Security for Resource Selection in Grid Computing Based On Trust and Reputation Responsiveness

V.Vijayakumar
PhD Research Scholar, Faculty of Information and Communication Engineering
Anna University, Chennai, Tamilnadu, India

R.S.D.Wahida Banu
PhD Research Supervisor, Faculty of Information and Communication Engineering,
Anna University, Chennai, Tamilnadu, India

Summary
In providing the infrastructure for the accomplishment of general purpose computational grids the main concern is security. Still, by properly authenticating users and hosts and in the interactions between them, most grid implementations focus their safety concerns. The effective and competent exploitation of grid computing services needs sophisticated and secured resource management systems. The wide range of selection and the high degree of strangeness leads to the problem in secured selection of grid. Without the assurance of a higher degree of confidence relationship, efficient resource allocation and utilization can not be attained. In recent times, with larger applications in e-commerce and on-line communities, reputation mechanisms have become one of the most important techniques underpinning the distributed application and system safety. We have proposed a new approach in this paper, which intends to offer trust and reputation aware security for resource selection in grid computing. The Trust Factor (TF) value of each entity is determined from the self-protection capability and reputation weightage of that particular entity; moreover the jobs are preferably assigned to the entities with higher TF values. The proposed approach has been found to cope with the ascending number of user jobs and grid entities. The experimental results demonstrate that the determination of the grid entities intended towards the secured execution of the job by the proposed approach is efficient and satisfactory.

Key words:
Grid Computing, Computational Grids, Security, Resource Management, Trust, Self-Protection Capability, Reputation

1. Introduction

Increased network bandwidth, more powerful computers, and the acceptance of the Internet have motivated the constant requirement for latest and improved ways to compute. In the late 1990's, a complex computation environment, Grid computing, had come out. The aspiration to share processing resources between many organizations to resolve large scale problems has provoked computational grids [1, 2]. In the recent years, grid computing is rising as a viable paradigm to convince the continuous growth of computation power requirement, which frequently can not be fulfilled exploiting the internal resources of a single organization [3]. Grid computing [4] is a collection of autonomous and distributed resources available over virtual organizations, and collaborate works with effective, efficient, and reliable way. The term "Grid" refers to systems and applications that integrate and manage resources and services distributed across multiple control domains [5].The upcoming computational Grids offer a new platform for implementing large-scale resource intensive applications on a number of heterogeneous computing resources across political and administrative domains.

Grid applications utilize high performance distributed resources similar to high performance systems, networks, databases, etc. These have enabled via grid middleware for instance Globus [12], Gridbus [15]. The resources in grid are dynamic. The resources of grid computing vary in level from a small number of large clusters (for example the TeraGrid [6]) to millions of PC-class machines (for example SETI@Home [7]). Developing a comprehensive set of mechanisms and policies for protecting the grid is most significant challenge for Grid computing questionably in many ways. At present, Grid security research and development turns around developing better solutions to take care of the following requirements: Authentication, Secure Communication, Effective Security Policies, Authorization, and Access Control.

Resources and security guarantee are the two fundamental requirements in Grid applications [8, 9]. Coordinated resource sharing and problem resolving in dynamic, multi-institutional virtual organizations are the actual and specific problems which underlies the grid concept [10]. Once infected shared grid resources through malicious codes planted by intruders possibly will spoil other applications running on the same Grid platform. The concerned sharing is not primarily file exchange but rather direct access to computers, software, data and other resources since it is required by a range of collaborative problem-solving and resource-brokering strategies emerging in industry, science and engineering [11]. The resource management in Grid systems is challenging due to: (a) geographical distribution of resources, (b) resource heterogeneity, (c) autonomously administered Grid domains having their own resource policies and practices,

Manuscript received November 5, 2008
Manuscript revised November 20, 2008

and (d) Grid domains using different access and cost models [14].

At present, security is put up into grid toolkits (e.g. the Globus toolkit [12]) used at the provider sites (parties that offer resources for use in the grid). The toolkit handles secure channels, authentication [13], unsupervised login, delegation, and resource usage [11]. These mechanisms generally do not concern themselves with protecting the grid user (the person or entity desires to utilize resources). Without verifying the justification of the trust, the user is compelled to trust the provider [16]. Users are able to submit jobs to remote resources and typically have no explicit control over the resources themselves. Therefore, mutually users and resources can be viewed as independent agents, having control of their own behavior. Since an individual cannot forecast the response of another to changing situations, this autonomy provides rise to inherent insecurity, [17]. The Grid service providers must guarantee the users with definite security, privacy protection, and dependable accessibility of all Grid-enabling platforms [9].

