Trust Assessment Using Cloud Broker

Pramod Pawar, Muttukrishnan Rajarajan, Theo Dimitrakos, Andrea Zisman

Trust Assessment Using Cloud Broker

Pramod S. Pawar[1,2], Muttukrishnan Rajarajan[1], Theo Dimitrakos[2], Andrea Zisman[3]

[1] City University London, London EC1V 0HB, United Kingdom
r.muttukrishnan@city.ac.uk
[2] British Telecommunications, Adastral Park, Ipswich IP5 3RE, United Kingdom
{pramod.s.pawar, theo.dimitrakos}@bt.com
[3]The Open University, Walton Hall,Milton Keynes MK7 6AA, UK
andrea.zisman@open.ac.uk

Abstract. Despite the advantages and rapid growth of Cloud computing, the cloud environments are still not sufficiently trustworthy from a customer's perspective. Several challenges such as specification of service level agreements, standards, security measures, selection of service providers and computation of trust still persists, that concerns the customer. To deal with these challenges and provide a trustworthy environment, a mediation layer may be essential. In this paper we propose a cloud broker as a mediation layer, to deal with complex decision of selecting a trustworthy cloud provider, that fulfils the service requirements, create agreements and also provisions security. The cloud broker operates in different modes and this enables a variety of trust assessments.

Keywords: cloud trust, cloud broker, multi-cloud, reputation

1 Introduction

Despite the advantages and rapid growth of cloud computing, most organizations still continue with their concerns about trust and security of cloud providers. Several challenges [1] such as specification of SLAs, standards, security measures, selection of service providers and computation of trust still persists, implying that the cloud environments are still not sufficiently trustworthy from customer's perspective. To deal with the challenge of identifying dependable cloud service providers for the service, cloud marketplaces are gaining popularity and allow consumers to select providers that best match their requirements. However, their complex requirements and the numerous choices available to the consumer make it difficult to decide on a provider to host their service. In addition, their concern about the trustworthiness of the providers remains unanswered. The cloud characteristics [2] such as elasticity and the complex deployment models like multi-cloud and federated clouds create major challenges in trust assessment of cloud providers. A unanimous trust assessment across all deployment architecture may not be suitable, this creates a compelling requirement to have a suitable separate trust assessment for every deployment architecture.

The assessment of the cloud computing environment leads to crucial requirements which are essential to evaluate the cloud provider's trustworthiness and they are: a)

An independent mediation layer capable of performing variety of trust assessment to evaluate the cloud providers b) An evaluation framework that is trusted enough such that malicious providers cannot manipulate the evaluation process c) An evaluation of cloud providers based on fine-grained QoS parameters together with consumer feedbacks, recommendations and additional distinguishing parameters that relate to the cloud computing environments [1]. Due to the complexity of service requirements and difficulty of trustworthiness evaluation of the cloud providers, third parties like cloud brokers can play an important role to assist the consumer in selecting an appropriate provider and also assist in deployment of the service.

The work presented in this paper was developed under the FP7 EU-funded project called OPTIMIS [3]. This paper, proposes the trust evaluation of the cloud providers with the use of OPTIMIS Cloud Broker (CBR) as a mediation layer. As a first step towards integration of trust and reputation systems in cloud environment, a set of parameters beyond QoS are identified that includes: SLA, Compliance, interoperability, geographical location of data centers, deployment models, security measures, user recommendations and feedbacks[1]. The trust model[4], [5] cohesively works with the cloud broker in different modes using SLA and cloud characteristic parameters for evaluating the trustworthiness of the providers, and is robust against malicious group of entities performing reputation based attacks. The OPTIMIS cloud broker supports SLA, compliance with data protection and locations, multi-cloud and federated cloud deployments, security as value additions and integrates trust model enabled with SLA monitoring and user ratings in terms of feedback for the service used.

The remaining paper is structured as follows. Section 2 describes the different modes of operation of cloud broker. Section 3 describes type of trust in each of the cloud broker modes. Section 4 provides trust evaluation using cloud broker. Section 5 provides the related work and finally, section 6 provides the concluding remarks.

