Proposed P2P Trust and Reputation based Model to Secure Grid

Damandeep Kaur
Society for Promotion In Chandigarh, Chandigarh Administration,Chandigarh.

Jyotsna SenGupta
Department of Computer Science, Punjabi Uiniversity,Patiala.

ABSTRACT
Grid resources and security issues go hand in hand in the success of any Grid application. The present research is moving towards achieving a secured architecture for resource management in Grid System, thereby allowing grid resource to enter the commercial area, where the gird resource cannot be accessed through grid service without the assurance of a higher degree of trust relationship of resource provider. In this paper, we present architecture for Resource Management in Global Grids to Handle Distributed Heterogeneous Resources along with an algorithm, which can be used in Trust Evaluation System, based on PeerTrust Model to compute dynamic trust values which can be used to find degree of trust of grid resource providers.

Keywords
P2P, Trust, Reputation, Grid Resource Management, Grid Services, Virtual Organization.

1. INTRODUCTION
Grid computing is a coordinated resource sharing and problem solving in any dynamic environment. Computing resources are highly heterogeneous. Grid resource management can be utilized to improve the quality of service offered by the grid so that various heterogeneous resources present in the grid can be managed properly. It just not only includes scheduling but also manages the manner in which resources are selected, allotted, authenticated, and accessed. Resource management is a complex task involving security, fault tolerance along with scheduling. Grid applications compete for resources that are very different in nature, including processors, data, scientific instruments and other services. As the current research is moving towards commercialization of grid, there is requirement for secured resource management. For A secured Grid Resource Management System allows it to enter the commercial area and without the assurance of a higher degree of trust relationship between consumer and provider, this cannot be achieved. This paper focus on implementation of security in grid resource management in the form how much trust can be done on a grid resource depending on various parameters like nature of job, performance , availability etc.

2. RELATED WORK
Trust and reputation management has recently become a very useful and powerful tool in some specific environments where a lack of previous knowledge about the system can lead participants to undesired situations, specifically in virtual communities where users do not know each other at all or, at least, do not know everyone. It is in those cases where the application of trust and reputation mechanisms is more effective, helping a peer to find out which is the most trustworthy or reputable participant to have an interaction with, preventing thus the selection of a fraudulent or malicious one.

2.1Trust and Reputation Model in P2P networks

This section will present some of the most representative trust and reputation models for distributed systems.

i)Eigen Trust[17]: This trust model is characterized by the assignment of a unique global trust value to each peer in a P2P file sharing system, based on the peer's history of contributions. The Eigen Trust system assumes some pre-trusted peers exist, and they are trusted by all peers in the system. Peers perform a distributed calculation approaching the eigenvector of the trust matrix over the peers. However, this assumption may be over optimistic in a distributed computing environment.

ii) PeerTrust [7]: It is a trust and reputation model that combines several important aspects related to the management of trust and reputation in distributed systems, such as: the feedback a peer receives from other peers, the total number of transactions of a peer, the credibility of the recommendations given by a peer, the transaction context factor and the community context factor.

The PeerTrust system requires a minimum number of interactions, which is a disadvantage for newcomers and reentry nodes, which are common in P2P systems. The system assumes that a peer with a higher trust value always gives more reliable feedback than a peer with a lower trust value, which might not be true.

iii)Power Trust[13] is a robust and scalable P2P reputation system which leverages the power-law feedback characteristics found applicable in dynamically growing P2P networks, either structured or unstructured. Authors made several comprehensive experiments over a data set extracted from e-Bay transactions and concluded that the feedback numbers in eBay follow a power-law distribution.

In Power Trust system, according to the power-law feedback characteristics, only small number of power nodes that are most reputable will be dynamically selected using a distributed ranking mechanism. Authors show that this system improves in global reputation accuracy and aggregation speed, and as a result, reduces the total job makespan and failure rate in large-scale, parameter-sweeping P2P Grid applications.

iv) BTRM-WSN [16] is a novel trust model for wireless sensor networks (WSN) based on the bio-inspired algorithm of ant colony system. It allows finding the most trustworthy path leading to the most reputable service provider in a network. Its intrinsic nature makes it to be easily adaptable to

sudden changes in the topology of the network as well as in the behavior of its participants.
In this model, a set of ants (artificial agents) is launched through the WSN. While they are searching for the most reputable service provider, they leave some pheromone traces in every link connecting two nodes. That pheromone between sensor a, b is denoted as τ_{ab}, is identified with the confidence sensor a, has on finding the most trustworthy path through sensor b. The last general step of every trust and reputation model consists of punishing or rewarding the selected service provider, according to the user's satisfaction. In BTRM-WSN this step is explicitly performed in terms of pheromone evaporation (punishment) or reinforcement (reward) of the path leading to the selected peer.

