ISSN:2249-5789
R N Mrudula et al, International Journal of Computer Science & Communication Networks,Vol 7(5),147-151

# An Efficient Feedback Based Trust Management Framework for Cloud Computing

**R. N. Mrudula**
M. Tech,
Department of CSE,
Shri Vishnu Engineering College for Women (A),
Vishnupur, Bhimavaram,
West Godavari District, Andhra Pradesh.

**Prof. V. Purushothama Raju**
Professor & HOD,
Department of CSE,
Shri Vishnu Engineering College for Women (A),
Vishnupur, Bhimavaram,
West Godavari District, Andhra Pradesh.

***ABSTRACT***

*Trust management is one of the big challenging problems for the growth and expansion of cloud computing in different areas. Other challenging issues are security, privacy, and availability of cloud service. A cloud service can be trusted if it handle these privacy, security and availability issues. In this paper, we implemented a secure feedback based trust framework that provides Trust as a Service (TAAS).*

*Cloud user feedbacks are the important source for assessing the reputation of the cloud service. But unknown attacks by malicious users may bring down the reputation of the service. This may be done by giving false feedbacks (i.e., Sybil attack). We identify the Sybil attack using this system.*

*The feedback based trust management system provides Trust As A Service (TAAS) and identifies the malicious users. The system includes a protocol (Zero- Knowledge Credibility Proof Protocol) to prove the credibility of feedbacks and keep the users' privacy, a credibility model for estimating the credibility of trusted feedbacks that protect cloud services from malicious users, an availability model to manage the availability of the decentralized implementation of the trust management service, and a dynamic cost estimation model to estimate the amount of bandwidth that is utilized for user activities.*

## I. INTRODUCTION

In the cloud computing, providing trust is the most challenging problem because all the users' data is stored on virtual servers. The dynamic, distributed and non-transparent nature of cloud services introduces some challenging issues in cloud environment like

- Privacy,
- Security, and
- Trust management service availability.

These are the critical and important issues for the adoption of trust in any cloud service. Assuring the user that these three issues can adopted, we can say that trust is established for a cloud service.

Providing cloud users' data protection is not an easy way to handle because sensitive information may be involved in the interaction between user and the cloud service providers. Providing cloud services to unknown persons is a big problem. This involves providing security

and privacy to users' data. Providing availability of the trust management service is another bigger problem due to the nature of the cloud (dynamic).

It is a typical practice that cloud users share their opinions on the cloud service in the form of rating/reviews (feedbacks) for any other cloud user benefit. These feedbacks can influence the view of the cloud users on cloud service. If these feedbacks are true then these can help users to select proper cloud service satisfying his/her requirements. On the opposite side, if feedbacks are manipulated or not genuine then it can mislead cloud user. Therefore, the feedbacks are important for selecting a good cloud service. We can say that reputation of the cloud service is based on these feedbacks. Manipulated reviews can be harmful to the cloud service as well as to the cloud user.

The trustworthiness of cloud service can estimated based on cloud user feedbacks. But the problem arises when malicious users give false feedbacks. The reputation of cloud service can be influenced both positively and negatively by these controlled feedbacks. Identifying manipulated online feedbacks is tough.

Several competences have been proposed recently for handling trust feedbacks in cloud environments. But, how to determine the credibility of the secure trust feedbacks is mostly abandoned. In this paper, we propose a feedback based trust management model that uses an aggregated opinion of users to assess the trustworthiness of cloud service.

The feedback based trust management system can identify the credibility of the feedbacks, measure the overall trustworthiness of cloud service and guarantees the availability of Trust Management Service (TMS) at any instant of time. Also, a bandwidth cost estimation model is used to improve the trust. It estimates the amount of bandwidth utilized by the user and calculates the amount of cost for the bandwidth utilization. This feature of the system supports cloud's pay-for-use model.