2 Cloud Broker Service

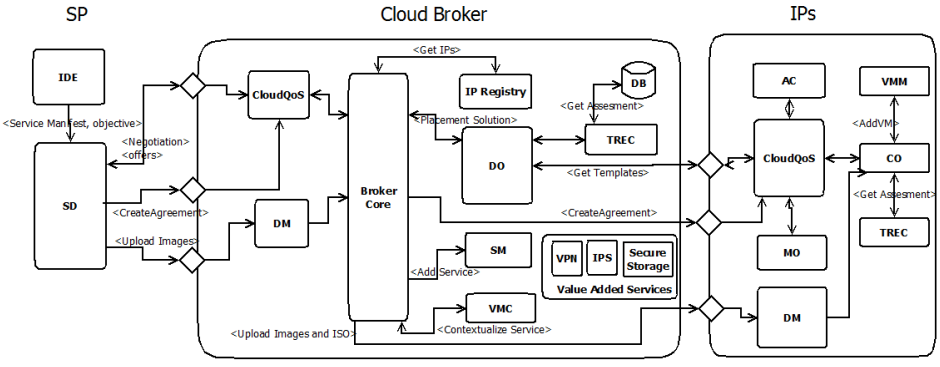

Fig. 1. High level component architecture of the Cloud Broker

This paper considers the OPTIMIS Cloud Broker (CBR) [3] for assessing trust of the Infrastructure Providers(IP). The OPTIMIS Cloud Broker (CBR) as shown in **Fig. 1** has architecture that enables multi-cloud deployment, provisions value added service

for the consumer's service deployed via cloud broker and also performs Trust, Risk, Eco-efficiency and Cost (TREC) assessment. Details of the components and the multi-cloud deployment process is available from the OPTIMIS toolkit website[6].

2.1 Cloud broker modes of operation

The OPTIMIS cloud broker has the capability to operate in four different modes: a) *cloud service recommendation* b) *cloud service intermediation* c) *cloud service aggregation* and d) *cloud service arbitrage.* Cloud broker used in *cloud service recommendation* mode enables the user to get recommendations from the cloud broker about the most suitable cloud infrastructure provider for hosting their service, based on the degree of Trust, Risk, Eco-efficiency and Cost (TREC). The cloud broker as a *recommender* reduces the effort from the consumer to identify a suitable cloud service provider for its service. However the actual deployment of the service to the cloud infrastructure is performed by the consumer after obtaining deployment solution from the cloud broker. Cloud broker used as *cloud service intermediation* provides management functionalities like *Value Added Services (VAS)* that are cloud provider specific, which may be essential for the consumer's service that is deployed in the cloud provider environment. As an *intermediary*, the cloud broker also takes complete responsibility of the consumer's/user's services to identify the most suitable IP based on TREC, then performs the deployment on the selected IP, and then manages smooth functioning of the service during its operational stage. The use of cloud broker as *cloud service aggregation* provides management functionalities for *multi-cloud* deployment and operation of a service by combining services from multiple cloud infrastructure providers. The cloud broker also provides VASs that are independent of cloud providers. Cloud broker used as *cloud service arbitrage* can be considered as dynamic aggregation wherein the multi-cloud deployment of consumer service is dynamically decided based on the service requirements. In this mode of operation, the cloud broker system decomposes the service requirements at component level and negotiates with multiple cloud providers for each of the service components to formulate an optimized deployment solution taking into account the basic service requirements as well as additional requirements such as TREC, compliance and security.

3 Trust Assessment using Cloud Broker

This section describes the trust assessments performed using the different modes of cloud broker. **Table 1** summarizes the feature provided by cloud broker in different modes of operation. Analysis of the summary information reveals that cloud broker in *cloud service recommendation* mode is only responsible to provide the deployment solution which determines that a standard trust model with cloud specific characteristics is sufficient for trust assessment of the cloud providers. Cloud broker as *cloud service intermediation* additionally provides value added services like security service and as for a comprehensive trust assessment it is essential to evaluate security reputation of the cloud provider. The cloud broker as *cloud service aggregation/arbitration* additionally provides support for multi-cloud deployment that compels the requirement of trust assessment for a group of cloud providers.

