BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **16**, No 3
Sofia • 2016 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.1515/cait-2016-0034

CCDEA: Consumer and Cloud – DEA Based Trust Assessment Model for the Adoption of Cloud Services

Sivakami Raja[1], *Saravanan Ramaiah*[2]

[1]*Department of Information Technology, PSNA College of Engineering and Technology, Dindigul, Tamilnadu, India*
[2]*Department of Computer Science and Engineering, RVS Educational Trust's Group of Institutions, Dindigul, Tamilnadu, India*
E-mails: rsivakami@psnacet.edu.in directorrvsetgi@rvsgroup.com

Abstract: *Knowing the trust level of cloud service providers is a significant issue in the field of cloud computing for privacy and security reasons. The idea of this paper is to build up a Consumer and Cloud-Data Envelopment Analysis* (*CCDEA*) *trust assessment model for evaluating cloud services in two stages. In first stage, the believability index of each cloud Consumer* (*C*) *is calculated. The second stage incorporates Cloud-Data Envelopment Analysis* (*C-DEA*) *model for the trust assessment of cloud services from the viewpoint of cloud consumers. Several experiments were conducted and the results were analyzed to show the stability of our method in measuring the relative efficiency and effectiveness of cloud services through ranking mechanism.*

Keywords: *Cloud computing, believability index, cloud service, trust assessment, Data envelopment analysis, cloud theory.*

1. Introduction

In the current age of computing, information is a major asset. From the local area network to the currently available highly connected internet, the world is being benefited from the easiness of data storage and access. By cloud computing, resources such as hardware, networks, servers, storage, applications and interfaces are provided as on-demand services to customers. But, this introduces data security as a major issue since intruders and hackers are also enjoying technologies for their security-threatening activities. Since cloud consumers permit external sources to hold control of their data, trust also becomes an important problem.

Trust may be defined as determination and guarantee that the trustee will perform in a specific way as anticipated by the trustor. In a cloud environment, cloud providers and cloud consumers should have mutual trust between them. In essence, earning the trust of consumers is essential for providers for the sake of their business benefits. On the other hand, since consumers leave their data with

providers, they have to know whether they can trust the particular Cloud Service Provider (CSP) or not. Moreover, if the provider seems to be trustable, consumers like to know to what extent they can be trusted. Estimating the trust index of CSP is a key issue in the field of cloud security. This is due to the fact that cloud users leave their valuable information with providers whose honest behavior matters a lot.

Consumers often find difficulty when choosing cloud services or cloud service providers for their needs. In addition to the cost, several parameters are involved in deciding the efficiency of cloud services. One consumer may look for security, whereas another consumer may prefer lower cost. So, the purpose of this paper is to apply Fuzzy-Data Envelopment Analysis (DEA) model to decide which cloud service is the most efficient one. DEA was proposed in [1] as a mathematical multi-criteria based programming model to obtain relative efficiency scores of peer entities (decision making units). It evaluates the efficiency of decision making units relative to other decision making units by processing multiple units to yield multiple outputs. It models a linear programming problem with multiple criteria to deal with real-world engineering problems which require efficiency analysis. All the decision making units under consideration should use same resources so that their efficiency can be measured uniformly. In our work, we employ output oriented method where we try to maximize the efficiency of cloud service providers by keeping input parameters as constant. According to a given set of cloud service parameters, cloud services have to be ranked from the viewpoint of consumers. We represent these cloud services as decision making units.

The rest of the paper is organized as follows: Section 2 outlines a brief overview of previous work on assessment of cloud trust and DEA. The concept of determining parameters which influence the cloud trust is discussed in Section 3. Section 4 gives an introduction to cloud theory. Evaluation of consumers' believability index and ranking mechanism of cloud services are explained in Sections 5 and 6, respectively. Results of experiments which show the analysis of our mechanism are presented in Section 7. At last, Section 8 concludes our work.

2. Previous work

An access control method based on mutual trust is proposed in [2] through authentication and authorization using ant colony optimization. For a multi-cloud environment, a trust management plan is suggested in [3] which several trust service providers are used. These providers cooperate with each other in evaluating the trust of cloud service providers. In [4], trust evaluation is done based on completeness, auditability and transparency. Similarly, another approach is recommended in [5] to prefer trustable cloud service providers by using parameters such as auditability and interoperability. Various mechanisms for trust assessment are explained in [6]. It further explains the association between individual components of cloud environment for measuring trust. An approach for workflow scheduling is conveyed in [7] by incorporating trust metrics. Various trust and reputation models are discussed in [8]. Further, the authors of [8] identified several important parameters in preparing consumers to judge the trustworthiness of cloud

service providers. In [9], a system for trust oriented management is presented based on Bayesian networks. This system explained how to intelligently make opinion with respect to public frameworks. Several protocols were proposed in [10] to calculate trust in a client within a multi-client environment. Instead of processing large number of messages, this method uses small number of messages in trust calculation. A trust-aware model is recommended in [11] by considering two parameters called clustering and typical path length between nodes. Finally, this system concluded that the tightly clustered network where the path length between nodes is as small as possible will give better results. A Cloud trust model proposed in [12] advises users in determining trustable cloud providers based on various trust attributes. A dynamic cloud based trusted scheduling is explained in [13] using Bayesian method. A tree structured fuzzy based trust model is developed in [14] to assess the trust value of cloud service providers. Nash equilibrium based trust model is suggested in [15] for a cloud environment using game theory.

In [16], Charnes, Cooper and Rhodes (CCR) model and Li, Jahanshahloo and Khodabakhshi (LJK) model are integrated for the analyzing the assessment of decision making units. A framework based on Analytical Hierarchical Process is suggested in [17] to enable cloud consumers to appraise cloud providers using various characteristics of cloud services. A model for evaluating public cloud services is suggested in [18] using performance parameters. In [19], several tools for estimating the performance of cloud services are presented and analyzed. Organizations such as [20] are also providing analysis of cloud services as a service. An integrated fuzzy DEA technique is used in [21] to measure the efficiency and effectiveness of decision making units. Another fuzzy DEA approach is presented in [22] which convert the DEA model into parametric model for evaluating the relative efficiency of decision making units. Performance assessment of cloud services is done in [23] using DEA. This system is based on the low level attributes like throughput, storage, and data transfer rate. A method is proposed in [24] which detect both efficient and inefficient components using data envelopment analysis. In [25], cloud trust is assessed using cloud model for addressing randomness and uncertainty. Further Bayesian network is used to deal with the dynamic nature of cloud services. Several models have been analyzed is [26] for providing secured services in an application layer. An approach based on fuzzy theory and ant colony optimization has been suggested in [27] for assessing the trust index of cloud service providers.

