A Trust Reputation Architecture for Virtual Organization Integration in Cloud Computing Environment

Luis Felipe Bilecki[1], Adriano Fiorese[1] and Fernando Matos[2]
[1]*Department of Computer Science (DCC), Santa Catarina State University (UDESC), Joinville, Brazil*
[2]*Department of Computer Systems (DSC), Federal University of Paraíba (UFPB), João Pessoa, Brazil*

Keywords: Trust, Virtual Organization, Reputation, Cloud Computing, Collaborative Networks.

Abstract: Virtual Organization (VO) represents a prominent collaboration initiative, where a set of entities share competencies and risks attending a common goal. Moreover, their interactions can be supported in an Internet basis, using Cloud Computing (CC) resources. The VO and CC integration brings several benefits, such as: reduction of costs and maintenance, interoperability, among others. However, there are issues related to privacy, trust and security that need to be addressed. One of the issues observed is how much trust VO members put in the cloud provider (CP), particularly, in a scenario where VO members use the resources provided by a CP to made available their services and in order to interact with other members. Thus, the proposed reputation architecture intends to assist the decision-making processes present in the VO's life-cycle reputing CP trust. The reputed trust is based on two sources: a) objective (Quality of Service (QoS) indicators) and b) subjective (feedback from users regarding those QoS indicators). The evaluation results show that the architecture is resilient to attacks on subjective trust during the reputation calculation. Also, it is possible to note that the proposed architecture presents an acceptable average time for each one operation, and a significant role during VO's creation and operation.

1 INTRODUCTION

The socioeconomic challenges faced by society (e.g. globalization and competitiveness), have motivated small and medium-sized enterprises in the adoption of collaborative methodologies, reducing time and costs of the production process (Esposito and Evangelista, 2014).

Virtual Organization (VO) is a collaborative network where via a temporary alliance, a set of legally independent entities (enterprises), heterogeneous and geographically disperse, share resources, skills, capabilities and risks in order to attend a collaboration opportunity (Camarinha-Matos et al., 2009). VOs may use technologies such as Cloud Computing, to support the transactions between people and enterprises.

In the cloud based scenario presented in (Ruaro and Rabelo, 2016), the exchange of information, hosting and execution of applications are performed in the cloud. This means that VO members can use cloud resources to execute and provide their services and information.

In this sense, Cloud Computing (CC) acts as a technology that provides access to computing resources (e.g. infrastructure and applications) on a practical and on-demand way (Mell and Grance, 2011).

This integration between VO and CC, presents some benefits, such as: cost reduction, competitive advantage, resources provided according to demand, among others (Ruaro and Rabelo, 2016). However, some issues could arise, such as: security, search and selection of cloud providers, and trust assessment (Noor et al., 2013). A particular challenge concerns the trust assessment from VO members to CC providers. This is an important issue since trust plays a significant role in the collaboration opportunity attendance (Arenas et al., 2010), because VO members use the provided resources as a support to execute their activities.

Considering the trust issue in this environment, this work presents a trust reputation architecture to support the several decision-making processes existing in the VO's life-cycle. The proposed reputation architecture is responsible for generate the trust indicators for reputation from two sources (objective and subjective), disseminate reputation and attend other requests through a centralized approach, monitor the

Bilecki, L., Fiorese, A. and Matos, F.
A Trust Reputation Architecture for Virtual Organization Integration in Cloud Computing Environment.
DOI: 10.5220/0006276506950702
In *Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017) - Volume 2*, pages 695-702
ISBN: 978-989-758-248-6
Copyright © 2017 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved

objective source during VO's operation, and receive feedbacks from VO's member to CC providers, in order to update the cloud provider's reputation.

Thus, the proposed architecture intends to cover all stages and decision-making processes existing in VO's life-cycle. During the VO's creation stage, the reputation can be used as an indicator in the process of cloud providers search and selection. In Operation stage, the reputation should be verified and evaluated. In the Evolution stage, a potential change of cloud providers may be necessary, and finally, in Dissolution the transactions feedbacks are collected, in order to update the subjective trust and consequently the reputation of any cloud provider.

