PROCEEDINGS OF SCIENCE

Trust Evaluation Method for the Perceptive Credibility of Tenants in the Cloud Platform

Jingpei Wang[1]
Information Security Research Center, China CEPREI Laboratory
Guangzhou, 510610, China
E-mail: wjpbupt@163.com

Shengmin Yang
Information Security Research Center, China CEPREI Laboratory
Guangzhou, 510610, China
E-mail: yangsm@ceprei.com

Jie Liu
Information Security Research Center, China CEPREI Laboratory
Guangzhou, 510610, China
E-mail: liujie@ceprei.com

The malicious usage of the cloud platform, untrusted providers, and untrusted perception from the users all contribute to the difficult application of the cloud services. In order to solve these issues, a trust evaluation method of the cloud service based on user perception is proposed. Based on fuzzy set theory, the behaviors of nodes in the cloud platform are quantitated, and the trust values of the services provider are measured; furthermore, an enhanced assessment mechanism in consideration of tenants' perceived credibility is studied, the fuzzy clustering algorithm is used to match the resource and task, and the hierarchical access control policy is deployed based on the credibility of the tenants; finally, a comprehensive assessment of the cloud services is integrated with the above three aspects of the evaluation. Analysis results show that the proposed method can filter malicious services in the cloud, match the optimal resource precisely, and prevent important data from being leaked to untrusted tenants. Experiments results further indicate the excellent performance of the proposed method. The proposed method can characterize the risk of the cloud platform and meet the diverse trusted needs of the cloud platform from varied tenants.

ISCC 2015
18-19, December, 2015
Guangzhou, China

[1]Speaker

PoS(ISCC2015)064

1. Introduction

With the development of distributed processing, parallel computing, and grid computing, the cloud computing has emerged in many fields [1]. However, due to the virtualization, resource pooling, ubiquitous access, etc. of the cloud computing, it faces huge challenges in information security [2]. The untrusted cloud application mainly comes from two aspects: the frequent security incidents triggered by malicious attacks, and the untrusted perception caused by the inconsistency between the individual needs of the tenants and the commitment of the cloud providers.

The cloud computing platform is an information system essentially, and will encounter security issues, such as security vulnerabilities, viruses, malicious attacks and Trojans backdoor. inevitably, which will lead to malicious usage of the cloud platform. On the other hand, the cloud platform is dependent on resource rental term. The personal data are stored in the cloud by tenants. In this mode, a tenant loses the forced control of the stored resources in the cloud platform. The tenants have no knowledge of how the cloud service providers handling their data and programs. After security incidents, it is difficult to affix the responsibility of cloud service providers. As a result, a tenant might not trust the cloud service providers. Even when the cloud service providers have achieved security and trusted environment in the most part, the tenant cannot perceive that, which will cause it difficult for users to trust the cloud platform.

In order to solve these problems, an objective and scientific third-party mechanism is needed urgently to assess the credibility of the cloud platform, in addition to deploy some technologies to ensure the trusted cloud platform. Therefore, studying the trusted evaluation method for cloud services, based on user perception, is of great significance to address the issue of credibility of the cloud platform.

2. Related Works

Current researches of trusted assessment mainly focuse on the computer and information systems, and trusted evaluation of the cloud platform has just started. The evaluation theory and methods for the cloud computing are mostly one-sided and imperfect. There is no methodology to prove the credibility of the cloud platform from theoretical perspective.

Rountree et al. elaborated related standards and evaluation systems of cloud security from a technical framework [3], which can assist establishing security assessment system in the cloud computing, but detailed evaluation methods were not described. In order to assess the credibility of cloud service from the perspective of the tenant, some experts introduced the SLA (Service Layer Agreement) into trust assessment [4]. The values of SLA parameters were taken as important factors in the trusted evaluation and prediction of the cloud services. Muchahari et al. calculated the trust of cloud service based on the feedbacks of the SLA, and designed a dynamic Trust Monitor to track the deviating trust values with the transaction time [5]. There are some deficiencies for the existing service evaluation framework: 1) ignore client monitoring; 2) the classification of the SLA parameter is not clear; 3) the trust factors are not comprehensive.