Most grid computing environments spotlight their security concerns in properly authenticating users and hosts and in the communications between them. To automatically and clearly ensure the fulfillment, the effective and efficient exploitation of Grid computing facilities requires advanced and secured resource management systems. This fulfillment is not only for functional requirements but for non-functional ones as well. The wide range of selection and the high degree of strangeness leads to the problem in secured selection of the resources in grid. Without the assurance of a higher degree of trust relationship, competent resource allocation and utilization can not be attained. In recent times, with larger applications in e-commerce and on-line communities, reputation mechanisms have become one of the most important techniques underpinning the distributed application and system safety for its better scalability and flexibility.

This is the enhanced version of our previous work with detailed analysis of the performance [31]. The most important target of this research is to develop a solution that could afford trust and reputation aware security for resource selection in Grid sites for scheduling large number of independent and indivisible jobs. The proposed approach aims the schedule of incoming jobs to available resource sites based on the Trust Factor value. The Trust Factor (TF) value of each resource site has estimated by its self-protection capability and reputation weightage acquired through the feedback from user community on its past behavior. The self-protection capability of a site includes its ability to detect intrusions, viruses, unauthorized access and secured file storage and job completing abilities. Reputation mechanisms offer a way for building trust through social control by using community based feedback about past experiences of entities. Our approach is meant to enforce security in Grids with security-assured resource allocation.

The remaining sections are organized as follows; Section 2 presents a brief review of related work. Section 3 confers an overview of Trust and Reputation. The proposed approach for secured resource selection for scheduling incoming jobs is discussed detailed in Section 4. Experimental results are given in Section 5 and conclusions are summarized up in Section 6.

2. Related Work

Our work is inspired by a number of previous works related to trust management and reputation based security enhancement for sustaining performance of grid computing. These related works are reviewed below.

Farag Azzedin and Muthucumaru Maheswaran [14] proposed a formal definition of both trust and reputation and discussed a model for incorporating trust into Grid systems. Rajkumar Buyya and Srikumar Venugopal [15] proposed an overview of an open source Grid toolkit, called Gridbus, whose architecture is fundamentally driven by the requirements of Grid economy. Gridbus technologies provide services for both computational and data grids that power the emerging eScience and eBusiness applications.

Ernesto Damiani et al. [24] proposed a self-regulating system for P2P network using robust reputation mechanism. In their system reputation sharing is realized through distributed polling algorithm. Chuang Liu et al. [26] proposed a general-purpose resource selection framework by defining a resource selection service for locating Grid resources that match application requirements and evaluated them based on specified performance model and mapping strategies, and returned a suitable collection of resources, if any are available.

Yao Wang and Julita Vassileva [22] proposed a bayesian network-based trust model and a method for building reputation based on recommendations in peer-to-peer networks. Sepandar D. Kamvar et al. [25] proposed a reputation management system, called EigenTrust, which can effectively reduce the number of downloads of inauthentic files in a P2P system. The reputation value of each peer is determined by the number of successful downloads and the “opinions” of other peers.

Shanshan Song and Kai Hwang [18] proposed a new fuzzy-logic trust model for securing Grid computing across multiple resources sites. They have developed a new Grid security scheme, called SARAH supported by encrypted channels among private networks. Justin R.D. Dyson et al. [17] described a trust framework model for Grid computing, which enables users to execute their jobs on reliable and efficient resources, thereby satisfying clients' quality-of-service (QoS) requirements.

Farag Azzedin and Muthucumaru Maheswaran [23] proposed a trust brokering system that operates in a peer-to-peer manner. They have developed a security-aware model between resource providers and the consumers that separates the concepts of accuracy and honesty. Shanshan Song et al. [27] proposed a new fuzzy-logic trust model for securing Grid resources. They have developed a SeGO scheduler for trusted Grid resource allocation.

Li Xiong and Ling Liu [28] proposed a reputation-based trust supporting framework, which includes a coherent adaptive trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system and a decentralized implementation of such a model over a structured P2P network.

Ian Foster [12] reviewed briefly the current status of Globus, focusing in particular on those aspects of the GT4 release that should be of interest to those wishing to work with the software. Chunqi Tian et al. [29] proposed ARTrust—an Attack Resistant Trust management model, a novel recommendation based trust model for P2P networks.

Baolin Ma et al. [30] proposed a trust model, which is used to compute and compare the trustworthiness of entities in the same autonomous and different domains. This model provides different methods to deal with the problems of users and related resources belonging to the same or different domains. Nadia Ranaldo and Eugenio Zimeo [3] proposed a framework for brokering of Grid resources, virtualized through web Services, which can be dynamically configured with respect to multiple syntactic and semantic description languages and related matching strategies.

