International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Security and Trust Management in Cloud Computing

Somanaboina. Rajeswari & Mallereddy. Sowjanya Reddy

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 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 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. 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. "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.

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.

3. Literature Review

[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 trust-overlay 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 multi-way 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 trustworthy 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.

4. Methodologies

4.1 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.

4.2 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).

4.3 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.

4.4 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.

5 System Design

5.1 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.

5.2 The Trust Management Service Layer

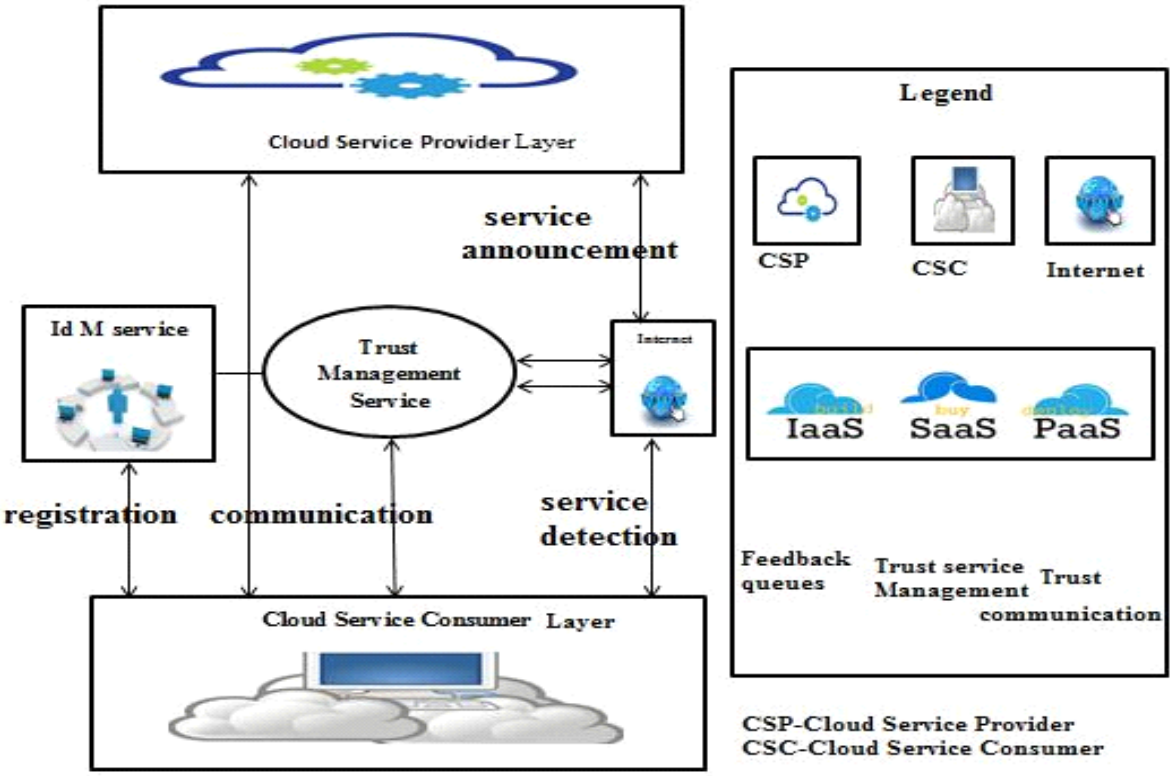
This layer consists of several distributed TMS nodes which are hosted in multiple cloud environments in different geographical areas. These TMS nodes expose interfaces so that users can give their feedback or inquire the trust results in a decentralized way. Interactions for this layer include:

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.

5.3 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 particularcloud 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, which is responsible for the registration where users register their credentials before using TMS and proving the credibility of a particular consumer's feedback through ZKC2P.

A service provider that includes customer storage or software services available through a private (private cloud) or public network (cloud).Usually, it means the storage and software is available for process through the Internet.



6. Conclusions

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 as well as the security.

7. 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.

- Jingwei Huang and David M Nicol, Trust mechanisms for cloud computing, April 2013

- J. Huang and D. M. Nicol, "Trust Mechanisms for Cloud Computing," Journal of Cloud Computing, vol. 2, no. 1, pp. 1–14, 2013.

- Kai Hwang Deyi Li, Trusted Cloud Computing with Secure Resources and Data Coloring, Sept.-Oct. 2010

- 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.

- Lina Yao Quan Z. Sheng Zakaria Maamar, Achieving High Availability of Web Services Based on A Particle Filtering Approach, 2012

- 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.

- Sheikh Mahbub Habib , Sebastian Ries y, Max M• uhlh• auser, Towards a Trust Management System for Cloud Computing

• Siani Pearson and Azzedine Benameur, Privacy, Security and Trust Issues Arising from Cloud Computing , 2010

• 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.