2.2 P2P Trust and Reputation Models in Grid

There are many similarities in P2P and grid environment. The Trust and Reputation Models used in P2P environment can be implemented in grid environment with few modifications. As Grids used for complex applications increase from tens to thousands of nodes, we should decentralize their functionalities to avoid bottlenecks. The P2P model could help to ensure Grid scalability.

i) The GridEigenTrust project proposes a reputation service uses an algorithm for evaluating Grid reputation by combining the eigenvectors method and global trust method [18]. In GridEigenTrust, the author exploits the beneficial properties of Eigen Trust , extending the model to allow its usage in grids. They integrate the trust management system as part of the QoS management framework, proposing to probabilistically pre-select the resources based on their likelihood to deliver the requested capability and capacity.

The global trust for an organization with regard to another organization will be built from the direct trust that can be acquired during time from transactions that happened between members of these organizations and by considering also trust information acquired from 3rd party sources. The same trust aggregation scheme can be employed at the level of organization members, each of them storing the trust values for its transaction partners. GridEigenTrust allows obtaining the trust value for an organization by aggregating the trust values of its members.

ii) Path Trust [19] is a reputation system proposed for member selection in the formation phase of a Virtual Organization. To enter the Virtual Organization formation process, a member must register with an Enterprise Network (EN) infrastructure by presenting some credentials. Besides user management, EN supplies with a centralized reputation service. At the dissolution of the VO, each member leaves feedback ratings to the reputation server for other members with whom they experienced transactions. The system requires each transaction to be rated by the participants.

Path Trust is one of the first attempts to apply reputation methods to grids by approaching VO management phases. They approached only partner selection and did not tackled organizational aspects. Their model still lacks dynamicity, as the feedback is collected only at the dissolution of the VO. But, the advance in the field is given by the fact that ideas from previous research were successfully transferred to the area of VOs and grids.

3. Proposed Model for Secured Grid

3.1 Basis of GridPeerTrust:

The basis of our trust model is PeerTrust P2P trust model[7]; the idea to adopt this trust model is its trust evaluating process. In PeerTrust model trust is not dependent on only one parameter but it depends on five different parameters. We have incorporated this model in the grid environment along with improving some of the drawbacks of PeerTrust model and named it as GridPeerTrust.
PeerTrust is a dynamic P2P trust model mainly used for quantifying and assessing the trustworthiness of peers in P2P e-commerce communities. A unique characteristic of this trust model is the identification of five important factors for evaluating the trustworthiness of a peer in an evolving P2P e-commerce community.
Trust Parameters
In PeerTrust, a peer's trustworthiness is defined by an evaluation of the peer it receives in providing service to other peers in the past. Such reputation reflects the degree of trust that other peers in the community have on the given peer based on their past experiences. Five important factors identified for trust evaluation:
1. Feedback in Terms of Amount of Satisfaction. Reputation-based systems rely on feedback to evaluate a peer. Feedback in terms of amount of satisfaction a peer receives during a transaction reflects how well this peer has fulfilled its part of the service agreement. Some existing reputation based systems use this factor alone and compute a peer u's trust value by a summation of all the feedback u receives through its transactions with other peers in the community.
For example, buyers and sellers in eBay can rate each other after each transaction (+1, 0, -1) and the overall reputation is the sum of these ratings over the last six months. From the past research it is seen that these feedback-only metrics are flawed. A peer who has performed dozens of transactions and cheated one out of every four cases will have a steadily rising reputation in a given time duration whereas a peer who has only performed 10 transactions during the given time duration, but has been completely honest, will be treated as less reputable if the reputation measures of peers are computed by a simple sum of the feedback they receive.
2. Number of Transactions. As described above, a peer may increase its trust value by increasing its transaction volume to hide the fact that it frequently misbehaves at a certain rate when a simple summation of feedback is used to model the trustworthiness of peers. The number of transactions is an important scope factor for comparing the feedback in terms of degree of satisfaction among different peers. An updated metric can be defined as the ratio of the total amount of satisfaction peer u receives over the total number of transactions peer u has, i.e., the average amount of satisfaction peer u receives for each transaction. However, this is still not sufficient to measure a peer's trustworthiness. While considering reputation information, account for the source of information and context is also important.
3. Credibility of Feedback. The feedback peer u receives from another peer v during a transaction is simply a statement from v regarding how satisfied v feels about the quality of the information or service provided by u. A peer may make false statements about another peer's service due to jealousy or other types of malicious motives. Consequently, a trustworthy peer may end up getting a large number of false statements and may be evaluated incorrectly because of them even though it provides satisfactory service in every transaction. In PeerTrust, the credibility of feedback is introduced as a basic trust building parameter, which is equally important as the

