EAI Endorsed Transactions
on Cloud Systems

Research Article EAI.EU

# TOWARDS A CLOUD CONSUMERS CREDIBILITY ASSESSMENT AND TRUST MANAGEMENT OF CLOUD SERVICES

E.Priyadharshini[1],V.Vijayakumar[1] and M.D.Abdul Quadir[1]

[1]VIT University, Chennai

## Abstract

In Cloud computing, several issues arises due to malicious users. The cloud service provider does not know whether the cloud consumer is authorized user or an unauthorized user when they access the data from cloud. Cloud service consumer can interact with the cloud providers. The malicious users can easily hack the user's private information. The cloud provider cannot able to find this problem. In this Paper we proposed the method is a Trust Management Service (TMS). The advantage of using this methodology is to secure our privacy information and also check whether it is a valid users or not. Protecting the cloud services against the malicious user is not an easy task. Our proposed method show that the capability of finding the malicious users and also misleading feedback.

**Keywords:** Trust Management Service, Credibility, Feedback.

Received on 06 April 2018, accepted on 14 May 2018, published on 16 May 2018



doi: 10.4108/eai.16-5-2018.154775

## 1. Introduction

Cloud computing can provide the unlimited computation, scalable and durable resources. It also provide the customer to access the large amount of data. It can be access at any time at anywhere. Trust management is one of the challenging problem for the development of cloud computing. Cloud services has become a very popular in recent years. It provide the flexibility of computing resources at very low cost. It can provide the unlimited computation, scalable and durable resources. Cloud computing having four deployment model. They are private cloud, public cloud, hybrid cloud and community cloud. It also having three types of services. They are Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS)

It can also provide the customer to access the large amount of data. It is one of the delivery model and it can provide the users with scalable services and successfully uses information technology as a service over the network and provides end-users with extremely strong computational capability. It can be access at any time at anywhere. It is currently used for web mail, web-hosting services and blogs. But security play vital role in cloud computing.

## 2. Related Works

Zhiguo Wan et al.published the paper on cloud computing is one of the most dominant paradigm in industry field. The existing method is the attribute based encryption (ASBE).This method cannot access the control of outsourced data from the cloud computing. This method acquire the expansible due to its hierarchical structure. It having the flexibility and fine grained access control. This method is well organized than existing methodology. It supports compound attributes due to adaptable attribute set of combination.

Jingwei Li et al. published the paper that cloud has been developed recently. To get the outsourced data, it facing so many issues and also privacy protection problem. The proposed method is to preserve a privacy storage and retrieval. This method not only ensures the privacy and security but also provides trustworthy for outsourced data. The storage and retrieval mechanism permits the cloud users to issue and searching the data across the multiple clouds. It can be managed by the different cloud service provider. The merits of using this methodology is to increasing the number

of cloud service provider and also reduce the data redundancy. It minimize the bandwidth for file retrieval.

LIN Guoyuan et al.presented the paper on new computing model can provide a scalable and virtualized web services. This computing model faced with many security challenges. To secure the cloud computing, one important measures is the access control. Cloud cannot directly solve the unpredictability and it can be caused by the open condition of cloud computing. To implement the new kind of access control method in cloud computing environment, we need to build a mutual trust relation between users and cloud platform. In this paper, we proposed the Mutual Based Trust Based Access control. The merits of using this methodology is to take both service node credibility and user behaviour. To implementing the MTBAC model, it can be easily solved by security control of access control. This method can make sure the interaction between users and cloud service nodes.

Xiao Chen et al. published the paper on how to manage the trust on Vehicular Social Network based on cloud. Traditional public key infrastructure cannot identify the malicious users so we introduced a trust management system to secure a vehicular social data.

In Feng et al.proposed to verify the honesty of the data in the cloud, we need to introduce the security facing problems and it require the independent services. The existing methods for verifying the honesty of data cannot handle problem very effectively. They cannot handle with the error condition. To secure and well organized dynamic auditing protocol should avoid the requests that are made with irregular validation. At last we provide an error response message and methods show that our solution has able to handle the error and the lower expenditure cost for communication and computation.

Nir Drucker et al.proposed the paper that if the user that run a trustworthy application on the hosting infrastructure would act as a trusted proxy. Networking overheads would decrease but new overheads for making an application trusted and make it visible. The efficiency of trusted proxy solution depends on the balance between these performance costs. They proposed local computation model that it does not bother about transformation of data over the network .This application that could serve the trusted proxy and also it having great potential.