	Deployment Solution	Deployment of Service	Provider specific VAS	Provider Independent VAS	Static Multi-cloud deployment	Dynamic multi-cloud
Recommender	X					
Intermediary	X	X	X			
Aggregator	X	X	X	X	X	
Arbitrage	X	X	X	X	X	X

Table 1. Features for cloud broker used in different modes

3.1 Cloud broker as cloud service recommendation

In this mode of operation the consumer interacts with cloud broker only for getting the deployment solution to identify the trustworhty cloud providers and takes the responsibility of deployment. In this mode the cloud broker uses the trust model as proposed in Pawar et al.[4], [7]. The *Trustworthiness* of an cloud Infrastructure Provider (IP) is modelled using *opinion* obtained from three different computations, namely (i) *compliance of SLA parameters (SLA monitoring),* (ii) *service provider satisfaction ratings (SP ratings)*, and (iii) *service provider behaviour (SP behaviour).* The SP behaviour is defined in terms of the credibility [16] for each of the SP based on the feedback provided. In addition to the credibility, the trust model is complimented with early filtering to reduce the impact of malicious feedback providers [7]. The cloud broker uses this trust model to provide recommendations about the cloud providers. The *trustworthiness (T)* of an IP is modelled as below:

$$T=\text{Expectation}\ (W_{(SPB \otimes SPR)\wedge SLA}) \tag{1}$$

$$W_{(SPB \otimes SPR) \wedge SLA}=(W_{SPB} \otimes W_{SPR}) \wedge W_{SLA} \tag{2}$$

where $W_{SLA,}$ W_{SPR}, W_{SPB} are opinions obtained from the SLA monitoring (SLA), SP ratings (SPR), and SP behavior (SPB) values, respectively. The symbol $\wedge$ is the *conjunction operator* used to combine the opinions, and $\otimes$ is the *discounting operator* used as the recommendation operator.

3.2 Cloud broker as cloud service intermediation

The cloud broker in the intermediary mode of operation, have capabilities to provision value added services such as security services. In this mode, the cloud broker inherits and expands on the role of security auditor, enabling the cloud broker to obtain access to security events due to the high value of trust placed, which may not be possible with the wider community. The cloud broker provisions the consumers with security reputation of cloud IP based on their security requirements. The reputation of a cloud IP [5] is calculated in terms of its *trustworthiness(T)* using opinion obtained from computations, namely i) *Incidence Monitoring(M)*: Security incedence events

received from monitoring ii) *Enterprise User Rating(EUR)*: Ratings provided by the enterprise user for satisfaction of the security features provided by cloud service providers. The *trustworthiness (T)* of cloud IP is given as:

$$T = \text{Expectation}\ (W_M\ \Lambda\ W_{EUR}) = \text{Expectation}\ (W_{M\ \Lambda\ EUR}) \quad (3)$$

Where $W_{M\ \Lambda\ EUR} = (b_{M\ \Lambda\ EUR}, d_{M\ \Lambda\ EUR}, u_{M\ \Lambda\ EUR}, a_{M\ \Lambda\ EUR})$.

3.3 Cloud broker as cloud service aggregation/arbitration

The cloud broker used as *cloud service aggregation/arbitration* is capable of devising multi-cloud deployment solution based on user requirements. This enables the cloud broker to perform trust assessment for a group of providers. Consider that the deployment solution provided contains two target cloud providers. Let T_1 and T_2 be the trust computed for the first and the second cloud provider. The individual trustworthiness T_1 and T_2, of the cloud provider are computed based on the parameters, *SLA monitoring*, *SP rating* and *SP behavior*, as described in Section 3.1. The global trust or the group trust for the cloud provider computed by the broker is as follows:

$$T_{12} = (W_1/(W_1 + W_2))\ T_1\ +\ (W_2/(W_1 + W_2))\ T_2 \quad (4)$$

Where W1 and W_2 are weights assigned for trust computed for each of the cloud providers such that $W1 + W_2 = 1$.

4 Evaluation

This section evaluates the trust assessment performed using cloud broker as a cloud service recommendation. The Trust model is evaluated using a simulation with a typical simulation run of 250 iterations, a total of 100 SP nodes and one cloud broker node trying to evaluate a single IP. This paper uses categorized groups of malicious feedback provider and two metrics as considered as in [8]. The malicious groups are: *complementary*, *exaggerated positive* and *exaggerated negative*. The SP nodes are tagged with one of the four categories: normal group (G1), exaggerated positive group (G2), exaggerated negative group (G3) and complementary group (G4). The experiments use different ratios G1:G2:G3:G4 of SP nodes. The remaining section is as follows: Section 4.1 demonstrates the trust model robustness due to credibility use in trust model. Section 4.2 demonstrates sensitivity of the model to uncertainty.

