International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(2): 140-151
The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2305-0012)

Trust Measurements Yeld Distributed Decision Support in Cloud Computing

[1]Edna Dias Canedo, [1]Rafael Timóteo de Sousa Junior, [2]Rhandy Rafhael de Carvalho and [1]Robson de Oliveira Albuquerque
[1]Electrical Engineering Department, University of Brasília – UNB – Campus Darcy Ribeiro – Asa Norte – Brasília – DF, Brazil, 70910-900.
[2]Informatics Institute – INF, University Federal of Goiás – UFG - Campus Samambaia – Bloco IMF I – Goiânia – GO, Brazil, 74001-970
ednacanedo@unb.br, desousa@unb.br, rhamoy@gmail.com, robson@redes.unb.br

ABSTRACT

This paper proposes the creation of a trust model to ensure the reliable files exchange between the users of a private cloud. To validate the proposed model, a simulation environment with the tool CloudSim was used. Its use to run the simulations of the adopted scenarios allowed us to calculate the nodes (virtual machines) trust table and select those considered more reliable; identify that the metrics adopted by us directly influenced the measurement of trust in a node and verify that the trust model proposed effectively allows the selection of the most suitable machine to perform the exchange of files.

KEYWORDS

Distributed system; cloud computing; availability; exchange of files and model trust.

1 INTRODUCTION

The development of virtualization technologies allows the sale on-demand, in a scalable form, of resource and computing infrastructure, which are able to sustain web applications. So it borns cloud computing, generating a increasing tendency for applications that can be accessed efficiently, independent from their location. This technology arrival creates the necessity to rethink how applications are developed and made available to users, at the same time that motivates the development of technologies that can support its enhancement.

Since IBM Corporation announced its program for cloud computing at the end of 2007, other major technology companies (IT) has adopted clouds progressively, for example, Google App Engine, which lets you create and host applications web with the same systems that power Google applications, Amazon Web Services (AWS) from Amazon, which was one of the first companies providing cloud services to the public, Elastic Compute Cloud (EC2) from Amazon, which allows users to rent a virtual machines that they can run their own applications providing a complete control over their computational resources and allowing the execution in the computing environment, Simple Storage Service (S3) of Amazon, which allows the storage of files in the storage service, and Apple iCloud Azure Services Platform from Microsoft, which introduced Cloud computing products [1]. However, the Cloud computing also presents risks related to data security in its different aspects, such as confidentiality, integrity and authenticity [2-3, 4].

This paper proposes a trust model to exchange of files between peers in a private cloud. Private cloud computing environment allows it to be working with a specific context of file distribution, so the files have a desired distribution and availability, being possible guarantees from the cloud manager that the access is restricted, and the identification of nodes is unique and controlled.

In the proposed model, the choice of the more reliable node is performed taking into account its availability. The selection of nodes and its evaluation of trust value will determine whether the node is reliable or not, which will be performed according to the storage system, operational system, processing capacity and node link. Trust is established based on requests and consultations held between nodes of the private cloud.

This paper is organized as follows. In Section II, we present an overview of the concepts of trust and reputation. In Section III, we present review some related work about security, file system and trust in the cloud. In section IV, we introduce the proposed trust model and practical results. Finally, in Section VI, we conclude with a summary of our results and directions for new research.

2 TRUST

The concepts of trust, trust models and trust management has been the object of several recent research projects. Trust is recognized as an important aspect for decision-making in distributed and auto-organized applications [5-6]. In spite of that, there is no consensus in the literature on the definition of trust and what trust management encompasses. In the computer science literature, Marsh [5] is among the first to study computational trust. Marsh [5] provided a clarification of trust concepts, presented an implementable formalism for trust, and applied a trust model to a distributed artificial intelligence (DAI) system in order to enable agents to make trust-based decisions.

The main definitions of trust, focused on the human aspect are based on relationships between individuals, demonstrating clearly the relationship between trust and the security feeling [7-8]. Thus, trust in the human aspect is related to the feeling of security focused on a particular context, to satisfy an expectation of a solution that is likely to be solved [7-8].