Mazhar Ali et al.proposed security concerns outsourced data to the third party administrative control play a serious role. In this situation many data leaks are occur due to the attacks. These attack may be occurred due to the users and also machine in the cloud. Data can be provided by the cloud service is another problem faced in the environment. They proposed the data security for cloud environment with trusted parties. The DaSCE utilizes the threshold DaSCE and also evaluating its performance based on time consuming and also formal model to analyse the working of DaCSE using high level petrinets. The merits of this methodology does not need any protocol and implementation level changes at the cloud.

Xiaoyong et al.suggested that the cloud computing, trust management is a very important in the field of communication and technologies. But the patterns are changing dynamically over the time. There are many aspects in the existing approaches like an attribute based trust management scheme for Service Level Agreement (SLA), an adaptive model for measuring multi-dimensional trust attributes. There are many trusted cloud service module. Each module consists of several sub modules. There are dynamic trust evaluation module (DTEM), SLA Manager, service monitoring module, normalization module of evidences and log information module. We proposed the cloud trust, which is used to analyse the history service information of the cloud provider.

Juan M et al. published the organization perimeter. Advanced cryptography technique are used because it avoid the cloud service provider being able to reveal the data without the acceptance of data owner. It cannot able to access the data, but also unable to release to its unauthorized parties.

Qi Xia et al.discussed the paper that spreading of medical records result in different risks to patient's privacy as unauthorized activities on these records. The parties are directed or indirectly to the data. Recent methods are effectively damage the medical records have been proved to be inadequate. The system is a block chain based and it provides data auditing, provenance and control for sharing the medical data in the cloud storage among the big data entities. It also monitors the access data for the malicious users from a data conservator system. The data can be shared and transmitted from one entity to another entity. It performs all the action on the medical share system. They are recorded in the tamper proof manner. The performance of medical share is compare to the recent cutting edge solution to the data sharing among the cloud service providers. The advantage of using this method will be able to achieve the data provenance and also auditing. It also minimize the risk of data privacy.

Uthpala Subodhani Premarathne et al. discussed that trust negotiation using associated identity management are playing a significant role for preserving a privacy in open system. The trust negotiation are needed to control the user access to the information resources in open system. Two parties are involved in these which are unknown to each other. It is used in collaborative application. We have demonstrated how these trust metrics can be computed by using the real life attack history data, mitigation and detection technique, recently discovered vulnerabilities using fuzzy arithmetic and fuzzy rule based inference models. The merits of this methodology is to support the cloud base utility services to ensure trust negotiation using federated identity management

