ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.3

Agent – Based Cloud Computing

N.Giridhan.M.E[1], Dhanya.R[2], Elakkiya.S[3], Arulrahav.S[4]
Assistant Professor[1]
Department of Computer Science[1, 2, 3]
K.S.Rangasamy College of Technology, Tiruchengode, India

Abstract:
Cloud computing facilitates better resource utilization by multiplexing the same physical resource among several tenants. Customer does not have to manage and maintain servers, and in turn, uses the resources of cloud provider as services, and is charged according to pay-as-you-use model. Cloud marketplace witnessed frequent emergence of new service providers with similar offerings due to rapid technological advancements, Service level agreements (SLAs), which document guaranteed quality of service levels, have not been found to be consistent among providers, even though they offer services with similar functionality. In service outsourcing cloud environments, the quality of service levels are of prime importance to customers, as they use third-party cloud services to store and process their clients' data. If loss of data occurs due to an outage, the customer's business gets affected. Therefore, the major challenge for a customer is to select an appropriate service provider to ensure guaranteed service quality. To support customers in reliably identifying ideal service provider, this work proposes a framework, SelCSP, which combines trustworthiness and competence to estimate risk of interaction. Trustworthiness is computed from personal experiences gained through direct interactions or from feedbacks related to reputations of vendors. Competence is assessed based on transparency in provider's SLA guarantees. A case study has been presented to demonstrate the application of our approach. The result validates the practicability of the proposed estimating mechanisms.

Keywords: Cloud, service provider, trust, reputation, relational risk, performance risk, competence, service level agreement, control, transparency.

I. INTRODUCTION

A cloud refers to a distinct IT environment that is designed for the purpose of remotely provisioning scalable and measured IT resources. The term originated as a metaphor for the Internet which is, in essence, a network of networks providing remote access to a set of decentralized IT resources. Prior to cloud computing becoming its own formalized IT industry segment, the symbol of a cloud was commonly used to represent the Internet in a variety of specifications and mainstream documentation of Web-based architectures. It is important to distinguish the term "cloud" and the cloud symbol from the Internet. As a specific environment used to remotely provision IT resources, a cloud has a finite boundary. There are many individual clouds that are accessible via the Internet. Whereas the Internet provides open access to many Web-based IT resources, a cloud is typically privately owned and offers access to IT resources that is metered. Much of the Internet is dedicated to the access of content-based IT resources published via the World Wide Web. IT resources provided by cloud environments, on the other hand, are dedicated to supplying back-end processing capabilities and user-based access to these capabilities. Another key distinction is that it is not necessary for clouds to be Web-based even if they are commonly based on Internet protocols and technologies. Protocols refer to standards and methods that allow computers to communicate with each other in a pre-defined and structured manner. A cloud can be based on the use of any protocols that allow for the remote access to its IT resources.

CLOUD SERVICE

Although a cloud is a remotely accessible environment, not all IT resources residing within a cloud can be made available for remote access. For example, a database or a physical server deployed within a cloud may only be accessible by other IT resources that are within the same cloud. A software program with a published API may be deployed specifically to enable access by remote clients. A cloud service is any IT resource that is made remotely accessible via a cloud. Unlike other IT fields that fall under the service technology umbrella - such as service-oriented architecture - the term "service" within the context of cloud computing is especially broad. A cloud service can exist as a simple Web-based software program with a technical interface invoked via the use of a messaging protocol, or as a remote access point for administrative tools or larger environments and other IT resources.

II. EXISTING SYSTEM

The existing system develops a framework, called SelCSP, to compute overall perceived interaction risk. It establishes a relationship among perceived interaction risk, trustworthiness and competence of service provider. It proposes a mechanism by which trustworthiness of a service provider may be estimated. It also proposes a mechanism by which transparency of any provider's SLA may be computed. The model constitutes the

- **Risk estimate.** It estimates perceived interaction risk relevant to a customer-CSP interaction by combining trustworthiness and competence.

