IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

SelCSP: A Framework to Facilitate Selection of Cloud Service Providers

K.E.ARCHANA Mr.GKV Narasimha

Abstract: With rapid technological advancements, cloud marketplace witnessed frequent emergence of new service providers with similar offerings. However, 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 environments, like cloud, 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. Experimental results validate the practicability of the proposed estimating mechanisms.

1 INTRODUCTION

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. Similar to other on-line distributed systems, like e-commerce, p2p networks, product reviews, and discussion forums, a cloud provides its services over the Internet.

Among several issues that prevented companies from moving their business onto public clouds, security is a major one. Some of the security concerns, specific to cloud environment are: multi-tenancy, lack of customer's control over their data and application , lack of assurances and violations for SLA guarantees , non-transparency with respect to security profiles of remote datacenter locations, , and so on. Recent advancements in computation, storage, service-oriented architecture, and network access have facilitated rapid growth in cloud marketplace. For any service, a cloud customer may have multiple service providers to choose from. Major challenge lies in selecting an "ideal" service provider among them. By the term ideal, we imply that a service provider is trustworthy as well as competent. Selection of an ideal service provider is non-trivial because a customer uses third-party cloud services to serve its clients in cost-effective and efficient manner. In such a scenario, from the cloud customer's perspective, persisting to a guaranteed level of service, as negotiated through establishing service level agreement (SLA), is of prime importance. Data loss owing to provider's incompetence or malicious intent can never be replaced by service credits. In the present work, we focus on selection of a trustworthy and competent service provider for business outsourcing. In 2010-11, a series of cloud outages1,2 have been reported which include commercial service providers viz. Amazon EC2, Google Mail, Yahoo Mail, Heroku, Sony, and so on. In most cases, it has been observed that the failover time is quite long and customers' businesses were hugely affected owing to lack of recovery strategy on vendor side. Moreover, in some instances, customers were not even intimated about the outage by providers. Cloud providers may use the high-quality first-replication (HQFR) strategy proposed in [4] to model their recovery mechanism. In this work, authors propose algorithms to minimize replication cost and the number of QoS-violated data replicas. It is desirable from customer's point-of-view to avoid such loss, rather than getting guarantees of service credits following a cloud outage. Avoidance of data loss requires reliable identification of competent service provider. As customer does not have control over its data deployed in cloud, there is a need to estimate risk prior to outsourcing any business onto a cloud. This motivated us to propose a risk estimation scheme which makes a quantitative assessment of risk involved while interacting with a given service provider. To the best of our knowledge, estimation of risk of interaction in cloud environment has not been addressed in prior works in this respect, the current work is significant as it proposes a framework, SelCSP,3 which attempts to compute risk

involved in interacting with a given cloud service provider (CSP). The framework estimates perceived level of interaction risk by combining trustworthiness and competence of cloud provider. Trustworthiness is computed from ratings obtained through either direct interaction or feedback. Competence is estimated from the transparency of SLA guarantees. We summarize the contributions of this work as follows: Develop a framework, called SelCSP, to compute overall perceived interaction risk. Establish a relationship among perceived interaction risk, trustworthiness and competence of service provider. Propose a mechanism by which trustworthiness of service provider may be estimated Propose a mechanism by which transparency of any provider's SLA may be computed. Comparison of trust and competence results generated by SelCSP and those obtained from models reported in literature. Analysis of results to provide insight into the behavior of the proposed risk model.

2 SELCSP FRAMEWORK

In this section, a framework, termed as SelCSP, has been proposed to facilitate customers in selecting an ideal cloud service provider for business outsourcing. Fig. 1 depicts different modules of the framework and how these modules are functionally related. As evident in Fig. 1a, the dotted boundary region denotes the SelCSP framework which acts as a third-party intermediator between customers and cloud service providers. SelCSP framework provides APIs through which both customers and providers can register themselves. After registering, customer can provide trust ratings based on interactions with provider. Cloud provider needs to submit its SLA to compute competence. At present, verifying the correctness of submitted ratings or sanitizing the erroneous data in the framework is beyond the scope. We assume that only registered customers can provide referrals/feedbacks and they do not have any malicious intents of submitting unfair ratings. Various modules constituting the framework are as follows:

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

2) Trust estimate. It computes trust between a customer- CSP pair provided direct interaction has occurred between them.

3) 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.

4) Trustworthiness computation. Function to evaluate a customer's trust on a given CSP.

5) 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.

6) Competence estimate. It estimates competence of a CSP based on the information available from its SLA.

7) Competence computation. It computes transparency with respect to a given SLA and hence evaluates the competence of the CSP.

8) Risk computation. It computes perceived interaction risk relevant to a customer-CSP interaction.

9) Interaction ratings. It is a data repository where customer provides feedback/ratings for CSP.

The broad objective of SelCSP framework is to evaluate risk involved in interacting with different cloud service providers. Risk evaluation is done by computing trust which a customer has on a particular provider and transparency obtained from latter's service level agreement guarantees.

