International Journal of Engineering & Technology, 7 (4) (2018) 4335-4340

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 9830
Research paper

Fuzzy and ant colony optimization based trust evaluation system for a cloud environment

R. Sivakami [1] *, A. Vincent Antony Kumar [1]

[1] Department of Information Technology, PSNA College of Engineering and Technology, Dindigul, Tamilnadu, India
**Corresponding author E-mail: rsivakami@psnacet.edu.in*

Abstract

From consumers' perspective, knowing the trust level of cloud service providers with maximum accuracy is often considered as a difficult task in cloud computing for security related arguments. The proposed trust evaluation system adopts the well-defined parameters for evaluating the trustworthiness of cloud service providers. This system employs fuzzy theory integrated with ant colony optimization. Initially, the believability index of each consumer is calculated. Then the fuzzy inference system is constructed for measuring the trust index of a cloud service provider. Several experiments were conducted and the results were analyzed to understand the impact of the four parameters on trust index. Then the system is applied for the developed cloud computing environment to show its efficiency. Experimental results demonstrate that the proposed system can give an effective solution to trust evaluation problems in open environments.

Keywords: *Believability Index; Cloud Computing; Evolutionary Algorithm; Trustworthiness; Trust Mechanism.*

1. Introduction

Cloud computing offers almost all types of resources as on-demand services to cloud service consumers and has become part of every human's life. This provides several benefits to consumers from the viewpoint of infrastructure and administration requirements. But at the same time, security is found to be a key question. Several cloud service providers are following different types of mechanisms to offer secured services to their consumers. Still, security breaches take place in cloud environment as it is open and dynamic. In secured services, trust plays a vital role. It is defined as a determination between two entities, namely, trustee and trustor. In any open environment, trustee should possess the behavior as expected by trustor. Moreover, trust should exist mutually between trustee and trustor. In this proposed work, cloud service providers (CSP) are assumed the role of trustees and cloud service consumers play the role of trustors. In essence, earning the trust of consumers is essential for providers for the sake of their business benefits. Cloud consumers are also exhibiting much interest in knowing the trustworthiness of cloud service providers as they depend on them for the security of their valuable data. Hence, estimating the trust index of CSP is a key issue in the field of cloud security.

An access control method based on mutual trust [1] is proposed through authentication and authorization using ant colony optimization. A trust model [2] that encompasses several parameters has been presented for measuring the trust value. This model adopts various service challenges for measuring the security strength of cloud service providers. Similarly, another approach [3] is recommended to prefer trustable cloud service providers by using parameters such as auditability and interoperability. Huang and Nicol [4] explained various mechanisms for trust assessment. Further, a policy-based trust assessment approach and an attribute-based trust assessment approach have been taken into consideration for formulating an evidence-based trust assessment. Another methodology that deals with cloud trust employs software-defined network technology [5]. This model allows service providers to have controlled routing so that they can enhance the quality of their service in terms of trust. Trust is designated as a common factor in both cloud and banks [6]. As bank clients leave their money in banks, cloud consumers leave their sensitive data in cloud providers. Hence, cloud service providers should have high level of trustworthiness so that they can attract large number of potential consumers. This shows the need of proving the trustworthiness of each service provider in front of service consumers. Some protocols were proposed by Dolev et al [7] to calculate trust in a client within a multi-client environment. This model adopts small number of messages in trust calculation. Another study which mainly focuses on privacy, security and trust has been portrayed by Alouane and Bakkali [8]. Approaches have been analyzed from the viewpoints of both service consumers and service providers.

A hybrid bee colony and particle swarm optimization techniques are used for scheduling available resources to the requests with low execution time [9]. Ant colony optimization (ACO) and Lorentz transformation based approach [10] is used to illustrate the rising usage of machine learning algorithms for the improvement of system performance. Chalotra et al [11] suggested Bee Colony Optimization to solve difficult optimization problems. Ant colony algorithms such as ants system, elite ants system, ranked ants system and maximum-minimum ants system are studied for the evaluation of their effectiveness in optimization problems [12]. In the field of knowledge-based decision support systems, ACO is found to be more appropriate for achieving precise and stable solution [13]. Hence, ant colony based approach is used in our work to provide improved results in the field of optimization and model has been explained [14-15]. An extensive analysis of trust evaluation is presented by Chiregi and Jafari Navimipour [16]. This study reveals the state-of-the-art report on cloud trust assessment by considering parameters such as confidentiality, integrity, safety, reliability and so on.