The process of trusting in an individual is the result of numerous analyzes that together generates the definition of trust.

Trust (or, symmetrically, distrust) is a particular level of subjective probability, which an agent believes that another agent or group of agents will perform a particular action, which can go through a monitoration (or independent of its ability to monitor it) and in a context which it affects his own action [8].

Trust is still defined in [8] as the most important social concept that assist humans to cooperate in their social environment and its present in all human interactions. In general, without trust (in other humans, agents, organizations, etc.) there is no cooperation and therefore there is no society. In an analogous situation, trust can be treated as a probability of an agent behavior to perform a given action expected by another agent.

An agent can check the execution of a requested action (if its capacity allows it), inside a context that the achievement of the expected action will affect the action itself of this agent (involving a

decision). So if someone is trustworthy, it means that there is a high enough probability that this person will perform an action considered beneficial some way, to its cooperation be considered. In an opposite situation, it simply believes that the probability is low enough to its cooperation be avoided.

Gambetta [8] proposes that trust would have a relation with the cooperation, making cooperation important for the acquisition of trust. If trust is unilateral, cooperation can't succeed. For example, if there is only mistrust between two agents, then there's not cooperation between them at all, so they cannot perform an operation together to solve a problem. So similarly, if there is a high level of trust, probably there is a high cooperation among agents to solve a particular problem.

Josang et al [9] define trust as the subjective probability which an individual, A, expects that another individual, B, perform a given action which its welfare depends on. This definition includes the concept of dependence and reliability (probability) of the trusted party, as seen by the relying party.

Using the trust, there is the prospect that an entity P request information from one entity Q to an entity R. Imagine that entity P need some information about an entity that she still didn't correlate (S entity). P can ask for entities that it has a relationship, if one of them knows the entity S, and what their opinion about it (experiences / relationships already performed with the entity S), providing an idea of the reputation of the entity S in relation to the queried entity.

In a scenario that an entity knows several other entities, but there is an entity that doesn't know a specific entity (R doesn't know the entity Z), it can send a question about that unknown entity to its related entities and wait their answers. If one of the entities knows the investigated entity, it will return the response to the requesting entity reporting its opinion about the unknown entity.

Figure 1 presents the trust relation. From the reviews about the behavior of an entity, it can be performed the calculation of trust, based on a model, and from the obtained result, a relationship decision is made, what determines if an entity will or not relate to another entity, in a given context.

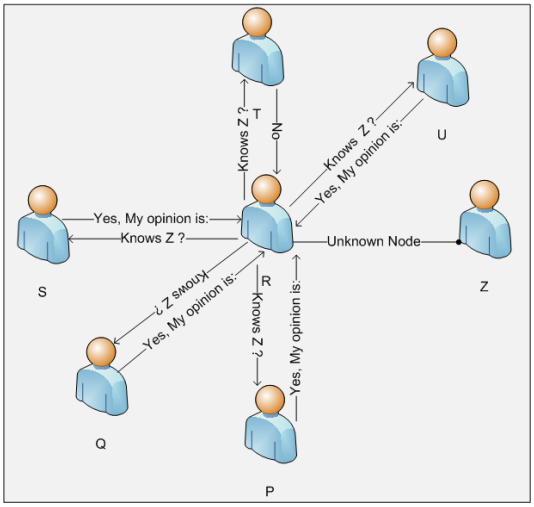

Figure 1 - Trust Relation

2.1 Reputation

Reputation can be defined in a scenario where there's not enough information to make the inference that an entity is or not reliable [10], and to achieve this inference value, an entity ask the opinion of other entities. From the obtained information of the questioned entities, the requesting entity performs the calculation of reputation from its own information, which is based on its values of trust and obtained information from third parties (the degree of trust in them). With the necessary information, the

entity assesses the context of the situation itself, being able to reach a value of reputation. The reputation calculation is obtained by analyzing the behavior of an entity over time.

