HAL open science

Trust Model for Cloud Based on Cloud Characteristics

Pramod S. Pawar, Muttukrishnan Rajarajan, Theo Dimitrakos, Andrea Zisman

To cite this version:

Pramod S. Pawar, Muttukrishnan Rajarajan, Theo Dimitrakos, Andrea Zisman. Trust Model for Cloud Based on Cloud Characteristics. 7th Trust Management (TM), Jun 2013, Malaga, Spain. pp.239-246, 10.1007/978-3-642-38323-6_18 . hal-01468175

HAL Id: hal-01468175

https://inria.hal.science/hal-01468175

Submitted on 15 Feb 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Trust Model for Cloud Based On Cloud Characteristics

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

[1] City University London, London EC1V 0HB, United Kingdom
r.muttukrishnan@city.ac.uk, a.zisman@soi.city.ac.uk
[2] British Telecommunications, Adastral Park, Ipswich IP5 3RE, United Kingdom
{pramod.s.pawar, theo.dimitrakos}@bt.com

Abstract: The wider adoption of cloud computing due to its inherent advantages also brings concerns of trust and security. Trust is a fundmental subject in human life. Although, several trust models exists in different areas including cloud, none of the trust models to-date are comprehensive enough to accommodate the characteristics of the cloud environment. This paper defines a trust model based on the essential cloud characteristics as the dimensions of the trust model together with several features relevant to the dimension to build the context. The proposed trust model is supported with an opinion model that considers uncertainty for building context specific trust and credibility complimented with early filtering to reduce the impact of malicous feedback providers. The proposed model is evaluated for its robustness against malicious feedback providers.

Keywords: Trust, Cloud characteristics, credibility, unfair ratings

1 Introduction

Cloud computing provides multi-fold advantages of sharing resources, unlimited scalability and flexibility and on-demand resources. With huge number of cloud service providers available in the market, it is challenging for the consumers/service providers to decide which cloud infrastructure provider will be trustworthy for their services to be deployed in the cloud environment. Trust being a fundamental subject, several trust model exist to date in different areas. However, cloud being the recent advancement in computing a very few trust models exists with none being comprehensive enough to accommodate the scope of the cloud [1] [13].

The scope and focus of this paper is mainly to evaluate the trustworthiness of the Infrastructure Provider (IP) performed by the Cloud Broker (CBR). The trust model described in this paper is comprehensively tailored specifically towards the cloud environment. The parameters of the trust model are derived from the essential cloud characteristics as defined by NIST[10]. The trust model considers the essential cloud characteristics as the dimensions of the trust model and for each of these dimension certain features are identified that assists in modelling the trust value. The trust model in this paper defines trust in the form of *reliability* and *reputation* taking into account the *credibility* of the feedback provider. A similar approach has been used in [8], but

the fundamental advantage of the model proposed in this paper is that it is sensitive to uncertainty of the information(i.e. feedback) provided by the feedback providers. The trust framework in this paper incorporates an additional early filtering mechanism to filter malicious node which complements the credibility approach of reducing the influence of malicious nodes. The work in this paper evaluates the trust model based on filtering of malicous nodes by using an outlier detection technique that is proposed in [7][16], showing the advantage of applying an early malicious node filtering technique

The rest of the paper is structured as follows: Section 2 describes a Cloud Computing Example that is used across the paper to illustrate the work. Section 3 describes the Trust model in details. Section 4 discuss the evaluation of the trust model. Section 5 details on the related work and Section 6 provides concluding remarks and future work.

2 Cloud Computing Example

In order to illustrate and evaluate the work in this paper, a cloud broker scenario that is being developed within the OPTIMIS project is used. For evaluating our proposed model we considered hundred Service Providers (SP's), hundred Infrastructure providers (IP's), and a single cloud broker (CBR). In the Scenario, we assume that the SPs register with the broker for getting infrastructure services from the IPs. The SPs may also have independently taken infrastructure services from the IPs and may be continuing to do so. The scenario consists of the Cloud Broker (CBR) evaluating the trust of an IP. The CBR receives feedback from SP1 to SP100 in the form of opinion, which passes through a filter, which in turn filters the nodes that provide the malicious ratings for IP1. In this scenario if we consider, SP1-SP70 passes successfully through the filter and then the feedback from SP71-SP100 are not considered for computing the reputation of IP1. The feedbacks OP1-OP70 provided by SP1-SP70 are weighted by the corresponding *credibility* CR1-CR70 which the CBR have for each of the feedback providers. The weighted ratings OPF1 – OPF70 obtained by multiplying the feedbacks with the credibility, are used by the CBR to compute the reputation score of IP1. The consensus opinion OPF obtained from OPF1 – OPF70, forms the reputation score for IP1.