number of transactions and the feedback. The feedback from those peers with higher credibility should be weighted more than those with lower credibility. Two mechanisms were developed to measure the credibility of a peer to provide feedback.

4. Transaction Context Factor. Transaction context is another important factor when aggregating the feedback from each transaction as transactions may differ from one another. For example, if a community is business savvy, the size of a transaction is an important context that should be incorporated to weight the feedback for that transaction. It can act as a defence against some of the subtle malicious attacks, such as the example where a seller develops a good reputation by being honest for small transactions and tries to make a profit by being dishonest for large transactions. In addition to using the value of the transaction, the functionality of the transactions is another important transaction context as one might trust another to supply books but not supply medical advice.

5. Community Context Factor. Community contexts can be used to address some of the community-specific issues and vulnerabilities. One example is to add a reward as a community context for peers who submit feedback. This may, to some extent, alleviate the feedback incentive problem. As another example, if a trust authority or pretrusted peers (e.g., with digital certificate from the community) are available, then incorporating these community-specific context factors into the trust computation can make the trust metric more robust against certain manipulation of malicious peers.

A general trust metric is formed that combines these parameters in a coherent scheme, and describe the formula we use to compute the values for each of the parameters given a peer and the community it belongs to.

$$T(u) = \alpha * \sum_{i=1}^{I(u)} S(u,i) * Cr(p(u,i)) * TF(u,i) + \beta * CF(u), \quad (1)$$

It is important to note that this general trust metric may have different appearances depending on which of the parameters are turned on and how the parameters and weight factors are set. The design choices depend on characteristics of online communities. The first three parameters—the feedback, the number of transactions, and the credibility of feedback source are important basic trust parameters that should be considered in computation of a peer's trustworthiness in any P2P communities.

3.2 GridPeerTrust Framework:

The proposed Trust-based Grid Manager is shown in figure 2. Trust data that are needed to compute the trust measure for resource provider are stored across the network in a distributed manner. The callout shows that each resource provider has a trust manager that is responsible for feedback submission and trust evaluation, a small database that stores a portion of the global trust data, and a data locator for placement and location of trust data over the network.

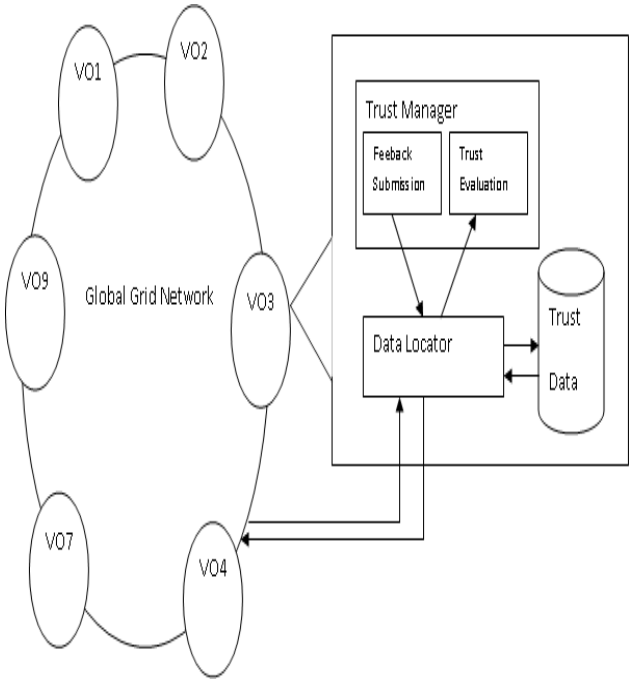

Figure 1: Trust Manager in Global Grid Architecture

The trust manager performs two main functions. First, it submits feedback to the network through the data locator, which will route the data to appropriate resource provider .Second; it is responsible for evaluating the trustworthiness of a particular resource provider. This task is performed in two steps. It first collects trust data about the target peer from the network through the data locator and then computes the trust value. The trust evaluation is executed in a dynamic and decentralized fashion at each resource provider. Instead of having a central server that computes each resource provider's trust value, trust manger acts grid services invoked at institution level obtains resource provider's trust data and computes the trust value of this resource provider.

