Randomized Algorithm for Trust Model in Grid Computing using GridSim Components

G. Mahesh Kumar
Assistant Professor,
Department of Computer Science,
Bhavan's Vivekananda College,
Sainikpuri, Secunderabad, India.
gmaheshkumar.cs@bhavansvc.org

Dr. S. Ramachandram
Professor,
Department of CSE,
Osmania University,
Hyderabad, India.
schandram@gmail.com

Dr. Jayadev Gyani
Professor, Department of CSE,
Jayamukhi Institute of Technological Sciences, Narsampet,
Warangal, India.
jayadevgyani@yahoo.com

***Abstract*— Grid Computing pools the resources from various heterogeneous computers to solve a particular problem which requires huge computation. In a grid, a number of known and unknown entities from same or different domain participate in communication where in every entity need to undergo a strong authentication and authorization scheme. There is risk while making the communication among untrusted entities since there is a chance of misusing resources. So, in-order to avoid this problem a strong trust establishment phenomenon is required. This paper demonstrates a randomized algorithm for developing a trust model which makes the user and service provider to maintain consistency among their ratings from each other every time, so that they reach the eligible criteria for communication.**

Keywords*— Grid Computing, GridSim, Grid Certificate, Trust, Resource Broker, Resource

I. INTRODUCTION

Day by day there are many problems raised with respective to computation in the computer field. The resources are very much limited in every organization and this will not help to compute a huge problem. There are many heterogeneous systems available in the world, wants to make the communication to solve the problem. Most of the time the computers are being idle and the resources are wasted, so to avoid this problem Grid Computing has enabled the concept of virtual organizations. These organizations are aiming to support and solve the huge problems by collecting the resources from various idle systems and also from various organizations. The entities (systems) which are ready to participate in communication can be from same domain or from different domains. The entities from same domain can do the communication very happily since they know each other, but the communication is very tough among the entities from different domains due to their differing terms and conditions.

Every entity should be an authenticated and authorized entity which involves in sharing of resources from some other entities. Every entity needs to be accountable for the resources used and they need to do very fair transactions with other entities in order to continue long run transactions in the coming years. Trust is the main concern which should be established among the entities because the entities involved in communication are of heterogeneous systems, are of various policies adapted by various organizations. This paper introduces a randomized algorithm for a trust model to implement security.

II. RELATED WORK

Junyu Xiao et al. [1] proposed an autonomy domain trust model in Manufacturing Grid, based on user trust agent. In this user trust agent acts as a liaison between grid user and grid service provider. Every grid user requests are handled by user trust agent and it lists out corresponding grid service providers based on grid user's request. The grid user will select a grid service provider from the list and returns the result to the user trust agent. The user trust agent based on the response issues a trust certificate extracted from autonomy domain to the grid user. The grid user approaches the grid service provider with the certificate, if it accepts the certificate, then conversation starts. The user trust agent will update the records of both the entities before the termination of the transaction.

Sourav Gayen et al. [2] proposed a trust model for selecting the best resource in grid. In this model, the calculation of direct trusts (in same and different domains) and also the calculation of total indirect trusts for same and distinguished domains are done by approaching different parameters like similarity, activity and popularity. Based on the maximum total trust, the best resource from the network is selected.

P Vivekananth [3] proposed a trust model based on reputation for resource selection in grid computing. In this model, the Spearman's Rank Coefficient method is used for eliminating the unreliable feedback values.

Srivaramangai P, Rengaramanujam Srinivasan [4] proposed a comprehensive trust model for improving reliability in grid, measures direct trust based on different parameters such as context and size of jobs. This model considers various types of jobs like printing documents, transferring files and also size of jobs like small, medium and large. This model has used three types of trust i.e, direct trust1, direct trust2 and indirect trust.

978-1-4799-8047-5/15/$31.00

P Vivekananth [5] proposed eigen trust algorithm for resource selection in grid computing. In this model, the sum of transactions of each service provider is calculated from each consumer table. If the calculated value is > 0, the transaction is accepted or else rejected. The sum of values is normalized and a matrix is formed. The resulted matrix is transposed and power of it is taken, then the reputation of a resource is calculated based on alpha and beta values from which the top four resources are ranked in the order of trust.

III. TRUST AND REPUTATION SYSTEMS

The definition of trust is defined in [6]:
"*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 is defined in [6]:
"*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*."

IV. GRIDSIM: GRID MODELING AND SIMULATION TOOLKIT

In grid computing there are many heterogeneous resources involved in communication from same or different domains in-order to solve huge problems. Each domain has their own policies for utilizing the resources. GridSim toolkit provides an opportunity for simulating users, resource brokers, applications and schedulers and various resources. In this every user has their own resource brokers basically used to discover, select and pooling various distributed resources [7].

