ONLINE TRUST MANAGEMENT TO PREVENT COLLUSION AND SYBIL ATTACKS

K.RAJAMANI [1], KEERTHI CHOUDHRY.K.V [2], J.PRIYA [3]

[1] Assistant Professor, Computer Science and Engineering, New Prince Shri Bhavani College of Engineering and Technology, Tamil Nadu, India
[2] Student, Computer Science and Engineering, New Prince Shri Bhavani College of Engineering and Technology, Tamil Nadu, India
[3] Student, Computer Science and Engineering, New Prince Shri Bhavani College of Engineering and Technology, Tamil Nadu, India

ABSTRACT

Cloud consumer's feedback is an important source to assess the overall trustworthiness of cloud services. It helps in improving trust management in cloud environments by proposing different ways to ensure the correctness of trust feedbacks. Credibility model is used for identify the misleading trust feedbacks from malicious user by filtering Collusion and Sybil attacks however these attacks may place in a long or short period of time. Cloud service providers advertise their cloud services in website. Thus the cloud consumer can interact with the provider through this and they can access the service they want. While the user who is new to the cloud service wants to have a review before registration, they can review the service by checking the comments of the old consumers who is already using the service. But the reviews or comment is not only given by the true user but also by the malicious user who gives comments without the experience of the cloud service. To avoid this we use the Trust Management Service by which the collusion and Sybil attacks are prevented by filtering the misleading feedbacks from malicious user.

Keyword: *Cloud computing, Trust Management, Trustworthy feedbacks, Collusion attack, Sybil attack.*

1. INTRODUCTION

Cloud Computing is a model of delivering computing resources from the Internet to the user. It enables convenient for, on demand network access to a shared pool of configurable computing resources that can be rapidly used and released with less management or service of cloud provider interaction. Services and solutions that are delivered and consumed in real time over internet are cloud services. The cloud infrastructure is much more powerful and reliable than personal computing devices. The storage solutions provide the users and enterprises with various capabilities to store and access the data in either privately owned or third party data centers that may be located far from the users ranging in distance from across a city to across the world. Now a day's sharing data using cloud becomes normal in our life. If a user wants to share data, when they are in different place means they will go for cloud hosting. Cloud computing is a set of services. Cloud is mainly used for storage purpose and it can be accessible anywhere at any time. Because of this added advantage cloud computing technology is growing day by day. If a user hosted a data in a cloud means that particular data can be accessed by other user from anywhere just by using their username and password.

When we are connected to cloud service this Gmail, Hotmail etc., we are really connecting to a massive pools of servers somewhere out there on the internet. The highly aggressive, shared and non-transparent nature of cloud services makes the trust management in cloud environment a significant challenge. Consumer feedback is an important source for improving the cloud service but it should be trustworthy. We introduce a credibility model which detects the collusion and Sybil attacks. Thus it filters the malicious feedbacks and displays only the trustworthy feedback about the cloud service. It focuses on improving trust management in cloud environment by proposing novel ways to ensure the credibility of trust feedbacks. Attackers can disadvantage a cloud service by giving multiple misleading feedbacks or by creating several accounts. Services which involve consumer’s data should preserve their privacy. There are several cases of privacy breaches such as leaks of sensitive information or behavioral information.

1.1 CLOUD PROVIDER

The cloud provider provides the cloud services to the cloud consumer. The services provided by the cloud provide includes the cloud storage, accessing the resources from the cloud from anywhere at any time and also provide the service of file sharing between two users.

1.2 CLOUD CONSUMER

The cloud consumer request for the cloud service to the cloud provider. The cloud consumer needs to choose the cloud service they prefer and trust. Thus the cloud consumer checks for the feedbacks from existing user of the particular service of the cloud. This feedback should be trustworthy, not a misleading feedback for a secure cloud access. Since they are more number of cloud consumers it is difficult to monitor the action of all the users.

1.3 CLOUD PRIVACY

The adoption of cloud computing raise privacy concerns. Consumers can have dynamic interactions with cloud providers, which may involve personal information. There are several cases of privacy crack such as leaks of sensitive which can be a personal information of a user which must be secured. Undoubtedly, services which involve consumer’s data should preserve their identity privacy.

1.4 CLOUD ARMOR

The Cloud Armor is a framework which provides the space of interaction between the cloud provider and the cloud consumers. This framework is based on the Service Oriented Architecture (SOA), which delivers trust as a service. SOA and web services are one of the most important technologies used in cloud computing where the resources such as infrastructures, platforms, and software are given in clouds as services. In the trust management service there are several options which provide interfaces where the users can access the resources, give their feedbacks about the service and can also have the view of the feedbacks and trust results.

