International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:4, No:12, 2010

Secure Resource Selection in Computational Grid Based on Quantitative Execution Trust

G.Kavitha, V.Sankaranarayanan

***Abstract*—**Grid computing provides a virtual framework for controlled sharing of resources across institutional boundaries. Recently, trust has been recognised as an important factor for selection of optimal resources in a grid. We introduce a new method that provides a quantitative trust value, based on the past interactions and present environment characteristics. This quantitative trust value is used to select a suitable resource for a job and eliminates run time failures arising from incompatible user-resource pairs. The proposed work will act as a tool to calculate the trust values of the various components of the grid and there by improves the success rate of the jobs submitted to the resource on the grid. The access to a resource not only depend on the identity and behaviour of the resource but also upon its context of transaction, time of transaction, connectivity bandwidth, availability of the resource and load on the resource. The quality of the recommender is also evaluated based on the accuracy of the feedback provided about a resource. The jobs are submitted for execution to the selected resource after finding the overall trust value of the resource. The overall trust value is computed with respect to the subjective and objective parameters.

***Keywords*—**access control, feedback**,** grid computing, reputation, security, trust, trust parameter.

I. Introduction

GRID Computing [1] [2] allows computing, storage and other resources that are geographically distributed and belong to different administrative domains to participate in a virtual organisation (VO). Resources are virtualised so that members of the VO can execute their application on coordinated resources obtained by specifying the requirements, rather than specifying the individual resource to be used. The context of grid computing introduces its own set of security challenges as the users and resource providers come from mutually distrusted administrative domains and either of the participants can behave maliciously. These malicious attacks can generally take two forms 1) user program may contain malicious code which could harm the resource provider node 2)shared grid resource node may be malicious or compromised to harm the users job running on the grid platform [3].

Security has been a central issue in grid computing and has been regarded as the most significant challenge for grid computing. Security of grid has been focussed on authentication, authorisation, resource protection and secured communication. Most of the existing trust models are designed to protect the resource provider nodes only. Security of the grid users are also equally important but not addressed effectively. We propose a novel trust model to calculate the quantitative value of execution trust. Execution trust is the belief that a resource provider node will faithfully execute a user code and complete the job request. The execution trust achieves a high level of security for the user.

To measure the level of trust, we define two metrics, quantitative trust and qualitative trust. The quantitative trust value is calculated by combining the subjective trust and objective trust. The qualitative trust value is obtained as the satisfaction value given by the user after the completion of the job request. The goal of the work is to provide a trust model for the virtual communities that assist the users in identifying trustworthy resources to execute their jobs in grid environment. The trust model is based on the existing computational environment of the grid infrastructure. Also it is simple to understand so that it is intuitive and usable. We believe that the implementation of the trust model in a VO would definitely help to automate the user side security decisions in a grid environment.

The rest of the paper is organised as follows. Related work is briefly discussed in section 2. Section 3 defines the notions of trust, reputation and its characteristics. The proposed trust model for grid systems is presented in section 4. The simulation and results are discussed in section 5. Finally, conclusion is presented in section 6.

II. Related Work

Trust has been addressed at different levels by many researchers. Several trust models that are related to our work has been proposed for integration into grid computing systems. In [4] the behaviour trust model is proposed where the trust is computed as a combination of direct experiences and reputation. This model accommodates inheritance for trust and the computed trust value decays with respect to time. Trust based on only subjective knowledge does not perform well in a dynamic grid environment. The execution environment parameters like communication speed, work load greatly influence the success of jobs in grids which are not addressed in this paper.

An adaptive trust model based on reputation is presented in [8]. The trust model quantifies and compares the trustworthiness of peers based on a transaction feedback system. The authors address about peer to peer trust and misbehaving of peers. Here, trust is evaluated based on community reputations. But the trust computed solely on

G.Kavitha is with the B.S.A. Crescent Engineering College, Chennai, India.(phone:+91-044-22741577;fax:+91-044-42114282; e-mail:gkavitha.78@gmail.com)
Dr.V.Sankaranarayanan is with B.S.A. Crescent Engineering College, Chennai, India. (e-mail:sankarammu@yahoo.com)

recommendation mechanism is inaccurate and inefficient. In this paper the proposed method considers transaction context factor to select the resources but has not explored any mechanism to identify false feedbacks and honesty of the recommender.

