Aswini *et al*, Journal of Computer - JoC,
Available Online at: www.journal.computer
Vol.1 Issue. 2, July- 2016, pg. 9-15 **ISSN: 2518-6205 (Online)**

An Efficient Approach to Trust Broker Module in Multiple Cloud Services

Aswini[1], Dr. K. R. Suneetha[2]
[1]Department of Computer Science, Bangalore Institute of Technology, Bangalore, India
[2]Associate Professor, Department of Computer Science, Bangalore Institute of Technology, Bangalore, India
[1] ashwini.sorade123@gmail.com; [2] suneetha.bit@gmail.com

Abstract- ***A trust aware service brokering scheme for efficient matching cloud services to satisfy various user requests for Multiple Cloud Collaborative Services. First, a trusted third party-based service brokering architecture is proposed for multiple cloud environments, in which the T-broker acts as a middleware for cloud trust management and service matching. Then, T-broker uses a hybrid and adaptive trust model to compute the overall trust degree of service resources, in which trust is defined as a fusion evaluation result from adaptively combining the direct monitored evidence with the social feedback of the service resources. T-broker uses a lightweight feedback mechanism, which can effectively reduce networking risk and improve system efficiency. The experimental results show that, compared with the existing approaches, our T-broker yields very good results in many typical cases, and the proposed system is robust to deal with various numbers of dynamic service behavior from multiple cloud infrastructures.***

Keywords: Multiple Cloud Computing, feedback aggregation, cloud computing, Trust

1. INTRODUCTION

Cloud computing approach is developing as a significant trend in high-performance computing. Cloud computing deliver a variety of IT enabled hardware, software resources and services to users over the internet. Cloud computing services are Software as a service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)[1]. Virtualization is an innermost part for cloud architecture. Today's, cloud computing normally used by technical, non technical field and academic societies, has been fast to enter the commercial field.

Trust management provides a good way for improving the security. Managing trust is fundamental part in cloud scenarios considering its characteristics such as dynamic in nature, scalability, resource pooling, on demand self service. It is a new security mode to provide security state, reliability, and access control policies. For assessment, identifying and distributing malicious entities based on changing and mining the detected results for security mechanism in different systems and collecting feedback assessment. Feedback, recommendation, reviews from the users is valuable for service selection in e-market. Recently, a cloud marketplace [2] has been launched to support consumers in identifying dependable cloud service providers.

They are rated based on questionnaire that needs to be filled in by current cloud service users. Cloud common aims to combine consumer feedback with technical measurements for assessing and comparing the trustworthiness of cloud providers.

Trust establishment is based on the facts of experiences collected from the previous interactions of entities. In general, if the interactions conform to the purpose of the cloud service provider, then trust evaluation will be correspondingly high in perception of service providers. Otherwise, it will be accordingly low. In this paper, a formal trust model has been proposed for cloud environment from the basic concepts of trust. In the proposed approach, moreover time based experience, reputation concepts and also has been considered trust relationship (direct or recommended trust) for calculating the rating based of both entities in cloud environment. In the model, it has been perceived that before providing or accessing the service from/to the cloud environment. Service user as well as service provider will ensure the trustworthiness of each other with different level of access according to SLAs, data security, performance, utilization etc. Further, the model is capable to update the rating value dynamically for each entity of the cloud.

The remaining sections of the paper are structured as follows. Section 2 discusses related research work carried out in the field of trust management in cloud computing. In Section 3 introduce trust factor and its definition. Overview of proposed trust model is presented in section 4. Section 5 describes the rating evaluation and updating methods for cloud entities. Finally conclusion and future work are presented in the last section.

2. LITERATURE REVIEW

In recent years, many research scholars have made a lot of research on trust model measuring the trustworthiness and managing the trust relationship. The most common one is reputation based trust management mechanism, which has been widely used in online electronic communities and distributed environment [3].

Tabaki et al.[4] illustrated the unique issues of cloud computing consisting of different modules to handle security and trust issues of key components. Khaled M. Khan[5] hold that trusting cloud computing might differ from trusting other systems, but any new technology must gradually build its reputation for good performance and security earning users' trust over time.

Ranchal et al. studied the identity management in cloud computing and proposed a system without the involvement of trusted third party [6]. Kwei-Jay Lin et al. [7] propose a distributed trust management for e-services such as e-commerce. In their broker framework where every user is associated with a broker who collects for its users the reputation ratings about any web services. The user provides its broker the service rating each interaction with any service in order to build up the reputation for the service. Shantanu pal et al. [8] proposed security and privacy solution lies both at the service provider level as well as service user level in a cloud environment. Their framework can provide security, infrastructure as well as data stored in cloud platform. Manuel et al. [9] have proposed trust model for both grid and cloud system that is integrated with CARE resource broker. Habib et al. [10] have survey the trust related issues in cloud computing i.e., SLAs, audits, rating and measuring, self assessment questionnaires etc.

