ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

Trust Management of Cloud Services Using Credibility Assessment Technique

Uppala Vyshnavi[1], P.Praveen Yadav[2]

M.Tech, Dept. of Computer Science and Engineering, G.Pulla Reddy Engineering College, Kurnool, AP, India [1]

Assistant Professor, Dept. of Computer Science and Engineering G.Pulla Reddy Engineering College, Kurnool, AP, India[2]

ABSTRACT: Trust management plays a significant role in the cloud computing application. Due to the dynamic nature of the cloud, continuous monitoring of the trust attributes is highly essential to enforce Service-Level Agreement (SLA) between the user and service provider. Existing access control techniques cannot satisfy the security prerequisites of the cloud environment. Trust is one of the most concerned obstacles for the adoption and growth of cloud computing. Although several solutions have been proposed recently in managing trust feedbacks in cloud environments, how to determine the credibility of trust feedbacks is mostly neglected. In this project the system proposed a Cloud Armor, a reputation-based trust management framework that provides a set of functionalities to deliver Trust as a Service (TaaS). “Trust as a Service” (TaaS) framework to improve ways on trust management in cloud environments. It is important to identify the feedback base attacks because less submission of fake feedbacks can also compromise the whole trustworthiness of service provider. The approaches have been validated by the prototype system and experimental results.

KEYWORDS: Cloud Computing, Trust Management, Malicious Feedback

I. INTRODUCTION

Cloud Computing has been emerged as new computing way which involves two main players: Cloud service providers and cloud end-users. There are several definitions proposed to define exactly what is cloud computing by different authors. Cloud computing is a relatively new business model in the computing world. According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [7]."

In the cloud environment, the detection of malicious behaviors poses several challenges. Firstly, 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 challenge. Secondly, users may have multiple 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).

Trust Management Service’s Availability: A trust management service (TMS) provides an interface between users and cloud services for effective trust management. However, guaranteeing the availability of TMS is a difficult problem due to the unpredictable number of users and the highly dynamic nature of the cloud environment. Approaches that require understanding of users’ interests and capabilities through similarity measurements or operational availability measurements (i.e., uptime to the total time) are inappropriate in cloud environments. TMS should be adaptive and highly scalable to be functional in cloud environments.

In this paper, we overview the design and implementation of the Trust as a Service (TaaS) framework. This framework helps distinguish between the credible and the malicious trust feedbacks through a credibility model. In a nutshell, the salient features of the TaaS framework are:

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

i)Zero-Knowledge Credibility Proof Protocol (ZKC2P): We introduce ZKC2P preserves the consumers' privacy and enables the TMS to prove the credibility of a particular consumer's feedback. The Identity Management Service (IdM) helps TMS in measuring the credibility of trust feedbacks.
ii) A Credibility Model: we develop a credibility model that not only distinguishes between trust feedbacks from experienced cloud service consumers and from amateur cloud service consumers, but also considers the majority consensus of feedbacks; iii) Distributed Trust Feedback Assessment and Storage: to avoid the drawbacks of centralized architectures, our trust management service allows trust feedback assessment and storage to be managed distributively.

