Generic Trust-Based Resource Broker Architecture for Grid

Damandeep Kaur[1], Dr Jyotsna Sengupta[2]

[1]SPIC, Chandigarh,
[2]Department of Computer Science, Punjabi University, Patiala,
daman_811@yahoo.com,jyotsna.sengupta@gmail.com

***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 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 a Generic Trust-based Resource Broker Architecture for Grid, along with various approaches which can be used in Trust Evaluation System to compute dynamic trust values which can be used to find degree of trust of grid resource providers**.**

***Keywords*:** Trust, Reputation, Grid Resource Management, Grid Services

1. Introduction

Grid resources and security issues play a vital role in the success of any Grid application. Grid security research and development turns around better solutions to take care of the following requirements: Authentication, Secure Communication, Effective Security Policies, Authorization and access control where as RMS focuses mainly on handling the following a) geographical distribution of resources b) resource heterogeneity c) autonomously administered Grid Domains having their own resource policies and practices d) Grid domains using different access and cost models. 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.

Trust and reputation mechanisms are used for large open systems. In general, *reputation* is the public's opinion about the character or standing (such as honesty, capability, reliability) of an entity, which could be a person, an agent, a product or a service. It is objective and represents a collective evaluation of a group of people/agents, while *trust* is personalized and subjective reflecting an individual's opinion. Trust can be transitive [1]. For example, Alice trusts her doctor and her doctor trusts an eye specialist. Then Alice can trust the eye specialist. The notions "trust" and "reputation" are closely related. Trust can be gained from a person/agent's own experiences with an entity or the reputation of the entity, while an entity's reputation relies on the aggregation of each individual person/agent's experiences with it. Trust and reputation are both used to evaluate an entity's trustworthiness. In this paper, in section 2, we present a Generic Trust-based Resource Broker Architecture for Grid and in Section 3, various approaches are discussed which can be used in Trust Evaluation System to compute dynamic trust values which can be used to find degree of trust.

2. Generic Trust-based Resource Broker Architecture for Grid

2.1 Layered Architecture

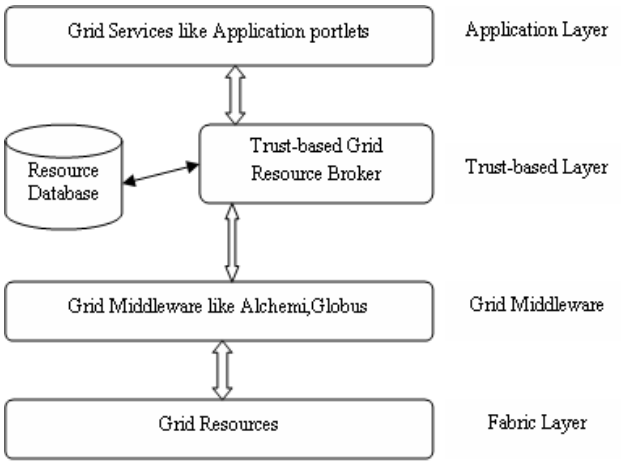

Figure 1: Layered Architecture of Trust-based Grid

The layered architecture of our trust-based grid is shown in Figure 1.

i) Fabric Layer: This layer represents all the physical infrastructure of the Grid, including computers and the communication networks. It is made up of the actual resources that are part of the Grid, such as computers, storage systems, electronic data catalogues and even sensors such as telescopes or other instruments, which can be connected directly to the network.

ii) Middleware Layer: This layer refers to the grid middleware that incorporates necessary components for authentication, monitoring and discovery of grid resources, execution of job in grid resources, file transfer between grid resources.

iii) Trust Based Layer: This layer evaluates the trust value of all the grid resource providers. It computes overall trust value using any Trust Evaluation System and stores them in the database. This trust value is used to identify the most trusted

resources for job execution. Suitable grid resources that match the job requirements are discovered and they are ranked on the basis of their trust value. The resource that has most trusted value is selected for grid services.

iv) Application layer: The highest layer of the structure is the application layer, which includes all different user applications (science, engineering, and business, financial), portals and development toolkits supporting the applications. This is the layer that users of the Grid will see and interact with.

