ISSN No. 0976-5697

Volume 4, No. 2, Jan-Feb 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# Multi Criteria Trust Model in Grid Computing Systems

Ahmad Habibizad Navin
Department of Computer Engineering
Islamic Azad University
Tabriz, Iran
Ah_habibi@iaut.ac.ir

Neda Azari Khosroshahi*
Department of Computer Engineering
Islamic Azad University
Tabriz, Iran
n.azari@iaut.ac.ir

Ali Asgar Pourhaji Kazem
Department of Computer Engineering
Islamic Azad University
Tabriz, Iran
A_pourhajikazem@iaut.ac.ir

*Abstract***:** One important problem in choosing a secure resource in grid is how we can put up with the vast range of selection and high degree of strangeness. To overcome this problem, trust-based solutions are suggested. Recent trust models focus on some security criteria to calculate trust factor. In this paper, a trust model is presented which aggregates criteria to select a secure resource by using a fuzzy Multi Criteria Decision Making method. For determining the trust factor and deciding whether or not to trust an entity, various criteria are considered. Among the existent criteria, self defense capability, direct trust and reputation are exploited. The obtained results show better performance of the presented method with respect to the number of failed requests, but it needs more execution time.

***Keywords:*** trust, reputation, multi criteria decision making

## I. INTRODUCTION

Grid computing is a distributed environment that enables sharing of heterogeneous resources such as computers, software, devices, disk capacity, network bandwidth, special devices (e.g. radio telescope) and people/collaborators. Some challenges of grid are resource discovery, resource allocation, security, computational economy, uniform access, resource selection, network management, and data locality [12]. This paper focuses on secure resource selection which has been recognized as an important factor of security.

Grid provides a virtual framework for sharing resources across institutional boundaries. Unfortunately, the opinion of having a virtual framework is not pleasant for entities because of the risk of being related with the notion of “sharing” services and resources. This concern forces the entities to use their own closed-box resources, instead of the utilization of grid system. That is an inefficient way to utilize resources [13]. To overcome this problem, two solutions are suggested. The ideal one is to have an environment with full trust. However, such a solution cannot be obtained. Thus, trust based solutions are applied [20]. Trust is a combination of human community and cyberspace security. Similar to human communications, trust in cyberspace has been determined by linguistic expressions in a nominal scale. Trust is a multiple concept that relates to a firm belief in attributes such as honesty, reliability, and competence of entities. Azzedin and Maheswaran defined trust as follows [10,13]:

> Trust is the firm belief in the competence of an entity to act as expected such that this firm belief is not a fixed value associated with the entity, but rather it is subject to the entity's behavior and applies only within a specific context at a given time. The firm belief is a dynamic value and spans over a set of values ranging from very trustworthy to very untrustworthy.

Because of the importance of trust, some trust models have been presented up to now. These trust models consider some security criteria to calculate the trust factor. By using a fuzzy multi criteria decision making [14-17], in this paper, a new trust model is presented which aggregates all criteria to select a secure resource, to handle uncertainties or fuzziness behind all trust attributes. Our model considers various criteria such as self defense capability, direct trust and reputation. To achieve a relatively complete trust model, we have studied the effect of self defense capability in term of the number of failed requests and execution time.

The rest of the paper is organized as follows: section 2 reviews the related literature in the area of reputation and trust. Section 3 presents the proposed method. The simulation results appear in section 4. The conclusions are in section 5.

## II. REVIEW OF THE RELATED LITERATURE

In this section, the literature related to reputation and trust-based security solutions are reviewed. Song et al. [1] presented a trust model based on fuzzy logic in order to secure grid resources. This model secures grid resources by propagating and updating trust values among different grid sites. In order to reduce vulnerability of platforms, they incorporated fuzzy trust with their model, and defended various sites. Also, they developed a SeGo scheduler, to optimize the computation power while assuring security under restricted budgets. In another work, Song et al. [2] proposed a trust model based on fuzzy theory in order to handle the uncertainties or fuzziness behind all trust attributes. This trust model integrates many features of reputation and measurable self-defense capability into numerical quantities, which can be used to signify the trust index of a grid resource site. They designed a secure grid outsourcing system for scheduling numerous independent and indivisible jobs to grid sites. Tajeddine et al. [3] proposed PATROL-F model (comprehensive reputation-based Trust mOdeL with Fuzzy subsystems) in order to defend interacting hosts in distributed systems. This model includes the various concepts which are vital in calculating reputation value and the decisions whether to trust or not. PATROL-F also incorporates similarity, popularity and activity among hosts. PATROL-F is the fuzzy version of PATROL [4]. Also a trust model using fuzzy logic is developed by Ramchurn et al [5] to determine prior interactions. In this model, reputation is calculated through gathered information from available agents in the community and confidence is obtained by direct interactions. Moreover, Castelfranchi et al [6,7] proposed a trust model using fuzzy maps. In this model, two classifications of attributes are used: internal and external attributes and four types of belief sources are considered including reputation, categorization, reasoning and direct experiences. A new method was developed by Vijayakumar et al. [8,11] to provide trust and reputation aware security for choosing resources in Grid computing. Self-defense capability and reputation weightage are used to calculate trust factor. Abdual Rahman et al [9] developed a model based on reputation and experiences in which the entities can decide on the trustworthiness of other entities. A nominal definition of trust and reputation is proposed by Azzedin and Maheswaran [10]; they also discussed a model for incorporating trust in grid systems.