The rest of this paper is formulated as follows: The concept of our proposed model is described in Section 2. The first two stages of this model are explained in sections 3 and 4, respectively. Results of experiments and their analysis on input parameters are presented in Section 5. Section 6 illustrates the results of implementation in a cloud environment. At last, Section 7 concludes our work.

2. Two-stage trust assessment model

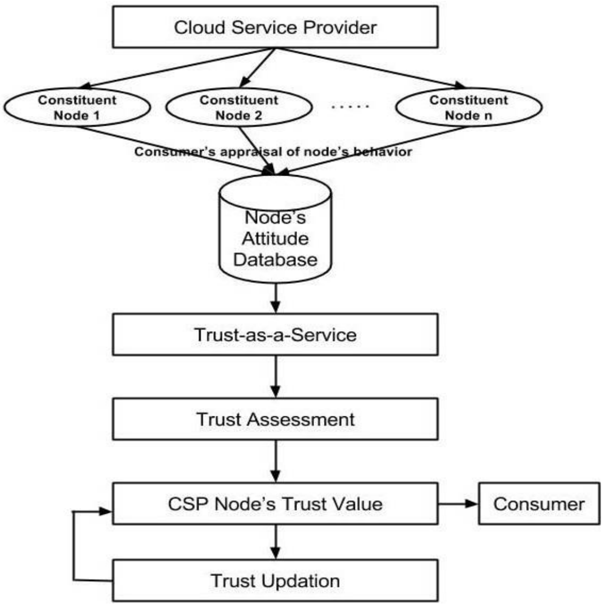

Fig. 1: Flowchart Representation of Proposed Model.

Consumers always prefer trusted services, where cloud service consumers are not an exception. Since they leave their valuable asset (data) with unknown cloud service providers, they always worry about security and privacy of their data. Hence, consumers wish to know the trustworthiness of cloud service providers so that they can opt desired services from respective providers. By considering this aspect, Trust-as-a-Service (TaaS) layer has been integrated into the architecture of cloud environment.

To measure the trust index of cloud providers, several parameters have been considered out of which Service Level Agreement (SLA), Security and Performance have been adopted. These parameters deal with the direct assessment of provider's trust index. For indirect assessment, User opinion has been used. Based on the previous experience with the provider, each consumer gives feedback about the quality of service offered by the corresponding provider. Values of these both types of parameters are stored in attitude database of the concerned provider. In turn, this database possesses the trust information of service providers. Whenever a new consumer wants to know about the trustworthiness details of service providers, they are given the exact trust index through trust assessment layer. Here, each consumer is gone through the process of their believability measurement so that genuine consumers alone are permitted to provide feedback for indirect assessment. Hence, consumer makes decisions regarding the fitness of cloud service provider to his/her requirements. This trust index is also stored in trust database so that it can be used by other consumers for their trust assessment process. This methodology is explained in Figure 1.

Assume $CSP = \{csp_1, csp_2, \ldots, csp_n\}$ as n number of cloud service providers and $C = \{c_1, c_2, \ldots, c_m\}$ as m number of cloud service consumers. Through peer-to-peer (P2P) communication network, each consumer can exchange information with the rest of consumers. When a consumer wishes to avail a service, it circulates a proposal $P = \{Rsrc, Param, Credit\}$ to all n cloud service providers. $Rsrc$ is a vector of length l_1 which specifies the amount of various resources (CPU, Storage, Bandwidth, Latency, and etc). $Param$ is a vector of length l_1 specifying QoS parameters (in terms of security and performance) as expected by a consumer. Credit expresses how much bill the provider can benefit once the service is accomplished. Assume TV as a trust vector of length $l_1 + l_2$, which specifies how much a consumer trusts a cloud service provider. It is fuzzy in the sense that it ranges from complete distrust to complete trust. It is considered that the customer opinion is connected to the past history of business between the customer and the service provider whose trust index is to be calculated.

