Trust Evaluation in Cloud Computing: A Survey

Kavita Rathi, Shivani Taneja

Abstract— **Trust is doubtless reliance on character, ability, strength or truth of someone or something. Before opting the services of any Cloud Service Provider (CSP) there is a need to evaluate trustworthiness of various CSPs available in market. Consumer or user should cherry-pick the CSPs collection. However, determining the trust and selecting best service provider according to users' own requirements is an arduous task. This paper represents various trust evaluation models that are available in literature. User can establish trust with the help of any one of these models. But there is no universally accepted model. Since trust is an idiomatic term, evaluating trust remains a major issue while making headway towards Cloud Computing.**

Index Terms— **Cloud Computing, Cloud Services, Trust, Trust Evaluation, Trust Evaluation Models.**

I. INTRODUCTION

Cloud computing is one of the emerging technology which provides on-demand services over the internet on utility-like basis i.e. pay only for the services you are using. Although many formal definitions have been proposed in both academia and industry, the one provided by U.S. NIST (National Institute of Standards and Technology) [1] appears to include key common elements widely used in the Cloud Computing community: *"Cloud computing is a model for enabling 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 [1] "*. In Cloud Computing the word "Cloud" corresponds to a natural cloud or a black box i.e. user has no idea where processes are running or where the data is stored. The services are generally provided in various forms like Software as a service (SaaS), Platform as a service (PaaS) and/or Infrastructure as a service (IaaS).

A. *Infrastructure as a service (IaaS) [2]:*

Cloud Service Providers even provide infrastructures such as storage, networks, processing power and other resources. The concept of Virtualization is used in cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers [2]. The virtualization helps to create independent virtual machines that use the same hardware but they are isolated from each other. Examples of IaaS are Amazon's EC2, Microsoft Azure.

Manuscript received January 22, 2015.
Kavita Rathi, CSE Department, Deenbandhu Chhotu Ram University of Science and Technology, Murthal, India, 8930220999,
Shivani Taneja, CSE Department, Deenbandhu Chhotu Ram University of Science and Technology, Murthal, India, 8929307778,

B. Platform as a Service (PaaS) [2]:

Cloud Computing also provides platform in form of service. It enables the cloud consumers to develop their own applications on cloud. The major difference between SaaS and PaaS is that SaaS only hosts completed cloud applications whereas PaaS offers a development platform that even hosts in-progress cloud applications [2].Thus PaaS possess complete programming environment and tools in addition to development infrastructure. Example of PaaS includes Google AppEngine, Microsoft Azure.

C. Software as a Service (SaaS) [2]:

Cloud consumers can transfer their applications on a hosting environment. Application users can access these applications with the help of various clients such as web browsers. However Cloud consumer does not have control over the Cloud infrastructure. Multi-tenancy strategy is generally employed, where different cloud consumers' applications are hosted in a single logical environment on the SaaS cloud in order to optimize in terms of speed, security, availability, disaster recovery, and maintenance [2]. Examples of SaaS include SalesForce.com, Google Mail, GoogleDocs etc.

An organization can make use of cloud services if its own security services are not enough or if the organization does not want to invest much in hardware. Every service has its own security issues. Security issues are posing major hindrance in Cloud Computing. Transferring sensitive data or running software at someone else's hard disk using someone else's CPU may put off many. The multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges [2].

A Service Level Agreement (SLA) is the only legal document or we can say a negotiation between Cloud Service Provider and Cloud Consumer. It specifies the Customer needs, the level of services and security features that will be provided by Cloud Service Provider along with billing information. It also states customer duties and responsibilities, disaster recovery and problem management [3]. In spite of various benefits of Cloud Computing, it is still not accepted universally because of various security issues.

1.1 Security and Trust Issues in Cloud Computing [4]

Security Issues

Data security: It is a major concern while opting for cloud computing. It includes the risk of loss of data, unauthorized use of data or there may be the case where Cloud Service Provider does not provide adequate controls to protect data.

Access: Unauthorized or malicious users may gain access to confidential information. Even the Government in a

country may have legal rights to view stored data. Hence there is need of proper access control mechanisms to be implemented by Service Provider.

Customer Control over data: It is another major issue for cloud is to ensure that the customer has control over the lifecycle of their data, and in particular deletion, in the sense of how to be sure that data that should be deleted really are deleted and are not recoverable by a Cloud Service Provider [4]. The problem is severe in cloud as there can be many copies of the data, potentially held by different entities.

