International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

An Exploration of Supporting Reputation Based Trust Management for Cloud Services

Akshitha Koluguri[1], Mareddy Yogeshwar[2], M.Vamshi Reddy[3], M. Sreedhar[4],
[1]Assistant Professor, Department of CSE, Guru Nanak Institutions, Ibrahimpatnam, Hyderabad, India
[2,3,4] B.Tech Students, Department of Computer Science & Engineering, Guru Nanak Institutions, Hyderabad, India

Abstract: *Cloud computing widely adopted by means of enterprises and people. Cloud computing offer several advantages however nevertheless there are numerous obstacles in cloud. Trust performs vital role in commercial cloud environments. Although numerous solutions had been proposed these days in handling accept as true with feedbacks in cloud environments, how to determine the credibility of trust feedbacks is mainly ignored. In this mission the system proposed a Cloud Armor, a popularity-primarily based agree with management framework that gives a fixed of functionalities to deliver Trust as a Service (TaaS). "Trust as a Service" (TaaS) framework to enhance approaches on agree with management in cloud environments. The techniques have been proven through the prototype system and investigational results.*

Index Terms–Cloud Computing, Trust Management, Trust, Obstacles, Reputation, Feedbacks

I. INTRODUCTION

Recently, cloud computing has been receiving much attention as a new computing paradigm for providing flexible and on-demand infrastructures, platforms, and software as services. According to National Institute of Standards and Technology (NIST) [1], "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". Cloud computing offers service dynamism, elasticity and wide variety of choices to enterprises. In today's competitive environment, enterprises cannot ignore these services. Flexible cloud computing services require one party (i.e. Cloud Consumer (CC)) rely on the actions of other party (i.e. Cloud Service Provider (CSP)), therefore, trust has become a vital component of such services.

Trust is a complex social phenomenon. Based on the concepts of trust developed in social sciences [2, 3], trust is a mental state comprising: (1) expectancy in which the trust or expects a specific behavior from the trustee such as providing valid information or effectively performing cooperative actions; (2) belief in which the trustor believes that the expected behavior occurs, based on the evidence of the trustee's competence, integrity, and goodwill; (3) willingness to take risk –in which the trustor is willing to take risk for that belief" [4]. Although intuitively easy to comprehend, the notion of trust has not been scholarly defined [5].

In order to use cloud services, an enterprise needs to give up control of its assets (i.e. data) to the CSP. Loss of control on stored data in cloud triggers uncertainty about data confidentiality, privacy, integrity and availability for CCs which adversely affects adoptability of cloud computing services. Enterprises have to remember that as compelling as cloud services are, it isn't without potential problems. Amazon Simple Storage Service (S3), as an example of cloud services, had suffered an outage for several hours in February 2008 that resulted in numerous customer Web applications going offline [6, 7].

CSPs and consumers can take advantage of the benefits of cloud computing technologies when an effective trust management system is designed and implemented for cloud computing services, properly. To guarantee effectiveness of trust management in offered cloud computing services, on-going and state-of-the-art evaluation techniques are required. Evaluation of trust in cloud computing is a challenging issue since trust is subjective and case sensitive. In order to evaluate trust in cloud services, different methods and techniques have been proposed which are commonly known as the "Trust Models" in literature.

According to researchers at Berkeley, trust and safety is ranked one of the pinnacle 10 obstacles for the adoption of cloud computing. Indeed, Service-Level Agreements (SLAs).Users' feedback is a great source to evaluate the general trustworthiness of cloud offerings. Several researchers have diagnosed the significance of agree with control and proposed solutions to assess and manage believe based totally on feedbacks accumulated from participants.

II. RELATED WORK

Author in [12] describe about, how security, trust and privacy issues occurring 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.

Author in [8] describe about, survey of existing mechanisms for establishing trust, and comment on their limitations. Also 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.

Author in [9] describe about, 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.

Author in [11] 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 systemprovides 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.

Author in [10] tackle these problems by exploiting particle filtering-based techniques. In particular, the developed algorithms 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.

III. SYSTEM DESIGN

The purpose of trusted computing is to solve some of today's security problems through hardware changes to personal computer. Trust is a crucial enabling factor in relations where there is uncertainty, interdependence, risk, and fear of opportunism. It has defined trust as a mental state which is consists of expectancy, belief and willingness to take risk. Based on this definition two types of trusts can be introduced. One of them is trust in performance which is the trust about what the trustee performs. The other one is trust in belief which is the trust about what the trustee believes. The trustee's performance should be based on what he says or what he does. Trust models are the techniques that are used for evaluating trust in cloud services. They can be categorized in certain categories named trust mechanisms.

Reputation Based: Trust and reputation are different from each other. Trust is the subjective expectation of one entity about another within a specific context at a given time. Reputation, on the other hand, is what is believed about an entity's standing by the community. This belief can be derived from direct or indirect experiences collected in previous interactions between entities.

