International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

Supporting Reputation-based Trust Management for Different Cloud Services in Cloud: Cloud Armor

Vimala Thulluri & Siva Krishna
[1]PG Scholar, Dept of CSE, MalineniLakshmaiah Engineering College, Singarayakonda, Prakasam(Dt), AP, India.
[2]Asst Professor, Dept of CSE, MalineniLakshmaiah Engineering College, Singarayakonda, Prakasam(Dt), AP, 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 changing 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 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. The approaches have been validated by the prototype system and experimental results.*

Keywords: *Cloud computing, Trust, Obstacles, Reputation, Feedbacks.*

1. 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 researchers 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 (e.g., collusion or Sybil attacks) from its users. This paper focuses on improving trust management in cloud environments by proposing novel ways 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.) . Undoubtedly, services which involve consumers' data (e.g., interaction histories) should preserve their privacy. 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 (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.

2.THE FRAMEWORK

We propose a framework using the Service Oriented Architecture (SOA) to de-liver trust as a service. SOA and Web services are one of the most important enabling technologies for cloud computing in the sense that resources (e.g., soft-ware, infrastructures, and platforms) are exposed in clouds as services [6,16]. In particular, our framework uses Web services to span several distributed TMS nodes that expose interfaces so that trust participants (i.e., the cloud service con-sumers) can give their trust feedbacks or inquire about the trust results based on SOAP or REST [15] messages. Figure 1 depicts the framework, which consists of three different layers, namely the Cloud Service Provider Layer, the TrustManagement Service Layer, and the Cloud Service Consumer Layer. The Cloud Service Provider Layer. This layer consists of different cloud service providers who provide cloud services. The minimum indicative feature that every cloud service provider should have is to provide the infrastructure as a service (i.e., the cloud provider should have a data center that provides the storage, the process, and the communication).

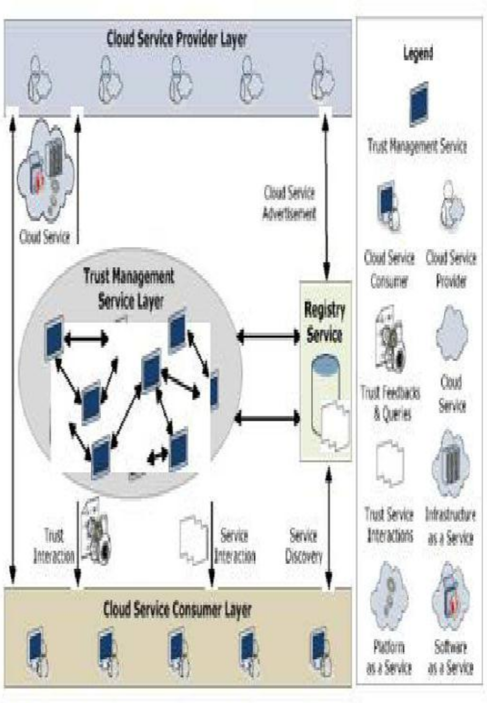

Fig. 1. Architecture of the Trust as a Service Framework

– The Trust Management Service Layer. This layer consists of several dis-tributed TMS nodes that expose interfaces so that cloud service consumers can give their trust feedbacks or inquire about the trust results represents. Our framework also contains a Registry Service (see Figure 1) that has several responsibilities including i) Service Advertisement: both cloud service providers and the TMS are able to advertise their services through the Service Registry; ii) Service Discovery: the TMS and cloud service consumers are able to access the Service Registry to discover services.

A. TRUST FEEDBACK COLLECTION AND ASSESSMENT

In our framework, the cloud service trust behavior is represented by a collection of invocation history records denoted as H. Each cloud service consumer c holds her point of view regarding the trustworthiness of a specific cloud service s which is managed by the assigned TMS. H is represented in a tuple that consists of the cloud consumer primary identity C, the cloud service identity S, a set of trust feedbacks F and the aggregated trust feedbacks weighted by the credibility F_c , i.e., H = (C, S, F, F_c). Each trust feedback in F is represented in numerical form in which the range of the normalized feedback is [0, 1], where 0, +1, and 0.5 ~~means negative,~~ positive, and neutral respectively. Whenever a cloud consumer inquires the TMS about the trustworthiness of a cloud service s, the trust result (Tr(s)), is calculated using: whereV(s) is all trust feedbacks given to the cloud service s and |V(s)| represents the length of the V(s). F_c (l, s) are trust feedbacks from the lth cloud consumer weighted by the credibility.

