International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2763
Issue 04, Volume 3 (April 2016) SPECIAL ISSUE www.ijirae.com

ANALYSIS OF MULTI APPLICATION SERVICE PROVIDER SELECTION FRAMEWORK USING SELCSP IN CLOUD ENVIRONMENT

B.NANDHINI
II-ME(CSE)
Department of Computer Science and Engineering,
Sengunthar College of Engineering,
Tirunchengode – 637 205

Mr. O.K. GOWRISHANKAR,
Assistant Professor,
Department of Computer Science and Engineering,
Sengunthar College of Engineering,
Tirunchengode – 637 205

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

INTRODUCTION

Service level agreements (SLAs) are one of the major considerations for every buyer of cloud computing services. The question often asked is how many nines of availability a given provider guarantees. Cloud-based services are increasingly becoming commonplace. These services include infrastructure as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Each service is typically accompanied by a service level agreement (SLA) which defines the minimal guarantees that a provider offers to its customers. The lack of standardization in cloud-based services implies a corresponding lack of clarity in the service level agreements offered by different providers.

Cloud Service Level Agreements (Cloud SLAs) form an important component of the contractual relationship between a cloud service customer and a cloud service provider of a cloud service. Given the global nature of the cloud, SLAs usually span many jurisdictions, with often varying applicable legal requirements, in particular with respect to the protection of the personal data hosted in the cloud service. Furthermore different cloud services and deployment models will require different approaches to SLAs, adding to the complexity of SLAs. Finally, SLA terminology today often differs from one cloud service provider to another, making it difficult for cloud service customers to compare cloud services. For the avoidance of doubt, this document does not address consumers as being cloud service customers. Standardizing aspects of SLAs improves the clarity and increases the understanding of SLAs for cloud services in the market, in particular by highlighting and providing information on the concepts usually covered by SLAs. The main objective of the paper following ways,

- *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; and*
- *Implementation of the developed resource management strategies and models into a real computing server in an operational data center.*

RELATED WORKS

In this paper [1], the authors 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. The SECURE project [17] analyses a notion of trust that is "inherently linked to risk". Risk is evaluated on every possible outcome of a particular action and is represented as a family of cost-PDFs (Probability Density Function) parameterized by the outcome's intrinsic cost. The considered action is then analysed by a trust engine to compute multidimensional trust information which is then used by a risk engine to select one cost-PDF. The decision to take the action is then made by applying a user-defined policy to select one of the possible outcomes' cost-PDFs.

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 natural side effect is that it also provides an incentive for good behavior, and therefore tends to have a positive effect on market quality. Reputation systems can be called collaborative sanctioning systems to reflect their collaborative nature, and are related to collaborative filtering systems. Reputation systems are already being used in successful commercial online applications. 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. Cloud computing paradigm is set to become the next explosive revolution on the Internet, but its adoption is still hindered by security problems. One of the fundamental issues is the need for better access control and identity management systems. In this context, Federated Identity Management (FIM) is identified by researchers and experts as an important security enabler, since it will play a vital role in allowing the global scalability that is required for the successful implantation of cloud technologies. However, current FIM frameworks are limited by the complexity of the underlying trust models that need to be put in place before inter-domain cooperation. Thus, the establishment of dynamic federations between the different cloud actors is still a major research challenge that remains unsolved

1. EXISTING SYSTEM

The existing system 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 satisfied 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.*

DRAWBACKS

- *It does not aim at using this risk-based provider selection.*
- *It does not ensure secure multi-domain collaboration in cloud.*
- *It does not compare the new coming cloud service providers with existing cloud providers.*

2. PROPOSED SYSTEM

The proposed system includes all the existing system approach which covers multiple cloud service provider environments. In addition, the framework estimates trust-worthiness in terms of context-specific, 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.

ADVANTAGES

The proposed system has following advantages.

- ***Level of uptime****: describes the time in a defined period th service was available, over the total possible available time, expressed as a percentage.*
- ***Percentage of successful requests****: describes the number of requests processed by the service without an error over the total number of submitted requests, expressed as a percentage.*
- ***Percentage of timely service provisioning requests****: describes the number of service provisioning requests completed within a defined time period over the total number of service provisioning requests, expressed as a percentage.*
- ***Average response time****: refers to the statistical mean over a set of cloud service response time observations for a particular form of request.*
- ***Maximum response time:*** *refers to the maximum response time target for a given particular form of request.*
- ***Maximum resource capacity:*** *refers to the maximum amount of a given resource available to an instance of the cloud service for a particular cloud service customer. Example resources include data storage, memory, number of CPU cores.*
- *It compares the new coming cloud service providers with existing cloud providers.*

ESELCSP FRAME WORK

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;

- ***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 customerCSP 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 satisfied 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.*

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.*

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 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 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.
[11]. D. H. McKnight and N. L. Chervany. The Meanings of Trust. Technical Report MISRC Working Paper Series 96-04, University of Minnesota, Management Information Systems Reseach Center, 1996. http://www.misrc.umn.edu/wpaper/wp96-04.htm.