3. Determination of cloud parameters

According to our another work explained in [27], Fig. 1 shows that before availing services from a cloud service provider, each consumer wants to know whether the CSP is trustable or not, and to what level. In order to make them to be aware of the trust level of service providers, Trust-as-a-Service (TaaS) layer is incorporated. Based on the personal experience with the current service provider, the rating in terms of Service Level Agreement (SLA), performance and security, is given by the consumer and stored in the opinion store. Trust database is a repository of trust

information about CSPs. It contains trust scores as assessed from the feedback of other consumers. The consumer, who needs to know the trust level, can use this information after validating the believability of other consumers. Trust appraisal is done according to the proposed method and the trust index is calculated based on which the consumer makes decisions regarding the fitness of cloud service provider to his/her requirements.

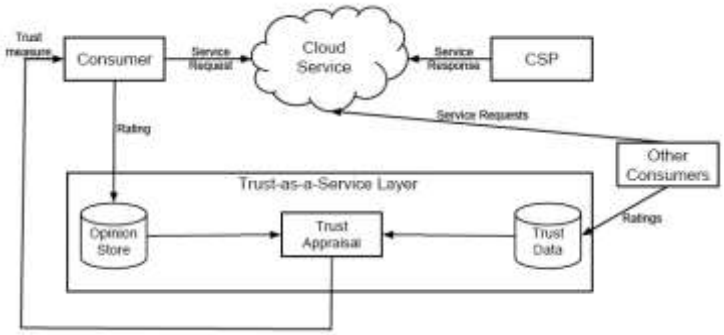

Fig. 1. Model for cloud trust assessment

The aim of this work is to propose a method for choosing the most feasible cloud service. For this selection, a list of parameters have been analyzed and screened as shown in Fig. 2. To measure the trust of a CSP, parameters are essential. We employed a bottom-up approach in this parameter identification process. We initially recognized several basic parameters and then grouped together into various categories called SLA, Performance, Security, and User opinion. Dynamic nature of cloud leads to confidentiality, integrity and availability issues. In order to address these issues successfully, all entities of a cloud environment should be free of distrust and also they should renew themselves corresponding to the changes happening in the cloud. Due to the distributed structure of cloud, diverse security tactics are offered in the market. Choosing a suitable combination of security approaches is a major challenge. So, these parameters are placed under a category *Security*.

Another important concern from the viewpoint of consumers is the reliability of cloud services. Both centralized and distributed managements may experience complications in offering services without interruptions. Apart from all these affairs, interoperability, accountability, flexibility, and agreement of regulations (laws) become significant in the context of trust. These parameters are grouped together into a category *Performance*. As organizations prefer to take up cloud services, service excellence becomes an influential factor. Service providers vary in terms of service features and service consumers also differ in their demands. Hence both of them try to establish a scale of service. This kind of bargaining results in a concurrence called as SLA. SLAs are vital to decision makers to properly fix promises for service between the cloud consumer and the cloud service provider. They give directions for taking decisions on what to look forward to and what to be aware of as SLAs are assessed. A healthy SLA targets to remedies, in spite of penalties. Depending on the requirements of individual delivery model, SLAs must

be formed carefully. SLA factors are established according to the business requirements of cloud consumer and cloud provider. For consumers, bandwidth, reliability, availability, trust, and billing are identified as the comprehensive metrics. For Providers, the requirements aim to be competent to carry out the consumer requirements. Common factors include abandonment rate, average speed, turn-around time, mean time to recover, resource utilization, and network uptime. Whenever issues arise between provider and consumer, a well-framed SLA should aspire to lessen their loss. They are possibly uncertain in rescuing consumers when they meet with disputes in cloud services. So SLA plays critical role in measuring the trustworthiness of cloud providers and hence become the most important parameter. It comprises of certification, customer support and IDentity (ID) management. The categorization and grouping of trust parameters is shown in Fig. 2.

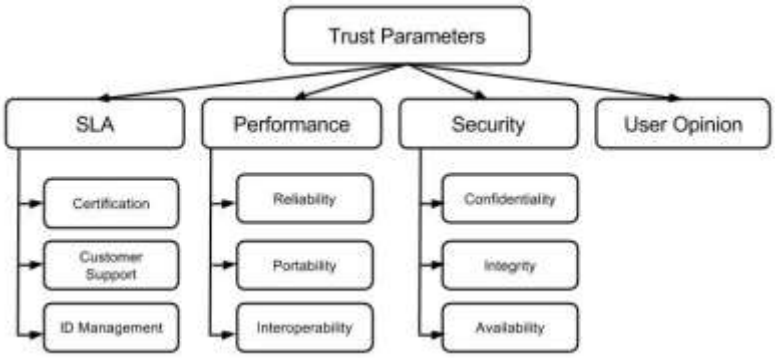

Fig. 2. Classification of trust parameters for a cloud environment

4. Introduction to cloud theory

Though probability theory and fuzzy theory are widely adopted in uncertain problems, they lag in representing vague and uncertain information. Probability theory employs normal distribution to deal with uncertainty. Unfortunately, the trust parameters are interdependent in our model. Hence, the application of probability becomes void. Similarly, determination of membership functions through qualitative reasoning in fuzzy theory requires rigid numerical expressions. This necessity makes fuzzy less appropriate. Hence, cloud theory (cloud model) is developed that intervenes between fuzzy set and probability distribution. It deals with uncertainty and encloses added information to make clear inferences than that of conventional statistical methods under uncertainty situations. This model finds its applications in various domains such as intelligent automation, decision making, data mining and etc. Hence, a cloud based trust assessment model is developed in this work, with reduced false rates.

The purpose of cloud theory is to convert each qualitative significance degree into a normal cloud. Fig. 3 shows a normal cloud generated with 1000 cloud droplets (drops). Similarly, *N* number of related clouds can be developed with the *N*-level scaling of normal clouds. A 5-level cloud system is shown in Fig. 4. In an

N-level scaling of normal clouds, numbers of *j*-th normal cloud are represented by the universe U_j. The universe U of the *N*-level cloud is defined as $U = \bigcup_{j=1}^{N} U_j$. The distance d between the centers of neighboring normal clouds for normalized values is calculated by $d = \frac{1}{N}$. The Expectation (Ex_j), Entropy (En_j) and Hyper-entropy (He_j) of *j*-th normal cloud are the three input qualitative significance degrees.