## III. MULTI CRITERIA TRUST MODEL

In this section, a new Multi Criteria Trust Model (MCTM), in grid computing systems is presented. This model uses the grid architecture. When an entity (an entity can contain several resources), forwards a request to the broker, the broker finds a set of entities which are able to perform the requests by using a common resource discovery method. The proposed method inputs this set of entities and selects one of them as a secure resource by using a fuzzy multi criteria decision making. Also, this model considers three necessary criteria consisting of self defense capability, direct trust and reputation in the selection phase which are discussed as follows. Each entity includes a trust agent and each trust agent maintains a direct trust table which includes the direct trust level between the entity and the other entities for context c.

### A. Decision criteria

*Self Defense Capability*

Some security factors may be considered as Self Defense Capability (SDC). In this model, the following factors are considered:

- Intrusion detection capability, the entity's ability to protect the system against network intrusions;
- Anti-virus capability, the entity's ability to defend against malicious codes and viruses; and
- Fire wall capability, the ability of protecting an entity against other network accesses.

All of these factors get a weight based on their contribution to security. For calculating the self defense capability, the weights are multiplied by the values of the factors using (1).

$$SDC = \sum_{i=1}^{3} W(i) * A(i) \qquad (1)$$

Note that in this formula, W(i) is the weight assigned to each factor and A(i) is the value of factor i. The values of SDCs are kept in the broker and used in the decision making process.

*Direct Trust Level (DTL)*

After having interaction between two entities, a trust level (TL) based on the satisfaction of requester entity is stored and updated in its own DTL table, for example Table 1 shows the direct trust level for entity m. The satisfaction value depends on considered factors by the requester entity via comparing the obtained results and their expectations.

Table 1. Direct trust table for entity m

| DTL | entity 1 | entity 2 | entity 3 | … | entity m-1 |
|---|---|---|---|---|---|
| context 1 | $TL_{m,1}^{c1}$ | $TL_{m,2}^{c1}$ | $TL_{m,3}^{c1}$ | … | $TL_{m,m-1}^{c1}$ |
| context 2 | $TL_{m,1}^{c2}$ | $TL_{m,2}^{c2}$ | $TL_{m,3}^{c2}$ | … | $TL_{m,m-1}^{c2}$ |
| … | … | … | … | … | … |
| context i | $TL_{m,1}^{ci}$ | $TL_{m,2}^{ci}$ | $TL_{m,3}^{ci}$ | … | $TL_{m,m-1}^{ci}$ |

After completion of the interaction, the result of the interaction between $E_i, E_j$ is updated according to (2).

$$DTL(E_i, E_j, c) = (1-\theta) \times DTL(E_i, E_j, c) + (\theta) \times STL(E_i, E_j, c) \qquad (2)$$

Where, $DTL(E_i, E_j, c)$ is the direct trust level which is evaluated and assigned by $E_i$ to $E_j$ for context $c$ before having interaction which is obtained from $E_i$ table. $STL(E_i, E_j, c)$ is the satisfaction of requester entity $E_i$ using the resources of $E_j$ for context $c$, θ is a value between 0 and 1. If θ>0.5, more priority is given to DTL rather than STL.