The reputation in the computing scenario, according to the work reviews related to trust, indicates that it may have a strong influence on the calculation of trust [10] and [8], allowing trust to be interconnected with a reputation in generation of trust values and these values, be subject not only for the perception of the behavior of an entity, but also self-evaluation by those interested in some kind of iteration in a given context.

3 SECURITY IN THE CLOUD

Privacy and security have been shown to be two important obstacles concerning the general adoption of the cloud computing paradigm. In order to solve these problems in the IaaS service layer, a model of trustworthy cloud computing which provides a closed execution environment for the confidential execution of virtual machines was proposed [11]. The proposed model, called Trusted Cloud Computing Platform (TCCP), is supposed to provide higher levels of reliability, availability and security. In this solution, there is a cluster node that acts as a Trusted Coordinator (TC). Other nodes in the cluster must register with the TC in order to certify and authenticate its key and measurement list. The TC keeps a list of trusted nodes. When a virtual machine is started or a migration takes place, the TC verifies whether the node is trustworthy so that the user of the virtual machine may be sure that the platform remains trustworthy. A key and a signature are used for identifying the node. In the TCCP model, the private certification authority is involved in each transaction together with the TC [11].

Shen et al. [12] presented a method for building a trustworthy cloud computing environment by integrating a Trusted Computing Platform (TCP) to the cloud computing system. The TCP is used to provide authentication, confidentiality and integrity [12]. This scheme displayed positive results for authentication, rule-based access and data protection in the cloud computing environment.

Zhimin et al. [13] propose a collaborative trust model for firewalls in cloud computing. The model has three advantages: a) it uses different security policies for different domains; b) it considers the transaction contexts, historic data of entities and their influence in the dynamic measurement of the trust value; and c) the trust model is compatible with the firewall and does not break its local control policies.

A model of domain trust is employed. Trust is measured by a trust value that depends on the entity's context and historical behavior, and is not fixed. The cloud is divided in a number of autonomous domains and the trust relations among the nodes are divided in intra and inter-domain trust relations. The intra-domain trust relations are based on transactions operated inside the domain. Each node keeps two tables: a direct trust table and a recommendation list. If a node needs to calculate the trust value of another node, it first checks the direct trust table and uses that value if the value corresponding to the desired node is already available. Otherwise, if this value is not locally available, the requesting node checks the recommendation list in order to determine a node that has a direct trust

table that includes the desired node. Then it checks the direct trust table of the recommended node for the trust value of the desired node.

The inter-domain trust values are calculated based on the transactions among the inter-domain nodes. The inter-domain trust value is a global value of the nodes direct trust values and the recommended trust value from other domains. Two tables are maintained in the Trust Agents deployed in each domain: form of Inter-domain trust relationships and the weight value table of this domain node.

In [14] a trusted cloud computing platform (TCCP) which enables IaaS providers to offer a closed box execution environment that guarantees confidential execution of guest virtual machines (VMs) is proposed. This system allows a customer to verify whether its computation will run securely, before requesting the service to launch a VM. TCCP assumes that there is a trusted coordinator hosted in a trustworthy external entity. The TCCP guarantees the confidentiality and the integrity of a user's VM, and allows a user to determine up front whether or not the IaaS enforces these properties.

The work [15] evaluates a number of trust models for distributed cloud systems and P2P networks. It also proposes a trustworthy cloud architecture (including trust delegation and reputation systems for cloud resource sites and datacenters) with guaranteed resources including datasets for on-demand services.

4 TRUST MODEL FOR FILE EXCHANGE IN PRIVATE CLOUD

According to the review and related research [3-11, 13-16], it is necessary to employ a cloud computing trust model to ensure the exchange of files among cloud users in a trustworthy manner. In this section, we introduce a trust model to establish a ranking of trustworthy nodes and enable the secure sharing of files among peers in a private cloud.

The environment computing private cloud was chosen because we work with a specific context of distributing files, where the files have a desired distribution and availability.

