IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 5, May 2010
ISSN (Online): 1694-0784
ISSN (Print): 1694-0814

REPUTATION BASED TWO WAY TRUST MODEL FOR RELIABLE TRANSACTIONS IN GRID COMPUTING

Srivaramangai P[1], Renagaramanujam Srinivasan[2]

**[1] MCA Department ,BS Abdur Rahman University
Chennai , Tamilnadu, India**

**[2] CSE Department, BS Abdur Rahman University
Chennai , Tamilnadu, India**

Abstract:-

Grids computing is a coordinated resource sharing and problem solving in any dynamic environment. Computing resources are highly heterogeneous. Grid computing and its related technologies will only be adopted by users, if they are confident that their data and privacy are secured and the system must be as scalable, robust and reliable as of their own in their places. Reliability is the probability that a process will successfully perform it's prescribed task with out failure at a given point of time. So allowing reliable transactions plays a vital role in grid computing. Reliability of any transaction increases when it passes through two way test criteria. That is the consumer is satisfied with the ability of the provider and the provider in turn is reasonably happy with and willing to provide service to the user. To achieve this kind of reliable transactions mutual trust must be established between the initiator and the provider. Trust is measured by using reputation and reputation is the collective opinion of others. This paper provides a model which will allow only reliable transactions in grid by using trust as a measure for both provider and consumer. This enhances the security in grid.

1. Introduction:

Now days the processing speed of any computer is enormously increased. Even then it is not enough to satisfy the needs of life science and physical sciences. Grid computing provides huge processing power in a distributed environment with variety of resources .The resources in Grid are shared in a flexible, coordinated and secured manner. Most of the Grid applications involve very large data bases with highly secured data. The services in grid may range from simple printing job to complex computing job. Security is one of the great issues in grid computing. The success of grid applications depends on effective usage of resources in a way that is expected.

Security mechanism in any system should prevent unauthorized entry in to the system. But in Grid environment the security should be much more than this. In grid applications the users should have reliable transactions. The reliability of any transaction is the probability of successful running or completion of a given task. So there is a need of trust system which ensures a level of robustness against malicious nodes. Trust must be established from both the sides.

In this paper we analyze the existing models and identify the needs of two way reputation. We argue that every transaction must pass through two way test criteria before it gets approved. First we made analysis of existing models. Second we propose a model which improves security and allow only reliable transactions. Trust relationship is one of the prevailing security issues in Grid computing. [14]

The rest of the paper is organized as follows. Section 2 discusses the related works; Section 3 proposes a new model with improved reliability; Section 4 discusses computation of trust; section 5 presents the design; and section 6 presents simulation of proposed model. In section 7 we conclude.

2. Related work: -

A reputation-based framework is presented by Li xiong and liu [5]. They claim that feed back values only are not enough for the calculation of trust and reputation. Y. Wang and J. Vassileva [6] propose a

ISSN (Online): 1694-0784
ISSN (Print): 1694-0814

reputation model based on Bayesian network. According to their model the peers needs are different in different situations. Selcuk et al. suggests in [7] a reputation based trust management system in which the reliability is calculated based on previous transactions. Ayman Tajeddine et al. in [8] propose a very impressive reputation based trust model. In this approach the initiator host calculates reputation value of target host based on its previous experiences and gathered feedbacks from other hosts. F.Azzedin,M.Maheswaran [9] discuss about managing trust in grid by proposing a behavior trust management model. Trust levels are graded from a to f. Both direct and indirect trust are considered.

Gui Xiaolin, Xie Bing [10] propose a trust model based on behavior tracks. Attenuation function is corporated for decaying factor. Baolin Ma et al in [11] present a reputation based trusted model .Their model considers both direct feed back and feed back from other entities Direct trust is given with more weightage than the indirect score.Beulah kurian, Gregor von laszewki [12] provide a way for efficient resource selection by considering Eigen trust algorithm. Their approach is similar to Azzedin approach [9] except for a new parameter context. In our previous publication [13] the trust system is made more robust by eliminating the unreliable feedbacks by using rank correlation method.