Zhiguo Shi et al. [10] proposed a novel anonymous coordination authentication scenario which can provide efficient and reliable anonymous identity authentication and remote platform attestation for Grid computing systems. Lohr et al. [16] proposed an approach to enhance the Grid security using a combination of trusted computing and virtualization technologies.

3. Trust and Reputation

This section furnishes a short foreword regarding trust and reputation in the context of Grid Computing.

3.1 Trust

Trust is the foundation of both human society and cyberspace security. Trust is not a black and white substance. Frequently grey area exists in conveying the trustworthiness of a computer site [18]. Similar to human relationship, trust is expressed by a linguistics term rather numerically. Trust differs with respect to time and environment. The concept of trust is a multipart subject related to a firm belief in attributes for instance reliability, honesty and competence of the trusted entity. The definition of trust proposed by Farag Azzedin and Muthucumaru Maheswaran [14] 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 behavior and applies only within a specific context at a given time. The firm belief is a dynamic value and spans over a set of values ranging from very trustworthy to very untrustworthy. The trust factor has built on the basis of past experiences and has given for a specific context. The trust factor is specified within a given time since the trust level between two entities is not necessarily the same from today to a year ago.

3.2 Reputation

In recent times, with larger applications in e-commerce and on-line communities, reputation mechanisms have become one of the most important techniques underpinning the distributed application and system safety for its better scalability and flexibility. Reputation systems [19] provide a technique for building trust through social control without trusting third parties. Using community based feedback about past experiences of entities; reputation mechanisms provide a technique for building trust through social control. This helps in making suggestion and judgment on quality and consistency of the transactions [20]. The definition of reputation proposed by Farag Azzedin and Muthucumaru Maheswaran [14] is as follows: The reputation of an entity is an expectation of its behavior based on other entities' observations or information about the entity's past behavior at a given time.

4. Secured Resource Selection for Scheduling Jobs

This section explains our proposed approach for resource selection designed for safe scheduling of independent and individual jobs to grid sites. The scale of resources and the strangeness of entities cause difficulties in the process of resource selection. Since a high-efficient society cannot go with a high-trustworthy social relationship, efficient resource sharing cannot be attained in Grid without certain trust relationship core. Entities can depend on others for information pertaining to a particular entity while making trust based decisions. This can be achieved by the reputation mechanism. By considering the above conditions, we have proposed an approach by combining both trust and reputation. The proposed approach aims for secure scheduling of incoming jobs based on the Trust Factor value to available resource sites. The Trust Factor (TF) value of each resource site is calculated through its self-protection capability and reputation weightage obtained from user community on its past behavior. Two necessary assumptions are made below: (a) all resource sites have prior agreements to participate in the Grid operations; and (b) the Grid sites truthfully report their self-protection capability to Grid organization manager (GOM). Selfish Grids [21] are not considered in our approach.

4.1 Self-Protection Capability

The grid organization manager maintains the self-protection capability of all entities in a grid organization. Every so often each entity reports its self-protection capability trustfully and honestly to the GOM. The self-protection capability of an entity is calculated by aggregating the values of the below mentioned security factors. The value of these factors differs in the range between 0 and 1.

- *IDS Capabilities:* - The ability of an entity to protect the system against host and network based intrusions.
- *Anti-virus Capabilities:* - The ability of an entity to defend against viruses and malicious codes.
- *Firewall Capabilities:* - The ability to protect the entity from other network accesses.
- *Authentication Mechanism:* - The ability of the mechanism to verify an identity claimed by or for a system security.
- *Secured File Storage Capabilities:* - The ability of an entity for securely storing the files needed for the execution of job.
- *Interoperability:* - The ability of an entity to restrict the interfacing between concurrent jobs.
- *Secured Job Execution:* - The ability of an entity for the secure execution of the job.

Based on their contribution to security, a weightage is given to all the security factors and as a final point aggregated to compute the self-protection capability. The weightage assigned to the security factors are listed in Table1.

Table 1: Weightage of Security Factors

Security Factors	**Weightage (W)**
IDS Capabilities	0.825
Anti-virus Capabilities	0.85
Firewall Capabilities	0.9
Authentication Mechanism	0.8
Secured File Storage Capabilities	0.7
Interoperability	0.6
Secured Job Execution	0.75

The self-protection capability is calculated using the following formula

$$SPC = \sum_{i=1}^{n} W(i) * A(i)$$

Where n is the total number of factors, W is the weightage and $A(i)$ value of the factor.

