International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Trust Management for Service Clouds

R.Kanimozhi[1], R.Veerathirumagan[2]
[1]Assistant Professor, [2]Final Year Student

Abstract*—This paper proposes a service operator-aware trust theme (SOTS) for resource matchmaking across multiple clouds. Through analyzing the inherent relationship between the users, the broker, and also the service resources, this paper proposes a middleware framework of trust management that may effectively reduce user burden and improve system reliableness. Supported three-dimensional resource service operators, we tend to model the matter of trust analysis as a method of multi-attribute decision-making, and develop associate degree and aptational trust analysis approach supported data entropy theory. This adaptational approach will overcome the constraints of ancient trust schemes, whereby the trusty operators are weighted manually or subjectively. As a result, using SOTS, the broker will with efficiency and accurately prepare the foremost trusty resources earlier, and so offer additional dependable resources to users. Our experiments yield attention-grabbing and meaningful observations that may facilitate the effective utilization of SOTS in an exceedingly large-scale multi-cloud setting.

I. INTRODUCTION

A vital part of cloud computing is trust, and therefore the downside of a trustworthy cloud service is of preponderating concern for enterprises and users [1]. Users are willing to send their most sensitive knowledge to cloud service centers, that relies on the trust relationship established between users and repair providers. an absence of trust between cloud users and suppliers will seriously hinder the universal acceptance of clouds as outsourced computing services [2].

II. MOTIVATION

Although many students are attracted by the trust question of cloud service, and lots of studies are distributed a universal and swollen trust theme designed specifically for a multi-cloud computing atmosphere continues to be lacking, and former studies have some key limitations:

(1)Few studies have targeted on a trust-aware brokering framework for multi-cloud environments. Cloud brokers will give intercession and aggregation capabilities to modify suppliers to deploy their virtual infrastructures across multiple clouds the longer term of cloud computing are going to be penetrate

A. Our Contributions

Inspired by the thought of associate expanded trust analysis approach in ,in commission operator-aware trust scheme(SOTS), we have a tendency to outline trust as a quantified belief by a cloud broker with relevance the protection, convenience, and dependability of a resource among many such time windows. This definition belongs to associate approach supported sure third party (TTP) The broker acts because the TTP, that consists of the many registered resources. The key innovations of SOTS transcend those of existing schemes in terms of the subsequent aspects:

A scientific trust management theme for multi-cloud environments, supported multi-dimensional resource service operators. SOTS evaluates the trust of a cloud resource in distinction to ancient trust schemes that continually concentrate on unilateral trust factors of service resources. It incorporates multiple factors into a trust vector to make associate expanded trust theme to judge a resource. This trust theme is additional per the essential attributes of a trust relationship, thus, it's additional in line with the expectations of cloud users.

An adaptational amalgamate computing approach for dynamic service operators, supported info entropy theory .SOTS models the matter of trust analysis as a method of multi-attribute decision-making, and then develops an adaptational trust analysis approach. This adaptational amalgamate computing approach will overcome the restrictions of ancient trust schemes, within which the trusty attributes square measure weighted manually or subjectively.

A primary service, last audit (FSLA) mechanism to beat the trust formatting drawback of new registered resources. When a resource at the start registers for business ,no user has interacted with it, and consequently, info on past service operators is non-existent. In SOTS, we have a tendency to introduce a penalty factor-based FSLA mechanism, which might effectively remedy this drawback of

©IJRASET 2013: All Rights are Reserved

new registered resources.These styles and different specific options (e.g., a statistics based activity approach for multi-dimensional trust operators and a time series-based world trust predicting method) together build SOTS an correct and economical answer that may be utilized in multi-cloud environments.The rest of this paper is organized as follows: Section two provides summary of connected work. The cloud brokering design is delineated in Section three. Sectionf our outlines the details of trust analysis for across-cloud resources. Section5 provides some key implementing technologies. The Experimental results square measure econferred in Section vi. Finally, Section 7summarizes this work and suggests some future directions.

III. RELATED WORK

Trust within the cloud system from the user's perspective. They analyzed problems with trust from a cloud users expectations, with relevancy their information in terms of security and privacy. So far, several innovative trust schemes for cloud computing are projected by researchers, and 3 main categories may be known as follows:

Reputations-based schemes. employing a trust-overlay network over multiple information centers to implement a name system for establishing trust between suppliers and information homeowners. information coloring and software package watermarking techniques shield shared information objects still as massively distributed software package modules. However, the authors solely targeted on reputation-based trust issues; they failed to mention the trust problem at server level. Self-assessment schemes. Kim et al. given a trust analysis model to allot cloud resources supported suppliers, self-assessment. Their trust model collects and analyzes dependableness supported the historical server info in an exceedingly cloud information center. Although the model in could be a multiple attribute theme, the authors fully unheeded the real time scenario in trust relationships, which can result in An incomplete trust decision-making outcome.

