International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.1, No.3, August 2012, pp. 116~123
ISSN: 2089-3337

Building trust into cloud

Wenjuan FAN*, Shanlin Yang*, Jun Pei*, He Luo*
* School of Management, Hefei University of Technology

Article Info

Article history:

Received July 02th, 2012
Accepted July 28th, 2012

Keyword:

cloud system,
cloud trust issues,

ABSTRACT

In this paper, a three-layer trust conceptive framework for cloud is introduced, which is including both the validity of the “hard trust” guaranteed by security mechanisms and technical devices, and “soft trust” ensured by social, legal and human factors. In addition, the trust relationship between consumers and cloud venders is considered in our framework. Through the combination and integration of the three layer trust in the framework, the gap between these trust factors can be bridged.

Corresponding Author:

Wenjuan Fan,
School of Management,
Hefei University of Technology,
193 Tunxi Road, Hefei City, Anhui Province, China
Email: sahala-18@163.com

1. INTRODUCTION

Despite the highly discussion and impressing fast development of cloud computing over the past few years, the characteristics of cloud that are benefit to every participant meanwhile arouse a lot of worry in some respects. As the result of the trust consideration to cloud, it is not unusual that currently quite a number of potential users, such as the small and medium business (SMB) which are increasingly realizing the business merits of cloud computing [1], are reluctant to believe the cloud can offer them trustworthy enough services.

Therefore, trust in cloud is increasingly grabbing the intention of most stakeholders, especially in public cloud due to its highly open environment to external users. Actually, cloud users are inevitably confronted the potential risk of putting their data and information involved different degrees of sensitivity into the remote data center of cloud service providers or a third party that providing cloud environment out of control of users for specific physical resources [2][3][4].

Trust related problems usually first go down to the security and privacy issues which are the prerequisites of particular security mechanism, that is, guarantees of “hard trust”, like access control, data segregation, network monitoring, etc. On the other hand, the “soft trust” is subtly impacting the trust relation from users to the cloud services, which is related to the cloud provider’s reputation or brand to some extent [5]. Furthermore, because most peers in cloud are temporal, dynamic and mobile entities which forms a potential threat to the trust relation among all the entities involved in the cloud service system, so that the trust relationship establishment between different entities, trust maintenance, trust propagation, etc, may affect the stability and trustworthiness of the whole system. With respect to the current practices of different cloud models, lack of synthesis and systematic trust managemnt framework is an unavoidable obstacle impeding fast development of cloud service system to mature.

Based on the existing research on the trust mechanism in information and network service domain, a three-layer trust conceptive management framework applied in cloud to realize the trustworthiness guaranteed cloud is built in this paper. The remainder sections are arranged as follows. In section two the background to trust notion and research in networking and existing computation paradigms is reviewed. Section three lists and analyzes trust issues in cloud. In section four the conceptive cloud trust framework is introduced. In section five we discuss the trust management framework in cloud computing environment. The paper is concluded in section six.

2. Background and Related Work

2.1. Background to trust notion

Trust has aroused much attention from different domains of scholars, such as psychology, sociology, economics, philosophy, computer science, and management science [6], while gained little consensus. There is no general definition of trust, and the definitions are usually discipline-specific [7]. Broadly speaking, trust means an act of faith; confidence and reliance in something that's expected to behave or deliver as promised [8]. The concept of trust adjusted to the case of two parties involved in a transaction can be described as follows: "An entity A is considered to trust another entity B when entity A believes that entity B will behave exactly as expected and required. The notion of trust in an organization could be defined as the customer's certainty that the organization is capable of providing the required services accurately and infallibly [9].