4.1 Average credibility decreases with time

The purpose of the credibility parameter is to ensure that the feedback provided by malicious nodes be weighted less to reduce the influence of malicious nodes and thus to correctly model the reputation of the trustee. In this experiment, the ratio of nodes G1:G2:G3:G4 is given as 70:10:10:10. After the cloud broker node performing transaction with the IP, it computes difference between the feedback provided and the real QoS provided by the IP. This enables cloud broker to compute the current credibility of feedback providers i.e. SPs. In each iteration, credibility of SPs are updated con-

sidering its previous credibility and then the average credibility is computed for each group G1, G2, G3 and G4. The result in **Fig. 2** shows that the average credibility for the malicious node groups G2, G3 and G4 decreases drastically within a few iterations and then remains low throughout rest of the iterations. This result indicates that malicious node achieve low credibility with time and that the feedbacks provided by the malicious nodes will have a low influence on the reputation computation since the feedbacks provided by these malicious nodes are weighted less.

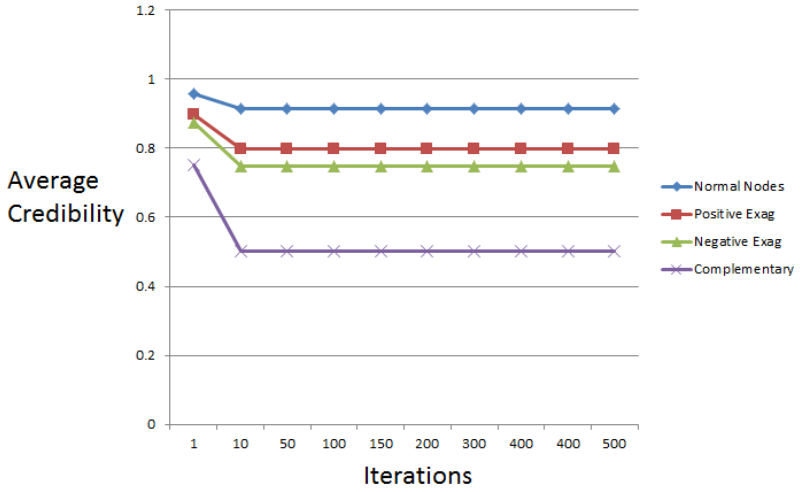

Fig. 2. : Average Credibility for different groups of SPs. G1:G2:G3:G4 is 70:10:10:10

4.2 Sensitivity to uncertainty

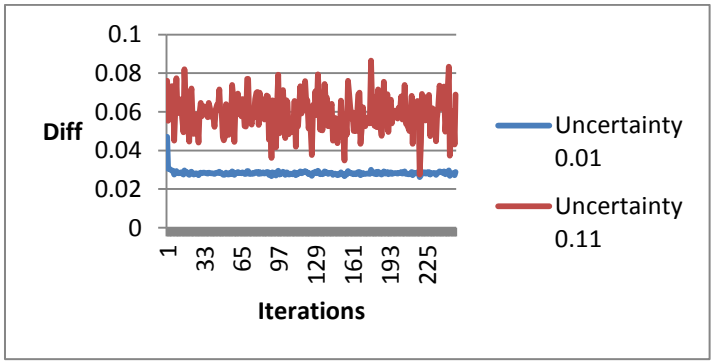

Fig. 3. : Diff for different levels of uncertainty by the feedback providers

It is important to consider the feedback providers confidence in their feedback about trustee. The aim of this experiment is to check if the confidence value of the feedback

provider has any impact on robustness of the model. For this experiment, keeping the reliability trust provided by feedback provider constant, it is executed for two cases of uncertainty for the feedback provided. In the first case a high uncertainty is maintained as u=0.11, while for the second case the uncertainty is reduced to 0.01. In both cases the malicious nodes ratio of 70:30:0:0 is considered for the experiment. It is observed from **Fig. 3** that the trust model is sensitive to uncertainty in the feedback value provided. Smaller the uncertainty, the corresponding *diff* value would be small. This result validates that with increase in evidence available, uncertainty in the feedback value reduces and the system robustness increases.