Traditional assessment methods are mainly based on TCSEC (Trusted Computer System Evaluation Criteria), CC (Common Criteria) and other standards, which are limited in assessing the credibility of the cloud platform. Dynamic and quantitative assessments are essential in the credibility assessment, and some assessed inference models have been established. Bernabe et

al. presented security ontology for the inter-cloud to formally describe the security issues in an inter-cloud security assessment, and used the ontology as input for a trust and security decision support system to quantify security expectations about the cloud service providers [6]. Many trust assessment methods studying one or more trusted attributes have been proposed in recent years, and the representative methods include: Bayesian network model [7], fuzzy theory trust model [8], trust evaluation model based on D-S evidence theory [9], etc. Li et al. proposed the concept of direct trust, indirect reputation, the weights of trust evaluation indexes with the inherent characteristics for the cloud manufacturing service platform, and defined a comprehensive assessment model [10]. Hosseini et al. considered that the tenants could manipulate the software, operating systems or even network infrastructure provided by the cloud vendors directly, and the credibility of tenants' behavior would directly affect the credibility of systems [11]. They established an evaluation system of tenant behaviors including credible layer, sub- credible layer and credible evidence layer in the cloud environment.

However, the existing trust evaluation methods merely consider the credibility of cloud terminal, tenants' behavior and task matching mechanism comprehensively, and there is a shortage in the perceptive assessment of the cloud service.

3. Service Scenarios and Evaluation Model Architecture

Firstly, the architecture and scene of a cloud service is described in Fig. 1. User stores the information through the terminal equipment, computers, mobile telephones, etc. of the access network, and uploads to the cloud through the routers, switches, and Internet public interface. Cloud platform stores and manages the resources, and provides service, i.e. data download, resource sharing, computing, etc. for tenants when necessary.

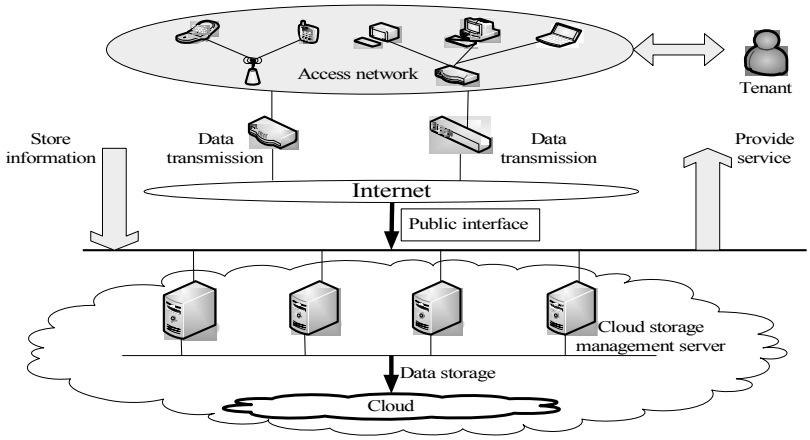


Figure 1: Block Diagram of the Architecture and Scene of a Cloud Service

Tenants can be divided into two categories: one is the resource contributor which entrusts the cloud computing managing its resources; the other is the resource users that have access to relevant resources, such as movies, music, and book through the cloud. Communication network can be wired or wireless, and the connection may be distributed or centralized.

In the cloud, the cloud storage management servers are mainly responsible for processing the data, such as encryption and fragmentation. and allocating resources, different resources are transferred to different management servers, and stored in the corresponding positions.

From the perspective of credibility, the untrusted factors mainly come from the risk of the management server and security threats induced by the defect of management strategies, which are worried about by the resource contributors. Resource users concern about whether the services meeting their perception, and whether the services being in accord with their assertion. The resource contributors and resource users can be considered as tenants. A credible assessment method is proposed from the perspective of tenants' perception in this paper.

