

Exploring Trust Models in Grid Computing

G Mahesh Kumar¹, Dr. S Ramachandram², Dr. Jayadev Gyani³

Assistant Professor, Department of Computer Science, Bhavan's Vivekananda College, Sainikpuri,
Secunderabad, India.¹

Professor, Department of CSE, Vice-Chancellor, Osmania University, Hyderabad, India.²

Professor, Department of CSE, Jayamukhi Institute of Technological Sciences, Narsampet, Warangal, India.³

ABSTRACT: Grid Computing is a network of computers in which resources are shared with other computers to solve critical applications which requires huge computations. Resources like memory, data storage, processing power are shared among various heterogeneous computers. In a grid, the computers involved in computation might be from same domain or from different domains. Every computer involved in grid need to undergo the process of authentication to ensure the validity of the user. There will be more risk from the un-trusted entities involved in the grid because they may misuse the resources. There is a requirement to prepare a robust trust model to identify the un-trusted entities to avoid misuse of resources. This paper presents various existing trust models used in grid computing for the best utilization of resources available in heterogeneous computers.

KEYWORDS: Grid Computing, Authentication, Trust, Resource, Reputation.

I. INTRODUCTION

Grid Computing is a technology which pools the resources available from various heterogeneous systems for huge computations. Every individual system has its own limited resources which may not be sufficient to process mission-critical applications. There are many systems throughout the world which may not be utilized completely for the whole day; so the resources of the idle systems need to be utilized for processing a huge request. The computers which are idle need to be part of a grid, so that their resources can be shared among different computers for computation.

The computers involved in a grid might be of same domain or different domains. The systems involved in communication from same domain will be done very smoothly since the users are known and they trust each other. The problems arise when the systems from other domains are involved since they are not known in the current domain. Computers from any other domain need to be a trusted entity for the best utilization of the resources. Every system needs to be authenticated prior to use or allocate resources from various other systems.

This paper explores various trust models used to establish trust among known and unknown entities for sharing various resources from heterogeneous systems to solve very complex problems.

II. TRUST

In grid computing there are many entities from various domains involved in communication. Trust is the strong belief that should be established between the trustor and trustee to do transactions genuinely according to the agreements made before the start of the transactions. Direct trust is the process where trustor and trustee both are well known to each other and there is no need to have an intermediary entity among them for recommendation. Indirect trust is the process where the trustor and trustee are not well known to each other where an intermediary is required among the entities for recommendation. Reputation is another factor through which we can build trust and it is based on building of confidence, and also on the past transactions done among the entities involved in transactions.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

III. TRUST MODELS

Ahmad Habibizad Navin et al. [1] proposed a multi criteria trust model in grid computing systems. In this model multiple criteria's like self-defence capability, direct trust and reputation are used to select a secured resource by applying fuzzy multi criteria decision making method. An entity, broker uses a common resource discovery method to find a set of systems to satisfy requests forwarded by a client. Every system has a component called trust agent which has information about the direct trust level between entities involved in communication for any context in a direct trust table. The criteria called self-defence capability use some secure factors like intrusion detection capability, anti-virus capability and fire wall capability for protecting resources. All the secure factors are allocated some weights based on their contribution to security. When any two entities complete their interaction with each other then they store and update the trust levels in their own direct trust level table.

In this, the direct trust level and satisfaction trust level both are calculated for each context. If the threshold value is greater than 0.5 then more priority is given to direct trust level rather than satisfaction trust level. In calculating the reputation of an entity, the broker issues a message to all the subscribed entities, those who had registered themselves with the broker for sending the direct trust values of that entity. Once the request from broker is received by the subscribed entities then they check the values in the trust table maintained by trust agent. The subscribed entities extract the trust values from the trust table and send to the broker. The broker collects all the trust values and calculates the reputation values of entities.

The steps to find the secure resource using multi criteria decision making are: creating the decision matrix, normalization, weighted matrix, determining trust factor for each entity and finally selection of secured entity.

