ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 4; Issue 2; March-April-2016; Page No. 10-16

Providing trusted services using cloud brokerage and aggregation approach in cloud environment

L.Pavithra[1], M.Azhagiri[2]

[1]PG Student, Computer Science and Engineering, Kingston Engineering College, Vellore, India

pavi26992@gmail.com

[2]Assistant Professor, Computer Science and Engineering, Kingston Engineering College, Vellore, India

azhagiri1687@gmail.com

Abstract

Cloud computing has become a recent surge in providing software ability without requiring huge or large expenses on operations. Clouds can dynamically provision virtual resources to applications hosted and clients who are using services to develop and store data and also access services remotely from anywhere. As multiple enterprises adopt for cloud computing service, cloud service providers are creating and enhancing technologies for cloud system capabilities. Since trust in resources has become a major concern in cloud computing industry, cloud brokerage and aggregation approach provides reliability by cumulatively aggregating and detecting the values of users of services. Also uses a hybrid adaptive trust computation for detecting the values of users of cloud. The cloud user utilizes the service resources of storage and retrieves files when needed. In order to get easy retrieval of files KNN based approach can be used to classify documents and place files appropriately and produces better result.

Key Words: Cloud brokerage, Aggregation, Feedback trust, Real time trust, Overall trust, KNN based approach.

Introduction

Clouds contain multiple network connected resource clusters such as data warehouses for geographically hosting distributed applications and components of storage for high reliability, high scalability, high availability, dependability. As in other IT systems, cloud security relies on establishing trust relationship among all other entities. The need for trust arises since a client has a direct control of its privacy and security of cloud service providers.

1. SERVICE MODELS

Infrastructure as a Service (IaaS): A type of service that is provided to the user for processing data, storage, networks, and other cloud computing resources in which the user can deploy and even run an arbitrary software, which includes operating systems and applications and other software.

Platform as a Service (PaaS): A type of service provided to the user for deploying onto the consumer-created cloud infrastructure or retrieved applications developed using programming languages, libraries, services, and tools supported by the cloud service provider.

Software as a Service (SaaS): A type of service provided to the user for utilizing the cloud infrastructure environment. The services offered over applications can be accessed through various devices such as interfaces or browsing applications such as internet technologies or any programming interfaces.

2. CLOUD BROKERS

Cloud brokers provide intermediation and aggregation capabilities between cloud users and cloud service providers. The future of cloud computing will be established only with the frequent emergence of many cloud brokers. Some of the cloud brokering systems which provide resources to users are Aeolus, Right scale, PCMONS, Spot cloud, Reservoir, Optimis.

Spot cloud is a secure central platform for buying or selling resources and computing capacity globally based on price, location and quality on a fast and secure platform and it also increases utilization and drives new revenue.

Corresponding author: L.Pavithra

Right scale is a web based cloud computing managing tool for managing cloud infrastructures from multiple cloud providers. This enables an organization to easily manage and deploy business applications across all types of cloud.

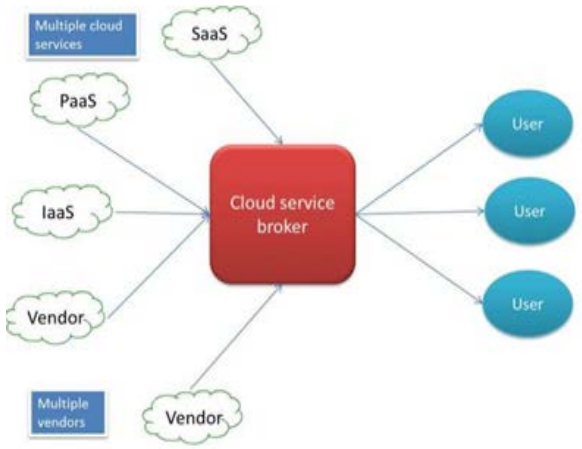

Figure 1: Service of broker

Aeolus is open source cloud management software which runs on Linux systems. It eases the burden of managing enormous number of clouds and also ensures cloud consumers can use large number of cloud. The components of Aeolus are Conductor-the application used for interacting by users and administrators, Orchestrator-where number of applications is considered as one machine, Composer-an application used for maintaining and building images.

Optimis can identify, capture and codify what an optimized cloud ecosystem driven by risk, trust and eco-efficiency.