We propose a trust model where the selection and trust value evaluation that determines whether a node is trustworthy can be performed based on node storage space, operating system, link and processing capacity. For example, if a given client has access to a storage space in a private cloud, it still has no selection criterion to determine to which cloud node it will send a particular file. When a node wants to share files with other users, it will select trusted nodes to store this file through the proposed following metrics: processing capacity (the average workload processed by the node, for example, if the node's processing capacity is 100% utilized, it will take longer to attend any demands), operating system (operating system that has a history of lower vulnerability will be less susceptible to crashes), storage capacity and link (better communication links and storage resources imply greater trust values, since they increase the node's capacity of transmitting and receiving information).

The trust value is established based on queries sent to nodes in the cloud, considering the metrics previously described.

Each node maintains two trust tables: direct trust table and the recommended list:

a) If a node needs to calculate the trust value of another node, it first checks the direct trust table and uses the trust value if the value for the node exists. If this value is not available yet, then the recommended lists are checked to find a node that has a direct trust relationship with the desired node the direct trust value from this node's direct trust table is used. If there's no value attached, then it sends a query to its peers requesting information on their storage space, processing capacity and link.

The trust values are calculated based on queries exchanged between nodes.

b) The requesting node will assign a greater trust value to nodes having greater storage capacity and / or processing and better link. In addition, the operating system will also be considered as a criterion of trust.

In this model is assumed that the node has a unique identity on the network. As trust is evolutionary, when a node joins the network, the requesting node doesn't know, soon it will be asked about his reputation to other network nodes. If no node has information about respective node (it has not had any experience with it), the requesting node will decide whether the requested relate to, initially asking some activity / demand for it to run. From its answers will be built trust with its node. Trust table node will contain a timer (saving behavior / events that raise and lower the trust of a given node) and will be updated at certain times.

Figure 2 presents a high level view the proposed trust model, where the nodes query their peers to obtain the information needed to build their local trust table.

In this model, a trust rank is established, allowing a node A to determine whether it is possible to trust a node B to perform storage operations in a private cloud. In order to determine the trust value of B, node A first has to obtain basic information about this node.

When node A needs to exchange a file in cloud and it wants to know if node B is trusted to send and store the file, it will use the proposed Protocol Trust Model, which can be described with the following scenario:

Step 1, node A sends a request to the nodes of cloud, including node B, asking about storage capacity, operating system, processing capacity and link.

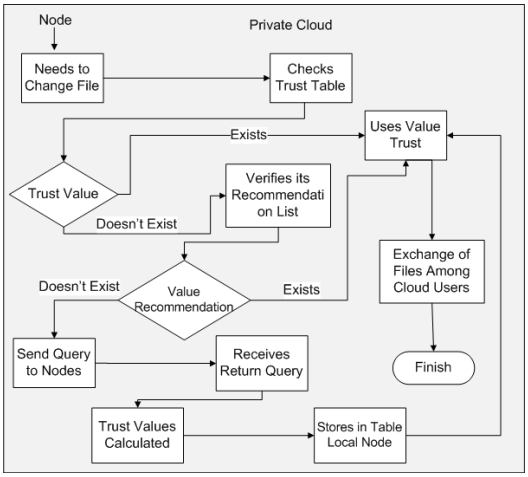

Figure 2 - High Level Trust Model

In step 2, nodes, including node B, send a response providing the requested information.

In step 3, node A evaluates the information received from B and from all nodes. If the information provided by B, are consistent with the expected, with the average value of the information of other nodes, the values are stored in local recommendations table of node A, after to make the calculation of trust and store in your local trust table.

The trust value of a node indicates its disposition/suitability to perform the operations between peers of cloud. This value is calculated based on the history

interactions/queries between the nodes, value ranging between [0, 1].