Srivaramangai P, Rengaramanujam Srinivasan [2] proposed a reputation based on two way trust model for reliable transactions in grid computing. In this model, the reliability is the major factor to be considered for transactions. Every grid client access the resources from the grid service provider, but the resources should not be misused by grid client. This model instructs both the grid client and service provider to give feedback about each other regarding the usage and allocation of resources by the entities involved in transactions. The feedback values of both entities are used to calculate trust in-order to take a better decision for allowing or rejecting the entities from further communication.

The process for calculating trusts by the grid client is that they get recommendations about providers from various other entities, and then apply rank correlation to decide for accepting the recommendations. If the correlation result is positive then the client accepts, otherwise they go to the next feedback. Finally client calculates total trust. If total trust is greater than threshold value then they choose that provider. Similarly providers get the recommendations about client from various other entities, and then apply rank correlation to decide for accepting the recommendations. If the correlation result is positive then the provider accepts, otherwise they go to the next feedback. Finally provider calculates total trust. If total trust is greater than threshold value then they choose that client. In this model both the client and service provider need to have the value greater than the threshold value for doing the reliable transaction.

P Suresh Kumar et al. [3] proposed purging of untrustworthy recommendations from a grid. This model evaluates the trust relationship between various entities based on direct trust or indirect trust. In direct trust the two participating entities are well know to each other and each one can share information without any further recommendations. In indirect trust, the participating entities are unknown to each other and they gather the information from other recommenders. In this model every recommended value is multiplied with the corresponding credibility factor. The credibility factor represents the trust of a host to give a valid recommendation about other entities. Credibility factor depends on three factors similarity, activity and popularity of an entity. The similarity factor determines how two hosts are similar in their reputation values and evaluation procedures. In this model Kendall's rank correlation method is used to find similarity between recommendations. If one entity is giving different recommendations compared to other entities, then the similarity factor is not valid; they are giving un-trusted information. The activity factor shows the level of activity of an entity in the past interval of time. Activity is calculated as the number of interactions made by an

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

entity in the past with respect to other entities. The popularity factor shows how much the entity is liked by other entities. The popularity of an entity is calculated as number of interactions other entities have done with a specific entity out of all interactions. All the above mentioned three factors are used to calculate the reputation of an entity. If the value is greater than the threshold value then job is assigned otherwise it is rejected.

G Mahesh Kumar et al. [4] proposed randomized algorithm for trust model in grid computing using gridsim components. This trust model uses a randomized algorithm on the client and service provider feedback values to maintain consistent transactions among them. This mechanism allows both the entities to face a strong authentication and authorization criteria throughout the communication by using the grid certificates and maintaining stability among their reputations.

In this model the client requests a grid certificate from the Certification Authority (CA) by sending the certificate signing request along with their credentials. 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 renews 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. The Certification Authority updates the entries of new or renewal of a grid certificate in the Reputation Server (RS) simultaneously. The acknowledgement is sent to the Certification Authority by the Reputation Server for each and every entry made by CA. The client uses their username, password and a grid certificate to log into the Reputation Server. 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. The client communicates the Resource Broker (RB) with the help of a token and submits the requirements. The Resource Broker contacts the Grid Information Service (GIS) to extract the resources available that suits the client requirements. 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. 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.

The steps to use 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 true 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 true 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.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

- (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.

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.

M Ashok et al. [5] proposed a logarithmic regression analysis of trust computation in 'grid resource broker'. In this paper a new methodology is proposed to find the best resource for computational grid. For most of the trust models the parameters like network bandwidth, system availability, execution time of the resource, latency, and failure rate of the resource are used for calculating trust of a resource. Apart from the above mentioned parameters, one additional parameter, hack rate is considered in this model. Every transaction is done through internet and there are lot of chances to hack the resources by the intruders. In this model once all the parameters are calculated individually, then, the failure rate and hack rate values are subtracted from the other parameter values, so that the trust of the resource can be very much accurate.