3. RELATED WORK

Cloud brokers are responsible for optimally distributing different components to various users of clouds. Enormous researchers are focusing on trust management in cloud. Several issues have been identified by the researchers. In order to enhance trust among cloud users four key factors have been identified which is control, security, prevention, ownership. These key factors enhance trust among cloud users, cloud brokers, cloud providers.

Max Muhlhauser et al have proposed trustworthy selection of cloud services as an issue in emerging cloud marketplaces. Cloud Security Alliance (CSA) a self-assessment framework for cloud providers to publish their cloud platform security control capabilities. Cloud security alliance proposes a trust-aware framework to verify and evaluate these security controls considering consumers requirements. Hybrid trust model that combines hard and soft trust mechanisms for verifying the trust properties. Hard trust from measurements and properties and Soft trust from past experiences and recommendations

Nirnay ghosh et al has identified Service level agreements (SLAs), which document guaranteed quality of service levels, have not been found to be consistent among providers, even though they offer services with similar functionality. QOS levels are prime important to customers, as they use third-party cloud services to store and process their client's data. If loss of data occurs due to an outage, the customer's business gets affected. In identifying ideal service provider SelCSP framework uses trustworthiness and competence. Trustworthiness is computed from personal experiences gained through direct interactions or from feedbacks related to reputations of vendors. Competence is assessed based on transparency in provider's Service Level Agreement guarantees.

Feng Zhou et al have proposed Service operator-aware trust scheme (SOTS) is proposed for resource matchmaking across multiple clouds. Through analyzing the built-in relationship between the users, the broker and the service resources. Service operator-aware trust scheme proposes a middleware framework of trust management that can effectively reduces user burden and improve system dependability. These model the problem of trust evaluation as a process of multi-attribute decision-making and develop an adaptive trust evaluation. This adaptive approach can overcome the limitations of traditional trust schemes. Using SOTS, the broker can efficiently and accurately prepare the most trusted resources and thus provide more dependable resources to users. This can facilitate the effective utilization of SOTS in a large-scale multi-cloud environment.

Hamid Mohammadi Fard et al describe the ultimate goal of cloud providers is by providing resources and increasing their revenues. This goal negatively affects the users of a commercial multi cloud environment. A pricing model and a truthful mechanism are introduced for scheduling single tasks considering two objectives: monetary cost and completion time. Minimizing the completion time and monetary cost,

we extend the mechanism for dynamic scheduling of scientific workflows and theoretically analyze the truthfulness and the efficiency of the mechanism and present extensive experimental results showing significant impact of the selfish behaviour of the cloud providers on the efficiency of the whole system.

Dheeraj Rane et al has discussed cloud computing is a paradigm of computing that aims at providing dynamically scalable computing resources over the internet as a service. Users do not need to bother about the management of technology infrastructure. One of the major challenges that faces the cloud computing is how to secure and protect the data and processes the data of the user. In this theory a novel algorithm is proposed that is Cloud Bursting Brokerage and Aggregation (CBBA) consider three clouds for bursting and aggregation operation and also used secure sharing mechanism so that the cloud resources are shared among different cloud environment.

Anne H.H. Ngu et al has described about guaranteeing the availability of trust management is an issue in cloud computing. The trust management in cloud plays a vital role in cloud computing. It describes the design and implementation of CloudArmor, a reputation-based trust management framework that provides a set of functionalities to deliver Trust as a Service (TaaS) which includes a novel protocol to prove the credibility of trust feedbacks and preserve user's privacy. An adaptive and robust credibility model for measuring the credibility of trust feedbacks toprotect cloud services from malicious users and to compare the trustworthiness of cloud services. An availability model to manage the availability of trust management service.

Junping Du et al has investigated in dynamic nature of the cloud, continuous monitoring on trust attributes is necessary to enforce service level agreements. In order to enforce SLA with users Cloud-Trust, an adaptive trust management model for efficiently evaluating the competence of a cloud service based on its multiple trust attributes. In Cloud-Trust, two kinds of adaptive modelling tools are used. Rough set to discover knowledge from trust attributes in which weights are assigned subjectively. Induced ordered weighted averaging (IOWA) operator to aggregate the global trust degree based on time series, thereby enabling better real-time performance.

P.Jamuna et al has detected that cloud security hinges on how to establish trust between service providers and data owners in the virtual storage environment. Thus providing data colouring technique based on cloud watermarking can significantly result to make the system robust as well as secure user's data. Cloud watermarking proposes a method of providing security by using RSA algorithm to ensure the security of data for the periodic authentication and also to ensure whether the legitimate users are accessing the data.