A vector model for developing trust has been proposed in [6]. The trust rating between a trustor and a trustee is determined by the component values of experience, knowledge and recommendation. The normalised trust rating is given by the normalisation of the trust policy vector and simple trust relationships. The model incorporates trust dynamics, change of trust and distrust with time. It also proposes a mathematical model to evaluate experience, knowledge and recommendation. The methods to manage and manipulate the trust relationships are not presented. The validity of this trust model in heterogeneous grids has not been experimented.

Trust in virtual communities is discussed in [5]. The reputation based trust defined is agent and context specific. The grade of outcome of an experience is given in terms of ordered set representing 'very good', 'good', 'bad', 'very bad'. The proposed model has uncertainty in the information if more than one value is returned as experience and therefore it is not robust to malicious encounters and risky environments.

In [7], a trust aware access control in service oriented grids is presented. Trust is applied to access control and the trust value is modified according to the increasing times of service. Trust is also used to determine the authorization of grid users and is a basic parameter of access control policy decision. Trust is computed with reference to the number of times a transaction is successful between a trustor and a trustee. This model has not considered time of past interactions. As trust changes over time, computing trust values based on time helps to find a more appropriate resource in the dynamic grid environment.

Trust as applied to scheduling in commercial grids is implemented in [9]. The proposed trust model evaluates trust based on affordability, success rate and bandwidth. User jobs are submitted to resources with higher trust values. The feedback values specified doesn't consider the credibility of the recommender. Hence, there is a chance that a malicious resource can be chosen by the trust model which could harm the user's job running on the Grid platform.

In the models discussed above, there exists a method to evaluate trust based on only subjective knowledge. Very little work is done about access control in grid systems based on trust value. In the existing methods, jobs submitted to a highly trusted resource may have a long response time as the resource is heavily loaded and the jobs may suffer long waiting time in the queue. But in our proposed method, trust value is calculated based on availability, load, success rate, credibility of the recommender and also the past performance about the resource. The resource thus selected not only satisfies the trust requirement for the job but also executes the job successfully compared with the previous stated trust models.

III. TRUST AND REPUTATION

A. Definition of Trust and Reputation

The notion of trust is a complex subject relating to a firm belief in attributes such as reliability, honesty, and competence of the trusted entity. The definition of trust as given by Farag azeedin [4] is as follows:

Trust is the firm belief in the competence of an entity to act as expected such that this firm belief is not a fixed value associated with the entity but rather it is subject to the entity's behaviour and applies only within a specific context at a given time.

When making trust based decisions, entities can rely on others for information pertaining to a specific entity. The behaviour of an entity can be analysed from other participants' information about that entity. The definition of reputation as given by [4] is as follows:

The reputation of an entity is an expectation of its behaviour based on other entity's observation or information about the entity's past behaviour within a specific context at a given time.

B. Characteristics of Trust

1) *Trust is dynamic and non-monotonic*: The trust level about an entity changes over time with respect to good and bad behaviour of the entity during a transaction.
2) *Trust is asymmetric:* The level that entity A trust entity B is not the same as entity B trusts entity A.
3) *Trust is subjective:* Different entities may have different perceptions of the same entity's trustworthiness.
4) *Trust is context dependent:* An entity that is trusted for one category of operation may not be the same for the other category.

