Research on trust issues in cloud computing

Lilei Lu[1,*], *Zhaohui* Li[2] , *Shukun* Wu[1], and *Yanhong* Shang[1]

[1]Department of Computer Science, Tangshan Normal University, 063000 Tangshan, China
[2]Department of Resource Management, Tangshan Normal University, 063000 Tangshan, China

Abstract. Although cloud computing has some eminent advantages such as low cost, resource elasticity, yet the highly dynamic, distributed and opaque nature of cloud services makes it a meaningful challenge to establish and manage trust between cloud service providers and consumers. Based on this background, this paper first describes the common concepts and classifications of trust issues and trust models, then generalize trust issues in cloud computing based on the research of existing work, next enumerates typical trust evaluation models from several different perspectives in cloud computing. Finally, conclusions including several potential trends are proposed for the future work.

1 Introduction

The most attractive features of cloud computing include low cost, reliability, availability, service flexibility, etc. [1]. Besides its benefits, cloud computing also confronts some challenging issues such as security and privacy of the data stored in the cloud [2]. On the one hand, cloud computing requires enterprises and individuals to transfer part or all of the control of the computing resources to cloud service providers (CSP) [3]. On the other hand, the cloud service provided usually consists of multiple service components, which are hosted in distributed systems across the globe and managed by multiple parties [4]. Although it is convenient to monitor and access data in terms of cloud-centered data models, there still exists the risk of data theft. That means, cloud computing makes organizations and individuals who adopt its service lose control over the data that is traditionally maintained within it, which can bring some new security management issues. With more and more enterprises start using cloud computing, these cloud security issues become important and cannot be ignored.

Trust has been regarded as a measurable belief that can help make trustworthy judgments. It was originally employed to establish relationships among humans in the social sciences. Since trust has many soft security properties such as reliability, dependency, confidence, honesty, belief, trustworthiness, security, capacity, now it forms an essential component of security mechanism in distributed computing environment[5]. This means that trust has become a way to solve security problems as an essential security relationship in the distributed network environment[6].

Trust issue is also one of the most concerned barriers to the adoption and development of cloud computing[7,8]. In the cloud computing environment, mutual trust between cloud

* Corresponding author: lulilei@tstc.edu.cn

service consumers and service providers are necessary [8]. It has been considered to be one of the most important factors to realize security, which is also essential to enhance the trustworthiness of cloud service providers and their services [9]. In the distributed cloud computing environment, cloud services with the same function can be provided by many providers, therefore, to select trustworthy cloud services has become an important concern for cloud consumers in the cloud market [10]. Whether cloud consumers trust the providers is significant, which has become a research hotspot in cloud security domain [9].

Based on the above background, Section 2 describes the definitions and explanations related to trust and common classifications of trust issues and trust models. Section 3 presents an overview of trust issues in cloud computing based on the existing research work. Section 4 enumerates typical trust models in cloud computing from several different perspectives. Section 5 concludes and proposes several potential trends for future work.

2 Overview of the basic issues of trust

2.1 Trust related concepts

Trust is a relatively complex concept that has different meanings in different contexts of scenarios [11]. Since the 1960s, many experts and scholars have successively put forward their respective opinions from different perspectives of disciplines and made different interpretations or definitions, concerning sociology, psychology, philosophy, economics, management, computer science, etc.. But until now there is no unified definition of trust. Next we first depict two related concepts, then present the descriptive definitions of trust and trustworthiness separately.

Definitions 1 Trustor: it refers to the subject who actively generates a sense of trust in trusting relationship, usually concerning people or various agency procedures.

Definition 2 Trustee: it refers to the object or entity that is trusted by a trustor in trusting relationship.