3 Trust Framework

As briefed in Section 1, the trustworthiness of the IP is modeled based on the cloud characteristics [10] to have dimensions as: *on-demand self-service(os)*, *resource pooling(rp)*, *rapid elasticity(re)* and *measured service(ms)*. The *on-demand self-service* characteristics, enables the consumer to unilaterally provision computing resources without requiring any human interaction. The *rapid elasticity* characteristics of the cloud provider enables the consumer to scale resources rapidly up and down based on demand. The *resource pooling* characteristics of the cloud environment enables cloud service providers to use multi-tenant model, dynamically assigning

physical and virtual resources with location independence. The *measured service* characteristic of cloud enables it to control and optimize the resources by metering capability at certain level of abstraction such as storage, bandwidth, processing etc. The controlling of resources can be as per the agreement between the consumer and the provider. The resource usage can be monitored, controlled and reported providing transparency to the provider and the consumer. Each of the dimension that represents a cloud characteristic, contains a list of features identified to specify the context within the dimension. The *on-demand self-service* dimension includes the following features: *availabiilty_d* and *timely_d*. The feature *availabiilty_d* contributes to the dimension by capturing the availability of resources in the event of an on-demand resource provisioning request. The feature *timely_d* contributes to the dimension with the provider's capability to provision the resource within a suitable time. The *availabiilty_e* and *timely_e* features contribute to the *rapid elasticity* dimension during the occurrence of the event that triggers elasticity. The *affinity* and the *legal* feature of *resource pooling*, capture the provider's capability/violations towards the provisioning of resources with the given affinity constraints and the location based constraints respectively. The features *viewable*, *controllable* and *reportable* of the *measured service*, provides the capability of the infrastructure provider to view, control and report resource usage.

3.1 Trust Model

The trust model comprises of *reliability* trust and *reputation* trust given as follows:

$$Trust = confidence * Reliability + (1 - confidence)Reputation \quad (1)$$

Where *confidence* is the trustee's confidence in the reliability trust evaluated through direct interaction. The *confidence* value ranges between [0-1]. Reputation trust is based on the feedback received.

Reliability trust

The reliability of another entity is based on the direct interaction. R(i,j) is the reliability of entity *j* from the perspective of entity *i*. The SP updates its rating and reliability for each feature of the dimension. The overall reliability of entity *j* from the perspective of entity *i*, for all the dimensions, is given as the weighted average:

$$\begin{aligned} R(i,j)_{on_demand, Elasticity, Resource\ pooling, Measured\ services} = \\ R(i,j)_{on_demand} * W1 + R(i,j)_{elasticity} * W2 + \\ R(i,j)_{resourcePooling} * W3 + R(i,j)_{measuredServices} * W4 \end{aligned} \quad (2)$$

Where *W1*, *W2*, *W3*, *W4* are weights with $W1 + W2 + W3 + W4 = 1$ and $R(i,j)_{on\text{-}demand}$, $R(i,j)_{elasticity}$, $R(i,j)_{resourcePooling}$, $R(i,j)_{measuredService}$ are the dimension considered in the trust model based on the cloud characteristics. Reliability of a single dimension is given as:

$$R(i,j)_{on_demand} = R(i,j)_{availability_d} * W11 + R(i,j)_{timely_d} * W12 \quad (3)$$

$$R(i,j)_{Elasticity} = R(i,j)_{availability_e} * W21 + R(i,j)_{timely_e} * W22 \quad (4)$$

$$R(i,j)_{Resource\ pooling} = R(i,j)_{afinity} * W31 + R(i,j)_{legal} * W32 \quad (5)$$

$$R(i,j)_{Measured\ Services} = (R(i,j)_{viewable} * W41 + R(i,j)_{controllable} * W42 + R(i,j)_{reportable} * W43) \quad (6)$$

Where *W11*, *W12*, *W21*, *W22*, *W31*, *W32*, *W41*, *W42*, *W43* are weights assigned such that *W11 + W12=1*, *W21+W22=1*, *W31+ W32=1* and *W41+ W42+ W43=1*.

