ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Trust Management of Cloud Services Using Credibility Assessment Technique

U.Vyshnavi
M.Tech Scholar
Department of CSE
G.Pulla Reddy Engineering College (Autonomous)
Kurnool.

P.Praveen Yadav
Assistant Professor
Department of CSE
G.Pulla Reddy Engineering College (Autonomous)
Kurnool.

Abstract

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 addition, managing trust feedbacks in cloud environments is a difficult problem due to unpredictable number of cloud service consumers and highly dynamic nature of cloud environments. In this paper, we propose the Trust Management framework to improve ways on management in cloud environments. In particular, we 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.

Keywords: ***Trust Management, Cloud Computing, Distributed Computing, Credibility Model.***

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 Services.Given the quick adoption of cloud computing in the industry, there is a significant challenge in managing trust among cloud service providers and cloud service consumers [1,3,8]. Recently, the significance of trust management is highly recognized and several solutions are proposed to assess and manage trust feedbacks 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 [7,9]; 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 a Service (TaaS) framework. This framework helps distinguish between the credible 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

develop a credibility model that not only distinguishes between trust feedbacks from experienced cloud service consumers and from amateur cloud service consumers, but also considers the majority consensus of feedbacks; ii) Distributed Trust Feedback Assessment and Storage: to avoid the drawbacks of centralized architectures, our trust management service allows trust feedback assessment and storage to be managed distributively.

2. RELATED WORK

According to Hatman: Intra-Cloud Trust Management for Hadoop - S. M. Khan and K. W. Hamlen, the authors quoted on Data and computation integrity and security are major concerns for users of cloud computing facilities. Many production-level clouds optimistically assume that all cloud nodes are equally trustworthy when dispatching jobs; jobs are dispatched based on node load, not reputation. This increases their vulnerability to attack, since compromising even one node suffices to corrupt the integrity of many distributed computations. This paper presents and evaluates Hatman: the first full-scale, data-centric, reputation-based trust management system for Hadoop clouds. Hatman dynamically assesses node integrity by comparing job replica outputs for consistency. This yields agreement feedback for a trust manager based on EigenTrust. Low overhead and high scalability is achieved by formulating both consistency checking and trust management as secure cloud computations; thus, the cloud's distributed computing power is leveraged to strengthen its security. Experiments demonstrate that with feedback from only 100 jobs, Hatman attains over 90% accuracy when 25% of the Hadoop cloud is malicious.

According to Privacy, Security and Trust in Cloud Computing - S. Pearson, the authors quoted on, Cloud computing refers to the underlying infrastructure for an emerging model of service provision that 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. These new features have a direct impact on information technology (IT) budgeting but also affect traditional security, trust and privacy mechanisms. The advantages of cloud computing—its ability to scale rapidly, store data remotely and share services in a dynamic environment—can become disadvantages in maintaining a level of assurance sufficient to sustain confidence in potential customers. Some core traditional mechanisms for addressing privacy (such as model contracts) are no longer flexible or dynamic enough, so new approaches need to be developed to fit this new paradigm.

In this chapter, we assess how security, trust and privacy issues occur in the context of cloud computing and discuss ways in which they may be addressed. According to Trust Mechanisms for Cloud Computing - J. Huang and D. M. Nicol, the authors quoted on, Trust is a critical factor in cloud computing; in present practice it depends largely on perception of reputation, and self assessment by providers of cloud services. 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 integratingvarious trust mechanisms together to reveal chains of trust in the cloud. According to Trusted Cloud Computing with Secure Resources and Data Coloring - K. Hwang and D. Li, the authors quoted on, Trust and security have prevented businesses from fully accepting cloud platforms. To protect clouds, providers must first secure virtualized data center resources, uphold user privacy, and preserve data integrity. 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

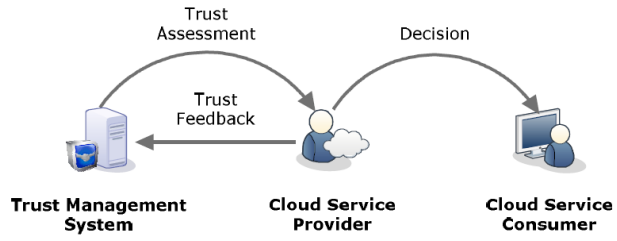
According to A View of Cloud Computing - M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, the authors quoted on, Cloud computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under provisioning for one that becomes wildly popular, thus missing potential customers and revenue.

Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1,000 servers for one hour costs no more than using one server for 1,000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT. As a result, cloud computing is a popular topic for blogging and white papers and has been featured in the title of workshops, conferences, and even magazines. Nevertheless, confusion remains about exactly what it is and when it's useful, causing Oracle's CEO Larry Ellison to vent his frustration: "The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do.... I don't understand what we would do differently in the light of cloud computing other than change the wording of some of our ads."