The remainder of this work is organized as follows. Section 2 presents the related concepts of this work. Section 3 presents the proposed trust reputation architecture. Section 4 presents the scenario where simulations are performed, the parameters used in simulation and shows and discusses results from the evaluation. Finally, Section 5 presents the conclusions and future work.

2 GENERAL BACKGROUND

2.1 Virtual Organizations and Cloud Computing

Due to dynamic environment and market competitiveness, enterprises have been noticing need to work together in order to operate with greater agility and flexibility, joining collaborative networks to achieve common goals (Alawamleh and Popplewell, 2010).

A Virtual Organization (VO), a form of collaborative network, is understood as a temporary alliance, where a set of legally independent and heterogeneous entities (usually enterprises) share skills, resources, competences and risks, in order to achieve specific business goals (to attend a collaboration opportunity) (Camarinha-Matos et al., 2009). A striking and decisive VO feature is the use of resources provided by a communication infrastructure to obtain competitive advantage. Thus, the VO is configured as a single entity through the union of the core competencies of its entities (Arenas et al., 2010).

The VO's life-cycle is composed of several stages (Camarinha-Matos et al., 2009). In the Creation stage, partners are discovered, selected and the network is configured. In Operation stage, partners interact and exchange information to achieve a common goal. The Evolution stage is performed during VO's operation, when minor changes occur in membership, roles or operation principles. Finally, in the Dissolution stage, the VO's finishes its operation and this stage can occur in two ways, where the business objectives are achieved successfully or due to serious problems in operation that invalidates the VO's existence.

The emergence of new concepts of information and communication technologies (ICT), such as grid computing and cloud computing, brought a new approach to VO and its operation, which could improve its service quality and enhance market survival.

Cloud Computing (CC) can be defined as a set of computing resources (processing, storage, connectivity, platforms, applications, and services) that are available over the network (Internet) and can be quickly provisioned without any human intervention (Mell and Grance, 2011).

The main characteristics of cloud computing are: on-demand self-service, resource pooling, broad network access, rapid elasticity and measured services (Mell and Grance, 2011). The CC provides services to the users based on three different models, SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service) (Ruaro and Rabelo, 2016).

Through the mentioned models, small and medium enterprises use these resources, for the development of business systems and information sharing in collaborative environment, that set up CC as a infrastructure to support VO's operation.

Nevertheless, the integration of CC and VO, offer several benefits. The necessary perception of trust arouses the need for trust assessment, specially during the several stages of VO's life-cycle. The trust in the cloud providers appears as a key element that can jeopardize the collaboration opportunity during VO's operation. Thus, Section 2.2 presents trust and reputation concepts and their relationship with VO.

2.2 Trust and Reputation

Trust is a multidisciplinary concept and it has been used in many areas. Besides multidisciplinary, trust is a complex concept and have different meanings on each context.

A formal definition about the concept of trust is provided by Gambetta (Gambetta et al., 2000): "trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action".

Thus, in a computational implementation, trust

can be defined as a numeric value that indicates how trustworthy an agent is, allowing others to consider this value to decide whether or not to interact with (Noor et al., 2013).

Some characteristics according to (Firdhous et al., 2012) are common to any trust definition, they are: helps to manage uncertain and high risk environments; it is used as a basis for decision-making; based in objective or subjective source; based in historical performance and past experience; context sensitive and dynamic over time.

In a VO environment, the trust assessment is guided by some requirements, such as: direct relationship (non symmetric), subjective (feedbacks) and/or objective (past performance) basis, automated management and trust is dynamic over time and new observations (Winkler et al., 2007).

The reputation concept is closely related to trust, and can be used in VO environments to assess confidence from members to cloud providers (Bilecki and Fiorese, 2016). Thus, reputation is defined as a collection of feedbacks about an object, character, or related to attributes of an entity (reliability, capability and usability) (Resnick and Zeckhauser, 2002). Therefore, in a VO and CC integration environment, reputation should be based on objective indicators (Bilecki and Fiorese, 2016) and subjective indicators (feedbacks) (Noor et al., 2013).

Nevertheless, some threats on reputation systems are described in literature, and these systems should be robust to cope with the attacks. There are many attacks types (Jøsang and Golbeck, 2009), however in the VO and CC integration, some are considered, such as: (i) *Feedback Collusion*: Set of fake feedbacks that aims to maximize or decrease the reputation of an entity; (ii) *Unfair Rating*: A VO's member provides malicious ratings to the CC provider, in order to increase or decrease reputation level. In this attack, the attacker can have a disproportionately influence over computed reputation.