4. The Proposed Evaluation Method

4.1 Trust Evaluation Model of Cloud Service

Firstly, extract the trust factors. The trust factors of the behaviors of a cloud service mainly include the risk assessment of the platform components (R), the interrupt probability of the virtual machine migration (Vm), the interrupt probability of the virtual machine escape (Ve), the probability of information integrity failure (In), the probability of privacy disclosure (P), etc.

These variable values can be calculated based on a series of tested recordings in the cloud platform within a period. A typical calculation of variable values is shown in (4.1):

$$T_x = \left[100\left(\frac{S}{S+N}\right)\left(1-\frac{1}{S+1}\right)\right] = \left[\frac{100S^2}{(S+N)(S+1)}\right] \tag{4.1}$$

Where S and N denote the statistical values of the number of successes and failures transactions within a time window T respectively, and T is an integer, $T \in [0,100]$.

After obtaining the quantization values of the trust factors, a fuzzy set theory is applied to infer the evaluated values of the cloud service. Suppose $U=\{R, Vm, Ve, In, P\}$ represents the evaluation factor set, and $V=\{v_1, v_2, v_3, v_4, v_5\}$ represents the discourse domain that indicates the range of trust values. The trust value is divided into five average levels from 0-1, and the interval is 0.2. Fuzzy inference is expressed as: $B_T = \{b_1, b_2, \ldots, b_n\} = (w_1, w_2,..., w_n) \circ (r_{ij})_{n\times m}$. Where $W=(w_1, w_2,..., w_n)$ denotes the weight vector related to the set of evaluation factors U, it identifies the importance of evaluation factors in U from peoples' viewpoints, and can be obtained by the method of entropy coefficient. And r_{ij} represents the degree of the factors u_i belonging to a comment v_j, b_j is the membership degree of factor set U relative to fuzzy set V.

Set a fuzzy transform f (i.e. trapezoidal membership function) from U to V, each element of U is judged individually based on f, and construct a fuzzy matrix $R = [r_{ij}]_{m\times n}$. A fuzzy set in discourse domain V is converted by R: $B_T = WR$. $B_T \in F(V)$ is the trust vector. Define trust $TV = \max(B_T)$, where $\max(B_T)$ represents the maximum membership degree of U relative to V. It is consistent with the principle that an optimal decision of the evaluated object is made by the priority principle of the greatest degree of the membership. TV is an evaluated value of

behaviors of a cloud server. All nodes in the cloud platform can be calculated with the corresponding trust values, those values are greater than a defined threshold (e.g. 0.5) and are permitted to transaction, and therefore, the malicious nodes are isolated.

4.2 The Optimization Algorithm Based on the Matching of Task and Cloud Resources

For a service node of which trust value is above the threshold or the commitment conforms to the expectation of tenants, further enhanced perceptive assessments are performed.

Different requests of tenants would lead to different perceptions for the cloud resources, scheduled task that mostly satisfies the needs of the tenants is considered to be the most credible on the perception. For the resources $R=\{R_1, R_2,\ldots, R_n\}$, n is the number of the resources, each resource is followed by a set of performance parameters, expressed as $R_p=\{p_1, p_2,\ldots, p_m\}$, and m is the number of parameters. For example, three parameters are used generally, and they are computing capability (p_c), storage capacity (p_s) and transmission capacity (p_b). The overall performance of a resource is integrated with each resource performance as (4.2):

$$R_p = \sqrt{\frac{a(p_c)^2 + b(p_s)^2 + c(p_b)^2}{a+b+c}} \tag{4.2}$$

Where a, b, c denote the experience coefficient of computing, storage and transmission respectively. Users would have different perceptions of credibility for nodes with different resource capacities. Firstly, cluster the resources with fuzzy C-means clustering method (FCM). The principles of FCM are as follows: for a given data set $X=\{x_1, x_2,\ldots, x_n\}$, the target of the FCM algorithm is to find a fuzzy clustering partition $U_{c\times n}$, and divide original data set X into c fuzzy groups, so that the dissimilarity index between each set of samples and its cluster center is minimum. Objective function of fuzzy clustering is defined as follow:

$$J(U, c_1, c_2, \ldots, c_c) = \sum_{i=1}^{c} J_i = \sum_{i=1}^{c}\sum_{j}^{n} u_{ij}^m d_{ij}^2 \tag{4.3}$$

Where u_{ij} denotes the membership of data j relative to i-th fuzzy group, and c_i is the cluster center of i-th fuzzy group. $d_{ij}=\|c_i-x_j\|$ is the Euclidean distance between i-th cluster center and j-th data, and m is a weighted index. Take the above 3 properties for example, we divide the nodes into three categories $\{C_c, C_s, C_b\}$ with the FCM method, which stand for the computational resources set, the storage resources set and the transmission resources set respectively.