In general, trust of node A in node B, in the context of a private cloud NP, can be represented by a value V which measures the expectation that a particular node will have good behavior in the private cloud, so trust can be expressed by:

$$T_{(a,b)}^{np} = V_{np}^{(a,b)} \quad (1)$$

$T_{(a,b)}^{np}$ Represent the trust of A in B in the private cloud NP and $V_{np}^{(a,b)}$ represent the trust value of B, in the private cloud NP analyzed by A. According to definition of trust, $V_{np}^{(a,b)}$ is equivalent to queries sent and received (interaction) by A related to B in cloud NP. As the interactions are made between the nodes of private cloud, the information is used for the calculation of trust.

Nodes of a private cloud should be able to consider whether a trust value is acceptable, generating trust level. If the node exceeds the level within a set of analyzed values, it must be able to judge the node in a certain degree of trust. Trust degree can vary according to a quantitative evaluation: a node has a very high trust in another one, a node has low trust in another one, a node doesn't have sufficient criteria to opine, a node trusts enough to opine, etc. In our model, one node trusts another node from trust value $T \geq 0.6$ [5].

The trust values are calculated from queries between the nodes of NP, allowing obtaining the necessary information for final calculation of trust. The trust information is stored through the individual records of interaction with the respective node, staying in local database information about the behavior of each node in the cloud that wants to exchange a file (local trust table and local recommendations table).

Four aspects can to have impact on calculation of direct trust of a node. Greater storage capacity and processing capacity have more weight in the choice of a node more reliable, because of these features are the responsible for ensure the integrity and file storage.

To calculate direct trust of a node, it is attributed by administrator of the private cloud: storage capacity and processing with weights of 35%, 15% to link and the remaining 15% to operating system. Knowing that a node can to have the trust value ranging from [0.1] and that these values are variable over time, a node can have its storage capacity increased or decreased, it's necessary that trust reflects the behavior of a node in a given period of time. Nodes with constant characteristics should therefore be more reliable because they have less variation in basic characteristics.

According to the weights attributed it's possible to calculate the trust of node. The calculation of trust node A in B in cloud NP will be represented by:

(2)

$$T_{(a,b)}^{fnp} = \sum_{np=1}^{j} V_{np}^{b}$$

$$\frac{(((b,m_1)*0{,}35)+((b,m_2)*0{,}35)+((b,m_3)*0{,}15)+((b,m_4)*0{,}15)) \leq 1}{j}$$

$T_{(a,b)}^{fnp}$ Represents the final trust of A in B in cloud NP. The trust value of B is defined as the sum of metrics values that the node B has (m) in the cloud NP; j represents the number of interactions of trust from node A in B in the cloud NP, where $j \geq 0$.

4.1 Description of the Simulated Environment

In order to demonstrate the proposed objectives, it's necessary to define a simulation environment capable to measure / validate the metrics used,

expecting to achieve results according to the parameters and criteria of reliable information used in this work. Furthermore, the simulation environment acts as basis for further discussion, as well as the evolution of this proposal through new cloud computing environments.

Through the implementation of the simulation environment, it's possible to discuss and analyze the required parameters for a trust model in a private cloud, evaluate the generation of the local trust table of the nodes, as well as the effectiveness of the adopted metrics, and finally generate results that serve to discuss the problem of reliable exchange of files among peers in a private cloud.

The CloudSim simulation environment reproduces the interaction between a Infrastructure provider as Service (IaaS) and their customers [17].

The scenarios of the simulations of this work through CloudSim framework comprising a IaaS provider, which has three datacenters and a client that afford this service.

The client uses the resources offered by the provider for sending and allocation of virtual machines that perform a set of tasks, called cloudlets.

The dynamic data center of choice for sending and allocation of virtual machines and execution of cloudlets is defined by the utilization profile of the client and the resources offered by the provider. Thus, the scenario simulated in this work consists of a IaaS provider that has three datacenters distributed in different locations, Goiania, GO, Anapolis - GO and Brasília-DF, a customer with a usage profile, 04 hosts, 30 VMs and 100 cloudlets.

4.1.1 Results and analysis

When the simulation environment of CloudSim is defined and configured, and once the weights of the metrics are assigned, it can be performed the calculation of the trust of a node running the scenarios implemented in the framework.