C. Trust and Security

In general, the purpose of security mechanism is to provide protection against malicious parties. Traditional security mechanisms typically protect the resources from malicious users by restricting access to only authorised users. However, in many situations within distributed applications one has to protect oneself from those who offer resources. For instance, a resource that provides information can act deceitfully by providing false or misleading information. The traditional mechanisms are unable to protect the users against these types of threats. Trust can be used to overcome such threats in a distributed grid system. Therefore, trust can be helpful to provide entry level security as authentication and access control. Trust is specified in terms of relation between a

trustor, trustee and the context in which the target entity is trusted.

IV. THE PROPOSED TRUST MODEL

The proposed trust model is concerned with evaluating every request submitted by the user to access a resource and determine the appropriate resource to which the request should be mapped to. The trust about an entity is evaluated as the quantitative value of trust based on the past experiences and present environment conditions. The measurable trust value is vital for selection of appropriate resources in a dynamic grid environment, to greatly reduce the runtime failure of jobs.

The grid environment is composed as three tier architecture, where the physical resources exist in the lower level, the user application at the higher level and the trust layer as the middle layer. The trust model (TM) contains two major components, one for the evaluation of trust and the other for updating the trust value. Trust is evaluated as a combination of subjective trust (SBT) and objective trust (OBT). Weights assigned to subjective trust and objective trust are based on the nature of the user job request. In Trust update, the Direct Trust Table (DTT) of the participating entities and the Overall Trust Table (OTT) are updated.

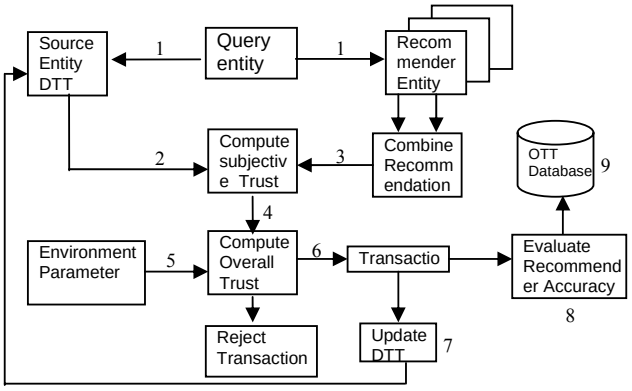

Fig. 1 Components of Trust Model

The various components of the trust model are shown in Fig.1. This model can be integrated into the trust layer and can protect the user from the malicious service providers. The client places the request for resources to the trust model. The set of resources that satisfy the client's requirements are identified and retrieved from the database. For the resources retrieved, the trust evaluation process is as follows:

The trust model sends a query to all the neighbouring entities including the user to provide trust value about a resource based on its previous transactions in a given context (1). Accordingly the entities will refer to their Direct Trust Table (DTT) and if there was a previous history of interaction, it responds to the query by giving the trust value along with the time of past interaction (2). The recommended values are aggregated to filter multiple feedbacks from the same entity (3). The weights are assigned to direct and recommended trust values and combined to a single value as Subjective Trust (4). The current execution environment of the resource is identified and the set of objective values are evaluated (5). The subjective value and the objective value are combined to give the overall trust value about a resource. If the overall trust value is greater than or equal to the required trust then the job is assigned to the resource for execution (6).

After completion of the transaction the DTT of the entities are updated accordingly (7). The deviation from the recommended value to the observed value is found and the accuracy of the recommender is evaluated (8). The trust update is done after completion of 'n' number of transactions by a resource. The overall database in the VO is updated (9).

In the proposed work, there are various parameters that contribute to the trust evaluation process including direct trust, recommended trust, number of recommenders, resource workload and network bandwidth. Therefore, fuzzy sets can be used to combine the values of the stated parameters and trust values are assigned by quantifying the fuzzy values. The Overall Trust value of a resource varies between 0 and 1. Table I represents the quantified trust value assigned initially based on fuzzy values, which may vary over time, as used in the initial design of Trust Model.