Various Attacks: Since Cloud Computing uses internet as a communication medium. Attacks such as Denial of Service (DoS), DNS attacks, Cookie Poisoning, Man in the Middle attacks may occur.

Availability and Backup [4]: It is not easy to guarantee adequate availability and backup. When data are hosted remotely in the cloud, backup is critical for businesses to recover in case of failure. But cloud providers enforcing resilience of their infrastructure might rely on seamless backups. This is a high security issue as these backups might be done without the customer's active informed consent and could lead to serious threats from an insider or external attacker.

Security concerns with the hypervisor

Cloud Computing rests mainly on the concept of virtualization. Hypervisor is generally defined as a controller popularly known as virtual machine manager (VMM) that allows multiple operating systems to be run on a system at a time, providing the resources to each operating system such that they do not interfere with each other. Virtual machines (VMs) are sandboxed environments and therefore completely isolated from each other. This assumption makes it safe for users to share the same hardware. However, this security can sometime break down, allowing attackers to escape the boundaries of this sandboxed environment and have full access to the host [4]

Trust Issues

Trust is a fascinating, complicated and multi-faceted concept [5].Everyone has its own perception about trust. If individuals have no idea why their personal information is being asked, or how and by whom it will be processed, this lack of control over data will finally lead to doubt and will ultimately result in distrust [4]. As a result, customers may restrain themselves from using cloud services. Establishing Trust between Cloud Service Provider and Cloud Consumer is a key criterion to adoption of Cloud services. Actually in Cloud Computing there is need of mutual trust between Cloud Service Provider and Cloud Consumer. For instance there may be some malicious users who may submit malicious code which could hamper working of cloud environment. On the other hand users lack control on sensitive data as they have no idea where the data is stored and how well it is protected [6]. Also a large number of Cloud Service Providers are available in market. In order to ensure security of data, it is required to establish trust on Cloud Service Provider before using its services. Since trust is a subjective and context-sensitive term so it is very difficult to select a trustworthy Cloud Service Provider [7]. In order to provide guidance to user to take up cloud computing, Cloud Security Alliance was formed. It devised a CAIQ (Consensus Assessments Initiative Questionnaire), a survey which has to be answered by Cloud Service Providers. It includes questions about security control and policies regarding services that are being provided. Thus it helps the cloud consumers to judge the security capabilities of various Service Providers and to select best one according to their requirements [8].

II. TRUST EVALUATION IN CLOUD COMPUTING

Trust is a subjective and context-sensitive term. There is no particular definition of trust. A trust can be defined as [9]:
"Trust is a mental state comprising: (1) expectancy – the trustor expects a specific behavior from the trustee (such as providing valid information or effectively performing cooperative actions); (2) belief - 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 - the trustor is willing to take risk for that belief."

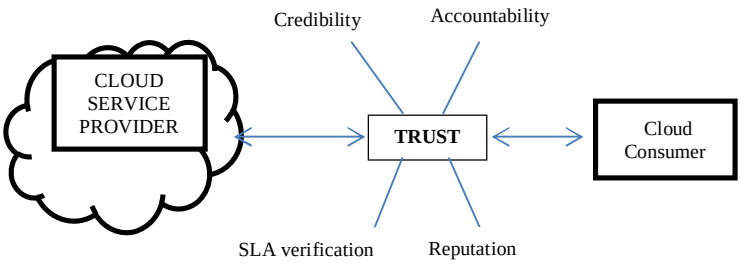

Figure 1: Trust Establishment

Figure 1 shows that trust can be established based on various factors such as credibility or accountability of Service Provider, SLA verification, Reputation of Service Provider in market and many more. Here the trustor is 'Cloud Consumer' and the trustee is 'Cloud Service Provider'

Due to availability of large number of Cloud Service Providers, it is necessary to establish trust on Service Providers before transferring sensitive data and using its services. A large number of trust evaluation models have been proposed till now to evaluate trustworthiness of Service Provider but there is no standard trust evaluation model in Cloud Computing.

A. Prevalent Methods for trust establishment [10]

SLAs: A Service Level Agreement (SLA) is the only legal document signed between Cloud Service Provider (CSP) and Cloud Consumer. Customer monitors SLA violations and ask the providers for compensation. However the compensation clauses in SLAs are written in such a way

that the customers are solely able to apply for compensation (e.g., service credits) in case of SLA violation. This problem arises for not having standardized SLAs for the stakeholders in Cloud computing marketplace.

