Sel Csp-A Frame Work to Facilitate Selection with Transparency of Cloud Service Providers

Dr.V.Goutham [1], B.Vijitha[2], P.Harshini[3]
[1,2,3]Department of Computer Science and Engineering, Teegala Krishna Reddy Engineering College, Meerpet, Telangana, India

Abstract— with the innovative advancements in technology, cloud marketplace countersigned frequent emergence of new service providers with similar offerings. Nevertheless, service level agreements (SLAs), which document assured eminence of service levels, have not been created to be reliable among providers, even though their proposal of services has with related functionality. In provision of outsourcing environs, like cloud, the quality of service levels are of primary prominence to customers, as they use third-party cloud services to pile and route their clients' data. The key encounter for a customer is to choose a suitable service provider to confirm assured service excellence. Supporting customers sustenance in consistently classifying ideal service provider and this lead in introducing a framework, SelCSP, which combines dependability and competence to assess risk of interaction. Dependability is computed from personal experiences added through straight connections or from comments linked to standings of sellers. Competence is measured based on limpidity in provider's SLA sureties.

Index Terms— Cloud, service provider, trust, reputation, relational risk, performance risk, competence, service level agreement, control, Transparency

1 INTRODUCTION

Regarding the security concerns, precise to cloud environment is lack of customer's control over their data and application [1], privation of declarations and desecrations for SLA guarantees [2], non-transparency with respect to security profiles of remote data center locations, [3], and so on. Topical progressions in reckoning, storage, service-oriented architecture, and network admission have simplified rapid growth in cloud marketplace. For any service, a cloud customer may have many service providers to choose from. Major challenge lies in choosing an "ideal" service provider among them. By the term ideal, we suggest that a service provider is trustworthy as well as competent. Range of an ideal service provider is non-trivial because a customer practises third-party cloud services to serve its clients in cost-effective and efficient manner. In this situation, from the cloud customer's perspective, persevering to a guaranteed level of service, as negotiated through starting service level agreement (SLA), is crucial.[10] 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 soon. 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. Averting of data loss needs consistent identification of capable service provider. As customer does [16] not have control over its data deployed in cloud, there is a need to evaluation risk prior to outsourcing any business onto a cloud. A risk estimation scheme which makes a quantitative assessment of risk involved while interacting with a given service provider. The estimation of risk of collaboration in cloud environment has not been addressed in prior works [10]. The assistances of the scheme are: developing a framework, called SelCSP, to calculate overall perceived interaction risk, establish a relationship among perceived interaction risk, trustworthiness and capability of service provider, a mechanism by which credibility of a service provider may be projected.

