Evaluating Trust in a Grid Environment

(Shashi[1], Seema Bawa[2])
Research Scholar, Computer Science and Engineering Department
Professor & Head, Computer Science and Engineering Department
Thapar University, Patiala-147004. INDIA.
{shashi, seema}@thapar.edu

Abstract

The migration of processing of computational jobs from centralized systems to open distributed systems have resulted in many communication channels and transactions, to span a range of domains and organizations, not all of which can be trusted to the same extent. Inconsistencies in current trust relationships highlight the need for a flexible, general-purpose trust management system that can navigate these (possibly) complex trust domains. In this paper, we have proposed a Trust Model for evaluating trust in these open distributed environments where the resources utilized are expensive and vulnerable to threats.

Key words: Grid Security; Trust Model

1. Introduction

Grid technology provides an infrastructure for sharing resources in dynamic and multi-institutional virtual organizations [1], enabling an open marketplace, in which hardware resources (i.e. computing power, storage, and bandwidth), software, and data can be traded across administration boundaries. With the development of grid, the number of users and potential threat to this massive infrastructure increases. Unfortunately, the notion of "sharing" poses some concerns such as privacy, confidentiality, and autonomy. Hence, "trust" should be addressed in such distributed environment. In this paper, a trust model is presented for evaluating trust in a grid environment. The trust model is based on using the trust score of the entity and domain, which is further, based on transactions and the feedback score. This model helps to improve grid security by accurately evaluating the trustworthiness of a node. Section 2 discusses the related work. Section 3 discusses some trust related issues in context to our Trust model. Section 4 discusses our Trust Model and Section 5 concludes the work and Section 6 lays emphasis on Future work.

2. Related Work

Trust is a complex subject relating to belief in the honesty, truthfulness, competence, reliability, etc., of the trusted person or service. There is no consensus in the literature on what trust is and on what constitutes trust management [2, 3], though many research scientists recognize its importance [4, 5]. A trust relationship can be one-to-one between two entities, however it may not be symmetric. In general, the entities involved in a trust relationship will be distributed and may have no direct knowledge of each other, so there is a need for mechanisms to support the establishment of trust relationships between distributed entities. According to Gambetta [6], trust refers to the subjective probability by which an individual A expects that another individual B performs a given action on which its welfare depends. Our Trust Model is based Feedback Score as used in ebay model [7]. There are various trust management systems (TMS) in the industry such as PeerTrust, XenoTrust, NICE TMS and SEGO which are Reputation Based TMS. PeerTrust Trust Builder and Trust Builder are Policy based TMS [8].

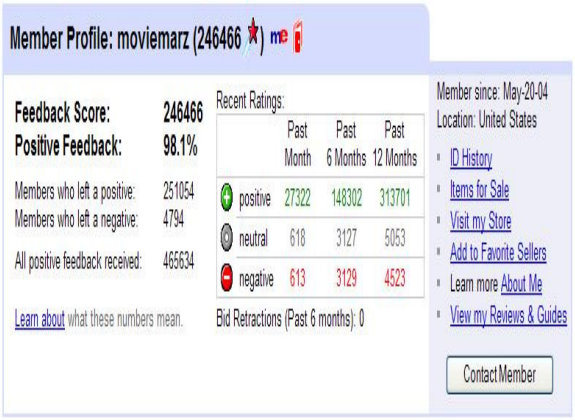

Figure 1. ebay Feedback System

3. Trust Related Issues

Having the notion of reputation and trust, many trust queries arise in grid environment. Due to the characteristics of grid, such as dynamics, instability and uncertainty, these trust queries are complex.

After an extensive literature survey of the taxonomy and models related to trust, we have proposed our Trust model for an open distributed environment i.e. Grid considering the following issues:

3.1 Reputation

Reputation is a measure of trustworthiness, in the sense of reliability. Trust can be built from (i) the confidence an agent derives from past interaction and (ii) the reputation the agent acquires from the social network. We have assessed reputation both from past transactions and trust score.

3.2 Trustworthiness (TR)

An entity's trustworthiness is an indicator of the quality of the entity's services. It is often used to predict the future behavior of the entity. Intuitively, if an entity is trustworthy, it is likely that the entity will provide good services in future transactions too.

3.3 Feedback

A piece of feedback is a statement issued by the client about the quality of a service provided by a server in a single transaction. We have assumed the service provider and service requestor rate each other's service in terms of feedback score. Here, the feedback score is based on secure services.

3.4 Trust relationships

Determining trust relationship is essential not only while accessing resources/services but also while enabling delegation. We have assumed the following three Trust Relationships for our model.

Direct Trust: Direct Trust is obtained when communicating entities hold each other's keys within their TAL (Trust Anchor List), so that their validity is established without reliance on intermediaries.

Indirect Trust: Indirect Trust is obtained when communicating entities ascertain the validity of each others' keys based on pre-existing trust established with an intermediary, as represented by a trust anchor.

Recommended Trust: Recommended Trust is the trust of one entity on second entity that is recommended by other entities.