1.5 MALICIOUS USER

Malicious users may give numerous fake feedbacks to manipulate trust results for cloud. Some researchers propose that the number of true feedbacks can help users to overcome such manipulation where the number of trusted feedbacks gives the evaluator a hint in finding the feedback possibility .However, the number of feedbacks given by the user is not enough in finding trust feedbacks.

1.6 SERVICES

SOA and Web services are one of the most important technologies used in cloud computing which provide service by offering several resources such as infrastructures, platforms, and software that are given to the cloud consumers in clouds as services. In the trust management service there are several options which provide interfaces where the users can access the resources, give their feedbacks about the service and can also have the view of the feedbacks and trust results.

2. EXISTING SYSTEM

The Identity Management Service (IDM) is used which facilitate trust management service in the detection of Sybil attacks against cloud service without breaching the privacy of users. When the users attempt to use TMS for the first time, the user needs to register details in IDM to establish their identity. In this it is easy to sear unwanted data and thus data storage is not secure and it does not detect collusion attack.

3. PROPOSED SYSTEM

The trust management service is used which provides an interface between users and cloud services for effective trust management. However, guaranteeing the availability of trust management service is a difficult problem due to the unpredictable number of users and the highly dynamic nature of the cloud environment. It is not unusual that a cloud service experiences attacks from its users. Attackers can disservice a cloud service by giving multiple misleading feedbacks (i.e Collusion attacks) or by creating several accounts (i.e Sybil attacks).In collusion attack we check whether the user is really a cloud consumer who is trustworthy by seeing whether the user giving the feedback is trustworthy or not. In Sybil attack we check for two things-for registered user and their usage of the cloud service if the cloud consumer giving the feedback is registered, we will be checking for the usage of the cloud by that cloud consumer. For example if the cloud service provide 800MB we check whether the cloud consumer has used minimum of 100Mb or not, if the user used it then the feedback from the user will be taken and displayed if not it will not be displayed, considering the user as a malicious user.

3.1 COLLUSION ATTACK

Collusion attack is an attack where the malicious user (i.e untrusted user) gives the wrong or misleading feedback about the cloud service provided by the cloud provider. In this malicious user means the user or an attacker who is never registered to the cloud service or the one who is not used the cloud service provided by the cloud provider. In this project we prevent the collusion attack by avoiding the misleading feedbacks from unregistered users. Thus we check whether the user who is giving the feedback is registered or not. If the user is an unregistered one, the admin accepts the feedback but does not display it in cloud service website. If the person giving the feedback is registered then he/she is called as the cloud consumer and their comments are accepted and displayed to the new user.

3.2 SYBIL ATTACK

The Sybil attack on a cloud service can be prevented by accepting feedbacks only from the registered users that too the users who used minimum of the cloud service. Thus the admin filters the misleading feedbacks by checking whether the user using the cloud service used minimum of cloud service or not. If not the admin accepts the feedback but does not display it in the cloud service website .So with this technique the Sybil attack can be prevented by displaying only the trustworthy feedbacks from the user who used minimum of service provided by the cloud provider.

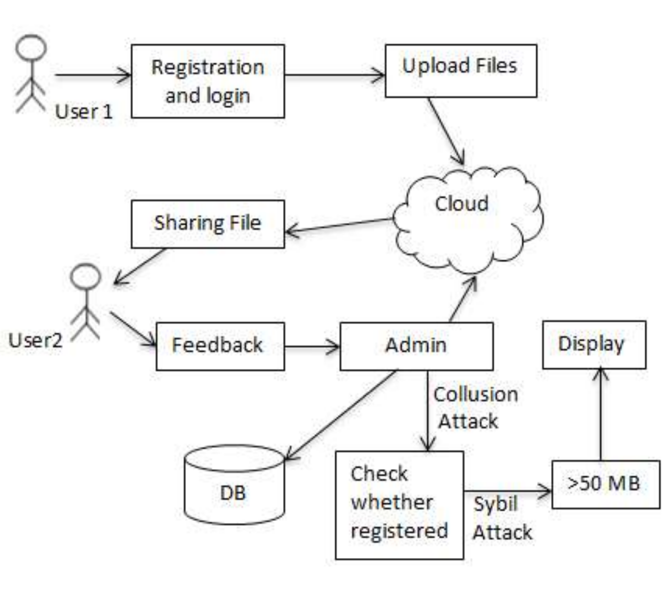

Fig1. Architecture of Trust Management Service

4. METHODOLOGY

We propose Trust Management Service in this paper to maintain trust between the cloud consumer and cloud provider. So the service provided to the cloud consumers will be trustworthy.