Measuring & Ratings: Cloud Service Providers are rated based on a questionnaire that needs to be filled in by current Cloud Consumers. Consumer feedbacks are combined with technical measurements in order to determine trustworthiness of Cloud Service Providers.

Self-assessment Questionnaires: The CSA (Cloud Security Alliance) has proposed a detailed questionnaire called the CAIQ (Consensus Assessment Initiative Questionnaire).This questionnaire has to filled by every Cloud Service Provider However, the CSA working group does not provide any metric to evaluate CAIQ. This is necessary for comparing the potential Cloud Service Providers based on the answered assessment questionnaire stored in the STAR (Security, Trust & Assurance Registry)[10].

These methods are either considering technical and functional features or the user feedback for establishing trust on Cloud Service Providers. However, there is a need of trust evaluation framework where all these methods or trends can be considered complementary to support the consumers in evaluating the providers and selecting the most trustworthy provider [10]. Section 2.2 describes in brief various trust evaluation models.

B. Proposed Models

The main focus of this paper is to discuss various trust evaluation models. Trust can generally be categorized into Direct Trust and Indirect Trust. Direct trust is established through past experience or satisfactory direct interaction with a service provider. On the other hand indirect trust about a Cloud Service Provider is established by a good recommendation from someone familiar or trusted third parties [10].

Author/Title	Description
Wejnjuan Fan, Harry Perros A Reliability-based Trust Management Mechanism for Cloud Services [11]	A trust management framework for Cloud Computing environment and filtering of feedbacks based on consistency and similarity between them, in order to differentiate between honest and dishonest feedbacks. Thus it helps the new users to select a trustworthy CSP based on feedbacks received from other users.
Z. Raghebi, M. R. Hashemi A New Trust Evaluation Method based on reliability of customer feedback for cloud computing[12]	In this method each new customer can determine its trust level using past experience of previous customers of the cloud service. This method consists of two steps. In first step, similarity in common services used by two customers is evaluated. In second step all the services that the customer has rated are compared with majority of feedbacks. The trust can be evaluated based on these two parameters.
Sarbjeet Singh, Deepak Chand Trust Evaluation in Cloud based on Friends and third Party's recommendations[13]	This model takes into consideration viewpoints of three different parties. Final value of trust on a service provider is calculated based on users past experience with service provider, friends and trusted third party's recommendations. It did not consider the change in value of trust with time.
Dehua Kong, Yuqing Zhai, Trust based recommendation system in service-oriented cloud computing (TRSC)[14]	There are three main modules - information management, trust computing and cloud service management. The information management module manages trust relationships between cloud service users and ratings of cloud services rated by cloud service users. The cloud service management module monitors the registered cloud services. The trust computing module computes trust values and provide users with a list of services that can satisfy their requirements. Here trust value is combination of both direct and indirect trust.
S.Habib, V. Varadharajan and M. Muhlhauser A Trust-aware framework for evaluating security controls of Service Providers in Cloud Marketplaces[15]	The proposed framework evaluates and verifies the security controls as published by cloud providers. Hence it helps consumers to select a trustworthy service provider. The framework depends on the notion of hybrid trust which is a combination of hard and soft trust. Hard trust is derived from SLA's validation whereas Soft trust is derived from past experience.
Ayesha Kanwal et al. Assessment criteria for Trust models in Cloud Computing[16]	The proposed assessment criteria help the enterprise to select which trust model to be used. It helps customers to evaluate benefits and weaknesses of trust models based on various parameters such as data integrity, data control and ownership, model complexity, detection of untrusted entities, process execution control, quality of services attributes and dynamic trust update and logging.
Q.Guo et al. Modeling and Evaluation of trust in Cloud Computing environments[17]	This work includes an extensible trust evaluation module named ETEC. It includes a time-variant comprehensive evaluation method for expressing direct trust and a space-variant evaluation method for calculating recommendation trust.