4.2 Reputation Computation

Since reputation is a multi-faceted concept [22], it has many aspects for instance truthfulness, honesty and so on. Reputation weightage is calculated via the feedback on quite a lot of security characteristics provided by the user community about their previous experiences. After the usage, users will provide feedback on the attributes to the Reputation manager (RM) based on their experience. The feedback is a value in the range between 0 and 1. An entity's feedback from all the users has aggregated. The reputation weightage is calculated with the algorithm in section 4.2.1. The RM in grid organization maintains the reputation weightage of all entities. The security attributes considered for the reputation are as follows.

- *Consistency:* - The ability of an entity to perform its required functions under stated conditions for a specified period of time
- *Confidentiality:*- The ability to keep information from being disclosed to unauthorized users
- *Truthfulness:* - The ability of the entity to ensure that the data is protected from unauthorized modifications
- *Security:* - The ability of the system to provide protection to job execution and file storage.
- *Privacy:* - The ability to keep some information solely to oneself
- *Non-repudiation:* - The inability of something that performed a particular action to later deny that they were indeed responsible for the event
- *Authentication:* - Defined as the process of verifying an identity claimed by or for a system entity. An authentication process consists of two steps: Identification and Verification
- *Authorization:* - Refers to the process of granting privileges to processes and, ultimately, users.

> This differs from authentication in that authentication is the process used to identify a user. Once identified (reliably), the privileges, rights, property, and permissible actions of the user are determined by authorization.

4.2.1. Algorithm For Reputation Weightage Calculation

The aggregated feedback of all the security attributes of an entity is represented as a Reputation Vector (R_V) as follows.

$$R_v = [SA_1, SA_2, \ldots\ldots, SA_n]$$

Where n is the total number of security attributes.

The aggregated feedback of all the entities in the Grid domain is represented as a Reputation Matrix (R_M) as follows. Each row in R_M represents the reputation vector R_V of an entity.

$$R_M = \begin{bmatrix} SA_{11} & \mathrm{SA}_{12} & \mathrm{SA}_{13} \ldots\ldots SA_{1j} \\ SA_{21} & \mathrm{SA}_{22} & \mathrm{SA}_{23} \ldots\ldots SA_{2j} \\ SA_{i1} & \mathrm{SA}_{i2} & \mathrm{SA}_{i3} \ldots\ldots SA_{ij} \end{bmatrix}$$

Where i represent the number of entities and j represent the number of attributes.

The reputation weightage of each entity is evaluated by its relativity with other entities in the Grid domain by forming a relativity matrix. The relativity matrix is formed as follows.

$$\mathrm{Re}\,l_{Mat} = \begin{bmatrix} \varphi(\mathrm{E}_1,E_1) & \varphi(\mathrm{E}_1,E_2) & \varphi(\mathrm{E}_1,E_3)\cdots\cdots\varphi(\mathrm{E}_1,E_n) \\ \varphi(E_2,E_1) & \varphi(\mathrm{E}_2,E_2) & \varphi(\mathrm{E}_2,E_3)\cdots\cdots\varphi(E_2,E_n) \\ \varphi(E_3,E_1) & \varphi(\mathrm{E}_3,E_2) & \varphi(\mathrm{E}_3,E_3)\cdots\cdots\varphi(E_3,E_n) \\ \vdots & \vdots & \vdots \qquad \vdots \\ \varphi(\mathrm{E}_n,E_1) & \varphi(\mathrm{E}_n,E_2) & \varphi(\mathrm{E}_n,E_3)\cdots\cdots\varphi(E_n,E_n) \\ \end{bmatrix}$$

Where n is the number of entities and $\varphi(E_a, E_b)$ represents the relativity between the entities E_a and E_b and calculated as follows

$$\varphi(E_a, E_b) = \begin{Bmatrix} 1, E_a > E_b \\ 0, E_a < E_b \\ 0.5, E_a = E_b \end{Bmatrix}$$

Finally the reputation weightage is calculated using the following equation.

$$RW(E_a) = \sum_{b=1}^{n} \varphi(E_a, E_b)$$

4.3.Trust Factor Calculation And Resource Selection

The trust factor (TF) of each entity is calculated by utilizing the self-protection capability (SPC) and Reputation Weigthage (R_W) calculated as discussed in above sections using the following equation.

$$TF\,(E_a) = SPC\,(E_a) + RW(E_a)$$

The resource is selected for the execution of incoming jobs using the following algorithm.

```
for each entity in Grid domain
        Obtain SPC from GOM
        Obtain RW from RM
        Calculate TF
end
$[STF, Ind] = DescSort(TF)$
for all i jobs
        Allocate Entity [Ind[i]] to job $J_i$
end
```

5. Experimental Results

In this section, we first describe the experimental setup and present the analysis of our experimental results. The proposed algorithm is implemented in Java. The experimental setup consists of ten grid entities and a Grid Organization Manager (GOM). At first, the users submit their jobs to GOM. The GOM will calculate the trust factor value of all the entities based on their Self protection capability and Reputation weightage. An entity with high trust factor value is selected for the execution of current job. The GOM will inform the user with the selected entity for their job execution. After the completion of job, the user is asked to provide feedback about the entity on some security attributes. The selected entity has provided high security for the job execution. The self protection capability of all the entities is updated by the GOM in a periodical manner. The reputation weightage is frequently updated for all the entities based on the feedback value from user communities.