4.1 ADVERTISEMENT FOR EACH CLOUD

The cloud provider advertises the cloud services they provide to the cloud consumer. Each Cloud Service as its own advantages and disadvantages. This advertisement includes all the services provided by a particular cloud service from which the cloud consumer can choose the service they want. The cloud consumer can check for the review about each cloud service provided before they use the particular cloud service, which will be trustworthy.

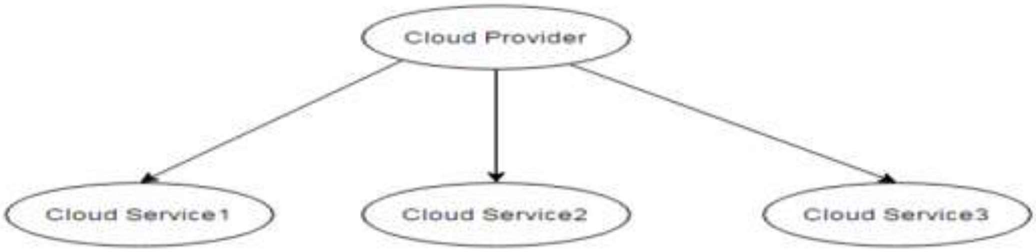

Fig2. Cloud Advertisement

4.2 REGISTRATION AND LOGIN

The user needs to register before they use a particular cloud service. In registration process they must give their identities like name, email-id, phone number etc. which will be secure. If the user is a registered user then they can directly login to use the cloud service were they can upload a file, share a file and can also access the file from anywhere at any time.

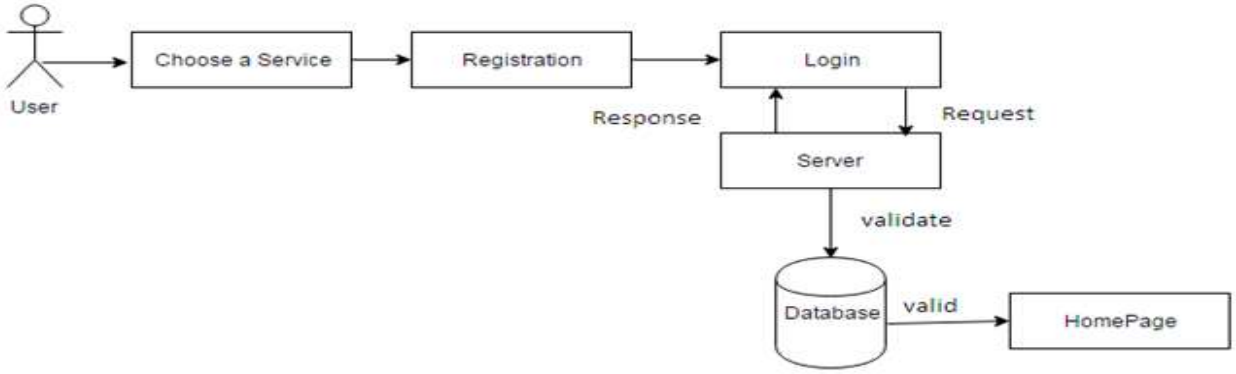

Fig3. Registration and Login

4.3 UPLOADING AND SHARING A FILE

The registered user can upload their files into the cloud storage provided which can accessed anytime from anywhere. The file uploaded can be of any format and extension. The uploaded file can also be shared. Thus the user can share multiple files in their storage to any one by attaching the file and specifying the receiver name.

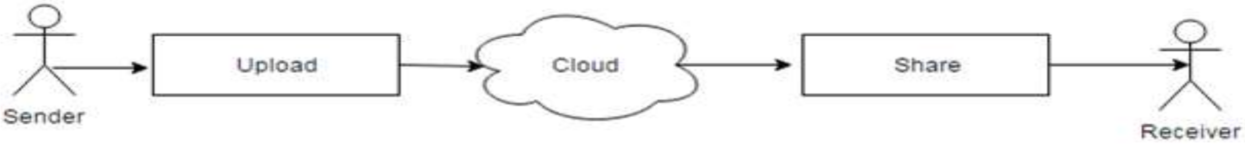

Fig4. Uploading and sharing a file

4.4 TRUSTWORTHY REVIEWS

Feedbacks are very important for both cloud provider and cloud consumer. The cloud provider can improve their service by updating their service based on the feedbacks from the user and the cloud consumer checks the feedback before he/she use the cloud service so that they come to know about services provided by cloud provider. Thus the feedbacks must be trustworthy; it should not be a misleading feedback. Here in this project the admin filters the misleading feedbacks by preventing Collusion and Sybil attacks and displays only the trustworthy feedbacks to the cloud consumers.