Evaluation of consumers' believability

In order to let legitimate consumers and no-one else to provide feedback about the trustworthiness of cloud services, their level of believability has been measured at first. This stage is crucial in the sense that, in any open environment, there may be quite a few deceptive consumers. These consumers may give either positive feedback for bad cloud services or negative feedback for good cloud services. These kinds of wrong opinions will result in potential disaster in the trust assessment process of cloud services. So the believability level of each consumer has to be evaluated before they are allowed to give their feedback. Since, this believability is vague and dynamic, fuzzy theory is adopted by using linguistic labels to smoothly represent interval values.

Believability level of each consumer is assessed by all other consumers who are all availing services from the same provider. The initial believability (B_0) value committed to a new consumer is 0. When a consumer j decides to assess the believability level of consumer i, equation 1 is followed with the constraints $0 \le B_{ji} \le 1$, $1 \le i, j \le m$ and $i \ne j$.

$$B_{ji} = B_0 + \frac{\sum_{k=1}^{N} w_k S_{ik}}{\sum_{k=1}^{N} w_k} + e(t) \qquad (1)$$

where m and N represent the total number of cloud consumers and services that can be accessed in a cloud environment, respectively. $e(t)$ corresponds to an error value in calculation at time t with $0 \le e(t) \le 1$ and w_k represents the weight committed to k^{th} service with $0 \le w_k \le 1$. Finally, S_{ik} is a binary element that specifies whether consumer i has availed k^{th} service or not, and is defined in equation 2 for $1 \le k \le N$, $1 \le i \le m$.

$$S_{ik} = \begin{cases} 1, & \textit{if } k^{th} \textit{ service is availed by consumer } i \\ 0, & \textit{if } k^{th} \textit{ service is not availed by consumer } i \end{cases} \qquad (2)$$

The value of B_{ji} is understood by the equation 3.

$$B_{ji} = \begin{cases} 1, & \textit{if consumer } j \textit{ has full believability on } i \\ 0, & \textit{if consumer } j \textit{ does not have any believability on } i \end{cases} \qquad (3)$$

Relative Believability $B^R(C_i)$ of each consumer C_i, and Believability Index $BI(C_i)$ of consumer C_i are calculated by equations 4 and 5, respectively, for $1 \le i \le m$.

$$B^R(C_i) = \frac{1}{m-1} \sum_{j=1}^{m} B_{ji} \qquad (4)$$

$$BI(C_i) = \frac{1}{m-1} \sum_{j=1}^{m} P\left(B^R(C_i) \succ B^R(C_j)\right) \qquad (5)$$

Here, $P\left(B^R(C_i) \succ B^R(C_j)\right)$ is the possibility degree [17]. Finally, $BI(C_i)$, $1 \le i \le m$, are compared in opposition to the previously-fixed believability threshold (BT). This comparison leads to the interpretation as mentioned in equation 6.

$$S_{ik} = \begin{cases} accept, & if\ BI(C_i) \geq BT \\ reject, & if\ BI(C_i) < BT \end{cases} \tag{6}$$

In equation 6, $accept$ indicates that the feedback suggested by consumer C_i is accepted for trust index calculation, whereas $reject$ indicates that the feedback suggested by consumer C_i is not taken into account for trust index calculation. In our experiments, two hosts are set to behave as bad hosts. Their believability index will be between 0 and 0.2, while remaining hosts will have their believability indices between 0.8 and 1.

3. Framework for cloud trust evaluation

Table 1: Input and Output Parameters with Membership Functions

Parameter	Membership function
SLA	$\mu_T^{SLA}(sla) = \{p_T(sla),\ q_T(sla),\ r_T(sla)\}$ with $p_T(sla) < q_T(sla) < r_T(sla)$
Performance	$\mu_T^{PERF}(perf) = \{p_T(perf),\ q_T(perf),\ r_T(perf)\}$ with $p_T(perf) < q_T(perf) < r_T(perf)$
Security	$\mu_T^{SEC}(sec) = \{p_T(sec),\ q_T(sec),\ r_T(sec)\}$ with $p_T(sec) < q_T(sec) < r_T(sec)$
User opinion	$\mu_T^{FB}(fb) = \{p_T(fb),\ q_T(fb),\ r_T(fb)\}$ with $p_T(sla) < q_T(sla) < r_T(sla)$
Trust index	$\mu_T^{TRUST}(trust) = \{p_T(trust),\ q_T(trust),\ r_T(trust),$ $s_T(trust),\ u_T(trust)\}$ with $p_T(trust) < q_T(trust) < r_T(trust) < s_T(trust) <$ $u_T(trust)$