There is a preference of resources for a task, suppose that the demand for resources set is $\{T_c, T_s, T_b\}$ for single task, set an experience weight vector for the demand, $W=\{w_c, w_s, w_b\}$, then the expected performance of required resources is calculate as follow:

$$T_p = \sqrt{\frac{w_c(T_c)^2 + w_s(T_s)^2 + w_b(T_b)^2}{w_c + w_s + w_b}} \tag{4.4}$$

The gap between the expected performance and the actual performance of resources is defined as the minimum value of Euclidean distance between T_p and the clustering center c_i.

$$T_{dif} = \min_{i\in[1,m]} \left\| T_p - c_i \right\| \tag{4.5}$$

Where m is the number of clusters, and m=3. The scheduling range of one task can be determined based on T_{dif}. For example, one task prefers resources with better computing speed (T_{dif} is closest to the center of C_c), then schedule the nodes in C_c providing the service, which has higher perceived credibility. Further quantify the Euclidean distance between R_p and T_p in the

selected resources set, and normalize it between [0, 1] based on the max-min method. The trust values are modeled as the opposite of the normalized values of Euclidean distance between R_p and T_p. Those nodes where trust values are greater than a credible threshold (e.g. 0.5) are permitted to anticipate in the service, and thereby improve the perceived credibility.

4.3 Trust Evaluation Method of Hierarchical Access Control Based on Tenants Behaviors

The constraint of credibility should be bidirectional for the tenants and cloud service providers. For a malicious tenant, if he can get access to the cloud resources freely, the cloud resources can also be perceived not credible. In addition, the privacy information of the tenants is stored in the cloud nodes. Hierarchical access control strategy is proposed to ensure that a tenant with sufficiently high credibility is permitted to obtain a higher level of resources.

Evaluate the credibility of behaviors of the tenants, the behaviors information includes the historical reputation, the successful rate of cooperation, and the compliance of implementing agreements, etc. Collect these behaviors, establish a trust model, and compute the trust values of the tenants' behaviors. The computing framework of the trust value of node i is shown in (4.6)

$$T_i = \alpha \cdot DT_i + \beta \cdot RT_i + RW \tag{4.6}$$

Where α and β are the weights of the direct trust value and reputation value respectively, and $\alpha+\beta=1$, RW is the reward value. The direct trust DT_i is calculated according to the fuzzy inference in 4.1 based on the collected direct trust information in certain time T. The indirect trust value is obtained by fuzzy inference of the historical reputation sequence of node i collected by a set of cloud nodes and tenants within the same domain of node i in the same time T. RW is determined by the degree of sustained good praise for node i. Within a observation time T, the reward value is $RW = 0.2\ N_s/N$, and N_s is the number of continued successful interactions. N is the total number of interactions. The reward value is below 0.2, and the change of T_i is less than the trust ratings step 0.2 after the addition of the award.

Implement different access control policies for tenants with different trust levels. Define a set of services decision function: suppose that the overall trust can be divided into p levels, which satisfy: $t_1<t_2<\ldots<t_p$ and $t_i \cap t_j = \emptyset$ $(i \neq j)$. Potential $p+1$ services can be provided, denoting as $S = \{s_0, s_1, \ldots, s_p\}$, and the service decision function between T and S is defined as follow: when $T \leq t_1$, $S(T) = s_0$; when $t_1 < T \leq t_2$, $S(T) = s_1$; and so on, when $T > t_p$, $S(T) = s_p$.