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016

ISSN: 2320-1363

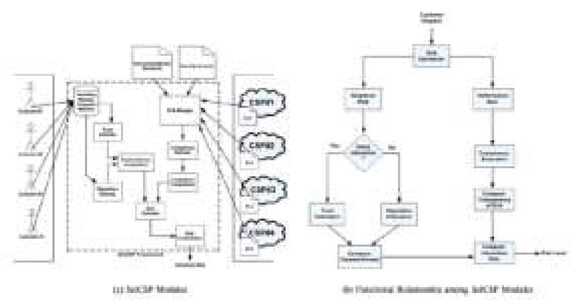

Fig. 1. SelCSP framework and module interactions.

For clear understanding, a high-level functional overview of the framework has been presented in Fig. 1b. The risk estimate block receives customer request regarding estimation of interaction risk for a provider. This block delegates the request to relation risk and performance risk blocks to compute trustworthiness and competence of the provider, respectively. The relational risk block checks if the requester has previous interaction ratings with the provider. If such ratings are available, trust is calculated, otherwise feedback-based reputation is computed, both eventually leading to estimation of trustworthiness. In contrast, performance risk is computed by evaluating the transparency of provider's SLA guarantees. Finally, trustworthiness and competence gives a measure of interaction risk through compute: interaction risk block.

3 ESTIMATING CLOUD SERVICE PROVIDER'S COMPETENCE

In cloud marketplace, vendors negotiate service quality levels with customers by means of SLA. Different vendors offer different SLA structures, service offerings, performance levels, and negotiation opportunities. SLA can be used to select a service provider on the basis of data protection, continuity, and cost [45]. A typical SLA will contain the following [46]:

(i) a set of services which the provider will deliver,

(ii) a complete, specific definition of each service,

(iii) responsibilities of the provider and the consumer,

(iv) a set of metrics to measure whether the provider is offering the services as guaranteed,

(v) exclusion clauses,

(vi) an auditing mechanism to monitor the services,

(vii) the remedies available to consumer and provider if the terms are not satisfied, and

(ix) how SLAs will change over time. Service qualities which provider guarantees to offer through SLA are measured by some metrics based on which its monitoring and auditing may be done. These metrics are known as SLA parameters. Each high-level SLA parameter is a function of one or more key performance indicators (KPIs) [47], [48] which are composed, aggregated, or converted to form the former. A precise and unbiased SLA helps to generate trust relationship among customer and provider. However, present day cloud SLAs contain vague clauses which do not convince the customers regarding assurances and compensations following a violation, if occurs [2]. Majority of cloud service providers guarantee "availability" of service. However, other than "availability" there exists other SLA parameters whose inclusion is necessary to render completeness to any SLA. This is because, consumers not only demand availability guarantee but also other performance related assurances which are equally business critical [49].

Therefore, it is essential to establish a standard set of parameters for cloud SLAs, since it reduces the perception of risk in outsourced services .

4 RESULT AND DISCUSSION

We have implemented the proposed framework using Java programming language and have simulated the following case study to demonstrate provider selection mechanism through SelCSP.

4.1 Case Study

Let us consider that at present six SaaS cloud service providers are registered with SelCSP framework. The CSPs are denoted as CSP1, CSP2, CSP3, CSP4, CSP5, and CSP6 respectively. A customer X, who is also registered with SelCSP, wants to choose ideal service providers for business outsourcing. The customer has set three qualitative levels for both Importance (I) and Utility (U) of a context: high (H), medium (M), low (L). The values assigned to these levels are 0.95, 0.55, and 0.25 respectively. These values have been given as input to

ISSN: 2320-1363

SelCSP framework. Combination of I and U produces nine different contexts of interaction given as: (a) email and office productivity, (b) billing, (c) customer relationship management, (d) collaboration, (e) content management, (f) document management, (g) human resources, (h) sales, and (i) enterprise resource planning. Now, X wants to determine which among the above six CSPs areideal for different contexts, such that the former can serve its clients in a cost-effective and efficient manner. Under such situation, X requests SelCSP framework to recommend service provider which is both trustworthy as well as competent for a given context. SelCSP estimates trustworthines

4.2 Validation of Competence Estimation

In the author has computed transparency of six independent cloud service providers from their self-service portals and published web contents. In this work, we use the same information and compute transparency with respect to SLA standards recommended by NIST. In ideal scenario, it is desirable that the service providers follow SLA standards recommended by NIST . However, in practical scenario, we find that these SLAs are customized to accommodate service provider's management policies. SLA related information available from their portals are customized according to our parameters and given as input to the SelCSP framework.

5 CONCLUSION

Cloud computing is an evolving paradigm, where new service providers are frequently coming into existence, offering services of similar functionality. Major challenge 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 makes 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 aprovider. Moreover, as customers are outsourcing their businesses onto a third-party cloud,

ISSN: 2320-1363

capability or competence of CSP determines if former's objectives are going to be accomplished. In this work, we propose a novel framework, SelCSP, which facilitates selection of trustworthy and competent service provider. The framework estimates trustworthiness 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 efficacy of the approach with respect to realistic scenarios. In future, we aim at using this risk-based provider selection to ensure secure multi-domain collaboration in cloud environment.