4. The Proposed Trust Model

A Trust Model can be defined as a system that allow service requesters and service providers to assess trustworthiness of each other as well as state, evaluate and enforce trust relationships among them. The Trust Model proposed here is well suited for open distributed applications where the service provider and service requestor is not known to each other.

4.1 Proposed Procedure

1. Create a Domain Evaluation table (DET) and an Entity Transaction table (ETT).
2. Update record in ETT of the entities that are requested to process a service request.
3. Update the feedback score in Domain Evaluation Table.

4. Check the Feedback score of the domains in DET before any transaction.

4.2 Calculating Trust values

Let us consider five different domains such as A, B, C, D and E to calculate the transactions and the rating of each entity in these domains for establishing trust in an open and dynamic environment where the possibility of interacting and executing an application on an unknown node i.e. Indirect trust likely increases.

There can be two tables designed for evaluating the credibility of a domain and entity in a Grid. The first table ETT maintains record and feedback score of each transaction of an entity in a domain with entities of other domains in a Grid.

Let us consider, Domain A

A={A1, A2, A3} be a set of values from A1 to A3, B={B1, B2}, C={C1, C2}, D={D1}, E={E1}.

In figure 2, the circle represents the domains having various entities, which are resources for processing service requests. The arrows show that the score will be calculated for both service provider as well as service requestor. We have assumed three kinds of TR in this Model i.e Direct, Indirect and Recommended Trust.

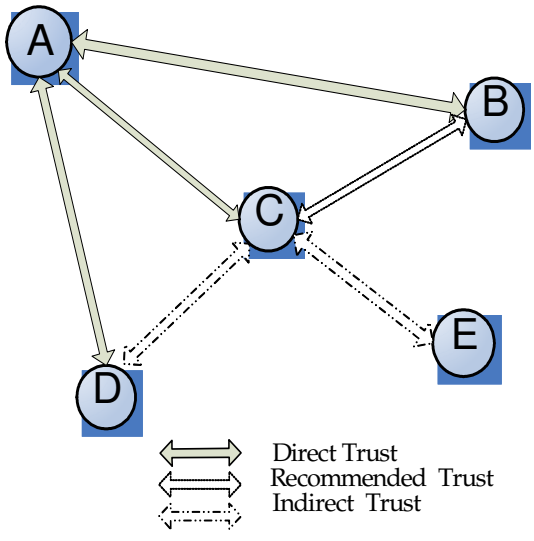

Figure 2. Directional Domains in a Grid

An Entity Transaction Table can be stored at the domain end where individual records of transaction with other entities shall be stored. An ETT can be designed considering the following attributes which is to be maintained at each domain:

i) Service Requestor (SR)
ii) Service Provider (SP)
iii) Number of transactions (N_T)
iv) Feedback Score (Fs)
v) Trust Relationship (TR)
vi) Total Entity Value (TEL)

Table 1: Entity Evaluation table

SR	SP	N_T	Fs		TEL		TR
			SR	SP	SR	SP	
A1	B1	1	1	1	1	1	0
B1	C2	1	0.5	0.5	0.5	0.5	0.5
C1	A1	1	1	1	1	1	0
A1	C2	1	0.5	0.5	0.5	0.5	0
C2	D1	1	0.5	0.5	0.5	0.5	1
A1	B1	1	1	1	2	2	0

The table presented here is for single transaction, between various domains under some Trusted third party which may be added further to calculate Feedback Score of each entity (for example A1, A2) in a domain A based on the transaction. We can store ETT of our own transaction also, for future consultation.

Here, the Feedback Score can be calculated by giving 1 for a good service, 0.5 for an average service and 0 for a poor service and the score may be provided for both the Service Requestor and the Service Provider. The service is rated on the basis of trust and reliability only.

Likewise, the Feedback score for an entity such as A1 in Domain A can be calculated as

$Fs(e) = \sum Fs / \sum N_T$ .....(1)

Here Fs= feedback score and e= entity for which the score is calculated. Further, the feedback score can be calculated on the basis of various Trust Relationships. For e.g. For Direct Trust, we have assumed 0 as the value, for Indirect Trust, 1 as the value and for recommended Trust 0.5 is assumed. When the entities are transacting for second time, the TR value will be 0 as the trust will be evaluated as Direct trust after one transaction. The rating R will be a composite of the Feedback score for the transaction and the TR.

Considering the malicious intent of some entities who would try to increase the rating of an entity by giving more score for the services provided, the overall score will reduced as the number of transaction will increase, by calculating the score on the basis of Equation 1.

The rating R of an entity such as A1 can be calculated as

$R(e)= Fs(e)+TR$ ……(2)

Table 2. Domain Evaluation Table

S. No	Domain Name	N_T	R	DT
1	A	5	5	B, C, D
2	B	10	6	A, C
3	C	5	8	A, D, B, E
4	D	8	8	A, C
5	E	6	10	C

The table can be referred with Figure 2, where there are different trust relationships between various domains consisting of various entities. In this table, the values of R and N_T are assumed. The rating factor R here is responsible for the trustworthiness of the domain in the open market. This DET can be considered before transacting with the domain. In the columns DT, which stands for domains transacted with, can be considered to take recommendation for service if the service requestor knows any of the domain.

