International Journal of Computer Sciences
June'2017 Issue
ISSN Number: 4142 3453

Support Reputation-Based Trust Management for Cloud Services

K. Munisekhar[1] ,A. K. Puneeth Kumar[2]

[1]M.Tech (CSE)., Dept of CSE, Siddartha Educational Academy Group of Institutions, C. Gollapalle, Tirupathi,Ap.

[2]Assistant Professor, Dept of CSE, Siddartha Educational Academy Group of Institutions, C. Gollapalle, Tirupathi,Ap.

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

Index Terms- Cloud Computing, Security, Privacy, Reputation, Credibility, Credentials, Trust Management, Availability.

1. INTRODUCTION

Over the past few years, cloud computing is gaining a considerable momentum as a new computing paradigm for providing flexible services, platforms, and infrastructures on demand [1,3]. For instance, it only took 24 hours, at the cost of merely $240, for the New York Times to archive its 11 million articles (1851-1980) using Amazon Web Services1 .Given the quick adoption of cloud computing in the industry, there is a signif-icant challenge in managing trust among cloud service providers and cloud ser-vice consumers [1,3,8]. Recently, the significance of trust management is highly recognized and several solutions are proposed to assess and manage trust feed-backs collected from participants [8,5]. However, one particular problem has been mostly neglected: to what extent can these trust feedbacks be credible. Trust management systems usually experience malicious behaviors from its users. On the other hand, the quality of trust feedbacks differs from one person to another, depending on how experienced she is. This paper focuses on the cloud serviceconsumers perspective (i.e., cloud service consumers assess the trust of cloud services). In particular, we distinguish several key issues of the trust management in cloud environments including i) Trust Results Accuracy: determining the credibility of trust feedbacks is a significant challenge due to the overlapping interactions between cloud service consumers and cloud service providers. It is difficult to know how experienced a cloud consumer is and from whom malicious trust feedbacks are expected that requires extensive probabilistic computations [17,9]; ii) Trust Feedback Assessment and Storage: the trust assessment of a service in existing techniques is usually centralized, whereas the trust feedbacks come from distributed trust participants. Trust models that use centralized architectures are prone to scalability and security issues [7]. In this paper, we overview the design and implementation of the Trust as aService(TaaS) framework. This framework helps distinguish between the credi-ble and the malicious trust feedbacks through a credibility model. In a nutshell, the salient features of the TaaS framework are i) A Credibility Model: we de-velop a credibility model that not only distinguishes between trust feedbacks from experienced cloud service consumers and from amateur cloud service con-sumers, but also considers the majority consensus of feedbacks; ii) DistributedTrust Feedback Assessment and Storage: to avoid the drawbacks of centralizedarchitectures, our trust management service allows trust feedback assessment and storage to be managed distributively.

The remainder of the paper is organized as follows. The design of the TaaS framework is presented in Section 2. Details of the trust management service (TMS) including the distributed trust feedback collection and assessment are described. Section 3 describes the credibility model. Section 4 reports the imple-mentation and several experimental evaluations. Finally, Section 5 discusses the related work and provides some concluding remarks. The highly dynamic, distributed, and nontransparent 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 access 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.

II.RELATED WORK

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. Here, it provides some drawbacks are, It is not unusual that a cloud service experiences malicious behaviors from its users, It is not sure whether they can trust the cloud providers, It not convincing enough for the consumers, SLAs are not consistent among the cloud providers even though they offer services with similar functionality, Customers are not sure whether they can identify a trustworthy cloud provider only based on its SLA. 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. In particular, the system introduce an adaptive credibility model that distinguishes between credible trust feedbacks and malicious feedbacks by considering cloud service consumers' capability and majority consensus of their feedbacks. The approaches have been validated by the prototype system and experimental results.

The system proposes a framework using the Service Oriented Architecture (SOA) to deliver trust as a service. Here it includes some benefits are, It not only preserves the consumers' privacy, but also enables the TMS to prove the credibility of a particular consumer's feedback, It also has the ability to detect strategic and occasional behaviors of collusion attacks, Load balancing techniques are exploited to share the workload, thereby always