3. Proposed model:-

The proposed work is an enhancement of the existing model [13] that uses rank correlation method for removing biased feed backs. It uses both direct trust and indirect trust. Direct trust is given more weightage Direct trust is calculated from the transactions which are done directly by the initiator and is given higher weightage. Indirect trust is measured by getting feed backs from entities in the same domain and also from other domains. This model calculates the credibility of the recommenders' feedback by considering different parameters such as similarity, activity and specificity.

In this model both the provider as well as the imitator collect the feed backs and the trust is calculated from both the ends. We calculate the reputation of both client as well as provider. The reputation of the client is evaluated by the provider whereas the reputation of the provider is evaluated by the client. Since the relationship between the client and provider is asymmetric and the corresponding trust reputation values will be calculated based on different parameters, the threshold values for the two will be different.

In the Earlier model the trust is calculated by the user and the decision is made based upon that trust. In the proposed model trust is measured from the provider side also and the transaction is allowed only if both the trust values are greater than a predefined threshold value. Since the reputation repository is decentralized we cannot completely depend on recommenders feed back. So here the main assumption is that there can be a few malicious entities that can give wrong feedbacks about other entities. Even if single entity is giving a wrong feedback, it is sufficient to alter the decision from one state (grant) to another (not grant) which is true for both the user and the provider. In the real world we expect a set of malicious entities trying to disrupt the smooth functioning of the grid system by false reporting giving false feedbacks. Also the entities may not be malicious but their method of evaluation may be totally different from one's own.

A, the initiator entity can evaluate the trustworthiness of provider I, based on views of colleagues, whose evaluation schemes are similar to his. The correlation can be obtained by any of the standard methods available such as Pearson Product Moment Correlation, Spearman rank Order Correlation (rho) or the Kendall rank order Correlation (tau) and we have chosen Spearman's Rank Coefficient. In the similar way the provider also has his own right to decide whether to allow the consumer to utilize his resource or not. So he also fixes a threshold value and if the calculated trust is greater than that values he allows the transaction else denies. Thus even if the initiator is ready to take up a particular resource from the provider the provider also should be in the position to share his resource. This is a two way test criteria which assures more reliable transaction which in turn improves security in grid environment. In this model every entity can be either a provider or a user for any particular transaction.

4. Computation of Trust:

The computation of trust is depicted in this section .Let us assume A is the provider and I is the user. The model decides the transaction as follows; First I as the initiator has to decide whether to accept the resource from A or not. The total trust (trust 1) is calculated by the expression;

Total trust = u*direct trust + v * indirect 1 + w * indirect 2 (1)

Where u+v+w=1 and u>v>w.

$$\text{indirect 1} = \frac{\sum_{i \neq j} \alpha_i \, \text{rep } y/xi}{\sum \alpha_i} \qquad (2)$$

ISSN (Online): 1694-0784
ISSN (Print): 1694-0814

$$i \neq k$$

$$\text{indirect 2} = \frac{\sum_{j \neq k} \beta_j \text{ rep y/xi}}{\sum_{j \neq k} \beta_j} \qquad (3)$$

α, β are credibility factors .

Direct trust is the value which is perceived by the initiator entity by his own experience. Indirect 1 & indirect 2 both are calculated by taking the recommenders' feed backs. In indirect 1 the feedbacks are collected from its neighbours. That is the entities from the same domain. In indirect 2 the feedbacks are collected from the entities in foreign domains. In this model the similarity between the requester and each recommender is estimated by rank correlation method. (Spearman rank Order Correlation (rho)). If the correlation is greater than zero then the entity's feedback is taken, thus avoiding biased feed backs. Credibility of each recommender is measured by using similarity, activity and specificity. [14]
The following data gives one sample output which explains the allocation procedure. Over all fifteen entities have been taken. Two domains are considered. The first model takes all the feed backs. The second and third model takes only the reliable feedbacks. G and O are both reputed. So the transaction is rightly granted for them by the proposed model.
Entities considered:
[A, B, C, D, E, F, G, H, I, J, K, L, M, N, O]
Domain1:[A, B, C, D, E, F, G]
Domain2:[H, I, J, K, L, M, N, O]
Malicious = [C,F,K,N]