The security factors utilized for determining the self-protection capability of the ten grid entities are enlisted along with their respective values in Table2. The security attributes that eventually aid in the estimation of reputation weightage with their respective values are as well listed subsequently in Table 3.

Table 2: Values of Security Factors for Ten Entities

Entity	**IDSC**	**AVC**	**FC**	**AM**	**SFSC**	**I**	**SJE**
E1	0.245	0.535	0.555	0.605	0.605	0.65	0.56
E2	0.21	0.5	0.7	0.57	0.61	0.44	0.39
E3	0.6	0.37	0.89	0.51	0.67	0.73	0.79
E4	0.15	0.21	0.45	0.57	0.39	0.23	0.38
E5	0.145	0.7725	0.7775	0.675	0.7075	0.675	0.7
E6	0.5	0.6	0.65	0.4	0.5	0.35	0.3
E7	0.51	0.42	0.5	0.56	0.7	0.4	0.61
E8	0.4	0.5	0.59	0.68	0.74	0.79	0.62
E9	0.6	0.37	0.89	0.51	0.67	0.73	0.79
E10	0.21	0.5	0.7	0.57	0.61	0.44	0.39

Table 3: Values of Security Attributes for Ten Entities

Entity	Consistency	Confidentiality	Truthfulness	Security	Privacy	Nonrepudiation	Authentication	Authorization
E1	0.245	0.285	0.305	0.355	0.355	0.4	0.31	0
E2	0.65	0.66	0.97	0.5	0.4	0.1	0.35	0.21
E3	0.6	0.7	0.8	0.58	0.25	0	0.21	0.6
E4	0.71	0.77	0.85	0.67	0.52	0.23	0.58	0.15
E5	0.46125	0.46375	0.47375	0.44625	0.43125	0.3875	0.44	0.1975
E6	0.54	0.725	0.75	0.6	0.465	0.4	0.5	0.5
E7	0.75	0.8	0.9	0.55	0.28	0.15	0.32	0.51
E8	0.82	0.75	0.5	0.63	0.21	0	0.3	0.4
E9	0.67	0.81	0.89	0.51	0.37	0.02	0.44	0.6
E10	0.41	0.5	0.7	0.57	0.31	0.2	0.39	0.21

A relativity matrix that is obtained on basis of the proposed approach with the values of various security attributes present in the foreshown table is given below. Further, this relativity matrix is employed in the estimation of reputation weightage.

$$Rel_{Mat} = \begin{bmatrix} 0.5 & 0.125 & 0.375 & 0.125 & 0.125 & 0.0625 & 0.25 & 0.375 & 0.125 & 0.25 \\ 0.875 & 0.5 & 0.625 & 0.25 & 0.625 & 0.25 & 0.375 & 0.5 & 0.375 & 0.5625 \\ 0.625 & 0.375 & 0.5 & 0.125 & 0.625 & 0.375 & 0.25 & 0.4375 & 0.1875 & 0.625 \\ 0.875 & 0.75 & 0.875 & 0.5 & 0.75 & 0.75 & 0.5 & 0.75 & 0.625 & 0.875 \\ 0.875 & 0.375 & 0.375 & 0.25 & 0.5 & 0.0 & 0.375 & 0.375 & 0.3125 & 0.5 \\ 0.9375 & 0.75 & 0.625 & 0.25 & 1.0 & 0.5 & 0.5 & 0.625 & 0.5 & 1.0 \\ 0.75 & 0.625 & 0.75 & 0.5 & 0.625 & 0.5 & 0.5 & 0.75 & 0.5 & 0.5 \\ 0.625 & 0.5 & 0.5625 & 0.25 & 0.625 & 0.375 & 0.25 & 0.5 & 0.25 & 0.5 \\ 0.875 & 0.625 & 0.8125 & 0.375 & 0.6875 & 0.5 & 0.5 & 0.75 & 0.5 & 0.75 \\ 0.75 & 0.4375 & 0.375 & 0.125 & 0.5 & 0.0 & 0.5 & 0.5 & 0.25 & 0.5 \end{bmatrix}$$

Figure 1-4 are the charts of data obtained from the various experimental setups. From these charts, it is very apparent to make a decision on selecting a secured entity for the current job. But the proposed approach has played witty solution to arrive the most secured entity among the available entities during a particular period of time under varying values of security attributes. The line marked dark is the selected entity.