2.2 Trust-Based Grid Resource Broker

The generic resource broker [9] consists of four main components, each having the basic functionality of providing standard interfaces to the rest of the application. The proposed Trust-based Grid Resource Broker shown in Figure 2 also has four components and each of these components is discussed next.

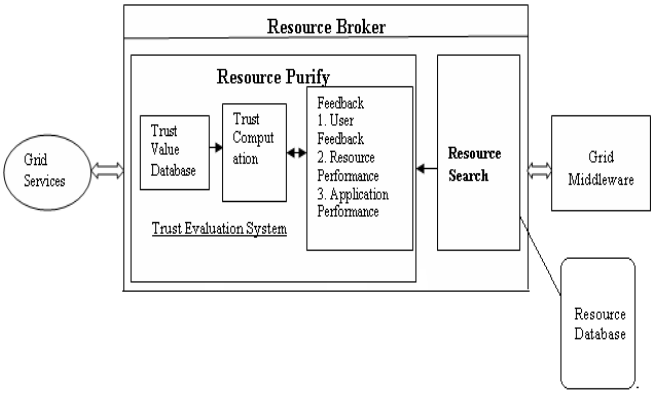

Figure 2: Trust-based Grid Resource Broker

1. Resource Search is a module responsible for fetching the list of all grid resources using any Grid Middleware tool like MDS, Gangalia and storing the list in the resource database. The Resource Search does not do any sort of data organization or processing, other than storing it in the resource database as it was received by the information source.

2 Resource Purify: It provides a standard interface where the implementation of the selection process can be easily adapted for various formats of user request. In the current implementation of the resource broker, the trust value of all grid resource providers is evaluated using various approaches discussed in next section and facilitates the selection of suitable resource for job execution based on the trust value.

It computes trust value of a resource provider based on any of the following three factors:-

- Infrastructure of the organization that provides a grid resource to the grid
- User FeedBack
- Performance metrics of the particular grid resource.

a) Feedback Factor
The feedback value is computed using three basic parameters:

1. User Feedback: This value is obtained using the user's feed back about a particular resource provider by prompting user to mention the level of satisfiability and willingness to recommend the resource to others. The two parameters namely the level of satisfiability and willingness to recommend are collectively called as user feedback parameters and they reflect the behavior of resource provider with user community.

2. Resource Performance /Application Performance: This value is obtained using various performance metrics of every resource providers or application and uses them in evaluating their trust. Various performance metrics like availability, number of success, number of failure, actual execution time, bandwidth, and latency can be considered.

b) Trust Evaluation System
This module can choose any of the various approaches discussed in next section, to compute the value of trust metrics received from underlying resources to calculate overall trust value and gathers the input from all the above modules and computes the overall trust of a resource provider and stores the value in trust value database, which acts as a small buffer. The trust value here represents the trustworthy of the resource provider at a given instant of time.

3. Various Trust-based Approaches

i) Trust Evaluation System can adopt various approaches which have already been applied in Grid

a) Quiz and Replication [15]: The basic idea is to insert indistinguishable quiz tasks with verifiable results known to the client within a package containing several normal tasks. The client can then accept or reject the normal tasks results based on the correctness of quiz results. By coupling Replication and Quiz, a client can potentially avoid malicious hosts and also reduce the overhead of verification and by adjusting the degree of result verification according to the trust value of a level of accuracy.

b) QoS[16]: With proposition that Grid resources and tasks are based on the trust QoS offset value, the most appropriate resources are allocated to specific service requests, which endeavors to achieve high QoS benefit value and allocate Grid resources on demand.

