ISSN:0975-9646

Proposed a Robust Trust Model for Reliable and Secure Transactions in Grid Computing

Biswajit Upadhyay , Abhishek Bandyopadhyay , Avijit Bhowmick

Dept. of CSE,Dr.B.C.Roy Engineering College ,
Durgapur,India

***Abstract*— Grid computing is a type of advanced computing system whereby resources are shared from different domains. Organizations will only adopt this technology if they are assured of their data privacy, consistency & integrity. In such a scenario, reliability plays a critical role. Reliability in Grids can be enhanced by both way model. The user is satisfied with resource provider's ability and the same is true in reverse case also. Trust relationship must be established between resource provider and user. Reputation decides the trustworthiness of an entity, whereby opinion of other entities is also sought. In this paper we propose a model which allows only trusted transactions for both providers and users which improves security in Grid computing.**

I. INTRODUCTION

Grid computing offers massive processing power in a distributed environment where hardware and software dispersed across multiple domains. The resources in Grid are shared in a harmonized and secured way. Almost all Grid applications require huge data bases with highly secured data and information. Security aspect is the most important issue in Grid computing. The success of Grid applications depends on proper usage of resources in a way that is expected of them. Security mechanism in any system should prevent unauthorized entry in to the system. But in Grid environment the security should be of highest priority order.Data reliability, data integrity and data consistency must be supported by the Grid .So there is a requirement of trust system which assures a level of toughness against malicious nodes. Here we have gone through the present models and recognize the needs of two way trust. Each and every transaction must pass through two way test criteria for data transactions. First we elaborately examined of existing models and then we propose a trust model which enhances security and allow only reliable trusted transactions.

II. RELATED WORK

Y. Wang and J. Vassileva [1] proposed a reputation model which is based on Bayesian network. According to their model the peer needs are different in different circumstances. Li xiong and liu presented a reputation-based framework [2]. They stated that feed back values only are not enough for the calculation of trust and reputation. Ayman Tajeddine et al. in [3] propose a very remarkable reputation based trust model. In this approach the initiator host calculates reputation value of target host based on its previous experiences and collected feedbacks from other hosts. F.Azzedin, M.Maheswaran [4] discussed regarding trust handling in Grid by proposing a behavior trust management model. Trust levels are scaled from a to f. Both direct and indirect trust are considered. Selcuk et al.suggests in [5] a reputation based trust management system where the reliability is calculated based on previous transactions. Vivekananth [6] proposed a behavior based trust model which provides the behavior conventionality. In this model author concentrated on behavior of entities in different domains, in different situations.The total trust will be calculated by direct trust and indirect trust. Both the trust will be evaluated by reputations. There will be tracking module, which will keep track of behavior. Based on experiences with the entities, an entity trust level will be increased or decreased. There can be a penalty factor, which can be levied for malicious behaviors. The trust factor between two Entities may depend on penalty, context and time. The penalty will be higher if the misbehavior creates heavy harm. Otherwise the penalty will be low. Based on this experience the trust will be updated. The penalty factor can be a number between 0 & 1. If the total trust is greater than the required trust then the resource is allocated. This model is still under revision. Beulah kurian, Gregor von laszewki [7] provide a way for efficient resource selection by considering Eigen trust algorithm. Their approach is similar to Azzedin approach [4] except for a new parameter context.

III.TRUST AND REPUTATION SYSTEMS

The defition of trust is defined in [8] :

"Trust is the firm belief in the competence of an entity to behave as expected such that this firm belief is a dynamic value associated with the entity and it is also subject to the entity's behavior and applies only within a specific context at a given time."

The definition of Reputation as presented in [8] :

"The reputation of an entity is an expectation of its behavior based on its identity and other entities' observations or information about the entity's past behavior within a specific context at a given time."

Reputation presents to the value given to the entity (it may be a resource, service, user) based on the trust shown by it in the previous experience.

The difference between trust and reputation may be clarified by the following statements:

* *"X trusts Y because Y has got good reputation."*
* *"X trust Y in spite of Y's bad reputation"*

The first sentence declares that the first party believes the second one since the second one has a very good reputation. The good reputation may be obtained from one's own past experience or from neighbour's feed backs.

The second sentence states that the first one believes the second in spite of the bad feedbacks from others .This may be due to the strong faith or trust the first one has on the second entity. Personal experience typically carries more weight than second hand trust referrals or reputation. Reputation can be considered as a collective measured parameters of trustworthiness based on the referrals or feed backs from members in the same domain. An individual's subjective trust can be derived from a combination of received referrals and personal past experience. Reputation systems provide a way for building trust through social control by utilizing community based feedback about past experiences of nodes to help making recommendation and decision on quality and reliability of the data transactions.