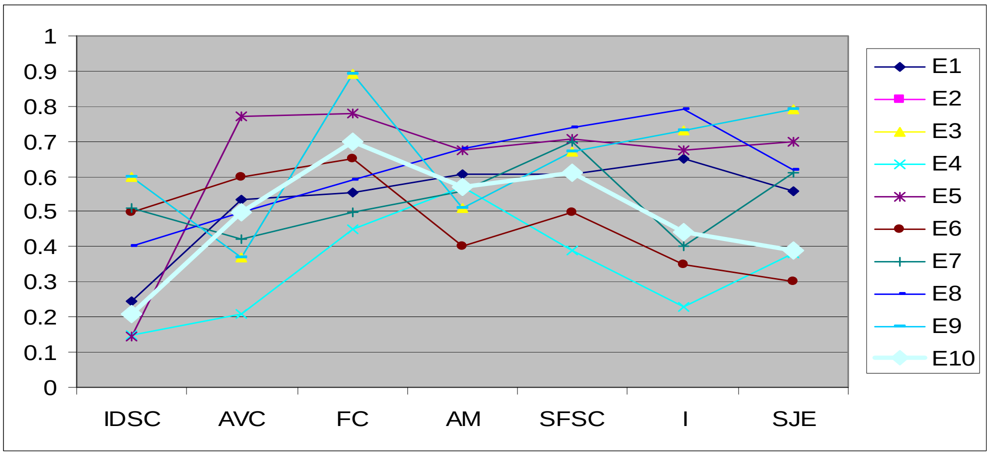

Fig. 1. Security Factors Graph with selected entity E10

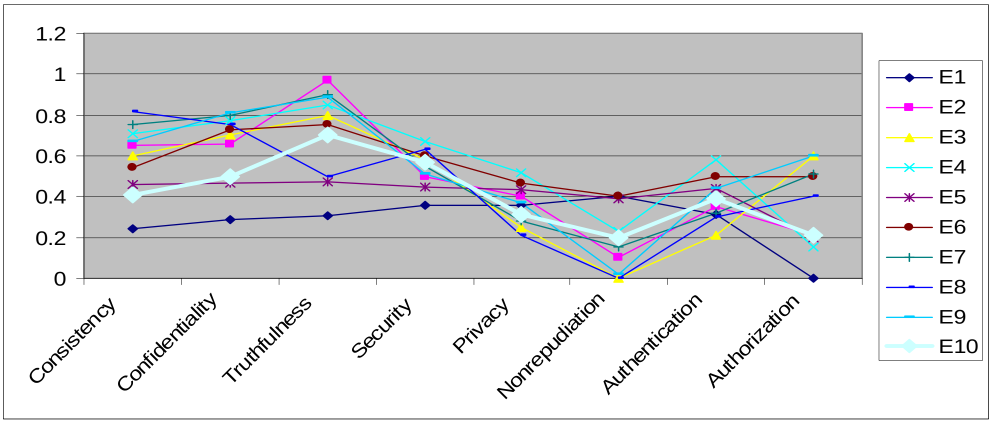

Fig. 2 Security Attributes Graph with selected entity E10

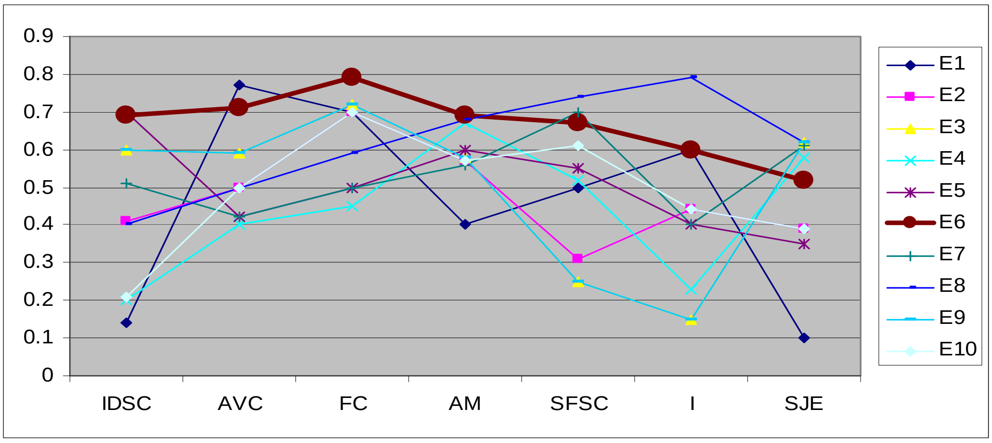

Fig. 3. Security Factors Graph with selected entity E6

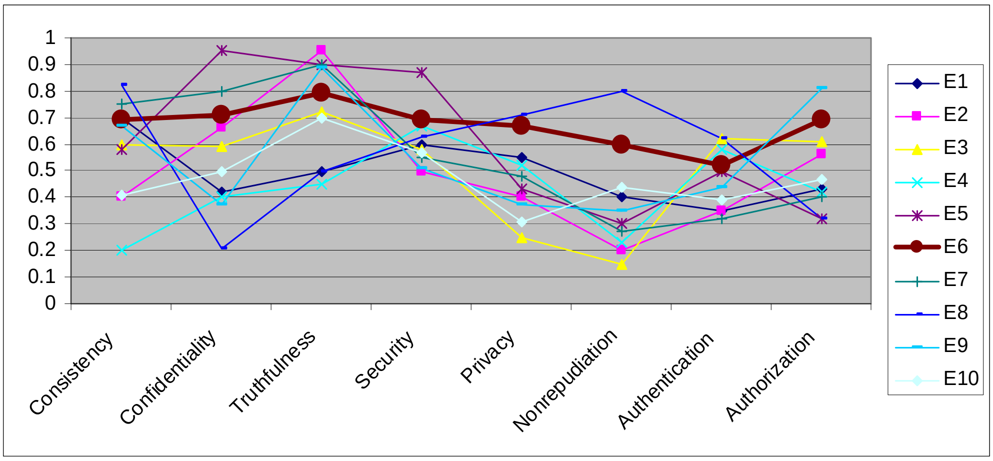

Fig. 4. Security Attributes Graph with selected entity E6

6. Conclusion

Computational Grids are quickly rising as a practical means by which to execute new science and develop new applications. The effective and efficient exploitation of Grid computing facilities needs highly advanced and protected resource management systems. Efficient resource sharing and accessing cannot go without the assurance of high trustworthiness. Reputation mechanisms provide a way for building trust through social control using community based feedback about previous experiences. In this paper, we have proposed a secured approach for the users in selecting the correct resource meant for their job execution. The proposed approach joint both trust and reputation to provide security for resource selection mechanism. Our approach aggregates several security related attributes for both self-protection capability and reputation into numerical values, which can be easily applied to calculate the Trust factor of grid entity. Our method is demonstrated effective in selecting secured entity for job execution from the available ones. Our scheme scales well with both number of jobs and number of Grid sites.

References

[1] F. Berman, G. Fox and T. Hey (eds.), Grid Computing: Making the Global Infrastructure a Reality. Wiley, 2003.