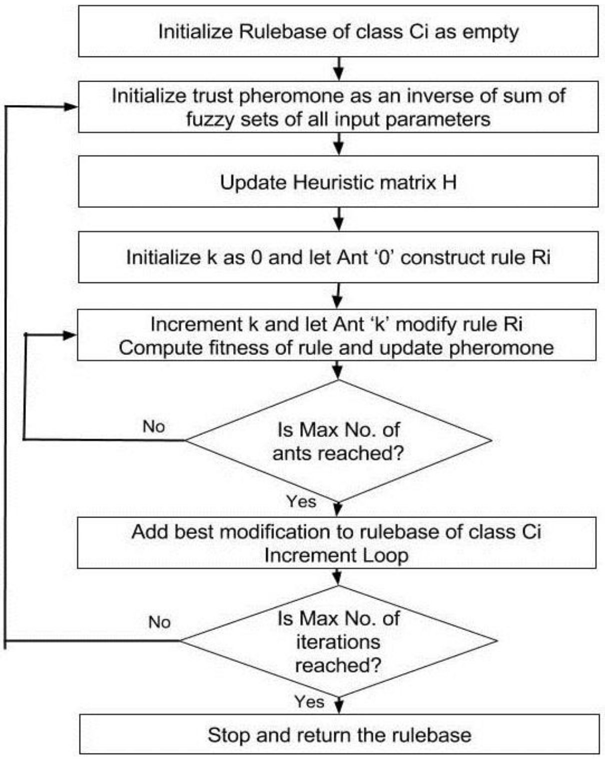
Initialize Rulebase of class Ci as empty
Initialize trust pheromone as an inverse of sum of fuzzy sets of all input parameters
Update Heuristic matrix H
Initialize k as 0 and let Ant '0' construct rule Ri
Increment k and let Ant 'k' modify rule Ri
Compute fitness of rule and update pheromone
No
Is Max No. of ants reached?
Yes
Add best modification to rulebase of class Ci
Increment Loop
No
Is Max No. of iterations reached?
Yes
Stop and return the rulebase

Fig. 2: ACO Based Approach to Generate Trust-Evaluating Fuzzy Rule base.

An interval-valued fuzzy system has been applied to evaluate the trustworthiness (trust index) of each cloud service provider. This system employs the four above-mentioned trust parameters as its input. The defuzzified trust index is produced as an output whose value represents the trustworthiness of the corresponding cloud service provider. Membership functions for the parameters are described in Table I. This table shows that the output parameter (trust index) is defined by any one of the five output classes namely, complete distrust, distrust, weak trust, moderate trust and complete trust. The system learns the rules of each output class in an independent style. Each fuzzy rule generated by this trust evaluation system is represented in equation (7).

$$If\ SLA\ is\ \mu_T^{SLA}(sla)\ and\ PERF\ is\ \mu_T^{PERF}(perf)\ and$$

$$SEC\ is\ \mu_T^{SEC}(\sec)\ and\ FB\ is\ \mu_T^{FB}(fb), \tag{7}$$

$Then\ TRUST\ is\ \mu_T^{TRUST}(trust)$From an extensive survey, ant colony optimization (ACO) is found to be suitable for quantifying the trust index of CSPs in the proposed model. Hence ACO based fuzzy rule extraction is carried out in our model. Artificial ants scrutinize the problem search space for the assembly of fuzzy rulebase. Rules extracted by this approach are precise due to the balanced participation of ants.

Initially fuzzy rule R_j is generated by ant_0 which is subsequently followed by number of iterations. In each iteration, fuzzy rules are revised by each ant in accordance with the probability as prescribed by equation 8. Here, k, i, j and τ_{ij} represent the iteration number, total number of input parameters, number of fuzzy sets to symbolize each input parameter, and trust pheromone.

$$prob_{ij} = \frac{\tau_{ij}(k)}{\sum_{i=1}^{4}\sum_{j=1}^{3}\tau_{ij}(k)} \tag{8}$$

Figure 2 presents the steps followed in the generation of trust-evaluating fuzzy rulebase for each of the five fuzzy output classes. The Heuristic matrix H is spelled out as mentioned in equation 9.

$$H = \{H_1, H_2, H_3, H_4, H_5\} \tag{9}$$

Here, each $H_c, 1 \leq c \leq 5$, is an $n \times m$ normalized matrix where n and m signifies the total number of input parameters and fuzzy values (small, medium, large).