Reliability of a single feature can be given as the expectation of the opinion. The reliability of the feature available_d for the on demand dimension is given as:

$$R(i,j)_{availability_d} = Exp(W^{i}_{availability_d}) \quad (7)$$

Where $W^{i}_{availability_d}$ is the opinion of entity *i* for the feature *availability_d*, for its direct interaction with entity *j*. $W^{i}_{availability_d} = (b^{i}_{availability_d}, d^{i}_{availability_d}, u^{i}_{availability_d}, a^{i}_{availability_d})$, where $b^{i}_{availability_d}$ is the belief in the proposition, $d^{i}_{availability_d}$ is the disbelief in the proposition, $u^{i}_{availability_d}$ is the uncertainty of the proposition, $a^{i}_{availability_d}$ is base rate that provides the weight of uncertainty that contributes to the probability expectation [13].

Reputation trust.

The reputation trust is calculated based on the feedbacks received from the other entities in the system. Rep(i,j) is the reputation trust of entity *j* from the perspective of entity *i*. The cloud broker (entity *i*) receives feedback from all SPs their reliability trust about entity *j* for each feature of the dimension and computes the reputation trust Rep(i,j) for each feature. The overall Reputation trust of entity *j* from the perspective of entity *i* for all the dimensions is computed similar to the reliability trust, except for the individual reputation of the feature.

The reputation trust for each feature identified for the dimension is given by first discounting or weighing the feedback with the credibility for the feedback provider and then taking consensus view of all the discounted opinion. For example the reputation trust for the availability feature of on-demand dimension is given as:

$$Rep_{availability_d} = Exp\left(\begin{matrix}\left(W^{k1}_{availability_d} \otimes W^{k1}_{credibility}\right) \oplus \ldots . \oplus \\ \left(W^{kn}_{availability_d} \otimes W^{kn}_{credibility}\right)\end{matrix}\right) \quad (8)$$

Where $W^{k1}_{availability_d}$ is the opinion of entity *k1* for the feature *availability_d* for its direct interaction with entity *j*. The symbol $\oplus$ is the consensus operator as given in [4]. $W^{k1}_{credibility}$ is credibility opinion for entity *k1*, as built by entity *i*, based on the trueness of feedback received.

Credibility.

The credibility is the trust in the feedback provider from the trustor's perspective. This enables the trustor to weight the information provided by the feedback provider about the trustee. The credibility is given as follows:

$$W^{k}_{\text{new credibility}} = W^{k}_{\text{current credibility}} \ \underline{\otimes} \ W^{k}_{\text{previous credibility}} \tag{9}$$

$$cv = 1 - |F_{kj} - Q_j| \tag{10}$$

$$W^{i}_{\text{current credibility}} = f(cv) \tag{11}$$

Where $\underline{\otimes}$ is a consensus operator to combine dependent trust as defined by Josang [2] and *cv* is credibility value which is used to build the current credibility opinion. The *cv* forms the positive evidence and *(1-cv)* provides the negative evidence to build the current credibility opinion $W^{k}_{\text{current credibility}}$. F_{kj} is the feedback response provided by witness *k* about trust *j* and the Q_j is the real QoS by trustee *j*. The initial value of the credibility is set to a high belief of 1.0.

3.2 Filtering Unfair ratings

The Reputation trust, depends mainly on the feedbacks provided by the providers. In systems with large number of feedback providers, the malicious groups of feedback providers may significantly impact the reputation of the trustee. Many studies[5] [8][15] exists to show how to reduce the effect of the malicious feedback providers. The study in this paper uses three categorized groups of malicious feedback provider as considered in [8]. The malicious groups are: *complementary, exaggerated positive* and *exaggerated negative*. $= \alpha +$ In this paper we demonstrate a case where early filtering of the malicious feedback providers significantly improves the robustness of the trust model. This improvement is complementary to the robustness achieved using the credibility metrics. Though any technique of excluding malicious feedback providers is applicable, we demonstrate our model using the outlier method to filter the exceptions in the feedback [7]. In this approach, the outlier is defined as the feedbacks that are inconsistent with majority of the feedbacks and has low probability that it originated from the same statistical distribution as other feedbacks in the overall set of feedback. This work has been initially discussed in the context of detecting of outliers in large databases [7]. The work in this paper uses the basic optimal algorithm [16] defined to find the subset with maximum smoothing factor which primarily is dependent on the outlier detection algorithm[7] in large databases.