GridSim is used to locate resources in different time zone, to reserve the resources in advance, to run applications in parallel to enable multiple users to submit their jobs for execution simultaneously, to support simulation of both static and dynamic schedulers. There are GridSim entities like Grid User, Broker, Grid Information Service (GIS), Input and Output, Resource. Grid User requests the service from service provider, Broker is used to schedule the resources, and GIS is responsible to store a dynamic list of free resources available at service provider.

V. GRID CERTIFICATE

Grid consists of many entities involved in-order to share resources for solving large problems. The entities may be from same or different organizations. Each organization is holding various policies with respective to the allocation and usage of resources [8]. There is a need of strong authentication and authorization process in-order to make the communication possible among distinguished entities from various organizations. The Grid Certification Authority (CA) is one of the official and authenticated organizations responsible for issuing grid certificate to the entities requesting permissions for sharing resources from various virtual organizations. Each Grid Certificate will hold information like person, host, service etc. Grid CA is also responsible for revocation of certificates of the entities who misuse the resources of service provider.

VI. THE PROPOSED TRUST MODEL

The proposed trust model is using a randomized algorithm on the client and service provider feedback values to maintain consistency ratings among them. This mechanism allows both the entities to face a strong authentication and authorization criteria throughout the communication by using the gird certificates and maintaining stability among their reputations.

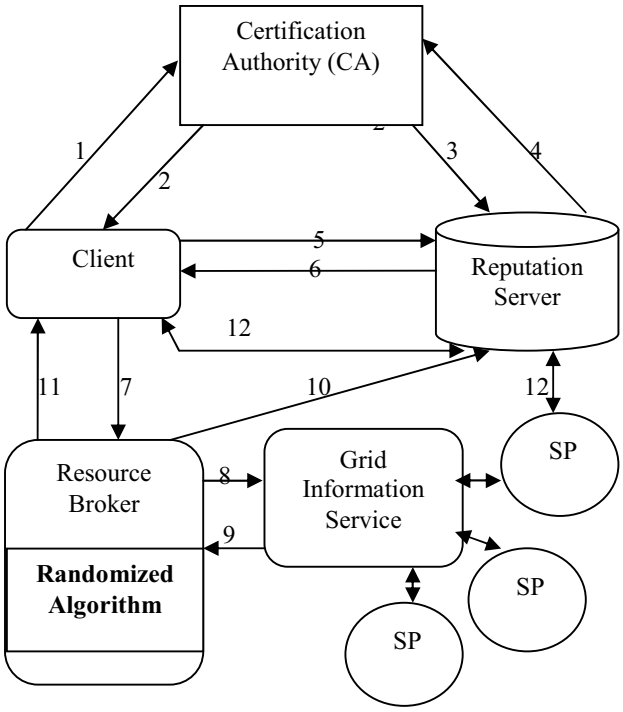

Figure 1: Trust model using randomized algorithm.

The entities of the trust model as shown in figure 1 are as follows:

Certification Authority (CA): The Certification Authority is an authorized entity which is responsible for issuing certificates to the authorized clients which helps in authentication of clients.

Client: The Client is the entity which requests the resources from the service providers for utilizing their resources. Each client in the grid is called as Grid User.

Resource Broker: The resource broker is an entity acting as a mediator between client and service provider which accepts the request from the clients and gets the available resources list from the Grid Information Service which acts as a directory service, negotiates for access costs using trading services, maps tasks to resources, stages the application and data for processing, starts job execution, and finally gathers the results. It is also responsible for monitoring and tracking application execution progress along with adapting to the changes in grid runtime environment conditions and resource failures.

Grid Information Service (GIS): The GIS acts as a directory service which maintains the list of all the available resources from various service providers. Every transaction is dynamic in nature and the GIS play a very critical role in updating itself.

Service Provider (SP): The SP is an entity which provides the resources to the requested users, but these resources need to be registered in the Grid Information Service by the service providers.

Reputation Server: This reputation server is an application server which maintains the Clients feedback database and Service Provider's feedback database. The Clients need to give their feedback about the service provider and the feedback value need to be between 0 & 1 before the termination of conversation. Similarly the service providers need to give their feedback about the user and the feedback value need to be between 0 & 1 before the termination of conversation.

The steps involved in the trust model using randomized algorithm as shown in figure 1 are as follows:

1. The client requests a grid certificate from the Certification Authority (CA) by sending the certificate signing request along with their credentials.

2. The Certification Authority receives the request and verifies the authenticity of the client based on the provided credentials like driving licence, etc., and then it creates or renewals a grid certificate if the credentials are correct. The CA issues a username, password and a grid certificate to the client signed by the CA's private key.

3. The Certification Authority updates the entries of new or renewal of grid certificate in the Reputation Server (RS) simultaneously.