In, Li and rule bestowed a sure knowledge acquisition mechanism for planning cloud resources and satisfying numerous user requests victimization their trust mechanism, cloud suppliers will expeditiously utilize their resources, yet as give extremely trustworthy resources and services to users. However, because of a scarcity of transparency, these self-assessment schemes don't fully eliminate users' trust considerations.

TTP-based schemes. Habib et al. projected a multi-attribute trust system for a cloud marketplace. this method provides means for distinctive cloud suppliers in terms of various attributes (e.g., security, performance, compliance) that area unit assessed by multiple sources of trust data.

However, mensuration these trust attributes while not giving details. though there area unit some similar works out there in literatures, e.g., that mentioned the multiple attribute issues of trust, very little detail has been provided.

IV. TRUST-AWARE BROKERING ARCHITECTURE

Referring to the description methods on "trust" in , we first give the related definitions of "trust" that are used in SOTS.

A. Definitions, Conceptual Model And Assumptions

Referring to the description methods on "trust" in ,we first give the related definitions of "trust" that are used in SOTS.

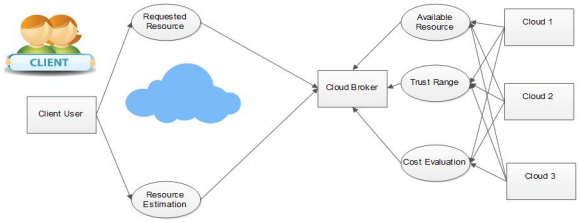


Fig. 1. Conceptual model

Definition 1 (Trust of a Resource). Trust is a quantified belief(or a measured value) in the competence of a resource to complete a task, based on its historical service operators. Definition 2 (TTP-based Trust Relationship). A user will trust a service resource if the matchmaker (broker) states that the resource's operators will match the user's request. Definition 3 (Trust Evaluation Factors). The trust worthiness of a resource is evaluated by the broker according to multiple service operators with respect to the security, availability, and reliability of this resource within several specified time windows. According to Definitions 1 and 2, SOTS belongs to the TTP-based approach , with the broker acting as the TTP.

According to Definition 3, SOTS is also an expanded trust evaluation approach , beyond traditional trust schemes, that always focus on one-sided trust factors of service resources. The expanded trust model incorporates security, reliability, and availability factors

©IJRASET 2013: All Rights are Reserved

into a trust vector. Thus, the new trust scheme will contain data that can be imported, from existing models (that is, security, reliability, availability)to form a comprehensive trust model for a multiple cloud environment.

Fig. 1 shows the conceptual model of the trust-aware resource matchmaking approach. According to Definition 2, our trust scheme depends on the cloud broker, who acts as the TTP for users. The broker can evaluate each resource performance during particular time windows, thereby configuring services dynamically and distributing tasks efficiently. Whenever a new resource wants to offer its services, it must join the service network. On the client side, a user looking for a service must send a query, together with his policies, to the trusted broker. According to the trust evaluation results, the broker will select a suitable resource by applying a matching algorithm. Whenever a service resource matches, the cloud broker will distribute the user's task to the resource through its manager.

The underlying assumption of this TTP-based approach is that users must trust the third-party broker they decide to consult. In actual cases, these brokering systems are often managed by larger ISPs with good reputation, so the services from these ISPs should have a higher dependability. We assume that all resources have unique identities, such as the IP address, and that each cloud manager (site) can register its resources through these unique identities. This paper mainly focuses on the trust management system of server sides; thus, we also assume that each cloud site has a security mechanism to resist attacks from malicious users.

B. Trust-Aware Brokering System Architecture

the proposed middleware architecture consists of a number of core modules, including the trusted resource matchmaking and distributing module, the adaptive trust evaluation module, the agent-based service operator acquisition module, and the resource management module, among others.

