ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Implementation of Trust Management in Cloud Services

Mahantesh Pujari
Department of Information Science and Engineering
The National Institute of Engineering, Mysuru.

Jagadeesha Kumar
Department of Information Science and Engineering
The National Institute of Engineering, Mysuru.

C K Vanamala
Department of Information Science and Engineering
The National Institute of Engineering, Mysuru.

ABSTRACT

Trust management is the important obstacles to the adoption and growth of Cloud Computing. Although many answers have been provided recently in managing trust feedbacks in a cloud environment. In increase, managing trust feedbacks in cloud environments are a hard case because many numbers of cloud environment, consumers and the highly dynamic, broadcast and non-crystalline nature of cloud services leads to the many challenging topics such as secrecy, security and accessibility. The trust management framework presents a lot of functionalities to deploy Trust as a Service (TaaS), which includes

i) A novel protocol to test the credibility of trust feedbacks and privacy of guests.

ii) Adoption and credibility model to assess the credibility of trust feedbacks to secure cloud services from malicious clients and to analyze the dependability of cloud services.

iii) An availability model to confirm the availability of the decentralized access of the trust management of cloud environment.

I. INTRODUCTION

Trust management is based on feedbacks collected from users' feedback which is a good output to assess the overall trustworthiness of cloud environment. Cloud computing consists of hardware and software resources made available on the Internet as managed by third-party services. In this paper, we implement The Trust as a Service (TaaS) framework. This fabric serves to distinguish

Among the credible and the malicious trust feedbacks. The characteristics of the TaaS framework are:

i) A Credibility Model:

This example not only identifies misleading trust feedbacks from collusion attacks but also detects Sybil attacks.

ii) Distributed Trust Feedback Approval and Storage:

To eliminate the disadvantage of centralized architectures, our trust management service allows trust feedback approval and storage to be maintained distributively.

II. SYSTEM DESIGN

This consists of three different layers, namely the Cloud Service Provider Layer, Service Consumer Layer and Trust Management Service Layer.

Cloud Service Provider Layer:

This layer consists of different cloud service providers such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service).These cloud services are accessible through Web portals and indexed on Web search engines such as Google, Yahoo, and Baidu .Interactions for this layer are considered as cloud service interaction with users' TMS and cloud services advertisements where providers are able to advertise their services on the web.

The Trust Management Service Layer:

This layer consists of different distributed Trust Management Service links which are uploaded in different cloud environment services in different wild Areas. These links interact with users and supply their feedback.This layer communicate with:

i) Cloud service interaction with cloud service providers.

ii) Service advertisement to promote the trust as a serving to users through the Internet.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

iii) Cloud service discovery through the Internet to permit users to access the trust of new cloud services.
iv) Zero-Knowledge Credibility Proof Protocol (ZKC2P) interactions, enabling TMS to customer's feedback.

The Cloud Service Consumer Layer:

Finally, this layer consists of different users who use cloud services. For instance, a new startup that has limited funding can consume cloud services.

Interactions for this layer include:

Service discovery where users are able to find out new cloud services and other services through the Internet, Faith and service interactions where users are able making their feedback or call back the trust results of a particular cloud service.

Registration where users build their identity through registering their credentials in IdM before using TMS.

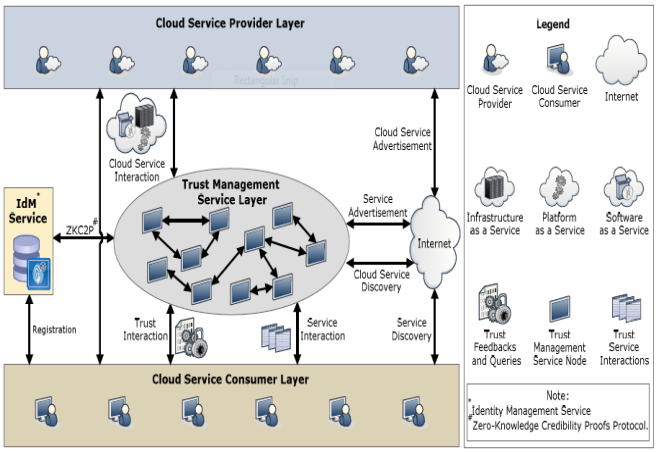

Fig.1. Architecture of the Cloud Armor Trust Management

III. DATA FLOW DIAGRAM

If user's wants to access cloud services they need to be registered and login into a cloud service.