The TMS distinguishes between credible trust feedbacks and malicious trust feedbacks through assigning the Cloud Consumer's Experience aggregated weights Exp(l) to trust feedbacks F(l, s) as shown in Equation 2, where the result $F_c(l, s)$ is held in the invocation history record h and updated in the assigned TMS.

$$F_C(l, s) = F(l, s)*Exp(l) \qquad (2)$$

3.CREDIBILITY MODEL

There is a considerable possibility that the TMS receives inaccurate or even malicious trust feedbacks from amateur cloud service consumers (e.g., who lackexperience) or vicious cloud service consumers (e.g., who submit lots of negative feedbacks to disadvantage a particular cloud service). To overcome these issues, we propose a credibility model, which is centered on the cloud consumer's experience. To differentiate between expert and amateur cloud service consumers,we consider the Majority Consensus and the Cloud Consumer's Capability.

Majority Consensus.It is well-known that the majority of people usually agreewith experts' judgments about what is good [4]. Similarly, we believe that the majority of cloud consumers agree with Expert cloud service consumers' judg-ments. In other words, any cloud service consumer whose trust feedback is close to the majority of trust feedbacks is considered an Expert Cloud Service Con-sumer(ECSC), or an Amateur Cloud Service Consumer (ACSC) otherwise. Inorder to measure how close the cloud service consumer's trust feedbacks to the majority (i.e., the Majority Consensus (J (c)) which is calculated as follows: the numerator represents the mean of the majority trust feedbacks given by other cloud service consumers (F(l, k)) (i.e., the l^{th} cloud service consumer, except the cloud service consumer c) to the k^{th} cloud service.

Cloud Service Consumer's Capability.It is a common sense that older peopleare likely to be more experienced in judging things than younger people [14]. However, this is only true if the older people have experienced considerable number of judging practices. As a result, we believe that "older" cloud service consumers who have many judging practices are likely to be more experienced and capable. A cloud service consumer's capability (B) is measured as follows:whereVc(c) represents all good feedbacks (i.e., feedbacks which are close to the majority) given by the cloud service consumer c. Ag(c) denotes the virtual Age of a certain cloud service consumer, measured in days since the registration in the TMS. The idea behind adding the number 1 to this ratio is to increase the value of a cloud service consumer experience based on B(c) result. In other words, we use B(c) as a reward factor. The higher B(c) is, the more experienced a cloud service consumer is. It should be noted that even if a malicious cloud service consumer attempts to manipulate the capability result, the capability result will not exceed 2.

Based on the specified cloud service consumer's experience factors (i.e., B(c) and J (c)), the TMS distinguishes between ECSC and ACSC through assigning the cloud service consumer's Experience aggregated weights Exp(c) to each of the cloud consumers' trust feedbacks as shown in Equation 2. Exp(c) is calculated as follows:

$$Exp(c) = \frac{\beta * B(c) + \mu * J(c)}{\Lambda} \quad (5)$$

whereβ and B(c) denote the cloud service consumer's Capability factor's normal-ized weight and the factor's value respectively. The second part of the equation represents the Majority Consensus factor where μ denotes the factor's normal-ized weight and J (c) denotes the factor's value. λ represents the number of fac-tors used to calculate Exp(c) (e.g., if we only consider cloud service consumer's capability, λ = 1; if we consider both cloud service consumer's capability and majority consensus, λ = 2). We use J (c) as a penalty factor (i.e., because J (c) ranges [0,1] as described in equation 3). The lower J (c) is, the lower the experience of the cloud service consumer c is. However, B(c) is used as a reward factor (i.e., because B(c) ranges [1, 2] as described in equation 4). Higher B(c) means more experienced of a cloud service consumer. It is worth mentioning that our credibility is dynamic and is able to detect behavior changes. For example, if a cloud service consumer behaves good for a period of time (e.g., to gain credibility) and then starts misbehaving, J (c) can detect such behavior through applying the standard deviation.

4.DISCUSSIONS

Trust management is one of the critical issues in cloud computing and a very active research area [10,12,8,2]. For instance, Hwang et al. [8] proposed a security-aware cloud architecture where trust negotiation and data coloring techniques are used to support the cloud service provider perspective. The cloud service consumer's perspective is supported using the trust-overlay networks to deploy a reputation-based trust management. Brandic et al. [2] proposed a central-ized approach for compliance management in cloud environments that supports the cloud service consumer's perspective using compliant management to help the cloud service consumers in selecting proper cloud services. Unlike previous works that use centralized architecture, we present a credibility model support-ing distributed trust feedback assessment and storage. This credibility model also distinguishes between trustworthy and malicious trust feedbacks. the feedback [18]. However, this ap-proach is inappropriate in cloud environments because peers give and receive services and they are evaluated on that base. In other words trust results are used to distinguish between credible and malicious feedbacks.