3. TRUST FACTOR

The factors used for proposed trust model are described below:

A. Trust

Trust is complex and an integral component in many kinds of human interaction, allowing people to act under uncertainty and with the risk of negative cost. Trust is related to a certainty in attributes such as honesty, dependability, timeliness, security, competence, reliability, truthfulness, etc., of the trusted entities to act as expected. Certainty is not a fixed value associated with the entity, but rather it is subjected to the entities activities and applied only within a specific context at a given time [11].

B. Reputation

The reputation of an entity is a belief of its activities based on other entities' observation or information about the entity's past activities at a given time [12].

C. Trustworthiness

The entity's trustworthiness is an indicator of quality of the entity's services.

D. Feedback Evaluator

A feedback is a statement issued by the users about the quality of service provided by provider in a single transaction [9]. Feedback evaluator is receiving user's feedback, verifying the feedback and updating the value in the feedback data repository. Service user feedback is an important factor in a cloud trust model for accessing cloud services. The feedback of the user can ensure the dependability of cloud resources. The service user's feedback helps to improve the performance of the service providers.

E. Definitions of Trust Type

1. *Direct Trust (DT):* DT is the principle that one participant trusted in other participant with use the

Aswini *et al*, Journal of Computer - JoC,
Available Online at: www.journal.computer
Vol.1 Issue. 2, July- 2016, pg. 9-15 **ISSN: 2518-6205 (Online)**

reference of trust value.

2. Recommendation Trust (RT): RT is the principle that the ability of a participant is decided by third participant whether it is reliable in a given trust value before recommending to other

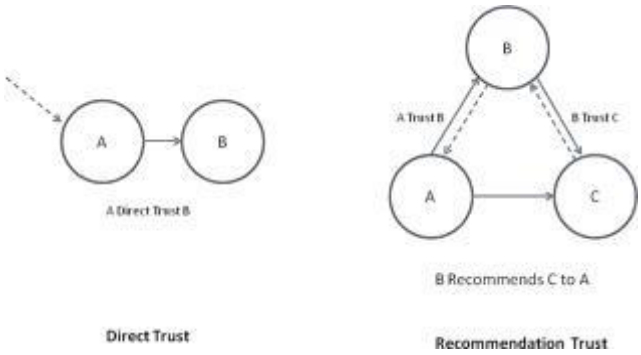

Figure 1. Direct and Recommendation Trust

4. OVERVIEW OF PROPOSED TRUST MODEL

Most current cloud brokering systems do not provide trust management capabilities to make trust decisions, which will greatly hinder the development of cloud computing. Depicts the brokering scenario in existing and Aeolus We can see that this existing brokering architecture for cloud computing do not consider user feedback only relying on some direct monitoring information.

As depicted T-broker architecture, a service brokering system is proposed based on direct monitoring information and indirect feedbacks for the multiple cloud environments, in which T-broker is designed as the TTP for cloud trust management and resource matching.

Before introducing the principles for assessing, representing and computing trust, we first present the basic architecture of T-broker and a brief description of its internal components.

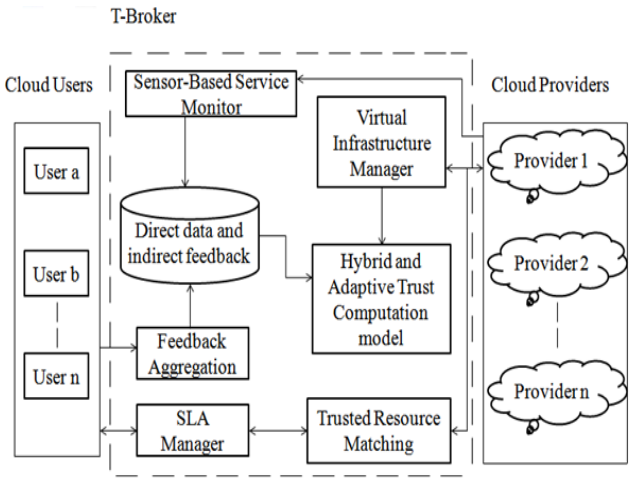

Fig. 2: T-Broker Architecture

T-Broker Module In this module T-broker uses some sub modules,

A. Trust-Aware Brokering Architecture

In which the broker itself acts as the TTP for trust management and resource scheduling. Through distributed soft-sensors, this brokering architecture can real-time monitor both dynamic service behavior of resource providers and feedbacks from users.

B. Hybrid and Adaptive Trust Computation Model (HATCM)

A hybrid and adaptive trust model to compute the overall trust degree of service resources, in which trust is defined as a fusion evaluation result from adaptively combining dynamic service behavior with the social feedback of the service resources.