4 Evaluation

The Trust model is evaluated using a simulation of the cloud computing scenario discussed in Section 2. A typical simulation is run for 250 iterations, with a total of 100 SP nodes, one CBR node trying to evaluate a single IP node. The SP nodes are tagged with one of the four categories which include: normal group (G1), exaggerated

positive group (G2), exaggerated negative group (G3) and complementary group(G4). The experiment use the different ratios G1:G2:G3:G4 of the SP nodes. Section 4.1 demonstrates the enhancement to the trust model over the credibility due to the introduction of malicious filter.

4.1 Effect on Trust due to Malicious filtering

The aim of this experiment is to evaluate the trustworthiness computed by the model for the IP and ensure that it does not largely deviate due to the malicious nodes present in the system. This experiment is performed in two stages. In the first stage the trust value for the IP is computed without any malicious node present in the system i.e. node ratio of 100:0:0:0. In the second stage, malicious nodes with ratio of 70:30:0:0 is introduced and different filters are applied to observe the trust value for the IP. The result of this experiment shows that the trust value obtained after introducing the positive exaggerated nodes with no filter (or filter=0) differs a lot from the original trust value with no malicious nodes. Due to the credibility defined in the trust model, the trust value does try to match the original trust value, but still there is a sizable difference between the two trust values. After introducing the malicious node filter of filter=30 and filter=n/2 (where number of nodes n=100), the trust value nearly overlaps with the original trust that is obtained without the malicious node.

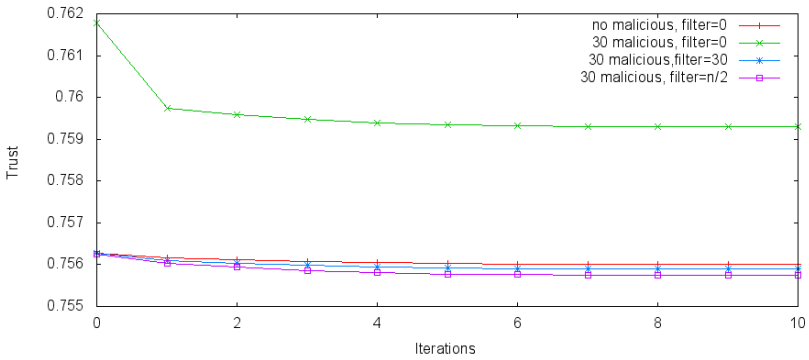

Fig. 1. Trust for different levels of filtering. SP node group ratio is 70:30:0:0

5 Related Work

The concept of trust is fundamentally applicable in diverse fields [9] like psychology, economics, sociology and political science and also extensively used in computer science. The use of trust in the field of computer science is observed in diverse areas such as e-commerce, peer-to-peer, multi-agent systems, security and access control in computer networks, reliability in distributed networks, game theory and agent systems and policies for making decision under uncertainty [8][11][12].

The Beta reputation model in [3] is based on the belief theory that allows opinion to be formed based on the evidence. The trust model discussed in this paper also uses the opinion model [13] that has improved accuracy due it its unique way of uncertainty modeling. Similar to the beta distribution, the opinion model in [13] considers two parameters, the amount of positive evidence and the amount of negative evidence based on which it estimates the reputation of an entity in a system.

Resnick *et al.* [12] discuss the importance of reputation systems in internet services where large number of producers and consumers may not know each other and how reputation systems assists in making trust decisions. However open systems like these are susceptible to variety of attacks [14] on reputation systems. Different types of attacks on reputation systems are described by Kerr et al. [14]. Several techniques [5] [15] to immunize the effect of unfair ratings or resist the attacks on reputation based system exist in literature. The work in this paper uses the outlier detection mechanism in [7][16] to detect unfair ratings and filter these ratings to reduce the impact on reputation due to unfair ratings.

