**A Method for Trust Determination in Cloud Computing Environments: Survey Paper**

**Outline:** Cloud computing is notably one of the most emerging trends in Information Technology by providing “Everything as a service” idea. Cloud Computing is of growing interest to most of the companies because of its easy deployment, connectivity, configuration, automation and scalability. Trust is one of the fundamental security concepts on storing and delivering such services. In this survey paper I analyze various models proposed by various authors for trust determination in cloud computing.

**Title: A Method for Trust Determination in Cloud Computing Environments**

**Abstract:** Analyze various trust determination models proposed by various authors working in this field is the most important motto of this survey paper. First solution talks about trust determination in SaaS (Software as a service), offered over the cloud. A trust management model has been introduced to manage the trust and its properties for SaaS in cloud computing environment. The model represent the direct trust, recommended trust, reputation etc. [1].

Second solution talks about plan and improve a fuzzy logic based trust and reputation model for safe resource allocation in cloud computing. First, the user access a resource block through the scheduling manager and a structure will send to the user following accessing the resource block to fill the characteristic values of Trust Factor (TF) and Reputation Factor (RF). The TF and reputation value is after that computed for the resource center and it is specified to the fuzzy logic system obtain the Security Score (SS) of a resource center. To offer the security controls is the advantage of the suggested method in accessing the cloud resources from cloud computing owing to different security issues occurred in networks, databases, resource scheduling, transaction management and load balancing [7].

Third solution author propose a method for trust determination based on fuzzy comprehensive evaluation theory for cloud computing to protect user data through trust determination of cloud services after the introduction of trust ontology for cloud services and define user preference trust values [18].

**Section 1: *Introduction -***

Cloud computing has emerged since 1999. Trust determination has been a concern. In present literatures, trust based on human notation is applied widely to cope with new security concern in cloud.

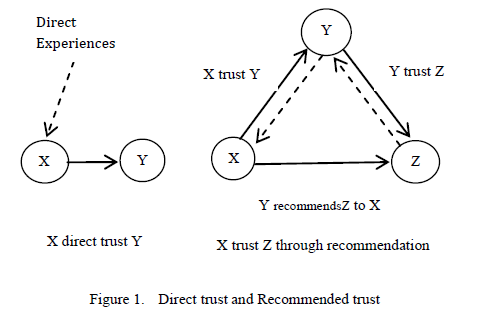
This survey paper is categorized into various sections. Section 1 is Introduction. It states the problem and its solution being analyzed in this paper. Section 2 talks about first solution i.e. Trust management in SaaS. Section 3 talks about second solution for trust determination in cloud computing i.e. fuzzy logic and neural network based trust and reputation model. Section 4 talks about trust determination based on fuzzy comprehensive evaluation theory for cloud computing. In Section 5 I try to present what I think about trust determination in clouding computing. Section 6 talks about conclusion drawn after analyzing various authors work. Section 7 states references used for this analysis.

**Section 2:**

**Introduction:** In this paper author has addressed to the problem of “Trust management in SaaS”. SaaS layer in cloud computing provides applications on demand over internet i.e. delivers technology needs of a business as a service [1]. User’s store and access confidential data to and from the cloud making security concern in SaaS layer of cloud computing crucial. In this paper author has proposed a formal trust model from the basic concepts of trust. Consumer will evaluate the trust of the SaaS before accessing it. Author claims that model proposed is capable of updating recommended trust value dynamically for each entity of cloud [1].

**Trust Basics:** Trust life cycle consist of three steps: trust establishment, trust update and trust revocation. Trust is divided into two classes: direct trust and recommended trust [2] [3] [4]. Main concepts involved in trust management are trustor (Service Providers), trustee (Consumers) and trust model.

1. **Trust Definition:** Author has mentioned various definitions of trust which mean X will trust Y, when Y behaves exactly the way X expects it to behave. It can be of two types, direct trust where X trust Y based on his own personnel experiences, recommended trust where X trust Z based on experiences/recommendations of Y [1].



1. **Trust Properties:** Authors proposed model is based on below mentioned trust properties [5] [6] [1]

**Asymmetry**: A trust relation is asymmetric. In fact, X trusting Y does not imply that Y trusts X, too. [1]

**Reflexivity**: Trust is reflexive because each entity trusts itself [1].

**Context dependence**: A trust relation concerns a precise action on a precise object and cannot be generalized to other actions or objects [1].