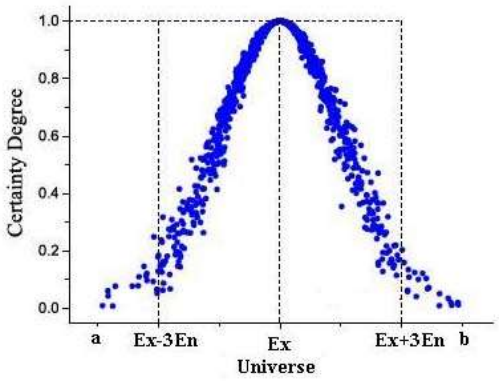

Fig. 3. Cloud system with 1000 cloud drops

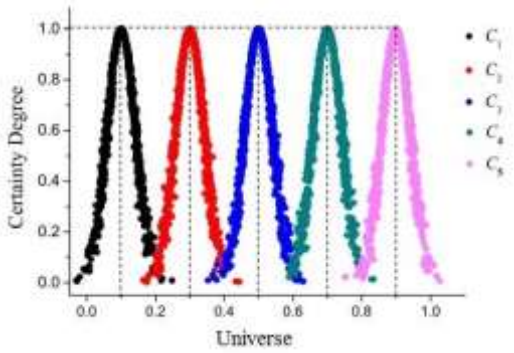

Fig. 4. Cloud system for 5-level evaluation scaling

The Expectation (Ex) is the qualitative mathematical significance degree that contributes the central point of the domain. In another words, it represents cloud's center point. The Entropy (En) indicates the margin of qualitative significance that can be included in the domain of evaluation. In turn, it estimates the ambiguity of qualitative significance degree and dispersing limit of each of the cloud drops. Hyper-entropy (He) or excess entropy or entropy of entropy is a parameter that gives the sign of dispersion of cloud drops and the uncertainty assessment of entropy. These parameters, Ex, En and He, are calculated by the equations from (1) to (3), respectively.

(1) $$\mathrm{Ex}_j = \frac{(2j-1)d}{2},$$

$$\mathrm{En}_j = \frac{\sqrt{\left(d - 3\mathrm{Ex}_j\right)d}}{3}, \tag{2}$$

$$\mathrm{He}_j = \frac{\mathrm{En}_j}{10}, \tag{3}$$

for $j = 1, 2, \ldots, N$, where 1/10 is a linearization coefficient. Then these qualitative input significance degrees (Ex, En and He) are converted into quantitative output degrees by producing cloud drops in an N-level cloud. Each cloud drop is represented by $x_i = \lfloor x_{1i}, x_{2i}, \ldots, x_{pi} \rfloor$ for p number of dimensions. Cloud drop$_s$ which lie within the interval [Ex – 3En, Ex + 3En] are considered for the evaluation and the remaining drops which fall beyond this interval are rejected. In our implementation, we considered [0, 1] as the interval of universe.

After converting the qualitative inputs into quantitative outputs, the proposed Consumer and Cloud-Data Envelopment Analysis (CCDEA) based trust assessment framework for a cloud environment calculates the relative efficiency and efficiency index of each cloud service as explained in Section 6.

5. Stage 1: Evaluation of consumers' believability

This level is previously illustrated in our work [27] for checking whether each cloud consumer is worth enough to give opinion about trustability of cloud services. While considering the feedback from peer consumers, their believability is an important thing in decision making. This level is important since there may be several fraudulent users in cloud who may give wrong opinion either to increase or decrease the trustability of a particular cloud service. This may lead to fluctuations in the measurement of cloud trust. In order to avoid this problem, the believability of each cloud consumer is assessed so that opinion is collected from genuine consumers only. The believability calculation is a challenging issue since anybody can join and take part in the process of trust calculation. Believability of peers is imprecise and dynamic with respect to the changes in their activities. Their trust can not be measured using crisp values. So, fuzzy theory, where linguistic labels can smoothly represent interval values, can be adopted.

While availing services from service providers, cloud consumers behave exactly like (artificial) ants of ant colony algorithm. As they wish to avail services from cloud service providers of high trust index, pheromone of ant colony algorithm can be used to represent trust index. Further, believability between cloud consumers is identical to the pheromone. So ant colony optimization can be applied to the trust measurement of cloud computing environment.

Out of four input parameters, the first three parameters are used to measure direct trust between consumer and CSP. User opinion is a fuzzy variable whose value indicates the degree of recommendation by another consumer. So, it is used to measure indirect trust between consumer and CSP. From these direct and indirect trusts, the overall trust is calculated.

Believability B_{ji}, $0 \le B_{ji} \le 1$, of consumer i by consumer j, $1 \le i, j \le m$, $i \ne j$, is

$$B_{ji} = B_0 + \frac{\sum_{k=1}^{N} w_k s_{ik}}{\sum_{k=1}^{N} w_k} + e(t), \tag{4}$$

where N is the total number of services available in a cloud computing environment, w_k, $1 \le k \le N$, is the weight associated with k-th service, B_0 is the initial value of believability assigned to any new cloud consumer, which is usually zero, $e(t)$ is an error at time t, and s_{ik}, $1 \le k \le N$, $1 \le i \le m$, indicates whether k-th service is availed by consumer i or not. It is expressed as

$$s_{ik} = \begin{cases} 1 & \text{if consumer } i \text{ has availed service } k, \\ 0 & \text{if consumer } i \text{ has not availed service } k. \end{cases}$$

We interpret the status $B_{ji} = 1$ as consumer j has full believability on consumer i and $B_{ji} = 0$ as consumer j does not have any believability on consumer i (Zero believability).

Believability matrix B on C is an interval-valued fuzzy matrix, which is defined by a relation C×C and membership function $\mu_B : C \times C \to \text{Interval}([0,1])$, and where Interval([0, 1]) is the set of closed subintervals within [0, 1].