The definition of trust accepted by many researchers in computer science derived from the sociologist Diego Gambetta [12]: trust is a kind of subjective probability that one agency assesses another or a set of agents who will perform some particular behavior. The opinion of trust from Audun Jøsang [13] is that trust is a direct relationship between the two parties, separately referred to as a trustor and a trustee. Sibel Adali [14] considers trust as a relationship which may be symmetric or asymmetric between a trustor and a trustee. Lik Mui et al. [6] regard trust as the subjective expectation that one agent has about the future behavior of another based on their interactive histories. In computer science, it was Marsh that first proposed the concept of trust and formalized it as a computable concept [1,15], and first introduced the computable model of trust into the distributed Artificial Intelligence community. Integrating the above views and related literature, its descriptive definition is given as follows:

Definition 3 Trust: it is a kind of quantifiable and direct relationship between a trustor and a trustee, representing the subjective willingness or expectation of the trustor to the trustee who can perform some particular behavior in a particular context with potential risk.

Trustworthiness is another common concept in trust related domains. In some literatures, trust and trustworthiness are often used interchangeably without distinction [16]. In fact, trustworthiness tends to describe the trust based on objective facts. It is defined as follows:

Definition 4 Trustworthiness: it is an internal and dynamic attribute of the trustee and reflects the objective basis needed by the trustor to generate subjective trust in the trustee's ability.

It is easy to find that trust emphasize subjective perception of a trustor, while trustworthiness tends to focus on the objective factors.

2.2 Classifications of trust issues and trust models

Although trust has been formalized as a computable model, it still implies different things for different researchers. Even in the same domain, trust can be defined in different ways, which depends on the applications and methodologies used to calculate trust [17].

For the classification research of trust issues, quite a few scholars have made related investigations and generalization. Ries et al. [18] have made the survey of the concept of trust realized in different fields of computer science, and divided the existing work in general as follows:

(1) Trust modeling: it deals with the representation and calculation of trust values.

(2) Trust management: it focuses on the evidence collection and risk assessment.

(3) Making decisions: it is one component of trust management, which can also be viewed as one separate module because of its importance.

Trust modelling issues, as mentioned earlier, has been studied by many researchers in different application contexts. The common classifications of trust models are shown in Table 1.

Table 1. Common classifications of trust models.

Classification criteria	Type of indicators	Update or not	Online or not	Deployment architecture
Classification result	qualitative	dynamic	online	centralized
	quantitative	static	offline	distributed

3 Trust and its overall classification in cloud computing

3.1 Basic concepts in cloud computing

There are usually two types of agents, consumer agent and provider agent in service oriented systems [19]. In cloud computing environment, there are also two types of agents, which we call cloud service provider (abbreviated as CSP) and cloud service consumer, respectively (abbreviated as CSC). The main focus of this article is on the issue of trust between CSCs and CSPs, especially on how CSCs carry out the trustworthiness evaluation of CSPs and their cloud services. For ease of understanding, several common terms are defined respectively based on existing work in this section.

Definition 5 Cloud service (abbreviated as CS): it broadly refers to services such as infrastructure services, platforms, and software provided by all levels of service providers in cloud computing environments, typically including IaaS, PaaS, and SaaS.

Definition 6 Cloud service provider (CSP): it refers to the collective term of all levels of providers providing cloud services, which typically includes infrastructure service providers, platform providers, and software providers in cloud computing environment.

Definition 7 Cloud service consumer (CSC): it refers to cloud service user or users, ranging from large-scale organizations, small enterprises, developers to individual users.

Definition 8 Cloud service trustworthiness: it reflects the objective basis whether a cloud service provided by a CSP is trusted by a CSC in cloud computing environment.

3.2 Overall classification of trust models in cloud computing

Some scholars [12,20] suggest that trust issues in cloud computing can be divided into four subcategories, including: (a) how to define and evaluate trust based on the unique properties of the cloud computing context; (b) how to handle malicious recommendation information, which is important for the cloud computing environment because trust relationship is temporary and dynamic; (c) how to consider and provide different levels of service security according to the level of trust degree; (d) how to manage the change of trust with interaction time and context, and how to monitor, adjust and really reflect the dynamic change of trust relationship with time and space. According to this classification, the main content of this research belongs to the above type of (a).

For the trustworthiness evaluation model in cloud computing environment, there are typically two different perspectives derived from two different trustors, which are referred to as CSP oriented trust model and CSC oriented trust model, respectively. The two types of models have different trustees, whose trustworthiness needs to be evaluated, and their relationships are shown in Table 2.