*Reputation*

According to Azzedin and Maheswaran, "The reputation of an entity is an expectation of its behavior based on other entities' observations or information about the entity's past behavior within a specific context at a given time" [10]. In our model for calculating the reputation of a specific entity, the broker forwards a message to all the entities that have subscription with that specific entity and requests the direct trust of that entity. By receiving the request, the direct trust table of that entity which is maintained in trust agent is checked. Trust level of that entity within a specific context is obtained from the direct trust table and ultimately is forwarded to the broker. All the trust values are gathered by the broker and the reputation levels are calculated by (3), and the results are maintained in Table 2 at the broker.

$$RL(E_i, c) = \sum_{j=1, i \neq j}^{m} DTL(E_i, E_j, c) \qquad (3)$$

Table 2. Reputation table

| RL | entity 1 | entity 2 | … | entity m-1 | entity m |
|---|---|---|---|---|---|
| context 1 | $RL_1^{c1}$ | $RL_2^{c1}$ | … | $RL_{m-1}^{c1}$ | $RL_m^{c1}$ |
| context 2 | $RL_1^{c2}$ | $RL_2^{c2}$ | … | $RL_{m-1}^{c2}$ | $RL_m^{c2}$ |
| … | … | … | … | … | … |
| context i | $RL_1^{ci}$ | $RL_2^{ci}$ | … | $RL_{m-1}^{ci}$ | $RL_m^{ci}$ |

By considering the criteria which are mentioned above, the secure resource is selected using multi criteria decision making as follows.

### B. Secure resource selection using multi criteria decision making

The main problem of decision making is the process of finding the best choice among all alternatives. In such problems, various criteria for judging about alternatives are pervasive. Therefore, Multi Criteria Decision Making (MCDM) method is used to solve such a problem. In this study we modify this method to select a secure resource in grid environment. Fig. 1 shows the flowchart of the proposed trust model using multi criteria decision making. The states of this flowchart are discussed as follows:

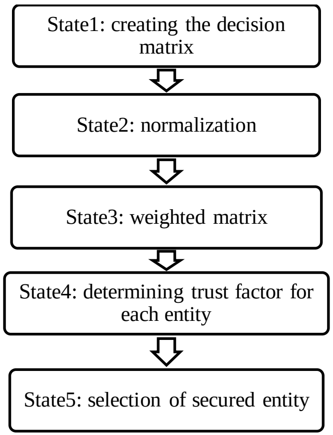
State1: creating the decision matrix
State2: normalization
State3: weighted matrix
State4: determining trust factor for each entity
State5: selection of secured entity

Fig. 1. A flowchart for MCDM method

### State 1: Creating the decision matrix

For selecting a secure resource we suppose m alternative entities $E_i$, i=1…m, which has been found by the broker, and based on the discussion in section 2.1, three criteria, consisting of self defense capability, direct trust and reputation are used respectively as $C_j$, j=1,2,3. The MCTM model is expressed by (4) and (5) as follows:

$$\tilde{D}=\begin{array}{c|ccc|} & C_1 & C_2 & C_3 \\ \hline E_1 & \tilde{d}11 & \tilde{d}12 & \tilde{d}_{13} \\ E_2 & \tilde{d}_{21} & \tilde{d}_{22} & \tilde{d}_{23} \\ \vdots & \vdots & & \\ Em & \tilde{d}_{m1} & \tilde{d}_{m2} & \tilde{d}_{m3} \\ \hline \end{array} \qquad (4)$$

$$W=[w_1\ w_2 ... w_3] \qquad (5)$$

$\tilde{D}$ is referred to a decision matrix where $\tilde{d}_{ij}$ is the fuzzy rating of entity $E_i$ with respect to criteria $C_j$, $W$ is the weight vector in which $w_j$ represents the fuzzy weight of $C_j$ ($j=1,2,3$). In general, criteria can be classified as either a or b:

a) Benefit criterion: (where the higher value of $d_{ij}$ is better for the decision maker). In MCTM $C_1, C_2$ and $C_3$ are benefit criteria.

b) Cost criterion: (where the lower value of $d_{ij}$ is better for the decision maker).

$\tilde{d}_{ij}$ is a fuzzy triangular number which is represented by a triplet $\left(d_{ij}^1, d_{ij}^2, d_{ij}^3\right)$. The membership function is presented as (6) as follows [18]:

$$\mu_{\tilde{d}_{ij}}(x)=\begin{cases} \dfrac{(x-d_{ij}^1)}{(d_{ij}^2-d_{ij}^1)} & ,d_{ij}^1 \le x \le d_{ij}^2 \\ \dfrac{(d_{ij}^3-x)}{(d_{ij}^3-d_{ij}^2)} & ,d_{ij}^2 \le x \le d_{ij}^3 \\ 0 & ,otherwise \end{cases} \qquad (6)$$

Fuzzy triangular number is based on three values: $d_{ij}^1$ is the minimum possible value, $d_{ij}^2$ is the most possible value and $d_{ij}^3$ is the maximum possible value.

