International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Trust as a Service : A Framework for Accountability and Trust Assessment In Cloud Environment

Jasmine S, Kavitha E, Ebenazer Roselin S
Department of Computer Science and Engineering, Prince Dr. k. Vasudevan College of Engineering and technology, Anna university, Chennai, Tamilnadu, India

ABSTRACT

Trust assessment is one in all the foremost difficult problems that arise in a cloud computing environment. Consumers feedback is a good source to assess the overall trustworthiness of cloud services. To make these difficult problems be simpler by getting feedbacks from users. Generally a cloud refers to a public semi-public space on transmission lines that exists between the end points of a transmission. Cloud providers can be chosen based on advertisements. Based on the usage of particular provider service users can be considered as real users. Reviews can be collected from all users. By the use of Trust Management Service (TMS) algorithm an original user reviews can be identified accurately because it provides an interface between users and cloud services for effectiveness in trust management. Attackers can disadvantage a cloud service by giving several multiple misleading feedbacks (i.e.,collusion attacks) or by creating a multiple accounts (i.e., Sybil attacks). Filtering of fake reviews done based on the attacks of Sybil and collusion. Consumer privacy is achieved through feedbacks. In order to protect cloud services from malicious users reviews can be filtered.

Keywords : Trust as a Service, Trust Assessment, Cloud Environment, Trust Management Service, Platform-as-Service, Software-as-Service, Infrastructure-as-Service, SOA, EC2, Collusion attacks

I. INTRODUCTION

Cloud computing is model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. They are divided into three categories namely Infrastructure-as-Service(IaaS), Platform-as-Service(PaaS) and Software-as-Service(SaaS).A cloud service has distinct characteristics that differentiate from traditional hosting. In this user can have as much or little service which is managed by the cloud service provider. The main advantage of cloud is cost saving.The primary disadvantage is security. Cloud computing is used by many software industries. Since the security is not provided in the cloud, many companies adopt their unique security structure. Data stored in the cloud is accessible to everyone so security is not guaranteed.It is noted that data owners lose ultimate control over the fate of their outsourced data; thus, the correctness, availability and integrity of the data are being put at risk. On the one hand, the cloud service is usually faced with a broad range of internal/external adversaries, who would maliciously delete or corrupt users' data.Security and privacy are thus very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced.cloud computing is receiving a lot of attention from both academic and industrial worlds. In cloud computing, users can outsource their computation and storage to servers (also called clouds) using Internet. Clouds can provide several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure). The risk of security is growing wide range in cloud computing. SOA and Web services are one of the most important enabling technologies for cloud computing in the sense that resources (e.g., infrastructures, platforms, and software) are exposed in clouds as services In particular, the trust management service spans several distributed nodes that expose interfaces so that users can give their feedbacks or inquire the trust results.

II. METHODS AND MATERIAL

1. Related Works

Here, we discuss the related work and presents the contribution of the trust assessment and accountability

A. Trust Assessment

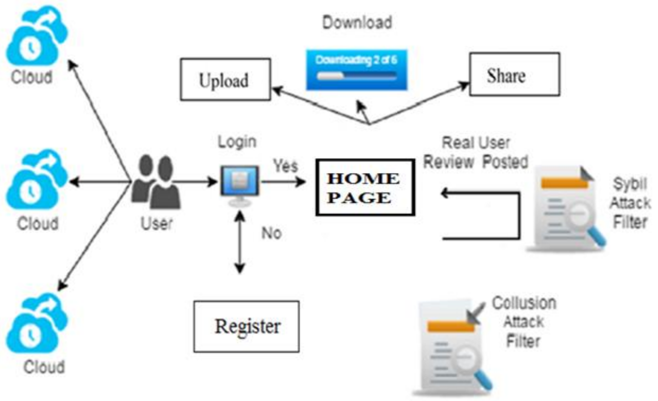
Trust assessment is an abstract system that processes symbolic representations of social trust, usually to aid automated decision-making process. Such representations, e.g. in a form of cryptographic credentials, can link the abstract system of trust management with results of trust assessment. Trust assessment is popular in implementing information security, specifically access control policies.The concept of trust assessment has been introduced by Matt Blaze to aid the automated verification of actions against security policies. In this concept, actions are allowed if they demonstrate sufficient credentials, irrespective of their actual identity, separating symbolic representation of trust from the actual person. Trust assessment can be best illustrated through the everyday experience of tickets. One can buy a ticket that entitles him e.g. to enter the stadium. The ticket acts as a symbol of trust, stating that the bearer of the ticket has paid for his seat and is entitled to enter. However, once bought, the ticket can be transferred to someone else, thus transferring such trust in a symbolic way. At the gate, only the ticket will be checked, not the identity of a bearer.

