider) and CC (Cloud Client). Client idea of trust is the trust framework enables customers to express their preferences towards some trust factors.

The trust factor comes while assessing the trust in CSP's. The common trust factors are data management, privacy and security.

Those trust factors is further divided into 1. SLA Trust Factors and 2. Non-SLA Trust Factors to assess the trust, SLA trust factors are collected from SLA's and Non-SLA trust factors are collected from the other sources shown in figure2.

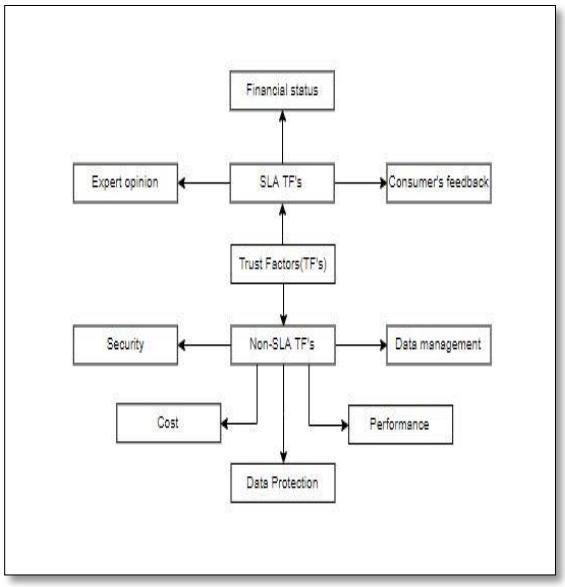

Fig2. Classification of trust factors.

Previously before the cloud computing there exists a Grid computing and trust is build by the inter cloud computing infrastructure figure4. The exits a reputation system for the grid management system which has number of attacks and issues that make weaken of trust management system, by the distributed computing trust administration framework and improves the reliability.

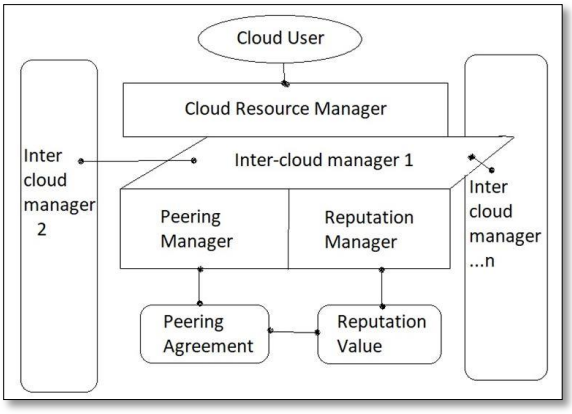

Fig3. Inter Cloud Computing Interface.

S.Chkraborty, K.Roy [4] prescribed a framework i.e., inter cloud computing and to implement they used update reputation algorithm for updating records. It

processes the G_i belongs to N experiences the interaction with that G_i belongs to N or it receives second hand rating from G_k belongs to N about G_j belongs to N after certain period is considered. The reputation manager captures and efficiently stores the conduct of other entities in the previous interactions. It is reliable as it helps clouds to define themselves from the malicious information. Trustworthiness is calculated by consumer's with reference through consumer's (x) trust on a CSP (y) can be expressed as

$$xTy = \sum_{i=1}^{k} Wi * \left(\frac{Pi}{\sum_{i=1}^{k} Pi}\right) \quad (1)$$

Here we assume the consumer x's trust on y is based on k parameters where i^{th} parameter has a value P_i and W_i is the weight assigned to it.

Runlian Zhang, Bing Zeng [5] presents the trust assessment demonstrate in view of the confirmation hypothesis and sliding window component for distributed computing which is easy to execute and the time intricacy is O(m*n) i.e., n CSP's and m CU's in the framework.

It is used to identify the malicious simulation experiments which the level of substances and provides the reliable information. The above architecture highlights only two components i.e., parameter extractor and trust calculator, it isn't certain that on what premise the parameters are separated and how weights are assigned. The Dempster-Shafer evidence mechanism theory is used to remove conflicts between evidences and the interactions among providers and users w.r.to time are examined in detail by sliding window mechanism [5].