2 RELATED WORK

Decision trust is the extent to which one party is willing to depend on another even though negative consequences are possible. In cloud scenario, both notions are prevalent as customer depends on third-party provider, believing that it is reliable enough to produce positive utility. Some works [7], [8] have proposed computation models for trust by incorporating the concept of risk. Like trust, reputation has also been studied extensively. From the perspective of social network researchers [9], reputation is perceived as an entity which is globally visible to all members of a social network community. In survey papers on trust [10], [11], the authors have classified trust into five categories viz. provision, access, delegation, identity, and context. These categories model trust relationships between a relying party and: (i) a service provider,(ii) accessing resources, (iii) third-party arbitrator, (iv) signed attributes, and (v) supporting transactions, respectively. In cloud context, trust between customer and provider is of provision type. Reputation system has been classified into two types [11]: centralized and distributed depending on the site of computation. In centralized type, a central authority (reputation center) collects all the ratings, computes a reputation score for every participant, and makes all scores publicly available, while in distributed type there can be distributed stores where ratings can be submitted, or each participant simply records the opinion about each experience with other parties, and provides this information on request. Distributed reputation systems are primarily deployed in peer-to-peer (P2P) networks. A number of methodologies have been proposed for evaluating reputation. Some of the noteworthy are summation or average of ratings, as used in eBay's reputation forum [12], Bayesian system [13], belief models [14], [15], and fuzzy models [7], [16]. The concepts of trust and reputation have been successfully implemented in multiple Internet mediated services viz., eBay's feedback forum,4 Epinions,5 Amazon,6 Slashdot,7 and so on. A cloud environment is similar in nature to these online services, where trust and reputation also need to be enforced. One major difference between cloud and the other online systems (P2P, e-commerce, etc.) is the degree of control which a customer has on his data/application while using these Internet-mediated systems. A customer outsources its data and applications to a third-party cloud vendor for ease of manageability and maintainability. For Software-as-a-Service (SaaS) cloud model, this control completely rests with the provider. On contrary, P2P is largely responsible for file sharing applications, online recommendation systems give[11] product reviews to support decision making, and in case of e-commerce, autonomous domains interoperate through service chaining, governed by predefined global policy. Usually, the cloud customer uses third-party cloud services to manage its clients' data in a cost-effective and convenient manner. Therefore, if there is any loss of such data from cloud provider's end, the customer loses both business and reputation to its clients. Hence, it is imperative to establish trust relationship between customer and service provider to facilitate reliable usage of cloud-based services [10]. A cloud customer demands not only availability of services from a provider, but also expects that the services should persist to the guaranteed quality levels. In any SLA, service guarantees are given in form of service level objectives (SLOs). Based on the following limitations of reported works on cloud-based trust model and service level agreement, we form the motivation of this work: No work addresses the issue of selecting trustworthy service provider in cloud marketplace. Estimation of risk of outsourcing a business onto third-party cloud has not been handled in reported works. In the state-of-the-art cloud, the security guarantees and responsibilities are specified in SLAs. However, vague clauses and unclear technical specifications of SLAs make selection of service provider difficult for customers [2]. Transparency of provider's SLA [31] is one of the provisions to deduce competence.

3 SYSTEM DESIGN: SELCSP FRAMEWORK

Sel CSP framework runs APIs through which both customers and providers can list themselves. After registration, customer can provide trust ratings based on communications with provider. Cloud provider requests to submit its SLA to compute proficiency. At present, confirming the correctness of submitted ratings of the erroneous data in the framework is beyond the scope. A supposition that only registered customers can provide referrals and they do not have any malicious intents of submitting unfair ratings. Different modules constituting the framework are as follows:[12]

1) Risk estimate: Estimating professed communication risk pertinent to a customer-CSP interaction by coalescing reliability and competency.

2) Trust estimate: It calculates trust between a customer-CSP pair provided straight interaction has happened among them.

3) Reputation estimate: It evaluates reputation of a CSP based on referrals from many sources and calculates 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 unlike standards and controls which are supposed to be satisfied by the SLAs.

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

7) Competence computation: It computes limpidity 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.

4 FRAMEWORK IMPLEMENTATION AND EVALUATION

Considering that presently six SaaS cloud service providers are registered with SelCSP framework. The CSPs are denoted as CSP1, CSP2, CSP3, CSP4, CSP5, and CSP6[14],[13] correspondingly. A customer X, who is also registered with SelCSP, wants to elect 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 SelCSP framework. Amalgamation of I and U creates nine unalike contexts of interaction.They are: (a) email and office productivity, (b) billing, (c) customer relationship management, (d) collaboration, (e) contentmanagement, (f) document management, (g) human resources,(h) sales, and (i) enterprise resource planning. X needs to define which among the above six CSPs are ideal 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 endorse[15] service provider which is both dependable as well as capable for a given context. SelCSP estimates fidelity and competence for all the service providers under nine different contexts. Using the above estimates, perceived interaction risk is evaluated. A user does not have to input all these parameters. Most of these parameters which are to be input by user are either subjective or has to be chosen from a predefinedset. SelCSP endorses a provider with whom the risk of interaction is less.

4.1 Validation of Trust and Reputation Estimations:

Focusing on authorising and analyzing the behaviors of suggested trust and proficiency estimation schemes. Crucial objective is to establish the fact that the trust and capability values generated by SelCSP are similar to those stimulated by testified mechanisms. It acts as evidence that our evaluation submodules produce valid results, which ultimately leads to generation of correct interaction risk-based recommendations towards unlike cloud service providers. In SelCSP framework, it is computed trustworthiness of a provider based on responses from customers.[17] Furthermore, framework also aims at ancillary customers in selecting cloud provider based on interaction risk. Outstanding to these comparisons, it has chosen Opinions dataset to validate our trust evaluation mechanism. Similar attempt by using Opinions data has also been observed in [6], where the authors have studied the performance of their credibility model in the context of providing feedbacks to cloud services.