## II. RELATED WORK

Trust can be established in many ways. In paper [1], policy-based approach is used to establish trust. This approach uses centralized architecture. Trust between cloud users and cloud providers are established by compliance management technique. The cloud providers are selected based on Compliance Level Agreements (CLAs) specified by the users.

In paper [2], trust is achieved by a multi-faceted trust management system. This aids the users to identify the trustworthy cloud service providers. This system collects trust information using a set of QoS attributes such as security, latency, availability, etc.

In contrast to these policy-based and multi-faceted approaches, we use feedback-based trust management system. The feedbacks given by the cloud users are used to assess the trustworthiness of cloud service. We also use bandwidth cost estimator to improve the trust of users on cloud service.

## III. PROPOSED METHOD

The recent attraction towards cloud computing is due to its distributed, flexible, pay per use, and on-demand nature. Distributed cloud computing offers a broad number of services like SAAS, PAAS, and IAAS.

In cloud environment the data is secured on various virtual servers that are handled by a third party. Consequently, the crucial issue to use the cloud service is privacy, security and availability. Through this paper we are providing Trust as a Service (TAAS). This ensures the customers' data is secure and protected. Also,

TAAS guarantees that the cloud service is available at any point of time.

Feedbacks given by the cloud users are nice source for estimating the trustworthiness of the cloud service. Opinions of the users on the cloud service can be influenced dramatically by these feedbacks. The problem arises when the malicious users attempt to give fake reviews to affect customer opinions on cloud service.

Manipulated reviews can be harmful to the cloud service as well as to the cloud consumer. The unusual attacks from the malicious user (for example, Sybil or collusion attack) can affect the reputation of the cloud service. Some users give false feedbacks to manipulate the reputation of the service. Therefore, there is a need for feedback-based framework in cloud environment for providing trust management. This framework provides Trust as a Service (TAAS). The feedback based trust management framework which validates the user feedbacks. As the user feedbacks on the cloud service are useful for assessing the quality of the cloud service, we use the user feedbacks as the basis for estimating the trustworthiness of cloud service. This framework is also useful for detecting Sybil attacks and make users aware of fake reviews.

Another feature that is included in this system is dynamic bandwidth cost estimation. It estimates the amount of bandwidth utilized by the user and calculates the cost for total bandwidth used. This information about the user bandwidth usage can improve the trust of the user on cloud service.

The architecture of this framework is shown below.

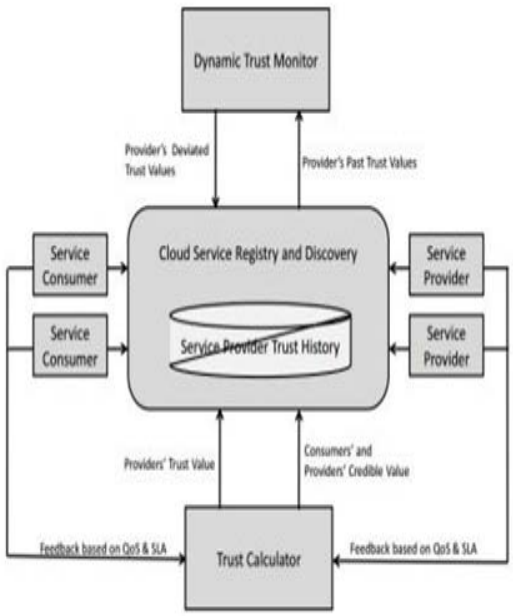


**Fig**:- Architecture of the trust management framework

The Trust Management Service (TMS) layer acts as a protection layer between cloud consumer and cloud service provider. It makes the communication between consumer and service provider secure and prevents the attacks on cloud service.

The key features of the system include

- Zero-Knowledge Credibility Proof Protocol (ZKC2P)
- Credibility Model
- Availability Model
- Dynamic Cost Estimation

***Zero – Knowledge Credibility Proof Protocol (ZKC2P):*** Providing client data privacy is critical due to the sensitive data (for example, address, phone number, email id, etc.) involved in the communication between client and the cloud service provider. Trust must be provided without breaching the users' privacy. ZKC2P is used to provide privacy and security in cloud. It also helps TMS (Trust Management Service) to

prove integrity of the user credentials. Anonymization technique is utilized to protect users from privacy breaches.

