Providing Trust as a Service by Feedback Analysis to Cloud Services

Santoshi Ravali Dantuluri [#1], Dhanarekha Doddi[#2], Ananth Kale[#3], Bhagavan G[#4]
Mr. B. A. Swamy[M.Tech] [*1]
[#1, 2, 3, 4] *students CSE Department, Lendi institute of engineering and technology,*
[*1]*Assisstent Professor CSE Department, Lendi institute of engineering and technology,*
VIZIANAGARAM, ANDHRA PRADESH, INDIA.
[1]santoshiravali5555@gmail.com [2]dhanarekha521@gmail.com [3]ananthkale1234@gmail.com
[4]bhagavandarling435@gmail.com

***Abstract*— Offering Trust to consumers of cloud services is the main obstacle for the endorsement of cloud computing. The cloud service's dynamic nature makes it even more difficult and challenging for providing Security, Privacy. Protecting Privacy of cloud service user and providing security to user's data is a critical job for a cloud service provider as a lot of crucial information is included in interaction between user and the trust management system. Defending service provider from their malicious users is one of the challenging issues as Attacks are performed on cloud service providers by its malicious users. These malicious users conspire together and give multiple deceptive feedbacks on a specific cloud service to endorse or damage the cloud service provider's esteem. In this paper effort is made to provide trust as a service by cloud service user's feedback analysis to cloud services and to preserve the cloud service provider's stature from malicious behaviour.**

***Keywords*— Cloud computing, Security, Privacy, Trust Management System**

I. INTRODUCTION

User's feedback is a robust source to analyse a cloud service's reliability. Many researchers provided solutions for analyzing trust on basis of feedback gathered from consumers [1], [2]. Malicious attacks on cloud services have become quite common these days, from its consumers. The objective of this paper is to improvise trust management and to protect the reliability of the user's feedback. For the trust management in cloud, we mainly focus on the following important issues:

- Consumer's privacy concerns have been increased since the endorsement of cloud computing [3]. As crucial information (e.g., user's personal information like phone number, address, interests, etc.) is involved in the interaction between the consumer and the cloud service provider, these services should protect the user's privacy.
- Cloud Service Protection is another significant challenge as occurrence of attacks from its malicious user's is not unusual. Attackers can damage the cloud service reputation by giving multiple deceptive feedbacks or by creating multiple user accounts. Thus, identifying such malicious activities is not an easy task because, users join and leave the cloud environment every day and this consumer dynamism makes the very difficult to identify where and when the occurrence of malicious behaviour will happen.
- Trust Management Service is made available as an interface between consumers and the cloud services in order to provide a more efficient trust management. However, assuring the availability of trust management service is the major concern because of the dynamic nature and uncertain number of consumers in the cloud domain.

In this paper we focus on providing the following silent features:

- Privacy. Here we provide a service that protects the users' privacy and the feedback credibility of a user.
- Credibility. In order to distinguish deceptive feedbacks from malicious users we introduce a credibility model as the trustworthiness of the feedbacks effect the trust management services' performance.

II. EXISTING SYSTEM

In Accordance with researchers at Berkeley [4], security and trust are rated among the top 10 complications for the endorsement of cloud computing. Certainly, just the Service-Level Agreements (SLAs) are insufficient to establish trust among cloud service provider and its consumers because of its uncertain and non-uniform stipulations [5]. Cloud service Users' feedback is a adequate source to evaluate the complete credibility of cloud services. Various researchers have identified the importance of providing effective trust management and presented solutions to evaluate and control trust based on feedbacks accumulated from users.

A. *Drawbacks Of Existing System:*

- Guaranteeing the availability of Trust Management System is a critical issue because of the uncertain number of users and the highly distributed, dynamic nature of the cloud System.
- There could be situations where, unknowingly the user would choose the cloud services on which Self-promoting attack have been performed.
- Malicious users can damage a cloud services' reputation by giving several deceptive trust feedbacks (i.e., collusion attacks).

- There could be situations which would trick users into trusting cloud services that are not credible by creating multiple fake accounts and giving misleading trust feedbacks through those accounts(i.e., Sybil attacks).

