ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Cloud Consumers Credibility Assessment Framework for Reputation-Based Trust Management (Cloud Armor) in Cloud Services: A Review

U.B. Bagal, Prof.S.U.Kadam

M. E Student, Department of Computer Engineering, Zeal College of Engineering and Research, Savitribai Phule Pune University Maharashtra, India

Professor, Department of Computer Engineering, Zeal College of Engineering and Research, Savitribai Phule Pune University, Maharashtra, India

ABSTRACT: Trust management is a standout amongst the most difficult issue for the tackling and development of cloud computing. 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. Protecting cloud services from malicious clients e.g., such clients may give misleading feedback to inconvenience a specific cloud service, is a complicated issue. Due to the dynamic nature of cloud environments, assuring the availability of the trust management service is a challenging issue. In this project the system proposed of Cloud Armor, a reputation-based trust management system to deliver Trust as a Service(TaaS), which includes I) a novel convention to demonstrate the credibility of trust feedbacks and save users' privacy, II) a versatile and robust credibility model for measuring the credibility of trust feedbacks to protect cloud services from malicious users and to analyze the dependability of cloud services, and III) an availability model to deal with the accessibility of the decentralized usage of the trust management service. The contribution work is to combine different trust management techniques such as reputation and recommendation to increase the trust results accuracy. Performance optimization of the trust management service is main challenging issue. The achievability and advantages of our methodology have been tried by a model and test studies utilizing a collection of true trust feedbacks on cloud services. The approaches have been validated by the prototype system and experimental results.

KEYWORDS: Availability, Cloud Computing, Collusion Attacks, Credentials, Credibility, Feedbacks, Privacy, Reputation, Security, Sybil Attacks, Trust Management, ZKC2P.

I. INTRODUCTION

The highly dynamic, distributed, and non-transparent nature of cloud services introduces several challenging issues such as privacy, security, and availability.Consumers' feedback is an excellent source to assess the overall trustworthiness of cloud services. Severalresearchers have known 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 presenting novel ways to ensure the credibility of trust feedbacks. In particular, we distinguish the following key issues of the trust management in cloud environments**.** The adoption of cloud computing raises privacy concerns. Customers 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

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.

It is not unusual that a cloud service experiences attacks from its users. Attackers can disadvantage a cloud service by giving multiple misleading feedbacks or by creating several accounts. 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 a significant challenge. Secondly, users may contain multiple accounts for a particular cloud service, which makes it difficult to detect Sybil attacks. Finally, it is difficult to guess when malicious behaviors occur.

In CloudConsumers Credibility Assessment Framework for Reputation-Based Trust Management in Cloud Services we review as, trust is main factor where TMS spans several distributed nodes to managefeedbacks in a decentralized way. CloudArmor exploitstechniques to identify credible feedbacks from maliciousones. The salient features of CloudArmor are:Zero-Knowledge Credibility Proof Protocol, our credibility model and availability model respectively.

II. REVIEW OF LITERATURE

Several researchers have recognized the significance of trust management and proposed solutions. One of the techniques among them is detection of reputation attacks to allow consumers to effectively identify trustworthy cloud services [1], [8]. Another category is Monarch's architecture generalizes too many web services being targeted by URL spam, accurate classification hinges on having an intimate understanding of theSpam campaigns abusing a service [2]. Additionally there is multi-faceted Trust Management (TM) system architecture. It is used for cloud computing marketplaces and related approaches [3], [4]. Also an additional approach based on the use of high-level identity verification policies expressed in terms of identity attributes, zero-knowledge proof protocols, and semantic matching techniques.It uses efficient cryptographic protocols and matching techniques to address heterogeneous naming [9], [10].

A. REPUTATION ATTACKS DETECTION FOR EFFECTIVE TRUST ASSESSMENT OF CLOUD SERVICES:

Talal H. Noor et al. [1], proposed the detection of reputation attacks to allow consumers to effectively identify trustworthy cloud services. The detection of reputation attacks involves several issues including

i) *Consumers Dynamism* where new users join the cloud environment and old users leave around the clock which makes the detection of feedback collusion a significant challenge,

ii) ii) *Multiplicity of Identities* where users may have multiple accounts for a particular cloud service1 which makes it difficult to detect whether a Sybil attack is performed because multiple identities can be used to give misleading information ,

iii) iii) *Attackers Behaviors* where it is difficult to predict when such malicious behaviorstake place either in a long or short period of time (i.e., strategic vs. occasional behaviors), and iv) *Consumers'Privacy* where the detection of attacks can make users subject to privacy breaches especially when the interactions involve sensitive information.