The trust relations between resources and tasks are classed into strong trust relation, weak trust relation and no trust relation. Since this algorithm aggregates tasks and resources based on matching offset and acquires QoS utility as much as possible in resource selection phase, meanwhile gets the smaller QoS matching offset and gains higher effective resource utility.

c) Managing Behavior of Resources [17]: basic idea of the approach is to view the interaction process between Grid participants similar to an industrial production process, and use statistical methods of quality assurance to discover deviations in the behavior of Grid participants in order to assess their behavior trust. Continuous Sampling Plan

approach for managing the behavior trust of Grid participants is presented.

The aim of a continuous sampling plan (CSP) is to control the verification process depending on the verification results in such a way that the maximum of the average outgoing quality (AOQ) does not exceed a specified limit. AOQ can be defined as the fraction of "defective/non-conforming" entities which are not detected through the verification process with respect to the total number of processed entities.

d) D_S theory [18]: The paper proposes a method to detect the supply situation of Grid resources based on D-S theory which is monitored by trust function and trust lost function.

In addition, we propose the representation and updating mechanism of trust function and likelihood function, which calculate the nodes' trust through detecting the cost of receiving trust of nodes in Grid environments. What's more, we have proved the speculation trust function is sensitive and timely in simulating experiments.

In the Grid environment, how to deal with fault-tolerant of the unreliable Grid service and enhances the use factor of the entire Grid system is a future problem waiting for research.

e) Fuzzy-Logic [12]: This trust model combines first-hand (direct experience) and second-hand (reputation) information to allow peers to represent and reason with uncertainty regarding other peers' trustworthiness.

Fuzzy logic can help in handling the imprecise nature and uncertainty of trust. Linguistic labels are used to enable peers assign a trust level intuitively. Fuzzy trust model is flexible such that inference rules are used to weight first-hand and second-hand accordingly.

f) Self Protection [19]: This approach, intends to offer trust and reputation aware security for resource selection in grid computing. The Trust Factor (TF) value of each entity is determined from the self-protection capability and reputation weight age of that particular entity. Moreover the jobs are preferably assigned to the entities with higher TF values. The proposed approach has been found to cope with the ascending number of user jobs and grid entities. It aggregates several security related attributes for both self-protection capability and reputation into numerical values, which can be easily applied to calculate the Trust factor of grid entity. This scheme scales well with both number of jobs and number of Grid sites. This approach is quite effective in selecting secured entity for job execution from the available ones.

g) Review-based Mechanism [11]: This approach uses an *accuracy* concept to enable peer review-based mechanisms to function with imprecise trust metrics, the imprecision is introduced by peers evaluating the same situation differently. Simulation results show that the reputation-based trust model reaches an acceptable level of capability after a certain number of transactions. However, as the number of dishonest domains increase, the model becomes slow in reaching the acceptable level of capability.

To reduce the trust model's sensitivity to dishonest domains, we introduced an *honesty* concept to handle the situation where domains intentionally lie about other domains for their own benefit. Another feature of our model is the flexibility to weigh direct trust and reputation differently. Another significant advantage of our scheme is that our scheme does not depend on a majority opinion as previous schemes did. Therefore, our scheme can work even when majority of the recommenders are malicious.

Actually as the malicious number of recommenders increase, the recommenders providing recommendations to a query reduces. The number of recommenders also provides another measure of trust on the overall system because all the recommenders are considered honest.

ii) Some Open Issues

1. To find efficient and scalable mechanisms for generating quizzes.
2. How to deal with fault-tolerant of unreliable Grid service
3. Focus on trust-driven DAG task scheduling
4. Accuracy and demand for a variety of reputation systems and verification schemes should be conducted.
5. A cooperative scheme to detect and estimate the fraction of malicious nodes behavior to make Accuracy on Demand more precise.