N. Iltaf, A. Ghafoor A fuzzy based credibility evaluation of recommended trust in pervasive computing environment[18]	The proposed model considers indirect trust computation. It uses fuzzy approach to measure the credibility of recommendations based on content of recommendations. In the end, a single recommended trust value is computed for the entity. It does not take into consideration direct trust.
W. Li, L. Ping Trust Model to enhance security and interoperability of cloud environment [19]	It is a domain-based trust evaluation model. A trust agent is associated with each domain. Each client stores or maintains a customer trust table. Agents stores and maintains a domain trust table. Trust decision is based on both direct as well as recommended trust.
S.Wang et al Reputation Measurement Of Cloud Services based on Unstable Feedback Ratings[20]	The proposed model is based on feedback ratings. The trust vector consists of Expected value, Entropy value and Hyper-Entropy value. Fuzzy set theory is used to calculate the reputation scores of Cloud services.
C.Qu , R. Buyya A Cloud Trust Evaluation System using hierarchical fuzzy inference system for service selection.[21]	The proposed system consists of various components such as web interface through which users can specify even their vague preferences in linguistic phrases, discovery service module which retrieves services based on past from repository, trust evaluation service module which evaluates trust and a cloud benchmark service which monitor the performances of clouds.
S. Ding et al. Combining QoS prediction and customer satisfaction to solve cloud service trustworthiness evaluation problems[22]	This model is based on the fact that trustworthiness can be evaluated by both objective measurement and subjective perception. The trust value includes customer satisfaction or perceived ratings along with Quality of Service values.
X. Li, J.Du Adaptive and attribute-based trust model for service level agreement guarantee in Cloud Computing[23]	The proposed model specifies an attribute based trust management scheme for SLA guarantee and an adaptive model for measuring multi-dimensional trust attributes.
F. Xie et al. A Risk Management Framework for Cloud Computing[24]	The proposed framework consists of various components that are used to establish trust between cloud users and cloud service providers. It consists of user requirement self-assessment, cloud service providers desktop management, risk assessment, third-party agency review and continuous monitoring.
S.Wang et al. Towards an accurate evaluation of quality of cloud service in service-oriented Cloud Computing[25]	Proposed approach consists of three modules. First module is used to evaluate the performance of cloud services according to cloud users' preferences by using fuzzy approach. Second module is used to compute uncertainty in Quality of Service. Third module synthetically evaluates Quality of Service by using fuzzy control based on results of first two modules.

Thus we can see various trust evaluation models have been proposed till now. They are either based on direct trust (direct interaction with service provider in past), indirect trust (good recommendation from peers or third party) or hybrid i.e. final trust value is combination of both direct and indirect trust. Every model has its own advantages and limitations. Certain assessment criteria have also been proposed to choose an efficient trust evaluation model [16].

III. CONCLUSION AND FUTURE WORK

This paper represents various trust evaluation models. Some models consider past experience of user as a base for evaluating trust. Other common criterion for evaluating trust is based on feedbacks or friend's recommendation for a Service Provider. Some of the models have consider both the factors i.e. feedbacks as well as past experience with the Service Provider to find the trust value. Fuzzy based approach is also used to measure credibility of recommendations based on their content. Using Fuzzy logic allows the customer to specify even their obscure requirements. However, trust may corrupt with time. There are only few models which are considering time as a factor for establishing trust. Although various trust evaluation models have been proposed yet there is a need of more efficient model to help consumers while choosing the services. The scenario where two or more Cloud Service Providers are inter-connected if there is high traffic, in that case trust establishment is more complex. More research needs to be done in this regard.

REFERENCES

[1] P. Mell and T. Grance, "Draft nist working definition of cloud computing - v15," *21. Aug 2009*, 2009.

[2] Tharam Dillon et al., "Cloud Computing: Issues and Challenges" *in proceedings of 24th IEEE International Conference on Advanced Information Networking and Applications*, 2010, pp. 29-33.

[3] Balachandra Reddy Kandukuri et al., "Cloud Security Issues" *IEEE International Conference on Services Computing*, 2009, pp. 517-520.

[4] Siani Pearson, Azzedine Benameur,"Privacy, Security and Trust Issues Arising from Cloud Computing" *in proceedings of 2nd IEEE International Conference on Cloud Computing Technology and Science*, pp. 696-702.

[5] A. Charabarty, *Grid Computing Security*. Springer-Verlag Berlin Heidelberg, 2007

[6] Tian li-qin, LIN Chuang, "Evaluation of User Behavior Trust in Cloud Computing" *IEEE International Conference on Computer Application and System Modeling (ICCASM 2010)*, 2010, pp. 567-572.