Even though author showed the mathematical model and highlighted the experimental results the real disadvantage of this model is subjective in nature and the validation of this model is difficult as the objective model builds on the QoS parameters are more accurate.

WenJuan Fan and Harry Perros [6] has mentioned trust administration in multi-cloud situations using trust management architecture shown in figure, in view of the gathering of dispersed TSP's (Trust Service Providers) which are free third-party suppliers, trusted by CP's (Cloud Providers), CSP's (Cloud Service Providers) and CSU's (Cloud Service Users). The TSP's are conveyed over clouds and they collect raw trust prove from various sources in various configurations.

W.Fan and S. Yang [7,8] discussed about the assessment issue as a multi-property basic leadership issue and a fluffy hole estimation in view of trust assessment system has been proposed which makes utilization of evidential thinking approach. As indicated by creator observation the trust related confirmations can be gotten from numerous sources. The fluffy hole assessment way to deal with decide the dependability of a cloud benefit. In these three sorts of holes are produced i.e., perception-importance, delivery-importance and perception-delivery.

Experiments have conducted considering fifteen attribute system and results shows that approach helps cloud vendors to evaluate trust. The practical adoption of this author presented model is difficult as it involves users and experts to show the reliability of each attribute and gaps are identified [7, 8]. This entire process puts burden on users and experts as this process is subjective also makes the usage of this model in real dynamic cloud environments is very difficult.

Farang Azzedin, M Maheswaran and A Mitra [9] have illustrated the trust brokering mechanism which operates in a peer-to-peer manner. The mechanism is used in public-resource grid systems. The main benefits of the work is it separately models the accuracy and the honesty concepts, at which these two concepts able to improve the performance.

In this model the author applied trust expediting framework to an asset director to portray its utility in an open asset matrix condition. As the no. of dishonest domains increases this model becomes slow in reaching level of capability.

Sarbjeet Singh and Jagpreet Sidhu [10] addresses the major issue of deciding the dependability of CSP's in a cloud computing, because of expansive number of CSP's offering comparative sorts of administrations in the cloud and it became the testing undertaking for Cloud Clients (CC's) to identify the separate between trustworthiness and untrustworthiness CSP's. The author proposed CMTES (Compliance-based Multi-dimensional Trust Evaluation System) that empowers CC's to decide the dependability of CSP from different points of view. The CMTES system [10] empowers customers to assess the reliability of CSP from CC's point of view, Cloud Auditor's Perspective, Cloud Broker's viewpoint and Peer's perspective.

The evaluation of this framework is finished with the assistance of manufactured information and its appropriateness has shown using the real cloud data. The major problem in this perspective is lack of trust on CSP's need to address on priority basis.

3. CONCLUSION

The hype of cloud model is changing the IT industry; it brings many benefits in several aspects. Even though

having several advantages, the cloud still has many security challenges. This is why security is the major challenge in the rental of the cloud. The consumers and providers are well known of these security threats.

The above survey attempted to show various security challenges in cloud computing, these cloud security issues arise from different characteristics of the cloud like public nature of cloud, sharing of resources…etc. In future, governments also planning to develop the cloud techno to improve the performance, quality and security in the services which they provide to people.

REFERENCES

[1] M. Deutch, cooperation and trust: some theoretical notes, in :Nebraska symposium on motivation, Nebraska university Press, 1962.

[2] A.Chakrabarti, Grid Computing Security, Springer, Berlin, Heidelberg, 2007.

[3] T.W. Grandison, Trust management for Internet applications (Doctoral Dissertation), Imperial College of Science, Technology and Medicine, University of London, 2003.

[4] S. Chakraborty, K. Roy, An SLA-based framework for estimating trustworthiness of a cloud, in: Proceedings of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 937–942.

[5] X. Wu, R. Zhang, B. Zeng, S. Zhou, A trust evaluation model for cloud computing, Procedia Comput. Sci. 17 (2013) 1170–1177.