EXISTING MODEL [13]
Initiator G
Provider: O
Recommenders:[A, B, C, D, E, F, H, I, J, K, L, M, N]
Total Trust Score: 2.92
Resource is not allocated

PROPOSED MODEL
Initiator: G
Provider: O
Recommenders:[A, B, D, E, H, I, J, L] (only reliable nodes)
Total Trust Score: 3.13
Resource is Allocated

In the same way the total trust about the user is measured by the provider. But this time only the provider entities are considered not the users, trust2. If Trust 1 > γ (minimum threshold value) and trust 2 > δ then the transaction is allowed else the transaction is denied.

5. Design of the proposed system:

Fig1 explains the overall architecture. The user uses the reputation model and decides whether to choose a particular provider or not. In turn providers also use the model with its own recommendations and make decisions.

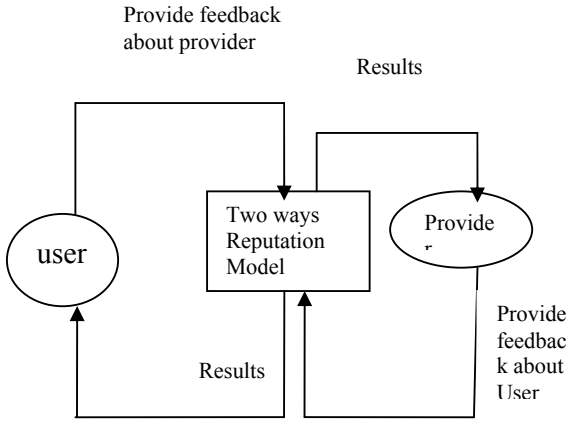

Fig 1 Context diagram for the proposed model.

Fig 2 explains about the calculation of user side trust. The user get the recommendation from other entities, calculate the rank correlation and decides whether to accept the recommendations. If the rank correlation is positive he accepts. Otherwise he goes to the next feedback. Then he calculates the total trust. If the total trust is greater than the minimum threshold he chooses that provider. Fig 3 depicts the procedure for provider side trust.