5 Related Work

Trust and reputation have been the focus of research for several open systems and the rapidly growing cloud computing technology also appreciates the importance of trust in the cloud computing environment. This is partially observed through the trust and reputation systems that have being discussed in [3], [4], [7], [9]. In OPTIMIS [3], trust is one of the core component used by SP, along with risk, eco-efficiency and cost for evaluating the IP for their service. Alhamad *et al*. [9] proposes a trust model for cloud computing based on the usage of SLA information and provides a high level architecture capturing major functionalities required. Pawar et al.[4][7] include SLA compliance information to model trust and also proposed a trust model based on cloud characteristics supported with credibility and early filtering mechanism to reduce the impact of malicious feedback providers. Significant research exists in the area of brokers used in various areas of computer science. Cloud brokers [1], [10] are also gaining popularity to identify dependable cloud service providers. The importance of cloud brokerage is also emphasized by Gartner research [11], which defines different types of brokerage. In line with Gartner research [11], Nair et al.[10] propose the use of cloud broker as 1) *cloud service intermediation* 2) *cloud service aggregation* and 3) *cloud service arbitrage* and provide an abstract architecture for the brokerage. The OPTIMIS cloud broker architecture, is in line with the concepts defined in [10] and [11]. In addition, it supports trust assessment, matching of consumer requirements, establishing agreements and also provides value added services such as security.

6 Conclusion and Final Remark

This paper communicates that a unanimous trust assessment across the cloud computing environment may not be suitable and exploits the use of OPTIMIS cloud broker and its various modes to perform variety of trust evaluations of the cloud providers. This paper uses the opinion based trust model to perform trust assessment of cloud providers to provide recommendations, security reputation and a group reputation in the different modes of cloud broker. The paper provides evaluation results for the trust assessment performed by the cloud broker in the recommendation mode and reserves the evaluation of the security reputation and group reputation as future work.

Acknowledgement

This work has been partially supported by the EU within the 7th Framework Programme under contract ICT-257115 - Optimized Infrastructure Services (OPTIMIS).

References

1. S. M. Habib, S. Ries, and M. Muhlhauser, "Cloud Computing Landscape and Research Challenges Regarding Trust and Reputation," 2010, pp. 410–415.
2. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *Httpcsrcnistgovpublicationsnistpubs800-145SP800-145pdf*, Sep. 2011.
3. A. J. Ferrer, F. Hernández, J. Tordsson, E. Elmroth, A. Ali-Eldin, C. Zsigri, R. Sirvent, J. Guitart, R. M. Badia, K. Djemame, W. Ziegler, T. Dimitrakos, S. K. Nair, G. Kousiouris, K. Konstanteli, T. Varvarigou, B. Hudzia, A. Kipp, S. Wesner, M. Corrales, N. Forgó, T. Sharif, and C. Sheridan, "OPTIMIS: A holistic approach to cloud service provisioning," *Future Gener. Comput. Syst.*, vol. 28, no. 1, pp. 66–77, Jan. 2012.
4. P. S. Pawar, M. Rajarajan, S. K. Nair, and A. Zisman, "Trust Model for Optimized Cloud Services," in *Trust Management VI*, vol. 374, T. Dimitrakos, R. Moona, D. Patel, and D. H. McKnight, Eds. Springer Berlin Heidelberg, 2012, pp. 97–112.
5. P. S. Pawar, S. K. Nair, F. El-Mousaa, T. Dimitrakos, M. Rajarajan, and A. Zisman, "Opinion Model Based Security Reputation Enabling Cloud Broker Architecture," presented at the CloudComp 2012 - 3rd International Conference on Cloud Computing, Vienna, Austria, 2012.
6. "OPTIMIS Toolkit | Home - Cloud, but better." [Online]. Available: http://www.optimistoolkit.com/. [Accessed: 15-Apr-2014].
7. P. S. Pawar, M. Rajarajan, T. Dimitrakos, and A. Zisman, "Trust Model for Cloud Based on Cloud Characteristics," in *Trust Management VII*, Springer, 2013, pp. 239–246.
8. C. Jia, L. Xie, X. Gan, W. Liu, and Z. Han, "A Trust and Reputation Model Considering Overall Peer Consulting Distribution," *IEEE Trans. Syst. Man Cybern. Part Syst. Hum.*, vol. 42, no. 1, pp. 164–177, 2012.
9. M. Alhamad, T. Dillon, and E. Chang, "SLA-Based Trust Model for Cloud Computing," in *2010 13th International Conference on Network-Based Information Systems (NBiS)*, 2010, pp. 321–324.
10. S. K. Nair, S. Porwal, T. Dimitrakos, A. J. Ferrer, J. Tordsson, T. Sharif, C. Sheridan, M. Rajarajan, and A. U. Khan, "Towards Secure Cloud Bursting, Brokerage and Aggregation," in *2010 IEEE 8th European Conference on Web Services (ECOWS)*, 2010, pp. 189–196.
11. Gartner, "Cloud Services Brokerage: The Dawn of the Next Intermediation Age." .