The fitness F of each fuzzy rule R_j is calculated by equation 10.

$$F(R_j) = \frac{TP + FN}{TP + TN + FN + FP} \tag{10}$$

where, TP (True Positives), FP(False Positives), TN(True Negatives) and FN(False Negatives) are the number of cases as defined in table II.

Table 2: Confusion Matrix

Actual Type of Rule	Predicted Type of Rule	
	R_j	Other than R_j
R_j	TP	FP
Other than R_j	TN	FN

4. Experimental results

To assess and demonstrate the efficiency of our proposed system, we have simulated a cloud environment with twenty five hosts treated as neighbors and three cloud servers were set up with Intel core 2 Duo CPU, 2.5GHz, 4GB memory and GNU / Linux kernel 2.6.32. Eucalyptus [18] has been used for architecting this cloud to assist cloud consumers for availing services from cloud.

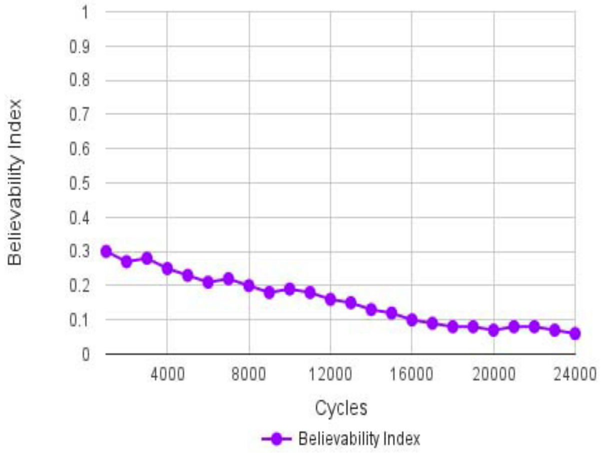

Fig. 3: Believability Index of Bad Host.

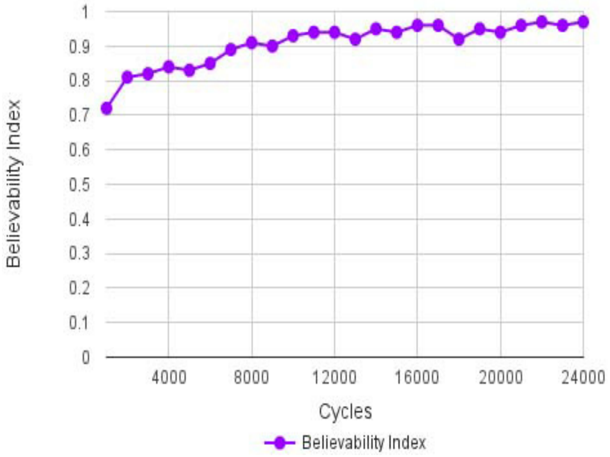

Fig. 4: Believability Index of Good Host.

The believability index of each bad host is moderate during the initial iterations. This is due to the reason that the good hosts initially assume positive believability index against bad hosts. Further, some bad hosts may also award high value to forge the bad host's trustworthiness. So some bad hosts may be guessed as good hosts. Later, as number of cycles increases, the trust evaluation system obviously identifies the negative behavior of bad hosts. Hence, all other hosts assign very minimum or negative believability value to each of the bad hosts. This leads to the decrease in index of believability and it settles down at the distrust region as shown in figure 3. In contrast, the good host's believability index is continuously increasing and sustains in the trust region. This scenario is shown in figure 4. Good hosts may initially be given low or negative index by some bad hosts for decreasing their trustworthiness. But this false impression can occur only during initial cycles. As iterations go on, the believability index of good hosts tend to improve by the sincere opinion given by parallel good hosts.