Talal H. Noor, presented novel techniques thathelp in detecting reputation attacks to allow consumers to effectively identify trustworthy cloud services. 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).

B. TRUST MANAGEMENT OF SERVICES IN CLOUD ENVIRONMENTS: OBSTACLES AND SOLUTIONS:

J. Yu et al [2] present an overview of the cloud service models and we survey the main techniques and research prototypes that efficiently support trust management of services in cloud environments. We present a generic

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

analytical framework that assesses existing trust management research prototypes in cloud computing and relevant areas using a set of assessment criteria. Open research issues for trust management in cloud environments are also discussed.

In this work, the main techniques, frameworks, and research prototypes on trust management in cloud computing and it's most relevant areas. They propose a generic framework that considers a holistic view of the issues related to the trust management for interactions in cloud environments.

In particular, they differentiate the trust managementperspectives and classify trust management techniques into four categories. Then compare thirty representative trust management research prototypes in cloud computing and the relevant research areas are using the proposed analytical framework. The framework consists of three layers and for each layer identify a set of dimensions (i.e., assessment criteria), which are used as a benchmark, to study these research prototypes. Several major cloud service providers are also compared.

Cloud Service modelhave three different models

1. including *Infrastructure as a Service*(IaaS),
2. *Platform as a Service* (PaaS),
3. *Software as a Service* (SaaS) based on different Service Level Agreements (SLAs) between a cloud service provider and acloud service consumer [Brandic et al. 2010; Grance2011].

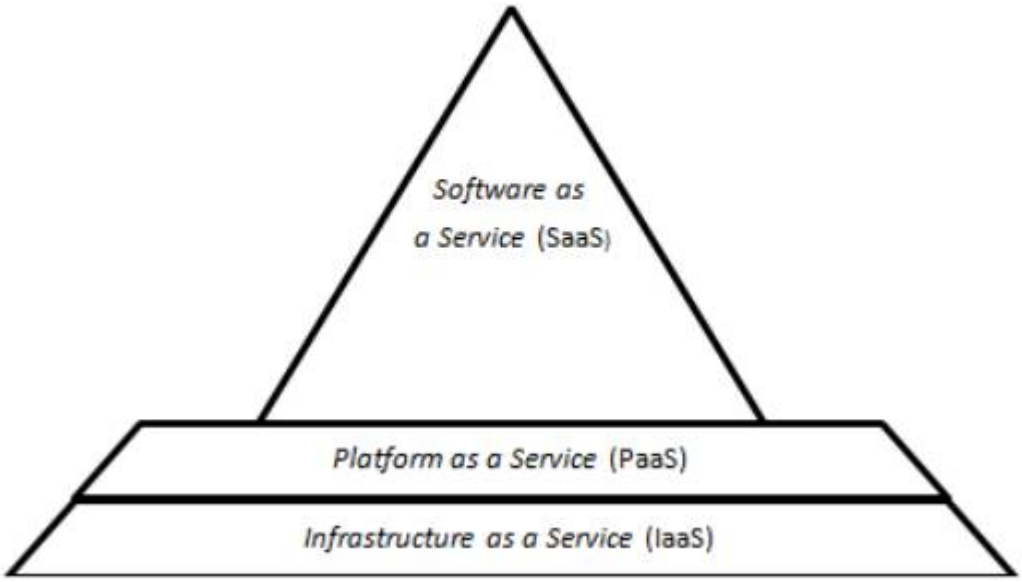

Fig.1. Cloud Service model

Figure 1 depicts the structured layers of cloud services:

- *Infrastructure as a Service (IaaS):* This model represents the foundation part of the cloud environment where a cloud service consumer can rent the storage, the processing and the communication through virtual machines provided by a cloud service provider. In this model, the cloud service provider controls and manages the underlying cloud environment, whereas the cloud service consumer has control over his/her virtual machine which includes the storage, the processing and can even select some network components for communication.
- *Platform as a Service (PaaS):* This model represents the integration part of the cloud environment and resides above the IaaS layer to support system integration and virtualization middleware. This allows a cloud service consumer to develop his/her own software where the cloud service provider provisions the soft-ware development tools and programming

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

– *Software as a Service (SaaS):* This model represents the application part of the cloud environment and resides above the (PaaS) layer to support remote accessibility where cloud service consumers can remotely access their data which is stored in the underlying cloud infrastructure using applications provided by the cloud service provider.