The access control policy can decide what quality of service can be provided according to users' trust values when users demanding a service. For example, S = {deny, partial, normal}, and T_p= {0.2, 0.5}, if T = 0.8, then he can acquire the normal service. It is vital to set proper trust thresholds according to the importance of service to avoid the risk of malicious access to the service. The cloud platform determines if the information or only a sample of it is disclosed, or if the request is rejected. This measurement protects the sensitive resource, and enhances tenants' perception of their own behaviors and importance.

4.4 Comprehensive Assessment and Summary

Integrate the above 3 evaluation procedures, get the comprehensive assessment of a cloud service, and the evaluation procedures are outlined as follows:

1) evaluate the credibility of a set of cloud computing nodes N that proclaim providing credible services, and filter nodes set N_t in N of which the trust values exceed the threshold to provide services;

2) based on the task requirements of tenants, further perform fuzzy clustering for the selected node set N_t, and select a set of sorted service nodes N_c of which the resource capacity meets the task mostly to provide services;

3) further set the access control policies for N_c based on the trust level of tenants. Match the resources based on the tenants' trusted status, and finally achieve the goal of "the most suitable resource services, the most suitable tenant" and enhance the perception of the tenants.

5. The Analysis and Simulations of the Proposed Method

5.1 Analysis and Discussion

The main features of the proposed scheme are addressed as follows:

1) it solves the consistency between the credibility of cloud platform and perceived credibility of the tenants. The proposed method integrates the credibility of the cloud platform, the credibility of the tenants and the credibility of matching the tasks and resources, and enhances perceived credibility of the tenants for the cloud platform;

2) it adopts resources fuzzy clustering method to achieve the scheduling mechanism of "right resources to serve the appropriate task" in conditional constraints. It avoids blind scheduling, improves the accuracy of resource matching, and increases the successful rate of task execution;

3) it has lower complexity. The computational complexity in the stage of credibility evaluation of behaviors of the cloud platform is $2O(n)$. In the stage of resource matching and scheduling optimization, the complexity is $O(m \times k)$, where m is the number of nodes greater than a threshold, $m<n$, k is the number of iterations of fuzzy clustering, and k is small. In the stage of hierarchical access control of tenants, the complexity is $O(l)$, where l is the number of iterations of recommended values. The overall complexity of the proposed scheme is $2O(n) + O(m \times k) + O(l)$. The space complexity is $O(n)$, and n is the number of nodes calculated.

5.2 Experimental Simulation

In this section, we perform experimental simulations to verify the effectiveness of the proposed method. The simulation tool is MATLAB. Set up a group of simulation parameters, as shown in Table 1. N is the size of network, M is the number of service requesters, h_1 is a credible threshold of the cloud service nodes, m_1 is the number of resource properties, a, b, c are the experience factors of calculation, storage and transmission, w_c, w_s, w_b are the experience weights of requested resources and α and β are the weights of direct trust value and reputation value. Based on the defined scene and parameters, perform 20 times of transactions, and the simulation results are shown in Fig. 2.