## 3. Architecture Diagram

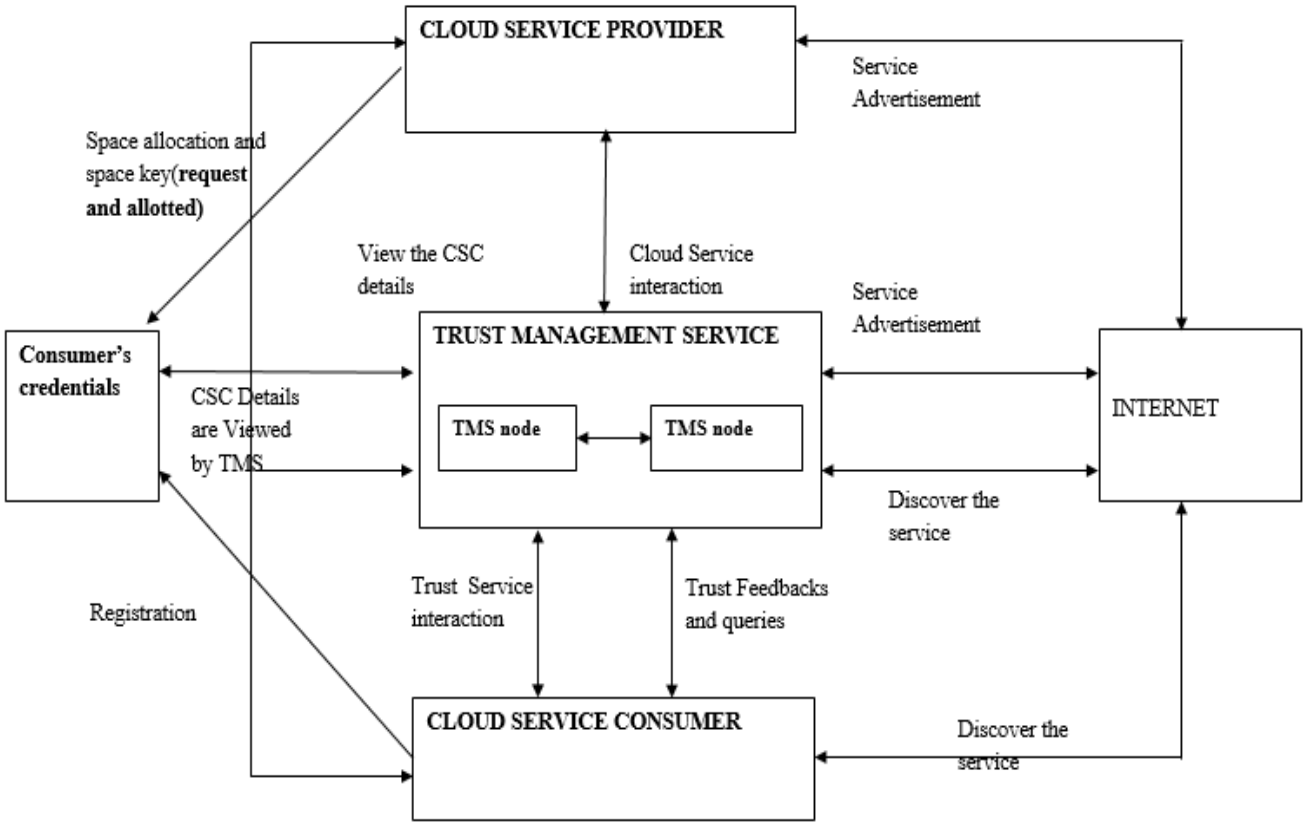



**Figure 2.Trust Management Service**

Architecture consists of Cloud service Provider, Trust management Service, Cloud service consumer. The CSP offers one or several cloud services publicly on the web. These cloud services accessible through on web search engine such as google. It having several nodes .They interact with both CSP and CSP. So TMS can be view the CSP's advertisement then, it advertise the trust as a service to users through the Internet and the CSC discover the cloud services through the Internet at the time TMS allows the users to assess the trust of new cloud services. The CSC register their credentials and login then view available CSP and its corresponding feedbacks can be viewed by CSC. Then, CSP Views request from CSC and allocate space for storage and send space key. The CSC gets space key through mail then, it can be upload the file into the cloud. Finally, put the feedback for CSP. These feedbacks are verified by trust management service.

## 4. Methodology

In proposed method we have to use trust management services.

There are 3 methods

i) Cloud services provider

ii) Trust management service

iii) Cloud consumer service

### i) The Cloud Service Provider:

Cloud Service Provider can be register our details and login. The following process are done by CSP, it can be view all of the Cloud Service Consumer details. CSC can request the space to the cloud, then the cloud service provider accept the request and allocate the space to the consumer. Cloud service provider send space key to CSC through the mail.

### ii) The Trust Management Service:

It can be manage all of the process. It is the intermediate of CSP and CSC. It can viewed the feedback of CSP from CSC, if it is trusted and then the information will stored in feedback database and evaluate the feedback. It can be view details of CSP, CSC and Storage request details.

### iii) The Cloud Service Consumer:

Consumers registered the personal details and login. Then, send the request for storage space to CSP and get space key via the mail. The space will be allocated for particular consumer. Finally, it will upload the file into the cloud and submit the feedback about CSP.

## 5. Algorithm

Trust Management Sequential Algorithm

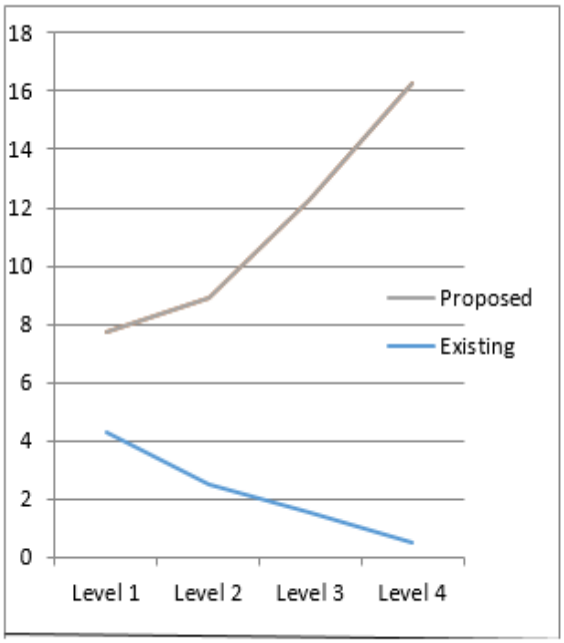
1. CONSUMER AND PROVIDER -space allocation (sA) and space Key (sK)
2. Trust - evaluation of sA sK; Feedback evaluation fE (sA, sK),
3. Consumer - CSP, CsA, CsK
4. Caching: T (CSC) starts caching trust results (CSC) and T (CSP) start caching trust results (CSP)
5. Input: S, Output: TR(S)

