International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume III, Issue V, May- 2016

IMPROVING SELECTIVE CSP FRAMEWORK FOR CLOUD SERVICE USING MULTIFACTORY ANALYSIS MODEL

A.Revathi
Department of Computer Science and Engineering
SSM College of Engineering, Komarapalayam,
Tamil Nadu, India
aarthiit21@*gmail.com*

K.Mahalakshmi
Department of Computer Science and Engineering
SSM College of Engineering, Komarapalayam
Tamil Nadu, India
vimalananthis@yahoo.com

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.

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

I-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 awys, 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.

II-RELATED WORKS

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 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. the authors 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 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 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.

In this paper [4[, the authors stated that the 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.

III- 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. Trust worthiness 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.

IV- 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. Level of uptime describes the time in a defined period the 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**.**

V-MODULE DESCRIPTION

1) RISK ESTIMATION. This module estimates perceived interaction risk relevant to a customer-CSP interaction by combining trustworthiness and competence. Risk is defined as a function of the likelihood of a given threat-source's exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization. Relational risk and performance risk is taken into account. Relational risk in any alliance increases if one of the partners finds it difficult to protect its proprietary resources from others. In contrast, performance risk related to multi-party cooperation becomes high, if the consumer agent expects higher return on investment (or utility) from non-recoverable investments made towards an alliance with strategic objectives. A customer's trust on a service providing agent reduces former's perceived relational risk in an interaction.

It is observed that decision-makers use potential gains and losses to estimate risk, which

implies that a higher non-recoverable investment leads to the perception of higher performance risk.

Proposition 2 Perceived performance risk in an interaction will be reduced if competence of service providing agent is high. Competence of a cooperating agent gives a sense of confidence that the partner firm is capable of accomplishing a given task successfully.

$$\mathcal{R}_r(c_j, p_k) \propto \frac{1}{\mathcal{T}(c_j, p_k)}, \quad (1)$$

Similarly, Proposition 2 is as follows:

$$\mathcal{R}_p(c_j, p_k) \propto \frac{1}{\mathcal{C}(p_k)}, \quad (2)$$

where Cpk is the competence of provider pk.

From Equations (1) and (2), the risk is modeled as

$$\mathcal{R}(c_j, p_k) = \kappa_1 . \frac{1}{\mathcal{T}(c_j, p_k)} + \kappa_2 . \frac{1}{\mathcal{C}(p_k)}, \quad (3)$$

where K1 and K2 are proportionality constants.

2) TRUST ESTIMATION This module computes trust between a customer-CSP pair provided direct interaction has occurred between them.

A history of trust values is maintained and Interaction matrix is calculated. Interactions in a cloud environment with P service providers over A contexts is represented in a matrix I, where any element □cj (pk, □i) indicates the expected degree of trust that the customer cj has on provider pk with respect to context □i. If there is no interaction with a provider on a particular context, it is indicated by -∞.

Interaction matrix for customer c is given as:

$$I_{|P|\times|A|}(c_j) = \begin{bmatrix} \mu_{1,1} & \mu_{1,2} & \cdots & \mu_{1,|A|} \\ \mu_{2,1} & \mu_{2,2} & \cdots & \mu_{2,|A|} \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{|P|,1} & \mu_{|P|,2} & \cdots & \mu_{|P|,|A|} \end{bmatrix}$$

Each element in matrix I is computed from ratings given in history of interaction H. Trust ratings in H occur in increasing order of recency.

The general trust vector for provider pk P from customer cj's perspective is a mean of expected trust degrees acquired for different contexts

$$\mathcal{G}^{\tau}(c_j, p_k) = \begin{cases} \frac{1}{|A|} \sum_{\alpha_i \in A} \mu_{c_j}(p_k, \alpha_i) & \text{if } C1 \text{ is true} \\ -\infty & \text{otherwise,} \end{cases}$$

where, | A | is the number of contexts on which interactions have been observed.

3) REPUTATION ESTIMATION. It evaluates reputation of a CSP based on referrals/feedbacks from various sources and computes the belief a customer has on former's reputation. Reputation model comes into effect when customer cj has not interacted with provider pk on current context in the past. Under this situation, cj has to believe in feedbacks/referrals from other customers who have directly interacted with pk. A history of trust values is maintained here also.

4) 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.

5) COMPETENCE ESTIMATION AND COMPUTATION. It estimates competence of a CSP based on the information available from its SLA. It also computes transparency with respect to a given SLA and hence evaluates the competence of the CSP. It is based on the following aspect. Given a customer cj that wants to make decision regarding initiation of an interaction with a service provider pk, a trust and competence-based risk estimator TCRISK is a seven-tuple TCRISK {□ □ □I , U , T,C , ϕ, R) , where,

□ is the current context of interaction,

I is the importance of the context subjective to cj,

U is the utility expected to be gained on context a by cj,

T is the degree of trustworthiness obtained by cj towards pk on context □, [Here Gt (Module 2) is used instead of T which is taken for sake of convenience].

C is competence of pk with respect to present SLA ϕ, and

R is a function to evaluate the perceived interaction risk associated with pk over context □.

VI-IMPLEMENTATION

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 organization. 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.

Algortihm

SLA-oriented Dynamic Provisioning
When a task finishes or a new job is received:
Updates estimation of task runtime;
Defines estimated job completion time with current amount of resources;
If completion time > deadline
Determines number of extra resources required
Submits a request for resources to the Provisionary
Else
If resources can be released
Submits request for release of resources to the Provisioner

SLAs are defined in terms of deadline for execution of applications. The deadline, along with an estimation of execution time of each task of the application is supplied by the user during a job submission. This process is briefly described proposed algorithm.

VII-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.

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.

VII- REFERENCES

[1] Arias-Cabarcos P. and anchez-Guerrero R.D. ,(2010)"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, vol. 6, pp. 2843–2848.

[2] Dillon.T, WuChang.E (April 2010) "Cloud Computing: Issues and Challenges"In: Proc. of AINA 2010, Perth, Australia .

[3] Falcone.R and Castelfranchi.C Social Trust(2001)"A Cognitive Approach", pages 55–99. Kluwer.

[4] Hardjono.T, Rutkowski.M(2011)(eds.)"Identity in the Cloud—Use Cases Version 1.0,DraftVersion0.1q".http://docs.oasis-open.org/id-cloud/IDCloud usecases/v1.0/IDCloud-usecases-v1.0.pdf .

[5] Hoffman.K.,Zage.D.,Nita-Rotaru.C(2009)"A Survey of Attack and Defense Techniques for Reputation Systems". ACM Computing Surveys 42(1), 1–31.

[6] Jøsang.A,Ismail.Rand Boyd.C,(Mar. 2007)"A survey of trust and reputation systems for online service provision," Decision Support Sys., vol. 43, no. 2, pp. 618–644.

[7] Mui.L,Halberstadt.A, and M.Mohtashemi (July 2002)Notions of Reputation in Multi-agent Systems: A Review. In Proceedings of the First Int. Joint Conference on Autonomous Agents &Multiagent Systems (AAMAS).

[8] Noor.T and Sheng.Q (2011)"Trust as a service: A framework for trust management in cloud environments," in Proc. 12th Int. Conf. Web Inf. Syst. Eng.,pp. 314–321.