## State2: Normalization

Since $\tilde{d}_{ij}=\left(d_{ij}^1, d_{ij}^2, d_{ij}^3\right)$ is generated in various scales, a normalization process is done by using (7)

$$\tilde{n}_{ij}=(\frac{d_{ij}^1}{M},\frac{d_{ij}^2}{M},\frac{d_{ij}^3}{M}) \qquad (7)$$

Where $M=\underset{i}{Max}\, d_{ij}^3$.

$\tilde{N}=\left[\tilde{n}_{ij}\right]$ is the normalized matrix of $\tilde{D}=\left[\tilde{d}_{ij}\right]$ which will be used as normalized decision matrix. It's obvious that $\tilde{n}_{ij}=\left(n_{ij}^1, n_{ij}^2, n_{ij}^3\right)$.

### State 3: Weighted matrix

Assuming that $\tilde{N}=\left[\tilde{n}_{ij}\right]$ , $\tilde{N}^W=\left[\tilde{n}_{ij}^w\right]$, is the weighted matrix. The weighted matrix is constructed by substituting the normalized matrix and the weight vector in (8).

$$\tilde{n}_{ij}^w=\left(n_{ij}^1 * w_j, n_{ij}^2 * w_j, n_{ij}^3 * w_j\right),\ i=1,2,...,m \text{ and } j=1,2,3. \qquad (8)$$

It's obvious that $\tilde{n}_{ij}^w$ is a fuzzy triangular number, therefore $\tilde{n}_{ij}^w=\left(n_{ij}^{w1}, n_{ij}^{w2}, n_{ij}^{w3}\right)$.

### State4: Determining trust factor for each entity

Trust factor of entity i is calculated as (9) as follows, where 3 is the number of criteria.

$$TF_i=(d_i^- + 3 - d_i^*)/6\ ,\ i=1,2,...,m \qquad (9)$$

Assume that $\tilde{p}_j^*=(1,1,1)$ and $\tilde{p}_j^-=(0,0,0)$. By using vertex method [19] $d_i^*$, $d_i^-$ are obtained by (10) and (11) respectively.

$$d_i^* = \sum_{j=1}^{3} d\left(\tilde{n}_{ij}^{w}, \tilde{p}_j^*\right) = \sum_{j=1}^{3} \left\{ \left[\left(n_{ij}^{w1}-1\right)^2 + \left(n_{ij}^{w2}-1\right)^2 + \left(n_{ij}^{w3}-1\right)^2\right] / 3 \right\}^{1/2}, \quad i = 1,2,\dots,m \qquad (10)$$

$$d_i^- = \sum_{j=1}^{3} d\left(\tilde{n}_{ij}^{w}, \tilde{p}_j^-\right) = \sum_{j=1}^{3} \left\{ \left[\left(n_{ij}^{w1}-0\right)^2 + \left(n_{ij}^{w2}-0\right)^2 + \left(n_{ij}^{w3}-0\right)^2\right] / 3 \right\}^{1/2}, \quad i = 1,2,\dots,m \qquad (11)$$

### State 5: Selection of secured entity

By forwarding a request to the broker, a set of entities that are able to satisfy it are chosen. For each member of this set, trust factor is calculated. According to (12) the entity with higher trust factor, SE, is selected for the interaction.

$$SE = \underset{i=1}{\overset{m}{Max}}\ TF_i \qquad (12)$$

## IV. Simulation Verification

We have simulated MCTM, to show the ability and performance of the presented model and also the effect of self defense capability on secure resource selection. As discussed above MCTM, is a trust model which considers all the necessary criteria.

### A. *Simulation Setup*

In order to assess the effectiveness of our trust model in grid systems, a network with one hundred entities is simulated using MATLAB software. Table 3 shows the simulation parameters. Number of jobs, Trust agent, Online/Offline rate, Direct Trust Level, Self Defense Capability and Reputation criteria are considered for the simulated entities.