Vandana Korde has surveyed different classification algorithms and proposed that most of the information is in text and text classification can classify documents and store in its predefined categories. This paper describes about the classification algorithms and stages that are followed for segregation. Naive bayes classifier, Decision tree, Decision rule, K-nearest neighbor (KNN), Support vector machine, Rocchio's algorithm are some techniques for classification.

Randeep kaur et al have analysed that security is an important criteria for cloud computing environment. Much number of users stores data and security is important for ensuring that client's data is placed in a secure mode. Authentication of data is important for securing data from the unauthorized third party. In order to guarantee independence between data isolation of different user's data guarantees security.

4. CLOUD TRUST COMPUTATION

This section contains some algorithms and equations for enhancing trust on cloud service resources utilization. Since cloud has a vast array of heterogeneous service resources which makes difficult task for cloud users to identify suitable cloud services. Classification of cloud services helps users find suitable service.

A. Hybrid Adaptive Trust Computation

Hybrid trust model based on subjective logic to combine 'hard' trust from measurements and properties and 'soft' trust from past experiences and recommendations to reduce such uncertainties. Adaptive credibility model that distinguishes between credible trust feedbacks and malicious feedbacks by considering cloud service consumers capability and majority consensus of their feedback.

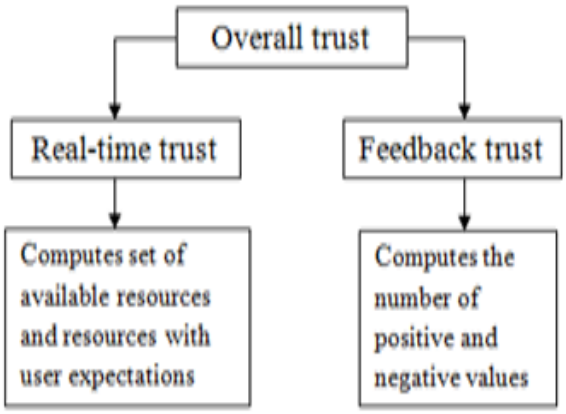

Figure 2: Trust calculation

Real-time trust is calculated by instant trust and weights assigned. Instant trust is R=SUO where S is the set of available resources and O is the set of resources with user expectations and R is trusted resource. Weights can be assigned by time based attenuation property. Two time stamps t_x and t_y are considered. Resource is distributed to different users and rating is determined based on completion. If the value is >0.5 then it is reliable. If the value is >0.5 it is unreliable. Time based attenuation property is always computed between two or more services and also it lies only between 0 and 1.

Feedback trust where the feedback system collects locally generated user ratings and aggregates these ratings. It is computed by

$$F_{\Delta\lambda}(r_i) = \frac{\zeta+1}{\zeta+\xi+2} \quad (1)$$

Table 1: Computing Feedback Values

Positive Feedback count	Negative Feedback count	Computed value	Results of Feedback categorization
70	30	0.69	Reliable
40	60	0.41	Unreliable
75	25	0.74	Reliable
15	85	0.11	Unreliable
90	10	0.89	Reliable
35	65	0.35	Unreliable
95	5	0.94	Reliable
28	72	0.21	Unreliable

Where ζ is the number of positive ratings (>0.5) towards service r_i and ξ is the number of negative ratings (<0.5) towards service r_i. If the rating exceeds the value then it may be a positive, if the rating does not exceed then it is a negative.

Usage of cloud services is becoming vast and a trend in IT industry for storing applications and data. There are enormous numbers of cloud service providers who are providing services with SLA guarantees to users, consumers. In order to increase the revenues many cloud providers do not bother about trust in services. To enhance trust the above hybrid and adaptive trust computation is described. Some of the cloud service providers are Google compute engine, Amazon web services, Cloud bees, Rack space, Cloud sigma, Sales force.com, Sun Microsystems, Joyent accelerators, Net suite and so on.

Table 1 illustrates the number of positive feedbacks and negative feedbacks for a cloud resource by several users of cloud environments.

The reviews of each user may vary based on their viewpoint. The table values are computed using Eq. 1. After computation the results are formalized and are categorized as reliable and non reliable services. Overall trust is computed by product of real-time trust and feedback trust of trusted resources.

$$\lambda = \frac{p(ri)+q(ri)}{2} \quad (2)$$

Determines number of positive and negative feedbacks and also the number of service undertaken by a resource r_i. Highly dynamic service behavior must have a high weight automatically. If the user rating is higher value is high .If the user rating is less value will get decreased.