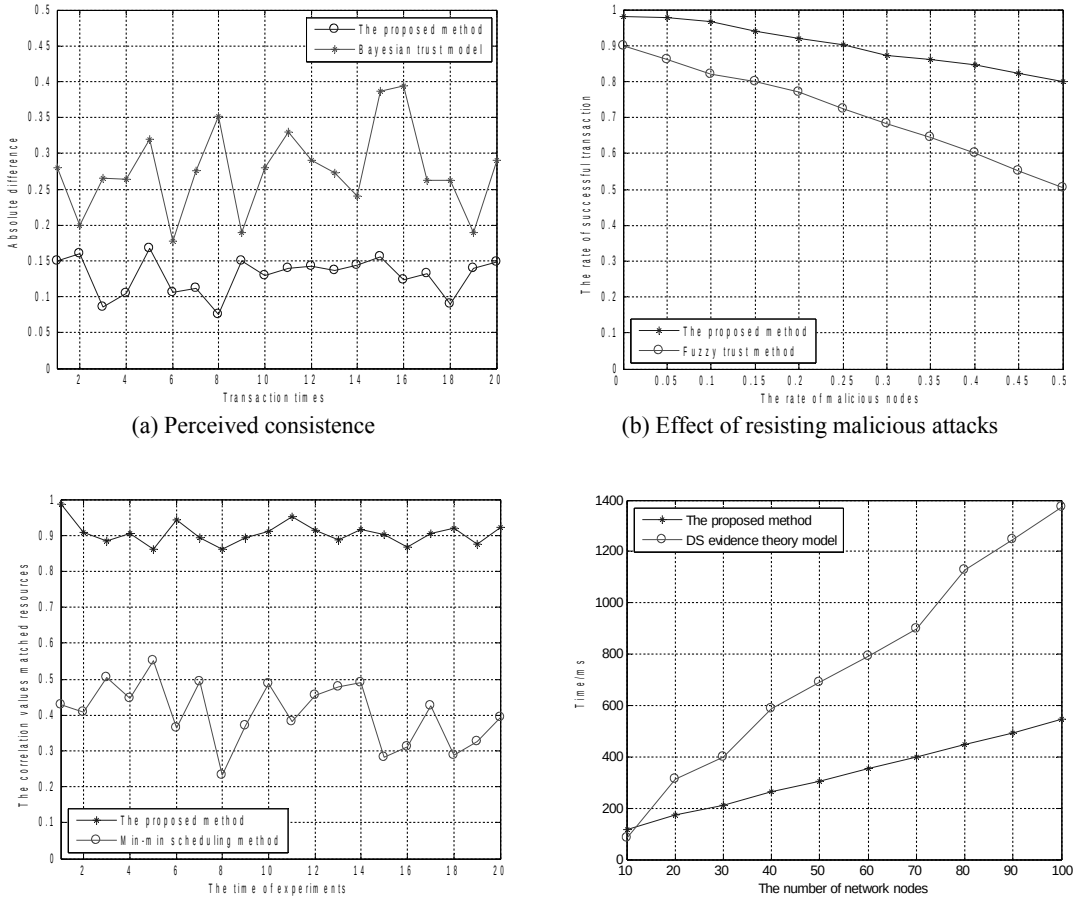
Table 1 Simulation Parameters

Parameters	N	M	h_1	m_1	a	b	c	w_c	w_s	w_b	α	β
Values	50	20	0.5	3	0.5	0.3	0.2	0.4	0.4	0.2	0.7	0.3

Fig. 2 evaluates the proposed trust model from four aspects: the perceived consistence, the robustness of trust model, the accuracy of scheduling and task execution efficiency.

Fig. 2 (a) describes the perceived consistence between the expected trust values and calculated ones of the cloud server. The expected trust values are the statistical average of the credibility of cloud services, and are obtained by a set of ratings from several volunteers in the same community with the same task. The actual trust values are calculated by the proposed method. The *y*-axis denotes the absolute difference between the expected trust values and the calculated ones. From Fig. 2 (a) we can see that absolute differences are controlled in 0.2 for the proposed method, which means better perceived consistence than the Bayesian trust model.

Fig. 2 (b) describes the robustness of the proposed model. The number of malicious nodes increases with the same percentage for cloud providers and tenants. With the increasing of the malicious nodes, the rate of successful transaction declines, the slower declining means the better performance. From Fig. 2 (b) we can see that the success rate of transactions decreases slowly for the proposed method. It has better performance than the fuzzy trust model [8].



(a) Perceived consistence

(b) Effect of resisting malicious attacks

(c) Accuracy of scheduling

(d) Efficiency of implementing task

Fig. 2: Simulation Results

Fig. 2 (c) describes the accuracy of resource scheduling. The *x*-axis denotes the time of experiments with different tasks, and *y*-axis denotes the correlation values of requested resources and scheduled resources. The result shows that the proposed method is more accurate in matching the task and resource compared with Min-min scheduling method [12]. The accuracy remains about 0.9 for the proposed method as the selected resources match the tasks based on fuzzy clustering, whereas the tenants' requests are not considered accordingly in the Min-min method.