Relative Believability $\text{B}^{\text{R}}(C_i)$ of each consumer C_i, and Believability Index $\text{BI}(C_i)$ of consumer C_i are calculated for $1 \le i \le m$:

$$\text{B}^{\text{R}}(C_i) = \frac{1}{m-1} \sum_{j=1}^{m} B_{ji}, \tag{5}$$

$$\text{BI}(C_i) = \frac{1}{m-1} \sum_{j=1}^{m} P\left(\text{B}^{\text{R}}(C_i) \succ \text{B}^{\text{R}}(C_j)\right). \tag{6}$$

Here, $P(\text{B}^{\text{R}}(C_i) \succ \text{B}^{\text{R}}(C_j))$ is the possibility degree [28] which is defined by

$$P(\text{B}^{\text{R}}(C_i) \succ \text{B}^{\text{R}}(C_j)) = \tag{7}$$

$$= \frac{\max\left\{0, \left[y_i^- + \delta\left(\text{B}^{\text{R}}(C_i)\right)\right] - y_j^-\right\} - \max\left\{0, y_i^- - \left[y_j^- + \delta\left(\text{B}^{\text{R}}(C_j)\right)\right]\right\}}{\delta\left(\text{B}^{\text{R}}(C_i)\right) + \delta\left(\text{B}^{\text{R}}(C_j)\right)},$$

where $\text{B}^{\text{R}}(C_i) = \left[y_i^-, y_i^+\right]$ and $\text{B}^{\text{R}}(C_j) = \left[y_j^-, y_j^+\right]$. Here,

$$\delta\left(B^R(C_i)\right) = 1 - y_i^- - y_i^+ \text{ and } \delta\left(B^R(C_j)\right) = 1 - y_j^- - y_j^+.$$

Finally, $\text{BI}(C_i)$, $1 \le i \le m$, are compared against the Believability Threshold (BT). If $\text{BI}(C_i)$ is greater than the BT value, opinion from consumer C_i is taken into

account for calculating the trust index of CSP. Else it is neglected. Since cloud consumer join and leave the cloud dynamically and due to the change in the behavior of consumers, their participation in the process of assessing CSPs trust index is appreciated or neglected based on the up-to-date value of their believability index. After calculating the believability index of the target, it is compared against *no believability* (0) and *full believability* (1) values. If it is less than or equal to 0.2, the target is not believed. Else, if it is greater than or equal to 0.8, the target will be believed and hence it can participate in the process of trust assessment. But if the believability index is between 0.2 and 0.8, an issue of deciding whether to believe or not to believe arises. When one customer decides to believe the target customer and another decides not to believe, the believability of the target customer is affected.

Consumers' believability will be evaporated gradually with respect to time. So we have used the next equation for updating it:

$$B_{ji}(t+1) = (1-\rho) B_{ji}(t) + \Delta B_{ji}(t,\ t+1), \tag{8}$$

where, ρ is an evaporation factor, $\Delta B_{ji}(t, t+1)$ is the change in believability index from time t to time $t+1$ which is calculated by

$$\Delta B_{ji}(t,\ t+1) = \mathrm{BI}^{t+1}(C_i) - \mathrm{BI}^{t}(C_i). \tag{9}$$

Here, $\mathrm{BI}^{t}(C_i)$ is the believability index of consumer i at time t and $\mathrm{BI}^{t+1}(C_i)$ is the believability index of consumer i at time $t+1$.

6. Stage 2: Ranking mechanism of cloud services by CCDEA

Fig. 5 shows the order of execution of our work in the trust assessment of cloud services. Assume that *m* represents the number of cloud services. They make use of an input vector $x_i = \lfloor x_{1i}, x_{2i}, \ldots, x_{pi} \rfloor$ to generate an output vector $y_i = \lfloor y_{1i}, y_{2i}, \ldots, y_{qi} \rfloor$, where p and q represents the dimensions of input vector and output vector, respectively. Efficiency indices (Eff) of cloud services are calculated by first translating qualitative degrees into corresponding quantitative degrees. For positive inputs and outputs, the relative Efficiency (Eff_k) of a Cloud Service CS_k, $1 \le k \le m$, is calculated by a Linear Programming Problem (LPP):

$$\mathrm{Eff}_k = \sum_{i=1}^{q} s_{1i} y_{ki} \Big/ \sum_{j=1}^{p} s_{2j} x_{kj},$$

where s_{2j} and s_{1i} are the weights of *j*-th input and *i*-th output, respectively.

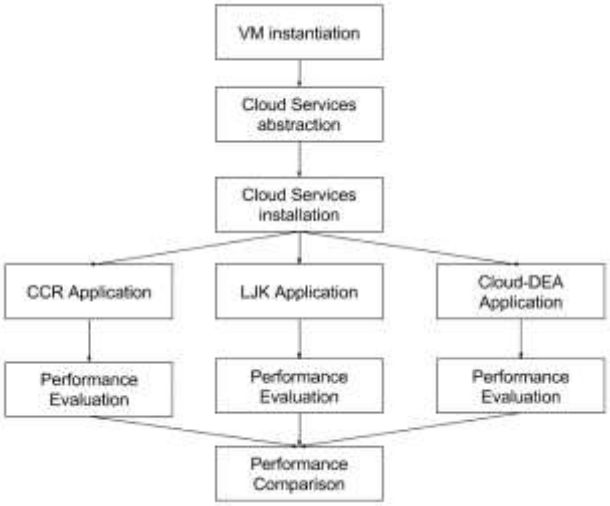

Fig. 5. Flowchart for ranking mechanism of cloud services

This can be illustrated as

$$\text{Maximize Eff}_k = \text{Maximize} \sum_{i=1}^{q} s_{1i} y_{ki} \Big/ \sum_{j=1}^{p} s_{2j} x_{kj}$$

subject to the constraints:

$$\sum_{i=1}^{q} s_{1i} y_{li} \Big/ \sum_{j=1}^{p} s_{2j} x_{lj} \le 1, \quad l = 1, 2, \ldots, m,$$

$$s_{1i} \ge 0, \quad 1 \le i \le q, \quad s_{2j} \ge 0, \quad 1 \le j \le p.$$

If this efficiency index is equal to 1, this cloud service is relatively efficient. Else, it is relatively inefficient. According to Charnes-Cooper and Rhodes variable transformation, the above model is written as the following output oriented LPP:

$$\max \sum_{i=1}^{q} s_{1i} y_{ki},$$

subject to

$$\sum_{j=1}^{p} s_{2j} x_{kj} = 1, \quad \sum_{i=1}^{q} s_{1i} y_{li} - \sum_{j=1}^{p} s_{2j} x_{lj} \le 0, \quad l = 1, 2, \ldots, m,$$