**Scalability**: Trust is scalable since it may evolve during communication. This evolution implies trust level modification which also implies a modification of entities reputation. Trust levels precise trust degree while reputation designates the general appreciation of a given entity [1].

**Partial Transitivity**: Trust follows transitivity property Y recommends Z to X if and only if X trusts Y and Y trusts Z otherwise, it’s not follow transitivity property [1].

**Subjective**: Trust is a level of subjective probability [1].

**Uncertainty**: It is important characteristic of trust which means trust relationships between entities are fuzzy and stochastic, especially for stranger entities [1].

**Space based**: Recommendation trust satisfies the space based variant property [1].

**Time based**: Direct trust satisfies the time-based variant property [1].

**Proposed Trust Management Model**

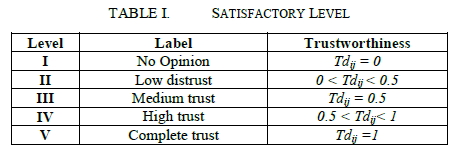
Author has proposed a trust management model for SaaS based on trust basics. Before accessing service and data from cloud, users verify the trust level of service provider in cloud environment. So the proposed trust model first verifies the trustworthiness of service provider then access services and/or data. The main idea in this proposed model is trust management system based on space variant evaluation for recommendation trust and time variant evaluation for direct trust [1]. In addition reputation concept has also been included.

**Proposed Trust Management Components**

1. Trust: Trust is a measure of trustor trusting a trustee, formed through direct or recommended trust. Trust is usually evaluated by trust degree and described with trust relation.
2. Trust Degree: [1] Used to evaluate degree of trust between trustor (user) and trustee (service provider). Tdij (Ti,Tj, Sk, t) wherei ≠ j; 0 ≤ Tdij (Ti,Tj, Sk,t) ≤ 1

Trustor Ti, trustee Tj, Sk is kth service and t is time.

1. Trust Relation: [1]Trust relation Trij is the relationship between trustor Ti and trustee Tj, trusted set Q. Directed binary relation Trij<Ti ,Tj > ϵ Q x Q. Direct and recommended trust are two types of trust.
2. Trust Levels: [1] Represents trust worthiness using degree of trust



1. Trust Model: [1] Trust management model is defined as

TM = ( Ti , Tj, Trij, Sk , RFi, t), i ≠ j;

Trustor Ti , trustee Tj, trust relation between trustor and trustee Trij, Sk is the kth service, RFi is the trust reputation factor, time t

1. Direct Trust: [1] Relationship between two entities which have had direct interactions. Direct trust degree is denoted by Dt (Ti,Tj, Sk,t), i ≠ j, Ti trustor, Tj trustee, Sk specified service, t is time of the interaction. Direct trust satisfies the time based variant property.

Time based experience: [1] Direct trust decay with time. The trust an entity has acquired at time t in a perspective of a specified service might not be same as the trust attributed to him in the same perspective at time t + Δt

Dt (Ti, Tj, Sk, t + Δt) < Dt (Ti, Tj, Sk, t)

Let tc and tl denote the current time and last interaction time then decay function γ is defined as



Where K ϵ {1, 2, 3…}, γ ( tc , tl ) ϵ [0,1]

K determines the rate of decay of the direct trust degree with time Δt. If RFi is the reputation factor of trustor i then calculate direct trust degree at present time tc using

[1]

Good reputation factor generally means better privileges.

1. Recommended Trust: If two entities do not have direct interaction, then trust relationship is established by another entity's recommendation, called recommended trust. In the model, each entity will maintain the list of all other entities with similar services and called as Recommended List Table. Rt(Ti, Tj,Sk,t), I ≠ j. Recommended trust of rth trust chain is calculated using [1],