5. LITERATURE SURVEY

The trust management will support the customers in making transparent assessment before selecting reliable trustworthy cloud providers. Cloud computing provides cost-efficient opportunities for enterprises by providing a variety of aggressive, adaptable and shared services. Usually, cloud providers provide assurances by specifying descriptions in Service Level Agreements (SLAs) for the services they offer. The descriptions in SLAs are not steady among the cloud providers even though they offer services with are similar. Therefore, customers are not sure whether they can identify a trustworthy cloud provider only based on its Service Level. This system defines to identify the trustworthy cloud providers assessed by multiple sources and trust information. [1]

Many reputation management systems have been developed under the consideration that each entity in the system will use different added function. Most of the previous work in reputation management has concentrated on providing robustness and improving the performance for a given method. In this paper, we present a reputation-based trust management that supports the synthesis of trust-related feedback from many different entities and also providing each entity to apply different added functions over the same feedback data for customized trust evaluations. We propose a scheme to cache trust values which dependent on recent client activity. To evaluate our approach, we implemented trust management service and tested it on a realistic application in both LAN and WAN environments. The results indicate that the trust management service can effectively support multiple scoring functions with low overhead and high availability. [2]

Consumers' feedback is a good source to help assess true cloud services. However, it is not unusual that a system experiences attacks from its users (collusion or Sybil attacks). In this paper, we propose techniques for the detection of attacks to allow consumers to identify true cloud services. We introduce a credibility model that not only identifies misleading feedbacks from collusion attacks and also detects Sybil. Have collected a large consumer's trust feedbacks given on real-world cloud services to evaluate and determine the application of our approach and show the capability of detecting such malicious behaviors. [3]

Cloud Computing is an emerging pattern for large scale infrastructures. It can reducing cost by sharing computing and storage resources, combined with an on-demand afforded mechanism relying on a pay-per-use business model. These new features have a direct impact on many budgeting but also affect traditional security, trust and privacy methods. Many of these methods are no longer adequate, but need to be re-thinking to fit this into new pattern. In this paper we assess how security, trust and privacy issues occur in the relation of cloud computing and discuss ways in which they may be addressed. Thus this paper is used as a reference the project were we concentrate on the privacy, security and the trust issues which arise a problem in cloud computing. So the information of the user will be secured with privacy. [4]

Trust management is one of the challenging issues in the cloud computing area. Over the past few years, many researches have suggested different methods to address trust management issues. However, despite of this several trust management issues such as identification, privacy, security, and scalability have been neglected and need to be defined before cloud computing can be fully grasped. It presents a generic framework that assesses existing trust management prototypes in cloud computing and relevant areas using a set of estimated principle. Open research issues for trust management in cloud environments are also discussed. [5]

6. CONCLUSION

In the cloud service managing and creating trust between cloud consumer and cloud providers is a large challenge. The trust between cloud user and the provider can be done by preventing Collusion and Sybil attacks. In this paper we propose the trust management services to detect the Collusion and Sybil attacks by filtering the misleading feedbacks given by the trustworthy user. Since there will be several users in the cloud service, it is a big challenge to maintain trustworthiness of the cloud. Thus by preventing the above two attacks-Collusion attack and Sybil Attack the cloud service consumer will get a trusted service. So the cloud service provided by the cloud provider will be trustworthy since we avoid malware feedbacks from the malicious user who is not a true cloud consumer. The true cloud consumer is a one who experienced the cloud service provided by the cloud provider at least for minimum amount.

There are few directions for future work were we can improve the trustworthiness of the feedbacks given by the cloud consumer by using an efficient method were the cloud consumer identities are secured without any malicious attacks. Thus also provide privacy to the cloud consumer.

7. REFERENCES

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

[2]. W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K.Nahrstedt, “A trust management framework for service-oriented environments,” in Proc. 18th Int. Conf. World Wide Web, 2009, pp. 891–900.

[3]. T. H. Noor, Q. Z. Sheng, and A. Alfazi, “Reputation attacks detection for effective trust assessment of cloud services,” in Proc.12th Int. Conf. Trust, Security Privacy Comput. Commun., 2013, pp. 469–476.

[4]. S. Pearson, “Privacy, security and trust in cloud computing,”In Privacy and Security for Cloud Computing, service. Computer Communications and Networks. New York, NY, USA: Springer, 2013, pp. 3–42.

[5]. T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, “Trust management of services in cloud environments: Obstacles and solutions,”ACM Comput.Surv., vol. 46, no. 1, pp. 12:1–12:30, 2013.