Fig. 2 (d) describes the efficiency of implementing task. As can be seen from the Figure, with the change of network size (each time randomly increase or decrease the same nodes on the basis of 50 nodes), the proposed method is more efficient to perform the task than the D-S evidence theory model [9]. It means that less time is required to complete the task (e.g. secure data transmission). Only a sample of the trusted nodes based on bi-directional trust evaluation and task matching is selected to perform the task for our method, and therefore, the proposed method is more effective and has better performance compared with other algorithms.

6. Conclusion

A trusted evaluation method for the cloud services based on user perception is proposed in this paper. The behaviors of nodes in the cloud platform are evaluated based on fuzzy set theory, followed by further trust assessment of the tenants' behaviors and enhanced perceived evaluation by matching the resource and task with fuzzy clustering, and finally comprehensive assessment of the cloud services is integrated. Analysis and simulation results show that the proposed method has higher accuracy of scheduling resources, better scalability and lower complexity. It solves the problems of malicious usage of the cloud computing platform and the cloud platform providers not to be trusted in perception.

References

[1] I. Alzamil, K. Djemame, D. Armstrong, R. Kavanagh. *Energy-Aware Profiling for Cloud Computing Environments* [J]. Electronic Notes in Theoretical Computer Science. 318(25): 91-108 (2015).

[2] M. Arun Fera, C. manikandaprabhu, I. Natarajan, K. Brinda, R. Darathiprincy. *Enhancing Security in Cloud Using Trusted Monitoring Framework* [C]. International Conference on Intelligent Computing, Communication & Convergence (ICCC 2015), Elsevier, India, 198-203 (2015).

[3] D. Rountree, I. Castrillo. *Evaluating Cloud Security: An Information Security Framework* [M]. The Basics of Cloud Computing, Elsevier B. V., USA, 101-121 (2014).

[4] H. L. zhang, P. P. Li, Z. G. Zhou. *Performance Difference Prediction in Cloud Services for SLA-Based Auditing* [C]. 2015 IEEE Symposium on Service-Oriented System Engineering (SOSE). San Francisco Bay, CA, IEEE, 253-258 (2015).

[5] M. K. Muchahari, S. K. Sinha. *A New Trust Management Architecture for Cloud Computing Environment* [C]. 2012 International Symposium on Cloud and Services Computing (ISCOS). Mangalore, IEEE, 136-140 (2012).

[6] J. B. Bernabe, G. M. Perez, A. F. S. Gomez. *Inter-cloud Trust and Security Decision Support System: an Ontology-based Approach* [J]. Journal of Grid Computing, 13(3): 425-456 (2015).

[7] O. Jules, A. Hafid, M. A. Serhani. *Bayesian network, and probabilistic ontology driven trust model for SLA management of Cloud services* [C]. 2014 IEEE 3rd International Conference on Cloud Networking (CloudNet), IEEE Conference Publications, Luxembourg, 77-83 (2014).

[8] M. Jaiganesh, M. Aarthi, A. Vincent Antony Kumar. *Fuzzy ART-Based User Behavior Trust in Cloud Computing* [M]. Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, 2014, vol. 324, Springer India, 341-348 (2014).

[9] X. N. Wu, R. L. Zhang, B. Zeng, S. Y. zhou. *A Trust Evaluation Model for Cloud Computing* [C]. First International Conference on Information Technology and Quantitative Management (ITQM 2013), Elsevier B. V., Suzhou, 1170-1177 (2013).

[10] C. Li, S. Wang, L. Kang, L. Guo, Y. Cao. *Trust evaluation model of cloud manufacturing service platform* [J]. The International Journal of Advanced Manufacturing Technology, 75(1): 489-501 (2014).

[11] S. B. Hosseini, A. Shojaee, N. Agheli. *A new method for evaluating cloud computing user behavior trust* [C]. 2015 7th Conference on Information and Knowledge Technology (IKT), Urmia: IEEE, 1-6 (2015).

[12] J. F. Tian, H. Zhou. *Study on Safety Scheduling Strategy with Cloud Computing Model* [C]. 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation (ICMTMA). Nanchang, IEEE, 1061-1065 (2015).