Based on the notion of trust, there are some other important issues that have been investigated by many researchers. Existing research on trust are mainly involving three categories of topics: Firstly, which factors contribute to and affect the system trustworthiness and trust relationship under different trust scenarios, and how they are acting on the trust [4][5][9][10]. Such research questions are the bases of trust issues analysis thus give a clear insight into the trust question analysis. Secondly, how the trust relationship are established, maintained and destroyed, which are performed as different trust models, mechanisms or framework that can ensure the trust in specific application contexts [11][12][13][14]. Thirdly, how trustworthiness can be measured by a variety of trust models, i.e., methodologies about trust measurement to evaluate, analyze, and decide the degree of system trustworthiness [15][16].

Further speaking, many scholars have proposed their trust models measuring the trustworthiness and managing the trust relationship. The most common one is reputation based trust management mechanisms, which have been widely employed in online electronic communities and distributed environments [17], i.e., used to provide a basis for the choice of transaction items and partners in service provision. The basic idea is to let participating nodes rate each other trust level, for example after the completion of a transaction and use the aggregated ratings about a given node to derive a trust or reputation. Most of them largely depend on feedback for the reputation computing. Reputation is categorized into three types [18]: positive reputation, negative reputation, or a combination of both. Relying only on a positive reputation or a negative reputation is incomplete for generating a reputation of a node in a comprehensive way.

2.2. Trust research in computing and networking service paradigms

Trust is not a new topic in most distributed computing systems, such as P2P computing, grid computing and wireless network computing, etc, as in those computing paradigm, nodes can freely join and leave the system and the group membership is very dynamic[19], thus the resources should be shared under secured trust management mechanism. Different distributed environments have different security areas in which many researchers have been bringing the study of the trust mechanism into distribution [20].

It is all known that trust issues have been discussed broadly and deeply in the ad hoc network, wireless sensor network and some other network service systems, and the trust management system is becoming mature. While the security problems in cloud have been paid attention to by some investigators, who mainly fall into two categories: 1) those who analyze and discuss a variety of trust issues unique in the cloud which are rarely considered before in traditional trust scenarios, and 2) those who mainly focus on the "hard trust" issues, while make not much effort on the "soft" part.

Besides, most work has no overall and systematic view of the trust-related problems and just gives some solutions and models to handle specific issues. Although the trust related problems have grabbed much attention and concerns of the researcher and developers, the security based trust is still a key problem have to be addressed not only through the technical devices but also by management mechanism, e.g., Dimitrios Z. et al [9] think that security in a cloud environment requires a systemic point of view, from which security will be constructed on trust, mitigating protection to a trusted third party. Other researchers have realized the specific part of particle problems impacting trust to cloud computing. Khaled M. Khan and Qutaibah Malluhi [8] hold that trusting cloud computing might differ from trusting other systems, but any new technology must gradually build its reputation for good performance and security earning users' trust over time. Ilkka Uusitalo et al [5] have highlighted main observations from an interview study on experts' views on trust in cloud services, and found that the most important factor affecting perceived trust in cloud services is Brand, including such sub-aspects as reputation, image, history and name of the CSP (Cloud service providers).

Referring to the specific trust mechanism design and innovation, researchers have gain a lot of chiesvemnt Kai H. and Deyi L. [21] suggest using a trust-overlay network over multiple data centers to implement a reputation system for establishing trust between service providers and data owners. Joshua S. et al. [22] propose a cloud service that generates integrity proofs for customers to verify the integrity and access control enforcement abilities of the cloud platform that protect the integrity of customer's application VMs. S. Subashini and V. Kavitha [1]discuss the various security issues in different service delivery models and investigate an integrated security model targeting different levels of security of data for a typical cloud infrastructure. Flavio L. and Roberto D. P. [23] have proposed an advanced cloud protection system (ACPS) for cloud protection that can monitor both guest and middleware integrity.

3. Cloud-specific trust issues analysis

Extending the research of Frank J. K [24], which divides the trust in cloud environment into trust in the service provider's platform and trust in the information owner's domain, and the combination of the two parts forms the "virtual environment trust", it can be inferred that the cloud trust comes down to two basic categories of issues: service trustworthiness under uncertainty and entity trust management issues. And the former one is referring to the technical, strategic and policy guarantee to the normal operation of cloud system provided by the cloud vendors, while the latter one is referring to the trust relationship management among different service roles (entities) in cloud.

