International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

Trust Based Management with User Feedback Service in Cloud Environment

Ms Swaroopa Shastri[1], Ms Sebastina[2]

[1]*Assistant Professor, Department of Computer Application, VTU PG Centre Kalaburgi, Karnataka, India*
[2]*Department of Computer Application, VTU PG Centre Kalaburgi, Karnataka, India*

Abstract - *Trust management is a standout amongst the most difficult issue for the tackling and development of cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services leads to many challenging issues such as privacy, security, and availability. Protecting cloud services against their malicious clients (e.g., such clients may give misleading feedback to inconvenience a specific cloud service) is a complicated issue. The trust management in cloud environments a significant challenge . According to researchers at Berkeley, trust and security are ranked one of the top 10 obstacles for the adoption of cloud computing. We introduce Trust Based Management with User Feedback Service in Cloud Environment by using RSA Algorithm that not only identifies misleading trust feedbacks from collusion attacks but also detects Sybil attacks. A novel protocol to prove the credibility of trust feedbacks and preserve users' privacy. The conclusion of the paper we want to summarize the challenges we faced while storing the data in the cloud with the various nature in the cloud. It has become highly important for the cloud providers to improve the security of the system as the cloud is highly dynamic, distributed and non transparent along with providing the security for the users we have to build the trust between the cloud and the users. we assess how security, trust and privacy issues occur in the context of cloud computing.*

Key Words: **cloud computing, privacy, security, attacks, availability.**

1. INTRODUCTION

It has become highly important for the cloud providers to improve the security of the system as the cloud shows vastly vibrant features, distributive in nature and non translucent for the users .along with providing the security for the users we have to build the trust between the cloud and the users. According to the survey trust and security are listed on top of as the challenges in cloud. To provide this customer's feedback is the good platform to build a trust for the cloud. In proposed work we proposed a system to build the trust among the cloud and the users based on the feedback of the customers who are already using the services. It not unusual that the cloud service will face a malicious behavior in the cloud from its users so, here we give importance to build a trust based system which provides a credibility of the trust feedbacks. The most exigent issue in the cloud computing, these issues involve the privacy, security, and availability problem is to preserve the cloud services from their users, such users may provide the misleading feedback for the particular cloud service. Since very sensitive data is involved between the trust management service and the clients, maintaining consumer's privacy is a not an easy work. To demonstrate the dependability of trust feedbacks and maintains user confidentiality a novel protocol.

2. LITERATURE SURVEY

[1]Maintaining the trust between the users and the cloud is a very challenging and important fact in the cloud computing environment, [2]The proposed system will provide a way for the users to decide the cloud service provider who are trust worthy based on different features and services,[3] Focus on the providing the trust based management framework which are supported and analyzed the trust related feedback given from the user and from different entities,[4] This system not only provides detect the malicious behavior but also detect the misleading feedback from the users. This identification is done using the collision attack and also identifies the Sybil attack,[5]client's criticism is the most solid and a decent source to examine the reliability of the cloud. These feedbacks are collected from the users. However it common that the user show the malicious behavior by the users in the cloud.

3. PROPOSED APPROACH

Cloud benefit clients criticism is good remain to gather the general points of interest trust in cloud administration. To help in identifying status based attacks and allow clients to efficiently view trustworthy cloud providers here, we have presented brief technique. The model detects Sybil attacks and identifies incorrect trust feedbacks from collusion attacks; the trust based feedbacks is collected from the user. To protect the trust about the cloud at a highest level. We developed the trust model which does the data analysis on the feedback.

3.1 Module Description

Identity Management Service (IMS) :

IMS can facilitate TMS in the detection of Sybil attacks against cloud services without breaching the privacy of users. When users attempt to use TMS for the first time, TMS requires them to register their credentials at the trust identity registry in IMS to establish their identities.

Trust Management Service (TMS):

In a typical interaction of the reputation-based TMS, a user either gives feedback regarding the trustworthiness of a particular cloud service or requests the trust assessment of the service.

Feedback Collusion Detection :

Malicious users may give numerous fake feedbacks to manipulate trust results for cloud services (i.e., Self promoting and Slandering attacks). Some researchers suggest that the number of trusted feedbacks can help users to overcome such manipulation where the number of trusted feedbacks gives the evaluator a hint in determining the feedback. However, the number of feedbacks is not enough in determining the credibility of trust feedbacks.