II. RELATED WORK

According to Hatman: Intra-Cloud Trust Management for Hadoop - S. M. Khan and K. W. Hamlen, the authors quoted on Data and computation integrity and security are major concerns for users of cloud computing facilities. Many production-level clouds optimistically assume that all cloud nodes are equally trustworthy when dispatching jobs; jobs are dispatched based on node load, not reputation. This increases their vulnerability to attack, since compromising even one node suffices to corrupt the integrity of many distributed computations. This paper presents and evaluates the first full-scale, data-centric, reputation-based trust management system for Hadoop clouds. Hatman dynamically assesses node integrity by comparing job replica outputs for consistency. This yields agreement feedback for a trust manager based on EigenTrust. Low overhead and high scalability is achieved by formulating both consistency checking and trust management as secure cloud computations; thus, the cloud's distributed computing power is leveraged to strengthen its security. Experiments demonstrate that with feedback from only 100 jobs, Hatman attains over 90% accuracy when 25% of the Hadoop cloud is malicious.
According to Privacy, Security and Trust in Cloud Computing - S. Pearson, the authors quoted on, Cloud computing refers to the underlying infrastructure for an emerging model of service provision that has the advantage of reducing cost by sharing computing and storage resources, combined with an on-demand provisioning mechanism relying on a pay-per-use business model. These new features have a direct impact on information technology (IT) budgeting but also affect traditional security, trust and privacy mechanisms. The advantages of cloud computing—its ability to scale rapidly, store data remotely and share services in a dynamic environment—can become disadvantages in maintaining a level of assurance sufficient to sustain confidence in potential customers. Some core traditional mechanisms for addressing privacy (such as model contracts) are no longer flexible or dynamic enough, so new approaches need to be developed to fit this new paradigm. In this chapter, we assess how security, trust and privacy issues occur in the context of cloud computing and discuss ways in which they may be addressed.
According to Trust Mechanisms for Cloud Computing - J. Huang and D. M. Nicol, the authors quoted on, Trust is a critical factor in cloud computing; in present practice it depends largely on perception of reputation, and self assessment by providers of cloud services. We begin this paper with a survey of existing mechanisms for establishing trust, and comment on their limitations. We then address those limitations by proposing more rigorous mechanisms based on evidence, attribute certification, and validation, and conclude by suggesting a framework for integrating.
According to A View of Cloud Computing - M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, the authors quoted on, Cloud computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1,000 servers for one hour costs no more than using one server for 1,000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT. As a result, cloud computing is a popular topic for blogging and white papers and has been featured in the title of workshops, conferences, and even magazines. Nevertheless, confusion remains about exactly what it is and when it's useful, causing Oracle's CEO Larry Ellison to vent his frustration: "The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do.... I don't understand what we would do differently in the light of cloud computing other than change the wording of some of our ads."

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

III. METHODOLOGIES

A. DETECTION OF SERVICE

This layer consists of different users who use cloud services. For example, a new startup that has limited funding can consume cloud services. Interactions for this layer include: i) service discovery where users are able to discover new cloud services and other services through the Internet, ii) trust and service interactions where users are able to give their feedback or retrieve the trust results of a particular cloud service, and iii) registration where users establish their identity through registering their credentials in IdM before using TMS.

B. TRUST COMMUNICATION

In a typical interaction of the reputation based TMS, a user either gives feedback regarding the trustworthiness of a particular cloud service or requests the trust assessment of the service 1. From users' feedback, the trust behavior of a cloud service is actually a collection of invocation history records, represented by a tuple H=(C, S, F, T f), where C is the user's primary identity, S is the cloud service's identity, and F is a set of Quality of Service (QOS) feedbacks (i.e., the 5 star rating).

Fig 1. Feedback of a cloud service.

C. IDM REGISTRATION

The system proposes to use the Identity Management Service (IdM) helping TMS in measuring the credibility of a consumer's feedback. However, processing the IdM information can breach the privacy of users. One way to preserve privacy is to use cryptographic encryption techniques. However, there is no efficient way to process encrypted data without breaching the privacy of users.

D. THE CLOUD SERVICE CONSUMER LAYER.

Finally, this layer consists of different users who use cloud services. For example, a new startup that has limited funding can consume cloud services (e.g., hosting their services in Amazon S3). Interactions for this layer include: i) service discovery where users are able to discover new cloud services and other services through the Internet, ii) trust and service interactions where users are able to give their feedback or retrieve the trust results of a particular cloud service, and iii) registration where users establish their identity through registering their credentials in IdM before using TMS. Our framework also exploits a Web crawling approach for automatic cloud services discovery, where cloud services are automatically discovered on the Internet and stored in a *cloud services repository*. Moreover, our framework contains an *Identity Management Service* (see Figure 2) which is responsible for the *registration* where users register their credentials before using TMS and proving the credibility of a particular consumer's feedback.