maintaining a desired availability level, This metric exploits particle filtering techniques to precisely predict the availability of each node, Cloud Armor exploits techniques to identify credible feedbacks from malicious ones [13] describe about, In this paper we assess how security, trust and privacy issues occur in the context of cloud computing and discuss ways in which they may be addressed It 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. This makes compliance with regulations related to data handling difficult to fulfill. [5] Describe about, 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 various trust mechanisms together to reveal chains of trust in the cloud. This system presents an integrated view of the trust mechanisms for cloud computing, and analyzes the trust chains connecting cloud entities. Some cloud clients cannot make decisions about employing a cloud service based solely on informal trust mechanisms. [7] describe about, The authors suggest using a trustoverlay network over multiple data centers to implement a reputation system for establishing trust between service providers and data owners. Data coloring and software watermarking techniques protect shared data objects and massively distributed software modules. These techniques safeguard multiway authentications, enable single sign-on in the cloud, and tighten access control for sensitive data in both public and private clouds. Once users move data into the cloud, they can't easily extract their data and programs from one cloud server to run on another. This leads to a data lock-in problem. [12] Describe about, the descriptions in SLAs are not consistent among the cloud providers even though the other services with similar functionality. Therefore, customers are not sure whether they can identify a trust worthy cloud provider only based on its SLA. This system provides means to identify the trustworthy cloud providers in terms of different attributes assessed by multiple sources and roots of trust information; they are not sure whether they can trust the cloud providers. [9] In this paper, we tackle these problems by exploiting particle filtering-based techniques. In particular, we developed algorithms to accurately predict the availability of Web services and dynamically maintain a subset of Web services with higher availability ready to join service compositions. Web services can be always selected from this smaller space, thereby ensuring good performance in service compositions. Unfortunately, how to provide real-time availability information of Web services is largely overlooked. I

III.METHODOLOGY

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 feedback represent several QOS parameters including availability, security, response time, accessibility, price).

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. Another way is to use anonymization techniques to process the IDM information without breaching the privacy of users. Clearly, there is a trade-off between high anonymity and utility.

D. Service Announcement and Communication

This layer consists of different cloud service providers who offer one or several cloud services, i.e., IaaS (Infrastructure as a Service), PaaS

(Platform as a Service), and SaaS (Soft-ware as a Service), publicly on the Web (more details about cloud services models and designs can be found). 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 and TMS.

IV.PROPOSED WORK

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). 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

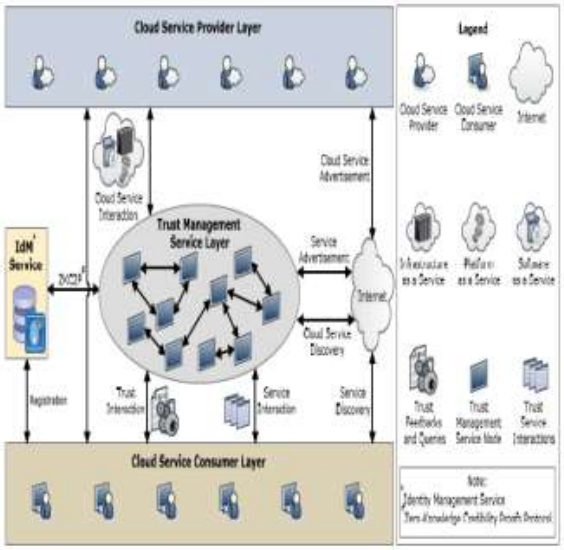

Fig.1. System Architecture.

The Cloud Service Provider Layer This layer consists of different cloud service providers who offer one or several cloud services, i.e., IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service), publicly on the Web (more details about cloud services models and designs). 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 and TMS, and cloud services advertisements where providers are able to advertise their services on the Web. B. The Trust Management Service Layer This layer consists of several distributed TMS nodes which are hosted in multiple cloud environments in different geographical areas. These TMS nodes expose interfaces so that users can give their feedback or inquire the trust results in a decentralized way. Interactions for this layer include: i) cloud service interaction with cloud service providers, ii) service advertisement to advertise the trust as a service to users through the Internet, iii) cloud service discovery through the Internet to allow users to assess the trust of new cloud services, and iv) Zero-Knowledge Credibility Proof Protocol (ZKC2P) interactions enabling TMS to customers feedback.

Cloud service users' feedback is a good source to assess the overall trustworthiness of cloud services. In this paper, we have presented novel techniques that help in detecting reputation based attacks and allowing users to effectively identify trustworthy cloud services as shown in Fig.1. 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 also develop an availability model that maintains the trust management service at a desired level.

V.RESULTS

Our implementation and experiments were developed to validate and study the performance of both the credibility model and the availability model.