5.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 paper, we have presented novel techniques that help in detecting reputationbased 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 (i.e., over 10,000 records) 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 the trust results accuracy. Performance optimization of the trust management service is another focus of our future research work.

REFERENCES

a. Armbrust, M., et al.: A View of Cloud Computing. Communiaction of the ACM 53(4), 50–58 (2010)

b. Brandic, I., Dustdar, S., Anstett, T., Schumm, D., Leymann, F., Konrad, R.: Com-pliant Cloud Computing (C3): Architecture and Language Support for User-Driven

[2] Compliance Management in Clouds. In: Proc. of IEEE CLOUD 2010, Miami, Florida, USA (July 2010)

a. Buyya, R., Yeo, C., Venugopal, S.: Market-oriented Cloud Computing: Vision, Hype, and Reality for Delivering it Services as Computing Utilities. In: Proc. of IEEE HPCC 2008, Dalian, China (September 2008)

b. Child, I.: The Psychological Meaning of Aesthetic Judgments. Visual Arts Research 9(2(18)), 51–59 (1983)

c. Conner, W., Iyengar, A., Mikalsen, T., Rouvellou, I., Nahrstedt, K.: A Trust Management Framework for Service-Oriented Environments. In: Proc. of WWW 2009, Madrid, Spain (April 2009)

d. Dillon, T., Wu, C., Chang, E.: Cloud Computing: Issues and Challenges. In: Proc. of AINA 2010, Perth, Australia (April 2010)

e. Hoffman, K., Zage, D., Nita-Rotaru, C.: A Survey of Attack and Defense Techniques for Reputation Systems. ACM Computing Surveys 42(1), 1–31 (2009)

f. Hwang, K., Li, D.: Trusted Cloud Computing with Secure Resources and Data Coloring. IEEE Internet Computing 14(5), 14–22 (2010)

g. Jøsang, A., Quattrociocchi, W.: Advanced Features in Bayesian Reputation Sys-tems. In: Fischer-H¨ubner, S., Lambrinoudakis, C., Pernul, G. (eds.) TrustBus 2009. LNCS, vol. 5695, pp. 105–114. Springer, Heidelberg (2009)

[3] Krautheim, F., Phatak, D., Sherman, A.: Introducing the Trusted Virtual Environment Module: A New Mechanism for Rooting Trust in Cloud Computing. In: Acquisti, A., Smith, S.W., Sadeghi, A.-R. (eds.) TRUST 2010. LNCS, vol. 6101, pp. 211–227. Springer, Heidelberg (2010)

[4] Malik, Z., Bouguettaya, A.: RATEWeb: Reputation Assessment for Trust Establishment Among Web services. The VLDB Journal 18(4), 885–911 (2009)

[5] Manuel, P., ThamaraiSelvi, S., Barr, M.E.: Trust Management System for Grid and Cloud Resources. In: Proc. of ICAC 2009, Chennai, India (December 2009)

[6] Massa, P., Avesani, P.: Trust Metrics in Recommender Systems. In: Computing with Social Trust. Human-Computer Interaction Series. Springer, Heidelberg (2009)

[7] Roosevelt, E.: Facing the problems of youth. The P.T.A. magazine: National Parent-Teacher Magazine 29(30), 1–6 (1935)

[8] Sheth, A.P., Gomadam, K., Lathem, J.: SA-REST: Semantically Interoperable and Easier-to-Use Services and Mashups. IEEE Internet Computing 11(6), 84–87 (2007)

[9] Wei, Y., Blake, M.B.: Service-oriented Computing and Cloud Computing: Challenges and Opportunities. IEEE Internet Computing 14(6), 72–75 (2010)

[10] Weng, J., Miao, C., Goh, A.: Protecting Online Rating Systems from Unfair Ratings. In: Katsikas, S.K., L´opez, J., Pernul, G. (eds.) TrustBus 2005. LNCS, vol. 3592, pp. 50–59. Springer, Heidelberg (2005)

[11] Xiong, L., Liu, L.: Peertrust: Supporting Reputation-based Trust for Peer-to-Peer Electronic Communities. IEEE TKDE 16(7), 843–857 (2004)

Author's profile

VIMALA THULLURI received B.Tech in Information Technology from Malineni Lakshmaiah Engineering College affiliated to the Jawaharlal Nehru technological university Kakinada in 2014, and pursing M. Tech in Computer Science and Engineering from Malineni Lakshmaiah Engineering College affiliated to the Jawaharlal Nehru technological university Kakinada in

SIVA KRISHNA is working as asst professor in CSE department in Malineni Lakshmaiah Engineering College, Singarayakonda, Prakasam(Dt), AP,