- **Trust estimate.** It computes trust between a customer-CSP pair provided direct interaction has occurred between them.
- **Reputation estimate.** It evaluates reputation of a CSP based on referrals/feedbacks from various sources and computes the belief a customer has on former's reputation.
- **Trustworthiness computation.** Function to evaluate a customer's trust on a given CSP.
- **SLA manager.** This module manages SLAs from different CSPs. It takes into account different recommendations /standards and controls which are supposed to be satisfied by the SLAs.
- **Competence estimate.** It estimates competence of a CSP based on the information available from its SLA.
- **Competence computation.** It computes transparency with respect to a given SLA and hence evaluates the competence of the CSP.
- **Risk computation.** It computes perceived interaction risk relevant to a customer-CSP interaction.
- **Interaction ratings.** It is a data repository where customer provides feedback/ratings for CSP.

Drawbacks of existing system

- It does not aim at using this risk-based provider selection.
- It does not ensure secure multi-domain collaboration in cloud.
- It does not compare the new coming cloud service providers with existing cloud providers.

III. PROPOSED SYSTEM

The proposed system includes all the existing system approach which covers multiple cloud service provider environments. In addition, the framework estimates trust-worthiness in terms of context-specific, dynamic trust and reputation feedbacks even from new coming cloud service providers. It also computes competence of a service provider in terms of transparency of SLAs. Both these entities are combined to model interaction risk, which gives an estimate of risk level involved in an interaction.

Advantages

The proposed system has following advantages

- **Level of uptime**: describes the time in a defined period the service was available, over the total possible available time, expressed as a percentage.
- **Percentage of successful requests**: describes the number of requests processed by the service without an error over the total number of submitted requests, expressed as a percentage.
- **Percentage of timely service provisioning requests**: describes the number of service provisioning requests completed within a defined time period over the total number of service provisioning requests, expressed as a percentage.
- **Average response time**: refers to the statistical mean over a set of cloud service response time observations for a particular form of request.
- **Maximum response time:** refers to the maximum response time target for a given particular form of request.
- **Maximum resource capacity:** refers to the maximum amount of a given resource available to an instance of the cloud service for a particular cloud service customer. Example resources include data storage, memory, number of CPU cores.
- It compares the new coming cloud service providers with existing cloud providers.

IV. METHODS

RISK ESTIMATION

This module estimates perceived interaction risk relevant to a customer-CSP interaction by combining trustworthiness and competence. Risk is defined as a function of the likelihood of a given threat-source's exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization. Relational risk and performance risk is taken into account. Relational risk in any alliance increases if one of the partners finds it difficult to protect its proprietary resources from others. In contrast, performance risk related to multi-party cooperation becomes high, if the consumer agent expects higher return on investment (or utility) from non-recoverable investments made towards an alliance with strategic objectives.

Proposition 1: A customer's trust on a service providing agent reduces former's perceived relational risk in an interaction. It is observed that decision-makers use potential gains and losses to estimate risk, which implies that a higher non-recoverable investment leads to the perception of higher performance risk.

Proposition 2: Perceived performance risk in an interaction will be reduced if competence of service providing agent is high. Competence of a cooperating agent gives a sense of confidence that the partner firm is capable of accomplishing a given task successfully.

Proposition 1 can be represented as:

$$R_r(c_j,p_k)\ \alpha\ \frac{1}{\tau(cj,pk)} \qquad (1)$$

where, cj is j^{th} customer who wishes to interact with k^{th} cloud service provider pk, cj;
pk is the trust which cj has on pk.

Similarly, Proposition 2 is as follows:

$$R_P(c_j,p_k)\alpha\frac{1}{C(pk)} \qquad (2)$$

where Cpk is the competence of provider pk.
From Equations (1) and (2), **the risk is modeled as**:

$$R(c_j,p_k)=K1.\frac{1}{(cj,pk)}+K2.\frac{1}{C(pk)} \qquad (3)$$

where K1 and K2 are proportionality constants.