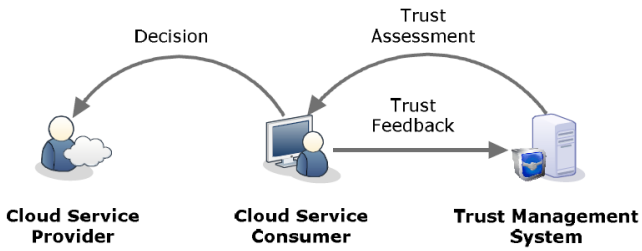
3. TRUST MANAGEMENT

Trust management is originally developed by Blaze et. al [Blaze et al. 1996] toovercome the issues of centralized security systems, such as centralized control oftrust relationships (i.e., global certifying authorities), inflexibility to support complex trust relationships in large-scale networks, and the heterogeneity of policylanguages. Policy languages in trust management are responsible for setting authorization roles and implementing security policies. Authorization roles are satisfiedthrough a set of security policies, which themselves are satisfied through a set ofcredentials. Some early attempts to implementing the trust management are PolicyMaker and KeyNote [Blaze et al. 1998; Blaze et al. 1998; Blaze et al. 1999;Blaze et al. 2000]. These techniques are considered as policy-based trust management because they rely on policy roles to provide automated authorizations. Later,trust management inspired many researchers to specify the same concept in different environments such as e-commerce, P2P systems, Web services, wireless sensornetworks, grid computing, and most recently cloud computing.

Trust management is an effective approach to assess and establish *trusted relationships*. Several approaches have been proposed for managing and assessing trust based on different perspectives. We classify trust management using two different perspectives, namely: *Service Provider Perspective* (SPP) and *Service Requester Perspective* (SRP). In SPP, the service provider is the main driver of thetrust management system where service requesters' trustworthiness is assessed On the other hand, in SRP, the service requester is the one who assessesthe trustworthiness of the service provider.



(a) Service Provider's Perspective (SPP)



(b) Service Requester's Perspective (SRP)

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

4. TRUST MANAGEMENT TECHNIQUES

Different trust management techniques have been reported in the literature, whichcan be classifiedinto four different categories: Policy, Recommendation, Reputation, and Prediction. To ease the discussion, we focus on explaining these trustmanagement techniques using the service requester perspective (i.e., cloud serviceconsumers perspective). The same techniques can be applied to the other perspective (i.e., cloud service providers perspective).

Policy as a Trust Management Technique (PocT)

Policy as a trust management technique (PocT) is one of the most popular and traditional ways to establish trust among parties and has been used in cloud environments [Yao et al.2010; Santos et al. 2009; Alhamad et al. 2010], the grid [Song et al. 2005], P2Psystems [Song et al. 2005], Web applications [De Capitani di Vimercati et al. 2012]and the service oriented environment [Skogsrud et al. 2007; Skogsrud et al. 2009].PocT uses a set of policies and each of which assumes several roles that controlauthorization levels and specifies a minimum trust threshold in order to authorizeaccess. The trust thresholds are based on the trust results or the credentials.For the trust results-based threshold, several approaches can be used. For in-stance, the *monitoring and auditing* approach proves Service Level Agreement(SLA) violations in cloud services (i.e., if the SLA is satisfied, then the cloud service is considered as trustworthy and vise versa). The *entities credibility* approachspecifies a set of parameters to measure the credibility of parties [Huynh et al.2006] while the *feedback credibility* approach considers a set of factors to measurethe credibility of feedbacks. SLA can be considered as a service plan (i.e., wherethe service level is specified) and as a service assurance where penalties can beassigned to the cloud service provider if there is a service level violation in the provisioned cloud services. SLA can establish trust between cloud service consumersand providers by specifying technical and functional descriptions with strict clauses. The literature reports some efforts of PocT in cloud computing. For example,Brandic et al. [Brandic et al. 2010] propose a novel language for specifying compliance requirements based on a model-driven technique and Ko et al. [Ko et al. 2011]present a TrustCloud framework that uses SLA detective controls and monitoringtechniques for achieving trusted cloud services. Hwang et al. [Hwang et al. 2009;Hwang and Li 2010] propose a security aware cloud architecture that uses predefined policies to evaluate the credibility of cloud services and Habib et al. [Habibet al. 2011] develop a multi-faceted Trust Management (TM) system to measure thecredibility of cloud services based on quality of service (QoS) attributes such as security, latency, availability, and customer support. Finally, Noor and Sheng [Noorand Sheng 2011b; 2011a] propose a credibility model that distinguishes crediblefeedbacks from the misleading ones. PocT is applicable for all three cloud servicemodels.