2.3 Related Work

With the prominent integration of CC as a form of VO's infrastructure, some contributions related to trust assessment and management, should be analyzed as related work.

PathTrust (Kerschbaum et al., 2006), is a centralized reputation system applied to the search and selection step during the VO's formation. To participate in the VO formation process, a member must register in an Enterprise Network (EN). At the VO's dissolution stage, each member sends his feedbacks regarding the performed transaction with other members. Thus, the utilization of a reputation system in VO's provides non-monetary benefits. Conversely, it provides a means to ensure a better or more reliable service (Kerschbaum et al., 2006).

In (Arenas et al., 2010), a centralized reputation system has been applied to a VO, which uses the Grid Computing infrastructure. The reputation of each user is evaluated according to the use of provided resources and jobs, and the user evaluates the quality of service provided by the service provider. Otherwise, a reputation algorithm is applied in VO's creation using cloud resources, where the resources are selected according to cloud provider's reputation (Pan et al., 2013). However, the algorithm does not cover all the VO's life cycle stages.

In (Mashayekhy and Grosu, 2012) a VO's formation mechanism based on reputation of Grid Service Provider's (GSP) is presented. This mechanism acts in the integration between VO and Grid Computing, where a key element is the GSP's reliability regarding the delivery of promised resources. The GSP reputation's is based on their past interactions, to evaluate how likely is to provide the requested resources. In some cases, a GSP agrees to participate in VO, but it fails to deliver the promised resources, affecting the operation step.

Stochastic Reputation Service for Virtual Organizations (STORE) (Haller, 2008) is a reputation system in order to assist the decision-making process existent in the VO's creation. The trust indicator, used as reputation model, represents an aggregation of a hierarchical indicators composed by financial, operational, organizational, externals, and third-party indicators that reflects the organizational's performance.

Despite the small sample of related work, it is possible to note that although one address the issue of VO's integration with CC, none of them provides means to attend the several stages of the VO's life-cycle, and, few studies address the issue of trust and reputation applied to VO's integration with CC.

Thus, this work intends to cover the existent lack of trust in the VO and CC integration, providing a trust reputation architecture, where reputation is composed by two trust sources (objective and subjective) and this reputation will help in the several decision-making process existent in VO's life-cycle.

3 PROPOSED ARCHITECTURE

The emergence of new ICT concepts, such as cloud computing, brought a new approach to VO and its operation. The cloud computing provides computational resources and the VO uses these resources to deliver

its service in a distributed manner, geographically dispersed, thereby facilitating the collaboration process.

Hence, to build a trust indicator for reputation in a VO and CC integration environment, the cloud computing providers quality of service (QoS) properties are exploited. In this integration scenario, the QoS indicators represent an important role in trust assessment, because the VO's members are using the CC resources to make available their systems and attend the collaboration opportunity.

In order to assess and manage the trust in this scenario, the reputation concept can be applied, aiming to cover all stages in the VO's life-cycle. Therefore, in the proposed architecture, depicted in Figure 1, data and reputation requests will be managed through a centralized approach.

The reputation architecture comprises four modules, namely: monitoring module, data repository, aggregation module and reputation broker service (RBS). The Monitoring Module is responsible for monitoring and updating QoS indicators of each CC provider, during the VO's operation stage. The Data Repository stores historical and current values for QoS indicators and VO's members feedbacks. The Aggregation Module is responsible for calculating the reputation for CC providers based on QoS indicators and users feedbacks. The RBS module is the interface through which communication occurs with others members. For example, the VO's member can send its feedback regarding a provider to RBS, or may request a cloud provider's reputation, at any time, to RBS.

3.1 Aggregation Module

Reputation and trust systems are used in different scenarios to assist someone in the choice of something that is reliable. In most e-commerce reputation and trust systems, the trust is based on the feedbacks given by consumers. Thus, in the VO environment using cloud resources, other sources of trust should be considered too, such as SLA, QoS indicators, among others, along with consumer feedbacks (Noor et al., 2013).