3.1. System trustworthiness under uncertainty

Traditional researches on trustworthiness of information service system most concentrate on the functionality and security of specific system units. Nevertheless, it is service capacity that users purchase and really concern in cloud computing service system, instead of a fixed hardware resource [25]. In addition, the physical resources are logically virtualized thus not bind to specific system units. So in cloud computing environment, the system trustworthiness is much complex than before, which should establish trust that is distinct for the virtual environment and separate from the hosting platform [26]. Therefore, when considering the cloud system trustworthiness, it will be not about a specific system unit, instead it is the virtualized system infrastructure, which is not only in the underlying physical resources layer, but also on the virtualized resources domain.

In addition, as trust is a measure of uncertainty with its value represented by entropy, and actually is the function of uncertainty [27] and trust and distrust matter more in an uncertain environment involving risk and vulnerability when consumers consider reaching a decision, it can be roughly inferred from these theories that trust is the function of the cloud system uncertainty, which is the trust evidence of the trust decision to the system, in which a range of fault or misbehavior (from the underlying system infrastructure to the service interface) can be reflected in the system performance and security. Cloud service system is a large complex computing system that is built on giant network connecting a mass of nodes of different roles and large-scaled data center on which the infrastructures are delivered outward as service resource and huge amounts of service instances and applications are running at all times. Obviously that the larger the system uncertainty is, the little the trust can be acquired. The system uncertainty with respect to trust is a source of untrustworthiness to the system performance and behavior, including system security and service security.

Based on the characteristics of cloud services, this paper considers trustworthiness of cloud system paying more attention to the virtualized system infrastructure both as a system configuration and a virtual service unit delivered to the out side of cloud. Then the general definition of cloud system trustworthiness is given as the measure of cloud system capacity that under any conditions of uncertainty (including all kinds of abnormal conditions of hard/software faults, failures, network attacks and so on) cloud service system can still provide secure virtual environment and quality- guaranteed key services for users, and at the same time ensure the data, services and transactions security, no matter inferences are as the result of internal or external, subjective or objective, systematic or non-systematic factors. Furthermore, Table.1 shows the details of the requirements to cloud service respectively on the three aspects.

3.2. Entity trust management issues

Since the cloud computing is a distributed computing environment in which the whole resources are virtualized as a resource pool and are allocated dynamically on distributed computational and storage nodes, the resource owners and users are separated, and the service users and managers are also separated. However, the role of an entity in the cloud service system may not be unique, which means that the "client" and "service" are two relative concepts and may be reflected on one entity. For example, a cloud service provider delivering some on-line application service to the external users may also at the same time be the user of the infrastructure service offered by the cloud providers. This kind of problem may introduce at least two categories of trust problems in cloud platform:

a. Cloud service platform offers services through virtualization and multi-tenancy technique to multi external individuals and organizations, which are usually mutually distrusted with each other, and may even be competitive rivals under the worse circumstance. Furthermore, in the cloud service platforms such as multi-tenant cloud services, third party datacenter, etc, one platform holder or service user may become an attacker, thus destroy the protection to data privacy or other specific rights. The entities are not quite the same as the nodes cooperating in other network computing paradigms, such as the ad hoc network or wireless sensor network, since an entity becomes malicious, the trust relation will be impacted in a more wide range.

b. The overlapping identities between client and service lead to the fact that the trustworthiness of a cloud service transaction is influenced by at least two different roles in cloud. And the trust relation between different entities is not only nonlinear but also coupling, making the problem of trust relation establishment more complicated. Taking the trust relation among the overlapping identities into consideration and clearly dividing the components of different identities' contribution to form, maintain or damage the trust relationship is essential to the establishment of cloud trust framework. It is clear that cloud computing has opened up a new frontier of challenges by introducing a different type of trust scenario.