a. Proposed GridPeerTrust Algorithm:

The PeerTrust model discussed above has certain limitations. First, a minimum number of interactions are required, which is a disadvantage for newcomers and reentry nodes, which are common in P2P systems. Second, the balance factor used is a peer's trust value; the system assumes that a peer with a higher trust value always gives more reliable feedback than a peer with a lower trust value, which might not be true. Third and important limitation is that peer's behavior changes over time. More recent feedback is closer to a peer's current behavior than older feedback. In this model, all previous feedback has the same weight in evaluating a peer's trust value. The major drawbacks of PeerTrust Model are handled in GridPeerTrust Algorithm by changing definition of Satisfaction Criteria and adding a Decay function, in our algorithm.

Trust Parameters:

1. Satisfaction: This trust parameter deals with number of desired features fulfilled by the resource provider. In grid to select a resource provider for performing grid service the basic necessity is to satisfy the basic needs desired by the resource consumer. The parameter acts as a initial parameter

for how well this resource provider has fulfilled the requirements of resource consumer.

2. Decay Function: This is an important trust parameter. It is based on the concept that nothing in grid is static so is the credibility of the feedback as resource provider's behaviour can change with time. The decay function is calculated using credibility of function and number of transactions.
   i) The number of transactions is an important scope factor for comparing the feedback in terms of degree of credibility of feedback.
   ii) While considering reputation information, account for the source of information and context is also important. The indirect feedback resource provider u receives from another resource provider v during a transaction is simply a statement from v regarding how satisfied v feels about the quality of the information or service provided by u. A provider may make false statements about another provider's service due to jealousy or other types of malicious motives. Consequently, a trustworthy resource provider may end up getting a large number of false statements and may be evaluated incorrectly because of them even though it provides satisfactory service in every transaction. To calculate the credibility of feedback, the feedback can be calculated from direct trust, indirect trust, and global trust.

3. Transaction context factor: Transaction context is another important factor when aggregating the feedback from each transaction as transactions may differ from one another. For example, if a community is business savvy, the size of a transaction is an important context that should be incorporated to weight the feedback for that transaction. It can act as a defence against some of the subtle malicious attacks, such as the example where a seller develops a good reputation by being honest for small transactions and tries to make a profit by being dishonest for large transactions. In addition to using the value of the transaction, the functionality of the transactions is another important transaction context as one might trust another to supply books but not supply medical advice.
4. Community context factor: Community contexts can be used to address some of the community-specific issues and vulnerabilities. One example is to add a reward as a community context for peers who submit feedback. This may, to some extent, alleviate the feedback incentive problem. As another example, if a trust authority or pretrusted peers (e.g., with digital certificate from the community) are available, then incorporating these community-specific context factors into the trust computation can make the trust metric more robust against certain manipulation of malicious peers.

Eq 1 is a general trust metric derived from the PeerTrust algorithm with few modifications to overcome the drawbacks of PeerTrust model.

Trust_final = α * Satisfaction + γ + TF + β *CF ------(Eq. 1)

Where

Satisfaction = is the amount of desired features fulfilled by the resource provider.

Decay function (γ) = ∑Cr / ∑Nt

Cr = Credibility of Feedback

Nt = Number of Transaction

Cr = (Feedback Value b/w (u, i) + Previous Feedback) / 2

Feedback Value can be from -1 to 1

-1 depicting a negative feedback for transaction

0 depicting no transaction for that time

1 depicting a positive feedback for transaction

TF = Transaction context factor

CF = Community Context Factor

α, β denote the normalized weight factors for the collective evaluation and the community context factor

Calculating the Trust of Entities:

There are few assumptions with respect to grid environment:

a) All resource providers must be part of any institution of Virtual object of global grid.
b) The basic information of resource provider is stored in trust data of VO.
c) Resource Consumer may or may not be part of grid

Consider a scenario that there are 100 grid resource providers/Grid Entities in a global grid. The resource consumer is not part of grid. The requirement is for a resource having 1000 MIPS and 2 GB RAM. In the basic filtering , the list of resource providers having equal or more 1000 MIPS and 2 GB RAM is fetched from resource search with some initial trust parameters. If there is no resource fulfilling both features then resources with maximum given requirement can be fetched. The trust can be calculated for trust ten fulfilling resource providers.