Taking this into account, the main objective of aggregation module is calculate the cloud computing providers' reputation, based on two sources of trust: objective and subjective.

The objective trust indicator is related to QoS indicators that reflect the performance of cloud computing provider. In this work, objective trust is composed of availability (A), response time (RT), security (S), stability (E) and cost (C) indicator (Garg et al., 2013).

The subjective trust is composed of the feedbacks provided by VO's members to cloud computing providers. During the VO's dissolution or operation, a VO's member sends its feedback related to QoS provided by its cloud computing provider.

During the reputation calculation, current objective values monitored by the monitoring module can be also used together with the historical ones to take a current reputation snapshot.

Thus, the reputation value R_s of a cloud computing provider s, according Equation 1, is defined as a combination of objective and subjective trust indicators by means of a weighted sum, where ω_{obj} and ω_{sub} are the weights defined by the VO's manager, $T_{obj}(s)$ and $T_{sub}(s)$ are the objective and subjective trust indicators, respectively.

$$R_s = \omega_{obj} * T_{obj}(s) + \omega_{sub} * T_{sub}(s) \quad (1)$$

3.1.1 Objective Trust

This section proposes a objective trust assessment methodology for cloud computing provider, using the aforementioned QoS indicators, where these indicators are independent of cloud service model.

The objective trust ($T_{obj}(s)$), represented by Equation 2, is calculated by two approaches: analyzing the efficiency ($Eff(s)$) of cloud providers based on the historical QoS data and scoring the QoS indicators by means of a multi-criteria approach ($MC(s)$).

$$T_{obj}(s) = Eff(s) * MC(s) \quad (2)$$

The cloud providers' (CP) efficiency is calculated by the Data Envelopment Analysis (DEA) method. The DEA is a nonparametric method that calculates the relative efficiency of multiple decision-making units (DMUs), where DMU refers an entity capable to convert multiple inputs to outputs (Banker et al., 1984).

Therefore, for DEA application, the input and output should be modeled and are related to the QoS indicators. Thus, the output (O_{kj}) for each cloud provider (k) as a DMU, represented by Equation 3, is understood as the average of historical data (VO's participations) for each QoS indicator (j). Moreover, the standard deviation is considered due to a possible fluctuation in CP's past performances.

$$O_{kj} = \overline{H_{kj}} + \sigma(H_{kj}) \quad (3)$$

The input data set (I_{ki}) is composed of the average of estimated values, by a linear regression from the QoS indicators (i) historical ones for each cloud provider (k). To generate the estimated values, the linear regression is used, taking the first and second

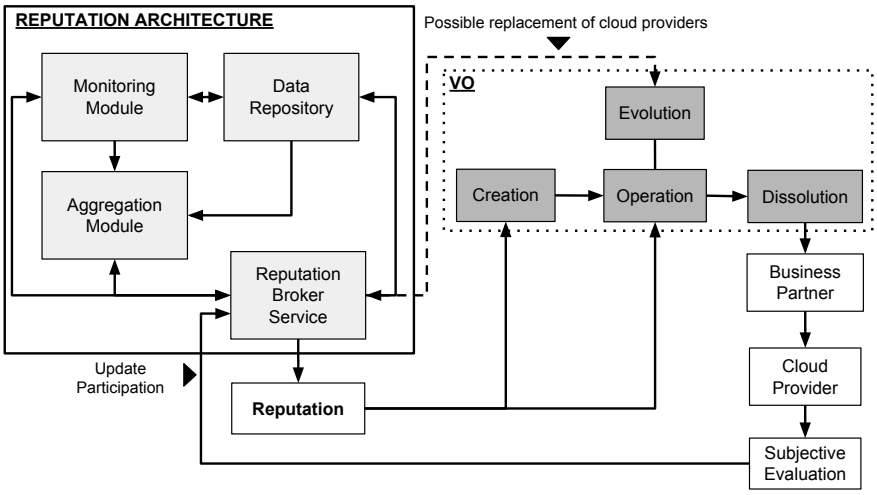

Figure 1: Conceptual Model Involving the Reputation Architecture.

historical values from QoS indicators and predicting the third, and so on, until the n-nth historical participation. This approach is necessary to verify the CP behavior at future VO's participations. Equation 4 represents the input calculated for each indicator using the aforementioned method.

$$I_{ki} = \overline{X_{ki}} - \sigma(X_{ki}) \tag{4}$$

Thus, after the input and output data set definition, the efficiency can be calculated. The efficiency is calculated solving a DEA model through linear programming. In this context, the DEA-BCC model output-oriented (Banker et al., 1984) will be used, because the output values are independent from the estimated ones.