Table. 1 Concerned Requirements on Cloud Service Trustworthiness

Key operational performance requirements [28]	Key QoS requirements	Key security and privacy requirements [29] [30]
Adaptability Resilience Scalability flexibility Continuity	Availability Reliability Usability Consistency Quick response	Openness and transparency Controllability Access and accuracy Limiting use Accountability Security safeguards

Furthermore, trust and the degree of lost control over the data and processes in cloud depends heavily on the cloud service model [1] i.e., in IaaS and PaaS, the provider usually has complete control of the server, storage facility, and network. It's the same with SaaS, but the provider also controls the applications. Cloud computing virtually requires consumers to relinquish control in varying degrees of running their applications and storing their data [24]. Therefore there is a problem that how to make correct distribution of safety responsibility between the users and providers, which will impact how the cloud participants to form a mature trust relationship. And it is obvious that the more entities of different and overlapped roles are involved in the cloud service process, the more complicated trust relationship becomes.

4. Conceptive cloud trust management framework

As discussed previously, the trust issues in cloud have been examined from two perspectives of system trustworthiness under uncertainty and entity trust management. Furthermore, building trust to cloud should be based on all the above considerations. In this section, an theoretical overview about the three-layer trust conception framework is introduced, including the safety and function guarantee of underlying infrastructure (hard trust-HT), security control of the virtualized systems (virtualization trust-VT), and the trust management of the service & client interface (entity trust-ET). The structure organization of the trust cloud framework is as follows:

- Hard trust-is the foundation of the trustworthiness of cloud service systems, and can be formalized as a set of functional mechanisms according to all the actions and conditions in the cloud environment;
- Virtualization trust-still is a set of trust evidence that cloud vendors present to uses, while based on the trustworthiness of the cloud virtual environment including the virtual server security and the separation mechanism on the virtual hosts;
- Entity trust-is the trust built in the cloud service users, which is based on the measurement of the behavior records of the external entities get access to the cloud.

Meanwhile, we shown more detailed illustration of the three level conceptive trust framework is as follows:

- HT- safety and function guarantee of underlying infrastructure : On this level cloud vendors provide the safety guarantee of underlying infrastructure including the attack defendant and recovery of failure, fault, and catastrophe. Thus, trust on this level implies that the cloud system can act in a normal state and performs the behaviors satisfying the requirements to the system function, based on which the cloud vendors can provide available, consistent and stable services to either the service providers or the end users. As a matter of fact, the system trustworthiness factors can not ignore the system running level. Many cloud vendors are making effort to enhance their trustworthiness on this level, for example, according to the cloud computing event data base (CCID) specially responsible to record the cloud computing service break, most cloud computing service provides have suffered from downtime range from several minute to hours. And in more serious instances there are circumstances that lasted more than 24 hours. In the service downtime, the users suffered can not get access to the cloud services, and may result in decline of performance and user interactivity.

- VT-security and privacy control of virtualized services and resources : As cloud provides virtual services and operation environment to clients, which is delivered based on unified virtualized resources. This situation places a significant level of risk on the privacy and security of the data processed by the VMs in the cloud. And there should be a unified control mechanism for all the resources and services applications. On the level of security and privacy control of virtualized services and resources, cloud provides various mechanisms that ensure the system operation and services management, including authorization and access control, data security and protection, privacy management and data separation between users. Therefore, trust on this level is referred to a set of mechanisms that ensure the security and privacy of all the data assets owned by different users and coordinates the resource occupied in cloud datacenter. Actually, there is no longer concentration on a specific physical hardware or software infrastructure in cloud virtual environment, so that the security and consistency corresponding to the same logical part of system occupancy is a key challenge.