The HATCM allows cloud users to specify their requirements and opinions when accessing the trust score of cloud providers. That is, users can specify their own preferences, according to their business policy and requirements, to get a customized trust value of the cloud providers.

C. Maximizing deviation method (MDM)

A maximizing deviation method to compute the direct trust of service resource, which can overcome the limitations of traditional trust models, in which the trusted attributes are weighted manually or subjectively. At the same time, this method has a faster convergence than other existing approaches.

D. Sensor-Based Service Monitoring (SSM)

This module is used to monitor the real-time service data of allocated resources in+ order to guarantee the SLA (Service Level Agreement) with the users. In the interactive process, this module dynamically monitors the service parameters and is responsible for getting run-time service data. The monitored data is stored in the evidence base, which is maintained by the broker.

To calculating QoS-based trustworthiness of a resource we mainly focus on five kinds of trusted attributes of cloud services, which consist of node spec profile, average resource usage information, average response time, average task success ratio, and the number of malicious access. The node spec profile includes four trusted evidences: CPU frequency, memory size, hard disk capacity and network bandwidth. The average resource usage information consists of the current CPU utilization rate, current memory utilization rate, current hard disk utilization rate and current bandwidth utilization rate. The number of malicious access includes the number of illegal connections and the times of scanning sensitive ports.

E. Virtual Infrastructure Manager (VIM)

Each cloud provider offers several VM configurations, often referred to as instance types. An instance type is defined in terms of hardware metrics such as CPU frequency, memory size, hard disk capacity, etc. In this work, the VIM component is based on the OpenNebula virtual infrastructure manager this module is used to collect and index all these resources information from multiple cloud providers. It obtains the information from each particular cloud provider and acts as a resource management interface for monitoring system.

Cloud providers register their resource information through the VIM module to be able to act as sellers in a multi-cloud marketplace. This component is also responsible for the deployment of each VM in the selected cloud as specified by the VM template, as well as for the management of the VM life-cycle.

The VIM caters for user interaction with the virtual infrastructure by making the respective IP addresses of the infrastructure components available to the user once it has deployed all VMs.

F. Service level agreement Manager (SLA)

In the multiple cloud computing environments, SLA can offer an appropriate guarantee for the service of quality of resource providers, and it serves as the foundation for the expected level of service between the users and the providers An SLA is a contract agreed between a user and a provider which defines a series of service quality characters.

Adding trust mechanism into the SLA management cloud brokering system can prepare the best trustworthiness resources for each service request in advance, and allocate the best resources to users. In general, the service resource registers its services on the cloud brokering system. The service user negotiates with the service provider about the SLA details; they finally make a SLA contract. According to the SLA contract, the resource matching module selects and composites highly trusted resources to users from the trusted resource pool.

G. Multiple Clouds Computing

Multiple cloud theories and technologies are the hot directions in the cloud computing industry, which a lot of companies and government are putting much concern to make sure that they have benefited from this new innovation However, compared with traditional networks, multiple cloud computing environment has many unique features such as resources belonging to each cloud provider, and such resources being completely distributed, heterogeneous, and totally virtualized; these features indicate that unmodified traditional trust mechanisms can no longer be used in multiple cloud computing environments

A lack of trust between cloud users and providers has hindered the universal acceptance of clouds as outsourced computing services. Thus, the development of trust awareness technology for cloud computing has become a key and urgent research direction

Today, the problem of trusted cloud computing has become a paramount concern for most users. It's not that the users don't trust cloud computing's capabilities; rather, they mainly question the cloud computing's trustworthiness.

H. Feedback Aggregation

The "Trust as a Service" (TaaS) framework to improve ways on trust management in cloud environments. In particular, the authors introduce an adaptive credibility model that distinguishes between credible trust feedbacks and malicious feedbacks by considering cloud service consumers' capability and majority consensus of their feedbacks.

However, this framework does not allow assessing trustworthiness based on monitoring information as well as users' feedback.

In large-scale distributed systems, such as grid computing, P2P computing, wireless sensor networks, and so on, feedback provides an efficient and effective way to build a social evaluation- based trust relationship among network entities. By the same token, feedbacks also can provider important reference in evaluating cloud resource trustworthiness.

Consider large-scale cloud collaborative computing environment which host hundreds of machines and handles thousands of requests per second, the delay induced by trust system can be one big problem. So, there is no doubt that the computational efficiency of a feedback aggregating mechanism is the most fundamental requirement. As depicted in Fig. 3, we build cloud social evaluation system using feedback technology among virtualized data centers and distributed cloud users, and we use a lightweight feedback mechanism, which can effectively reduce networking risk and improve system efficiency.

5. CLOUD TRUST COMPUTATION MODEL

Trustworthiness computation model and approaches are the core technologies of trust management.