Adaptive trust evaluation module. This module is the core of the trust-aware cloud computing system, and is the major focus of this paper. Using this module, the broker can dynamically sort high-performance resources by analyzing the historic resource information in terms of providing highly trusted resources. Trusted resource matchmaking and distributing module. In general, each cloud manager registers its service resources through the cloud broker. The service user negotiates with the service broker on the service-level agreement (SLA) details ; they eventually prepare an SLA contract. According to this contract, the broker selects, and then presents highly trusted resources to users from the trusted resource pool.

Agent publish and service operator acquisition module. This module is used to monitor the usage of allocated resources in order to guarantee the SLA with the user. In interaction, the module monitors the resource operators and is responsible for getting run-time service operators. Another task ofthe module is to publish automatically the monitoring agents (MA) in a remote site when a computing task is assigned to the site.

Resource register module. It manages and indexes all the resources available from multiple cloud providers, and obtains information from each particular cloud resource, acting as pricing interface for users, and updating the database when new information is available.

C. Statistics-Based Service Operator Measurement

When matchmaking a resource for users, the cloud broker must first consider whether the resource has the required capabilities (for example, CPU frequency, memory size, and hard disk capacity), and second, whether it is likely to complete the task successfully . The first of these considerations can be evaluated by the resource's availability, which can determine whether a resource has the required capability or not. The second consideration mainly focuses on the reliability and security of the resource, which can be evaluated by the resource's service operators. Reliability refers to the probability of service for a given duration, and we use, six operators to reflect this factor. The most basic needs of security pertain to the absence of unauthorized access to a system. We use the security levels of a service site to evaluate security

V. ADAPTIVE AND EFFICIENT TRUST EVALUATION

A. Evaluation Matrix Normalization

In the process of trust evaluation, the operator set should be normalized to eliminate deviations in the results caused by each operator item's difference in the value domain.

B. Real-Time Trust Degree (RTD)

In the proposed scheme, RTD is used to evaluate recent cloud resource service operators, and RTD is evaluated by knowledge of a resource's quality of service. Hence, RTD is a time window-based trusted indicator for service operators, and it should be more

©IJRASET 2013: All Rights are Reserved

sensitive to new operators. RTD is generated in the time window when an interaction takes place between a user and a resource

C. Algorithm Explanation

1) Global Trust Degree (GTD) Calculation: Step1: Calculate the values for CPU frequency, memory size, hard disk capacity and the average bandwidth using evaluation of matrix normalization.

Step2: Calculate the information entropy expression of the trust decision factor, based on their self-information using entropy based and adaptive weight calculation.

Step3: RTD (Real-time Trust Degree) is used to evaluate recent cloud resource service operators. RTD is generated in the time window when an interaction takes place between a user and a resource.

VI. IMPLEMENTATION TECHNOLOGIES

A. Overall Implementation Algorithm

We use an example to illustrate the overall algorithm for GTD calculation. Suppose that six cloud resources need to be evaluated by the broker.

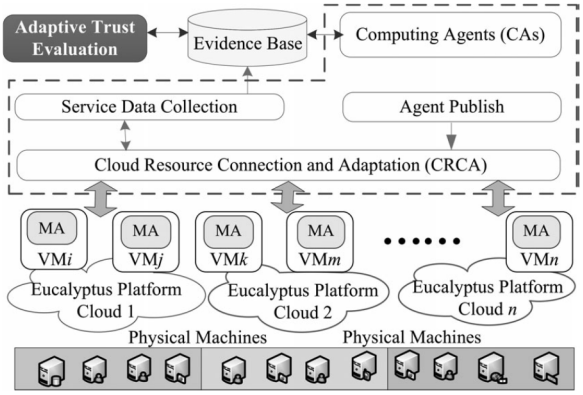
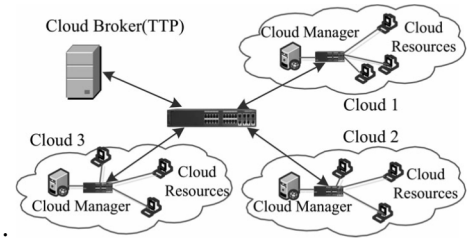


Fig. 2.

VII. EVALUATION AND COMPARISON

In this section, we first describe how to set up the experimental prototype system in an Eucalyptus-based cloud environment, including how to deploy SOTS on the Eucalyptus-based environment and how to set the experiment configurations. Then, the experimental results are described.