Monitoring sensors are responsible for collecting the direct performance indicators of computing resources. Computing sensors are responsible for collecting and computing the indirect performance indicators of computing resources.

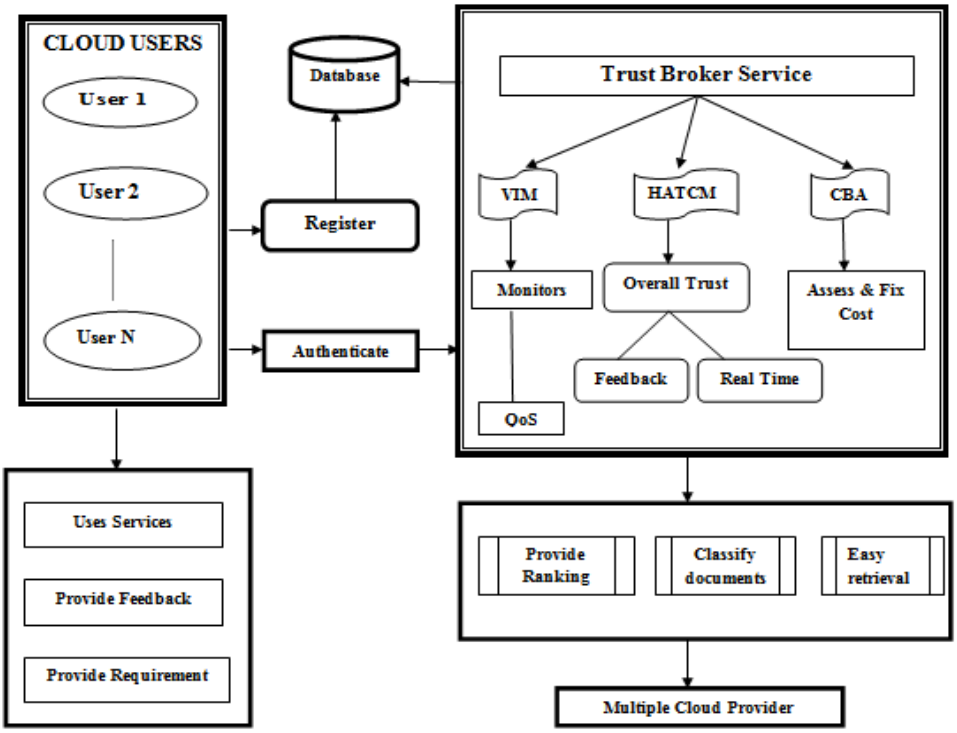

Figure 3: Architecture design

B. Cloud Brokerage and Aggregation Assumption

CBBA-Cloud Brokerage and Aggregation
CE –Cloud Environment
FPositive (FP) - Count the no of feedbacks [Initialize to 0]
FNegative(FN) - Count the no of feedbacks [Initialize to 0]

Algorithm CBBA (CE)

If (Cloud1)
{
[Select the Cloud provider data for aggregation]
If (Positive)
FP++;
If (Negative)
FN++;
[Print the value according to the count of positive and negative]
}
Else If (Cloud2)
{
[Select the Cloud provider data for aggregation]
If (Positive)
FP++;
If (Negative)
FN++;
[Print the value according to the count of positive and negative]
}
Else If (Cloud3)
{
[Select the Cloud provider data for aggregation]
If (Positive)
FP++;
If (Negative)
FN++;
[Print the value according to the count of positive and negative]
}
[Assign rank for each cloud provider for selecting]
Else if (Ranking)
{
If (Cloud n)
{
[Enter the Rank number]
If (Rank 1)

{
Select the cloud provider
}
Else {Check for ranking list}
} }
Else
{
Exit (0)
}

The above algorithm describes about various different clouds provided by cloud environment. Based on the cloud service provider's user feedbacks are collected. Not all users who are using services provide feedbacks but it is forced to give proper feedbacks for each cloud services. Every time the resources are analyzed the values are counted and initially it is set to count 0. Then after all count it is computed for positive and negative values. All computed values are aggregated and all cloud providers are given ranking based on which the new users of cloud may choose an optimal cloud services.