[7] Ayesha Kanwal et al. "Assessment Criteria for Trust Models in Cloud Computing" *in proceedings of IEEE International Conference on Green Computing and Communications*, 2013,pp. 254-261

[8] Cloud Security Alliance (CSA), "Consensus Assessments Initiative Questionnaire," https://cloudsecurityalliance.org/media/news/consensus-assessments-initiative-questionnaire-caiq-v-3-review/ Accessed Jan 15 2015.

[9] Jingwei Huang* and David M Nicol, "Trust mechanisms for cloud computing" *Journal of Cloud Computing: Advances, Systems and Applications*, 2013, 2:9.

[10] Habib *et al.,* "Trust as a facilitator in cloud computing: a survey" *Journal of Cloud Computing: Advances, Systems and Applications*, 2012, 1:19.
[11] Wejnjuan Fan, Harry Perros, "A Reliability-based Trust Management Mechanism for Cloud Services" *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*,2013, 1581-1586.
[12]Z. Raghebi, M. R. Hashemi, "A New Trust Evaluation Model based on Reliability of Customer Feedback for Cloud Computing", *National CSI computer conference, Tehran, Iran*, 2013.
[13] Sarbjeet Singh, Deepak Chand ,"Trust Evaluation in Cloud based on Friends and Third Party's Recommendations" *in proceedings of IEEE International Conference on Recent Advances in Engineering and Computational Sciences* , 2014.
[14] Dehua Kong, Yuqing Zhai, "Trust based recommendation system in service-oriented cloud computing" *in proceedings of IEEE International Conference on Cloud Computing and Service Computing*, 2013, pp. 176-179.
[15] S.Habib, V. Varadharajan and M. Muhlhauser , " A Trust-aware Framework for Evaluating Security Controls of Service Providers in Cloud Marketplaces" , *in proceedings of IEEE Conference on Trust, Security and Privacy in Computing and Computations*,2013, pp.459-468
[16] Ayesha Kanwal et al. "Assessment Criteria for Trust Models in Cloud Computing" *in proceedings of IEEE International Conference on Green Computing and Communications*, 2013,pp. 254-261.
[17] Q.Guo et al. "Modeling and Evaluation of Trust in Cloud Computing Environments"*3rd IEEE International Conference on Advanced Computer*, 2011, pp. 112-116.
[18] N. Iltaf, A. Ghafoor, "A fuzzy based credibility evaluation of recommended trust in pervasive computing environment" in *10th Annual IEEE CCNC*, 2013, pp. 669-672.
[19] W. Li, L. Ping. "Trust Model to Enhance Security and Interoperability of Cloud environment" *CloudCom2009, LNCS 5931*, 2009, pp. 69-79
[20] S.Wang et al. "Reputation Measurement of Cloud Services based on Unstable Feedback Ratings" *IEEE International Conference on Parallel and Distributed Systems*, 2013,pp. 474-479.
[21] C.Qu , R. Buyya , " A Cloud Trust Evaluation System using Hierarchical Fuzzy Inference System for Service Selection" *IEEE Conference on Advanced Information Networking and Applications*, 2014,pp.850-857.
[22] S. Ding et al.,"Combining QoS Prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems" *Knowledge-Based Systems 56*, 2014, pp.216-225.
[23] X. Li, J.Du, "Adaptive and attribute-based trust model for service-level agreement guarantee in cloud computing" *IET Inf. Secur.*, 2013, Vol.7, Iss. 1, pp. 39-50.
[24] F. Xie et al., "A Risk Management Framework for Cloud Computing" *in proceedings of IEEE CCIS*, 2012, pp. 476-480.
[25] S.Wang et al., "Towards an accurate evaluation of quality of cloud service in service-oriented cloud computing" *Springer Science+Business Media LLC*, 2012, pp.283-291

Prof. Kavita Rathi, CSE Department , Deenbandhu Chhotu Ram University of Science and Technology, Bachelors and Master's Degree in the field of Computer Science and Engineering. She has keen interest in the area of Cloud Computing, and has published several papers in National and International conferences and journals. Prof. Kavita Rathi has more than five years of experience in teaching undergraduate as well as postgraduate students. She has attended several workshops and faculty development programs.

Shivani Taneja, Master of Technology, Computer Science and Engineering, Student, Deenbandhu Chhotu Ram University of Science and Technology, Murtha l, Sonipat . Area of Interest: Cloud Computing