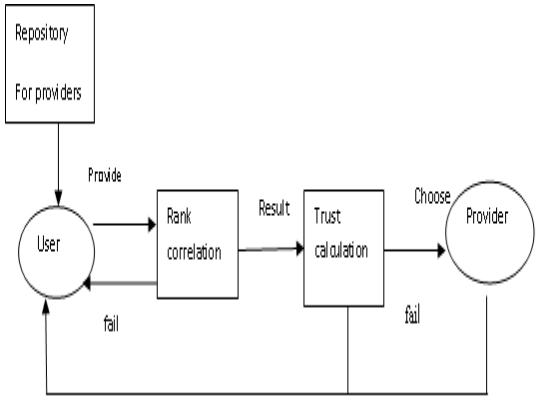

Fig 2 Procedure for user side trust

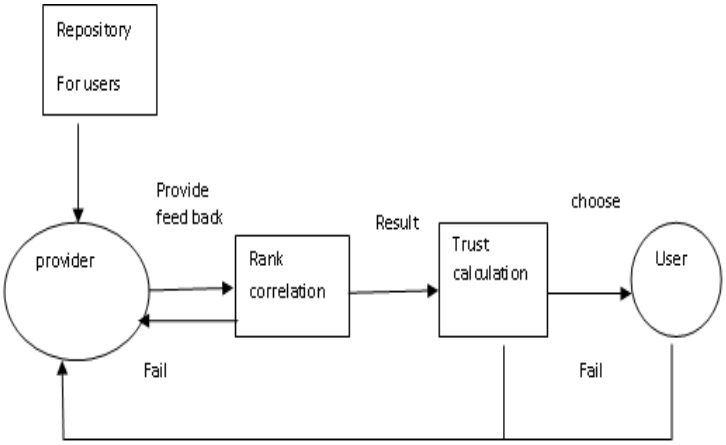

Fig 3 Procedure for provider side trust

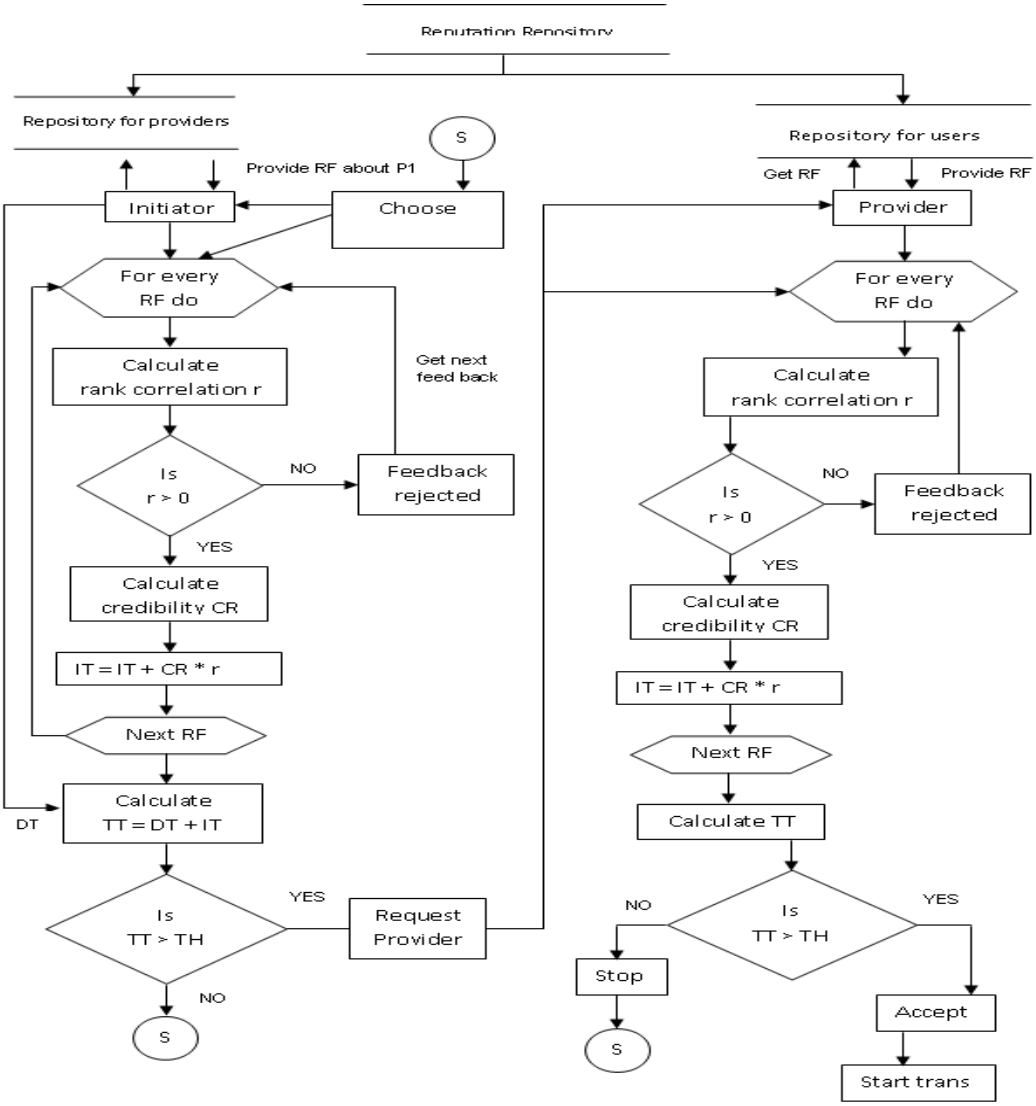

Fig 4 – Flow chart for the overall process

ISSN (Online): 1694-0784
ISSN (Print): 1694-0814

The above flowchart explains the system flow as a whole. First the initiator entity I choose a provider P. It gets the recommendations from all of its neighbours. Credibility of feedbacks are calculated and based upon the credibility value the initiator considers the feed backs which is reliable. Then total trust and indirect trust are calculated using the equations 1, 2 & 3 . If the trust value is greater than the chosen threshold then the user requests the resource from the provider. Provider goes through all the steps and if the calculated trust value satisfies his threshold he agrees to offer his resource else he sets the status as busy. If both the provider and consumer agree upon their trust value the transaction is executed.

6. Experiments and results:

Simulation studies have best conducted using three models as follows.
Model 1: Existing model as proposed by [8]
Model2: Model proposed by us earlier [13], which depends on feedbacks from users only. Any initiator obtains feedbacks from other users, eliminates biased/malicious feedbacks and makes a decision based upon trust evaluated from remaining feed backs.
Model3: Present proposal, which is an improvement over model 2. Here providers also get feedback from other providers about the user /initiator who is making request for services. Identification of malicious feedbacks is done using ranking coefficients. Thus the two ways model eliminates biased feedbacks from both users and providers.
Three sets of simulation studies have been done each with 100 runs. The results are presented in Table 1 and 2 and Fig. 5. Table 1 provides the cumulative summary of all the three simulations while Table 2 presents detailed analysis of disagreement cases corresponding to a particular study – study 2.