The trust evaluation component is responsible for computing the trust measure based on the reputation data that are collected about a grid resource.

The following is a listing of steps for calculating Trust using GridPeerTrust Algorithm

Trust Data contains the following information about any resource provider.

Features; Number of Transaction; Current Feedback (u,i); Previous Feedback

The feedback is direct if resource provider and resource consumer are both part of grid and had directly interacted with each other.

The feedback is indirect if resource provider and resource consumer are both part of grid and but never directly interacted with each other. The feedback is calculated on the recommendation of neighbors.

The feedback is global if resource consumer is not part of grid and the feedback is calculated on type of requirement.

Inputs: Client's requirement

1. The Trust Manager receives Grid Resource Provider List; J [n] created in the Grid, where n is the number of resource Providers.
2. Sort the resources as per client's (Resource Consumer) requirement.
3. Select first ten sorted resource providers
4. While trust calculated for ten resource provider from Resource Database

5. Get the Satisfaction value for the resource provider from Resource Database
6. Get the Credibility of feedback(direct/indirect/global) for the resource provider using

Cr = (FeedBack value (u, i) + Previous FeedBack)/2

7. Get the Number of transaction from Resource Database
8. Calculate the Decay function

Decay function (γ) = $\sum Cr / \sum Nt$

9. If TF= yes
   Trust_final = α * Satisfaction + γ + TF
10. if CF = yes
    Trust_final = α * Satisfaction + γ + β *CF
11. if both TF & CF =yes
    Trust_final = α * Satisfaction + γ + TF + β *CF
12. else
    Trust_final = α * Satisfaction + γ
13. End While

Output: Sorted Trust based Resource Provider List

4. COMPARATIVE ANALYSIS

In this section we compare the proposed GridPeer Trust algorithm with GridEigen Trust and Path Trust.

1. In GridEigen Trust and Path Trust , when a new peer joins the grid as resource provider, its assigns a fixed low trust value, where as in GridPeer Trust, the initial trust is evaluated based on the satisfaction criteria.

2. Path Trust does not accounts global trust where as GridEigen Trust and GridPeer Trust both take care about global trust.

3. Majority of the security attack [16] are tackled by using Peer Trust model. The accurate management of the credibility of a peer as a recommender, as well as the context factor or the community one allows GridPeerTrust model to effectively overcome many of the security threats. Thus, malicious individual peers, malicious collectives, malicious collectives with camouflage and driving down the reputation of a reliable peer are some of the threats that are solved by GridPeer Trust. This ability to deal with those threats is due to, among other factors, the definition of credibility in terms of the similarity between two peers, which allows the model to accurately detect and identify in the community malicious service providers as well as malicious recommenders.
4. Additionally it stimulates the community to supply recommendations by building incentives or rewards to those peers who provide feedbacks to others. And this is done through the context factor.

System	**GridEigen Trust**	**Path Trust**	**GridPeer Trust**
Classification	Probalistic>> Flow Model	Probalistic>> Flow Model	Probalistic>> Flow Model
Centralized Data	Yes	Yes	No
Trust Metric	[0,1]	[0,1]	[0,1]
Trust Aggregation	Yes	Yes	Yes
Type of Feedback	Continuous	Negative & Positive	Continuous
Storage Cost	No	No	No
Scalabiltiy	Not Applicable	Medium	High

Table 1: Comparative Analysis

5. CONCLUSION AND FUTURE WORK

In this paper, we have described a framework for calculating trust in Grid environment. The paper mostly focused on issues related to implementation of security in grid resource management in the form how much trust can be done on a grid resource depending on various parameters like nature of job, performance, availability etc. We have identified several of these issues. Second we have experimented with an architecture
and algorithm to gain experience with this new area of research for the Grid community. We have identified a framework and algorithm that is a combination of other research efforts. The underlying algorithm is based on introducing decay function that is updated with feedback based trust calculation algorithm. At present we are enhancing and evaluating our framework by introducing a variety of reputation measurements that are controlled through adaptive parameters.