Authentication Based: Encryption and Key Management are important technologies that can help secure applications and data in cloud. PKI is a technology that introduces a trust mechanism to support digital signature, key certification and validation, attribute certification and validation.

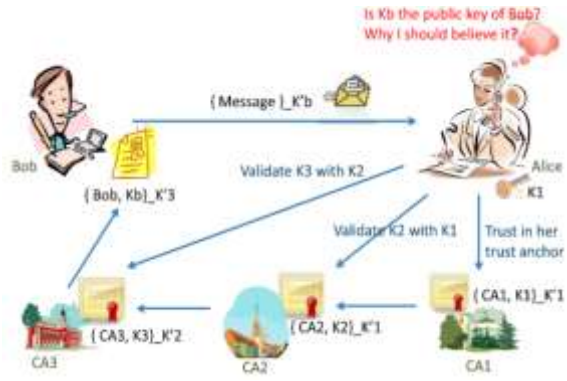

Fig.1. Trust relations in public key validation and certificate [13]

A. The Cloud Service Provider Layer

This layer consists of different cloud service providerswho offer one or several cloud services, i.e., IaaS (Infrastructure as a Service), PaaS (Platform as aService), 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 indifferent geographical areas. These TMS nodes expose inter faces 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.

C. 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).

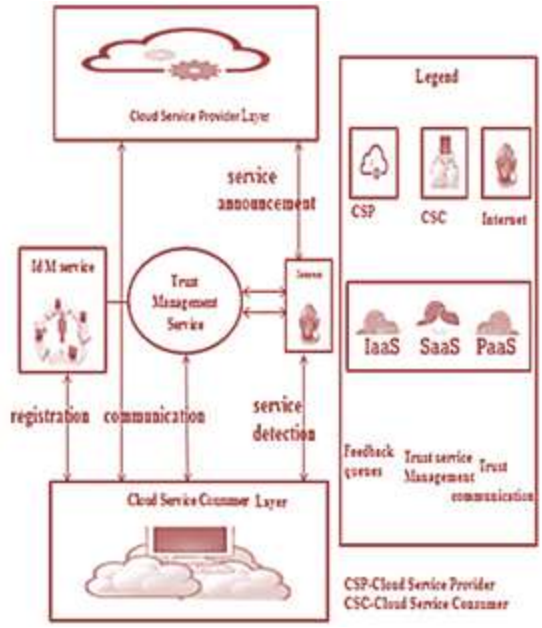

Fig.2. Framework of the system

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 frameworkcontains 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 throughZKC2P. 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.

IV. CONCLUSION

From this Cloud Armor Supporting Reputation based Trust Management for Cloud Services has been implemented. In cloud computing increase, the management of consider detail is most hard trouble. Cloud computing has produce high challenges in protection and privacy by the changing of environments. Trust is one of the maximum worried obstacles for the adoption and boom of cloud computing. Although numerous answers were proposed these days in managing agree with feedbacks in cloud environments, how-to decide the credibility of agree with feedbacks is typically omitted.

REFERENCES

[1] P. Mell and T.Grance. "The NIST definition of cloud computing," National Institute of Standards and Technology, 2009.

[2] M. Firdhous, O. Ghazali and S. Hassan. "Trust Management in Cloud Computing: A Critical Review," International Journal on Advances in ICT for Emerging Regions, Vol.4 no. 2, pp. 24-36, 2011.

[3] J. Staten. "Is cloud computing ready for the enterprise?" Forrester Research, 2008.

[4] X. Li and L. Liu. "A Reputation-based Trust Model for Peer-to-Peer E-CommerceCommunities," in IEEE International Conference on E-Commerce Technology, 2003, pp.275-284.

[5] D. Zhou. "Security Issues in Ad-hoc Networks," The Handbook of Ad-hoc Wireless Networks Boca Raton, FL, USA: CRC Press, Inc, 2003, pp. 569 – 582.

[6] O. Malik. "Amazon S3 Storage Service Does Down, Still Not Up," Internet:https://gigaom.com/2008/02/15/amazon-s3-service-goes-down/, Feb 15, 2008 [Jan. 24,2016].

[7] N. Gohring. "Amazon's S3 Down for Several Hours," Internet:http://www.pcworld.com/article/142549/article.html, Feb 15, 2008 [Jan. 24, 2016].

[8]. Jingwei Huang and David M Nicol, Trust mechanisms for cloud computing, April 2013.

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

[10]. Lina Yao Quan Z. Sheng ZakariaMaamar, Achieving High Availability of Web Services Based on A Particle Filtering Approach, 2012.

[11]. Sheikh Mahbub Habib, Sebastian Ries Y, Max Muhlh auser, Towards a Trust Management System for Cloud Computing.

[12]. Siani Pearson and Azzedine Benameur, Privacy, Security and Trust Issues Arising from Cloud Computing, 2010.

[13] J. Huang and D. M. Nicol. "Trust mechanisms for cloud computing." Journal of Cloud Computing: Advances, Systems and Applications, vol. 2, no. 9, pp. 2-14, April 2013.