4. The acknowledgement is send to the Certification Authority by the Reputation Server for each and every entry made by CA.

5. The client uses their username, password and grid certificate to log into the Reputation Server.

6. The Reputation Server verifies the client credentials and generates a transaction ticket called as a token and sends to the client. The validity of the token is only for single conversation.

7. The client communicates with the Resource Broker (RB) with the help of a token and submits the requirements.

8. The Resource Broker contacts the Grid Information Service (GIS) to extract the resources available that suits the client requirements.

9. The Grid Information Service has a resource availability list based on the user requirements, since all the service providers dynamically register their resources which are available for service.

10. Once the client and selected service provider accepts each other's terms and conditions, then the Resource Broker get the feedback values of client and service provider using Randomized Algorithm (RA) from the Reputation Server to establish trust with more security.

Randomized Algorithm for Trust Model

a) There are two tables namely Client's Feedback Table and Service Providers Feedback Table in the Reputation Server. At the end of every transaction the client and the service provider need to rate each other in the range of 0 - 1.

b) In-order to calculate the feedback of existing client and service provider , we need to consider the following points:

(i) If a client or a service provider interacts with each other for the first time then the Resource Broker can allow the communication based on indirect trust i.e., recommendation from some other client or a service provider respectively by assigning a threshold value >=0.5

(ii) If a client or a service provider interacts with each other where they have only one entry in respective feedback tables, then the Resource Broker has to take that value separately from both tables and compare them with the threshold value i.e., >=0.5, if both the

results are yes then communication proceeds else no communication.

(iii) If a client or a service provider interacts with each other where they have two entries in respective feedback tables, then the Resource Broker has to take the average of both the values separately from both tables and compare them with the threshold value i.e., >=0.5, if both the results are yes then communication starts else no communication.

(iv) If a client or a service provider interacts with each other where they have three entries in respective feedback tables, then the Resource Broker has to consider last two recent transactions as one set of values and get their average, the other element will be considered as it is. Then find the summation of average value and other element and at last find the average of the summation value. If the final value is >=0.5 of both client and service provider then communication proceeds, otherwise it stops.

(v) If a client or a service provider interacts with each other where they have four or more entries in respective feedback tables, then the Resource Broker need to consider two set of values from their respective feedback tables.

- ✓ In one set we take feedback of two recent transactions.
- ✓ In another set we take feedback of two more transactions randomly apart from two recent transactions already considered.
- ✓ Take the average of two sets separately.
- ✓ Find the summation of the average values and again calculate its average.
- ✓ If the final average of client and service provider is >=0.5 threshold value, then the Resource Broker starts the execution otherwise it simply terminates the transaction.

Note: If the client or a service provider does not reach the threshold criteria, then they can approach each other after 45 days with respective to the indirect trust given by other client or service provider with the minimum reputation of 0.5 and above. If any kind of misbehaviour is done by the new entrant, then the new entrant as well as their introducer (either client or service provider) will be penalized and penalty will be imposed on them.

The Reputation server contains Clients feedback table and Service Providers feedback table:

Table 1: Clients Feedback Table

CID	SP1	SP2	SP3	SP4	SP5
C1	0.7	0.2	X	X	X
C2	X	0.7	0.3	X	X
C1	0.8	X	X	0.6	0.6
C4	X	0.3	X	0.2	0.4
C5	0.4	0.9	X	0.9	X
C2	0.1	X	X	0.4	0.3
C3	X	X	X	0.3	0.5
C7	X	X	0.8	0.7	X
C1	X	X	0.1	0.6	0.4
C6	0.7	X	0.4	X	0.6
C1	X	X	0.9	0.8	X
C2	0.2	0.6	X	X	0.5
C1	0.1	0.5	X	0.7	x
C3	X	X	0.4	0.5	X
C1	X	0.6	X	0.3	X
C5	X	0.3	0.6	X	0.6
C1	0.6	X	0.4	X	X

Table 2: Service Provider's Feedback Table

SPID	C1	C2	C3	C4	C5	C6	C7
SP1	0.6	0.5	X	X	0.8	0.5	X
SP2	0.5	0.2	X	0.7	0.1	X	X
SP3	0.4	0.2	0.8	X	0.6	0.6	0.8
SP1	0.6	0.3	X	X	X	X	X
SP4	0.5	0.5	0.5	0.6	0.3	X	0.6
SP5	0.4	0.3	0.7	0.5	0.6	0.4	X
SP4	0.7	X	0.3	X	X	X	X
SP5	0.4	0.5	X	X	X	X	X
SP3	0.3	X	X	X	X	X	X
SP4	0.4	X	X	X	X	X	X
SP2	0.2	0.6	X	X	0.8	X	X
SP1	0.6	X	X	X	X	X	X
SP4	0.7	X	X	X	X	X	X
SP2	0.3	X	X	X	X	X	X
SP4	0.6	X	X	X	X	X	X
SP1	0.5	X	X	X	X	X	X
SP3	0.6	X	X	X	X	X	X