***Credibility Model:*** The credibility model is used to identify the misleading feedbacks. Cloud services are prone to numerous attacks. Securing Cloud services from their attacker users (ex: such users will give misleading feedbacks which may affect the trustworthiness of cloud service) is a huge issue. Authorized person can view the file details and provide feedback. TMS can view all the feedbacks given by clients and lists all positive and negative feedbacks. Secure feedback-based trust model can identify and view the intruders in cloud servers. The consumer credentials are checked to recognize Sybil attack. The IP addresses of the users who give feedbacks are checked to ensure credibility of the feedbacks. Same IP address for any two or more feedbacks is considered as Sybil attack.

***Availability Model:*** Availability is one important issue in cloud environment. High availability of TMS is desirable to make the cloud service transparent. The feedbacks at different nodes must be handled in a decentralized way. This is achieved by availability model which use load balancing technique to manage workload at different TMS nodes.

***Dynamic Cost Estimation Model:*** Another interesting feature in the feedback based trust management model is the implementation bandwidth estimator that can track user's usage utilities and can support a Cloud's pay per use models. So we propose to extend the prior system using a dynamic bandwidth cost estimation model which is both cloud and user friendly without involving any additional complexities. The bandwidth utilized for activities of the users (either data owner or data user) are estimated. The activities may be data uploading or data downloading. The cost charged for estimated bandwidth is displayed. We estimate the cost for the activities of the users in a dynamic cloud environment.

An algorithmic implementation for bandwidth estimation is as follows.

**Algorithm**

**Require:** Start state s*, threshold value c, type System T
**Ensure:** predicted optimal solution cost
1: d← h(s*)
2: initialize N(1,t) and p(1,t)
3: loop
4: for i=2 to d do
5: for all t ε T do
6: p(i, t)← compute-probability (i, t, d)
7: if t is a goal type AND p(i,t)>c then
8: return d
9: end if
10: end for
11: end for
12: d← d+1
13: end loop

## IV. CONCLUSION

The current framework provides Trust as a Service (TAAS) and ensures the users their data is private, secured and available at any time. A secure feedback based trust management model identifies the credibility of the trust feedbacks. An interesting augmentation to this work is the approximation of bandwidth transfer capacity that can track cloud users activities and their bandwidth utilities. So we propose a feedback based trust management framework with a dynamic transfer bandwidth/cost estimation which improves trust in cloud and is easy to understand without including any extra complexities.

## V. REFERENCES

[1] I. Brandi, S. Dustcart, T. Inset, D. Scum, F. Layman, and R. Kennard, “Compliance Cloud Computing (C3): Architecture and language support for user-driven compliance management in clouds,” in Proc. 3rd Int. Conf. Cloud Comput., 2010, pp. 244-251.

[2] S. Habit, S. Rise, and M. Muhlhauser, “Towards a trust management system for cloud computing,” in Proc. 10th Int. Conf. Trust, Security Privacy Comput. Common., 2011, pp. 933–939.

[3] S. M. Khan and K. W. Hameln, "Hatman: Intra-cloud trust in organization for Hadoop," in Proc. fifth Int. Conf. Cloud Comput., 2012, pp. 494– 501.

[4] S. Pearson, "Assurance, security and trust in circulated processing," in Privacy and Security for Cloud Computing, ser. PC Communications besides, Networks. New York, NY, USA: Springer, 2013, pp. 3– 42.

[5] J. Huang and D. M. Nichol, "Trust in segments for cloud handling," J. Cloud Comput., vol. 2, no. 1, pp. 1– 14, 2013.

[6] K. Hwang and D. Li, "Trusted disseminated processing with secure resources and data shading," IEEE Internet Comput., vol. 14, no. 5, pp. 14– 22, Sep./Oct. 2010.