Also, the proposed objective trust also considers a multi-criteria trust ($MC(s)$), understood as a score which represents the importance assigned by the VO's manager to the QoS indicators. To calculate $MC(s)$, the comparison matrix of the Analytical Hierarchy Process (AHP) multi-criteria method is used.

To determine the weights of indicators the Saaty's scale is used (Saaty, 1990). This scale is composed by degrees of importance (from 1 to 9), where for example, 9 represents the largest discrepancy between the indicators. Through this scale, a judgment matrix is created to perform a pairwise comparison of the QoS indicators and by means of some normalization and averaging processes result in the weight of each indicator.

Therefore, multi-criteria trust ($MC(s)$), presented in Equation 5, is calculated by multiplying the normalized average historical QoS indicator values ($\overline{A}$, $\overline{RT}$, $\overline{S}$, $\overline{E}$, and $\overline{C}$) by their corresponding weights ($w_1 ... w_5$).

$$MC(s) = (w1 * \overline{A}) + (w2 * \overline{RT}) + (w3 * \overline{S}) + (w4 * \overline{E}) + (w5 * \overline{C}) \tag{5}$$

3.1.2 Subjective Trust

The subjective trust assessment of a CP exploits users' ratings about the QoS provided. This subjective source was adapted from (Noor et al., 2013) and these ratings are collected and stored by the proposed architecture.

Each VO's member gives its feedback, during VO's dissolution or operation stage, about the transaction performed with a CP. The feedback is composed by a set of ratings ranging from 0 to 5, to each one of the QoS indicators. The subjective trust assessment of a CP s made by a VO's member c is seen as $Q_c(c,s)$ and it is understood as a weighted sum of all QoS ratings, where the weights are calculated according the multi-criteria trust approach (see more in Subsection 3.1.1).

Then, the subjective trust of a CP s, is calculated as a ratio between the subjective assessments $Q_c(c,s)$ given by the VO's members c to a CP multiplied by the credibility factor ($C_f(c,s)$), and the total of subjective assessments ($|V(s)|$). Thus, the subjective trust is represented by Equation 6, in which n refers to the VO's members who evaluated a CP s.

$$T_{sub}(s) = \frac{\sum_{c=1}^{n} Q_c(c,s) * C_f(c,s)}{|V(s)|} \tag{6}$$

The credibility factor allows to identify some misleading feedbacks from attacks (Noor et al., 2013). Particularly at the VO's dissolution stage, the subjective trust should be evaluated, analyzing the credibility of the feedbacks' set provided by a VO's member. The attack types presented in Section 2.2 are

considered in the credibility analysis, where $D(s)$ and $U(c,s)$, respectively, represent the feedback density (collusion) and unfair rating attack.

Then, the credibility factor, presented by Equation 7, is understood as the average of these attack factors multiplied by their weights (ρ and Ω) determined by the VO's manager.

$$C_f(c,s) = \frac{(\rho * D(s)) + (\Omega * U(c,s))}{2} \quad (7)$$

The feedback density ($D(s)$), exposed in Equation 8, aims to address the scenario where VO's members give numerous feedbacks to manipulate the subjective trust (Noor et al., 2013). This factor consists of the feedback mass $M(s)$, which denotes the total number of VO's members who gave feedback to a CP s, $|V(s)|$ represents the total number of feedbacks given to a CP s, and $L(s)$ represents the feedback collusion factor.

$$D(s) = \frac{M(s)}{|V(s)| * L(s)} \quad (8)$$

The feedback collusion factor ($L(s)$), identified by Equation 9, aims to reduce the credibility of those VO's members who send multiple feedbacks to the same CP (Noor et al., 2013). This factor is calculated as the ratio of the number of feedbacks given by VO's members $|V_c(c,s)|$, who gave more feedbacks than specified in volume collusion threshold $e_v(s)$, defined by VO's manager, over the total of feedbacks received by that CP s.