B. Accountability

The obligation of an individual or organization to account for its activities, accept responsibility for them, and to disclose the results in a transparent manner. It also includes the responsibility for money or other entrusted property accountability is answerability, blame worthiness, liability, and the expectation of account-giving. As an aspect of governance, it has been central to discussions related to problems in the public sector, nonprofit and private(corporate) and individual contexts.

2. Architecture of Trust Management Service(TMS)

It will check the user is valid or not the User get the key value the .Also known as collusive malicious feedback behaviors, such attacks occur when several vicious users collaborate together to give numerous misleading feedbacks to increase the trust result of cloud services a self-promoting attack or to decrease the trust result of cloud services a slandering attack This type of malicious behavior can occur in a non-collusive way where a particular malicious user gives multiple misleading feedbacks to conduct a self-promoting attack or a slandering attack.



Sybil Attacks. Such an attack arises when malicious users exploit multiple. We assume a transaction-based feedback where all feedbacks are held in TMS to give numerous misleading feedbacks (e.g., producing a large number of transactions by creating multiple virtual machines for a short period of time to leave fake feedbacks) for a self-promoting or slandering attack.

3. Algorithm

Trust Management Service (TMS)

A trust management service (TMS) provides an interface between users and cloud services for effective trust management.However,the availability of TMS is a difficult problem due to the unpredictable number of users and the highly dynamic nature of the cloud environment.

4. Consumers Privacy

The adoption of cloud computing raise privacy concerns.Consumers can have dynamic interactions with cloud providers, which may involve sensitive

information. There are several cases of privacy breaches such as leaks of sensitive information (e.g., date of birth and address) or behavioral information (e.g., with whom the consumer interacted, the kind of cloud services the consumer showed interest, etc.). Undoubtedly, services which involve consumers' data (e.g., interaction histories)
should preserve their privacy.

5. Modules

- Cloud Advertisement
- Best Cloud Selection, Account Creation
- File Sharing in Inter cloud users
- Review posted on all Users
- Real user command only posted
- Admin Monitoring

Cloud Advertisement

The important role for the advertisement to the best cloud providers. This module has created for the security purpose. In this webpage we have to select any cloud providers. It is different cloud providers for each advertisement to the best reviews based on the consumer. All cloud providers to upload, download share document to the end users.

Best Cloud Selection, Account Creation

This module for select best cloud providers to the consumer based on reviews and provide large facility to users. One cloud free storage for 500 MB another cloud 800 MB so best on the either one or two is best. So easy select best cloud providers and more facility to provide on the best select.

File Sharing in Inter cloud users

This is the module for sharing and uploads data process. It easy to generate each file attached one key and send inter cloud users. It easy to store and retrieve data securely. And send the all friends data share in with in single seconds. So time reduce for compare with other clouds.

Review posted on all Users

In this module we give provide post on command all user in any clouds. So review means positive and negative all commands posted to the all clouds. So any customer new entering to choose any clouds based on the reviews. So review real user only provide that is good to the commands.

Real user command only posted

In this module summarization is important to we commands on only real user provides. 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 credibility. However, the number of feedbacks is not enough in determining the credibility of trust feedbacks. fake user reviews will not be post in the homepage.

Admin Monitoring

In this module we find to collusion and Sybil attacks find easy. Also known as collusive malicious feedback behaviors, such attacks occur when several vicious users collaborate together to give numerous misleading feedbacks to increase the trust result of cloud services a self-promoting attack or to decrease the trust result of cloud services a slandering attack It is not unusual that a cloud service experiences attacks from its users. Attackers can disadvantage a cloud service by giving multiple misleading feedbacks (i.e., collusion attacks) or by creating several accounts (i.e., Sybil attacks). Indeed, the detection of such malicious behaviors poses several challenges. First, new users join the cloud environment and old users leave around the clock. This consumer dynamism makes the detection of malicious behaviors (e.g., feedback collusion) a significant accounts for a particular cloud service, which makes it difficult to detect Sybil attacks . Finally, it is difficult to predict when malicious behaviors occur(i.e., strategic vs. occasional behaviors) .