Table 3. Simulation parameters

| PARAMETERS | VALUES |
|---|---|
| Number of entities | 100 |
| Type of context | 50 |
| Number of context | 20 |
| Number of requests | {1000, 2000,…,10000} |
| Job arrival rate | Poisson distribution with average rate of 0.5 |
| Service time of entity | Exponential distribution with parameter λ=2 |

The criteria considered in this model are triangle fuzzy numbers that are based on three-value judgment: minimum possible value, most possible value, and maximum possible value. The initial numbers of self defense capability is generated randomly at the beginning of the simulation. The initial direct trust levels which are maintained in trust agents are developed randomly about (0.2,0.3,0.5). For determining the reputation of specific entity, Eq. (3) is used. The values of direct trust table are updated as time passes. For each job, entities trust values are updated based on the quality of their performance using Eq. (2).

Jobs are generated randomly as requests which follow Poisson distribution with average rate of 0.5 and the service time follows Exponential distribution with parameter λ which equals 2. Offline/Online rate of resources follow Poisson distribution with average rate of 0.01.

After creating the decision matrix ( $\tilde{D}$ ) a normalization process is applied. By this method the ranges of normalized triangular fuzzy numbers are preserved to [0,1]. Creating the weighted matrix by substituting the normalized matrix and the weight vector is the next phase. All entities based on their contribution to security, give a weight to all the three criteria. In this paper we suppose that all weights are equal so $w_j = 0.2$, for $j = 1,2,3$. Finally, according to (9-11), a trust factor is calculated for each resource and the resource with maximum trust factor is selected as the secure resource.

Simulation process is terminated based on the number of requests which will be received as an entry at the beginning of the simulation. The result of simulation is evaluated based on the number of requests as 1000,2000,…,10000. Performance of the models is evaluated in term of failure jobs and execution time. The rate of failure jobs will be determined by considering Self Defense Capability criterion. The failure happens when a resource is not capable to respond to a request, or a resource attaches viruses, or is unable to respond in the given time. The execution time is considered from the beginning of receiving requests till the end of responding them.

According to the variety of the existing trust models, we decide to simulate two trust models which are shown in table 4. MCTM is a comprehensive model which aggregates all the three factors. WSDC is MCTM without considering self defense capability criterion.

Table 4. Comparison of trust models

| Trust Models | Self defense capability | Reputation | Direct Trust |
|---|---|---|---|
| MCTM | × | × | × |
| WSDC | | × | × |

### B. *Simulation Results*

To evaluate the performance of the presented model we setup two experiments:

The first experiment evaluates the number of failure jobs in term of request numbers, for the trust models shown in table 4. As shown in fig. 2, MCTM reduces the number of failure jobs to %9.16 compared with WSDC.

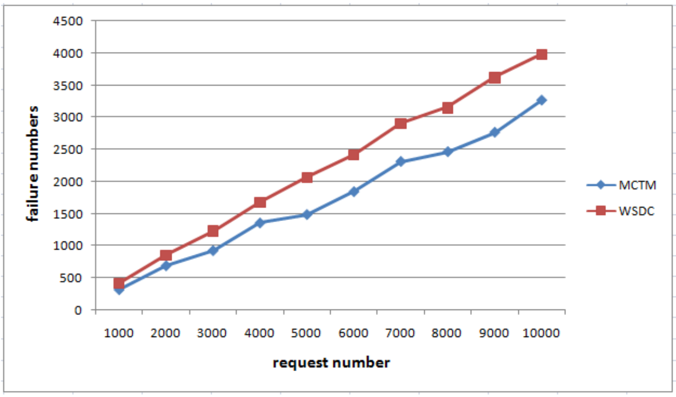

Fig. 2. Average number of failure jobs

The second experiment tests the execution time of two models in term of number of requests. Fig. 3 shows that MCTM demands more execution time than other model. MCTM increases execution time %0.019 compared with WSDC model.

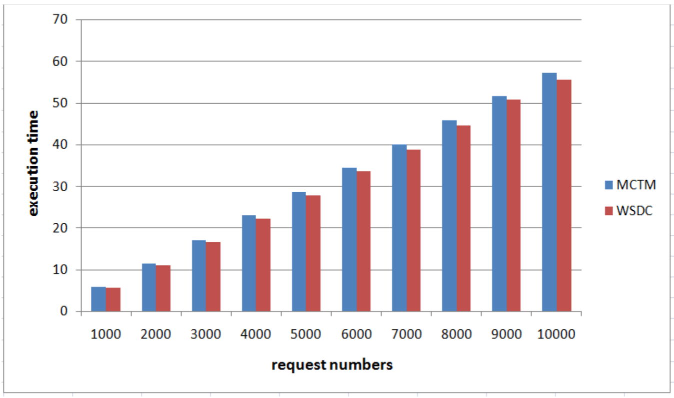

Fig. 3. Average execution time

## V. Conclusion

In this paper, we presented MCTM, Multi Criteria Trust Model that can be used in any grid system. This model is a trust model which aggregates three basic and important criteria including various criteria such as self defense capability, direct trust, and reputation to select secure resources. Fuzzy multi criteria decision making is used to calculate trust factor. Based on the interaction values the decision is made on whether to trust or not.

