International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

Supporting Reputation Based Trust Management for Cloud Services

1.**G.Soumya**, M.Tech, Department of CSE, Vaagdevi college of Engineering, Bollikunta, Warangal, Telangana, Mail ID : soumyagampa652@gmail.com
2.**A.Raju**, Assistant Professor,Department of CSE, Vaagdevi College Of Engineering, Bollikunta, Warangal, Telangana.
3. **V.Janaki** ,HOD prof. Depatment of CSE, Vaagdevi College of Enginering, Bollikunta, Warangal, Telangana.

ABSTRACT:Trust management is one of the most challenging issues for the adoption and growth of cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services introduces several challenging issues such as privacy, security, and availability. Preserving consumers' privacy is not an easy task due to the sensitive information involved in the interactions between consumers and the trust management service. Protecting cloud services against their malicious users (e.g., such users might give misleading feedback to disadvantage a particular cloud service) is a difficult problem. Guaranteeing the availability ofthe trust management service is another significant challenge because of the dynamic nature of cloud environments.

In this article,we describe the design and implementation of CloudArmor, a reputation-based trust management framework that provides a set offunctionalities to deliver Trust as a Service (TaaS), which includes i) a novel protocol to prove the credibility of trust feedbacks andpreserve users' privacy, ii) an adaptive and robust credibility model for measuring **the credibility of trust feedbacks to protect** cloudservices from malicious users and to compare the trustworthiness of cloud services, and iii) an availability model to manage theavailability of the decentralized implementation of the trust management service. The feasibility and benefits of our approach havebeen validated by a prototype and experimental studies using a collection

of real-world trust feedbacks on cloud services.

Index Terms—Cloud computing, trust management, reputation, credibility, credentials, security, privacy, availability.

1 INTRODUCTION

THE highly dynamic, distributed, and nontransparent nature of cloud services make thetrust management in cloud environments a significant challenge [1], [2], [3], [4]. According to researchers at Berkeley [5], trust and security are ranked one of thetop 10 obstacles for the adoption of cloud computing .Indeed, Service-Level Agreements (SLAs) alone areinadequate to establish trust between cloud consumers and providers because of its unclear and inconsistent clauses .Consumers' feedback is a good source to assessthe overall trustworthiness of cloud services. Several researchers have recognized the significance of trustmanagement and proposed solutions to assess andmanage trust based on feedbacks collected from participants[7], [6], [8], [9]. In reality, it is not unusualthat a cloud service experiences malicious behaviors(e.g., collusion or Sybil attacks) from its users [6], [10].This paper focuses on improving trust managementin cloud environments by proposing novel ways toensure the credibility of trust feedbacks. In particularwe distinguish the following key issues of the trustmanagement in cloud environments:

• **Consumers' Privacy**. The adoption of cloud computingraise privacy concerns [11]. Consumers canhave dynamic interactions with cloud providers,which may involve sensitive information. There areseveral cases of privacy breaches such as leaks ofsensitive information (e.g., date of birth and address)or behavioral information (e.g., with whomthe consumer interacted, the kind of cloud servicesthe consumer showed interest, etc.). Undoubtedly,services which involve consumers' data (e.g., interactionhistories) should preserve their privacy.

• **Cloud Services Protection**. It is not unusual that acloud service experiences attacks from its users.Attackers can disadvantage a cloud service by givingmultiple misleading feedbacks (i.e., collusionattacks) or by creating several accounts (i.e., Sybilattacks). Indeed, the detection of such malicious behaviorsposes several challenges. Firstly, new usersjoin the cloud environment and old users leavearound the clock. This consumer dynamism makesthe detection of malicious behaviors (e.g., feedbackcollusion) a significant challenge. Secondly, usersmay have multiple accounts for a particular cloudservice, which makes it difficult to

detect Sybilattacks [13]. Finally, it is difficult to predict whenmalicious behaviors occur (i.e., strategic VS. occasionalbehaviors) [14].

• **Trust Management Service's Availability.**A trust managementservice (TMS) provides an interface be1045-between users and cloud services for effective trustmanagement. However, guaranteeing the availabilityof TMS is a difficult problem due to the unpredictablenumber of users and the highly dynamicnature of the cloud environment [7], [6],[10]. Approaches that require understanding ofusers' interests and capabilities through similaritymeasurements [15] or operational availability measurements[16] (i.e., uptime to the total time) areinappropriate in cloud environments. TMS shouldbe adaptive and highly scalable to be functional incloud environments.