IV. ATTACK MODELS

Collusion Attacks

In collusion attacks, attackers seek to falsely augment their own reputation. Such attacks are only possible in systems that consider positive feedback in the formulation. Fundamentally, this is an attack against the formulation, but attackers may also exploit weaknesses in the calculation or dissemination dimensions to falsely increase reputation metric values. collusion attacks can be performed by attacker alone or organized in groups of collaborating identities. One very basic form of the attack occurs when an attacker fabricates fake positive feedback about itself or modifies its own reputation during the dissemination. Systems that lack data authentication and integrity are vulnerable

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

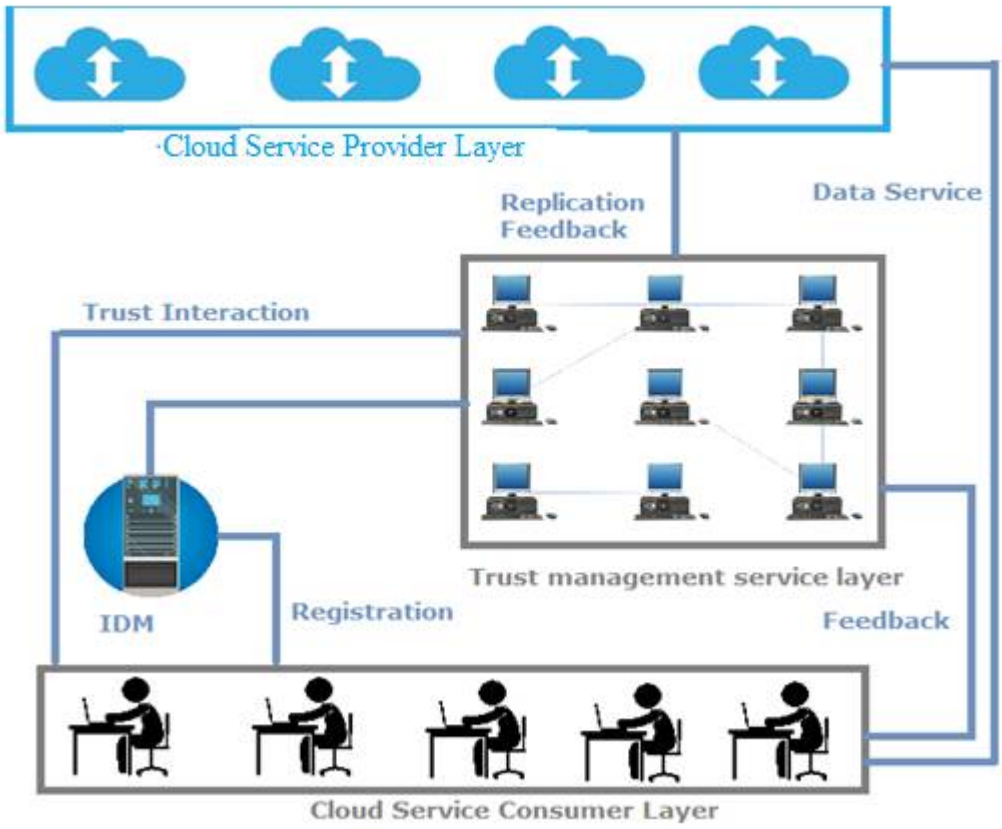

Fig. 2. Architecture of the CloudArmor Trust Management Framework

to such attacks as they are not able to discern between fabricated and legitimate feedbacks. However, even if source data is authenticated, self promotion attacks are possible if disparate identities or a single physical identity acquiring multiple identities through a collude to promote each other. Systems that do not require participants to provide proof of interactions which result in positive reputations are particularly vulnerable to this attack. To perform the attack, colluding identities mutually participate in events that generate real feedback, resulting in high volumes of positive feedback for the colluding participants.

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).

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

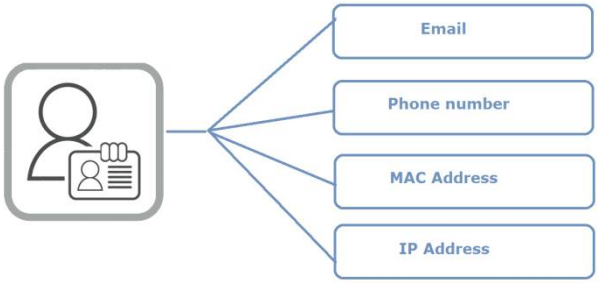

Fig 3. Identities of Sybil Attacks

V. EXPERIMENTAL RESULTS

Fig 4. Cloud server files by user.