Table 2. Overall classification of trust models in cloud computing.

Oriented object	Trustor	Trustee	Evaluation object
CSP oriented	CSP	CSC	CSC
CSC oriented	CSC	CSP	CSP

3.2.1. CSP oriented trust evaluation models

In cloud computing, the software and operating systems, or even the basic programming environment and network infrastructure provided by CSPs are used and operated directly by CSCs. Therefore, the impact and destruction of cloud resources derived from CSCs on software and hardware is more serious than that of Internet users using Internet shared resources. Whether user behavior is trustworthy and how to evaluate the trustworthiness of users' behavior is more important in cloud computing [8]. The CSP oriented trust evaluation models are exactly proposed and established in the above context, and this type of models is to evaluate the trustworthiness of the trustee CSC from the perspective of the CSP as a trustor, including the trustworthiness properties of the CSC itself and its feedback information. The target is to prevent the destructive behavior of malicious CSCs in order to preserve the interests of CSPs.

3.2.2. CSC oriented trust evaluation models

As mentioned earlier, cloud computing requires businesses and individuals to transfer part or all of the control of the computing resources to CSPs, which places the data at risk of being exposed or exploited. On the other hand, CSPs have the potential to violate commitments of security and privacy [21]. Thus, CSCs confront security threats from outside and inside of the cloud [22].

CSC oriented trust evaluation models are essentially the evaluation process of CSPs' trustworthiness for the interests of CSCs. Therefore, this type of model is to evaluate the trustworthiness of a trustee CSP from the perspective of a CSC as a trustor. The evaluation content concerns the trustworthiness attributes of the CSP itself and the cloud service provided, with the goal of aiding the CSC to select a more trustworthy CSP and its service.

In practice, there are several other perspectives used for classification of cloud service trust models. For example, according to the service model or business model of cloud

computing, the trust model can be divided into IaaS based, PaaS based and SaaS based trust evaluation models separately. From the perspective of evaluation content, the cloud service models include QoS (Quality of Service) based, SLA(Service Level Agreement) based, user behavior based trust models, and so on.

4 Typical trust models in cloud computing environment

Combined with the previous description as well as the research purpose of this article, this section outlines the existing trust models in cloud computing environment mainly from the perspective of evaluation content. Typical models are analyzed and briefly reviewed.

4.1 QoS based trust models

To select Web service in terms of QoS indicators has been adopted by many researchers. For Web services, QoS is usually used to describe the nonfunctional needs such as response time, availability, throughput, price, and so on [23]. The QoS approach in cloud computing has become a significant topic. Since many open challenges related to trust in cloud services need to be addressed, the QoS approach plays an important role to ensure that CSCs trust cloud services [23]. Nowadays, some scholars have proposed QoS based models for service trust computing or evaluation. And the QoS properties or its combination was taken as part of the evaluation indicators for the trustworthiness of cloud services.

Manuel [24] proposed a cloud computing trust model based on the QoS. This trust model can calculate the CSC's trust in the CSP based on the past credentials and current capabilities of the CSP. When calculating the trust value of the CSP credentials, four QoS properties are defined and quantified: Availability, Reliability, and Turnaround Efficiency and Data Integrity. These properties are considered as trustworthy attributes of CSPs and weighted according to given priorities to calculate the trust values. For example, the Availability of resources is defined as the ratio of the number of tasks served by that resource to the total number of tasks submitted to the resource during a period. The obvious feature of this trust model is the quantification of the qualitative properties of QoS.

Xiaoyong Li et al. [25] presented a trusted third party based service agent architecture for multi-cloud environment, in which T-broker serves as a middleware for cloud trust management and service matching. They propose a hybrid and adaptive trust model to calculate the overall trust in a service resource. Five trustworthy attributes of cloud services are proposed to calculate the trustworthiness of a certain resource, including node specification profile, average source usage information, average response time, and average task success ratio and the number of malicious access. Each of them is extended and defined based on the original QoS indicators.

