International Journal of Research and Advanced Development (IJRAD)

Security Challenges for Privacy and Trust Issues Arising in Cloud Services

S. Kayalvili[1], K. Sivaraj[2], P. Soundarya[3], G. Yuvaramachandran[4]

[1, 2, 3, 4] Department of Computer Science and Engineering,
Velalar College of Engineering and Technology, TN, India.

Received Date: 17th March, 2017, Accepted Date: 28th May, 2017.

Abstract-Trust management is one of the issues through the development of cloud computing and the most challenging. Highly Dynamic cloud services, and distributed opacity introduced some challenging issues, such as privacy, security, and availability. Protecting consumer privacy is not an easy task, due to the sensitive information, participate in interactive between consumers and trust management services. Protection of their cloud services malicious users (for example, those users Switch misleading feedback may disadvantage a particular cloud service) is a problem. Ensure the availability of Trust management business because of the dynamic nature of the environment of another significant challenge for cloud computing. In this article, Cloud Armor, reputation-based trust management framework is discussed, which provides a set of design and implementation Feature provides trust services (TaaS), including: a new protocol to demonstrate credibility and trust feedback Protect users' privacy, two) for measuring trust feedback, in order to protect the credibility of the adaptive cloud and strong credibility model Malicious users and services are relatively cloud service reliability, and the availability of models to manage Trust management services to implement the availability of decentralization. The feasibility and benefits of our approach by using a set of confidence-building real-world feedback on the prototype and experimental research in cloud services confirmed.

Keywords: Cloud Services, Security, Identity, Trust Management Services, Cloud Login.

I. INTRODUCTION

The trust management in cloud environments makes a significant challenge which is highly dynamic, distributed, and nontransparent nature of cloud services. One of the top ten obstacles for the adoption of cloud computing is trust and security. To make a service level agreement is inadequate for establishing the trust and the trust providing services between the cloud consumers and the providers [3]. Because the connection between them is unclear and inconsistent clauses. In case of the trustworthiness of the cloud service consumers' feedback is one of the good sources to assess it. Some of the researchers had recognize the significance of trust management and the proposed solutions to assess it and it will manage the feedback which is collected from the participants where it's a trust based on feedbacks. In this process, Cloud services experiences a malicious behaviors which is not unusual (e.g. Sybil attacks (hackers) or collusion) from its users. In this paper, the combined form of all the trust management service and to improve the trust management in cloud environments to ensure the credibility of trust feedbacks.

II. RELATED WORKS

Accountability and Trust in cloud computing by using Trust Cloud framework. Specifically, there are five layers including workflow, data, system, policies and laws, and regulations layers which is to address accountability for the cloud environment. These five layer will maintain the cloud accountability life cycle which is of seven phases [1]. The seven phases are reporting, auditing, replaying etc. Cloud environments can have compliance management to establish trust between different parties. It is developed by using a centralized architecture and uses compliant Trust Management technique which is to establish trust between cloud service providers and cloud service users. As this method uses policy-based trust management techniques, trust services cloud use the reputation-based trust management techniques.

As to modulate the reputation based filtering method the account register by the user is prevented and the multiple account for a single user is avoided. One of the main specifications of the user can be given and so the user can have only a single account [2]. By using this techniques Prevention of account from the malicious user can be avoided. Over the past few years in the area of cloud computing, the trust management has lot of topics. Some of research efforts use policy-based trust management techniques. Trust-Cloud framework for trust and accountability in cloud computing. Trust-Cloud consists of five layers includes data, workflow, policies, laws and system. To address accountability in the cloud environment, regulation layers are used. These layers maintain the cloud accountability life. It consists of seven phases includes logging, trace and sense, reporting and replaying, policy planning, safe-keeping of logs, optimizing and rectifying, auditing [4]. To establish trust between different parties, propose a novel approach for compliance management in the cloud. This approach is developed using centralized architecture and which uses compliance management technique to establish trust between Cloud Service Provider (CSP) and Cloud Service Users (CSU). We propose a security aware architecture of cloud which assesses the trust of both cloud service provider and cloud service users. In this paper, a credibility model which not only identifies the trust feedback from the Sybil and Collusion attacks is proposed. But it has the ability to adjust the trust result of the cloud services which affected by malicious behaviors.

III. ATTACKS AND ASSUMPTIONS

In this project the feasibility study is analyzed by the following phase and a general plan for the project is the business proposal which is put with some cost estimate. At the time of analyzing the system the feedback system in the reputation based form and the Sybil attack of the product is find by feedback mechanism. Thus the process has to ensure that the proposed system of the project is not a burden to the industry or the company. For analyzing the feasibility, some of the requirements for the system control for the Sybil attackers is essential in analyzing the new attackers. In analyzing the feasibility there are three key features. They are (1) Economical feasibility, (2) Technical feasibility and (3) Social feasibility

IV. ECONOMICAL FEASIBILITY

The economic study has to carry out the attackers for making the Sybil attacker. The one using the account of others by knowing the secret password and the feedback is provided in the wrong way. As the majority of cases, it failed so the security provided by the misleading feedbacks provided by the users. For minimizing the misleading feedbacks which are created by the Sybil attackers and Trust management system mechanisms are used.

V. TECHNICAL FEASIBILITY

The one using the account of others by knowing the secret password and the feedback is provided in the wrong way. As the majority cases, it failed so the security provided by the misleading feedbacks provided by the users. At the time of analyzing the system the feedback system in the reputation based form and the Sybil attack of the product is finding by feedback mechanism. Thus the process has to ensure that the proposed system of the project is not a burden to the industry or the company.