In our T-broker, we propose a hybrid and adaptive trust model to compute the overall trust degree of service resources, in which trust is a fusion evaluation result from adaptively combining real-time trust computation with the feedback of the service resources. There are two approaches, namely

1. Adaptive Real-Time Trust Computation
2. Light-Weight Feedback Trust Computation

Then these approaches are combined as, trust calculation approach

A. Adaptive Real-Time Trust Computation

For calculating resource trust degree from the perspective of QoS guaranteeing. There are total 12 QoS indicators (or service behavior) needed to be acquired, quantified and analyzed.

B. Light-Weight Feedback Trust Computation

The feedback system collects locally-generated users' ratings and aggregates these ratings to yield the global evaluation scores. After a user completes a transaction, the user will provide his or her rating as a reference for other users in future transactions.

C. Hybrid and Adaptive OTD Aggregation

We adopt the idea that overall trust degree (OTD) comprises two parts: First-hand trust (trust based on real-time and multi-source service data) and second-hand trust (feedback)

This hybrid trust calculation approach is based on a combination of two kinds of known trust methodologies: feedback-based trust and experience-based trust. The key idea is that by combining two different methodologies, the resulting integrated framework improves some weaknesses of the constituent methodologies and, consequently, the overall assessment of cloud services.

6. CONCLUSION

In this paper, we present T-broker, a trust-aware service brokering system for efficient matching multiple cloud services to satisfy various user requests. Experimental results show that T-broker yields very good results in many typical cases, and the proposed mechanism is robust to deal with various number of service resources. In the future, we will continue our research from two aspects. First is how to accurately calculate the trust value of resources with only few monitored evidences reports and how to motivate more users to submit their feedback to the trust measurement engine. Implementing and evaluating the proposed mechanism in a large-scale multiple cloud system, such as distributed data sharing and remote computing, is another important direction for future research.

REFERENCES

[1] P. Mell and T. Grance, ―The NIST definition of cloud computing (draft),‖ NIST special publication, 2011, 800 no.(145), 7.

[2] S.K Garg, S. Versteeg, and R. Buyya, ―Smicloud: A framework for comparing and ranking cloud services,‖ Fourth IEEE International Conference on Utility and Cloud Computing (UCC), 2011, pp. 210-218.

[3] D. Quercia, S. Hailes, and L. Capra, "B-trust: Bayesian trust framework for pervasive computing," In Proceedings of iTrust. LNCS, 2006, pp. 298-312.

[4] H. Tabaki, J. Joshi, and G.-J. Ahn, ―Security and privacy challenges in cloud computing environments,‖ IEEE Security & Privacy, vol. 8, no. 6, Nov.-Dec. 2010, pp. 24–3.

[5] K.M. Khan and Q. Malluhi, ―Establishing Trust in Cloud Computing,‖ IT Professional, Vol. 12 no.5, Sept.-Oct. 2010, pp. 20 - 27.

[6] R. Ranchal, B. Bhargava, L. B. Othmane, A. Kim, M. Kang, & M. Linderman, ―Protection of identity information in cloud computing without trusted third party,29th IEEE Symposium on Reliable Distributed Systems, Oct. 2010, pp. 368-372.

[7] Kwei-Jay Lin , Haiyin Lu , Tao Yu , Chia-en Tai, ―A Reputation and Trust Management Broker Framework for Web Applications‖, Proceedings of the 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'05) on e-Technology, e-Commerce and e-Service, March-April 2005 pp .262-269, [doi>10.1109/EEE.2005.14].

[8] S. Pal, S. Khatua, N. Chaki, & S. Sanyal, (2011). ―A new trusted and collaborative agent based approach for ensuring cloud security,‖ Annals of Faculty Engineering Hunedoara International Journal of

Engineering; scheduled for publication in Vol. 10, Issue 1, February, 2012. ISSN: 1584-2665.

[9] P. D. Manuel, S. Thamarai Selvi, & M. E. Barr, ―Trust management system for grid and cloud resources,‖ IEEE *First International Conference on* Advanced *Computing, ICAC 2009*. pp. 176-181.

[10] Sheikh MahbubHabib, SaschaHauke, Sebastian Ries and Max M¨ uhlh¨auser, ―Trust as a facilitator in cloud computing: a survey, Journal of Cloud Computing: Advances, Systems and Applications,Springer2012. http://www.journalofcloudcomputing.com/content/1/1/19.

[11] T. Grandison, M. Sloman, ―A Survey of Trust in Internet Applications,‖. IEEE Communications Surveys and Tutorials, 3, 2000

[12] B. Ma, S. Jizhou, and Y. Ce, ―Reputation-based Trust Model in Grid Security System,‖ Journal of Communication and Computer, Vol. 3, no.8, 2006.