[2] M. Cosnard and A. Merzky, “Meta- and Grid-Computing”, in Proceedings of the 8th International Euro-Par Conference, August 2002, pp. 861–862.

[3] Nadia Ranaldo, Eugenio Zimeo. A Framework for QoS-based Resource Brokering in Grid Computing. In 5th IEEE ECOWS, the 2nd Workshop on Emerging Web Services Technology, Halle, Germany, 2007.

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

[5] Foster, I. and Kesselman, C. Computational Grids. Foster, I. and Kesselman, C. eds. The Grid: Blueprint for a New Computing Infrastructure, Morgan Kaufmann, 1999, 2-48.

[6] “National Science Foundation TeraGrid”. from http://www.teragrid.org.

[7] SETI@Home: The Search for Extraterrestrial Intelligence. http://setiathome.ssl. berkeley.edu/

[8] F. Berman, R. Wolski, H. Casanova, W. Cirne, H. Dail, M. Faerman, S. Figueira, J. Hayes, G. Obertelli, J. Schopf, G. Shao, S. Smallen, N. Spring, A. Su and D. Zagorodnov, “Adaptive Computing on the Grid Using AppLeS”, IEEE Trans. on Parallel and Distributed Systems, Vol. 14, April 2003.

[9] V.Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S.Meder, L. Pearlman and S. Tuecke, “Security for Grid Services”, in Proceedings of the HPDC-12, 2003.

[10] Zhiguo Shi, Yeping He, Xiaoyong Huai, Hong Zhang. Identity Anonymity for Grid Computing Coordination based on Trusted Computing. Proceedings of the Sixth International Conference on Grid and Cooperative Computing. pp.403-410, 2007.

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

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

[13] J. Basney, W. Nejdl, D. Olmedilla, V. Welch, and M. Winslett. Negotiating trust on the grid. In 2nd Workshop on Semantics in P2P and Grid Computing, New York, May 2004.