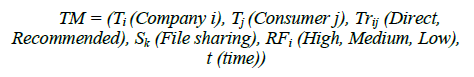


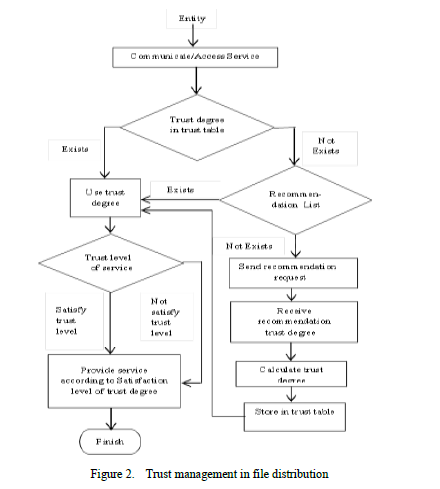
The weight between the node m and m+1 in the rth trust chain Tcij(r) is defined as [1]:



Where, np is the number of positive interaction between node m and m+1, n is total no of interaction which is the summation of number of positive np and negative nn interaction; sl is [1] defined as satisfaction level. Sl is depends on availability, processing capacity, recovery time, connectivity and peak-load performance which is defined in service level agreement, sl ϵ [0,1].

**Case Study:** Author has explained the trust management model TM = (Ti, Tj,Trij, Sk, RFi, t) using an example [1]:





**Authors Conclusion:** Author has introduced direct trust with a time variant evaluation method and the recommended trust with space variant evaluation method. Future work will include development of separate algorithms for evaluation of direct trust and recommendation trust schemes proposed in this model.

**Section 3:**

**Introduction:** In this paper author has proposed fuzzy logic based trust and reputation model. The main features of this work are [7]:

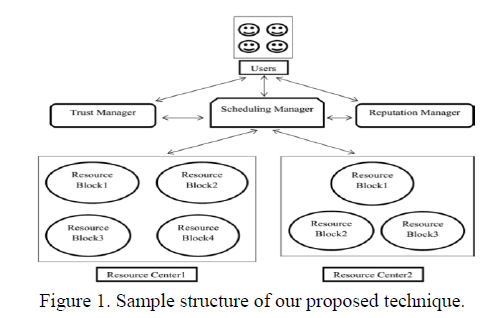
1. Author has progressed a mathematical model for computing the TF (trust factor) and RF (reputation factor) based on the characteristic values.
2. Author has suggested algorithm based on trusts and reputations based security score (SS) algorithm.

**Need for Security in Resource Allocation of Cloud Computing:**

The main security aspect with the cloud computing is that the owner of the data will not have power to know where his data is located [7].

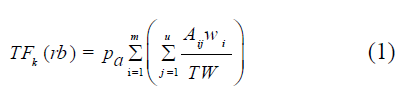
**Proposed Resource Allocation in Cloud Computing**

Using fuzzy logic and neural network based trust and reputation factor, author describes suggested model for the allocation of resources in cloud computing [7].



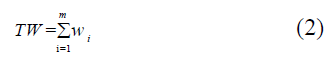
**Proposed model works as follows:** To access the resource block, the users offer a task which is in the resource center through the scheduling manager. The scheduling manager makes sure that the resource block where it is situated provides the path to the related resource center. The user presents the attributes value for TF and RF after access the resource block. TF value and RF value are then given to the fuzzy logic system and then neural network to acquire SS [7].

**TF of resource center:** The computation of TF of each resource block is as follows:

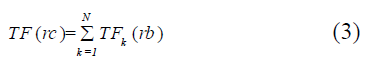
[7]

Where TF k(rb): TF of resource block, Pa: Probability of users applied the resource block, Aij: TF characteristic values given by each user, wi: Weight value of each TF characteristics. TW: Total weight value, m: Total number of characteristics regarded for TF, and u: Total number of users.

Sum of the weight values of every characteristic is calculated as:

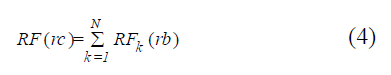


Author says that we need to calculate TF for the resource center after finding the TF for each resource block. It is calculated by below formula:



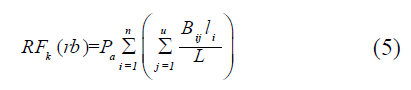
Where TF (rc): TF of a resource center, and N: Total number of resource blocks in a resource center [7].

**RF of a Resource Center:** RF for a resource center is calculated as [8]:



Where RF(rc): Reputation Factor of a resource center, RFk(rb): Reputation Factor of each resource block in a resource center, and N: Total number of resource blocks in a resource center.