TABLE I
TRUST VALUES AND THEIR MEANING

Trust Value	Meaning
0.8 – 1	Absolutely Trustworthy
0.6 - 0.8	Very Trustworthy
0.3 – 0.6	Trustworthy
0.1 – 0.3	Not Trustworthy
0.0 - 0.1	Absolutely Untrustworthy

A. Evaluating Direct Trust

When an entity A has directly involved in a transaction with entity B, the resulting trust value is termed as Direct trust (DT). The direct trust for a transaction is computed with respect to the context of transaction such as remote code execution, file transfer, data storage etc. and the size of the job that was completed. The direct trust value changes over a period of time. For example, the trust between entity A and B two years ago will not be the same now. Hence trust value changes over time. Trust rating is defined as the degree to which A trusts B and the value ranges between 0 and 1. The trust value between two entities A and B at a given time t_2 for a specific context c is evaluated as,

$$DT(A,B,t_2) = DT(A,B,t_1) * T \qquad (1)$$

where DT(A, B, t_1) is the direct trust value obtained at time t_1 and T is the time-dependant trust value given as an exponentiation function of (t_2 - t_1) and DT(A, B, t_1). The difference of current time of interaction t_2 and past time last

interacted t_1 is given as $(t_2 - t_1)$. The time-dependant trust value T of a trust relationship as given by [6],

$$T = e^{-DT(A,B,t_1)(t_2-t_1)} \quad (2)$$

The value of equation (2) conveys the change in the value of trust over a period of time.

The time difference $(t_2 - t_1)$ is computed in real time and for simulation purposes, the values of $(t_2 - t_1)$ are expressed as number of days and a relative time factor is assigned as given in Table II.

TABLE II
TIME DIFFERENCE AND ITS FACTOR

Time Difference (days)	Time factor
0-180	0.5
181-365	1
366-730	2
731-1460	3

B. Evaluating Reputation Trust

In a distributed environment, entities may form alliances and may trust them to provide recommendations about other entity or a resource. When an entity A wants to have a transaction with entity B, for a specific context c at a given time t, A can rely on the recommendation from other collaborative entities to compute B's trustworthiness pertaining to c. A recommender entity may provide multiple recommendations about entity B to improve the reputation of B. To avoid this, average of the recommendations are done. The reputation trust rating is a value that varies between 0 and 1. Let us assume that A receives a recommendation from Z. Entity A cannot evaluate the truthfulness of Z's recommendation until A has directly interacted with B. After completion of a transaction, A updates the credibility for its set of recommenders based on the deviation of the observed value and recommended value. To average the recommendations, the credibility of each recommender is inferred from the overall trust table. If the recommender is new to that VO, then an initial credibility level of 0.5 is assigned. The Reputation trust value, RT (Z_i, B, t2) is computed as,

$$RT(Z_i, B, t_2) = \frac{\sum_{i=1}^{n} DT(Z_i, B, t_1) * T * C(i)}{n} \quad (3)$$

where, Z ∈ n, Z≠B and n is the number of recommenders in the list. The time-dependant trust value T obtained from equation (2) is utilized in equation (3).

From the direct trust and reputation trust values, the Subjective Trust (SBT) can be computed as,

$$SBT(A, B, c, t_2) = w1 * DT(A, B, t_2) + w2 * RT(Z_i, B, t_2) \quad (4)$$

The weights for direct and reputation trust are assigned according to the type of user application or they can be weighed equally as w1=w2=0.5.

C. Evaluating Objective Trust

The idea of selecting a suitable resource for a user application is to reduce the failure rate of user's jobs. Considering only past experiences do not provide an effective way for resource selection in a grid environment. The environmental execution parameters at the time of job submission have to be considered equally as subjective knowledge about a resource. The execution parameters are the network bandwidth to which the resource is connected, the load on the resource at the time of job request and the availability of the resource.

The network communication speed between a user and a resource are defined in terms of data transfer rate. Every resource is connected to the grid by a communication link. The network bandwidth varies from one link to another. We consider the bandwidth criterion to reduce the delay and to maximize the Grid utilization. The actual bandwidth of all the links in the grid are scaled down to reduce the simulation volume and to match the study purposes. The resulting bandwidth of low capacity link is less than 1 Mbps, medium capacity link is between 1 and 2 Mbps and high capacity link is more than 2Mbps.The links are assumed to be symmetric where the upload and download speed are at equivalent transfer rate.