IV. CONCEPT OF THE MODEL

The proposed work 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 resource provider. Indirect trust is calculated by receiving feed backs from neighbors in the same domain and also from other domains. This model can calculates the credibility of the recommenders' feedback by considering different parameters such as similarity, activity, specificity, idleness. The resource provider as well as the imitator can gather the feed backs and the trust is calculated from both the ends in this model. We assess the reputation of both user as well as resource provider. The user can estimate the reputation of resource provider and the provider can evaluate the reputation of the user. Since the connection between the user and resource provider is dissimilar then corresponding trust reputation values will be calculated based on different parameters. There is a threshold values for the user and resource which is different. In the earlier model the trust is calculated by the user and the judgment is made based upon that trust.

In the proposed model trust is measured from both sides user as well as the resource provider's side. The transaction is permitted only if both the trust values are greater than a predefined threshold value. Since the reputation repository is not centralized we cannot completely rely upon recommender's feedback. So here the main assumption is that there may be a few malicious nodes that can give false feedbacks about other entities. Even if single entity is giving a false feedback, it is essential to change the decision from acceptance to rejection which is applicable for both the user and the resource provider. In the real scenario we expect a set of malicious nodes trying to upset the smooth functioning of the Grid system by giving false feedbacks

V. TRUST COMPUTATIONS METHOD

Suppose A is the initiator and he wants to get feedbacks about a potential entity P. B and C have already transacted business with P. A would like to use the feedbacks of B and C about P, so as to determine whether to shortlist P as a candidate provider or drop him from listing. The existing method simply uses the scores given by B and C and evaluates the trustworthiness of the provider as a function of above feedbacks. Now the question arises whether feedbacks given by entities are reliable or not. We can answer the above question if A, B, and C have given feedbacks about some common entities say E1, E2, E3, E4 and E5. A compares his feedbacks about these common entities with those given by B and C. If there is a positive correlation then A takes the feedback back into account; and if the correlation is <=0 A ignores the corresponding feedbacks. For example if A's evaluations regarding entities E1, E2, E3, E4 and E5 are 4.8, 4, 3.6, 2.4 & 2 and the evaluations of B and C respectively are 4.2, 3.9, 3.5, 2.5, 2.1 and 2.9, 2.7, 3, 3.5, 4.2 then A will not consider the feedback of C. Thus 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 it has been chosen Spearman's Rank Coefficient. Thus even if an entity tries to play havoc by giving false or unreliable feedback values they can be identified and eliminated from consideration.

Ranking:

Since the feedbacks are collected from multi domains, there is a chance of receiving biased inputs. The feedbacks are sorted and concerned rank is assigned. Rank correlation is calculated. If the result is found positive then that entities feedback will be taken, otherwise feedback values will not be considered. Only the feedbacks of entities with positive correlation are considered for calculating reputation.

Similarity $= 1 - 6 \Sigma d i^2 / n (n^2 - 1)$

$$\text{Activity} = \frac{\text{Number interactions by recommenders}}{\text{Total number interactions by all recommenders}}$$

$$\text{Specificity} = \frac{\text{Number of interactions with initiator}}{\text{Total number of interactions with all other hosts}}$$

$$\text{Idleness} = 1 - \frac{\text{Total processing time for submitted jobs within that time period T}}{\text{Total Specific time T}}$$

Credibility = m * similarity + n * activity + o * specificity+ p * idleness

where m>n>o>p and m+n+o+p=1

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

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

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

$$\text{Direct trust (DT)} = \frac{\text{Number of Successful Transactions within the time period T}}{\text{Total submitted jobs Within same time period T}}$$

Considering, DT= 0 if DT<=0.5
Else DT= 1

$$\text{Indirect Trust1} = \frac{(1\text{-Cr})*\text{Average Feedbacks from same domain}}{\text{Credit factor}}$$

Here, Credit factor = 0.5 for same domain.

$$\text{Indirect Trust2} = \frac{(1\text{-Cr})*\text{Average FeedbacksFrom other domain}}{\text{Credit factor}}$$

Here, Credit factor = 0.25

Direct trust is the value which is calculated by the initiator. Indirect 1 & indirect 2 both are calculated by taking the recommenders' feed backs. In indirect 1 the feedbacks are collected from its neighbors. 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, specificity and idealness. 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.

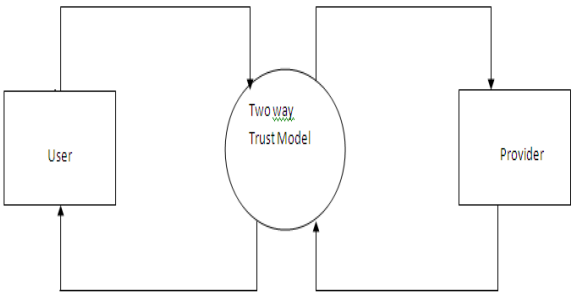
[A, B, C, D, E, F, G, H, I, J, K, L, M, N, O]
Domain1:[A, B, C, D, E, F, G]
Domain2:[H, I, J, K, L, M, N, O]
Malicious = [C,F,K,N]

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

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

5. DESIGN OF THE PROPOSED SYSTEM:

Figure below explains the overall architecture. The user uses the Trust 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.