6. REFERENCES

[1] I. Foster, C. Kesselman, and S. Tuecke, "The anatomy of the Grid: Enabling scalable virtual organizations." International Journal of Supercomputing, vol. 15, no. 3, pp. 200-222, 2001.

[2] Foster, I. and Kesselman, C. Computational Grids. Foster, I. and Kesselman, C. eds. The Grid: Blueprint for a New Computing Infrastructure, Morgan Kaufmann, 1999, 2-48.

[3] R. Buyya and S. Venugopal, The Gridbus Toolkit for Service Oriented Grid and Utility Computing: An Overview and Status Report, Proceedings of the First IEEE International Workshop on Grid Economics and Business Models (GECON), 2004.

[4] Felix Gomez Marmol, Gregorio Martınez Perez, "Security Threats Scenarios in Trust and Reputation Models for Distributed Systems", Elsevier Computers & Security, vol. 28, no. 7, pp. 545-556, 2009

[5] V.Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S.Meder, L. Pearlman and S. Tuecke, "Security for Grid Services", in Proceedings of the HPDC-12, 2003.

[6] Farag Azzedin, Muthucumaru Maheswaran, "Towards Trust-Aware Resource Management in Grid Computing Systems," ccgrid, p. 452, 2nd IEEE/ACM International

Symposium on Cluster Computing and the Grid (CCGRID'02), 2002.

[7] L. Xiong and L. Liu, "PeerTrust: Supporting Reputationbased Trust to P2P E-Communities", IEEE Trans. Knowledge and Data Engineering, July 2004, pp. 843–857.

[8] Chunqi Tian, Shihong Zou, Wendong Wang, Shiduan Cheng,An Efficient Attack-Resistant Trust Model for P2P Networks, IJCSNS, Vol. 6 No. 11 pp. 251-258, 2006.

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

[10] Ran Li, Jiong Yu: QoS Matching Offset Algorithm Based on Trust-Driven for Computing Grid International Conference on Computer Science and Software Engineering, CSSE 2008, Volume 3: Grid Computing / Distributed and Parallel Computing / Information Security, December 12-14, 2008, Wuhan, China. 170-173.

[11] Elvis Papalilo and Bernd Freisleben, Managing Behaviour Trust in Grid Computing Environments, Journal of Information Assurance and Security, Volume 3, Issue 1, March 2008, page 27-38.

[12] V.Vijayakumar and Dr. R.S.D. Wahida Banu, "Security for Resource Selection in Grid Computing Based On Trust and Reputation Responsiveness," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.11, November 2008.Page 107-118.

[13] Zhou R, Hwang K. PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing. Transactions on Parallel and Distributed Systems 2007.

[14] Wang Y, Cahill V, Gray E, Harris C, Liao L. Bayesian network based trust management. In: Autonomic and trusted computing, Third international conference, ATC. LNCS, vol. 4158. Wuhan,China: Springer; 2006. p. 246–57.

[15] Sabater J, Sierra C. Review on computational trust and reputation models. Artificial Intelligence Review 2005;24(1):33–60.

[16] Felix Gomez Marmol, Gregorio Martinez Perez, "Security Threats Scenarios in Trust and Reputation Models for Distributed Systems", Elsevier Computers & Security, vol. 28, no. 7, pp. 545-556, 2009.

[17] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina.The EigenTrust Algorithm for Reputation Management in P2P Networks. In Twelfth International World Wide Web Conference,2003, Budapest, Hungary, May 20-24 2003. ACM Press.

[18] Alunkal B. K., "Grid Eigen Trust: a framework for computing reputation in grids", Thesis Master of Science in Computer Science in the Graduate College of the Illinois Institute of Technology, 2003, http://www.iit.edu/~alunbeu/thesis/thesis-final.pdf

[19] F. Kerschbaum, J. Haller, Y. Karabulut, and P. Robinson. Pathtrust,"A trust-based reputation service for virtual organization formation," In iTrust2006: Proceedings of the 4th International Conference on Trust Management, volume 3986 of Lecture Notes in Computer Science, pages 193–205.Springer, 2006