- ET-trust relationship management of the service & client interaction：The trust on service level refers to the trust relationship built from the cloud service to all the service users, which will be the foundation of entity trust management in cloud system. On this level, cloud providers establish a set of trust models and mechanisms to monitor /manage, record and control (in a proper manner) the behavior of entities. All the actions of entities will contribute to form their trustworthiness with different degrees in the cloud service systems, and thus of course will be relatively dynamical and changes with times during different transactions. The difference between the entity trust and virtualization trust is that there are two critical trust relationships that must be established in the service layer, which are respectively service provider trust and cloud user trust, and the accountability is another important factor to ensure the trust on this layer.

5. Cloud trust management framework

Since cloud entities and nodes are representing the same function and responsibility, and in order to facilitate the discussion next, here we equalize the meaning of them. We divide the nodes in the cloud into three categories: server nodes, virtual nodes and client nodes, which are respectively means the cloud infrastructure nodes (physical servers), logical nodes (VM servers or virtualized application services running on the VMs), and client side nodes (personal computers, mobile phone or any other devices that can get access to cloud). For all the nodes in the cloud, they have the following characteristics that can have a great influence to the entity trust management: (1) the roles of the cloud system nodes are multiple, so the trust records of a nodes have to be complete and clearly, (2) the physical nodes and the logical nodes are not consistent all the time, for example, the relation established between client node A who is running his software and server node B which is the host node of the software may be changed on the next time. (3) the client nodes topology changes. Because the client nodes may be mobile and the network route can be another reason that change the structure of the nodes distribution. (4) the server nodes (VM) are dynamically migrating as the result of requirements to load balance and as a result that the server nodes are not bind to a fixed physical nodes.

The management domains of virtual nodes are not necessarily centralized and can be distributed in a wide range of the server nodes domains. The responsibilities for the management nodes are concluded as the following three parts:

- They are responsible to monitor the virtual nodes and evaluate the trustworthiness of them, based on which can divide the virtual nodes into two sub-domains: trusted node domain and untrusted node domain. Besides, take specific action respectively to the two sub-domains, and establish the trust relation among the nodes in the trusted part while implementing some resource restriction to the nodes of untrusted part and making some of them change into trusted nodes if they behave innocently for a considerable period of time.

- Based on the trust evaluation to the virtual nodes, the management nodes should select proper trusted nodes to allocate tasks running on them according to the system real conditions, at the same time satisfy some objectives like the trustworthiness maximum, the cost of resources minimum, etc.
- The management nodes can also authorize some of the trusted virtual nodes to management the client nodes domain, and the virtual nodes can also establish and maintain the trust relation with client nodes who they trust.

It can be concluded from the above discussion that on virtual nodes trust records completed by the management domain nodes, there generates sets of trusted virtual nodes that can help to monitor the neighbor virtual nodes, which always have a lot of applications running on them, so the cumulative node trust supervision mechanism can provide a secured approach to protect the server nodes and the client nodes too. The schematic diagram of the mechanism model is as Figure 1 present:

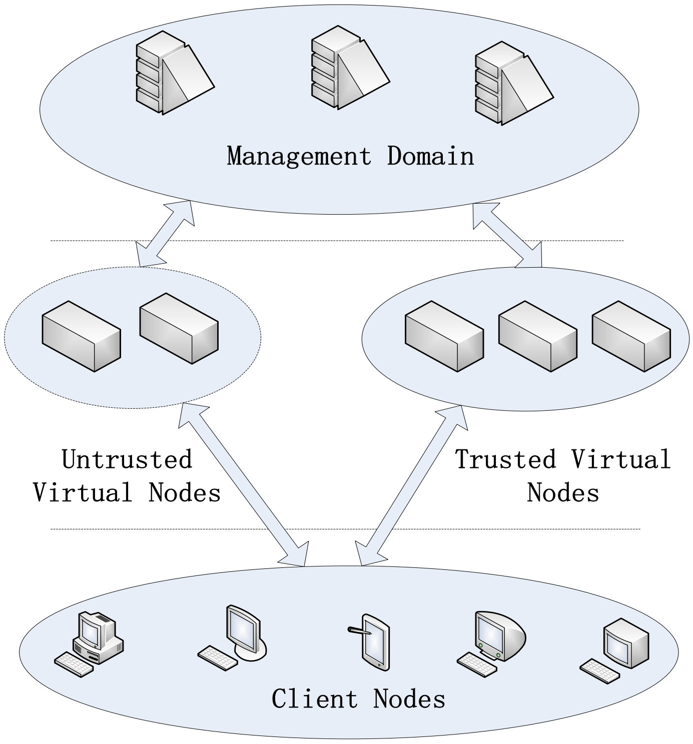

Figure 1. cloud system nodes cumulative supervision model

In the mechanism model, the client nodes trust is also a significant aspect of cloud trust. As the client nodes are out of cloud extension and typically mobile, and can pretend to be innocent, the trust management to them absolutely necessary. Since the client nodes interact with the virtual nodes on one specific application, the client behaviors are supervised by the virtual nodes and the behavior records are maintained by them.

In addition to the trust built between the virtual nodes and client nodes, the trust among the client nodes also should be established in the cloud environment. For example, a SaaS service user do not know the other tenants who are on the same VM as him, while he can get the trust records from the VM node that are hosting the SaaS application, or from the trusted virtual nodes that have been authorized by the management nodes to establish trust relation with client nodes so that without having to be the host VM of them. Besides the mechanism guarantee, the trust among client nodes has to consider non-technical factors such as laws and business process relation. And a valid trustworthiness evaluation model will reflect all the factors.

6. Conclusion

In this paper, we discuss the main trust-related problems in cloud ,which can be concluded as following the following trust-related problems:

(1) system trustworthiness under uncertainty;
(2) virtualization security issues; and
(3) entity trust relationship management.

Aiming to the problems above, we introduce a three-layered cloud trust management framework which can provide an overview of the important parts contributing to the trustworthiness cloud computing environment. As there existing the broad gap between "hard trust" and "soft trust" in cloud, mature trust relationship can not be built on security mechanism effectively. Through the combination and integration of the three layers, the gap between the different levels of trust factors can be bridged in cloud, from the underlying infrastructure to the virtual systems and to the service interaction level, the trust field in cloud environment can be established in a more deep and robust manner.

ACKNOWLEDGEMENTS

This research work is supported by the Nature Science foundation of China under Grant Nos. 71131002, 71071045 and 71171071.

REFERENCES

[1] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, vol. 34, pp. 1-11, 2010.

[2] Zhidong Shen, Qiang Tong. The Security of Cloud Computing System enabled by Trusted Computing Technology, In Proceedings of *2nd International Conference on Signal Processing System*s, pp. 11-15. 2010

[3] Imad M. Abbadi, Andrew Martin, Trust in the Cloud, *Information Security Technology Repor*t, vol 16, no. 3-4, pp. 108-114, 2011

[4] David Teneyuca. Internet cloud security: The illusion of inclusion, *Information Security Technology Report*, vol 16, no. 3-4, pp. 102-107, 2011

[5] Ilkka Uusitalo, Kaarina Karppinen, Arto Juhola. Trust and cloud service-An interview study, In Proceedings of *2nd IEEE International Conference on Cloud Computing Technology and Science,* pp. 712 - 720, 2010

[6] Fan Z.P. Trusted estimation in a virtual team-A decision support method, *Expert System with Application.* (2011)

[7] N. V. Ozaa, T. Halla, and A. Rainera. Trust in software outsourcing relationships: An empirical investigation of Indian software companies. *Information and Software Technology*, vol. 48, no. 5, pp. 245-354, 2006

[8] Khaled M. K. and Qutaibah M. Establishing trust in cloud computing, *cloud computing, IT Professiona*l, vol. 12, no.5, pp. 20-27, 2010

[9] Dimitrios Z and Dimitrios, L. Addressing cloud computing security issues, *Future Generation Computer Systems*. Vol. 28, no. 3, pp. 583-592, 2010