Count |C1 (f, s) |Cache
if |C1 (f, s) |Cache ≥ cccache (f) then
Compute Cid(c), Compute CR (f, s)
end if
Count |C1 (f) |Cache
if |C1 (f) |Cache ≥ cpCache (f) then
Compute D(s), Compute CR (f, s)
Compute TR(S)
end if

EXPLANATION

STEP 1: Feedback given by the particular consumer
Count |C1 (f, s)|Cache
if |C1 (f, s) |Cache ≥CCcache (f) then
STEP 2: Calculation is required
Compute Cid(c), Compute CR (f, s)
end if
STEP 3: Trust result
Count |C1 (f) |Cache
if |C1 (f) |Cache ≥ cpCache (f) then
STEP 4: Recalculate the feedback
Compute D(s), Compute CR (f, s)
Compute TR(S)
End if

## 6. Analysis




In this paper we proposed Trust Management System. This method should evaluate the feedbacks from the cloud service consumers. If it is trusted, it is to be stored in feedback database. Hence we find out the misleading feedback. It also find out when malicious behaviour occur. But in the existing system could not find out the misleading feedback .It cannot find out the unauthorized user. The user information was not secured in the existing methodology. So we proposed the TMS.

## 7. Conclusion

Trust management service allow the trust feedback and the storage is to be maintained in a distributed environment. It provides the more security and reliability. It also check the feedback whether it is comes from authorized user are or not. It facing more challenging problem such as whitewashing attack and syllabi attack.

## 8. Future Work

In future work, we introduce a dynamic trust computation model. Normally it is assumed that the good agent always provide the true feedback and malicious users sends the false feedback. However, this is not always real scenario as

good users might provide false feedback and malicious agents sometimes provide false feedback to hide their real nature. So credibility feedback is needed to determine the trustworthiness of feedback. During the evaluation of the trust, feedback given by the agent with higher credibility are trust worthier and therefore weighted more than those agents with lower credibility.

## References


[1] Ali, Mazhar, Saif Malik, and Samee Khan. "DaSCE: Data security for cloud environment with semi-trusted third party." IEEE Transactions on Cloud Computing (2015).

[2] Bacon, Jean, et al. "Information flow control for secure cloud computing." IEEE Transactions on network and Service Management 11.1 (2014): 76-89.

[3] Chen, Xiao, and Liangmin Wang. "A cloud-based trust management framework for vehicular social networks." IEEE Access 5 (2017): 2967-2980

[4] Drucker, Nir, Shay Gueron, and Benny Pinkas. "Faster Secure Cloud Computations with a Trusted Proxy." IEEE Security & Privacy 15.6 (2017): 61-67.

[5] Feng, Bin, et al. "An efficient protocol with bidirectional verification for storage security in cloud computing." IEEE Access 4 (2016): 7899-7911.

[6] Jin, Xin, et al. "Trusted attestation architecture on an infrastructure-as-a-service." Tsinghua Science and Technology22.5 (2017): 469-477.

[7] Ko, Ryan KL, et al. "TrustCloud: A framework for accountability and trust in cloud computing." Services (SERVICES), 2011 IEEE World Congress on. IEEE, 2011.

[8] Li, Xiaoyong, and Junping Du. "Adaptive and attribute-based trust model for service-level agreement guarantee in cloud computing." IET Information Security 7.1 (2013): 39-50.

[9] Lin, Guoyuan, et al. "MTBAC: A mutual trust based access control model in cloud computing." China Communications11.4 (2014): 154-162.

[10] Martucci, Leonardo A., et al. "Privacy, security and trust in cloud computing: The perspective of the telecommunication industry." Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on. IEEE, 2012.

[11] Noor, Talal H., Quan Z. Sheng, and Abdullah Alfazi. "Reputation attacks detection for effective trust assessment among cloud services." Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on. IEEE, 2013.

[12] Patel, Subhash Chandra, Ravi Shankar Singh, and Sumit Jaiswal. "Secure and privacy enhanced authentication framework for cloud computing." Electronics and Communication Systems (ICECS), 2015 2nd International Conference on. IEEE, 2015.

[13] Perez, Juan M. Marin, Gregorio Martinez Perez, and Antonio F. Skarmeta Gomez. "SecRBAC: Secure data in the Clouds." IEEE Transactions on Services Computing 10.5 (2017): 726-740.

[14] Premarathne, Uthpala Subodhani, et al. "Cloud-based utility service framework for trust negotiations using federated identity management." IEEE Transactions on Cloud Computing 5.2 (2017): 290-302.

[15] Wan, Zhiguo, Jun'E. Liu, and Robert H. Deng. "HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing." IEEE transactions on information forensics and security 7.2 (2012): 743-754.

[16] Xia, Qi, et al. "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain." IEEE Access5 (2017): 14757-14767...