$$s_{1i} \ge 0, \quad 1 \le i \le q, \quad s_{2j} \ge 0, \quad 1 \le j \le p.$$

Efficiency index of each CS_j is calculated by rerunning the proposed method for n times. The average efficiency index of j-th cloud service is $\text{Eff}_j = \left(\sum_{k=1}^{n} \text{Eff}_{jk} \right) \Big/ n$, j = 1, 2, …, m, where m is the number of the assessed cloud service provider, and Eff_{jk} is the efficiency index calculated in k-th iteration for j-th cloud service provider. Once the efficiency index calculation of all cloud services is accomplished, they can be prioritized in the order of their efficiency index values. In our work, we consider SLA, Performance, Security and User opinion as input

parameters (attributes) and trust of cloud service as an output attribute. Tables 1-5 show the cloud system of our input and output attributes to convert qualitative attribute values into quantitative numbers. Similarly, the relative Effectiveness $(\text{Effec}_k = \text{actual output/desired output})$ of a cloud service CS_k, $1 \le k \le m$, is calculated by

$$\max \ \text{Effec}_k = \sum_{i=1}^{q} s_{1i} y_{ki} \Big/ \sum_{j=1}^{r} \rho_j d_{kj} \ ,$$

subject to

$$\sum_{i=1}^{q} s_{1i} y_{li} \Big/ \sum_{j=1}^{r} \rho_j d_{lj} \le 1, \quad l = 1, 2, \ldots, m, \quad s_{1i} \ge 0, \quad 1 \le i \le q, \quad \rho_j \ge 0, \quad 1 \le j \le r,$$

where d_{kj} is the j-th desired output for k-th cloud service, and ρ_j is the weight associated with j-th desired output.

7. Experimental results and discussion

To assess and demonstrate the efficiency of our proposed system, we have simulated a cloud environment with the following ten cloud service providers: Amazon, Azure, Century Link, City-Cloud, Cloudera, Google Compute Engine, HP, IBM, OpenNebula, and Rackspace. For each of them, 2 or 3 cloud services are taken and the corresponding description is shown in Table 1 for the total of 26 cloud services in our experiments.

Table 1. Description of cloud services using qualitative values

CSP	Cloud Service	SLA	Performance	Security	User opinion
C1	C1S1	Weak	Medium	Medium	Negative
	C1S2	Moderate	Good	Medium	Neutral
	C1S3	Moderate	Good	Medium	Positive
C2	C2S1	Moderate	Good	Low	Neutral
	C2S2	Weak	Poor	Medium	Neutral
C3	C3S1	Strong	Poor	Medium	Positive
	C3S2	Strong	Medium	High	Positive
	C3S3	Moderate	Medium	Medium	Neutral
C4	C4S1	Strong	Medium	Low	Positive
	C4S2	Weak	Medium	Medium	Negative
	C4S3	Moderate	Good	High	Positive
C5	C5S1	Moderate	Poor	High	Neutral
	C5S2	Weak	Medium	Low	Neutral
C6	C6S1	Weak	Good	Medium	Negative
	C6S2	Strong	Medium	High	Positive
	C6S3	Strong	Poor	High	Positive
C7	C7S1	Moderate	Good	Medium	Positive
	C7S2	Weak	Medium	Low	Negative
	C7S3	Moderate	Poor	Low	Negative
C8	C8S1	Strong	Good	High	Positive
	C8S2	Weak	Poor	Medium	Neutral
C9	C9S1	Strong	Medium	High	Positive
	C9S2	Weak	Good	Medium	Neutral
C10	C10S1	Moderate	Medium	Low	Negative
	C10S2	Moderate	Good	High	Positive
	C10S3	Strong	Medium	Medium	Positive

