Volume 3, Issue 6, June-2016, pp. 295-302 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Secure Grid System for T-Broker: A Trust-Aware Service Brokering Scheme Multiple Cloud Collaborative Services

[1]Mr. C.CHAITANYA, [2] Mr. V.N.VENU GOPAL

[1] Pursuing M.Tech(CSE) from Jagruti Institute of Engineering and Technology
[2] Associate Professor, Department of Computer Science and Engineering,
Jagruti Institute of Engineering and Technology, Telangana State, India.

Abstract:

To facilitate extensive collaborations, today's organizations raise increasing needs for information sharing via on-demand information access. Information Brokering System (IBS) a top a peer-topeer overlay has been proposed to support information sharing among loosely federated data sources. It consists of diverse data servers and brokering components, which help client queries to locate the data servers. However, many existing IBSs adopt server side access control deployment and honest assumptions on brokers, and shed little attention on privacy of data and metadata stored and exchanged within the IBS. More importantly, T-broker uses the maximizing deviation method to compute the direct experience based on multiple key trusted attributes of service resources, which can overcome the limitations of traditional trust schemes, in which the trusted attributes are weighted manually or subjectively. Finally, 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 sites.

Key Words: Information Broking System, Automation segmentation, coordinates broker, privacy preserving, and Attribute-correlation attack.

I. INTRODUCTION

Most of the existing systems work on two extremes of the spectrum: (1) in the query answering model for on-demand information access, peers are fully autonomous but there is no system-wide coordination; so that participants create pair wise client-server connections for information sharing; (2) in the traditional distributed database systems, all the participates lost autonomy and are managed by a unified DBMS. Unfortunately, neither of them is suitable for many newly emerged applications, such as information sharing for healthcare or law enforcement, in which organizations share information in a conservative and controlled manner, not only from business considerations but also due to legal reasons. In such scenarios, sharing a complete copy of the data with others or "pouring" data into a centralized repository becomes impractical. To address the need for autonomy, federated database technology has

been proposed to manage locally stored data with a federated DBMS and provide unified data access. However, the centralized DBMS still introduces data heterogeneity, privacy, and trust issues. Meanwhile, the peer-to-peer information sharing framework is often considered a solution between "sharing nothing" and "sharing everything". In its basic form, every pair of peers establishes two symmetric client-server relationships, and requestors send queries to multiple databases. This approach assumes 2n relationships for n peers, and is not scalable. In the context of sensitive data and autonomous data owners, a more practical and adaptable solution is to construct a data centric overlay including the data sources and a set of brokers helping to locate data sources for queries Such infrastructure builds up semantic-aware index mechanisms to route the queries based on their content, which allows users to submit queries without knowing data or server location. In our previous study, such a distributed system providing data access through a set of brokers is referred to as Information Brokering System (IBS).

While the IBS approach provides scalability and server autonomy, privacy concerns arise, as brokers are no longer assumed fully trustable – they may be abused by insiders or compromised by outsiders. In this article, we present a general solution to the privacy-preserving information sharing problem. First, to address the need for privacy protection, we propose a novel IBS, named Privacy Preserving Information Brokering (PPIB). It is an overlay infrastructure consisting of two types of brokering components: brokers and coordinators. The brokers, acting as mix anonymizers, are mainly responsible for user authentication and query forwarding. The coordinators, concatenated in a tree structure, enforce access control and query routing based on the embedded nondeterministic finite automata – the query brokering automata. To prevent curious or corrupted coordinators from inferring private information, we design two novel schemes: (a) to segment the query brokering automata, and (b) to encrypt corresponding query segments. While providing full capability to enforce in-network access control and to route queries to the right data sources, these two schemes ensure that a curious or corrupted coordinator is not capable to collect enough information to infer privacy, such as "which data is being queried", "where certain data is located", or "what are the access control policies", etc. We show that PPIB provides comprehensive privacy protection for on-demand information brokering, with insignificant overhead and very good scalability.

2. RELATED WORK

Research areas such as information integration, peer-to-peer file sharing systems and publish-subscribe systems provide partial solutions to the problem of large scale data sharing. Information integration approaches focus on providing an integrated view over large numbers of heterogeneous data sources by exploiting the semantic relationship between schemas of different sources. The PPIB study assumes that a global schema exists within the consortium, therefore, information integration is out of our scope. Peer-to-peer systems are designed to share files and data sets (e.g. in collaborative science applications). Distributed hash table technology is adopted to locate replicas based on keyword queries. the coarse granularity (e.g. files and documents) still makes them short of our expressiveness needs. Further, P2P systems may not provide complete set of answers to a request while we need to locate all relevant data.