III. RESULTS AND DISCUSSION

Evaluation

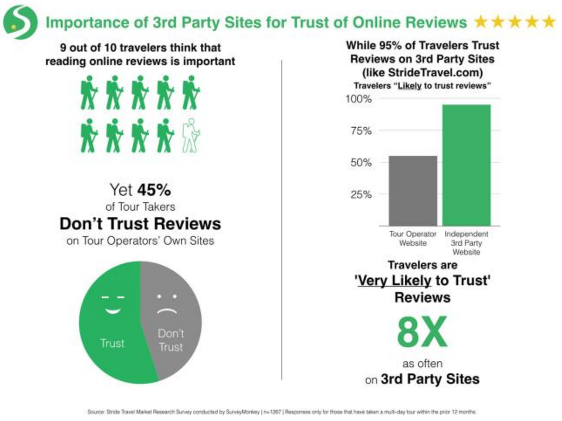
Attack Models

Collusion attacks : Also known as collusive malicious feedback behaviors, such attacks occur when several vicious users collaborate together to give numerous misleading feedbacks to increase the trust result of cloud services (i.e., a self-promoting attack) or to decrease the trust result of cloud services (i.e., a slanderingattack). This type of malicious behavior can occur in a non-collusive way where a particular malicious user gives multiple misleading feedbacks to conduct a self-promoting attack or a slandering attack.

Sybil attacks: Such an attack arises when malicious users exploit multiple identities to give numerous misleading feedbacks (e.g., producing a large number of transactions by creating multiple virtual machines for a short period of time to leave fake feedbacks) for a self-promoting or slandering attack. It is interesting to note that attackers can also use multiple identities to disguise their negative historical trust records (i.e., whitewashing attacks).

IV.CONCLUSION AND FUTURE WORK

We conclude that Trust Management Algorithm is efficient algorithm than Identity Management Algorithm based on trust result. It also provides an interface between users and cloud services for effective trust management. As an enhancement, prediction of fake reviews can be done by blocking fake users. An application which can be used by cloud providers in order to predict the risk by themselves.



V. REFERENCES

[1] Talal H. Noor, Quan Z. Sheng, Lina Yao,Schahram Dustdar, Anne H.H. Ngu, "CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services" 2016.

[2] T. Dillon, C. Wu, and E. Chang, "Cloud computing: Issuesandchallenges" in Proc. IEEE 24th Int. Conf. Adv. Inf. Netw. Appl.,2010, pp. 27–33.

[3] Georgia Athanasiou, Georgios Mantas, Maria-Anna Fengou and Dimitrios Lymberopoulos, "Towards Personalization of Trust Management Service forUbiquitous Healthcare Environment"2014.

[4] J. Huang and D. M. Nicol"Trust mechanisms for cloudcomputing" J. Cloud Comput., vol. 2, no. 1, pp. 1–14, 2013.

[5] Ivona Brandic, Schahram Dustdar, Tobias Anstett, David Schumm, Frank Leymann , "Compliant Cloud Computing (C3): Architecture and Language Support for User-driven Compliance Management in Clouds",2010.

[6] Jia Guo, lng-Ray Chen,Jeffrey J.P. Tsai,Hamid AlHamadi"AHierarchicalCloud Architecture for Integrated Mobility, Service, and Trust Management of Service-Oriented IoT Systems"2016.

[7] Martin Kuehnhausen, Victor S. Frost and Gary J. Minden, "Framework for Assessing the Trustworthiness of Cloud Resources",2012.

[8] T. H. Noor, Q. Z. Sheng, A. H. Ngu, A. Alfazi, and J. Law"CloudArmor: A platform for credibility-based trust managementof cloud services" in Proc. 22nd ACM Conf. Inf. Knowl. Manage.,2013, pp. 2509–2512.

[9] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust managementof services in cloud environments: Obstacles and solutions"ACM Comput. Surv., vol. 46, no. 1, pp, 2013.

[10] S. Pearson, "Privacy, security and trust in cloud computing"in Privacy and Security for Cloud Computing, ser. Computer Communicationsand Networks. New York, NY, USA: Springer, 2013,pp. 3–42.

[11] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud" IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan./Feb.2012.

[12] Safwan Mahmud Khan and Kevin W. Hamlen. "Hatman: Intra-cloud Trust Management for Hadoop",2012.

[13] WenAn Tan, Yong Sun, Ling Xia Li, GuangZhen Lu, and Tong Wang "A Trust Service-Oriented Scheduling Model for Workflow Applications in Cloud Computing",2013.

[14] L. Yao and Q. Z. Sheng, "Particle filtering based availability prediction for web services" in Proc. 9th Int. Conf. Service-Oriented Comput., 2011, pp. 566–573.

[15] Zhongxue YANG, Yingjie YANG, Xiaolin QIN, Tarjana YAGNIK "A Hybrid Trust Service Architecture for Cloud Computing",2013.