MCTM has been simulated in MATLAB by use of fuzzy toolbox. Also, in this paper we have studied the effect of Self Defense Capability criterion in trust. The results show the better performance of our model considering the number of failed requests, but this advantage needs more execution time.

## VI. References

[1] S.Song, K.Hwang and M.Macwan, "Fuzzy Trust Integration for Security Enforcement in Grid Computing", IFIP International Symposium on Network and Parallel Computing (2004), pp.18-22.

[2] S.Song, K.Hwang and Yu-K, "Trusted Grid Computing with Security Binding and Trusted Integration", Journal of Grid Computing, (2005).

[3] Ayman.Tajeddine, Ayman.Kayssi, Ali.Chehab, Hassan.Artail "Fuzzy Reputation-based Trust Model", Applied Soft Computing Journal (2011) pp.345-355.

[4] A. Tajeddine, A. Kayssi, A. Chehab, H. Artail, "PATROL: a comprehensive reputation-based trust model", International Journal of Internet Technology and Secured Transactions 1 (2007) 108–131.R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[5] S.D. Ramchurn, N.R. Jennings, C. Sierra, L. Godo, "Devising a trust model for multi-agent interactions using confidence and reputation", Applied Artificial Intelligence 18 (2004) 833–852.M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[6] C. Castelfranchi, R. Falcone, G. Pezzulo, "Trust in information sources as a source for trust: a fuzzy approach", in: Proceedings of the Second International Joint Conference on Autonomous Agents and Multi agent Systems, (2003), pp. 89–96.

[7] R. Falcone, G. Pezzulo, C. Castelfranchi, "Quantifying belief credibility for trust based decision", in: Proceedings of the Workshop on Deception, Fraud, and Trust in Agent Societies at AAMAS-02, Bologna, Italy, (2002), pp. 41–48.

[8] V.Vijayakumar, R.S.D. Wahida Banu, "Secured Resource Selection in Grid Computing: Secured Resource selection Sentient Scheme", springer-verlay belin Heidelberg (2002), pp.169-183.

[9] A. Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities", Hawaii Int’l Conference on System Sciences, (2000).

[10] F.Azzedin, M.Maheswaran, "Towards Trust-Aware Resource Management in Grid Computing Systems" In: 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid (2002), pp.452.

[11] V.Vijayakumar, R.S.D. Wahida Banu, "performance analysis in secured grid resource selection based on trust and reputation”, International Journal of Computer Applications (0975-8887), volume 31-No.1, October (2011).

[12] R. Buyya, S. Venugopal, "A Gentle Introduction to Grid Computing and Technologies", in: Computer Society of India (CSI), vol. 29, no. 1, (2005), pp. 9-19

[13] F.Azzedin, M.Maheswaran, "Evolving and Managing Trust in Grid Computing Systems” Proceedings of the 2002 IEEE Canadian Conference on Electrical Computer Engineering 0-7802 xxxx-x/02/$10 c 2002 IEEE

[14] S.J. Chen, C.L. Hwang, "Fuzzy Multiple Attribute Decision Making Methods and Applications", Springer-Verlag, Berlin, Heidelberg, (1992).

[15] C.C. Robert, R. Fulle´r, "Fuzzy multiple criteria decision making: recent developments", Fuzzy Sets and Systems 78 (1996), pp.139–153.

[16] R.E. Bellman, L.A. Zadeh, "Decision-making in a fuzzy environment", Management Science 17 (1970), pp.141–164.

[17] R.A. Ribeiro, "Fuzzy multiple attribute decision making: A review and new preference elicitation techniques", Fuzzy Sets and Systems 78, (1996), pp.155–181.

[18] Fenton, N., Wang, W., "Risk and confidence analysis for fuzzy multi criteria decision making", Knowledge-Based Systems 19, Elsevier, (2006), pp.430–437.

[19] Chen, C.T., Extensions of the TOPSIS for group decision-making under fuzzy environment, Fuzzy Sets and Systems 114, (2000), pp.1–9.

[20] Cody, E., Sharman, R., Rao, R.H., Upadhyaya, s., "Security in grid computing", Decision Support Systems 44, (September 2007), pp. 749–764.