The workload is estimated based on the observed load conditions. The Load represents the number of active jobs currently in execution on the resource. Assigning jobs to a resource with light load minimizes the response time of the job. Many times a resource with a very good trust rating may be heavily loaded and hence cannot provide a satisfactory service.

The Objective Trust value (OBT), about a resource can be calculated as,

$$OBT = w3 * BW_R + w4 * (Load_R * AVL_R) \quad (5)$$

Where, BW_R represents the connectivity bandwidth of the resource, $Load_R$ represents the current load on the resource and AVL_R, the availability of the resource on the grid. The weights w3and w4 are assigned and can be changed according to the type of user application As the dimensions of bandwidth, load and availability are not the same, we convert the obtained real time values into its appropriate factor. For convenience, it is assumed that a maximum of 2 Mbps bandwidth on the grid for simulation purposes. The connectivity bandwidth of the resource and its appropriate values are expressed as,

TABLE III
BANDWIDTH AND ITS VALUE

Bandwidth (Mbps)	Factor Value
0- 1	0.3
1- 2	0.6
> 2	0.9

Link bandwidths are assumed to be near 2.0 Mbps. In real situations if correct bandwidths are known, accordingly values can be assigned. We assign a load factor that represents the percentage of load on the resource. The assigned load factor for the load on the selected resource is given as,

TABLE IV
PERCENTAGE OF LOAD AND ITS LOAD

Percentage of Load	Load factor
0 – 5 %	1.0
5% - 20%	0.8
20% - 40%	0.6
40% - 60%	0.4
60% - 80%	0.2
>80%	0

The assumption is, for simulation purposes, the values are assigned. But in real time, if the maximum load that is possible is known, the percentage use and the corresponding load factor can be calculated.

Both the objective trust and the subjective trust weigh equally for selection of a resource in a grid environment. We arrive at a quantitative trust value about a resource by considering the subjective and objective nature of a resource and weigh them equally. The overall trust value (OTV), about a resource is computed as,

$$OTV = \alpha * SBT + \beta * OBT \quad (6)$$

Where, α=β=0.5 and OTV varies between 0 and 1.

D. Evaluating Credibility Of Recommenders

The exaggerated feedback of recommenders can mislead in choosing optimal resources for a user's job. The false feedbacks should be identified and the recommender that provided a good trust rating for a malicious service provider is found and accordingly the credibility of the recommender is updated in the Overall Trust Table (OTT). The credibility C(i), for i^{th} recommender is found as,

$$C(i) = e^{-|D|} \quad (7)$$

Where, D is the deviation calculated as the difference between the observed value and the recommended value. Hence, Credibility is a function of deviation found after completion of a user job. For each of the recommender in the given set, assign the respective credibility after job completion. The user returns the satisfaction value based on the response time for the job submitted (RT_J), status of job completion (ST_J), and the size of the job submitted to the resource (JS_J). The user satisfaction is evaluated from the actual experiences of the user involved in the transaction with the selected resource. The user satisfaction about a resource R, (US_R) is calculated as,

$$US_R = RT_J * ST_J * JS_J \quad (8)$$

E. Trust Update

The Overall Trust Table is updated in the database after completion of every 'n' transaction of the resource by various users. Frequent updating in the overall database leads to heavy network traffic in the environment. Hence updating OTT is done after 'n' transactions. The results of every completed job are sent to the client and a feedback is submitted to the trust model(TM) about the transaction.