Sybil Attacks Detection :

Since users have to register their credentials at the Trust Identity Registry, we believe that Multi-Identity Recognition is applicable by comparing the values of users' credential attributes from the identity records I. The main goal of this factor is to protect cloud services from malicious users who use multiple identities (i.e., Sybil attacks) to manipulate the trust results.

3.2 Objective

The foremost focus is to maintain the user's protection, security, and accessibility in cloud administrations. The structure and the development of trust based feedbacks, to deliver belief as a tune-up (TaaS) has to be done, TaaS is a fame-based trust maintaining framework, which provides a set of applications.

4. METHODOLOGY

RSA Algorithm :

This algorithm is used to encrypt an decrypt the messages to provide the security to the system and the data. RSA algorithm is considered as the asymmetric cryptographic algorithm which have two keys private key and public key. The public key of this algorithm can be given to everyone which will encrypt data. The private key is reserved secret, as it is used to decrypt the information .The RSA algorithm named after creators of this algorithm who are Ron Rivest, Adi Shamir and Leonard Adleman, which are print in 1978.

The following steps shows how this algorithm is used in the system:

Step 1: In the first system the system takes two prime number and assigns it to the variable p and q respectively. The numbers are generated by using the random function and then checked weather the number is prime. If the number is prime the values will be given to the changeable.
Step 2: in the 2nd step the values of the variable p & q will be reduced by 1 . i.e (p-1) and (q-1)
Step 3: in the third step , values of the variables are multiplied and stored in the new variable n.
N=(p-1)X(q-1).
Step 4: in the fourth step the values of p and q are stored in the new variable 'np'.
Np=pxq;
Step 5: in the fifth step the a common factor of the N and Np will be generated. And this common factor will be the private key which is used to encrypt the data .
Step 6: in the sixth step the text are converted into binary format and "AND" operation is performed between the binary values and the private key. these resulting values are again converted into the character format which will be in the encrypted format .

5. RESULTS

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. Efficient and intelligent output design improves the system's relationship to help user decision-making. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively.

6. CONCLUSION

In the conclusion of the paper we want to summarize the challenges we faced while storing the data in the cloud with the various nature in the cloud. It has become highly important for the cloud providers to improve the security of the system as the cloud is highly dynamic, distributed and non transparent .along with providing the security for the users we have to build the trust between the cloud and the users. According to the survey trust and security are listed on top of as the challenges in cloud. To provide this customer's feedback is the good platform to build a trust for the cloud. In proposed system aims to build the trust among cloud and the users based on the feedback of the

customers who are already using the services. It not unusual that the cloud service will face a malicious behaviour in the cloud from its users so, here we give importance to build a trust based system which provides a credibility of the trust feedbacks.

REFERENCES

[1] S. M. Khan and K. W. Hamlen, "Hatman: Intra Cloud Trust Management for Hadoop," in Proc. CLOUD'12, 2012.
[2] S. Pearson, "Privacy, Security and Trust in Cloud Computing," in Privacy and Security for Cloud Computing, ser. Computer Communications and Networks, 2013, pp. 3–42.
[3] J. Huang and D. M. Nicol, "Trust Mechanisms for Cloud Computing," Journal of Cloud Computing, vol. 2, no. 1, pp. 1–14, 2013.
[4] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14 2010.
[5] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
[6] S. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing," in Proc. of TrustCom'11, 2011.
[7] I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, and R. Konrad, "Compliant Cloud Computing (C3): Architecture and Language Support for User-Driven Compliance Management in Clouds," in Proc. of CLOUD'10, 2010.
[8] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrstedt, "A Trust Management Framework for Service-Oriented Environments," in Proc. of WWW'09, 2009.
[9] T. H. Noor, Q. Z. Sheng, and A. Alfazi, "Reputation Attacks Detection for Effective Trust Assessment of Cloud Services," in Proc. of TrustCom'13, 2013.
[10] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust Management of Services in Cloud Environments: Obstacles and Solutions," ACM Computing Surveys, vol. 46, no. 1, pp. 12:1– 12:30, 2013.