Table 3: Accuracy of Trust Measurement

Number of rules	10	27	45	62
Number of runs	70	70	70	70
Number of iterations	5000	5000	5000	5000
Number of evaluations	500000	1350000	2250000	3100000
Average RMSE – Training	0.0093	0.0081	0.0064	0.0048
Standard RMSE – Training	0.0012	0.00095	0.00078	0.00052
Best RMSE – Testing	0.0084	0.0069	0.0043	0.0027
CPU Time (Minutes)	15.71	83.26	134.29	200.17

To study the impact of number of fuzzy rules on the accuracy of trust measurement, several tests were conducted with different number of fuzzy rules and the results are shown in table III. In all tests, same numbers of iterations were done. The error tends to increase when trust measurement is done with too many numbers of fuzzy rules. Same situation arises for less numbers of rules also. For moderately large number of rules, trust value is measured with low error. But this accuracy is achieved at the expense of CPU utilization during learning process. An efficient clustering algorithm can be used here to achieve high accuracy in trust measurement with probably less number of rules.

3D representations of our results illustrate the progression of trust index with respect to the input parameters SLA and security, while performance and user opinion are fixed. Figure 5 shows the evolution of trust assessment for different performance values with reference to negative user opinion. From Figure 5, we infer that, the maximum trust what we gain is 0.5 irrespective of the value of user opinion. For poor performance, the trust index (0.3) is in distrust region, as shown in Figure 5a. Figure 5c shows that, even for good performance value, the highest trust index is only 0.5. But, it exceeds 0.3 for medium level values of SLA and security. Further, it is gradually increasing from 0 with respect to increasing values of SLA and security. But for medium performance, though we get 0.5 as a maximum trust index, the increase is uneven. Figures 6 and 7 demonstrate the progress of trust, for neutral and positive user opinions, which illustrates the relationship between the values of user opinion, and trust.

5. Implementation of a proposed system in a cloud environment

Table 4: Values of Antecedent Parameters for Three CSPS

Antecedent parameter	CSP1	CSP2	CSP3
SLA	0.7	0.8	0.6
Performance	0.6	0.8	0.8
Security	0.9	0.9	0.8
User opinion	0.8	0.9	0.7

Table 5: Trust Index (Consequent Parameter) of Three CSPS under Various Aggregation Methods

Evaluation	CSP1	CSP2	CSP3
Trust index - Center of gravity	0.8266	0.9000	0.7000
Trust index - MOM	0.9	0.9	0.695
Trust index - LOM	0.94	0.94	0.74
Trust index - SOM	0.86	0.86	0.65

After evaluating the believability of consumers, the decision making system is given with the values for the input parameters as shown in table IV, for the three clouds. CSP2 is given the highest value (0.9) for the parameter user opinion according to the feedback given by consumers. But still, it is not able to reach the highest value (1) due to the lack of maximum values in their SLA and performance parameters. Though CSP2 and CSP3 have equal values in performance, due to the difference in SLA and security, user opinions about two providers vary. This is mainly for the reason of lesser membership value in security. But CSP1 has 0.8 as a value for its user opinion. Though it has higher security value, its SLA and performance values are not optimum.

Different values are consigned to each of the 4 input parameters. In this regard, disparate fuzzy rules are set off by the fuzzy inference system. The consequences of these are aggregated by various methods to assess the trust index. Table V gives information about the three cloud service providers along with their trust indices which identifies CSP2 as the most trustworthy cloud in all aggregation methods.

6. Conclusion

In this paper, a trust assessment model is suggested for a cloud environment. Since the feedback information from cloud consumers is used in the trust assessment of cloud service providers, believability of each consumer is first evaluated using ant colony optimization by which their feedback are taken into account. Then, a rule-based fuzzy inference system is developed to neutrally assess the trust level of cloud service providers based on various parameters. Results of experiments suggest that this system is appropriate to cloud trust evaluation problems and can be used as a ranking tool for dynamic applications either explicitly or Implicitly. Using the believability indices of consumers, cloud service providers can also distinguish between trustworthy and doubtful consumers. This model has to be extended in future to help cloud providers in assessing the trust of cloud consumers for the sake of their business benefits. Hence a planned research path is to develop a methodology for the trust assessment of cloud consumers.