Srivaramangai P, Rengaramanujam Srinivasan [6] proposed enhancements to reputation based trust models for improved reliability in grid computing. In this, two new reputation based trust models are proposed. In model 1 a new factor called compatibility is used based on Spearman's rank correlation along with the credibility factor which involves similarity, activity and popularity. This compatibility factor is used to eliminate the incompatible feedbacks about the initiator given by recommenders. The model 2 is an improvement on model 1 in which two important factors - context and size are embedded to evaluate the trustworthiness of the entities. The model 2 assumes that every feedback is different for every kind of job done by an entity. This model is using three types of trusts namely direct trust 1, direct trust 2 and indirect trust. Direct trust 1 is used when user and a provider do the same kind of transactions and Direct trust 2 represents trust when a different kind of transactions are done by user and provider. Indirect trust is considered when users and providers trust values are extracted by recommendations from other entities. So, this model considers that reputation values are not same for all kinds of transactions. When there is no interaction between user and provider then their reputations will fall down.

Vivek Ananth P [7] proposed a trust model to present a pool of providers for resource selection in grid computing. In this model trust is measured by reputation which are the opinions given by others. In this model a service provider must be selected from the available pool of providers. When an initiator requests for a resource provider then the proposed model checks all the available providers in the pool and calculates the total trust of every provider and displays the providers rank list based on its trustworthiness. Among the providers rank list the initiator will be allocated a provider with highest rank. In-order to generate the complete providers list with respective to ranking it takes a lot of time, so this model generates the top four providers list based on trustworthiness to minimize the time wastage for selecting the best service provider.

Sourav Gayen et al. [8] proposed developing a novel trust model for the best resource selection among the resources in grid environment. This model first calculates the feedback of each resource which is given by other entities and then calculates the reputation of each resource belonging to same or different domain. Then the direct trust and total indirect trust need to be calculated with the parameters like similarity, activity and popularity. Finally, we need to calculate the total trust for every resource. Once the total trust is prepared for all the resources, then select the resource with

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

maximum total trust. The resource with the maximum total trust in the network is considered as the best resource for transactions.

IV. CONCLUSION

This paper presents taxonomy of various trust models used in grid computing. These trust models are used to find the malicious users from misusing the resources. Few trust models are using the parameters like similarity, popularity, and activity to find out which resources the entities are using frequently to create a positive trust. A trust model, highlighting a randomized algorithm selects feedback values of clients and service provider's randomly and also its recent transactions to calculate the final feedback value. This trust model ensures that the client and service provider maintain consistency in making the proper use of resources. Another trust model is based on providing security by using self-defence capability, direct trust and reputation to select a secure resource.

REFERENCES

- [1] Ahmad Habibzad Navin, Neda Azari Khosroshahi, Ali Sagar Pourhaji Kazem, "Multi Criteria Trust Model in Grid Computing Systems", International Journal of Advanced Research in Computer Science, Volume 4, No.2, Jan-Feb 2013, Page(s): 55-59.
- [2] Srivaramangai P, Rengaramanujam Srinivasan, "Reputation Based Two Way Trust Model for Reliable Transactions in Grid", International Journal of Computer Science Issues", Volume 7, Issue 3, No.5, May 2010, Page(s): 33-38.
- [3] P Suresh Kumar, P Sateesh Kumar, S Ramachandram, "Purging of Untrustworthy Recommendations from a grid", International Journal of Next-Generation Networks, Volume 3, No.4, December 2001.
- [4] G Mahesh Kumar, Dr.S.Ramachandram, Dr. Jayadev Gyani, "Randomized Algorithm for Trust Model in Grid Computing using GridSim Components", IEEE International Advance Computing Conference, June 2015, Page(s): 936-941.
- [5] M Ashok, S Sathiyam, "Logarithmic Regression Analysis of Trust Computation in Grid Resource Broker", International Journal of Computer Science & Information Technology Advanced Research", Volume 2, SP-1, Feb-2014, Page(s) 140-142.
- [6] 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.
- [7] Vivek Ananth P, "Trust Model to present a pool of providers for resource selection in Grid Computing", Computer Science & Telecommunications, 2011, No.3(32), Page(s):53-58.
- [8] 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.