After the login users will get three services: Cloud Provider Service, Identity Management Service and Trust Management Service along with the user's Service.
i) The Cloud Services Provider which provides added the service, service list, access list, update rate to the cloud user's.
ii) The Identity Management Service interacts with TMS layer and Consumer layer and handles the user's details, attacker's (sybill and collusion attack).
iii) The Trust Management Service interacts with consumer service, Idm service and cloud provider services. This service manages user details, service details, feedback, publish and revoke the details.
iv) Finally, User Serviceable view profile, search the adds, purchase and give the feedback about the service.

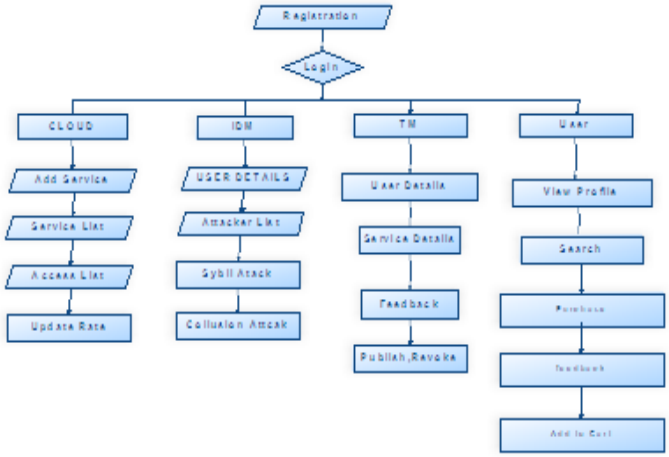

Fig 2.Data Flow Diagram

V. SEQUENCE DIAGRAM

The user registration details are stored in cloud database and the cloud manages the service such as add the services show the service list and update the rate for service these are all data stored in the cloud database. The IdM service manages the user details and attacker details and the information is stored in cloud database.

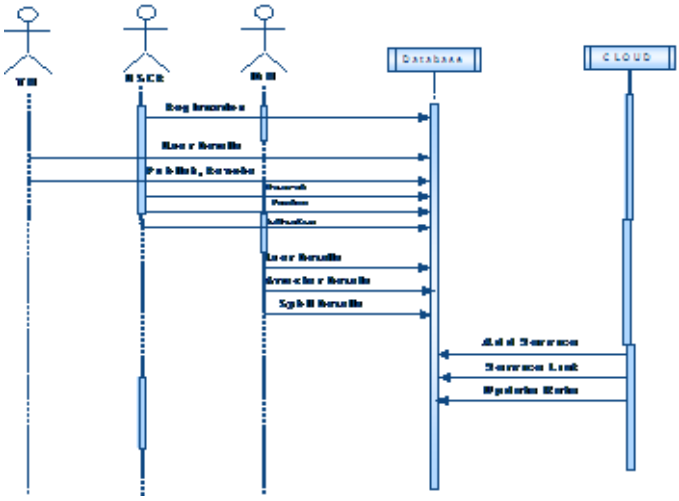

Fig 3.Sequence Diagram

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CONCLUSION

The highly dynamic, distributed and nontransparent nature of cloud services, managing and building trust between cloud service users and cloud services remains a substantial challenge. Cloud service user feedback is an honest beginning to evaluate the overall trustworthiness of cloud services. In this paper, we have proposed novel techniques that assist in detecting reputation based attacks and letting users to effectively identify trustworthy cloud services. In particular, we present a credibility model that not only identifies misleading trust feedbacks from collusion attacks, but also detects Sybil attacks, no matter where these attacks take place in a long or short period of time. We also build up an availability model that holds the trust management service at a desired point. We have accumulated a great act of consumer trust feedbacks given on real-world cloud services to evaluate our proposed techniques.

REFERENCES

[1] S. M. Khan and K. W. Hamlen, "Hatman: Intra-Cloud TrustManagement 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 Communicationsand 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 SecureResources and Data Coloring," IEEE Internet Computing, vol. 14,no. 5, pp. 14–22, 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, "AView 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 ManagementSystem for Cloud Computing," in Proc. of TrustCom'11,2011.

[7] I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, andR. Konrad, "Compliant Cloud Computing (C3): Architecture andLanguage Support for User-Driven Compliance Management inClouds," in Proc. of CLOUD'10, 2010.

[8] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrstedt,"A Trust Management Framework for Service-OrientedEnvironments," in Proc. of WWW'09, 2009.

[9] T. H. Noor, Q. Z. Sheng, and A. Alfazi, "Reputation AttacksDetection for Effective Trust Assessment of Cloud Services," inProc. of TrustCom'13, 2013.

[10] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust Managementof Services in Cloud Environments: Obstacles andSolutions," ACM Computing Surveys, vol. 46, no. 1, pp. 12:1–12:30, 2013.