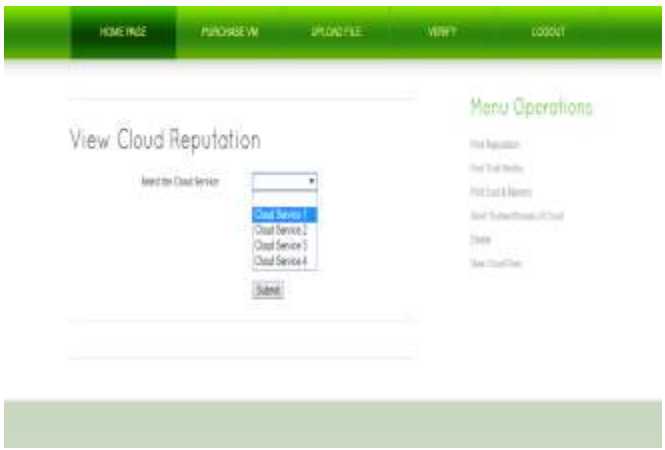
III. PROPOSED SYSTEM

Cloud service consumers' feedback is an effective source to evaluate trust and credibility of a cloud service. The trust management service provides users the capacity to choose a specific cloud service they want to evaluate. Here, we proposed novel technologies that can assist in identifying malicious behaviours from users and enabling the consumers to efficiently identify trustworthy cloud service that best meets their requirements. We proposed credibility model that will identify deceptive trust feedbacks occurred due to collusion attacks [6] (attacks that take place when deceptive users work together to give multiple misleading feedbacks for self-promotion of trust results of a particular cloud services or to slander the trust results of a particular cloud service) and also identifies Sybil attacks [7] (attacks that take place when malicious consumers make use of several identities to provide several deceptive feedbacks for self-promotion or slandering a particular cloud service). These metrics will identify deceptive feedbacks from malicious users, allow trust management system to identify users with multiple identities and provide credible trust results.

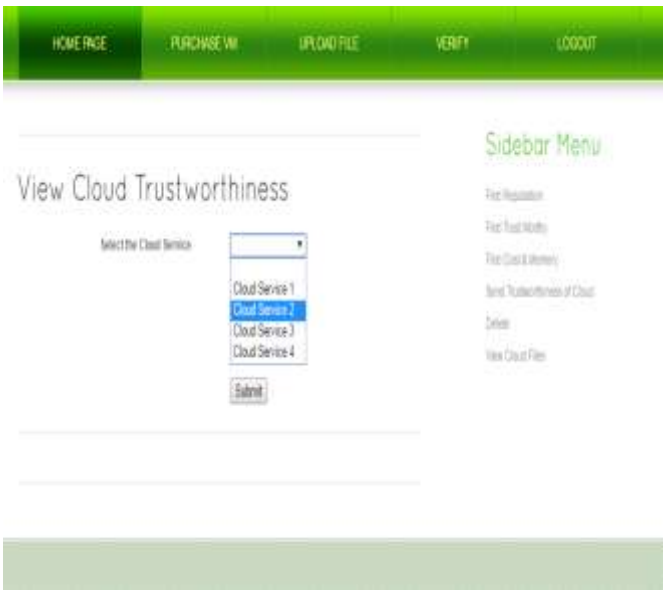
A. *Advantages Of Proposed System:*

- *This will allow the cloud service consumers to search for cloud services and to identify trustworthy cloud service providers.*
- *It provides techniques to identify credible feedbacks from malicious ones.*
- *It also allows consumers to view number of attacks performed on each service. Therefore, user can choose a service with least number of attacks.*

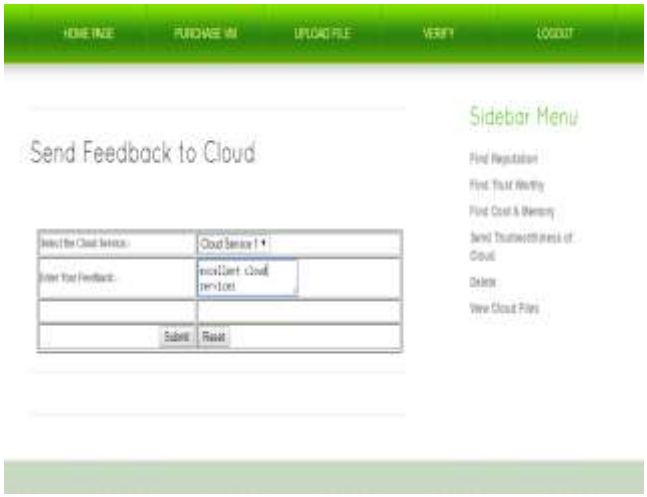
B. *Interface for Finding Reputation of a cloud service:*