II RELATED WORK

Over the past few years, trust management has beenone of the hot topics especially in the area of cloud computing [14], [10]. Some of the research efforts usepolicy-based trust management techniques. For example,Ko et al. [33] propose TrustCloud framework for accountabilityand trust in cloud computing. In particular,TrustCloud consists of five layers including workflow,data, system, policies and laws, and regulations layersto address accountability in the cloud environmentfrom all aspects. All of these layers maintain the cloudaccountability life cycle which consists of seven phasesincluding policy planning, sense and trace, logging,safe-keeping of logs, reporting and replaying, auditing,and optimizing and rectifying. Brandic et al. [7] proposea novel approach for compliance management incloud environments to establish trust between differentparties. The approach is developed using a centralizedarchitecture and uses compliant management techniqueto establish trust between cloud service users andcloud service providers. Unlike previous works that usepolicy-based trust management techniques, we assess
the trustworthiness of a cloud service using reputationbasedtrust management techniques. Reputation representsa high influence that cloud service users haveover the trust management system especially thatthe opinions of the various cloud service users candramatically influence the reputation of a cloud serviceeither positively or negatively.Some research efforts also consider the reputationbasedtrust management techniques. For instance,Habib et al. [6] propose a multi-faceted Trust Management(TM) system architecture for

cloud computingto help the cloud service users to identify trustworthycloud service providers. In particular, the architecture models uncertainty of trust information collected frommultiple sources using a set of Quality of Service (QoS)attributes such as security, latency, availability, and customersupport. The architecture combines two differenttrust management techniques including reputationand recommendation where operators (e.g., AND, OR,NOT, FUSION, CONSENSUS, and DISCOUNTING) areused. Hwang et al. [4] propose a security aware cloudarchitecture that assesses the trust for both cloud serviceproviders and cloud service users. To assess thetrustworthiness of cloud service providers, the authorspropose the trust negotiation approach and the datacoloring (integration) using fuzzy logic techniques. Toassess the trustworthiness of cloud service users, theydevelop the Distributed-Hash-Table (DHT)-based trustoverlaynetworks among several data centers to deploya reputation-based trust management technique. Unlikeprevious works which do not consider the problem ofunpredictable reputation attacks against cloud services,we present a credibility model that not only detectsthe misleading trust feedbacks from collusion and Sybilattacks, but also has the ability to adaptively adjust thetrust results for cloud services that have been affectedby malicious behaviors.

III THE CLOUDARMOR FRAMEWORK

The CloudArmor framework is based on the serviceoriented architecture (SOA), which delivers trust as aservice. SOA and Web services are one of the mostimportant enabling technologies for cloud computing inthe sense that resources (e.g., infrastructures, platforms,and software) are exposed in clouds as services [17], In particular, the trust management service spansseveral distributed nodes that expose interfaces so thatusers can give their feedbacks or inquire the trust results.the framework, which consists ofthree different layers, namely the Cloud Service ProviderLayer, the Trust Management Service Layer, and the CloudService Consumer Layer.The Cloud Service Provider Layer. This layer consistsof different cloud service providers who offer one orseveral cloud services, i.e., IaaS (Infrastructure as aService), PaaS (Platform as a Service), and SaaS (Softwareas a Service), publicly on the Web (more detailsabout cloud services models and designs can be foundin [19]). These cloud services are accessible throughWeb portals and indexed on Web search engines suchas

Google, Yahoo, and Baidu. Interactions for this layerare considered as cloud service interaction with users andTMS, and cloud services advertisements where providersare able to advertise their services on the Web.The Trust Management Service Layer. This layer consistsof several distributed TMS nodes which are hosted inmultiple cloud environments in different geographicalareas. These TMS nodes expose interfaces so that userscan give their feedback or inquire the trust results in adecentralized way. Interactions for this layer include: i)cloud service interaction with cloud service providers, ii)service advertisement to advertise the trust as a serviceto users through the Internet, iii) cloud service discoverythrough the Internet to allow users to assess the trustof new cloud services, and iv) Zero-Knowledge CredibilityProof Protocol (ZKC2P) interactions enabling TMS to

The Cloud Service Consumer Layer. Finally, this layerconsists of different users who use cloud services. Forexample, a new startup that has limited funding canconsume cloud services (e.g., hosting their services inAmazon S3). Interactions for this layer include: i) servicediscovery where users are able to discover new cloudservices and other services through the Internet, ii) trustand service interactions where users are able to givetheir feedback or retrieve the trust results of a particularcloud service, and iii) registration where users establishtheir identity through registering their credentials inIdM before using TMS.Our framework also exploits a Web crawling approachfor automatic cloud services discovery, wherecloud services are automatically discovered on the Internetand stored in a cloud services repository. Moreover,our framework contains an Identity Management Servicewhich is responsible for the registration

where users register their credentials before using TMSand proving the credibility of a particular consumer'sfeedback through ZKC2P.

IV ZERO-KNOWLEDGE CREDIBILITY PROOFPROTOCOL (ZKC2P)

Since there is a strong relation between trust and identificationas emphasized in [20], we propose to usethe Identity Management Service (IdM) helping TMS inmeasuring the credibility of a consumer's feedback.However, processing the IdM information can breachthe privacy of users. One way to preserve privacy isto use cryptographic encryption techniques. However,there is no efficient way to process encrypted data [11].Another way is to use anonymization techniques toprocess the IdM

information without breaching the privacyof users. Clearly, there is a trade-off between highanonymity and utility. Full anonymization means betterprivacy, while full utility results in no privacy protection(e.g., using a de-identification anonymization

technique can still leak sensitive information throughlinking attacks [21]).Thus, we propose a Zero-Knowledge Credibility ProofProtocol (ZKC2P) to allow TMS to process IdM's information(i.e., credentials) using the Multi-Identity Recognitionfactor .In other words,TMS will prove the users' feedback credibility withoutknowing the users' credentials. TMS processes credentialswithout including the sensitive information.Instead, anonymized information is used via consistenthashing (e.g., sha-256). The anonymization process coversall the credentials' attributes except the Timestampsattribute.