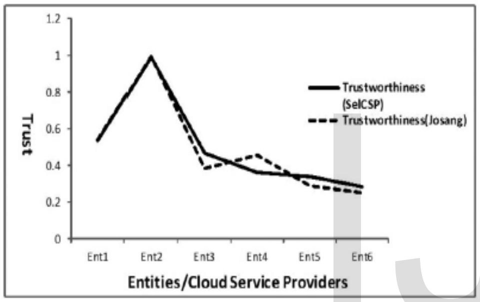

Fig.1.Comparison of trust

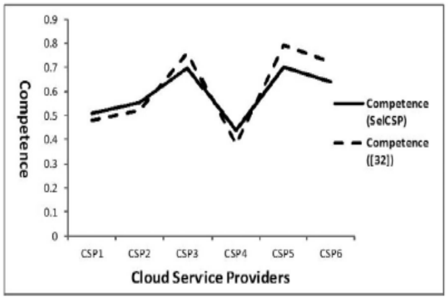

Fig. 2. Comparison of CSP competence.

4.2 Validation of Competence Estimation:

It was computed transparency of six independent cloud service providers from their self-service portals and available web contents. Here it is used the same information and compute transparency with deference to SLA standards suggested by NIST. In supreme situation, it is necessary that the service providers follow SLA standards recommended by NIST[15]. Conversely, in concrete development, it is found that these SLAs are modified to place service provider's management policies. SLA connected information available from their portals are customized according to our parameters and given as input to the SelCSP framework. Transparencies of these CSPs obtained from [11]. The competence values based on transparency of respective SLAs are almost similar for CSP1, CSP2, CSP3, and CSP4, whereas they vary in contexts of CSP5 and CSP6. This variation in transparency is attributed
by differences in the mode of assessment followed in two[18] procedures. In [20], the scoring system is strictly binary and deals only with security, privacy, external audits or certification, and service levels offered by SLA. Furthermore, while determining these parameters, NIST endorsements and values have not been taken into account. While, in the proficiency estimation, SLAs are evaluated based on NIST suggested SLA parameters and relevant controls. It is also more granular in terms of assigning values for computing overall degree of transparency.

5 CONCLUSION

In this Sel CSP-a frame work to enable selection with transparency of cloud service providers, the main task for a cloud customer is to choose an suitable service provider from the cloud market place to backing its business essentials. Nevertheless, service guarantees provided by vendors through SLAs contain mystifying openings which makes the job of selecting an perfect provider even more problematic. As customers use cloud services to route and hoard their individual client's data, assurances related to service quality level is of utmost importance. It is imperative from a customer's perspective to create trust relationship with a provider. Furthermore, as customers are outsourcing their businesses onto a third-party cloud, competence of CSP determines if former's objectives are going to be accomplished.

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 ratings in Bayesian reputation systems," in Proc. 7th Int. Workshop Trust Agent Soc., 2004, pp. 1–13.

[14] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," 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.

AUTHORS

[1] Dr V. Goutham is a Professor and Head of the Department of Computer Science And Engineering at Teegala Krishna Reddy Engineering College affiliated to J.N.T.U Hyderabad. He received Ph.d from Acharya Nagarjuna University, M.Tech from Andhra University and B.Tech from J.N.T.U Hyderabad. He worked for various MNC Companies in Software Testing and Quality as Senior Test Engineer. His research interests are Software Reliability Engineering, software testing, software Metrics, and cloud computing.

[2] Mrs. B.Vijitha is working as a Assistant Professor in the Department of Computer Science And Engineering at Teegala Krishna Reddy Engineering College affiliated to J.N.T.U Hyderabad.

[3] Ms. P.Harshini Department of Computer Science And Engineering at Teegala Krishna Reddy Engineering College affiliated to J.N.T.U Hyderabad.