Shuai Ding et al. [26] considered the fact that many trustworthiness evaluation issues include not only objective measurement but also subjective perception and design a framework called CSTrust to perform cloud service trustworthiness evaluation. The predicted value of QoS and user satisfaction estimation are combined in it. The authors suggested that many trustworthy attributes can be measured by QoS values such as Throughput, Failure Rate, Response Time. The common used attributes for cloud service trustworthiness consist of Availability, Performance, Security, Privacy, Maturation and Controllability.

Obviously, the QoS based trust models or frameworks above usually employ the attributes of QoS directly or their deformation as the objective basis of the trustworthiness evaluation of cloud services. However, few factors other than QoS considered may be subject to certain limitations. More comprehensive analyses focused on the cloud service context deserve deep investigation.

4.2 SLA based trust models

SLA (service level agreement) is a contract between a web service provider and consumers, in which service types, service quality, etc. are defined. In cloud computing environment, SLA can be viewed as a document of established business contract between CSC and CSP, which is significant for a CSC to use a CS.

The requirements for using SLA in cloud computing include [27]: (1) it presents the definite idea about cloud service provider; (2) it depicts a list of services (SaaS, PaaS and IaaS) that the provider will provide according to the complete description of each service, (3) a transparent SLA specifies the objective of the business level policy including the roles of CSPs and CSCs, (4) it concerns the policies regarding important security and privacy management, (5) it monitors service quality, performance, priorities and responsibilities from a service perspective; (6) it provides a transparent view to understand service management needs when cloud services fail.

Alhamad et al. [28,29] built a trust model to evaluate cloud services based on the conceptual framework of SLA which was proposed in previous work. The basic components include a SLA agent, a directory of cloud services, a CSC model and CSP entities. The SLA agent acts as the mediator between CSC and CSP. With the model, CSPs first need to release their services in the cloud service directory. The CSC utilizes discovery operations to find a list of CSPs that meet its requirements. This list is submitted to the trust management system, which filters out untrustworthy CSPs using reliability values and a SLA agent report. The list of trusted CSPs is sent to a SLA agent along with the detailed business objectives. When the CSC submits a CS request, waiting to obtain the ID and the detailed SLA agreement. If the CSC agrees to continue the contract, it is required to sign SLA using the SLA agent and start to contact with the CSP.

SLA based trust models can address the trustworthiness evaluation of CSs to some extent. However, traditional SLA trust management methods are not sufficient for complex cloud environments. The ambiguous terms and unclear technical specifications of SLA will lead to the difficulties of CSCs in identifying trustworthy cloud services [30].

4.3 User behaviour based trust models

Tianli Qin, Linchuang [8] proposed the trust evaluation method based on user behavior for cloud computing, which is a CSP oriented trust evaluation type. The trustees here, referred to as CSCs, include three types: normal cloud users who directly utilize cloud computing, enterprise cloud users who utilize not only local resources but also cloud computing functions to establish their own service industry, and enterprise users who only utilize enterprise services from enterprise services. The basic idea of the method of evaluating trust in user behavior is the divide-and-conquer strategy based on the hierarchical model. It is required to decompose the complex user behavior trust (UT) into a small sub trust (ST), then further decompose the behavior sub trust (ST) into a smaller data unit called behavioral trust evidence (BE), and finally combine it from the bottom to the top layers scientifically.

The trust evaluation method in which the user behavior is first decomposed and then combined, can help solve the uncertainty, subjectivity and ambiguity of the evaluation of user behavior in cloud computing. However, if trust in users is simply regarded as the behaviour trust, this can lead to limitation to some extent.

4.4 Trust management framework of trust as a service

Talal H.Noor [7] proposed a trust management framework of trust as a service (TaaS) from the perspective of CSCs. This framework uses a service oriented architecture (SOA) to deliver trust as a service. It distinguishes key issues of trust management in cloud environment, including the accuracy of trust results and evaluation and storage of trust feedback. Service trust assessment in existing research is usually centralized, whereas trust feedback comes from distributed trust participants. A trust model using a centralized architecture is prone to scalability and security problems. To address the above problems, the model used in the framework assesses the trustworthiness of cloud services and distinguishes between reliable and malicious trust feedback. It especially introduces the capacity of CSCs and Majority Consensus factors when calculating the trustworthiness of a CS. Additionally, it adopts a distributed trust feedback assessment and storage mechanism to allow distributed management of trust assessment and storage.