[10] Brian J. Corbitt , Theerasak Thanasankit , Han Yi .Trust and e-commerce: a study of consumer perceptions, *Electronic Commerce Research and Applications*, vol. 2, pp. 203-215, 2003

[11] Wei Kei Wong, Sai On Cheung, Tak Wing Yiu, Hoi Yan Pang. A framework for trust in construction contracting, *International Journal of Project Management*, vol. 26, pp. 821-829, 2008

[12] Zhengping Wu. Federated Trust Management for Service-oriented Computing. Ph.D Dissertation of Computer Science, *University of Virginia*. 2008

[13] Brent Jason Lagesse. Autonomic Trust management in Dynamic Systems. Ph.D Dissertation, T*he University of Taxes at Arlington*. 2009

[14] Olufunmilola Onolaja, Rami Bahsoon, Georgios Theodoropoulos. Conceptual Framework for Dynamic Trust Monitoring and Prediction, *International Conference on Computational Science, ICCS*, vol. 1, no. 1, pp. 1241-1250, 2010.

[15] Cynthia L. Corritore, Beverly Kracher, Susan Wiedenbeck. On-line trust: concepts, evolving themes, model, *International Journal of Human-Computer Studies*, vol. 58, pp. 737-758, 2003

[16] Weihua Song. Evaluating Onling Trust Using Machining Learning Methods. Ph.D Dissertation, *Louisiana Technology University*. 2005

[17] Dichao Peng. A trust supportive framework for pervasive computing. Ph.D Dissertation, *The University of North Carolina at Charlotte.* 2009

[18] D. Henrici and P. Muller. Hash-based enhancement of location privacy for radiofrequency identification devices using varying identifiers, In Proceedings of *the 2nd IEEE Annual Conference on Pervasive Computing and Communications Security*, pp. 149-153, 2004

[19] Chunqi T. and Baijian Y. R2Trust, a reputation and risk based trust management framework for large-scale, fully decentralized overlay networks. *Future Generation Computer Systems*, vol. 27, no. 8, pp. 1135-1141, 2011

[20] Ma Li, Zhang Yongmei, Ma Lan. A Synthesize Trust Degree Evaluation Method in Distributed System. In Proceedings of the *8th World Congress on Intelligent Control and Automation*, pp. 6-9, 2010

[21] Kai w. and Deyi L. Trusted cloud computing with secure resources and data coloring. Trust and Reputation Management, Internet Computing, IEEE, vol. 14, no. 5, pp. 14-22, 2010

[22] Joshua S. et al. Seeding Clouds with Trust Anchors, In Proceedings of *the 2010 ACM workshop on Cloud computing security workshop*, pp. 43-46, 2010

[23] Flavio L. and Roberto D. P. Secure virtualization for cloud computing. *Journal of Network and Applications*, vol. 34, no. 4, pp, 1113-1122, 2010

[24] Frank Joh n. K. Building trust into utility cloud computing. Ph.D Dissertations. *University of Maryland Baltimore County*, 2010

[25] Lei Wanyun. Cloud Computing: Enterprise Informatization Strategy and Practice, *Qsing Hua University Press*, 2010

[26] Frank. John K. et al. Introducing the Trusted Virtual Environment Module: A new Mechanism for Rooting Trust in Cloud Computing, *Trust and Trustworthy Computing*, vol. 6101, pp. 211-277, 2010

[27] Yan L.S. et al. Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE Journal on Selected Areas in Communications*. vol. 24, no.2, pp. 305-317, 2006

[28] Abbadi, I.M. Operational Trust in Clouds. In proceedings of *2011 IEEE Symposium on Computers and communications (ISCC*), pp. 141-145, 2011

[29] Siani Pearson. Taking privacy into account when designing cloud services. In Proceedings of *the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing IEEE Computer Society Washington*, pp. 44-52, 2009

[30] Tim Mather, Subra aKumaraswamy, Shahed Latif. Cloud Security and Privacy, *China Machine Press*, 2011