C. K-Nearest Neighbor (KNN)

Text categorization is also known as text classification, is a process of classifying a set of documents into a predefined set. If a document belongs to one category it is a single label otherwise multi label. Indexing a document makes accessing and reduces complexity easier.

This approach mainly works on major scenarios. Firstly classifying a documents into various categories and secondly user enters keywords which shows relevant document to users.

Classification deals with different stages which includes document collection where the different formats of document are collected, pre-processing stage which works on tokenization where each document is treated as string and partitioned into a list of tokens and removing stop words and stemming word which converts different word form into a canonical form, indexing reduces complexity and easier access, feature selection is selecting subset of features base on similarity, classification is a process of classifying and performance are evaluated.

KNN is based on distance and similarity and it is widely used in many applications for its effectiveness and accurate results and implementing a K- nearest neighbor approach is easier. This finds it difficult to find an optimal value of k and the value must reduce noise on classification. This approach must first learn the total weights of all the documents that are stored.

Algorithm

1. Assign values for every document in the training set and to appropriate class
2. Find a optimal or central value for training set
3. Calculate similarity between each document
4. Document belong to class which finds maximum similarity

For example, automatically label each incoming document type like pdf, word, image, video, etc., A training set contains n number of documents type and labeling each document must be labeled with a appropriate category. After classifying implementing it is performed by using various techniques.

1. Bag of words – Collect or extracts a keywords from a list of documents
2. Stop words removal – Insignificant words must be stopped and removed
3. TF-IDF – Term frequency Inverse document frequency is used to select candidate word
4. Case folding – Collected words are documented
5. Normalization – Is a process of eliminating redundancy

Accuracy is defined as the percentage of correctly classified documents to the total number of documents. So compared with other classification algorithm this KNN based approach provides best and accurate results.

5. CONCLUSION

It is concluded that the trust computation mechanism provides reliable and trusted services to cloud users and offers only reliable resource. CBA algorithm is used for finding best cloud provider and provides ranking. KNN based approach produces better results for its effectiveness.

6. REFERENCES

1. Anne H.H. Ngu, Quan Z. Sheng, Schahram Dustdar, Talal H. Noor "CloudArmor: Supporting Reputation-based Trust Management for Cloud Services", IEEE transactions on parallel and distributed systems, 1-14, Vol. 0, No. 0, 1045-9219,2014.
2. Dheeraj Rane, Pritesh Jain, Shyam Patidar,"A Novel Cloud Bursting Brokerage and Aggregation (CBBA) Algorithm for Multi Cloud Environment", Second International Conference on Advanced Computing & Communication Technologies, 978-0-7695-4640-7, 383- 387, 2012

3. Feng Zhou, HuaDong Ma, Xiaolin Gui, Xiaoyong Li,"Service Operator-Aware Trust Scheme for Resource Matchmaking across Multiple Clouds", IEEE transactions on parallel and distributed systems, 1045-9219, Vol.26, No.5,2015.
4. Junping Du, Xiaoyong Li "Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing", IET Information Security, ISSN 1751-8709, Vol.7, Issue.1, pp: 39-50, 2011.
5. Max Muhlhauser, Sheikh Mahbub Habib, Vijay Varadharajan, "A Trust-aware Framework for Evaluating Security Controls of Service Providers in Cloud Marketplaces, 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 978-0-7695-5022-0, 460-468, 2013.
6. H.F.Mohammadi, Radu Prodan, Thomas Fahringer "A Truthful Dynamic Workflow Scheduling Mechanism for Commercial Multi cloud Environment", IEEE transactions on parallel and distributed systems, 1045-9219, Vol.24, No.6, 1203-1213, 2012.
7. Randeep kaur, Supriya kinger "Analysis of security algorithms in cloud computing", International journal of application or innovation in engineering & management, Volume 3, Issue 3, March 2014.
8. Nirnay ghosh, Sajal K. Das, Soumya K. Ghosh "SelCSP: A Framework to Facilitate Selection of Cloud Service Providers", IEEE transactions on cloud computing, 2168-7161, Vol. 3, No. 1, 66-80, 2015.
9. A. Ranabahu, A. Sheth, P. Patel "Service Level Agreement in Cloud Computing", IEEE Green Technologies Conference, 978-0-7695-4966-8,167-175, 2012.
10. Vandana korde, "Text classification and classifiers: A survey", International journal of artificial intelligence & applications, Vol.3, No. 2, March 2012.