[6] W. Fan, H. Perros, A novel trust management framework for multi-cloud environments based on trust service providers, Knowl.-Based Syst. 70 (2014) 392–406.

[7] W. Fan, S. Yang, J. Pei, A novel two−stage model for cloud service trustworthiness evaluation, Expert Syst. 31 (2) (2014) 136–153.

[8] W.J. Fan, S.L. Yang, H. Perros, J. Pei, A multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning approach, Int. J. Autom. Comput. 12 (2) (2015) 208–219.

[9] F. Azzedin, M. Maheswaran, A. Mitra, Trust brokering and its use for resource matchmaking in public-resource grids, J. Grid Comput. 4 (3) (2006) 247–263.

[10] Sarbjeet Singh, Jagpreet Sidhu, Compliance based multi dimensional trust evaluation system for determining trustworthiness of cloud service providers, Future Generated Computer Systems 67(2017) 109-132.

[11] S. Ding, S. Yang, Y. Zhang, C. Liang, C. Xia, Combining QoS prediction and customer satisfaction estimation to solve cloud service trustworthinessevaluation problems, Knowl.-Based Syst. 56 (2014) 216–225.

[12] C. Wang, Y. Wang, C. Liu, X. Wang, An audit-based trustworthiness verification scheme for monitoring the integrity of cloud servers, J. Comput. Inf. Syst. 10(23) (2014) 9923–9937.

[13] W.J. Fan, S.L. Yang, H. Perros, J. Pei, A multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning approach, Int. J. Autom. Comput. 12 (2) (2015) 208–219.

[14] M. Deutsch, Cooperation and trust: Some theoretical notes, in: Nebraska Symposium on Motivation, Nebraska University Press, 1962.

[15] A. Chakrabarti, Grid Computing Security, Springer, Berlin, Heidelberg, 2007.

[16] T. Grandison, M. Sloman, A survey of trust in Internet applications, IEEE Commun. Surv. Tutor. 3 (4) (2000) 2–16.

[17] T.W. Grandison, Trust management for Internet applications (Doctoral Dissertation), Imperial College of Science, Technology and Medicine, University of London, 2003.

[18] J. Abawajy, Determining service trustworthiness in intercloud computing environments, in: Proceedings of IEEE 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009, pp. 784–788.

[19] W. Fan, H. Perros, A novel trust management framework for multi-cloud environments based

on trust service providers, Knowl.-Based Syst. 70 (2014) 392–406.

[20] J. Huang, D.M. Nicol, Trust mechanisms for cloud computing, J. Cloud Comput. 2 (1) (2013) 1–14.

[21] S.X. Wang, L. Zhang, S. Wang, X. Qiu, A cloud-based trust model for evaluating quality of web services, J. Comput. Sci. Tech. 25 (6) (2010) 1130–1142.

[22] F.Z. Filali, B. Yagoubi, A general trust management framework for provider selection in cloud environment, in: Proceedings of 19th East European Conference Advances in Databases and Information Systems, Springer International Publishing, Switzerland, 2015, pp. 446–457.

[23] Q. Guo, D. Sun, G. Chang, L. Sun, X. Wang, Modeling and evaluation of trust in cloud computing environments, in: Proceedings of 3rd IEEE International Conference on Advanced Computer Control, 2011, pp. 112–116.

[24] K. Thirunarayan, P. Anantharam, C. Henson, A. Sheth, Comparative trust management with applications: Bayesian approaches emphasis, Future Gener. Comput. Syst. 31 (2014) 182–199.

[25] T. Eymann, S. König, R. Matros, A framework for trust and reputation in grid environments, J. Grid Comput. 6 (3) (2008) 225–237.

[26] S.K. Chong, J. Abawajy, M. Ahmad, I.R.A. Hamid, Enhancing trust management in cloud environment, Procedia-Soc. Behav. Sci.s 129 (2014) 314–321.

[27] W. Tang, Z. Yan, CloudRec: A mobile cloud service recommender system based on adaptive QoS management, in: Proceedings of IEEE Trustcom/ BigDataSE/ISPA, Vol. 1, 2015, pp. 9–16.