To perform the simulation of the proposed environment it's initially necessary to define the settings that are considered ideal for a machine that is reliable, and then define the baseline machine configuration in order to compare with the values of other virtual machines of the simulation environment. As in the context of this application tasks are small and low complexity, the baseline configuration used is the one defined by the Amazon standard [18], trying to get closer as possible to the existing cost benefit in real clouds, where the settings of the machines are compatible with the charges and services offered.

The configuration used in this work is shown in Table 1.

Table 1. Configuration of the Baseline Machine [17]

Values Ideal	
HD Size	163840 MB
Memory RAM Size	1740 MB
MIPS Size	5000
Bandwidth Size	1024 Kbytes

In order to make comparisons and analysis of the results in various scenarios, several simulations were performed during the proposed work.

The trust of a virtual machine in the simulated model increases in proportion as human being, example, when an individual performs an activity or solve a

particular problem for us successfully, our trust is increased gradually. Thus, each cloudlet successfully executed, the trust value of a VM will be increased by 2.5%, until the trust level arrives at 0.85. Above 0.85, reliability increases 5% until it reaches the maximum trust of 1.0.

If a machine doesn't perform a certain task successfully, it doesn't solve its problem, it loses trust. The weight of suspicion is usually greater than the weight of trust. Thus, in our simulated model the rate of suspicion is 5% for each task performed without success.

In the attempt to simulate an environment closer to the reality, was conducted a simulation scenario which the cloudlets are not fully executed, allowing virtual machines to change their behavior over time, reflecting a fact more similar to a real environment of a private cloud computing. It was defined that an unsuccessful task is chosen randomly and that will occur when the random number is higher than 0.8, it means that the possibility of a successfully task in this scenario would be 80%. Thus, the simulation scenario can be changed, as desired.

Analyzing the results of the simulations, it's possible to identify the trust level of the virtual machines that performed the cloudlets. According to the reference information, a node trusts another from the value of trust $T \geq 0.6$.

In the simulation of the proposed scenario, some machines didn't perform cloudlets because they didn't fulfill the checking conditions of a reliable machine to perform a task, compared to the baseline machine.

The Table 2 presents the virtual machines that performed cloudlets. The other virtual machines did not perform any cloudlet do not satisfy the trust level desirable.

The simulation result is shown in Figure 3.

Table 2. Cloudlets/Tasks Performed Virtual Machines with Success and without Success.

Virtual Machines	Tasks performed successfully	Tasks performed unsuccessfully	Total
VM 03	00	01	01
VM 04	12	02	14
VM 05	08	02	10
VM 06	09	06	15
VM 07	01	02	03
VM 08	08	02	10
VM 13	03	01	04
VM 14	00	01	01
VM 15	07	01	08
VM 16	00	01	01
VM 24	00	01	01
VM 25	12	02	14
VM 26	13	01	14
VM 27	01	02	03
VM 28	00	01	01

The Figure 4 presents trust level of the virtual machine 09 that didn't perform any cloudlet during simulation, so there is no variation in the graph. All machines not performed any task have graph similar.

The Figure 5 presents the trust threshold of virtual machine 15 after changing its processing capacity (HD and RAM). During the simulation VM 15 performed 07 tasks/cloudlets successfully and 01 unsuccessfully. The variation trust level of the VM 15 was calculated in accordance to the successfully and unsuccessfully interactions. Every interaction successfully performed the trust value is increased by 2.5% and for

each interaction performed without success, the value is decremented by 5% of the threshold, as established weight.
Evaluating the results obtained with the change of both parameters of the VM 15 configuration, it's also possible to identify that all the simulated scenario has changed, impacting not only on the modified machine, but in the other virtual machines too. Moreover, the number of tasks/cloudlets executed with the change of the two scenarios was very close to the result obtained with the change made in storage capacity. With the results is possible to identify that the processing capacity has greater impact in the simulation results.