Fig. 3



A. Experimental Methodology

To evaluate the trust scheme based on technologies introduced in Sections 3 and 5, we set up a multiple cloud environment that is composed of three clusters (Fig. 3). Each cluster is managed by a cloud manager (3.2 GHz CPU, 4 GB memory, and 1 TB hard disk) running Ubuntu Linux 10.04(kernel 2.6.35-24) and Eucalyptus version 1.6.1. In each cluster(cloud), the operating system running in the virtual machines is a customized Scientific Computing as a Service(SCaaS). Each cloud under test is fully based on the Eucalyptus framework and the KVM hypervisor .In Fig. machines in each cluster act as VM providers, in which an agent-based service operator acquisition module is deployed. A separate machine acts as the trust management server (cloud broker) where the core functional modules of the broker are deployed, including a trusted resource matchmaking and distributing module, an adaptive trust evaluation module, and a resource management module. We have designed several performance mechanisms for a

©IJRASET 2013: All Rights are Reserved

comprehensive trust evaluation scheme. Due to the restrictions of paper length, we mainly evaluate the performance of SOTS based on the following two aspects:

Accuracy is used to check whether the proposed scheme and its related algorithms can accurately and consistently provide trust calculation;

Efficiency is used to evaluate the overhead and the average job failure rate (AJFR) of the proposed scheme;

User request. In the experimental environment, there are nearly 100 VMs in the resource pool of the cloud broker system (we deployed about 30 VMs in each cluster). According to Algorithm 1 in Appendix E, available in the online supplementary material, our resource match making approach should be "trust with cost." The user's request contains the job descriptions; namely, Job ID, minimum GTD required, and cost limits. Considering the job requirements, a resource is selected from a resource pool that has more than the minimum GTD given by the user. Types of VMs. To reduce complexity, in the initial stage of the experimental environment, we mainly observe the results according to the following 6 key operators: CPU frequency(CPU), average response time, average task success rate (ATSR), authentication type, authorization type, and self-security competence. Types of VMs in the resource pool and the classification threshold are listed in Table 3, including high trusted node (H), normal trusted node (N), low trusted node (L) and malicious node (M).

B. Accuracy Evaluation

Some service operators are more sensitive to users requirements, including average response time, average task success rate and resource security levels. Relative to a given user-sensitive trust operator, an accuracy trust scheme should be robust enough to detect operators with a smaller value. Hence, we observe the detecting capacity of the proposed scheme for low-value operators.

Using 10 time windows we gather 1,500 training samples from three clusters. For purposes of comparison, we also implement two other typical trust evaluation schemes: the weighted average trust model (WATM) [3] and the multi-dimensional trust model (MDTM)

C. Efficiency Evaluation

According to the VM types listed in Table 3, we set up two typical resource scenarios which are described in Table onsiders the community to be a trusted resource scenario with 90 percent trusted VMs the community to be a malicious resource scenario with 20 percent malicious nodes and 20 percent low trusted VMs. Based on AJFR, we evaluate the efficiency of SOTS with respect to the resource matchmaking problem. In these experiments, once the job is recorded as a failure, it is resubmitted until all the jobs are successfully executed.

VIII. CONCLUSION AND FUTURE WORK

In this SOTS for trustworthy resource match making across multiple clouds. We have shown that SOTS yields very good results in many typical cases. However, there are still some open issues we can apply to the current scheme. First, we are interested in combining our trust scheme with reputation management to address concerns in users' feedback. A universal measurement and quantitative method to assess the security levels of a resource is another interesting direction. Evaluation of the proposed scheme in a larger-scale multiple cloud environment is also an important task to be addressed in future research.

REFERENCES

[1] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing," IT Prof., vol. 12, no. 5, pp. 20–27, Sep./Oct. 2010.
[2] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5,pp. 14–22, Sep./Oct. 2010.
[3] H. Kim, H. Lee, W. Kim, and Y. Kim, "A trust evaluation model for QoS guarantee in cloud systems," Int. J. Grid Distrib. Comput.,vol. 3, no. 1, pp. 1–10, 2010.
[4] P. D. Manuel, S. ThamaraiSelvi, and M. I. A. E. Barr, "Trust management system for grid and cloud resources," in Proc. 1st Int. Conf. Adv. Comput., Dec. 2009, pp.176–181.
[5] S. M. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in Proc. IEEE 10th Int. Conf. Trust, Security Privacy Comput. Commu., 2011, pp. 933–939.
[6] N. Dragoni, "A survey on trust-based web service provision approaches," in Proc. 3rd Int. Conf. Dependability, 2010, pp. 83–99.

©IJRASET 2013: All Rights are Reserved