International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 2, ISSN No. 2455-2143, Pages 139-140
Published Online December-January 2016 in IJEAST (http://www.ijeast.com)

TRUST MANAGEMENT FOR CLOUD SERVICES TO PRESERVE CONSUMER'S PRIVACY

Parashiva Murthy B M
Asistant Professor, Dept. of CSE
GSSSIETW, Mysuru, Karnataka, India

Rajath A N
Asistant Professor, Dept. of CSE
GSSSIETW, Mysuru, Karnataka, India

ABSTRACT: In cloud computing growth, the management of trust element is most challenging issue. Cloud computing has produce high challenges in security and privacy by the challenging of environments. 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 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. The approaches have been validated by the prototype system and experimental results.

Keywords: Cloud computing, trust, Obstacles, reputation, feedbacks

I. INTRODUCTION

The highly dynamic, distributed, and non-transparent nature of cloud services make the trust management in cloud environments a significant challenge. According to researchers at Berkeley, trust and security is ranked one of the top 10 obstacles for the adoption of cloud computing. Indeed Service–Level Agreements (SLAs) alone are inadequate to establish trust between cloud consumers and providers because of its unclear and inconsistent clauses. Consumers feedback is a good source to assess the overall trustworthiness of cloud services. Several researches have recognized the significance of trust management and proposed solutions to assess and manage trust based on feedbacks collected from participants, in reality; it is not unusual that a cloud service experiences malicious behaviors from its users. This project focuses on improving trust management in cloud environments by proposing novel techniques to ensure the credibility of trust feedbacks. In particular, we distinguish the following key issues of the trust management in cloud environments.

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.)

Cloud Services Protection: 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. 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.

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 user's interests and capabilities through similarity measurements or operational availability measurements are inappropriate in cloud environments. TMS should be adoptive and highly scalable to be functional in cloud environments.

In this project, trust is delivered as a service (TaaS) where TMS spans several distributed nodes to manage feedbacks in a decentralized way. We proposed some techniques to identify credible feedback from malicious ones.

II. SURVEY MADE ON METHODS FOR AUTOMATING IN DIFFERENT AREAS

Optimizing the websites by adopting many proposed system or methods is a challenging job. Manually working is a tedious job and time overhead too, hence it is very essential for automating many of the work in various fields that avoids the time consumption. The different methods discussed are as follows.

1. The Sybil Attack [8] Large scale peer-to-peer system face security threads from faulty or hostile remote computing elements. To resist these threads, many such systems employ redundancy. One approach for prevent the "Sybil Attacks" is to have a trusted agency certify identities. If distinct identities for remote entities are not established either by a explicit certification authority or by an implicit one, these systems are susceptible to Sybil attacks. This paper shows that, without a logical centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities. We assume that the attacker's resources are limited. Entities can thus issue resource demanding challenges to validated identities and entities can collectively pool the identities they have separately validated.

2. Achieving High Availability of Web Services based on a Particle Filtering Approach [9] Guaranteeing the availability of a web service is a significant challenge due to the varying number of invocation requests the web service has to handle at a time, as well as the dynamic nature of the web. Over the last few years, many works have emerged in addressing wed services availability problem. Almost all of these approaches are based on the concept of service community where web services with similar functionalities are grouped in a particle "cluster". In this paper they designed a mobile for accessing web services availability using particle filter technique, which can return precise and dynamic prediction of this availability. They introduces service availability model and the particle filter techniques , a novel approach is introduced to monitor and predict web service's availability based on particle filter techniques and also developed algorithm to filter web services from service communities for efficient service selection.

3. On Resampling Algorithms for Particle Filters[10]. In this paper a comparison is made between four frequently encountered resampling algorithms for particle filters. A theoretical framework is introduced to be able to understand and explain the difference between the resampling algorithms. This facilitates a comparison of the algorithms with respect to their resampling quality and computational complexity. They reduce the computational complexity while giving identical or perhaps slightly improved particle filter estimates. Additionally, from a uniform distribution perspective systematic resampling is theoretically superior.

III. PROPOSED METHOD

Cloud service user's feedback is a good source to assess the overall trustworthiness of cloud services. In this project, we are presenting novel techniques that helps in detecting reputation based attacks and allow users to effectively identify trustworthy cloud services. A credibility model that not only identifies misleading trust feedbacks from collusion attacks also detects Sybil attacks. Also an availability model that maintains the TMS at a desired level. We proposed a multi-faced Trust Management (TM) cloud computing to help the cloud service users to identify trustworthy cloud services.

IV. CONCLUSIONS

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 paper, 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. The experimental results demonstrate the applicability of our approach and show the capability of detecting such malicious behaviors.Performance optimization of the trust management service is another focus of our future research work.

V. REFERENCES

[1]. S. M. Khan and K. W. Hamlen, "Hatman: Intra-Cloud Trust Management for Hadoop," in Proc. CLOUD'12, 2012.

[2]. T.H.NoorandQ.Z.Sheng,"Trust as a Service: A Framework for Trust Management in Cloud Environments," in Proc. of WISE'11, 2011.

[3]. 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.

[4]. Yaser Ghanam, Jennifer Ferreira, and Frank Maurer, "Emerging Issues & Challenges in Cloud Computing"

[5]. 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.

[6]. Dr.Sandeep Sharma & Navdeep Kaur Khiva, "Secure Cloud Architecture for Preserving Privacy in Cloud Computing".

[7].Ali Gholami and Erwin Laure, "Security and Privacy of Sensitive Data in Cloud Computing: A Survey of recent developments".

[8]. J. R. Douceur, "The Sybil Attack," in Proc. of IPTPS'02, 2002.

[9]. Lina Yao,Quan z. Shengf,Zakaria maamer, "Achieving High Availability of Web Services based on a Particle Filtering Approach".

[10]. Jeroen D. Hol, Thomas B. Schon,FredrikGustafsson, "On Resampling Algorithms for Practicle Filters".