RF for each resource block is calculated as:

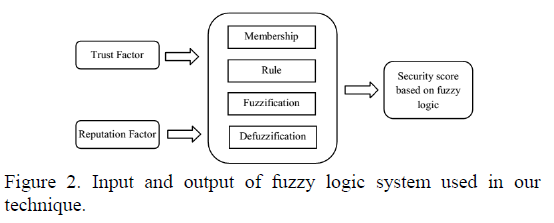


Where Pa: Probability of users applied the resource block, Bij: RF characteristics values specified by the user, li: Weight value of each RF characteristics, L: Total weight value of the characteristics regarded for RF, n: Total number of characteristics regarded for RF, and u: Total number of users.

The computation of total weight value L of the characteristics for the RF is specified as:



**Fuzzy Logic Model**: Here author describes fuzzy logic method. TF value TF (rc) and RF value RF (rc) are giving as input to the fuzzy logic system to discover SS of the resource center.



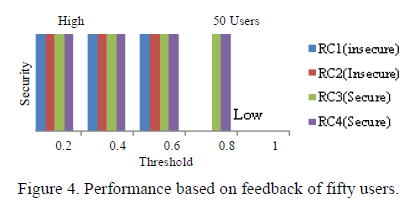
SS is obtained from fuzzy logic based on below equation. Here TF (rc) and RF (rc) are input to fuzzy logic system.

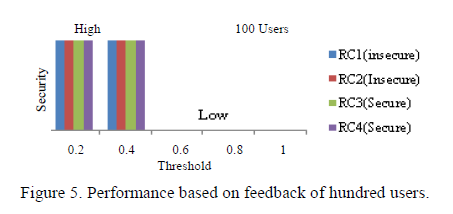


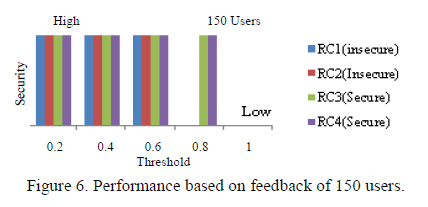
**Results and Discussions**

**Experimental setup:** Author has used 4GB ram and executed method in java (jdk1.6). Three data sets financial, medical and RDB are used. Four dissimilar resource centers having three dissimilar resource blocks (3 data sets as resource blocks) are used. Different users provide different TF, RF values after applying resource and examine presentation of the method.

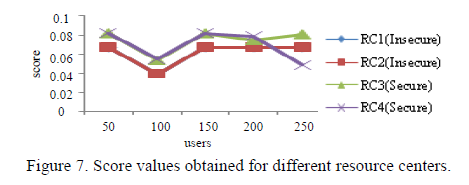
**Fuzzy System Results:** [7] When the thresholds is set as 0.2, 0.4 and 0.6, authors system demonstrates the complete resource centers applied as secured and when threshold was set as 0.8, system demonstrates the third and fourth resource centers as secured and for the threshold 1, system demonstrates the complete resource centers author applied for the method is not secured.







**Performance Analysis:** Based on the feedback of the users, the first and second resource centers are insecure and the third and fourth resource centers are secure

****

**Authors Conclusion:** Author has suggested a method for secure resource allocation in cloud computing by means of fuzzy logic based on trust and reputation model. Author has applied the trust manager and reputation manager to revise the security of a resource center. At first, user executed a task through the scheduling manager and following the task, user give the characteristic values for TF and RF of the resource user applied. Based on the characteristics values specified by the users, TF and RF is computed and specified to the fuzzy logic system. With the comment of dissimilar number of users, author have executed the experimentation of the method and with dissimilar threshold values to make a decision whether a resource center is protected or not [7].

**Section 4:**

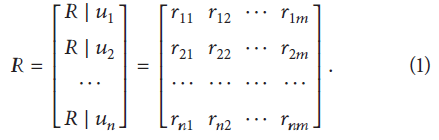
Here author has discussed trust determination based on **fuzzy comprehensive evaluation theory** for cloud computing to protect user data after introducing **trust ontology** for cloud services and defining **user preference trust values**. Author introduces some cloud service attributes to study layered service representation for trust preference and then apply Fuzzy comprehensive evaluation theory to perform trust determination.