The Direct Trust Table (DTT) of the participating entities is updated after every transaction. The Trust Model aggregates the feedbacks from various clients and modifies recommender credibility in Reputation Trust Table (RTT). The following metrics are evaluated to assess the performance of the resource in the grid environment.

a) Success Rate: The success rate of a resource, SR_R is defined as the ratio of the number of jobs completed successfully to the total number of jobs submitted to the resource.

$$SR_R = \frac{\text{Total Number of completed jobs}}{\text{Total number of submitted jobs}}$$

b) Availability: Availability of a resource, AVL_R is defined as the ratio of the number of times the resource available to the user to the total number of times the resource was requested.

$$AVL_R = \frac{\text{Total number of times resource available}}{\text{Total number of attempts to access resource}}$$

The performance metrics are greatly improved in our work as the resources are selected based on quantitative trust values.

V. SIMULATION AND RESULTS

In this section, the performance of the proposed algorithm is analyzed. The simulation was based on the grid simulation toolkit GridSim Toolkit 4.0 which allows modeling and simulation of entities in grid computing systems. In this simulation environment the trust model has been incorporated as the middle layer component for calculation of trust about resources. The heterogeneous Grid environment is built by using various resource specifications. The resources differ in their operating system type, CPU speed, RAM memory, Baud rate. In GridSim, application jobs are modeled as Gridlet

objects that contains all information related to the job and execution management.

We have simulated 5 resources with different characteristics such as number of processing elements (PE) in a machine, MIPS rating of a processing element, type of operating system and cost of using the machine. The simulation is done for different user's jobs and the overall trust value of resources is found. The simulation set up is shown in Table 5. The experimental configurations are to bring up the performance of the trust evaluation algorithm.

TABLE V
SIMULATION SETUP

Resource ID	No.Of PE	Capacity of PE (MIPS)	BW (Mbps)	Trust Value
R1	10	200	2	0.7
R2	12	200	1.5	0.6
R3	5	150	1	0.5
R4	10	150	1.5	0.8
R5	10	200	1	0.5

According to the simulation set up, a resource R1 is assigned a high trust value (0.7) as it has a good record of successful completion of jobs submitted to it, it has been connected to high speed link and is almost available at requested times. We analyze the performance of the trust evaluation algorithm based on the load conditions, availability conditions and success rate of the jobs submitted to the resources. We performed simulation for computational intensive jobs only. Hence the resources were selected only upon the context of transaction.

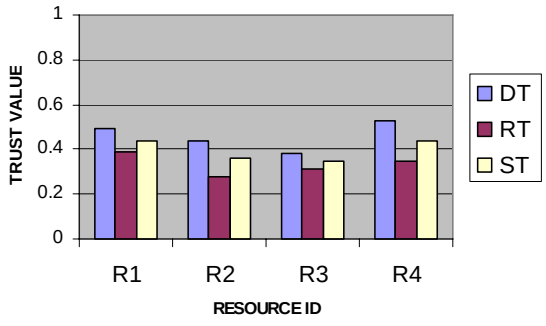

Fig. 2. Subjective Trust of Resources

The trust value about a resource is calculated by combining the subjective trust and objective trust values. The subjective trust value is computed by combining Direct Trust (DT) and Reputation Trust (RT). Figure2 shows the subjective trust values of R1, R2, R3 and R4. The context of interaction of the above resources is "Computation Jobs". But the resource R5 was assigned for "Data storage Jobs" and was not selected for job submission. The maximum number of Recommenders considered was 3.

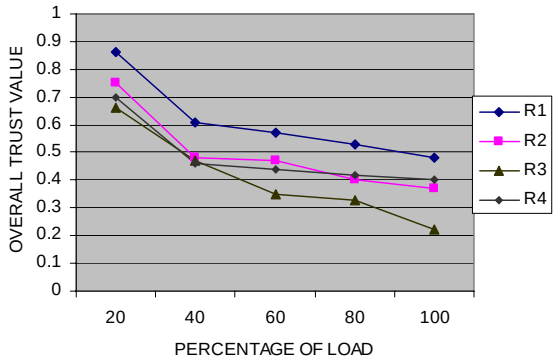

Fig. 3. Overall Trust Value of Resources

The overall trust value of resources under various load conditions in a simulated grid environment are depicted in Figure3. This trust value is compared with the required trust level of the job and if satisfied the user is granted access to the specified resource. Figure 3 shows that the resource R1 has a high trust value compared to the other resources in the grid even under heavy load conditions.