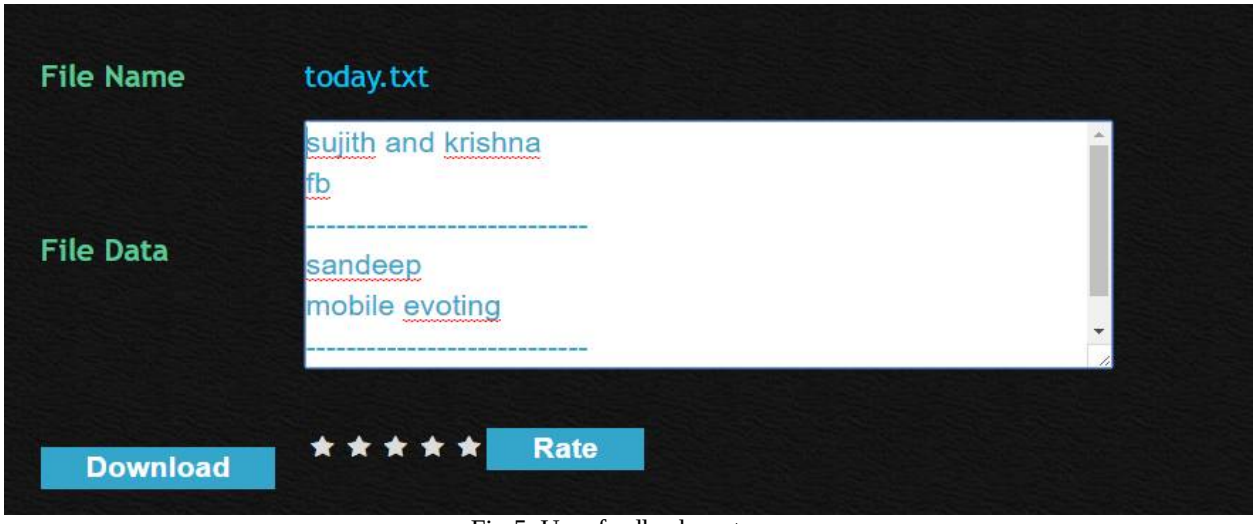

Fig 5. User feedback system.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