**Related Work:** Trust in cloud computing involve **spatial** and **temporal** factors, which has the characteristics of **subjectiveness and fuzziness**. Therefore trust can be determined using fuzzy mathematical theory that involves one or more factors to **deal with vagueness** and *subjective judgment of multiple factors according to their importance* [9-11].

Trust itself may be subjective. Thus, dynamic trust determination on cloud services has to involve some fuzzy subjective information of cloud services to cloud users [12-17].

STEPS:

1. Determine evaluation factors 𝑈 = {𝑢 1, 𝑢2,. . . , 𝑢𝑛}, where 𝑢𝑖 (𝑖 = 1, 2, . . . , 𝑛) is the 𝑖th evaluation factor.
2. Determine set of evaluation levels V = {V1, V2,. . . , V𝑚}, where V𝑗 (𝑗 = 1, 2, . . . , 𝑚) is the 𝑖th evaluation level that corresponds to a fuzzy subset.
3. Evaluate single factor ui through establishing a fuzzy relationship matrix (R|ui) based on U and V



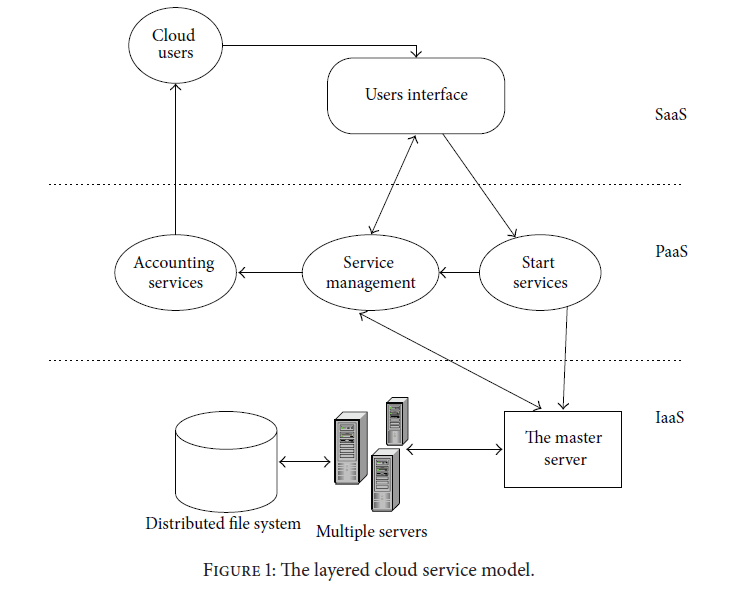
1. W is the weight vector to determine relative importance of the evaluation factor.
2. W\*R = B fuzzy comprehensive evaluation result vector B

A cloud user can perform trust evaluation on services in accordance with the service properties. However current research on trust metrics mainly describes the trust of service provider on the user without considering the need of mutual trust.

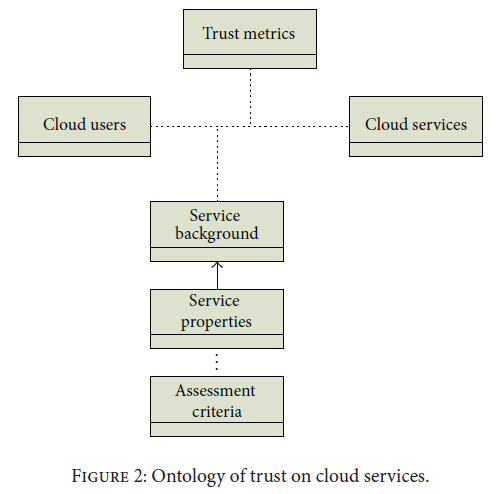
In this paper author has aimed to propose a method of trust evaluation from the point of view of protecting user's data in cloud.