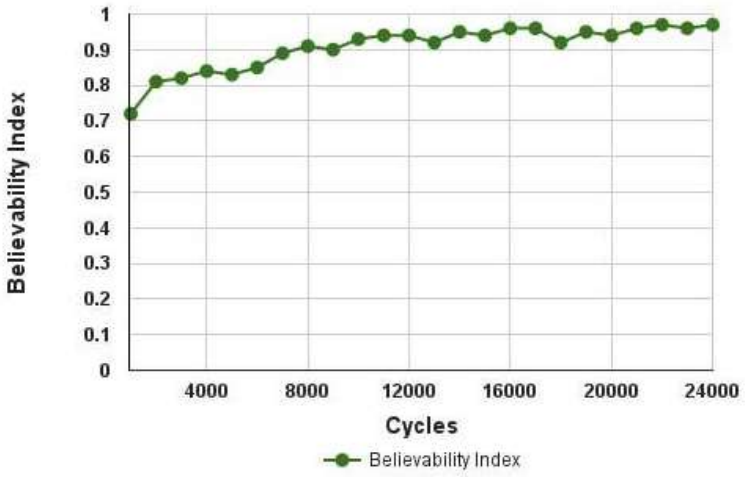

Fig. 6. Believability index of good host

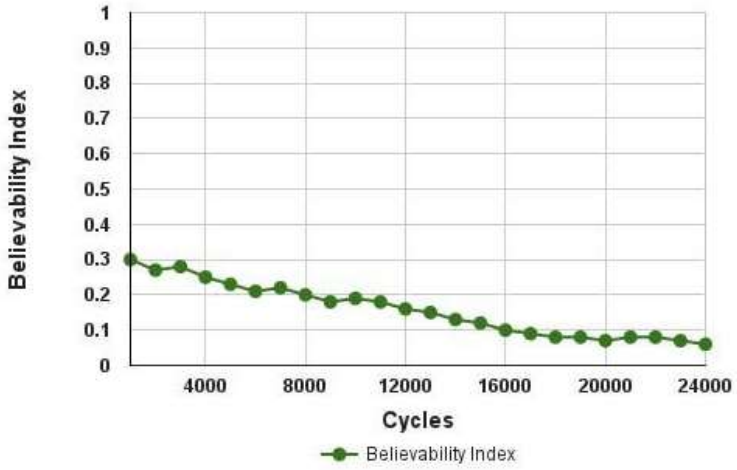

Fig. 7. Believability index of bad host

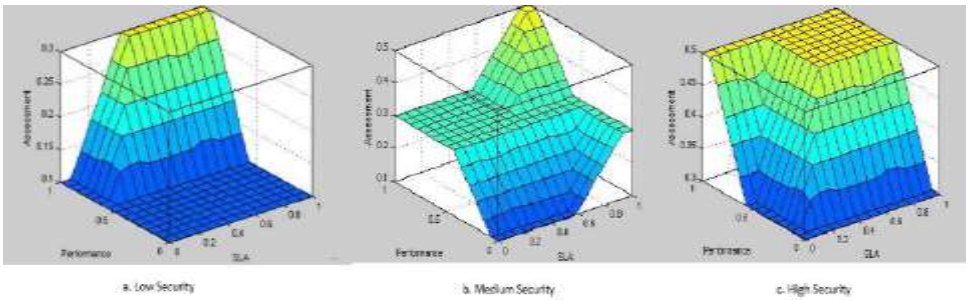

Fig. 8. Evolution of trust with respect to negative user opinion

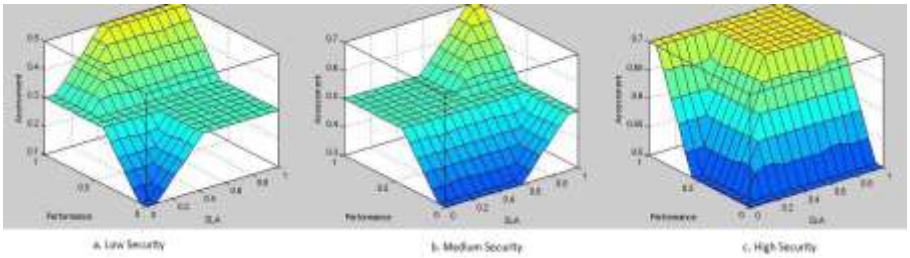

Fig. 9. Evolution of trust with respect to neutral user opinion

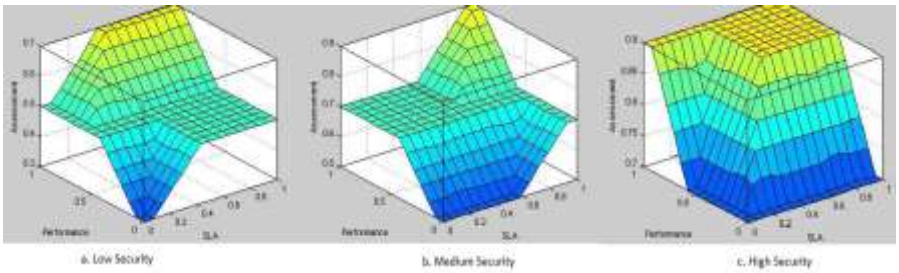

Fig. 10. Evolution of trust with respect to positive user opinion

3D representations of our results illustrate the progression of trust index with respect to the input parameters SLA and *performance*, while *security* and *user opinion* are fixed. Fig. 8 shows that as security increases, it affects the trust value positively. For medium and higher levels of SLA and performance, security greatly influences the trust assessment. But for lower levels of SLA and Performance, security does not give a significant impact on trust value. For medium and high valued securities, we get identical trust values as maximum values. But the difference lies in the membership value of SLA parameter. For medium security levels, we obtain maximum trust value for higher SLA levels, whereas the same maximum trust value is achieved for medium and higher SLA levels. Even though for high security, the maximum value for trust index is only 0.5 due to negative opinion of customers. This means that the trust value cannot be improved by these parameters alone. It gives major importance to user opinion. Since Fig. 8 gives results for negative opinion, trust index does not go beyond 0.5, even for the full membership values of remaining parameters. On another side, trust value does not drop below 0.3 for the full membership values of SLA and Performance, even for low security. Thus the significance of these parameters are compared to others is shown in Fig. 8. Fig. 9 and Fig. 10 show the progression of trust evaluation with respect to SLA and Performance, where customers have given neutral and positive opinions, respectively. Even for zero membership value of security, their trust value is uniformly increased by 0.2 in Fig. 9 for neutral opinion and by 0.4 in Fig. 10 for positive opinion. This shows the significance of user opinion in the process of trust evaluation. This provides justification for the reason why we give major importance in measuring the believability of customers who provide opinion or feedback about the efficient service provision of cloud service providers.

After evaluating the believability of consumers, the decision making system is given the values for the input parameters as shown in Tables 2-5 which give the 3-level scaling cloud system of our four input parameters and Table 6 shows the 5-level scaling cloud system of our output parameter.

Table 2. 3-level evaluation scale cloud system of SLA

Level	Attribute value	Ex	En	He
1	Weak	0.1667	0.0687	0.0069
2	Moderate	0.5000	0.0687	0.0069
3	Strong	0.8333	0.0687	0.0069

Table 3. 3-level evaluation scale cloud system of Performance

Level	Attribute value	Ex	En	He
1	Poor	0.1667	0.0687	0.0069
2	Medium	0.5000	0.0687	0.0069
3	Good	0.8333	0.0687	0.0069

Table 4. 3-level evaluation scale cloud system of Security

Level	Attribute value	Ex	En	He
1	Low	0.1667	0.0687	0.0069
2	Medium	0.5000	0.0687	0.0069
3	High	0.8333	0.0687	0.0069

Table 5. 3-level evaluation scale cloud system of User opinion

Level	Attribute value	Ex	En	He
1	Negative	0.1667	0.0687	0.0069
2	Neutral	0.5000	0.0687	0.0069
3	Positive	0.8333	0.0687	0.0069

Table 6. 5-level evaluation scale cloud system of CS trust

Level	Attribute value	Ex	En	He
1	Complete distrust (Untrustworthy)	0.1	0.0412	0.0041
2	Distrust	0.3	0.0412	0.0041
3	Weak trust	0.5	0.0412	0.0041
4	Moderate trust	0.7	0.0412	0.0041
5	Complete trust (Trustworthy)	0.9	0.0412	0.0041

Table 7 shows how different methods assess ranks for various cloud services based on efficiency using CCR, LJK and Cloud-DEA model. Table 8 shows the ranks for the same based on effectiveness. From the Tables 7 and 8, we understand that the ranks awarded by CCR and LJK models often differ from each other. Comparison between each pair of methods in ranking is presented in Table 9 from which we infer that our proposed method achieves minimum deviation and constant results with respect to other methods. When we compare ranking based on efficiency and effectiveness indices, we find consistency in the ranking of cloud services with the use of our proposed method as shown in Table 10. But the other two methods provide different ranking for the same set of cloud services with the same set of resources.

