INTERNATIONAL JOURNAL OF MERGING TECHNOLOGY AND ADVANCED RESEARCH IN COMPUTING

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

ISSN: 2320-1363

A Framework to Facilitate Selection of Enhanced Multi Cloud Service Providers

P. Suresh Babu
MTech(SE)
SLC's Institute of Engineering and Technology

Adavelli ramesh$_{Mtech}$
Assoc. Prof Dep. of computer Science
Email Ramesh.adavalli@gmail.com
SLC's Institute of Engineering and Technology

Soma Preethi $_{Mtech}$
Asst. Prof Dep. of computer Science
SLC's Institute of Engineering and Technology.

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.

Key words

Cloud Computing, Services Quality, CSP, SelCSP, ESELSP, SLAs.

I. Objectives

I. Support for customer-driven service management based on customer profiles and QoS requirements;
II. 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;
III. 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;
IV. Incorporation of autonomic resource management models that effectively self-manage changes in service requirements to satisfy both new service demands and existing service obligations;
V. Leverage of Virtual Machine (VM) technology to dynamically assign resource shares according to service requirements;
VI. Implementation of the developed resource management strategies and models into a real computing server in an operational data center.

II. 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.

III. Review of Literature

1. Related Work

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. 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.

D. A Trust-Evaluation Metric for Cloud Applications

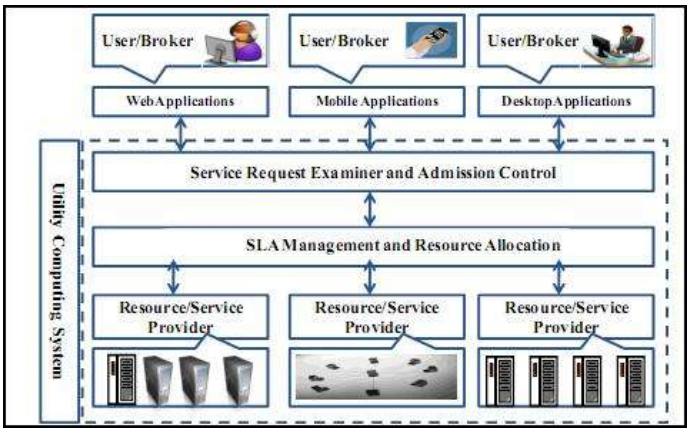
In this paper, the authors stated that Cloud services are becoming popular in terms of distributed technology because they allow cloud users to rent well-specified resources of computing, network, and storage infrastructure. Users pay for their use of services without needing to spend massive amounts 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.

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:

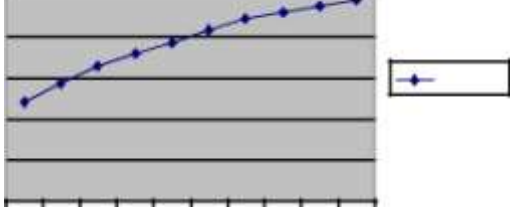
- Enhanced customer satisfaction level: A clearly and concisely defined SLA increases the customer satisfaction level, as it helps providers to focus on the customer requirements and ensures that the effort is put on the right direction.
- Improved Service Quality: Each item in an SLA corresponds to 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.

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

Table 1.2 Selection Cloud Services Provider- Ratio Analysis

S.NO	NUMBER OF TIME SLOT (M)	RATIO OF SELECTION CSP
1	10	0.43
2	20	0.52
3	40	0.61
4	60	0.69

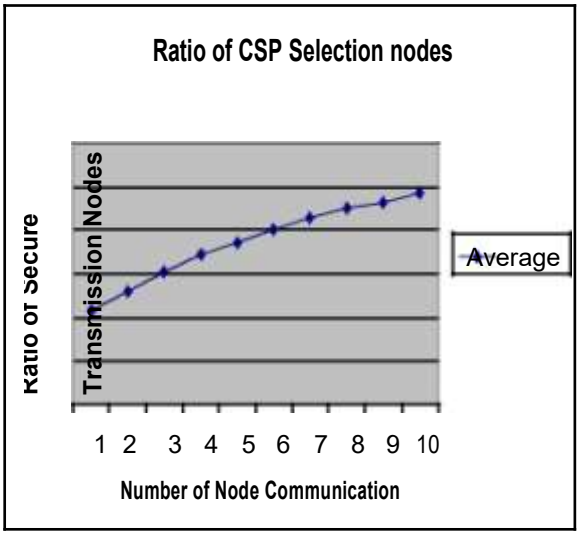


Number of Node Communication

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.

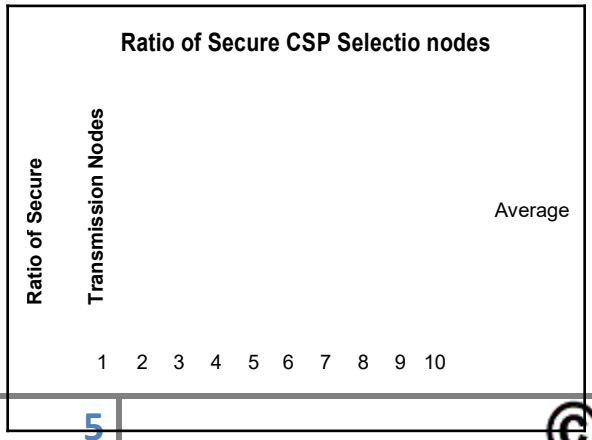
5	80	0.74
6	100	0.80



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 table contains number of time slot interval and given time interval to calculate average numbers of send transmission node details are shown



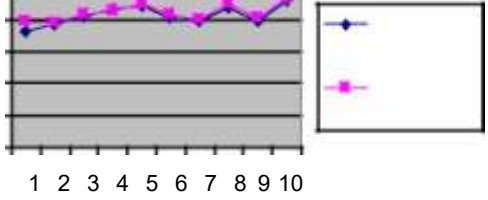
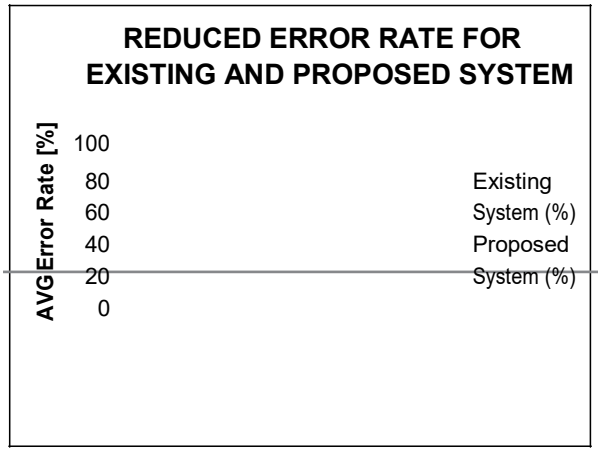


Fig 1.6 : Reduced Error Rate For Existing And Proposed System

Table 1.5 : Reduced Error Rate For Existing And Proposed System

Member Node	Existing System (%)	Proposed System (%)
8	72.54	78.62
12	76.13	78.11
16	82.42	83.13
24	86.66	84.67
30	88.13	89.78
32	80.44	82.66

The following **Figure 1.6** describes experimental result for proposed system error rate analysis. The table contains average cloud services provider and average percentages for existing and proposed system in cloud environment detection are shown.



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] *W. Li and L. Ping, "Trust model to enhance security and interoperability of cloud environment," in Proc. 1st Int. Conf. Cloud Comput., 2009, vol. 5931, pp. 69–79.*

[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.*