$$L(s) = 1 + \left(\frac{1}{|V(s)|} \sum_{c=1}^{n} |V_c(c,s)|_{\,[|V_c(c,s)| > e_v(s)]} \right) \quad (9)$$

Lastly, regarding unfair rating attacks, malicious VO's members give several misleading feedbacks, in a period of time to promote or prejudice the subjective trust of a CP s. This attack can be identified by applying a K-Means clustering algorithm, on all historical feedbacks to form K clusters, and the centroid of the most densely populated cluster is called majority cluster (M) (Malik and Bouguettaya, 2009). Then, the unfair rating factor ($U(c,s)$), is understood as the euclidean distance between M and the reported ratings (V_i), where σ is the standard deviation, and n are the total number of ratings for a VO's member c.

$$U(c,s) = \begin{cases} 1 - \frac{\sqrt{\sum_{i=1}^{n}(M-V_i)^2}}{\sigma}, & \text{if } \sqrt{\sum_{i=1}^{n}(M-V_i)^2} < \sigma \\ 1 - \frac{\sigma}{\sqrt{\sum_{i=1}^{n}(M-V_i)^2}}, & \text{otherwise} \end{cases} \quad (10)$$

4 EXPERIMENTAL SCENARIO AND RESULTS

An experiment scenario simulating VO and CC integration was developed to evaluate the proposed work. This scenario, depicted in Figure 2, was built in a P2P network simulator, called PeerFactSim.KOM (Stingl et al., 2011). Thus, different network nodes are created to represent each element presents in the proposed architecture. The scenario concerns the exchange of messages and operations between VO's members and the proposed architecture, allowing to evaluate trust assessment and reputation provided.

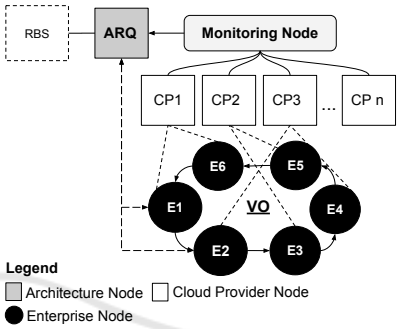

Figure 2: Experimental Scenario.

The following are the node types developed:

(i) *Architecture Node* (ARQ): receives messages destined to architecture, such as feedback ratings send operation, request reputation list, request cloud provider's reputation, and monitoring actions. This node has implemented the functionality of Reputation Broker Service (RBS);

(ii) *Enterprise Node* (E*n*): it is a VO's member in an organized VO as a logical ring topology;

(iii) *Cloud Provider Node* (CP): represents the cloud providers offering their services to the VO;

(iv) *Monitoring Node*: perform the QoS Monitoring of each CP.

During the simulation step, the following parameters were used: VO's duration (simulation time 10080 min), ten cloud providers, ten historical participations, ten simulation rounds and, the weights for each QoS indicator are defined as: A (0.3830), RT (0.2317), E (0.1861), S (0.1350), and C (0.0642), obtained by means of multi-criteria trust assessment. Thus, in the following sections the experimental results are presented.

4.1 Reputation

The reputation of a cloud provider's s uses the historical objective and subjective trust according to the

methodology proposed in the Section 3.1.

In this sense, to compose the historical objective CP's data, random values were generated to each one QoS indicator. The values were generated through a linear distribution, and the average values of ten past participations are presented in Table 1, where each column refers to QoS indicators.

Table 1: QoS Indicators values.

Provider	A	RT	E	S	C
Rackspace	0,9648	99ms	62	3	$ 0,75
GreenGeeks	0,9439	647ms	58	4	$ 0,65
Dot5Hosting	0,9188	114ms	57	7	$ 0,53
Cari	0,9683	20ms	59	8	$ 0,79
JustCloud	0,8924	535ms	64	7	$ 0,84
GoGrid	0,5743	250ms	36	5	$ 0,32
ElephantDrive	0,5604	869ms	67	7	$ 0,64
GoDaddy	0,7809	691ms	12	2	$ 0,52
EpmSolutions	0,4959	332ms	33	9	$ 0,48
AgileIT	0,6370	696ms	49	8	$ 0,64

Then, the historical subjective CP's data was based in the dataset presented in (Noor et al., 2013). In the dataset was performed a pre-processing step with the purpose of extract ten subjective evaluations from ten cloud providers, where each one subjective evaluation is composed by a ratings set, comprising values in a scale from 0 to 5, for each one QoS indicator.