**The Proposed Trust Determination Method**: Here author explains service trust ontology (existence) through a layered cloud service model. Three different service model defined for the cloud, that is, IaaS, PaaS, and SaaS

1. *Hierarchical representation of Cloud Service Information:* The **IaaS** layer provides the basic services such as **databases, file systems, and storage** (infrastructure). The **PaaS** layer provides services related to the **development environments** (platform), and the **SaaS** layer provides **software as a service** to meet user application needs (software). [18]



1.1 *Trust Ontology*



1. Trust metrics: Based on the past trust relationship, cloud users measures the cloud services. Trust metric may also consist of direct and recommendation trust, which affects the selection of services in the future.
2. The cloud users who are the service requesters and who perform trust evaluation on cloud services.
3. The cloud services that are offered by a service provider and are thus evaluated by the cloud users.
4. The properties of a cloud service as described by service attributes such as temporal and spatial factors, user trust factors, and historical behavioral factors.
5. The assessment criteria that are used to measure the trust on each attribute of a service.
6. Service background that refers to the nature of a service, such as “storage service.” [18]
   1. *Preference Trust:* Preference trust is used to evaluate trust on service providers in order to meet personalized service needs of cloud users based on the ontology of trust on cloud services from the aspects of time, space, historical behavior, and so forth.

Preference trust is based on various factors:

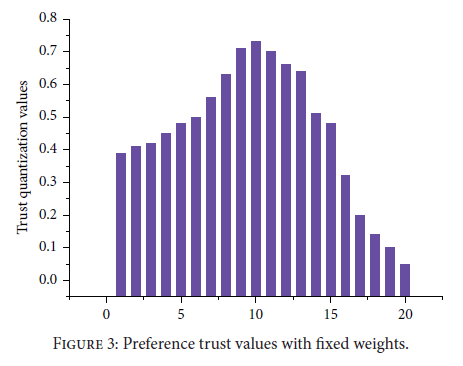
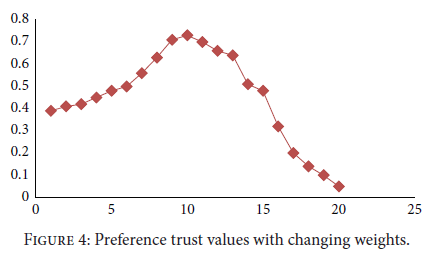
1. Interactive process between cloud users and cloud services, which depends on user preference expressed using temporal, spatial, and other factors such as behavior and history.
2. Feedback on historical behavior of cloud service, which can be used to check integrity of cloud services.
3. Determination of service trust is to establish a quantitative evaluation system to apply trust evaluation on cloud services.
4. Determination of preference trust is to perform trust evaluation using a given preference system to determine the different factors 𝑇0, 𝑇1, . . . , 𝑇𝑛−1 and to apply the various preference weights 𝑊0,𝑊1, . . . , 𝑊𝑛−1, where to arrive at a trust value  

*Description of the method:*

Determination of service preference trust consists of two steps:

1. Determine the best weight distribution for each factor based on different trust preferences.

2. Establish a method to determine the factors of trust based on different trust preferences to get a comprehensive value for the cloud service preference trust.

**Authors Conclusion:** The results in Figures 3 and 4 clearly show that when the *cloud service performs honestly, preference trust gradually increases along with the improvement of the historical behavior value.* However, when the service provider’s behavior becomes dishonest, feedback from cloud users would cause the value of the historical behavior factor to go lower, dragging down the preference trust values over the weights of the factors. Thus, the proposed trust quantification method is effective according to the results of the experiment.

**Section 5: My proposed solution**

While going through all the papers and reading all the proposed solutions by all the three authors in this survey paper, I feel if we can combine all the solutions into one solution, it can give better trust determination.

In first paper author is talking about direct and recommended trust. In second paper author is talking about trust determination based on TF (Trust Factor) and RF (Reputation Factor) applying to fuzzy logic and in third paper author is talking about preference trust applied to fuzzy logic. If by some means we can combine all these factors while determining trust, I believe it can give better result as trust is based on all the factors proposed in different papers and all the factors have huge impact on trust value.

**Section 6: Conclusions** - In first solution direct and recommended trust is proposed but limitation is that there needs to be some approach to calculate this trust value.

In second solution fuzzy logic based on TF and RF value is proposed. Security score is calculated and based on this score a resource center is said to be protected or not. Limitation is that in this approach personalized service needs of cloud users is not taken into account.

I third solution personalized needs of cloud users is taken into account to determine trust through fuzzy comprehensive evaluation theory, but TF and RF values are not taken into account.