Approaches	Basic idea	Advantage
Quiz and Replication	Sampling-based result verification scheme called Quiz	1. By coupling Replication and Quiz, a client can potentially avoid malicious hosts and also reduce the overhead of verification. 2. By adjusting the degree of result verification according to the trust value of a level of accuracy.
QoS	Trust-Driven QoS Matching Offset	1. To achieve high QoS benefit value 2. Allocate Grid resources on demand
Managing Behavior of Resources	Behavior trust	1. Helps in establishing quality of the collaboration(s) among participants. 2. Evaluate the behavior trust.
D_S theory	Expectation trust benefit driven algorithm.	1. Helps to detect behaviors of resource providers in Grid environment. 2. Prevent the malicious ones accessing the Grid system effectively.
Fuzzy Logic	(a) redefining the honesty concept and its usage by differentiating between consistency and honesty, (b) utilizing the decay function and including two input parameters, namely the time stamp and the transaction frequency, and (c) Extensively using fuzzy logic to model trust representation, trust aggregation, and trust evolution.	
Self Protection	Self-protection Capability and Reputation Weightage.	It aggregates several security related attributes for both self-protection capability and reputation into numerical values, which can be easily applied to calculate the Trust factor of grid entity.
Review-based Mechanism	Trust-aware resource matchmaking strategies	Models the accuracy and honest concepts.

4. Conclusion and Future Work

This paper introduces a generic trust-based resource broker that bridges the gap between a user's requirement and secured grid services on the basis of trust values, along with various approaches for Trust Evaluation System. Finally we

have also tried to address few open issues in regard to the future direction of the research.

References

[1] A. Jøsang, L. Gray and M. Kinateder. Simplification and Analysis of Transitive Trust Networks 4(2) 2006,pp.139-161 . Web Intelligence and Agent Systems Journal. 2006

[2] L.-H. Vu, M. Hauswirth, K. Aberer, QoS-based service selection and ranking with trust and reputation management, Proceedings of OTM'05, R. Meersman and Z. Tari (Eds.), LNCS 3760, p.p. 466-483, 2005.

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

[4] 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.

[4] I. Foster. Globus toolkit version 4: Software for service oriented systems. In Proc. of the IFIP International Conference on Network and Parallel Computing, 2005.

[5] 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.

[6] 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.

[7] Foster, I., Kesselman, C., Tsudik, G. and Tuecke, S. A Security Architecture for Computational Grids. ACM Conference on Computers and Security, 1998, pp: 83-91.

[8] 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.

[9]Enis Afgan, Vijay Velusamy, Purushotham V. Bangalore, Grid Resource Broker Using Application Benchmarking, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, Advances in Grid Computing - EGC 2005, Volume 3470/2005 ,Pages 691-701.

[10]. F. Azzedin and M. Maheswaran, "A Trust Brokering System and Its Application to Resource Management in Public- Resource Grids", in Proceedings of IPDPS 2004.

[11] S. Song, K. Hwang and M. Macwan, "Fuzzy Trust Integration for Security Enforcement in Grid Computing", in Proceedings of IFIP International Conf. on Network and Parallel Computing, (NPC-2004), Wuhan, China, October 18–20, 2004, pp. 9–21.

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

[13] 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.

[14] 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.

[15]. S. Zhao and V. Lo, "Result Verification and Trust-based Scheduling in Open Peer-to-Peer Cycle Sharing Systems," in IEEE Fifth International Conference on Peer-to-Peer Systems, Sept. 2005.

[16] 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.

[17] 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.

[18] Yongsheng Hao, Guanfeng Liu, Yuebin Xu and Junyan Wang, A New Expectation Trust Benefit Driven Algorithm for Grid Environments, International Journal of Hybrid Information Technology Vol. 2, No. 1, January, 2009.

[19] 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.

Author Biographies

Damandeep Kaur, 1980 holds M.E (Software Engineering) degree form Thapar University, Patiala. She is currently pursuing PhD from Punjabi University Patiala and working as Senior Software Engineer in Department of Excise & Taxation, Chandigarh.. Her area of interests includes Parallel and Distributed Computing, Grid Computing, Resource Management, Resource Discovery and Peer-to-Peer Networks.

Jyotsna Sengupta holds PhD degree from Thapar University, Patiala. She is currently H.o.D & reader in Department of Computer Science, Punjabi University, Patiala. Her area of interests includes Parallel and Distributed Computing, Grid Computing, Adhoc Networks.