2.1. Vulnerabilities and the Threat model

We adopt the semi-honest assumption for the brokers, and assume two types of adversaries, outside attackers and curious or corrupted brokering components. Outside attackers passively eaves drop communication channels. Curious or corrupted brokering components follow the protocols properly to fulfill their functions, while trying their best to infer others' private information from the information disclosed in the querying process

2.2. Attribute-correlation attack.

An attacker intercepts a query (in plaintext), which typically contains several predicates. Each predicate describes a condition, which sometimes involves sensitive and private data (e.g. name, SSN or credit card number, etc.). If a query has multiple predicates or composite predicate expressions, the attacker can "correlate" the corresponding attributes to infer sensitive information about the data owner. This attack is known as the attribute correlation attack:

3. SYSTEM STUDY

3.1. Presented System:

- The existing brokering architecture for cloud computing do not consider user feedback only relying on some direct monitoring information.
- There is no doubt that the efficiency of a trust system is an important requirement for multiple cloud environments. That is, the trust brokering system should be fast convergence and light-weight to serve for a large number of users and providers. However, existing studies paid little attention to this question, which greatly affects scalability and availability of the trust system

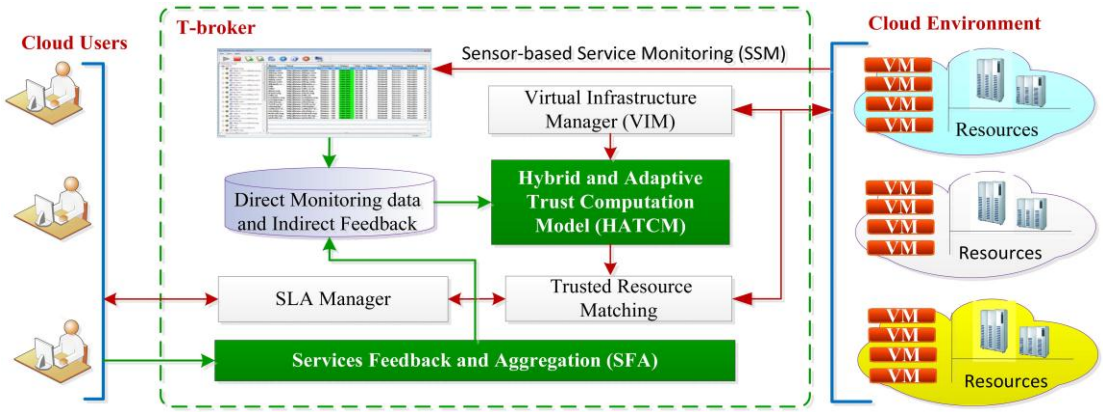
3.2. Proposed System:

- The proposed system is robust to deal with various numbers of dynamic service behavior from multiple cloud sites.
- Some hybrid trust models are proposed for cloud computing environment It is no doubt that how to adaptively fuse direct trust (first-hand trust) and indirect trust (users' feedback) should be an important problem, however, most current studies in hybrid trust models either ignore the problem or using subjective or manual methods to assign weight to this two trust factors (first-hand trust and users' feedback).
- The proposed trust management framework for a multi-cloud environment is based on the proposed trust evaluation model and the trust propagation network.
- First, a trusted third party-based service brokering architecture is proposed for multiple cloud environment, in which the T-broker acts as a middleware for cloud trust management and service matching.
- 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.

Problem Statement:

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

4. SYSTEM ARCHITECTURE



4.1System Implementation

Cloud User Module

Cloud users can send request to the T-broker for accessing the cloud resources, 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.

Cloud Resources Module(Admin)

Cloud resource module will provide the cloud resources. web based cloud computing managing tool for managing cloud infrastructure from multiple providers. RightScale enables organizations to easily deploy and manage business-critical applications across public, private, and hybrid clouds. SpotCloud provides a structured cloud capacity marketplace where service providers sell the extra capacity they have and the buyers can take advantage of cheap rates selecting the best service provider at each moment. a cloud is modeled in seven layers: Facility, network, hardware, OS, middle ware, application, and the user. These layers can be controlled by either the cloud provider or the cloud customer. In , the author presents a set of recommended restrictions and audits to facilitate cloud security. The recommendations might be overkill for deployments involving no sensitive data, they might be insufficient to allow certain information to be hosted in any public or community cloud.

T-Broker Module:

In this module T-broker uses some sub modules ,

(i)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.

(ii)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

(iii)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.

(iv)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 consists 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.

(v)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.

(vi)Service level agreement Manager(SLA)

In the multiple cloud computing environment, 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 register 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.

Multiple cloud 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 manyunique 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 .

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 to assess 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 socialevaluation- based trust relationship among network entities. By the same token, feedback 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 request 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. 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] M. Singhal et al., "Collaboration in multicloud computing environments: Framework and security issues," Computer, vol. 46, no. 2, pp. 76–84, Feb. 2013.

[2] H. M. Fard, R. Prodan, and T. Fahringer, "A truthful dynamic workflow scheduling mechanism for commercial multicloud environments," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1203–1212, Jun. 2013.

[3] F. Paraiso, N. Haderer, P. Merle, R. Rouvoy, and L. Seinturier, "A federated multi-cloud PaaS infrastructure," in Proc. 5th IEEE Int. Conf. Cloud Comput. (CLOUD), Jun. 2012, pp. 392–399.

[4] P. Jain, D. Rane, and S. Patidar, "A novel cloud bursting brokerage and aggregation (CBBA) algorithm for multi cloud environment," in Proc. 2nd Int. Conf. Adv. Comput. Commun. Technol. (ACCT), Jan. 2012, pp. 383–387.

[5] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing," IT Prof., vol. 12, no. 5, pp. 20–27, Sep./Oct. 2010. [6] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring,"

ABOUT THE AUTHORS

Mr. CHAITANYA is pursuing M.Tech degree in, Computer Science and Engineering from Jagruti Institute of Engineering and Technology, Telangana State, India.

Mr. V.N.VENU GOPAL, presently working as Associate Professor in, Department of computer science and engineering, Telangana State,India.