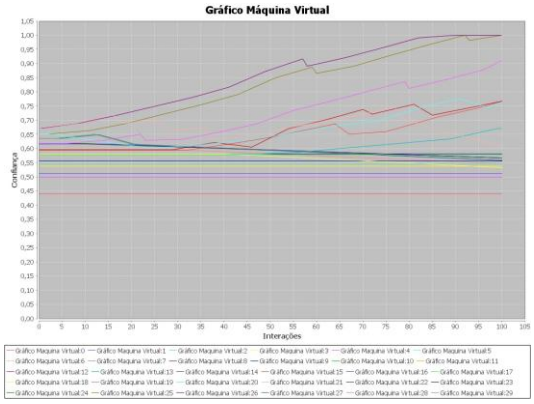

Figure 3 - Trust Virtual Machines after Task Execution.

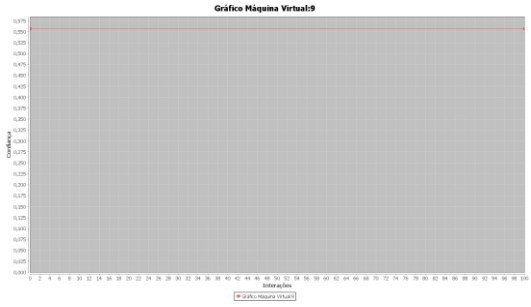

Figure 4 - Trust Virtual Machines 09 after 0 Task Execution.

The initial value trust threshold of the virtual machine 15 was 0.5935552586206897 and the final value 0.7442351812748581, as presents in Table 3.

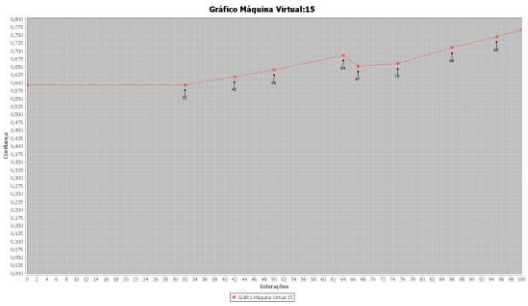

Figure 5 - Trust Virtual Machines 15 after 8 Task Execution.

Table 3. **Erro! Nenhum texto com o estilo especificado foi encontrado no documento.**Trust virtual machine 15 Running 07 Cloudlets with Success and 01 without Success.

Task Number	Trust threshold Virtual Machine 15 every Interaction
32	0.5935552586206897
42	0.6185552586206897
50	0.6402076105818058
54	0.6864683466109688
67	0.6514683466109688
75	0.6602111892581934
86	0.7098601812748581
95	0.7442351812748581

5 CONCLUSIONS

Cloud computing has been the focus of research in several recent studies, which demonstrate the importance and necessity of a trust model to ensure reliable and secure exchange of files. It is a promising area to be explored through research and experimental analyzes, using a computational trust to mitigate existing problems in aspects related to security, trust and reputation, to guarantee the integrity of exchange of information in private cloud environments, reducing the possibility of failure or alteration of information in the exchange of files, involving metrics that are able to represent or map the trust level of a network node in order to make the exchange of files in a private cloud.
The proposal discussed in this paper, to develop a new trust model for trusted

exchange of files, in an environment of private cloud computing, using the concepts of trust and reputation, seems to be promising, due to the identification of problems and vulnerabilities related to security, privacy and trust that a cloud computing environment presents.

Simulations and results allow to identify which adopted metrics directly influence the calculation of the trust in a node. The future simulations using a real environment will allow to evaluate the behavior of nodes in an environment of private cloud computing as well as historical of its iterations and assumed values throughout the execution of the machines.

The use of open platform, CloudSim [17], to execute the simulations of the adopted scenarios allowed to calculate the table trust of a node (virtual machines) and select those considered more reliable. Furthermore, the adequacy of the used metrics were evaluated in the proposed trust model, allowing to identify and select the most appropriate in relation to the historical behavior of the nodes belonging to the analyzed environment.