C. *Interface for Finding Trustworthiness of a Cloud service:*



D. Interface for Sending Feedback about cloud service:



IV. SYSTEM ARCHITECTURE

The system architecture is built on the basis of service oriented architecture (SOA), which provides trust as a service. For cloud computing, Web services and SOA are the major enabling technologies as the resources (e.g., platform, software and infrastructure) are exhibited as services. Here, Trust management service exhibits interfaces so that consumers can provide their feedbacks or request the trust results. Figure 1 represents the framework, which is comprised of three layers, they are the cloud service provider layer, trust management service layer, cloud service consumer layer.

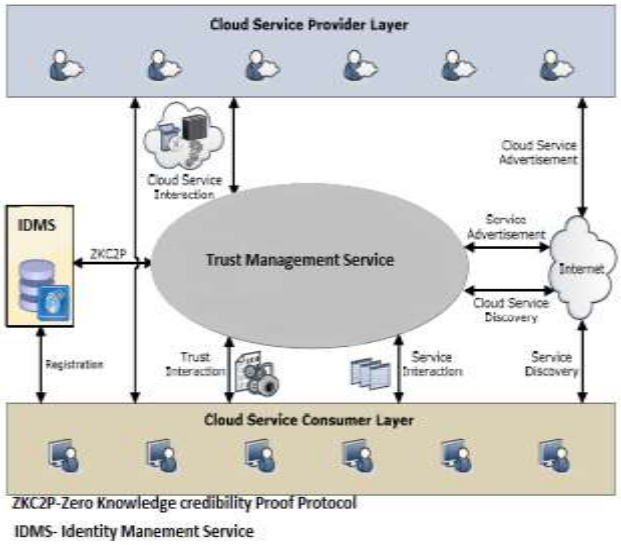


Fig. 1 System Architecture

The cloud service provider layer contains many cloud service providers who provide one or multiple cloud services (e.g., Saas-software as a service, Paas-platform as a service, Iaas-Infrastructure as a service). The interactions between this layer and the user are called cloud service interactions.

The Trust Management Service Layer provides interfaces so that consumers can provide their feedbacks or inspect the trusted services. This layer includes interactions like: i) cloud service interactions with service providers, ii) service advertisement to advertise the trust as a service to consumers iii) cloud service discovery will permit consumers' assess the credibility of the new cloud services, and iv) Zero-Knowledge Credibility Proof Protocol (ZKC2P) interactions will allow trust management service to determine the credibility of a particular user's feedback.

The cloud service consumer layer is composed of several consumers' who utilize cloud services. For example, a start-up with limited finance can utilize cloud services and lower their budget. This layer includes interactions like: i) service discovery will allow consumers to find new cloud services, ii) trust interaction and service interaction will allow consumers to provide their feedback or retrieve the trustworthiness of a particular cloud service, and iii) registration for the consumers is required for establishing their identity by registering their ID in identity management prior to using Trust management.

V. CONCLUSIONS

Consumer's feedback is reliable source to evaluate the trustworthiness of a particular cloud service. But, malicious users might try to mislead the trust result of a cloud service but performing reputation based collusion or Sybil attacks (i.e., self-promotion or slandering techniques). Here, we introduced credibility model that helps in identifying these reputation based attacks and allow consumers to efficiently recognise the trustworthy cloud services. We have evaluated the proposed technique and the experimental results show the capability of identifying such malicious behaviour and the applicability of the proposed approach.

In our future work we plan to collaborate various trust management techniques (recommendations and reputation) to improve the accuracy of trust result.

References

[1] 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.
[2] 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.
[3] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising From Cloud Computing," in *Proc. CloudCom'10*, 2010.
[4] 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.
[5]S. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing," in *Proc. of TrustCom'11*, 2011.
[6]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.
[7] J. R. Douceur, "The Sybil Attack," in *Proc. of IPTPS'02,* 2002