[14] Farag Azzedin, Muthucumaru Maheswaran, "Towards Trust-Aware Resource Management in Grid Computing Systems," ccgrid, p. 452, 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID'02), 2002.

[15] R. Buyya and S. Venugopal, The Gridbus Toolkit for Service Oriented Grid and Utility Computing: An Overview

and Status Report, Proceedings of the First IEEE International Workshop on Grid Economics and Business Models (GECON), 2004.

[16] Lohr, H. Ramasamy, H. V. Sadeghi, A.-R. Schulz, S. Schunter, M. Stuble, C., Enhancing Grid Security Using Trusted Virtualization, Lecture Notes in Computer Science, pp. 372-384, Springer, 2007.

[17] J. R. D. Dyson, N. Griffiths, H. N. Lim Choi Jeung, S. A. Jarvis, and G. R. Nudd, Trusting Agents for Grid Computing, in Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (SMC 2004), pp. 3187-3192, IEEE Press, October 2004.

[18] Shanshan Song and Kai Hwang, Dynamic Grid Security with Trust Integration and Optimized Resource Allocation, Internet and Grid Computing Laboratory, University of Southern California, Los Angeles, CA. 90089 USA.

[19] R. A. Malaga. Web-based reputation management systems: Problems and suggested solutions. Electronic Commerce Research, 1(4), 2001.

[20] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara. Reputation Systems. Communications of the ACM, 43(12), December 2000: 45–48.

[21] Y.-K. Kwok, S. Song and K. Hwang, “Selfish Grid Computing: Game-Theoretic Modeling and NAS Performance Results”, in Proceedings of CCGrid 2005, Cardiff, UK, May 2005.

[22] Yao Wang and Julita Vassileva: Trust and Reputation Model in Peer-to-Peer Networks. In Proceedings of the 3rd IEEE International Conference on Peer-to-Peer Computing. Linkŏping: IEEE Computer Society (2003), 150–158.

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

[24] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, P. Samarati and F. Violante, “A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks”, in Proceedings of ACM CCS 2002.

[25] S.D. Kamvar, M.T. Schlosser and H. Garcia-Molina, “The Eigentrust Algorithm for Reputation Management in P2P Networks”, in Proceedings of ACM WWW 2003.

[26] C. Liu, L. Yang, I. Foster and D. Angulo, “Design and Evaluation of a Resource Selection Framework for Grid Applications”, in Proceedings of HPDC-11, 2002.

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

[28] L. Xiong and L. Liu, “PeerTrust: Supporting Reputation-based Trust to P2P E-Communities”, IEEE Trans. Knowledge and Data Engineering, July 2004, pp. 843–857.

[29] Chunqi Tian, Shihong Zou, Wendong Wang, Shiduan Cheng, An Efficient Attack-Resistant Trust Model for P2P Networks, IJCSNS, Vol. 6 No. 11 pp. 251-258, 2006.

[30] Baolin Ma, Jizhou Sun, Ce Yu, Reputation-based Trust Model in Grid Security System, Journal of Communication and Computer, Volume 3, No.8 (Serial No.21), 2006.

[31] V.Vijayakumar and Dr.R.S.D.Wahida Banu, “Trust and Reputation Aware Security for Resource Selection in Grid Computing," International Conference on Security Technology (SecTech 2008), December 13 ~ 15, 2008. (Accepted for Publication).

V.Vijayakumar obtained B.E. degree in 1999 and his M.E. degree in 2001 from University of Madras with First Class. He was awarded for First Rank in M.E from Vellore Engineering College. He also completed Diploma in Computer Technology with First Class Honors from State Board of Tamilnadu and he also had completed M.B.A. in HRD from the Periyar University. He is the life member of ISTE. Currently, he is doing his research in the area of Grid Computing under Anna University, Chennai.

R.S.D.Wahida Banu obtained B.E. degree in 1981 and her M.E. degree in Jan ‘85 from GCT, Coimbatore, and Madras University. She got the Ph.D. degree from Anna University, Chennai. First lady to acquire Ph.D. in Chennai zone and second qualified Ph.D. supervisor in the area of Computer Science and Engineering related areas. As expertise is less it continues in the Directorate of Technical Education, Tamilnadu. She has more than 25 years of Teaching Experience. She is the member of ISOC, IAENG, VDAT and life member of ISTE, IE, CSI and SSI. She has published more than 100 National and International Journals. She has produced 5 PhD Scholars. She is currently working as Professor and Head of Electronics and Communication Engineering, Government College of Engineering, Salem. Her area of interest includes Artificial Intelligence, Network Security, and Grid Computing.