September'2016 Issue
International Journal of Computer Sciences
ISSN Number: 4142 3453

A Framework to Facilitate Selection of Enhanced Multi Cloud Service Providers

G. SAMEERA KHANAM[1] and G. SUVARNA[*2]

[1]M.Tech (CSE),PG Scholar ,Department of CSE, Bharath College of Engineering and Technology for Women,Kadapa

[2]Assistant Professor , Department of CSE, Bharath College of Engineering and Technology for Women,Kadapa

***Abstract*— Cloud computing facilitates better resource utilization by multiplexing the same physical resource among several tenants. 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. The result validates the practicability of the proposed estimating mechanisms.**

***Index Terms*— Cloud computing, service quality, CSP SelCSP.**

I. 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 scen ario, 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.

A. *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.

II. II.RELATEDWORKS

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.

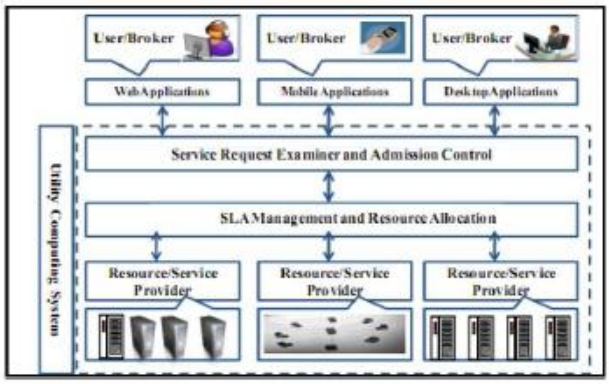
A Survey Of Trust And Reputation Systems For Online Service Provision In this paper [2], the authors R.ISMAIL, and C. B OYD stated that Trust and reputation systems represent a significant trend in decision support for Internet mediated service provision. The basic idea is to let parties rate each other, 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.

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. However, when distributed services are used, the question arises of to what extent we can trust service providers to not violate security requirements, whether in isolation or jointly. Answering this question is crucial for designing trustworthy distributed systems and selecting trustworthy service providers.

This paper presents a novel trust measurement method for distributed systems, and makes use of propositional logic and probability theory. The results of the qualitative part include the specification of a formal trust language and the representation of its terms by means of propositional logic formulas. 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.

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. SLA-oriented Resource Allocation Through Virtualization Recently, virtualization [24,25] has enabled the abstraction of computing resources such that a single physical machine is able to function as multiple logical VMs (Virtual Machines). A key benefit of VMs is the ability to host multiple operating system environments which are completely isolated from one another on the same physical machine. Another benefit is the capability to configure VMs to utilize different partitions of resources on the same physical machine. Physical machine, one VM can be allocated 10% of the processing power, while another VM can be allocated 20% of the processing power. Hence, VMs can be started and stopped dynamically to meet the changing demand of resources by users as opposed to limited resources on a physical machine.

In particular, VMs may be assigned various resource management policies catering to different user needs and demands to better support the implementation of SLA-oriented resource allocation.

Good SLA sets boundaries and expectations of service provisioning and provides the following benefits:

- Enhanced customer satisfaction level: A clearly and concisely defined SLA increases the customer satisfaction level, as it helps providers to focus on the customer requirements and ensures that the effort is put on the right direction.
- Improved Service Quality: Each item in an SLA corresponds to a Key Performance Indicator (KPI) that specifies the customer service within an internal organisation.
- Improved relationship between two parties: A clear SLA indicates the reward and penalty policies of a service provision. The consumer can monitor services according to Service Level Objectives (SLO) specified in the SLA. Moreover, the precise contract helps parties to resolve conflicts more easily.

International Journal of Computer Sciences
September'2016 Issue
ISSN Number: 4142 3453

III. PROBLEM STATEMENT

A. EXISTING MODEL

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.

B. PROPOSED SYSTEM:

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.

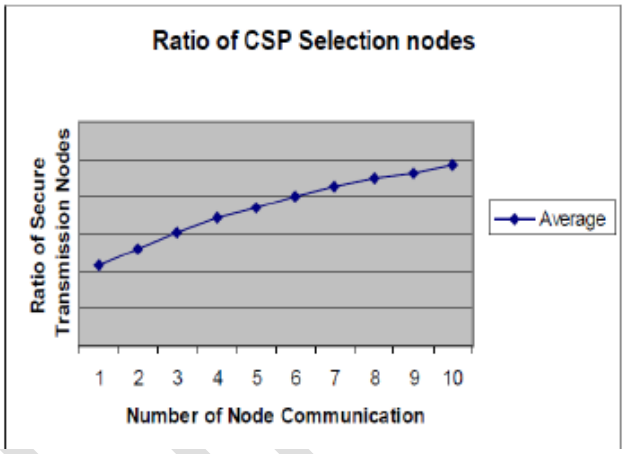
SelCSP framework provides APIs through which both customers and providers can register themselves. After registering, customer can provide trust ratings based on interactions with provider. Cloud provider needs to submit its SLA to compute competence.

