ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 12, March 2016

A CONSTRUCTION TO ASSIST SELECTION OF CLOUD SERVICE PROVIDERS BASED ON TRUST AND SERVICE LEVEL AGREEMENT

Manoj.K [1], Sumithradevi.C [2]

1. P.G. Student, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India
2. Asst.Professor, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India

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.**

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

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 [1], lack of assurances and violations for SLA guarantees [2], non-transparency with respect to security profiles of remote datacenter locations, [3], 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. Hence, 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 a 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.

II LITERATURE SURVEY

A. Analysing The Relationship Between Risk And Trust

In this paper [1], the authors JOSANG and S. L. PRESTI Analysing the relationship between risk and trust stated that among the various human factors impinging upon making a decision in an uncertain environment, risk and trust are surely crucial ones. Several models for trust have been proposed in the literature but few explicitly take risk into account. This paper analyses the relationship between the two concepts by first looking at how a decision is made to enter into a transaction based on the risk information. They then drew a model of the invested fraction of the capital function of a decision surface. They finally defined a model of trust composed of a reliability trust as the probability of transaction success and a decision trust derived from the decision surface.

B. A Survey Of Trust And Reputation Systems For Online Service Provision

In this paper [2], the authors R.ISMAIL, and C. BOYD stated that Trust and reputation systems represent a significant trend in decision support for Internet mediated service provision. The basic idea is to let parties rate each other, for example after the completion of a transaction, and use the aggregated ratings about a given party to derive a trust or reputation score, which can assist other parties in deciding whether or not to transact with that party in the future.

C. A Formal Approach Towards Measuring Trust In Distributed Systems

In this paper [3], the authors stated that emerging digital environments and infrastructures, such as distributed security services and distributed computing services, have generated new options of communication, information sharing, and resource utilization in past years. Christo Ananth et al. [7] discussed about a method, Wireless sensor networks utilize large numbers of wireless sensor nodes to collect information from their sensing terrain. Wireless sensor nodes are battery-powered devices. Energy saving is always crucial to the lifetime of a wireless sensor network. Recently, many algorithms are proposed to tackle the energy saving problem in wireless sensor networks. There are strong needs to develop wireless sensor networks algorithms with optimization priorities biased to aspects besides energy saving. In this project, a delay-aware data collection network structure for wireless sensor networks is proposed based on Multi hop Cluster Network. The objective of the proposed network structure is to determine delays in the data collection processes. The path with minimized delay through which the data can be transmitted from source to destination is also determined. AODV protocol is used to route the data packets from the source to the destination.Based on these formulas, the quantitative part returns trust metrics for the determination of trustworthiness with which given distributed systems are assumed to fulfill a particular security requirement.

D. A Trust-Evaluation Metric for Cloud Applications

In this paper, the authors stated that Cloud services are becoming popular in terms of distributed technology because they allow cloud users to rent well-specified resources of computing, network, and storage infrastructure. Users pay for their use of services without needing to spend massive amounts for integration, maintenance, or management of the IT infrastructure. Before interaction occurs between cloud providers and users, trust in the cloud relationship is very important to minimize the security risk and malicious attacks. The notion of trust involves several dimensions. By this we form the motivation of this paper,

- Some works 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, reputation is perceived as an entity which is globally visible to all members of a social network community.
- 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.
- Models proposed in reported works lack experimentation and analysis. 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.Transparency of provider’s SLA is one of the provisions to deduce competence. We have used this approach in the present work to estimate cloud provider’s competence.

Drawbacks

- No mathematical model presented.
- No experiment or validation done.
- Some results have been given to establish higher accuracy of the model, but lacks analysis.

III. SelCSP FRAMEWORK

The current work is significant as it proposes a framework, SelCSP, 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. A framework, termed as SelCSP, has been proposed to facilitate customers in selecting an ideal cloud service provider for business outsourcing which depicts different modules of the framework and how these modules are functionally related. 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.

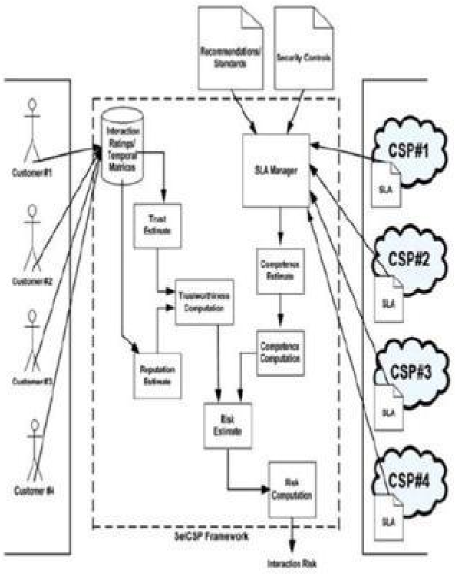

Fig.1 System Architecture

3.1 Objectives

- Support for customer-driven service management based on customer profiles and QoS requirements;
- Definition of computational risk management tactics to identify, assess, and manage risks involved in the execution of applications with regards to service requirements and customer needs;
- Derivation of appropriate market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain SLA-oriented resource allocation;Incorporation of autonomic resource management models that effectively self-manage changes in service requirements to satisfy both new service demands and existing service obligations;
- Leverage of Virtual Machine (VM) technology to dynamically assign resource shares according to service requirements;
- Implementation of the developed resource management strategies and models into a real computing server in an operational data center.

3.2 Problem Definition

The main purpose of 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 satisfiied 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.
- In Proposed the framework estimates trust-worthiness in terms of context-specifiic, 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.

3.3 Advantages of Proposed System:

- 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 a 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.

IV. CONCLUSION AND FUTURE WORKS

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 this study, proposed a novel framework- SelCSP, which facilitates selection of trustworthy and competent service provider. The framework estimates trust worthiness in terms of context-specifiic, 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.

Scope for Future Development

Several algorithms are proposed for select an appropriate service provider to ensure guaranteed service quality. To support customers in reliably identifying ideal service provider, the proposed searching SelCSP algorithm efficiency can be improved in future works. In future, for selecting the cloud service providers, data mining techniques and aggregation methodologies may apply for combines trustworthiness and competence to estimate risk of interaction and compute the Trustworthiness from personal experiences gained through direct interactions or from feedbacks related to reputations of vendors

- If the experimental study is tested with real environment, then it can assist the further proceeding of the algorithm implementation practically.

The new system becomes useful if the above enhancements are made in future. The new system is designed such that those enhancements can be integrated with current modules easily with less integration work. The following enhancements are should be in future.

- The application if developed as web services, then many applications can make use of the records.
- The data integrity in cloud environment is not considered. The error situation can be recovered if there is any mismatch.
- The web site and database can be hosted in real cloud place during the implementation.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] Christo Ananth, T.Rashmi Anns, R.K.Shunmuga Priya, K.Mala, “Delay-Aware Data Collection Network Structure For WSN”, International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.17-21

[8] 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.

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

[10] 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.

[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.

[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.

[21] Nirnay Ghosh, Student Member, Ieee, Soumya K. Ghosh, Member, Ieee, And Sajal K. Das, Senior Member, Ieee, “Selcsp: A Framework To Facilitate Selection Of Cloud Service Providers”, Ieee Transactions On Cloud Computing, Vol. 3, No. 1, January-March 2015.