TRUST ESTIMATION

This module computes trust between a customer-CSP pair provided direct interaction has occurred between them. A history of trust values is maintained and Interaction matrix is calculated. Interactions in a cloud environment with P service providers over A contexts is represented in a matrix I, where any element µcj (pk,α i) indicates the expected degree of trust that the customer cj has on provider pk with respect to context αi. If

there is no interaction with a provider on a particular context, it is indicated by -∞.
Interaction matrix for customer c is given as:

$$\mathrm{I}|P| \times |A|(\mathrm{C_j}) = \begin{bmatrix} \mu 1,1 & \mu 1,2 & \mu 1,|A| \\ \mu 2,1 & \mu 2,2 & \mu 2,|A| \\ \mu |P|,1 & \mu |P|,2 & \mu |P|,|A| \end{bmatrix}$$

Each element in matrix I is computed from ratings given in history of interaction H. Trust ratings in H occur in increasing order of recency.
The general trust vector for provider pk P from customer cj's perspective is a mean of expected trust degrees acquired for different contexts

$$\mathcal{G}^{\tau}(\mathrm{c_j,p_k}) = \begin{Bmatrix} \frac{1}{|A|} . \sum_{\alpha i \in A} \mu cj(pk, \alpha i) & if\ c1\ is\ true, \\ -\infty & o/w \end{Bmatrix}$$

where, | A | is the number of contexts on which interactions have been observed.

REPUTATION ESTIMATION

It evaluates reputation of a CSP based on referrals/feedbacks from various sources and computes the belief a customer has on former's reputation. Reputation model comes into effect when customer cj has not interacted with provider pk on current context in the past. Under this situation, cj has to believe in feedbacks/referrals from other customers who have directly interacted with pk. A history of trust values is maintained here also.

SLA MANAGER

This module manages SLAs from different CSPs. It takes into account different recommendations/standards and controls which are supposed to be satisfied by the SLAs.

COMPETENCE ESTIMATION AND COMPUTATION

It estimates competence of a CSP based on the information available from its SLA. It also computes transparency with respect to a given SLA and hence evaluates the competence of the CSP. It is based on the following aspect. **(Trust and Competence-based Risk).** Given a customer cj that wants to make decision regarding initiation of an interaction with a service provider pk, a trust and competence-based risk estimator TCRISK is a seven-tuple TCRISK {α, I , U , T,C , ϕ, R) , where,
α is the current context of interaction,
I is the importance of the context subjective to cj,
U is the utility expected to be gained on context a by cj,
T is the degree of trustworthiness obtained by cj towards pk on context □, [Here Gt (Module 2) is used instead of T which is taken for sake of convenience].
C is competence of pk with respect to present SLA ϕ, and
R is a function to evaluate the perceived interaction risk associated with pk over context α.

V. CONCLUSION

Cloud computing is an evolving paradigm where new service providers are frequently coming into existence offering services of similar functionality. In this thesis work problem for a cloud customer is to select an appropriate service provider from the cloud marketplace to support its business needs. However, service guarantees provided by vendors through SLAs contain ambiguous clauses which make the job of selecting an ideal provider even more difficult. As customers use cloud services to process and store their individual client's data, guarantees related to service quality level is of utmost importance. For this purpose, it is imperative from a customer's perspective to establish trust relationship with a provider. In this proposed system is competence and assessed based on transparency in provider's SLA guarantees. A case study has been presented to demonstrate the application of our approach. The result validates the practicability of the proposed estimating mechanisms using multi cloud services provider. In project, proposed a novel framework-Selection of Cloud Service Provider, which facilitates selection of trustworthy and competent service provider. The framework estimates trust worthiness in terms of context-specific, dynamic trust and reputation feedbacks. It also computes competence of a service provider in terms of transparency of SLAs. Both these entities are combined to model interaction risk, which gives an estimate of risk level involved in an interaction. Such estimate enables a customer to make decisions regarding choosing a service provider for a given context of interaction. A case study has been described to demonstrate the application of the framework. Results establish validity and efficiency of the approach with respect to realistic scenarios.