Afterwards the objective and subjective trust data are defined, a VO composed by ten business partners and five cloud providers was simulated, with the purpose of presenting the updated CP's reputation after a new VO's participation. In this sense, to calculate the reputation, weights are defined as 0.85 and 0.15, respectively, to objective and subjective sources.

Therefore, the reputation of each cloud provider is depicted in Figure 3, and it is calculated considering subjective trust with credibility analysis (*Reputation W/ F. Cred.*) and disregarding credibility (*Reputation W/O F. Cred.*).

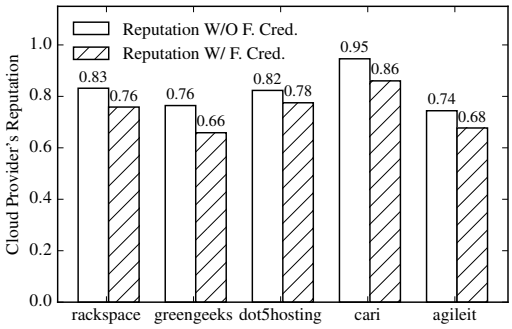

Figure 3: Cloud Provider's Reputation.

It is possible to note that some of the cloud providers (rackspace, dot5hosting, and cari) have higher reputation values, because they present best past performances and they are best subjectively assessed. Otherwise, when subjective credibility factor was not considered, the CP's reputation disproportionately increases, under malicious attack, regarding to real behavior.

4.2 Architecture Evaluation

The average time for each architecture operation during VO's operation stage was analyzed in architecture evaluation. The analyzed operations were reputation of a CP, subjective assessment of a VO's member to a CP, and the QoS monitoring.

In this sense, the simulation are performed considering business partners (VO's members) varying from 5 to 25 to verify the scalability and the aforementioned operations are uniformly distributed over simulation time. Thus, Figure 4 presents the results of simulation.

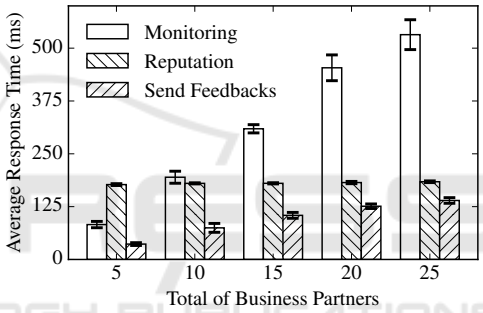

Figure 4: Average Response Time.

It is possible to note that send feedback operation is tightly coupled to the number of business partners. The monitoring operations, which consists of messages carrying data about QoS being exchanged between monitoring node, cloud providers and the arc node. Therefore, one can conclude that monitoring operation, according to the presented approach, consumes most of the time during VO's operation, and increases in relation to the number of business partners. This assumption is due to the fact that when there are more business partners, consequently more monitoring actions will be carried out.

5 CONCLUSION

This paper presented a trust reputation architecture applied to a VO which uses CC resources. The proposed architecture allows to assist the VO's manager during the decision-making processes of the VO's life-cycle. It was also presented a proposal to address the trust issue existent in this integration.

The proposed architecture presents a centralized approach composed of four modules: the Aggregation Module, Monitoring Module, Reputation Broker Service and Data Repository. The CP's reputation is calculated by the aggregation module, using two trust sources: objective and subjective.

For the evaluating purpose, a simulation environment was developed in PeerFactSim.KOM, comprising the architecture and the VO's elements (cloud providers and enterprises). The achieved results demonstrate that this work provided a promising way to deal with the attack types during reputation calculation. Moreover, the presented average time results show that the reputation architecture can be used during the VO's operation, given the trust importance in this context.

Finally, future works include to analyze other aspects, such as scalability feedback optimization, testing of objective trust using historical data generated by other probability distributions, and a objective reward and penalty mechanism.