C. TOWARDS A TRUST MANAGEMENT SYSTEM FOR CLOUD COMPUTING:

In order to support customers in reliably identifying trustworthy cloud providers, this system propose a multi-faceted Trust Management (TM) system architecture for cloud computing marketplaces and related approaches. This system provides the means for identifying trustworthy cloud providers in terms of different attributes, e.g., compliance, datagovernance, information security.In this system, the first realization of their proposed TM systemusing the Consensus Assessment Initiative Questionnaire (CAIQ), initiated by the Cloud Security Alliance(CSA), as one of the sources of trust information. In particular, the proposed approach contributes to thechallenge of extracting trust information from CAIQs completed by cloud providers.

This paper provides the first realization of proposed TM system for cloud computing marketplaces. This system aims to reflect the multifaceted nature of trust assessment by considering multiple attributes, sources, and roots of trust. It also aims to support customers in identifying trustworthy services providers, as well as service providers in standing out. We contribute to the approach by extracting trust information from CAIQs completed by cloud providers. Also the implementation of the required components of the proposed TM system that is used to assess the trustworthiness of cloud providers based on the extracted trust information from the CAIQ.

In addition implementation includes an intuitive graphical interface for the cloud providers, allowing for convenient and faster input than the current approach for filling out the CAIQ. The graphical interface also allows consumers to navigate through the different domains and check thedetailed assessment results under each domain of the CAIQ.

CAIQ BASED TRUST MANAGEMENT:

The CAIQ includes 11 domains (e.g., Compliance (CO), Data Governance (DG)) which are aligned with the CSA guidelines for moving IT resources to the cloud. Each of the domains consists of several controls that resemble specific requirements to comply with the corresponding domain. There are,in total, 98 controls under 11 domains in the CAIQ framework. Each of those controls has one or morequestions that are designed to query about cloudproviders' capabilities and competencies regarding different attributes (e.g., audit planning, securitypolicies, risk assessments).

Domains	r	s	u	NA	N	Resulting Opinion (t, c, f)	Final Assessment (t, c, f); E
CO	16	0	0	0	16	(1,1,0.99)	
DG	16	0	0	0	16	(1,1,0.99)	
FS	9	0	0	0	9	(1,1,0.99)	
HS	4	0	0	0	4	(1,1,0.99)	
IS	75	0	0	0	75	(1,1,0.99)	
LG	4	0	0	0	4	(1,1,0.99)	(1,1,0.8953); E=1
OM	9	0	0	0	9	(1,1,0.99)	
RI	14	0	0	0	14	(1,1,0.99)	
RM	6	0	0	0	6	(1,1,0.99)	
RS	12	0	0	0	12	(1,1,0.99)	
SA	32	0	0	0	32	(1,1,0.99)	

Table I. Cloud Control Assessment for Cloud 'X': Best case

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

This system evaluated (i.e., CCA tool) using three cases (i.e., best, practical, customised). Shown in Table I and Table II.For the best case, it is assumed that the cloud provider `X' provides all positive assertions when filling out the CAIQ. In the practical (or real world) case, use assertions from the cloud-based service providers published in the STAR hosted by CSA. For the customised case, assume that the customers might have individual preferences on selecting domains (e.g., CO, DG, SA) when assessing the capabilities of cloud providers.

Domains	r	s	u	NA	N	Resulting Opinion (t, c, f)	Final Assessment (t, c, f);E
CO	15	1	0	0	16	(0.9375,1,0.99)	
DG	15	1	0	0	16	(0.9375,1,0.99)	
FS	7	0	2	0	9	(1,0.9403,0.99)	
HS	4	0	0	0	4	(1,1,0.99)	
IS	72	2	0	1	74	(0.973,1,0.9865)	
LG	2	2	0	0	4	(0.5,1,0.99)	(0.2239,0.9976,0.8953);E=0.2255
OM	4	3	0	2	7	(0.5714,1,0.99)	
RI	12	1	1	0	14	(0.9231,0.9891,0.99)	
RM	5	0	0	1	5	(1,1,0.99)	
RS	9	0	2	1	11	(1,0.9612,0.99)	
SA	22	0	0	10	22	(1,1,0.99)	

Table II.Cloud Control Assessment for Cloud `Y': Practical case

1. Best case: Table II shows the positive assertions in the evidence space and their resulting opinions (t; c; f). The last column of the table shows the final assessment based on the aggregation of all resulting opinions using the AND operator.
2. Practical case: The STAR repository has several sets of completed questionnaires from different cloud providers. We choose two sets of CAIQs completed by Cloud `A' and `B' to evaluate the identities of the cloud providers are anonymized due to STAR's usage restrictions.