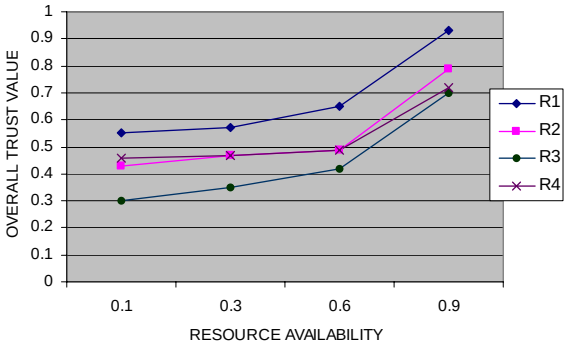

Fig. 4. Availability of Resources

The Overall trust value of resources under different availability conditions are shown in Figure 4. The resources perform well if it has a high availability. But even in case of low availability the resource R1 gives a comparatively high trust value. Hence R1 is selected as it satisfies the user's job requirement and it also outperforms other resources under heavy load conditions subject to minimum availability. The subjective and objective trust values are computed for R1, and the job is submitted to R1. On successful completion of the job, the results are returned to the user and trust values of the

entities involved in the transaction are also updated accordingly.

Selection of such suitable resources avoids run time failures and hence improves the success rate of jobs submitted to the resource. Figure.5 shows the success rate of jobs submitted to different resources on the grid. We have simulated the performance of resources by submitting 10 different users jobs to each resource. From the output of simulations it is implicit that the highly trusted resources are R1 and R4 because they complete the assigned tasks submitted to them even under different environment conditions.

The success rate is high as the jobs are submitted only to highly trusted resources. The failure rate of jobs is due to two reasons. First, the resources that are available in the grid do not satisfy the required trust level of the job and the other is there are no available resources that match the users requirements. Therefore there may also be cases of job failure in the trusted grid environment but, it is under rare conditions. Simulation is performed only with 5 resources. Hence when there is increase in number of jobs submitted, the success rate decreases.

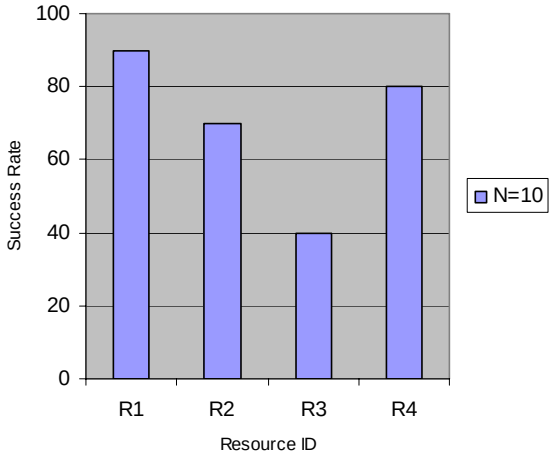

Fig. 5. Success Rate of Jobs

VI. Conclusions

The emergence and rapid growth of distributed service infrastructures in recent years make trust an important issue for resource selection and code protection. In this paper, we have presented a trust model and a trust evaluation procedure to find a highly trusted resource. Trust model is a secure model based on behavior trust and current resource's capability. The value of trust evolved is both subjective and objective in nature and it makes advantage over the other models which considers only the subjective nature. Hence selection of resources in grid is based on user's past behavior and resource provider's system features. The proposed secure resource selection method in computational grids greatly improves the success rate of the jobs submitted to the dynamic grid environment. The results show that the failure rates of jobs are greatly minimized by implementing our method of resource selection. We have used the trust model to find trusted resources in a virtual organization. The future direction of the work is to build trust among multiple virtual organizations that spans over various domains.