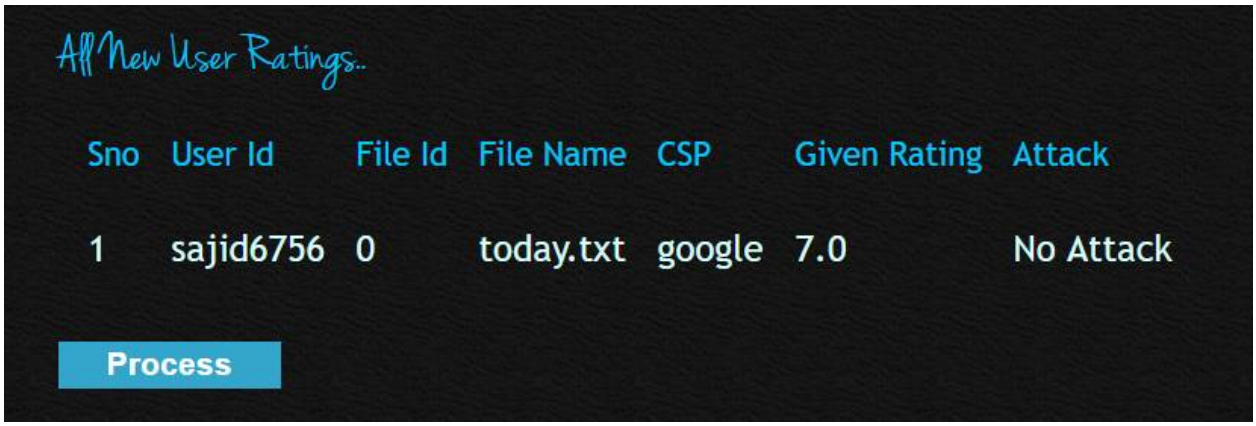

Fig 6. At Trust Management without attack

Fig 7. At Trust Management with Sybil Attack

Fig 8. At Trust Management with Collusion Attack

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

VI. CONCLUSION

Given the highly dynamic, distributed, and nontransparent nature of cloud services, managing and establishing trust between cloud service users and cloud services remains a significant challenge. Cloud service users' feedback is a good source to assess the overall trustworthiness of cloud services. However, malicious users may collaborate together to i) disadvantage a cloud service by giving multiple misleading trust feedbacks (i.e., collusion attacks) or ii) trick users into trusting cloud services that are not trustworthy by creating several accounts and giving misleading trust feedbacks (i.e., Sybil attacks). In this system, we have presented novel techniques that help in detecting reputation based attacks and allowing users to effectively identify trustworthy cloud services. In particular, we introduce a credibility model that not only identifies misleading trust feedbacks from collusion attacks but also detects Sybil attacks no matter these attacks take place in a long or short period of time (i.e., strategic or occasional attacks respectively). We also develop an availability model that maintains the trust management service at a desired level. We have collected a large number of consumer's trust feedbacks given on real-world cloud services to evaluate our proposed techniques. The experimental results demonstrate the applicability of our approach and show the capability of detecting such malicious behaviors. There are a few directions for our future work. We plan to combine different trust management techniques such as reputation and recommendation to increase he trust results accuracy. Performance optimization of the trust management service is another focus of our future research work.

REFERENCES

[1] A. Birolini, Reliability Engineering: Theory and Practice. Springer2010.
[2] C. Dellarocas, "The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms," Management Science, vol. 49, no. 10, pp. 1407–1424, 2003.
[3] E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy-preserving Digital Identity Management for Cloud Computing," IEEE Data Eng. Bull, vol. 32, no. 1, pp. 21–27, 2009.
[4] 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.
[5] Jingwei Huang and David M Nicol, Trust mechanisms for cloud computing, April 2013
[6] J. Huang and D. M. Nicol, "Trust Mechanisms for Cloud Computing," Journal of Cloud Computing, vol. 2, no. 1, pp. 1–14, 2013.
[7] Kai Hwang Deyi Li, Trusted Cloud Computing with Secure Resources and Data Coloring, Sept.-Oct. 2010
[8] K. Hoffman, D. Zage, and C. NitaRotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," ACM Computing Surveys, vol. 42, no. 1, pp. 1– 31, 2009.
[9] Lina Yao Quan Z. Sheng ZakariaMaamar, Achieving High Availability of Web Services Based on A Particle Filtering Approach, 2012
[10] R. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. Lee, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," in Proc. SERVICES'11, 2011.
[11] S. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing," in Proc. of TrustCom'11, 2011.
[12] Sheikh MahbubHabib , Sebastian Ries y, Max M• uhlh• auser, Towards a Trust Management System for Cloud Computing
[13] Siani Pearson and AzzedineBenameur, Privacy, Security and Trust Issues Arising from Cloud Computing , 2010
[14] S. M. Khan and K. W. Hamlen, "Hatman: Intra-Cloud Trust Management for Hadoop," in Proc. CLOUD'12, 2012.
[15] S. Pearson, "Privacy, Security and Trust in Cloud Computing," in Privacy and Security for Cloud Computing, ser. Computer Communications and Networks, 2013, pp. 3–42.
[16] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising From Cloud Computing," in Proc. CloudCom'10, 2010.
[17] 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.
[18] T. H. Noor, Q. Z. Sheng, A. H. Ngu, A. Alfazi, and J. Law, "CloudArmor: A Platform for Credibility-based Trust Management of Cloud Services," in Proc. of CIKM'13, 2013.
[19] T. Noor and Q. Z. Sheng, "CredibilityBased Trust Management for Services in Cloud Environments," in Proc. of ICSOC'11, 2011.
[20] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrst-edt, "A Trust Management Framework for ServiceOriented Environments," in Proc. of WWW'09, 2009.