The recently growing trend of cloud computing brings in concerns of security and trust. Trust based on reputation systems for cloud environment has been discussed in [1] [6] [13]. In [1], 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.* [6] proposes a trust model for cloud computing based on the usage of SLA information. The model in [13] also includes SLA compliance information to model trust and complements the trust model with SP ratings and SP behavior to assist modeling. However, the trust model for cloud environment discussed in this paper is very comprehensive that includes the cloud characteristics as dimensions, supported along with features of each dimension to be included in the trust model. This trust model represents the credibility parameter as in [8], however the work in this paper, due to its usage of belief based opinion, to exchange feedbacks, makes it more sensitive to uncertainty.

6 Conclusion and Future Work

The paper presents trust model that comprehensively captures the cloud characteristics as dimensions and identifies several features associated with the dimensions. The trust framework proposes to consider an early malicious filter which along with the credibility defined in the trust model enhances the robustness of the model against malicious feedbacks. The work in this paper is evaluated using simulation experiments. We are currently exploring to evaluate the trust model using the real cloud data for different dimensions of the model.

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. 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 Generation Computer Systems (2011)
2. A. Jøsang, S. Pope, and S. Marsh. Exploring Different Types of Trust Propagation. In Proceedings of the 4th International Conference on Trust Management. *(iTrust)*, Pisa, May (2006)
3. A. Josang, R. Ismail. The Beta Reputation System. In Proceedings of the 15th Bled Electronic Commerce Conference e-Reality: Constructing the e-Economy (2002)
4. A. Josang. A Logic for Uncertain Probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 9(3):279311 (2001)
5. A. Whitby, A. Jøsang, and J. Indulska, "Filtering out unfair ratings in Bayesian reputation systems," in Proc. 7th Int. Workshop on Trust in Agent Societies, 2004.
6. Alhamad, M., Dillon, T., Chang, E.: SLA-Based Trust Model for Cloud Computing 13th International Conference on Network-Based Information Systems (2010)
7. Andreas Arning, Rakesh Agrawal, and Prabhakar Raghavan, A linear method for deviation detection in large databases, Data Mining and Knowledge Discovery, Portland, Oregon, August (1996)
8. Chen Jia, Lei Xie, Xiaocong Gan, Wenhui Liu, and Zhangang Han. A Trust and Reputation Model Considering Overall Peer Consulting Distribution. IEEE Transaction on Systems, MAN, and Cybernetics – Part A: Systems and Humans, Vol. 42, No. 1, January (2012).
9. D. Harrison Mcknight and Norman L. Chervany. The Meanings of Trust. Technical Report 94-04. Management Information Systems Research Center, Carlson School of Management, University of Minnesota(1996)
10. http://csrc.nist.gov/publications/PubsSPs.html#800-145. The NIST Definition of Cloud Computing. Special Publication 800-145.
11. J.M. Pujol, R. Sanguesa, J. Delgado. Extracting Reputation in Multi Agent Systems by Means of Social Network Topology. Proc. International Joint Conference Autonomous Agents and Multiagent Systems (2002)
12. Paul Resnick, Richard Zeckhauser, Eric Friedman, K. Kuwabara, "Reputation Systems." Communications of the ACM, 43(12): 45-48(2000)
13. Pramod S. Pawar, Muttukrishnan Rajarajan, Srijith Krishna Nair, and Andrea Zisman. Trust Model for Optimized Cloud Services. Sixth IFIP International Conference on Trust Management (2012)
14. R. Kerr and R. Cohen. Smart Cheaters Do Prosper: Defeating Trust and Reputation Systems. 8th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2009), 10–15 May(2009)
15. Y. Yang, Y. L. Sun, S. Kay, and Q. Yang, "Defending online reputation systems against collaborative unfair raters through signal modeling and trust," in Proc. of the 24th ACM Symposium on Applied Computing, Mar(2009)
16. Zhiyuan Zhang and Xia Feng, "New methods for deviation-based outlier detection in large database", 6th International Conference on Fuzzy Systems and Knowledge Discovery. (2009)