REFERENCES

[1] Y. Chen, V. Paxson, and R. H. Katz, "What's new about cloud computing security," EECS Dept., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2010-5, Jan. 20, 2010.

[2] 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.

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

[4] J. Lin, C. Chen, and J. Chang, "Qos-aware data replication for data intensive applications in cloud computing systems," IEEE Trans. Cloud Comput., vol. 1, no. 1, pp. 101–115, Jan.–Jun. 2013.

[5] D. Gambetta, "Can we trust trust?" in Trust: Making and Breaking Cooperative Relations, D. Gambetta, Ed. Oxford, U.K.: Blackwell, 1990, ch. 13, pp. 213–237.

[6] D. H. Mcknight and N. L. Chervany, "The meanings of trust," Manage. Inf. Syst. Res. Center, Univ. Minnesota, Minneapolis, MN, USA, Tech. Rep. MISRC Working Paper Series 96-04, 1996.

[7] D. Manchala, "Trust metrics, models and protocols for electronic commerce transactions," in Proc. 18th Int. Conf. Distrib. Comput. Syst., 1998, pp. 312–321.

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

[9] L. Freeman, "Centrality on social networks," Social Netw., vol. 1, pp. 215–239, 1979.

[10] T. Grandison and M. Sloman, "A survey of trust in internet applications," IEEE Commun. Surv. Tutorials, vol. 3, no. 4, pp. 2– 16, Fourth Quarter 2000.

[11] A. 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.

[12] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system," in The Economics of the Internet and ECommerce, series Advances in Applied Microeconomics, vol. 11, M. Baye, Ed. Amsterdam, The Netherlands: Elsevier, 2002, pp. 127–157.

[13] A. Withby, A. Jøsang, and J. Indulska, "Filtering out unfair ratingsin Bayesian reputation systems," in Proc. 7th Int. Workshop TrustAgent Soc., 2004, pp. 1–13.

[14] B. Yu and M. P. Singh, "An evidential model of distributed reputationmanagement," in Proc. 1st Int. Joint Conf. Autonom. Agents Multiagent Syst.: Part 1, Jul. 2002, pp. 294–301.

[15] A. Jøsang, "A logic for uncertain probabilities," Int. J. Uncertainty Fuzziness Knowl.-Based Syst., vol. 9, no. 3, pp. 279–311, Jun. 2001.

[16] J. Sabater, and C. Sierra, "Regret: A reputation model for gregarious societies," in Proc. 4th Int. Workshop Deception, Fraud Trust Agent Soc., 5th Int. Conf. Auton. Agents, 2001, pp. 61–69.

[17] S. K. Habib, S. Ries, and M. Muhlhauser, "Cloud computing landscape and research challenges regarding trust and reputation," in Proc. 7th Int. Conf. Ubiquitous Intell. Comput. 7th Int. Conf. Auton. Trusted Comput., 2010, pp. 410–415.

[18] I. M. Abbadi and A. Martin, "Trust in the cloud," Inf. Security Tech. Rep., vol. 16, no. 3, pp. 108–114, 2011.

[19] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Secur. Privacy, vol. 8, no. 6, pp. 24–31, Nov./Dec. 2010.

[20] H. Sato, A. Kanai, and S. Tanimoto, "A cloud trust model in a security aware cloud," in Proc. 10th IEEE/IPSJ Int. Symp. Appl. Internet, 2010, pp. 121–124.

[21] 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.

[22] I. M. Abbadi and M. Alawneh, "A framework for establishing trust in the cloud," Comput. Elect. Eng., vol. 38, pp. 1073–1087, 2012.

[23] P. Arias-Cabarcos, F. Almen_arez-Mendoza, A. Mar_ın-L_opez, D. D_ıaz-S_anchez, 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. 78 IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 3, NO. 1, JANUARY-MARCH 2015

[24] X. Li, L. Zhou, Y. Shi, and Y. Guo, "A trusted computing environment model in cloud architecture," in Proc. Int. Conf. Mach. Learn. Cybern., 2010, vol. 6, pp. 2843–2848.

[25] M. Alhamad, T. Dillon, and E. Chang, "A trust-evaluation metric for cloud applications," Int. J. Mach. Learn. Comput., vol. 1, no. 4, pp. 416–421, 2011.

vol1.l9, no.1, pp.15-25, February 2003.

[3] GSM networks: protocols, terminology and implementation by Gunnar Heine.

[4]. Rathinakumar, R. & Manivannan, D. (2012). "Wireless Accident Information System with GSM and GPS".

Author's profile:

Mr.GKV Narasimha reddy received Ph.D from Annamalai University and received M.tech degree from Sathyabama University. He is currently working as Associate professor, Department

ISSN: 2320-1363

of CSE, in St.Johns college of engineering and technology, Kurnool, Andhra Pradesh, India. His interests includes Computer Networks,Operating system,Data Base Management Systems.

K.E.ARCHANA received B.Tech Degree from Indira priyadarshini college of engineering and technology for women in Kurnool. She is currently pursuing M.Tech Degree in computer science Engineering specialization in St.Johns college of engineering and technology, Kurnool, India.