From a perusal of Table 1 , We find that there are altogether eight combinations of results . YYY signifies that all the three models agree to grant a request by the initiator while NNN denotes that all the models reject the request.
We find that out of a total of 300 instances there is complete agreement among all the three models in 258 (138+120) cases constituting 86% of runs. The disagreement in 42 cases can be spilt into six categories. Let us focus our attention to each one of these categories.
Column 4 corresponds to YNN situation where Model 1 grants request while Models 2 and 3 refuse. We have checked each one and have found Models 2 and 3 have correctly eliminated malicious / biased provider,
Columns 5 & 6 (NYN, YYN) correspond to a situation where providers assessments about the initiators/users based on feedbacks given by the other providers, fail to meet the minimum threshold limits. That means the providers are not satisfied with the trustworthiness of the users and fail to do business with them. In all there are 14 instances corresponding to these combinations, constitute 4.7 % of the total instances.
Column 7 (NYY) pertains to the situation where Model 1 rejects while Models 2 and 3 grant the request. The numbers of instances are 25 constituting 8.3% of the population. The first model has taken the biased feedbacks also in to calculation of trust and wrongly rejects the request. Models 2 & 3 have arrived at the correct decision of granting the request after successfully eliminated the malicious nodes.
Columns 8 and 9, corresponding to YNY and NNY contain zero entries since these correspond to the cases where the second model rejects, since threshold limits are not satisfied regarding a provider, so also does Model 3 which is a superset of Model 2.