6 REFERENCES

1. Zhang Jian-jun and Xue Jing."A Brief Survey on the Security odel of Cloud Computing," 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES), Hong Kong IEEE, pp. 475 – 478, 2010.
2. Wang Han-zhang and Huang Liu-sheng."An improved trusted cloud computing platform model based on DAA and Privacy CA scheme," IEEE International Conference on Computer Application and System Modeling (ICCASM 2010). 978-1-4244-7235-2, 2010.
3. Uppoor, S., M. Flouris, and A. Bilas. "Cloud-based synchronization of distributed file system hierarchies," Cluster Computing Workshops and Posters (CLUSTER WORKSHOPS), IEEE International Conference, pp. 1-4. 2010.
4. Popovic, K. and Z. Hocenski. "Cloud computing security issues and challenges," MIPRO, 2010 Proceedings of the 33rd International Convention, pp. 344-349, 24-28 May 2010.
5. Stephen Paul Marsh, "Formalising Trust as a Computational Concept", Ph.D. Thesis, University of Stirling, 1994.
6. Thomas Beth, M. Borcherding, and B. Klein, "Valuation of trust in open networks," In ESORICS 94. Brighton, UK, November 1994.
7. Lamsal Pradip. (2006). "Understanding Trust and Security". Department of Computer Science University of Helsiki, Finland, October 2001. Acessado em 13/02/2006. Disponível em: http://www.cs.helsinki.fi/u/lamsal/asgn/trust/UnderstandingTrustAndSecurity.pdf
8. Gambetta Diego. (2000). "Can We Trust Trust?", in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, chapter 13, 213-237.
9. Josang Audun, Roslan Ismail, Colin Boyd. (2007). A Survey of Trust and Reputation Systems for Online Service Provision. Decision Support Systems. Volume 43 Issue 2, March. Elsevier Science Publishers B. V. Amsterdam, The Netherlands, The Netherlands.
10. Patel, Jigar. "A Trust and Reputation Model for Agent-Based Virtual Organizations". Thesis of Doctor of Philosophy. Faculty of Engineering and Applied Science. School of Electronics and Computer Science. University of Southampton. January. 2007.
11. Xiao-Yong Li, Li-Tao Zhou, Yong Shi, and Yu Guo, "A Trusted Computing Environment Model in Cloud Architecture," Proceedings of the Ninth International Conference on Machine Learning and Cybernetics, 978-1-4244-6526-2. Qingdao, pp. 11-14. China. July 2010.
12. Zhidong Shen, Li Li, Fei Yan, and Xiaoping Wu, "Cloud Computing System Based on Trusted Computing Platform," Intelligent Computation Technology and Automation (ICICTA), IEEE International Conference on Volume: 1, pp. 942-945. China. 2010.
13. Zhimin Yang, Lixiang Qiao, Chang Liu, Chi Yang, and Guangming Wan, "A collaborative trust model of firewall-through

based on Cloud Computing," Proceedings of the 2010 14th International Conference on Computer Supported Cooperative Work in Design. Shanghai, China. pp. 329-334, 14-16. 2010.

14. Santos Nuno, K. Gummadi, and R. Rodrigues, "Towards Trusted Cloud Computing," Proc. HotCloud. June 2009.
15. Chang. E, T. Dillon and Chen Wu, "Cloud Computing: Issues and Challenges," 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 27-33. Australia, 2010.
16. Kai Hwang, Sameer Kulkareni, and Yue Hu, "Cloud Security with Virtualized Defense and Reputation-Based Trust Mangement," 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC '09), pp. 717-722, 2009.
17. Calheiros, Rodrigo, N.; Rajiv Ranjan; Anton Beloglazov; De Rose, Cesar, A. F.; Buyya, Rajkumar. (2011). "CloudSim: A Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms, Software: Practice and Experience (SPE)", Volume 41, Number 1, 23-50, ISSN: 0038-0644, Wiley Press, New York, USA, January.
18. Amazon (2012). "Amazon Web Services". Accessed in 01/06/2012. Available: http://aws.amazon.com/pt/ec2/instance-types/.