So a better solution can be if we can combine the positive aspects of all three solution proposed, i.e. direct and recommended trust values, TF and RF values and preference trust to determine trust value.

**References**: List all the sources you have referenced. It should include the author name, title of the paper, conference or journal name, year of publication, etc. 

[1] Somesh Kumar Prajapati, Suvamoy Changder, Anirban Sarkar 2013

[2] H. Zhu, B. Feng, R.H. Deng, “Computing of trust in distributed networks”, http://eprint.iacr.org/2003/056, 2003.

[3] Alfarez Abdul Rahman, Stephen Hailes, “Supporting Trust in Virtual Communities”. 33rd Hawaii International Conference on System Sciences, 2000.

[4] F. Azzedin, M.Maheswaran, “Towards Trust-Aware Resource Management in Grid Computing Systems”, 2ndIEEE/ACM International Symposium on Cluster Computing and the Grid, pp. 452, 2002.

[5] R. Abassi, S. G. El Fatmi, “Towards A Generic Trust Management Model”, 19thInternational Conference on Telecommunication (ICT), pp. 1 – 6, 2012.

[6] Q. Guo, D. Sun, G. Chang, L. Sun, X. Wang. “Modeling and evaluation of trust in cloud computing environments”, 3rdIntl. Conf. on Advanced Computer Control, pp. 112-116, 2011.

[7] Kamalanathan Chandran, Valarmathy Shanmugasudaram, and Kirubakaran Subramani, “Designing a Fuzzy-Logic Based Trust and Reputation Model for Secure Resource Allocation in Cloud Computing,” http://dblp.unitrier.de/search?q=trust%2C+cloud+computing 2015

[8] Malaga R., “Web-Based Reputation Management Systems: Problems and Suggested Solutions,” *Journal of Electronic Commerce Research*, Springer Netherlands, vol. 1, no. 4, pp. 403-417, 2001.

[9] E. J.Chang, K. F.Hussain, and T. S.Dillon, “Fuzzy nature of trust and dynamic trustmodeling in service oriented environments,” in *Proceedings of the Workshop on Secure Web Services (SWS* *’05)*, pp. 75–83, ACM Press, 2005.

[10] M. Jaiganesh, M.Aarthi, and A.V. A. Kumar, “Fuzzy ART-based user behavior trust in cloud computing,” *Advances in Intelligent* *Systems & Computing*, vol. 324, pp. 341–348, 2015.

[11] R. Klinger and K. Tomanek, “Classical probabilistic models and conditional random fields,” Algorithm Engineering Report TR07-2-013, 2007.

[12] B. Li, B.-Q. Cao, K.-M. Wen, and R.-X. Li, “Trustworthy assurance of service interoperation in cloud environment,” *International Journal of Automation and Computing*, vol. 8, no. 3, pp. 297–308, 2011.

[13] M. Armbrust, A. Fox, R. Griffith et al., “Above the clouds:a berkeley view of cloud computing,” *Communications of the* *ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[14] J. Harauz, L. M. Kaufman, and B. Potter, “Data security in the world of cloud computing,” *IEEE Security & Privacy*, vol. 7, no. 4, pp. 61–64, 2009.

[15] S. M. Habib, S. Ries, M. M¨uhlh¨auser, and P. Varikkattu, “Towards a trust management system for cloud computing marketplaces: using CAIQ as a trust information source,” *Security & Communication Networks*, vol. 7, no. 11, pp. 2185 2200, 2014.

[16] A. Jøsang, R. Ismail, and C. Boyd, “A survey of trust and reputation systems for online service provision,” *Decision Support* *Systems*, vol. 43, no. 2, pp. 618–644, 2007.

[17] M. Brock and A. Goscinski, “Enhancing cloud computing environments using a cluster as a service,” in *Cloud Computing:* *Principles and Paradigms*, chapter 7, JohnWiley & Sons, Hoboken, NJ, USA, 2011.

[18] Xiaohui Li,1,2 Jingsha He,1 Bin Zhao,1 Jing Fang,1 Yixuan Zhang,1 andHongxing Liang3, “A Method for Trust Quantification in Cloud Computing Environments,”http://dblp.unitrier.de/search?q=trust%2C+cloud+computing 2015