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.

IV. EXPERIMENTAL RESULTS

The following **Table 1.1** describes experimental result for existing system secure transmission node analysis. The table contains number of time slot interval and given time interval to calculate average numbers of CSP details are shown

The following **Table 1.3** describes experimental result for proposed system secure transmission node analysis. The table contains number of time slot interval and given time interval to calculate average numbers of send transmission node details are shown



S.NO	NUMBER OF TIME SLOT (M)	RATIO OF CSP NODE
1	10	0.48
2	20	0.57
3	40	0.66
4	60	0.72
5	80	0.77
6	100	0.83

The following **Figure 1.4** describes experimental result for proposed system secure transmission node analysis. The tablecontains number of time slot interval and given time interval to calculate average numbers of send transmission node details are shown

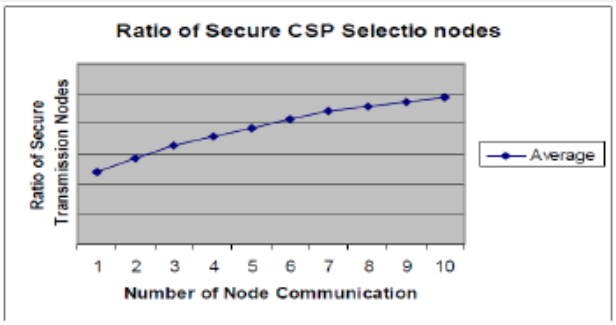


Fig 1.4 : Selection Multi Cloud Services Provider- Ratio Analysis The following **Table 1.5** describes experimental result for proposed system error rate analysis. The table contains average of cloud services provider and average percentages for existing and proposed system in cloud environment detection are shown.

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

REFERENCES

[1] 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 managementsystem 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] K. Sentz and S. Ferson, "Combination of evidence in Dempster- Shafer theory," Sandia Nat. Laboratories, Albuquerque, NM, USA, Tech. Rep. SAND 2002-0835, Apr. 2002.

[12] G. Shafer, A Mathematical Theory of Evidence, vol. 76. Princeton, NJ, USA: Princeton Univ. Press, 1976.

[13] J. Gordon and E. H. Shortliffe, "The Dempster-Shafer theory of evidence," in Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project 3, Reading, MA: Addison-Wesley, 1984, ch. 13, pp. 832–838.

[14] I. Ruthven and M. Lalmas, "Using Dempster-Shafer's theory of evidence to combine aspects of information use," J. Intell. Inf. Syst., vol. 19, no. 3, pp. 267–301, Nov. 2002.

[15] A. Jøsang and R. Ismail, "The beta reputation system," in Proc. 15th Bled Electron. Commerce Conf., 2002, pp. 41–55.

[16] K. Buck and D. Hanf. (2010, Sep.). Cloud SLA consideration for government consumer, System Eng. Mitre, Bedford, MA, Tech. Rep. Case: 10-2902 [Online]. Available: http://www.mitre.org/work/tech_papers/2010/10_2902/

[17] Cloud computing use cases white paper - Version 4.0. (2010, Jul.).[Online]. Available: http://opencloudmanifesto.org/Cloud_-Computing_Use_Cases_Whitepaper–4_0 .pdf

[18] I. Brandic, V. C. Emeakaroha, M. Maurer, S. Dustdar, S. Acs, A.Kertesz, and G. Kecskemeti, "LAYSI-A layered approach for SLAviolation propagation in self-manageable cloud infrastructures,"in Proc. 34th IEEE Annu. Comput. Softw. Appl. Conf. Workshops, Jul.2010, pp. 365–370.

[19] V. C. Emeakaroha, I. Brandic, M. Maurer, and S. Dustder, "Low level metrics to high level SLAs-LoM2HiS framework: Bridging the gap between monitored metrics and SLA parameters in cloud environments," in Proc. Int. Conf. High-Perform. Comput. Simul., Jun. 28–Jul. 2, 2010, pp. 48–54.

[20] G. S. Machado and B. Stiller, "Investigation of an SLA support system for cloud computing (SLACC)," PIK (Praxis der Informations verarbeitung und Kommunikation), vol. 34, no. 2, pp. 80–86, Jun. 2011.