D. PRIVACY- PRESERVING DIGITAL IDENTITY MANAGEMENT FOR CLOUD COMPUTING:

S. Pearson et al [10], Proposes this new computing paradigm is referred to as *cloud computing*.Examples of cloud computing applications are Amazon's Simple Storage Service (S3), Elastic Computing Cloud (EC2) for storing photos on Smugmug an on line photo service, and Google Apps for word-processing.Cloud services make easier for users to access their personal information from databases and make it availableto services distributed across Internet. Users have typically to establish their identity each time they use a new cloud service, usually by filling out an online form and providing sensitive personal information (e.g., name, home address, credit card number, phone number, etc.). This leaves a trail of personal information that, if not properly protected, may be misused. Therefore, the development of digital identity management (IdM for short) systems suitable for cloud computing is crucial.

An important requirement is that users of cloud services must have control on which personal information is disclosed and how this information is used in order to minimize the risk of identity theft and fraud. Another major issue concerning IdMin cloud platforms is interoperability. Interoperability issues range from the use of different identity tokens, such those encoded in X.509 certificates and SAML assertions, and different identity negotiation protocols, such as the client-centric protocols and the identity-provider centric protocols, to the use of different names for identity attributes.

An *identity attribute* encodes specific identity information about an individual, such as the social-security-number; it consists of an attribute name, also called identity tag, and a value. The use of different names for identity attributes, that we refer to as *naming heterogeneity*, typically occurs whenever users and cloud service providers use different vocabularies for identity attribute names.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

In this case, whenever a cloud service provider requests from a user a set of identity attributes to verify the user identity, the user may not understand which identity attributes he/she has to provide. To address the problem of privacy-preserving management of digital identity attributes in domains with heterogeneous name spaces, we propose a privacy-preserving multi-factor identity attribute verification protocol supporting a matching technique based on look-up tables, dictionaries, and ontology mapping techniques to match cloud service providers and clients' vocabularies. The protocol uses an aggregate zero knowledge proofs of knowledge (AgZKPK) cryptographic protocol to allow clients to prove with a single interactive proof the knowledge of multiple identity attributes without the need to provide them in clear.

III. ACKNOWLEDGMENT

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

IV. CONCLUSION

The paper presents the different trust management techniques like novel techniques that help in detecting reputation based attacks and allowing users tooeffectively to find trustworthy cloud services. Next establishment is 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. And also another one an availability model that maintains the trust management service at a desired level. Trust is one of the most concerned obstacles for the adoption and growth of cloud computing.

REFERENCES

[1] T. H. Noor, Q. Z. Sheng, and A. Alfazi, "Reputation attacks detection for effective trust assessment of cloud services," in Proc. 12th Int. Conf. Trust, Security Privacy Comput. Commun., 2013, pp. 469–476.
[2] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust management of services in cloud environments: Obstacles and solutions," ACM Comput. Surv., vol. 46, no. 1, pp. 12:1–12:30, 2013.
[3] S. M. Khan and K. W. Hamlen, "Hatman: Intra-cloud trust management for Hadoop," in Proc. 5th Int. Conf. Cloud Comput., 2012,pp. 494–501.
[4] S. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in Proc. 10th Int. Conf. Trust, Security Privacy Comput. Commun., 2011, pp. 933–939.
[5] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.
[6] 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. 3rd Int. Conf. Cloud Comput., 2010, pp. 244–251.
[7] Y. Wei and M. B. Blake, "Service-oriented computing and cloud computing: Challenges and opportunities," IEEE Internet Comput., vol. 14, no. 6, pp. 72–75, Nov./Dec. 2010.
[8] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrstedt, "A trust management framework for service-oriented environments," in Proc. 18th Int. Conf. World Wide Web, 2009, pp. 891–900.
[9] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in Proc. 2nd Int. Conf. Cloud Comput., 2010, pp. 693–702.
[10] 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, Mar. 2009.