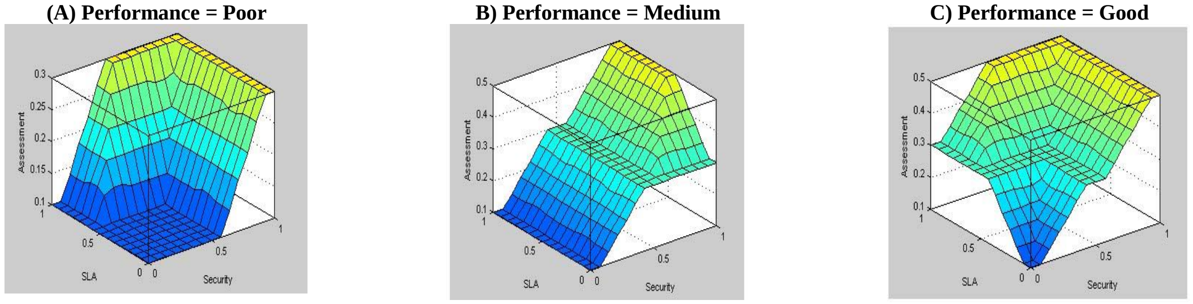
(A) Performance = Poor
B) Performance = Medium
C) Performance = Good

Fig. 5: Evolution of Trust with Respect to Negative User Opinion

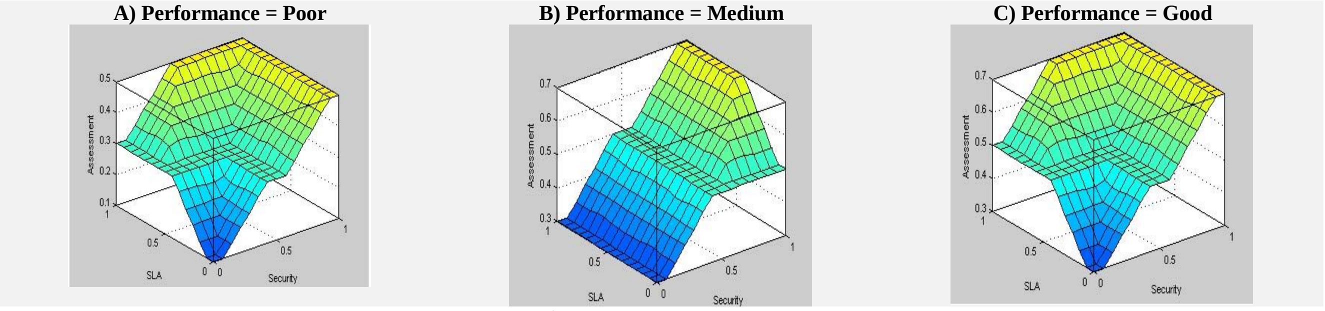
A) Performance = Poor
B) Performance = Medium
C) Performance = Good

Fig. 6: Evolution of Trust with Respect to Neutral User Opinion.

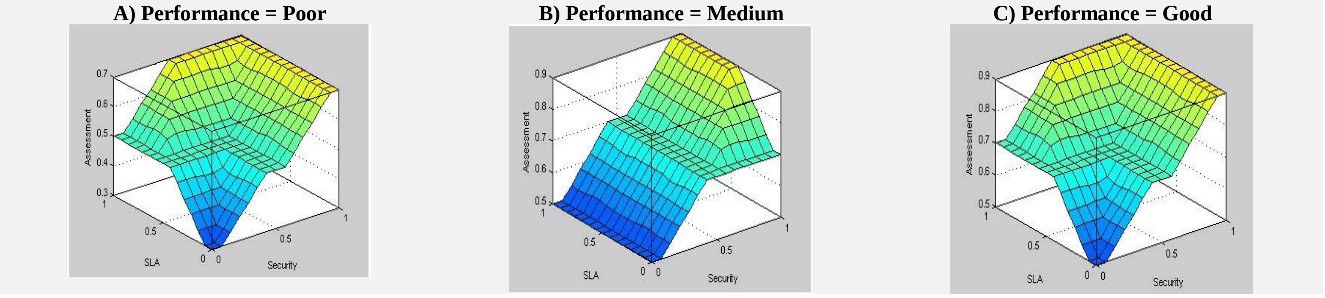
A) Performance = Poor
B) Performance = Medium
C) Performance = Good

Fig. 7: Evolution of Trust with Respect to Positive User Opinion.

Acknowledgement

The authors would like to express thanks to the anonymous reviewers for their comments, who were supportive in improving the quality and presentation of this paper.