Table 1: Cumulative results

S. NO	User	Provider	Model1	Model2	Model3
1	C	J	YES	YES	NO
2	K	F			
3	C	D			
4	C	J			
5	K	B			
6	C	J			
7	N	K	NO	YES	NO
8	B	I	NO	YES	YES
9	E	O			
10	G	H			
11	K	C			
12	B	I			
13	G	H			
14	L	E			

Table 2 – Disagreement cases

Simulation	YYY	NNN	YNN	NYN	YYN	NYY	YNY	NNY	Total Runs
1.	41	44	2	1	1	11	0	0	100
2.	46	40	0	1	6	7	0	0	100
3.	51	36	1	3	2	7	0	0	100
Tot	138	120	3	5	9	25	0	0	300
Per	46	40	1	1.6	3	8.4	0	0	

ISSN (Online): 1694-0784
ISSN (Print): 1694-0814

In the first set of results that is no 1 to 6 the first two models accept the transaction. But the proposed model denies the transaction. In all the six cases the user is malicious. The proposed model considers the reputation from both the sides. It denies the transaction by applying the two way test criteria. The malicious nodes are prevented from accessing the resources there by the reliability of transaction are improved in the proposed model. In transaction 7 the user is malicious. In Model 3 the provider knows the malicious behavior of users. So it correctly denies the resource. In transaction 11 both the user and the provider are malicious. So they agree upon each other and the transaction begins. Other transactions 8 to14 both have good reputations and hence the transaction is executed. But Model 1 wrongly denies the transaction for the right nodes.
Out of all 14 disagreement cases our proposed model makes right decision with the malicious nodes.

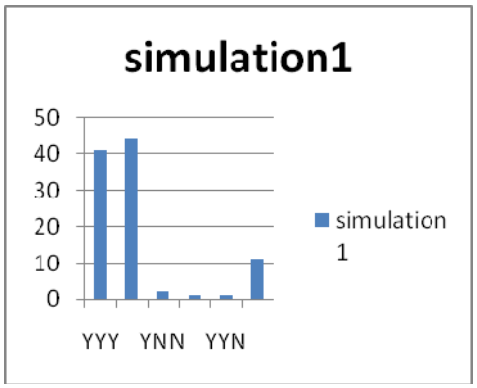

Fig 5.a: Allocations for three simulations

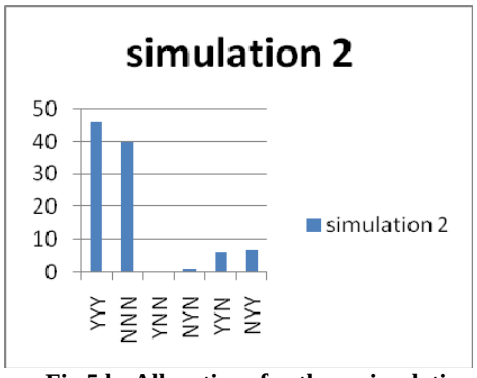

Fig 5.b: Allocations for three simulations

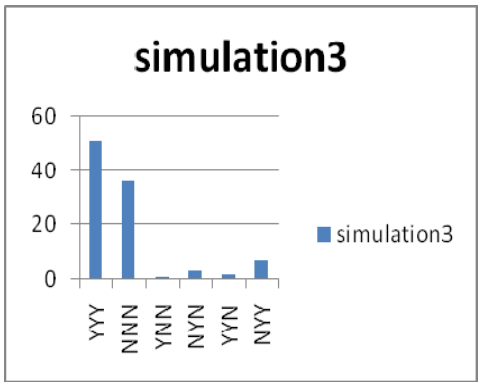

Fig 5.c: Allocations for three simulations

Another analysis of the results brings out interesting information. From Table 1 we find model 1 grants 150 (138+3+9) of the 300 requests by the initiator, while model 2 grants 177 (138+5+9+25) of the total requests. For model 3 we find that in all 163 (138+25) requests are sanctioned. Initially when we design the two way trust model we felt through put as measured by the number of requests granted as compared to the requests made will come down because of the two level filtering features – one at the provider and the other at the user level. This has not happened because model 1 the existing model is affected by the biased feedbacks, and has arrived at wrong decision for 25 cases. Fig 6 brings out this aspect.