A. System Implementation

The trust management service's implementation is part of our large research project, named Cloud Armor, which offers a platform for reputation-based trust management of cloud services [10]. The platform provides an environment where users can give feedback and request trust assessment for a particular cloud service. Specifically, the trust management service (TMS) consists of two main components: the Trust Data Provisioning and the Trust Assessment Function. The Trust Data Provisioning: This component is responsible for collecting cloud services and trust information. We developed the Cloud Services Crawler module based on the Open Source Web Crawler for Java (crawler4j) and extended it to allow the platform to automatically discover cloud services on the Internet. We implemented a set of functionalities to simplify the crawling process and made the crawled data more comprehensive (e.g., add Seeds (), select Crawling Domain (), add Crawling Time ()). In addition, we developed the Trust Feedbacks Collector module to collect feedbacks directly from users in the form of history records and stored them in the Trust

Feedbacks Database: Indeed, users typically have to establish their identities for the first time they attempt to use the platform through registering their

credentials at the Identity Management Service (IdM) which stores the credentials in the Trust.

Identity Registry: Moreover, we developed the Identity Info Collector module to collect the total number of established identities among the whole identity behavior (i.e., all established identities for users who gave feedbacks to a particular cloud service).

The Trust Assessment Function: This function is responsible for handling trust assessment requests from users where the trustworthiness of cloud services are compared and the factors of trust feedbacks are calculated (i.e., the credibility factors). We developed the Factors Calculator for attacks detection based on a set of factors (more details on how the credibility factors are calculated can be found). Moreover, we developed the Trust Assessor to compare the trustworthiness of cloud services through requesting the aggregated factors weights from the Factors Calculator to weigh feedbacks and then calculate the mean of all feedbacks given to each cloud service. The trust results for each cloud service and the factors' weights for trust feedbacks are stored in the Trust Results and Factors Weights Storage.

B. Experimental Evaluation

We particularly focused on validating and studying the robustness of the proposed credibility model against different malicious behaviors, namely collusion and Sybil attacks under several behaviors, as well as the performance of our availability model.

C. Credibility Model Experiments

We tested our credibility model using real world trust feedbacks on cloud services. In particular, we crawled several review websites such as cloud-computing. findthebest.com, cloud storage provider sreviews.com, and CloudHostingReviewer.com, and where users give their feedbacks on cloud services that they have used. The collected data is represented in a tuple H where the feedback represents several QoS parameters as mentioned earlier and augmented with a set of credentials for each corresponding consumer. We managed to collect 10,076 feedbacks given by 6,982 users to 113 real-world cloud services. The collected dataset has been released to the research community via the project website. For experimental purposes, the collected data was divided into six groups of cloud services, three of which were used to validate the credibility model against collusion attacks, and the other three groups were used to validate the model against Sybil attacks where each group consists of 100 users.

VI.CONCLUSION AND FUTURE

From this Cloud Armor Supporting Reputation-based Trust Management for Cloud Services has been implemented. 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. Additionally in future, we also enhance the performance of cloud .

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. Nita- Rotaru, "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 Zakaria Maamar, 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 Mahbub Habib , Sebastian Ries y, Max M• uhlh• auser, Towards a Trust Management System for Cloud Computing
[13]Siani Pearson and Azzedine Benameur, Privacy, Security and Trust Issues Arising from Cloud Computing , 2010
[14]S. M. Khan and K. W. Hamlen, "Hatman: IntraCloud 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] Talal H. Noor, Quan Z. Sheng, Member, IEEE, Lina Yao, Schahram Dustdar, Senior Member, IEEE, and Anne H.H. Ngu, "CloudArmor: Supporting Reputation-based Trust Management for Cloud Services", IEEE Transactions on Parallel and Distributed Systems, Vol. 0, No. 0, 2014.
[18] S. M. Khan and K. W. Hamlen, "Hatman: Intra-Cloud Trust Management for Hadoop," in Proc. CLOUD'12, 2012.
[19] 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.
[20] J. Huang and D. M. Nicol, "Trust Mechanisms for Cloud Computing," Journal of Cloud Computing, vol. 2, no. 1, pp. 1–14, 2013.
[21] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14–22, 2010.
[22] 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.
[23] S. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing," in Proc. of TrustCom'11, 2011.
[24] 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.
[25] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrstedt, "A Trust Management Framework for ServiceOriented Environments," in Proc. of WWW'09, 2009.
[26] 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.
[27] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust Management of Services in Cloud Environments: Obstacles and Solutions," ACM Computing Surveys, vol. 46, no. 1, pp. 12:1–12:30, 2013.
[28] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising From Cloud Computing," in Proc. CloudCom'10, 2010.
.