References

[1] Foster. I, Kesselman.C and Tuecke.S, "The anatomy of the grid: Enabling scalable virtual organizations", International Journal of High performance computing Applications,V.15 n.3,August 2001, pp. 200-222.

[2] Foster.I , Kesselman.C , Nick.J, Tuecke.S, "The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration", Open Grid Service Infrastructure WG,Global Grid Forum, June 22, 2002,pp 37-46.

[3] Ching Lin,Vijay Varadharajan, Yan Wang, Vineet Pruthi, "Enhancing Grid security with trust management", Proc.Of IEEE International Conference on Services Computing ,2004, pp 303-310.

[4] Farag.A.Azzedin and Maheswaran.M , "Evolving and managing trust in grid computing systems", Proceedings of the 2002 IEEE Canadian Conference on Electrical Computer Engineering, 2002, pp 1424-1429.

[5] Abdul-Rahman.A and Hailes.S, Supporting trust in virtual communities," *Hawaii Int'l Conference on System Sciences*, Jan. 2000, pg.6007.

[6] Indrajit Ray and Sudip Chakraborty, "A Vector model of trust for developing trustworthy systems",Proc.Of 9th European Symposium on Research in Computer Soceity, 2004, pp 260-275.

[7] Xudong Ni , Junzhou Luo, " A Trust aware access control in service-oriented grid environment", International Conference On Grid and Cooperative Computing ,2007, pp 417-422.

[8] Li Xiong, Ling Liu "A Reputation based trust model for peer-to-peer e-commerce communities",Proc.Of the IEEEconference on ecommerce, June 2003.

[9] Thamaraiselvi.S, Balakrishnan.P, Kumar.R, Rajendar.K, "Trust based Grid scheduling algorithm for commercial grids" ,International Conference on Computational Intelligence and Multimedia Applications,2007, pp 545-558.

[10] Yao Wang, Julita Vassileva ," A Review on Trust and Reputation for Web Service Selection" , 27th International Conference on Distributed Computing Systems Workshops ,2007, pg.25.

[11] Marty Humphrey , Mary R..Thompson ," Security Implications Of Typical Grid Computing Usage Scenarios ", Proc. Of 10th IEEE International Symposium on High Performance Distributed Computing, 2001, pg.0095.

[12] Michael Brinklov ,Robin Sharp, " Incremental Trust in Grid Computing "7th IEEE International Symposium on Cluster Computing and the Grid,2007, pp 135-144.

[13] Vijayakumar.V , Wahida Banu.R.S.D , " Security for Resource Selection in Grid Computing Based on Trust and Reputation Responsiveness", International Journal of Computer Science and Network Security, November 2008 ,pp 107-115.

[14] Isaac Agudo, Carmen Fernandez, Javier Lopez," An Evolutionary Trust and Distrust Model " , Electronic notes in Theoretical Computer Science,2009, pp 3-12.

[15] Bendahmane. A, Essaidi.M , A. El Moussaoui, Younus.A , "Grid Computing Security Mechanisms: State-Of-The-Art" , ICMCS 2009, pp 4-10.

[16] Ryutov.T, Neumann.C ,Zhou.L , " Adaptive Trust Negotiation and Access Control For Grids" , International Conference on Grid Computing ,2005, pp 55-62.

[17] Muhammad Hanif Durad, Yuanda Cao, "A Vision for the Trust Managed Grid," , Sixth IEEE International Symposium on Cluster Computing and the Grid Workshops (CCGRIDW'06), 2006, pg.34.

[18] Papalilo E. and Freisleben B., "Towards a Flexible Trust Model for Grid Environments" GSEM 2004, LNCS 3270 Springer- Verlag Berlin Heidelberg 2004, pp. 94–106.

[19] Runfang Zhou and Kai Hwang, "Trust Overlay Networks for Global ReputationAggregation in P2P Grid Computing", IEEE International Parallel and Distributed Processing Symposium, IPDPS ,2006,pg.10.