The TaaS framework analyzes and solves the source reliability problem of the data and overcomes the deficiencies of the centralized architecture, but there is still a performance optimization problem. Meanwhile, it lack of more comprehensive consideration of the trust relationship context.

5 Conclusions and future work

Combined with the previous analysis of existing work, it is easy to find that to evaluate the CSCs' trust in CSPs and their cloud services is a main challenge in recent years [31]. In the cloud service market, services with the same or similar functions are usually provided by multiple different CSPs, thus CSCs need to combine their needs to decide which CSP or CS is more trustworthy before they adopt the service [31]. Currently, although some different computational and evaluation methods or models have been proposed in cloud computing environment, it is far from sufficient. In practice, it is necessary to build certain guidelines and comprehensive evaluation models from the perspective of a trustworthy third party.

On the one hand, there still lack of general guidelines to be followed when modeling trust. Since one important task is to identify the various trustworthiness factors and their significance degrees of a cloud service, according to what criteria to effectively select the important factors or indicators should be one of the first job to be considered and addressed.

On the other hand, the investigation to the existing research work show that the proposed models or frameworks to evaluate the trustworthiness of a CSP or CS mainly focus on the analysis of QoS and SLA, while ignore comprehensive consideration and analysis of the cloud service context. For example, it is easy to ignore the willingness or preference of the CSC itself.

In addition, the information of existing models for trustworthiness assessment mainly rely on user feedback and lack of consideration of other information sources. Meanwhile, these models usually focus on concrete algorithms while lack of consideration of the versatility and scalability.

In conclusion, to form general guidelines and based on them to further build comprehensive trustworthiness evaluation models in different trust contexts are practical and significant in cloud computing environment.

The Natural Science Foundation of Hebei Province (Grant No. F2019105134), Science and Technology Plan Project of Tangshan, Tangshan Foundation Innovation Team of Digital Media Security (Grant No. 21130212D) , Science and Technology Project of Hebei Education Department (Grant No.ZC2021030), China.

References

1. A. Abdelmaboud, D.N.A. Jawawi, I. Ghani, A. Elsafi, and B. Kitchenham. Quality of service approaches in cloud computing: A systematic mapping study [J]. Journal of Systems and Software, 2015,101: 159-179.
2. A. Kanwal, R. Masood, U.E. Ghazia, M.A. Shibli, and A.G. Abbasi. Assessment Criteria for Trust Models in Cloud Computing [C]. CPSCom 2013: 254-261.
3. P.J. Ryan K L Ko, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui and B.S.L. Liang. TrustCloud: A Framework for Accountability and Trust in Cloud Computing [C]. Services (SERVICES), 2011 IEEE World Congress on IEEE, 2011.
4. S.M. Habib, Trust Establishment Mechanisms for Distributed Service Environments [D]. Darmstadt, German: der Technischen Universität Darmstadt, 2013: 1-184.
5. D. Sun, G. Chang, L. Sun, and X. Wang. Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments [J]. Procedia Engineering, 2011. 15: 2852-2856.
6. Lik M., Mojdeh M., Ari H. . A Computational Model of Trust and Reputation [C]. Proceedings of the 35th Hawaii International Conference on System Sciences,2002:1-9.
7. Q.Z.S. TALAL H. NOOR. Trust as a Service-A Framework for Trust Management in Cloud Environments [C]. WISE, 2011: 8.
8. L.C. Tian Li-qin. Evaluation of User Behavior Trust in Cloud Computing [C]. ICCSM, 2010.
9. R.A.R. Shaikh and M. Sasikumar. Trust model for a cloud computing application and service [C]. IEEE International Conference on Computational Intelligence & Computing Research, 2012:1-4.
10. S.M. Habib, V. Varadharajan, and M. Muhlhauser. A Trust-Aware Framework for Evaluating Security Controls of Service Providers in Cloud Marketplaces [C]. TRUSTCOM, 2013:459-468.
11. Yan, K. ; Cheng, Y. ; and Tao, F. . A trust evaluation model towards cloud manufacturing [J]. International Journal of Advanced Manufacturing Technology,2016, 84(1-4):133-146.
12. Gambetta, D. . Can we trust trust? [EB/OL]. Trust: making and breaking cooperative relations, Department of Sociology, University of Oxford, Chapter13, 2000:213-237. *http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf.*
13. Jøsang Audun. Trust and Reputation Systems[J]. Springer LNCS 4677, 2007:1-38.
14. Adali, Sibel. Modeling Trust Context In Networks[M]. New York:Springer,2013:1-60.
15. Marsh, Stephen Paul. Formalising Trust as a Computational Concept [D]. Stirling: University of Stirling,1994:1-184.
16. Lu,L.;Yuan,Y. A Novel TOPSIS Evaluation Scheme for Cloud Service Trustworthiness Combining Objective and Subjective Aspects. J.Syst.Softw.2018,143,71–86.
17. Momani, Mohammad. Bayesian Methods for Modeling and Management of Trust in Wireless Sensor Networks [D].Sydney: University of Technology, Sydney, 2008:1-185.
18. Sebastian Ries,et al.. A Classification of Trust Systems [C]. On the Move to Meaningful Internet Systems 2006:OTM 2006 workshops pt.1. 2006:894-903.
19. X. Su, M. Zhang, Y. Mu, and Q. Bai. A robust trust model for service-oriented systems [J]. Journal of Computer and System Sciences, 2013. 79(5): 596-608.