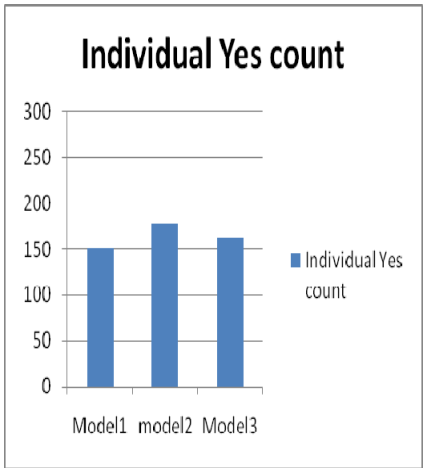

Fig 6 Comparison of Allocation.

Another aspect to be considered is the accuracy of the models – What percentage of each model decision is correct. We find that Models 1,2 and 3 have accuracy values of (258/300) 86%, (286/300) 95.33% and (300/300) 100% respectively . Thus Model 3 arrives at the correct decision in all the cases

ISSN (Online): 1694-0784
ISSN (Print): 1694-0814

7. Conclusion:

The paper has presented a new trust model which is comprehensive in the sense it takes cognizance of both provider and user sensibilities. Further by eliminating biased feedbacks from both user and provider groups the resultant transactions become more reliable and secure .Simulation study establish the superiority of the proposed two way trust model over the existing models.

Acknowledgements

The authors would like to express their thanks to Dr. P. Kanniappan, Vice chancellor, Dr.V.M.Periasamy , Registrar, Dr.K.M.Mehata the Dean and Dr.P.Sheik abdul Khader , HOD/Dept of Computer Applications of B.S.Abdur Rahman University for the environment provided.

References:

[1] A.Arenas "State of art survey on trust and security in grid computing system " march 2006.

[2] *Gheorghe Cosmin Silaghi, Alvaro E. Arenas, Luis Moura Silva* ," Reputation-based trust management systems and their applicability to grids "CoreGRID Technical Report Number TR-0064 February 23, 2007

[3] Marcim Adamski, Alvaro Arenas, Angelos Bilas " "Trust and Security in Grids: A State of the Art" CoreGRID White Paper Number WHP-0001 May 26, 2008

[4] A. Abdul-Rahman and S. Hailes. "Supporting trust in virtual communities". In *HICSS '00: Proceedings of the 33rd Hawaii International Conference on System Sciences-Volume 6*, page 6007, Washington, DC, USA, 2000. IEEE Computer Society.

[5] L. Xiong, and L. Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 7, July 2004.

[6] Y. Wang and J. Vassileva, "Trust and Reputation Model in Peer-to-Peer Networks," Proceedings of the Third International Conference on Peer-to-Peer Computing (P2P'03), 2003.

[7] A. Selcuk, E. Uzun, and M. Pariente, "A Reputation-Based Trust Management System for P2P Networks," IEEE International Symposium on Cluster Computing and the Grid 2004.

[8] Ayman Tajeddine Ayman Kayssi Ali Chehab Hassan Artail "A Comprehensive Reputation-Based Trust Model for Distributed Systems " IEEE 2005.

[9] F.Azzedin,M.Maheswaran "Evolving and managing trust in grid computing system" IEEE CCECE,2002.

[10] Gui Xiaolin, Xie Bing "Study on behavior based trust model in grid security system" "Proceedings of the 2004 IEEE International Conference on Services Computing (SCC'04).

[11] Baolin Ma, Jizhou Sun, Ce Yu " Reputation-based Trust Model in Grid Security System " , Aug. 2006, Volume 3, No.8 (Serial No.21) Journal of Communication and Computer, ISSN1548-7709, USA.

[12] Beulah kurian, Gregor von laszewki "Reputation based grid resource selection"

[13] P.Srivaramangai , .R.Srinivasan " Reputation based trust model with elimination of unreliable feedbacks " International journal of information technology and knowledge management Vol2 , 2009. No 2,pp.455-459

[14] P.Srivaramangai , R.Srinivasan " An overview of Trust model for Grid Security" National conference ,March 2007.