References

[1] Lin G, Wang D, Bie Y, Lei M, “MTBAC: A Mutual Trust Based Access Control Model in Cloud Computing”, *Communications China*, (2014), pp.154-162.

[2] Rizwana Shaikh, Sasikumar M, “Trust model for measuring security strength of cloud computing service”, *Procedia Computer Science*, 45, (2015), pp.380-389. https://doi.org/10.1016/j.procs.2015.03.165.

[3] Tang C, Liu J, “Selecting a trusted cloud service provider for your SaaS program”, *Computers & Security*, 50, (2015), pp.60 - 73. https://doi.org/10.1016/j.cose.2015.02.001.

[4] Huang J, Nicol D M, “Trust mechanisms for cloud computing”, *Journal of Cloud Computing: Advances, Systems and Applications*, Vol.2, No.9, (2013), pp.1-14.

[5] Dan Pitt, “Trust in the cloud: The role of SDN”, *Network Security*, 3, (2013), pp.5-6. https://doi.org/10.1016/S1353-4858(13)70039-4.

[6] Ranjit Bose, Xin (Robert) Luo, Yuan Liu, “The roles of security and trust: Comparing cloud computing and banking”, *Procedia – Social and Behavioral Sciences*, 73, (2013), pp.30-34. https://doi.org/10.1016/j.sbspro.2013.02.015.

[7] Dolev S, Gilboa N, Kopeetsky M, “Efficient private multi-party computations of trust in the presence of curious and malicious users”, *Journal of Trust Management*, Vol.1, No.8, (2014), pp.1-21. https://doi.org/10.1186/2196-064X-1-8.

[8] Meryeme Alouane, Hanan EI Bakkali, “Security, Privacy and Trust in cloud computing: A comparative study”, *IEEE International conference on cloud technologies and applications*, (2015).

[9] Priyadarsini R J, Arockiam L, “PBCOPSO: A Parallel Optimization Algorithm for Task Scheduling in Cloud Environment”, *Indian Journal of Science and Technology*, Vol.8, No.16, (2015), pp.1-5. https://doi.org/10.17485/ijst/2015/v8i16/63248.

[10] Dizaji Z A, Gharehchopogh F S, “A Hybrid of Ant Colony Optimization and Chaos Optimization Algorithms Approach for Software Cost Estimation”, *Indian Journal of Science and Technology*, Vol.8, No.2, (2015), pp.128-133. https://doi.org/10.17485/ijst/2015/v8i2/57776.

[11] Chalotra S, Sehra S K, Brar Y S, Kaur N, “Tuning of COCOMO Model Parameters by using Bee Colony Optimization”, *Indian Journal of Science and Technology*, Vol.8, No.14, (2015). Pp.1-5. https://doi.org/10.17485/ijst/2015/v8i14/70010.

[12] Rezaeean A, Mirzaei A, Khozein A, “Optimization of Embankments by Ant Colony Optimization Algorithm”, *Indian Journal of Science and Technology*, Vol.5, No.1, (2012). pp.1863-1869.

[13] Ghanbari A, Kazemi S M R, Mehmanpazir F, Nakhostin M M, “A Cooperative Ant Colony Optimization-Genetic Algorithm approach for construction of energy demand forecasting knowledge-based expert systems”, *Knowledge-Based Systems*, 39, (2013), pp.194-206. https://doi.org/10.1016/j.knosys.2012.10.017.

[14] Sivakami Raja, Saravanan Ramaiah, “2S-FAT based DLS Model for Cloud Environment”, *Arabian Journal for Science and Engineering*, Vol. 41, No. 8, (2016), pp.3099-3112. https://doi.org/10.1007/s13369-016-2084-8.

[15] Sivakami Raja, Saravanan Ramaiah, “CCDEA: Consumer and Cloud – DEA Based Trust Assessment Model for the Adoption of Cloud Services”, *Cybernetics and Information Technologies*, Vol. 16, No. 3, (2016), pp. 52-69. https://doi.org/10.1515/cait-2016-0034.

[16] Chiregi, M., Jafari Navimipour N., “Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms”, *Journal of Electrical systems and Information Technology* (2017).

[17] Wei C P, Tang X, “Possibility Degree Method for Ranking Intuitionistic Fuzzy Numbers”, *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, Toronto (2010), pp. 142-145.

[18] Eucalyptus. http://www.eucalyptus.com.