20. S. Subashini and V. Kavitha. Review: A survey on security issues in service delivery models of cloud computing [J]. Journal of Ne twork & Computer Applications, 2011. 35(1): 1-11.
21. R. Trapero, J. Luna, and N. Suri. Quantifiably Trusting the Cloud: Putting Metrics to Work [J]. IEEE Security & Privacy, 2016. 14 (3): 73-77.
22. M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, and A. Rabkin. A view of cloud computing [J]. Communications of the ACM, 2010. 53(4): 50.
23. S.-Y. Lin, C.-H. Lai, C.-H. Wu, and C.-C. Lo. A trustworthy QoS-based collaborative filtering approach for web service discovery [J]. Journal of Systems and Software, 2014,93: 217-228.
24. P. Manuel. A trust model of cloud computing based on Quality of Service [J]. Annals of Operations Research, 2015. 233(1): 281 -292.
25. X.Y. Li, H.D. Ma, F. Zhou, and W.B. Yao. T-Broker: A Trust-Aware Service Brokering Scheme for Multiple Cloud Collaborative Services [J]. Ieee Transactions on Information Forensics and Security, 2015. 10(7): 1402-1415.
26. S. Ding, S.L. Yang, Y.T. Zhang, C.Y. Liang, and C.Y. Xia. Combining QoS prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems [J]. Knowledge-Based Systems, 2014. 56: 216-225.
27. S.B.D.e. al. Service Level Agreement Assurance in Cloud Computing - A Trust Issue [J]. International Journal of Computer Science and Information Technologies, 2014,5(3): 2899-2906.
28. M. Alhamad, T. Dillon, and E. Chang. SLA-Based Trust Model for Cloud Computing [C]. 2010 13th International Conference on Network-Based Information Systems, 2010: 321-324.
29. M.e.a. Alhamad. Conceptual SLA framework for cloud computing. [A]. 4th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2010) [C], IEEE. 2010: 606-610. 2010.
30. Q.Z.S. TALAL H. NOOR. Trust Management of Services in Cloud Environments-Obstacles and Solutions [J]. Acm Computing Surveys, 2013: 1–35.
31. S.M.e.a. Habib. A Framework for Evaluating Trust of Service Providers in Cloud Marketplaces [C]. SAC '13: Proceedings of the 28th Annual ACM Symposium on Applied Computing, ACMSAC, ACM. 2013: 1963-1965.