Table 7. Results of comparison of cloud services on efficiency index

Cloud Service	CCR		LJK		Cloud-DEA	
	Efficiency index	Ranking	Efficiency index	Ranking	Efficiency index	Ranking
C1S1	0.3127	24	0.3643	24	0.365289	23
C1S2	0.5873	16	0.7016	14	0.694796	13
C1S3	0.6742	13	0.8823	9	0.862913	10
C2S1	0.4473	19	0.5971	17	0.573544	17
C2S2	0.5054	17	0.5061	18	0.505643	19
C3S1	0.8013	10	0.8173	12	0.793552	12
C3S2	0.9213	5	0.8876	8	0.96278	7
C3S3	0.7216	12	0.7642	13	0.611473	16
C4S1	0.7549	11	0.8462	11	0.8514	11
C4S2	0.4106	20	0.4346	21	0.420206	22
C4S3	0.9965	1	0.9769	4	1.032762	5
C5S1	0.6542	14	0.6613	15	0.654184	14
C5S2	0.4713	18	0.4735	20	0.458406	20
C6S1	0.3984	21	0.4127	22	0.438954	21
C6S2	0.9546	3	0.9314	6	0.977872	6
C6S3	0.8966	6	0.8993	7	0.92893	8
C7S1	0.8775	8	0.8677	10	0.877051	9
C7S2	0.2958	25	0.2944	25	0.28628	25
C7S3	0.2693	26	0.2746	26	0.249162	26
C8S1	0.9476	4	0.9976	2	1.064108	2
C8S2	0.3647	23	0.4997	19	0.524108	18
C9S1	0.8875	7	0.9567	5	1.057161	3
C9S2	0.6389	15	0.6336	16	0.629694	15
C10S1	0.3967	22	0.3882	23	0.327391	24
C10S2	0.9768	2	1.0912	1	1.09061	1
C10S3	0.8754	9	0.9876	3	1.053479	4

Table 8. Results of comparison of cloud services on effectiveness index

Cloud Service	CCR		LJK		Cloud-DEA	
	Effectiveness	Ranking	Effectiveness	Ranking	Effectiveness	Ranking
C1S1	0.2796	24	0.2741	24	0.3372	23
C1S2	0.3975	16	0.4633	15	0.5543	13
C1S3	0.4464	12	0.6317	9	0.6554	10
C2S1	0.3501	19	0.4211	17	0.4963	17
C2S2	0.3843	17	0.3994	18	0.4457	19
C3S1	0.5242	10	0.5134	12	0.5968	12
C3S2	0.7543	5	0.6796	8	0.7316	7
C3S3	0.4651	13	0.4963	13	0.5212	16
C4S1	0.5015	11	0.5546	11	0.6217	11
C4S2	0.3424	20	0.3276	21	0.3684	22
C4S3	0.8176	1	0.7996	4	0.7953	5
C5S1	0.4587	14	0.4492	16	0.5218	14
C5S2	0.3697	18	0.3492	20	0.4126	20
C6S1	0.3229	21	0.3016	22	0.3982	21
C6S2	0.7988	3	0.7863	5	0.7764	6
C6S3	0.6679	6	0.7107	7	0.7150	8
C7S1	0.5542	7	0.5938	10	0.6843	9
C7S2	0.2543	25	0.2533	25	0.2540	25
C7S3	0.2447	26	0.2416	26	0.2473	26
C8S1	0.7941	4	0.8256	2	0.8316	2
C8S2	0.2901	23	0.3610	19	0.4760	18
C9S1	0.5510	8	0.7543	6	0.8121	3
C9S2	0.4573	15	0.4873	14	0.5679	15
C10S1	0.2946	22	0.2869	23	0.2977	24
C10S2	0.8140	2	0.8317	1	0.9010	1
C10S3	0.5735	9	0.8014	3	0.8109	4

Table 9. Rate of difference between three methods

Criteria	CCR and LJK	Cloud-DEA and LJK	Cloud-DEA and CCR
Based on Efficiency index	0.8462	0.6538	0.7692
Based on Effectiveness index	0.8077	0.6923	0.7692

Table 10. Results of consistency comparison

Method	Rate of deviation
CCR	0.1538
LJK	0.1923
Cloud-DEA	0.0000

Experiments are conducted to measure the execution time of ranking for different number of cloud services. Fig. 11 shows that, for small number of cloud services, all the three methods are almost equal in terms of execution time. But as the number of cloud services increase, they exhibit a difference. Further, even for 1000 cloud services, Cloud-DEA method consumes about 6.9 s only. This shows the sign of competence of Cloud-DEA for ranking cloud services.

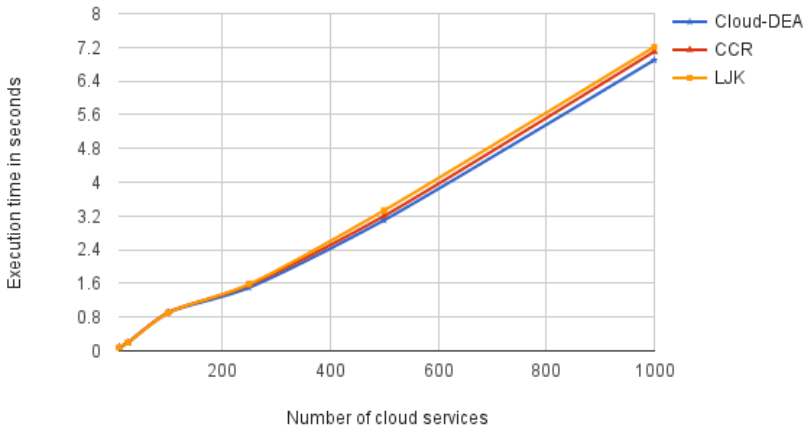

Fig 11. Execution time of various methods for ranking cloud services

8. Conclusion

In this paper, we have proposed a CCDEA based trust assessment framework for a cloud environment, where the believability of consumers is first evaluated and then the trustworthiness of cloud service providers is assessed based on cloud theory and data envelopment analysis. Here, each cloud service is symbolized as a decision making unit. By representing input parameters using a set of 3-level cloud system, trust of each cloud service is evaluated by a 5-level cloud system. Then, cloud services are ranked in terms of efficiency and effectiveness indices. Similar experiments with same set of resources are conducted using CCR model and LJK model to compare the results and to show the goodness of our proposed method.