5. FRAMEWORK FOR TRUST MANAGEMENT

In this section, we propose a generic analytical framework for trust managementin cloud environments (see Figure d). In the framework, interactions in cloudapplications occur at three layers.

5.1. Layers of the Trust Management Analytical Framework

The three layers of the trust management framework include: the trust feedbacksharing layer, the trust assessment layer, and the trust result distribution layer

5.1.1. Trust Feedback Sharing Layer (TFSL)

TFSL consists of different parties including cloud service consumers and providers, which give trust feedbacks to eachother. These feedbacks are maintained via a module called the Trust FeedbackCollector. The feedbacks storage relies on the trust management systems, in theform of centralized, decentralized or even in the cloud environment through atrusted cloud service provider.

5.1.2. Trust Assessment Layer (TAL)

This layer represents the core of any trust management system: trust assessment. The assessment might

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

contain more than onemetrics. TAL handles a huge amount of trust assessment queries from severalparties through a module called the Trust Result Distributor. This typically involves checking the trust results database and performing the assessment basedon different trust management techniques TAL delivers the trust results to adatabase in the trust results distribution layer through the module of the trustresult distributor. This procedure is taken to avoid redundancy issues in trustassessment.

Fig c: Trust Management (TM) Techniques

5.1.2. Trust Result Distribution Layer (TRDL)

Similar to TFSL, this layer consistsof different parties including cloud service consumers and providers, which issuetrust assessment inquiries about other parties (e.g., a cloud service consumerinquires about a specified cloud service).

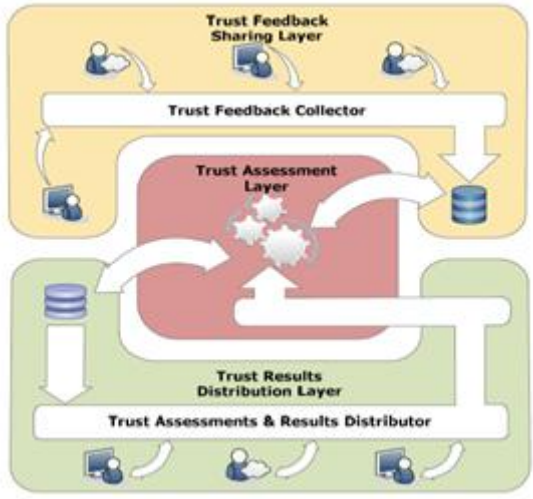


Fig d. Architecture of the Trust Management Analytical Framework

All trust assessment inquiries are transmitted to the trust assessment function through the module of trust assessmentand results distributor. The final results are maintained in a database wherecloud service consumers and providers can retrieve.

6. EVALUATION OF TRUST MANAGEMENT RESEARCH PROTOTYPES

The evaluation of trust management prototypes covers 30 representative researchprototypes where 69% of these research prototypes have been published in the last6 years and the rest represents some classical research prototypes that we cannotresist taking notice of them, due to their fundamental contribution and influence inthe field of trust management. The evaluation is organized toassess research prototypes using three different layers (i.e., the trust feedback sharinglayer, the trust assessment layer and the trust result distribution layer) based on aset of dimensions.

7. CONCLUSION

In recent years, cloud computing has become a vibrant and rapidly expanding areaof research and development. Trust is widely regarded as one of the top obstaclesfor the adoption and the growth of cloud computing. In this article, we havepresented a comprehensive survey that is, to the best of our knowledge, the first tofocus on the trust management of services in cloud environments. We distinguishthe trust management perspectives and classify trust management techniques intofour different categories. We further propose a generic analytical framework thatcan be used to compare different trust management research prototypes based ona set of assessment criteria. We overview and compare 30 representative researchprototypes on trust management in cloud computing and the relevant researchareas. Along with the current research efforts, we encourage more insight anddevelopment of innovative solutions to address the various open research issuesthat we have identified in this work.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[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. NitaRotaru, "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 ZakariaMaamar, 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 MahbubHabib , Sebastian Ries y, Max M• uhlh• auser, Towards a Trust Management System for Cloud Computing

[13] Siani Pearson and AzzedineBenameur, Privacy, Security and Trust Issues Arising from Cloud Computing , 2010

[14] 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.

[17] 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.

[18] T. H. Noor, Q. Z. Sheng, A. H. Ngu, A. Alfazi, and J. Law, "CloudArmor: A Platform for Credibility-based Trust Management of Cloud Services," in Proc. of CIKM'13, 2013.

[19] T. Noor and Q. Z. Sheng, "CredibilityBased Trust Management for Services in Cloud Environments," in Proc. of ICSOC'11, 2011.

[20] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrst-edt, "A Trust Management Framework for ServiceOriented Environments," in Proc. of WWW'09, 2009.