V CONCLUSION

Given the highly dynamic, distributed, and nontransparentnature of cloud services, managing and establishingtrust between cloud service users and cloudservices remains a significant challenge. Cloud serviceusers' feedback is a good source to assess the overalltrustworthiness of cloud services. However, malicioususers may collaborate together to i) disadvantage acloud service by giving multiple misleading trust feedbacks(i.e., collusion attacks) or ii) trick users into trustingcloud services that are not trustworthy by creatingseveral accounts and giving misleading trust feedbacks(i.e., Sybil attacks). In this paper, we have presentednovel techniques that help in detecting reputationbasedattacks and allowing users to effectively identifytrustworthy cloud services. In particular, we introducea credibility model that not only identifies misleadingtrust feedbacks from collusion attacks but also detectsSybil attacks no matter these attacks take place in along or short period of time (i.e., strategic or occasionalattacks respectively). We also develop an availabilitymodel that maintains the trust management service at adesired level. We have collected a large number of consumer'strust feedbacks given on real-world cloud services(i.e., over 10,000 records) to evaluate our proposedtechniques. The experimental results demonstrate theapplicability of our approach and show the capabilityof detecting such malicious behaviors.There are a few directions for our future work. Weplan to combine different trust management techniquessuch as reputation and recommendation to increase thetrust results accuracy. Performance

optimization of thetrust management service is another focus of our futureresearch work.

REFERENCES

[1] S. M. Khan and K. W. Hamlen, "Hatman: Intra-Cloud TrustManagement for Hadoop," in Proc. CLOUD'12, 2012.

[2] S. Pearson, "Privacy, Security and Trust in Cloud Computing,"in Privacy and Security for Cloud Computing, ser. Computer Communicationsand Networks, 2013, pp. 3–42.

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

[4] K. Hwang and D. Li, "Trusted Cloud Computing with SecureResources and Data Coloring," IEEE Internet Computing, vol. 14,no. 5, pp. 14–22, 2010.

[5] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski,G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "AView of Cloud Computing," Communications of the ACM, vol. 53,no. 4, pp. 50–58, 2010.

[6] S. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust ManagementSystem for Cloud Computing," in Proc. of TrustCom'11,2011.

[7] I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, andR. Konrad, "Compliant Cloud Computing (C3): Architecture andLanguage Support for User-Driven Compliance Management inClouds," in Proc. of CLOUD'10, 2010.

[8] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrstedt,"A Trust Management Framework for Service-OrientedEnvironments," in Proc. of WWW'09, 2009.

[9] T. H. Noor, Q. Z. Sheng, and A. Alfazi, "Reputation AttacksDetection for Effective Trust Assessment of Cloud Services," inProc. of TrustCom'13, 2013.

[10] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust Managementof Services in Cloud Environments: Obstacles andSolutions," ACM Computing Surveys, vol. 46, no. 1, pp. 12:1–12:30, 2013.

[11] S. Pearson and A. Benameur, "Privacy, Security and Trust IssuesArising From Cloud Computing," in Proc. CloudCom'10, 2010.

[12] E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy-preservingDigital Identity Management for Cloud Computing," IEEE DataEng. Bull, vol. 32, no. 1, pp. 21–27, 2009.

[13] E. Friedman, P. Resnick, and R. Sami, Algorithmic Game Theory.New York, USA: Cambridge University Press, 2007, ch.Manipulation-Resistant Reputation Systems, pp. 677–697.

[14] K. Ren, C. Wang, and Q. Wang, "Security Challenges for thePublic Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[15] F. Skopik, D. Schall, and S. Dustdar, "Start Trusting Strangers?Bootstrapping and Prediction of Trust," in Proc. of WISE'09, 2009.

[16] H. Guo, J. Huai, Y. Li, and T. Deng, "KAF: Kalman FilterBased Adaptive Maintenance for Dependability of CompositeServices," in Proc. of CAiSE'018, 2008.

[17] T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues andChallenges," in Proc. of AINA'10, 2010.

[18] Y. Wei and M. B. Blake, "Service-oriented Computing and CloudComputing: Challenges and Opportunities," Internet Computing,IEEE, vol. 14, no. 6, pp. 72–75, 2010.

[19] P. Mell and T. Grance, "The NIST Definition of CloudComputing," Sep 2011, accessed: 05/06/2012, Available at:http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145 cloud-definition. pdf.

[20] O. David and C. Jaquet, "Trust and Identification in the Light ofVirtual Persons," pp. 1–103, Jun 2009, accessed 10/3/2011, Availableat: http://www.fidis.net/resources/deliverables/identityof-identity/.