4.3 Evaluating Trust

An example given here explains how to update the value of domain evaluation table. Assume that there are two domains A and B, entity A1 belonging to domain A wants to transact with entity B1 belonging to domain B. Let us suppose, domain evaluation table has the following initial values for (A, 5) and (B, 10) which is calculated after adding Feedback score of all entities of domain A and B respectively. After the transaction, domain A gives a score 1 to domain B for the services of entity B1, and updates its domain evaluation table value using the rating. At the same time domain B sends its rating 0.5 to domain A for its services of entity A1. The Domain Evaluation Table add the values to respective domains and updated values may be (A, 5.5) and (B, 11).

It can be concluded from the above example that the trustworthiness of domain is associated with the behaviors of entities belonging to it. If the entities' behavior is secure, the domain will have a higher trustworthiness; otherwise, the entities malicious behavior will reduce its trustworthiness.

4.4 Trust Decay Function

Trust decays with time and the entities may form alliances and they may trust their allies and business partners more than others. The TR may be considered as indirect trust i.e 0 for a period of time lapsed after the trust variable t_v decays after a period of time, where the relationship should be formed again between transacting entities or domains. The trust variable

t_v= Sum of Trust score between two entities……(3)

In this function, Time is inversely proportional to decay variable. As the time of transactions between two nodes increases the trust factor decreases with a 10%(assumed), which finally decays. This Function will be further explored for our Trust Model where issues such as by what factor the variable should decay so that the

relationship is to be considered as indirect for a new transaction where the transaction has already taken place, earlier.

5. Conclusion and Future Work

In this paper, a solution to evaluate trustworthiness of a domain is proposed while considering that the domains update their experience with other domains by assigning a feedback score to the transacting entity (service requestor/service provider). The solution is effective for open environments where the market players are dynamic. The trust relationship is considered for open distributed environments where service requestors and providers are not known to each other. The future work will conclude in several directions. The model will be expanded further while considering other factors responsible for determining trust in such environments such as trust decay factor and then assigning trust weights to the paths and accessing the recommended path. Secondly, the model is to be tested for real work environment. Thirdly, the decay factor is to be calculated for determining trust in real time work environment. The factors such as authentication and authorization are to be explored further for this model, for which again weight can be assigned on behavior trust.

Future Scope

In this Proposed Analysis chart, a Decay Function is shown where Trust variable decays finally to form trust again. We intend to develop the trust model considering the trust decay factor t_v which decays on the lapse of time of transaction between two entities. As the chart depicts, when there is no transaction between entities for a period, the trust factor decays completely enforcing re-establishment of trust between entities.

References

[1] I Foster, C. Kesselman, S Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations", International Journal of High Performance Computing Applications (2001).

[2] K. Konrad, G. Fuchs, and J. Bathel, "Trust and Electronic Commerce - More than a Technical Problem," The 18th Symp. Reliable Distributed Systems, 1999, Lausanne, Switzerland.

[3] D. Povey, "Trust Management," 1999, http://security.dstc.edu.,au/presentations/trust/.

[4] "Building a Foundation of Trust in the PC," 2000, The Trusted Computing Platform Alliance, http://www.trustedpc.org .

[5] N. M. Frank and L. Peters, "Building Trust: the Importance of Both Task and Social Precursors," Int'l. Conf. Engineering and Technology Management: Pioneering New Technologies - Management Issues and Challenges in the Third Millennium, IEEE Communications Surveys , Fourth Quarter 20001998, http://ieeexplore.ieee.org/iel4/5884/15675/00727781.pdf.

[6] Diego Gambetta, "Trust: Making and Breaking Cooperative Relations", chapter Can We Trust Trust?, pages 213–237. Department of Sociology, University of Oxford, 1988. http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf.

[7] http://ebaystrategies.blogs.com/ebay_strategies/2006/03/google_and_onli.html.

[8] Anirban Chakrabarti, "Grid Computing Security", ISBN 978-3-540-44492-3 Springer, Berlin Heidelberg, New York.

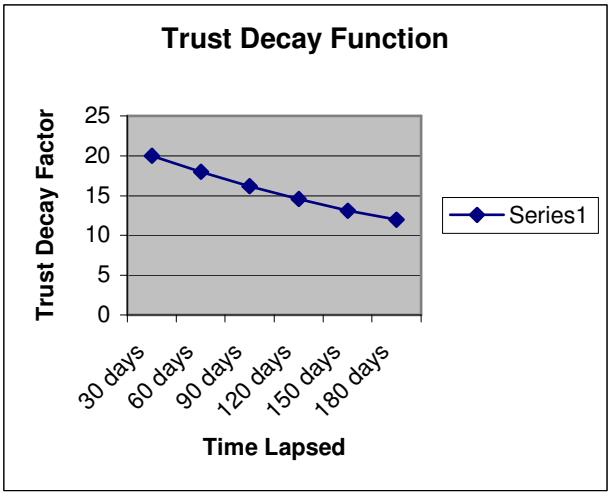

Figure 3. Time versus Decay Variable t_v