SPID – Service Provider Identity

CID - Client Identity

[C1, C2, C3, C4, C5, C6, C7] – Clients

[SP1, SP2, SP3, SP4, SP5] – Service Providers

X – No Transaction

Calculation procedure for Service Provider's Feedback:

$$\mathbf{SPF1} = \frac{\text{Sum of two recent feedback values given by service provider with respective to client}}{2}$$

$$\mathbf{SPF2} = \frac{\text{Sum of two feedback values selected randomly apart from two recent transactions given by service provider with respective to client}}{2}$$

$$\mathbf{SPF} = \frac{SPF1+SPF2}{2}$$

Calculation procedure for Clients Feedback:

$$\mathbf{CF1} = \frac{\text{Sum of two recent feedback values given by client with respective to service provider}}{2}$$

$$\mathbf{CF2} = \frac{\text{Sum of two feedback values selected randomly apart from two recent transactions given by client with respective to service provider}}{2}$$

$$\mathbf{CF} = \frac{CF1+CF2}{2}$$

CF - Clients Feedback

SPF - Service Provider's Feedback

For example: Client = C1, Service Provider = SP4 from Table 1 and Table 2:

Calculation of CF1 from Clients Feedback Table:

$$CF1 = \frac{(0.3+0.7)}{2} = \frac{1.0}{2} = 0.5$$

$$CF2 = \frac{(0.6+0.6)}{2} = \frac{1.2}{2} = 0.6$$

$$CF = \frac{(0.5+0.6)}{2} = \frac{1.1}{2} = 0.55$$

Calculation of SPF from Service Provider's Feedback Table:

$$SPF1 = \frac{(0.6+0.7)}{2} = \frac{1.3}{2} = 0.65$$

$$SPF2 = \frac{(0.5+04)}{2} = \frac{0.9}{2} = 0.45$$

$$SPF = \frac{(0.65+0.45)}{2} = \frac{1.10}{2} = 0.55$$

11. Based on the above results, the client and service provider's feedback i.e., CF and SPF is greater than 0.5. Hence, the resource broker accepts the communication.

12. The client and service provider need to send the feedback values to the reputation server just before the termination of the conversation and also the reputation server sends the acknowledgement to both.

VII. Conclusion

This paper presents a trust model, highlighting a randomized algorithm which concentrates recent transactions feedback values and also other transactions feedback values selected randomly apart from recent transactions for calculating clients and service providers threshold value. This trust model makes the client and service provider to maintain consistency in the feedback values whenever a transaction is done. This model also highlights the grid certificate issued by Certification Authority which enables strong authentication and authorization. This model has used GridSim Components like Resource Broker used to connect client and service provider for the resource scheduling and the list of available resources are taken from the Grid Information Service component.

References

[1] Junyu Xiao, Zhangwei Yang, Feng Jiang, "Autonomy Domain Trust Model in Manufacturing Grid based on User Trust Agent" TELKOMNIKA, Volume II, No.11, November 2013, Page(s): 6534-6539.

[2] Sourav Gayen, Avijit Bhowmick, Biswajit Upadhyay, "Developing a Novel Trust Model for the Best Resource Selection among the Resources in Grid Environment", International Journal of Computer Applications, Volume 70, No.6, May 2013, Page(s): 28-34.

[3] P Vivekananth, "An Overview of Trust Models and Proposal of New Model Based on Reputation for Resource Selection in Grid Computing", International Journal of Engineering and Technology, Volume 2, No.4, August 2010, Page(s):387-389

[4] Srivaramangai P, Rengaramanujam Srinivasan, "Enhancements to Reputation based Trust Models for Improved Reliability in Grid Computing", WSEAS TRANSACTIONS ON COMPUTERS, Volume 10, July 2011, Page(s): 220-233.

[5] P Vivekananth, "Eigen Trust Algorithm for Resource Selection in Grid Computing", International Journal of Computer Applications, Volume 16, No.4, February 2011, Page(s): 50-54.

[6] A.Arenas,"State of art survey on trust and security in Grid Computing sytem",march 2006.

[7] Manzur Murshed, Rajkumar Buyya,"GridSim: A Toolkit for Modeling and Simulation of Distributed Resource Management and Schedulig for Grid Computing".

[8] Mary R. Thompson,Doug Olson,Robert Cowles, Shawn Mullen, Mike Helm,"CA – based Trust Model for Grid Authentication and Identity Delegaatio",October 2002.