VI. REFERENCES

[1]. Jøsang and S. L. Presti, "Analysing the relationship between risk and trust," in Proc. 2nd Int. Conf. Trust Manage., Mar. 2004, pp. 135–145.

[2]. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Sys., vol. 43, no. 2, pp. 618–644, Mar. 2007.

[3]. Arias, P., Almena ́rez, F., Marı ́n, A., Dı ́az., D.: Enabling SAML for dynamic identity federation management. In.: Proceedings of Wireless and Mobile Networking Conference, pp. 173–184. Gdansk, Poland (2009)

[4].Buyya, R., Broberg, J., Goscinski, A.: Cloud Computing: Principles and Paradigms. Wiley, New York, NY, USA (2011)

[5]. Dillon, T., Wu, C., Chang, E.: Cloud Computing: Issues and Challenges. In: Proc. of AINA 2010, Perth, Australia (April 2010)

[6]. G. Schryen, M. Volkamer, S. Ries, and S. M. Habib, "A formal approach towards measuring trust in distributed systems," in Proc. ACM Symp. Appl. Comput., 2011, pp. 1739–1745.

[7]. Hardjono, T., Rutkowski, M. (eds.): Identity in the Cloud—Use Cases Version 1.0, Draft Version 0.1q. http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/IDCloud-usecases-v1.0.pdf (2011).

[8]. Hoffman, K., Zage, D., Nita-Rotaru, C.: A Survey of Attack and Defense Techniques for Reputation Systems. ACM Computing Surveys 42(1), 1–31 (2009)

[9]. K. M. Khan and Q. Malluhi, “Establishing trust in cloud computing,” IT Prof., vol. 12, no. 5, pp. 20–27, Oct. 2010.

[10]. L. Mui, A. Halberstadt, and M. Mohtashemi. Notions of Reputation in Multi-agent Systems: A Review. In Proceedings of the First Int. Joint Conference on Autonomous Agents & Multiagent Systems (AAMAS), July 2002.

[11]. Open Cloud Manifesto: Open Cloud anifesto.http: //www.opencloudmanifesto.org/ (2009).

[12]. P. Arias-Cabarcos, F. Almenarez-Mendoza, A. Marın-Lopez, D. Dıaz-Sanchez, and R. S. anchez-Guerrero, “A metric-based approach to assess risk for “on cloud” federated identity management,” J. Netw. Syst.Manage., vol. 20, no. 4, pp. 1–21, 2012. Cybern., 2010, vol. 6, pp. 2843–2848.

[13]. R. Falcone and C. Castelfranchi. Social Trust: A Cognitive Approach, pages 55–99. Kluwer, 2001.

[14]. R. Guttman, A. Moukas, and P. Maes. Agent-mediated Electronic Commerce: A Survey. Knowledge Engineering Review, 13(3), June 1998.

[15]. S. C. Payne. A guide to security metrics. Technical report, The SANS Institute, 2006.

[16]. S. K. Habib, S. Ries, and M. Muhlhauser, “Towards a trust management system for cloud computing,” in Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun., 2011, pp. 933–939.

[17]. T. Noor and Q. Sheng, “Trust as a service: A framework for trust management in cloud environments,” in Proc. 12th Int. Conf. Web Inf. Syst. Eng., 2011, pp. 314–321.

[18]. Urquhart, J.: The Biggest Cloud-Computing Issue of 2009 is Trust (2009), http:// news.cnet.com/ 8301- 19413_3-10133 487-240.html

[19]. Xiong, L., Liu, L.: Peertrust: Supporting Reputation-based Trust for Peer-to-Peer Electronic Communities. IEEE TKDE 16(7), 843–857 (2004)