References

1. Cooper, C. W., E. Rhodes. Measuring the Efficiency of Decision Making Units. – European Journal of Operational Research, Vol. **2**, 1978, No 6, pp. 429-444.
2. Lin, G., D. Wang, Y. Bie, M. Lei. MTBAC: A Mutual Trust Based Access Control Model in Cloud Computing Information Security. China Communications, 2014, pp. 154-162.
3. Fan, W., H. Perros. A Novel Trust Management Framework for Multi-Cloud Environments Based on Trust Service Providers. – Knowledge-Based Systems, Vol. **70**, 2014, pp. 392-406.
4. Ouedraogo, M., H. Mouratidis. Selecting a Cloud Service Provider in the Age of Cybercrime. – Computers & Security, Vol. **38**, 2013, pp. 3-13.
5. Tang, C., J. Liu. Selecting a Trusted Cloud Service Provider for Your SaaS Program. – Computers & Security, Vol. **50**, 2015, pp. 60-73.
6. Huang, J., D. M. Nicol. Trust Mechanisms for Cloud Computing. – Journal of Cloud Computing: Advances, Systems and Applications, Vol. **2**, 2013, No 9.
7. Tan, W. A., Y. Sun, L. X. Li, G. Z. Lu, T. Wang. A Trust Service-Oriented Scheduling Model for Workflow Applications in Cloud Computing. – IEEE Systems Journal, Vol. **8**, 2014, No 3, pp. 868-878.
8. Habib, S. M., S. Hauke, S. Ries, M. Muhlhauser. Trust as a Facilitator in Cloud Computing: A Survey. – Journal of Cloud Computing: Advances, Systems and Applications, Vol. **1**, 2012, No 19.
9. Wißner, M., S. Hammer, E. Kurdyukova, E. André. Trust-Based Decision-Making for the Adaptation of Public Displays in Changing Social Contexts. – Journal of Trust Management, Vol. **1**, 2014, No 6.
10. Dolev, S., N. Gilboa, M. Kopeetsky. Efficient Private Multi-Party Computations of Trust in the Presence of Curious and Malicious Users. – Journal of Trust Management, Vol. **1**, 2014, No 8.
11. Yuan, W., D. Guan, Y.-K. Lee, S. Lee, S. J. Hur. Improved Trust-Aware Recommender System Using Small-Worldness of Trust Networks. – Knowledge-Based Systems, Vol. **23**, 2010, pp. 232-238.
12. Li, X., J. Du. Adaptive and Attribute-Based Trust Model for Service Level Agreement Guarantee in Cloud Computing. – IET Information Security, Special Issue – Trust and Identity Management in Mobile and Internet Computing and Communications, Vol. **7**, 2013, No 1, pp. 39-50.
13. Wang, W., G. Zeng, D. Tang, J. Yao. Cloud-DLS: Dynamic Trusted Scheduling for Cloud Computing. – Expert Systems with Applications, Vol. 39, 2012, pp. 2321-2329.
14. Gu, L., J. Zhong, C. Wang, Z. Ni, Y. Zhang. Trust Model in Cloud Computing Environment Based on Fuzzy Theory. – International Journal of Computers Communications & Control, Vol. **9**, 2014, No 5, pp. 570-583.
15. Gokulnath, K., R. Uthariaraj. Game Theory Based Trust Model for Cloud Environment. – The Scientific World Journal, Article ID 709827, 2015, Hindawi Publishing Corporation. 10 p.
16. Zhou, Y., Z. Yan, N. Li, L. Yu, L. Zhou, L. Chen. Cloud-Data Envelopment Analysis Method Used for Assessment of Restoration Building Block Schemes. – CSEE Journal of Power and Energy Systems, Vol. **1**, 2015, No 2, pp. 43-52.
17. Kumar, S. G., S. B. Versteeg, R. Buyyaa. A Framework for Ranking of Cloud Computing Services. – Future Generation Computer Systems, Vol. **29**, 2013, pp. 1012-1023.
18. Li, A., X. Yang, S. Kandula, M. Zhang. CloudCmp: Comparing Public Cloud Providers. – In: Proc. of 10th Annual Conference on Internet Measurement, Melbourne, Australia, 2010.
19. Iosup, A., S. Ostermann, N. Yigitbasi, R. Prodan, T. Fahringer, D. Epema. Performance Analysis of Cloud Computing Services for Many-Tasks Scientific Computing. – IEEE Transactions on Parallel and Distributed Systems, Vol. **22**, 2011, No 6, pp. 931-945.
20. Harmony, Cloudharmony.com, February 2012.
http://cloudharmony.com/

21. A z a d i, M., M. J a f a r i a n, R. F. S a e n, S. M. M i r h e d a y a t i a n. A New Fuzzy DEA Model for Evaluation of Efficiency and Effectiveness of Suppliers in Sustainable Supply Chain Management Context. – Computers & Operations Research, Vol. **54**, 2015, pp. 274-285.
22. R a z a v i, S. H., H. A m o o z a d, E. K. Z a v a d s k a s, S. S. H a s h e m i. A Fuzzy Data Envelopment Analysis Approach Based on Parametric Programming. – International Journal of Computer Communication, Vol. **8**, 2013, No 4, pp. 594-607.
23. D e S o u z a, L. M., M. P. F e r n a n d e z. Performance Evaluation Methodology for Cloud Computing Using Data Envelopment Analysis. – In: Proc. of 14th International Conference on Networks, IARIA, 2015, pp. 58-64. ISBN: 978-1-61208-398-8.
24. C h e n, W.-C., A. L. J o h n s o n. A Unified Model for Detecting Efficient and Inefficient Outliers in Data Envelopment Analysis. – Computers & Operations Research, Vol. **37**, 2010, No 2, pp. 417-425.
25. J i n, B., Y. W a n g, Z. L i u, J. X u e. A Trust Model Based on Cloud Model and Bayesian Networks. – Procedia Environmental Sciences, Vol. **11**, 2011, pp. 452-459.
26. S h u a i b u, B. M., N. M. N o r w a w i, M. H. S e l a m a t, A. A l-A l w a n i. Systematic Review of Web Application Security Development Model. – Artificial Intelligence Review, Vol. **43**, 2015, pp. 259-276.
27. R a j a, S., S. R a m a i a h. 2S-FAT-Based DLS Model for Cloud Environment. – Arabian Journal for Science and Engineering, Vol. **41**, 2016, No 8, pp. 3099-3112.
28. W e i, C. P., X. T a n g. Possibility Degree Method for Ranking Intuitionistic Fuzzy Numbers. – In: Proc. of IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2010, pp.142-145.