VI. IMPLEMENTATION

A. User Details

In this process of registration, the user has to register the details using the specification like Aadhar card. The Aadhar card specification is given because the user can have only single account and the multiple account is avoided by the combination of some techniques thus the misleading feedbacks can be avoided. The “pdf” form of Aadhar card should be uploaded during the registration process. The user can order the products which are placed or uploaded by the cloud. The user can give the feedback for the product which they ordered.

B. Cloud Armor

The process of cloud armor is to update the product and the product details in the cloud. The User details are stored in the cloud. The cloud armor will give the details of current user in the cloud. The user will give the feedback for the product and the feedback details are stored in the cloud armor. The user feedback is preserved from the Sybil attackers.

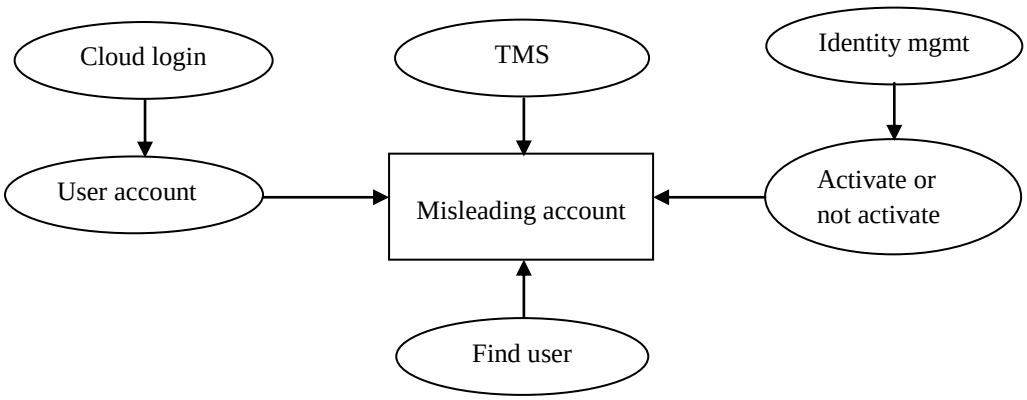

Fig. 1 Proposed Method

C. Trust Management Service

In a typical interaction of reputation-based TMS, the user either requests the trust assessment of the service or gives feedback regarding the trustworthiness of a particular cloud service. From the user’s feedback, the cloud service’s trust behavior is a collection of invocation history, represented by H= (C, S, F, Tf), where C is user primary identity, S is cloud service identity, F is set of QoS feedbacks. Each trust feedback represented in the numerical range of [0, 1]. Tf is timestamps if feedbacks are given. TMS calculates trust results whenever a user gives request to assess the cloud services.

D. Identity Management Service

To establish their identities, TMS requires them to register their credentials at the trust identity registry. For every user trust identity registry stores an identity record represented by T= (C, Ca, Ti). C is the user’s primary identity. Ca is set of credentials attributes. Ti is user registration time. We propose a Zero-Knowledge credibility proof protocol to allow the

TMS to process IDM's information. Without knowing the user's credentials, TMS will prove the user's feedback credibility.

E. Attacks in the Cloud Services

A trusted third party handles Trust Management Service (TMS) which acquires secure communication. The attack which takes place here are Sybil attack and collusion attack. The collusion attack is that many users will provide feedbacks at the same time and during that time the collusion attacks takes place. And the combined form of techniques is used for securing the feedbacks and the user details stored in the cloud armor. In order to increase the trust results of cloud services for example self-promoting attack is to decrease the trust results of cloud services slandering attack because several users collaborate to give numerous misleading feedbacks. In Sybil attack, to give numerous misleading feedbacks several user exploit multiple identities. To disguise the negative historical trust records attacker use multiple identities.

F. Feedback Collusion Detection

To manipulate the trust results for cloud service user give numerous fake feedbacks. Trusted feedback can help users an evaluator hint in determining the feedback credibility. User usually prefers cloud service with higher aggregator with trust feedback. To overcome the collusion attacks and the Sybil attacks there is a proposed model is by using the feedback mass, feedback density and feedback volume. Feedback density is used for the determination of the credible feedbacks. Feedback mass is the total number of users who gives trust feedback to the cloud service. Those total number of trust feedback is known as feedback volume. Feedback volume collusion is a factor that influences feedback volume. By the use of specified volume threshold, feedback volume collusion can be controlled. The overall trusted feedback volume is colluded by the multiple trust feedbacks. The occasional feedback collusion is the collusion against cloud services. In occasional feedback, one of the most important factors is time where it is used to detect the occasional and periodic feedback. Percentage of the occasional changes is measured by the total number of feedbacks given by the users.

VII. CONCLUSION

Given the distributed, non-transparent, highly distributed nature of cloud services, establishing and managing between cloud services and cloud service users has a significant challenge. As the conclusion, user can have only single account we have overcome the process of creating multiple account for the single user. By using the Trust management Techniques, the combined level of techniques for preventing from the Sybil attackers. In this paper, we have presented combined form of Trust Management Techniques for the detection of reputation based attacks. The future work of this paper is to make support for the mobile applications. In particular, we present a credibility model which detects the trust feedback from collusion attacks. It also identifies the Sybil attacks no matter these attacks occur in a short or long period of time. We created availability model which keeps the service of trust management at required level. To evaluate proposed techniques, we collected a numerous trust feedbacks given real-world cloud services.

REFERENCES

[1] S. M. Khan and K. W. Hamlen, "Hatman: Intra-cloud trust management for Hadoop," in Proc. 5th Int. Conf. Cloud Computer, pp.494-501, 2012.
[2] S. Pearson, "Privacy, security and trust in cloud computing," in Privacy and Security for Cloud Computing, Computer Communications and Networks. New York, NY, USA: Springer, 2013.
[3] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," J. Cloud Computer, 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 computer, Vol. 14, No. 5, pp. 171-178, 2015.