ACKNOWLEDGEMENTS

The authors would like to thank to UDESC PROMOP financial programme as well as to LabP2D.

REFERENCES

Alawamleh, M. and Popplewell, K. (2010). Risk Sources Identification in Virtual Organisation. In *Enterprise Interoperability IV*, pages 265–277. Springer Science + Business Media.

Arenas, A. E., Aziz, B., and Silaghi, G. C. (2010). Reputation management in collaborative computing systems. *Security and Communication Networks*, 3(6):546–564.

Banker, R. D., Charnes, A., and Cooper, W. W. (1984). Some models for estimating technical and scale inefficiencies in data envelopment analysis. *Management science*, 30(9):1078–1092.

Bilecki, L. F. and Fiorese, A. (2016). A confidence indicator model for virtual organization creation in cloud computing environment. In *PRO-VE 2016*. Springer.

Camarinha-Matos, L. M., Afsarmanesh, H., Galeano, N., and Molina, A. (2009). Collaborative networked organizations–concepts and practice in manufacturing enterprises. *Computers & Industrial Engineering*, 57(1):46–60.

Esposito, E. and Evangelista, P. (2014). Investigating virtual enterprise models: literature review and empirical findings. *International Journal of Production Economics*, 148:145 – 157.

Firdhous, M., Ghazali, O., and Hassan, S. (2012). Trust Management in Cloud Computing: A Critical Review. *International Journal on Advances in ICT for Emerging Regions*, 4(2):24–36.

Gambetta, D. et al. (2000). Can we trust trust ? *Trust: Making and breaking cooperative relations*, 13:213–237.

Garg, S. K., Versteeg, S., and Buyya, R. (2013). A framework for ranking of cloud computing services. *Future Generation Computer Systems*, 29(4):1012–1023.

Haller, J. (2008). STORE Stochastic Reputation Service for Virtual Organisations. In *IFIP International Conference on Trust Management*, pages 367–370. Springer.

Jøsang, A. and Golbeck, J. (2009). Challenges for robust trust and reputation systems. In *SMT*.

Kerschbaum, F., Haller, J., Karabulut, Y., and Robinson, P. (2006). Pathtrust: A trust-based reputation service for virtual organization formation. In *iTrust 2006*, pages 193–205. Springer.

Malik, Z. and Bouguettaya, A. (2009). Rateweb: Reputation assessment for trust establishment among web services. *The VLDB Journal*, 18(4):885–911.

Mashayekhy, L. and Grosu, D. (2012). A reputation-based mechanism for dynamic virtual organization formation in grids. In *ICPP 2012*, pages 108–117. IEEE.

Mell, P. M. and Grance, T. (2011). SP 800-145. The NIST Definition of Cloud Computing. Technical report, National Institute of Standards & Technology.

Noor, T. H., Sheng, Q. Z., Ngu, A. H., Alfazi, A., and Law, J. (2013). Cloud Armor: A Platform for Credibility-based Trust Management of Cloud Services. In *CIKM '13*, pages 2509–2512. ACM.

Pan, M., Li, M., and Yu, Y. (2013). A group-choose algorithm supporting virtual organization creation for workflow deployment in cloud environment. *Concurrency and Computation: Practice and Experience*, 25(13):1894–1908.

Resnick, P. and Zeckhauser, R. (2002). Trust among strangers in internet transactions: Empirical analysis of eBay reputation system. *The Economics of the Internet and E-commerce*, 11(2):23–25.

Ruaro, A. F. and Rabelo, R. J. (2016). Do cloud computing tools support the needs of virtual enterprises? In *PRO-VE 2016*, pages 481–493. Springer.

Saaty, T. L. (1990). How to make a decision: the analytic hierarchy process. *European journal of operational research*, 48(1):9–26.

Stingl, D., Gross, C., Rückert, J., Nobach, L., Kovacevic, A., and Steinmetz, R. (2011). PeerfactSim.KOM: A simulation framework for Peer-to-Peer systems. In *HPCS 2011*, pages 577–584.

Winkler, T. J., Haller, J., Gimpel, H., and Weinhardt, C. (2007). Trust Indicator Modeling for a Reputation Service in Virtual Organizations. *ECIS 2007*, 1(April):1584–1595.