Functionality and Procedure of The Proposed model :

Step1: We have taken a database called Feedback database. It is divided into two parts. First part is called Provider Feedback database and second part is called User Feedback database.

Step2: The client or the user takes the feedback from Provider Feedback database. If Provider is new then take a non harmful value.

Step3: Calculate Direct Trust if there is any transaction directly by the user and the provider.

Step4: Rank Co-relation(R) is calculated from the feedback of the provider. If Rank Co-Relation is greater than zero than goto next step otherwise that feedback is rejected and next feedback is taken.

Step5: Calculation of Credibility (CR) is done.

Step6: Calculation of the Indirect Trust.

Step7: From Step6 to Step7 is executed in a loop to get other indirect trust value and then average the indirect trust value.

Step8: Calculate Total Trust (TT)

Step9: If the Total trust is greater than threshold value than the provider gets the feedback from user feedback database. Otherwise stop the transaction.

Step10: Rank Co-relation(R) is calculated from the user feedback database. If R is greater than zero than calculate Credibility (CR) Otherwise go to the next feedback.

Step11: Calculate Indirect Trust.

Step12: From Step10 to Step11 is executed in a loop to get all indirect trust. Average all the indirect trust value.

Step13: Calculate total Total Trust. If Total trust is greater than threshold value than start transaction otherwise stop.

	A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*
A	——	4.31	3.23	4.73	4.41	3.47	4.32	4.25	4.21	4.79	2.72	4.19	4.21	2.65	4.11
B	4.67	———	3.11	4.21	4.37	3.36	4.22	4.22	4.19	4.87	2.43	4.87	4.9	3.21	4.05
C	1.87	1.32	———	1.49	1.92	3.82	0.78	1.09	1.01	1.66	3.76	1.36	1.54	3.82	2.01
D	4.42	4.55	2.87	———	4.21	2.56	4.01	4.56	3.99	4.32	3.05	4.45	4.12	2.14	4.03
E	3.51	3.21	1.92	2.75	———	1.91	3.44	3.11	3.57	3.35	1.49	2.66	3.33	1.34	3.21
F	1.25	1.19	3.78	1.23	1.81	——-	1.12	1.43	1.04	1.9	4.01	1.38	1.09	4.73	1.25
G	3.11	2.89	1.86	2.94	3.65	1.78	——	3.32	3.45	2.61	1.76	3.99	2.1	1.33	3.2
H	2.88	3.7	1.65	3.2	3.87	1.54	3.65	———	3.22	3.81	1.14	3.19	3.89	1.89	3.98
I	3.34	3.19	1.45	3.48	3.79	1.14	3.24	3.09	——-	3.02	1.64	3.72	2.58	1.65	3.58
J	4.28	4.17	2.86	4.07	4.01	2.11	4.21	4.17	4.97	——-	3.34	4.52	4.37	2.98	4.67
K	1.32	1.09	4.32	1.34	1.73	4.91	1.08	1.19	1.09	1.55	——-	1.83	1.99	3.67	1.14
L	4.41	4.69	2.52	4.17	4.09	2.34	3.99	3.98	4.56	4.44	2.12	——	4.53	3.09	4.55
M	4.11	4.45	2.13	4.61	3.38	2.66	4.09	4.15	4.35	4.84	3.23	4.39	——	2.45	4.22
N	1.52	1.45	4.67	1.45	1.57	2.67	1.43	1.47	1.86	1.84	4.81	1.19	2.16	——	1.01
O	3.11	3.45	1.23	3.54	2.99	1.34	2.99	3.23	3.19	2.96	1.99	3.03	3.72	1.45	——-

FeedbackTable

6. EXPERIMENTS AND RESULT:

No	Initiator	Provider	Old Model	New Model
1	B	I	NO	Yes
2	C	I	Yes	No
3	D	N	No	No
4	N	A	Yes	No
5	J	M	Yes	Yes
6	B	I	no	Yes

Here we see the results of old model and new model proposed by us.

CONCLUSION:

Security is the most important issue in Grid computing environment because of the concept of virtual organisation where more than one domain exists. This paper represents a novel trust model which is appropriate for both user and provider. In this model the biased feed backs are eliminated and obtain only correct feedback. From the experimental results it can be concluded that this trust model is more reliable for secure transactions in Grid computing environment.

REFERENCE:

[1] 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.

[2] 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.

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

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

[5] 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.

[6] Vivekananth.P "A Behavior Based Trust Model for Grid Security", International Journal of Computer Applications (0975 – 8887) Volume 5– No.6, August 2010, Published by Foundation of Computer Science.

[7] Beulah kurian, Gregor von laszewki "Reputation based Grid resource selection"

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

[9] *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

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

[11] 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).