Performance Analysis in Secured Grid Resource Selection based on Trust and Reputation

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.

ABSTRACT

Grid computing is the robust technology which is used to utilize the idle or available resources very effectively is solving the large scale or scientific problems. The security is a major concern in selecting a high degree of strange resources available. In this paper we have compared our proposed approach with the previous approach and the experimental analysis have proved that the proposed approach is best in selecting the secured resource based on trust and reputation. This also ensures that the proposed approach provides better results for large number of malicious nodes compared with the previous approach.

Keywords

Grid Computing, security, trust and reputation.

1. INTRODUCTION

The anxious sharing is not primarily file exchange, rather direct access to systems, software, data and many other resources which are vital for assorted Collaborative problem-solving and resource-brokering Strategies emerging in industry, science and engineering [6]. Resource and security guarantee are the two fundamental necessities of Grid applications [7]. Users submit jobs to way away resources and usually have no clear weight over the resources themselves. Therefore, commonly the users and resources can be considered as independent agents, possessing power of their own behavior.

The independence causes an increase in intrinsic insecurity owing to the fact that an individual is not proficient of predicting the response of another to varying situations. It is essential that the grid service providers proffer guaranteed security, privacy protection, and reliable accessibility of all Grid-enabling platforms [8].

The rock-hard problems underneath the grid concept include coordinated resource allocation and problem solving in vibrant, multi-institutional virtual organizations [9]. Contaminated grid resources can probably break the applications running on the same grid platform via the wicked codes designed by intruders.

Grid computing demands robust resource allocation of jobs with security assurance at all grid resources. Large scale Grid applications are being hindered by lack of security assurance from grid resource.

Our ultimate aim is to develop a standard approach for secured allocation of jobs in grid resources based on trust and reputation. The proposed model is shown in fig.1. The figure indicates the proposed methodology of the secured grid resource allocation based on trust and reputation.

The proposed approach [2] performs the setting up of the incoming jobs in harmony with the computed Trust Factor value. Feedback [5] from user communities and also the feedback received from other entities in the Grid are engaged in determining an entity's reputation weightage which in turn is utilized along with Self-protection capability to compute the entity's Trust Factor (TF) value as shown in the equation (1). The ability of an entity to handle intrusions, viruses, unauthorized access and secured file storage are denoted as self protection capability of that site. Reputation mechanisms provide a way for building trust through social control using community based feedback about past experiences of entities.

$$TF\,(E_a) = SPC\,(E_a) + RW(E_a) \qquad (1)$$

where TF = Trust Factor, SPC = Self Protection Capability, RW = Reputation Weightage and Ea = Entity.

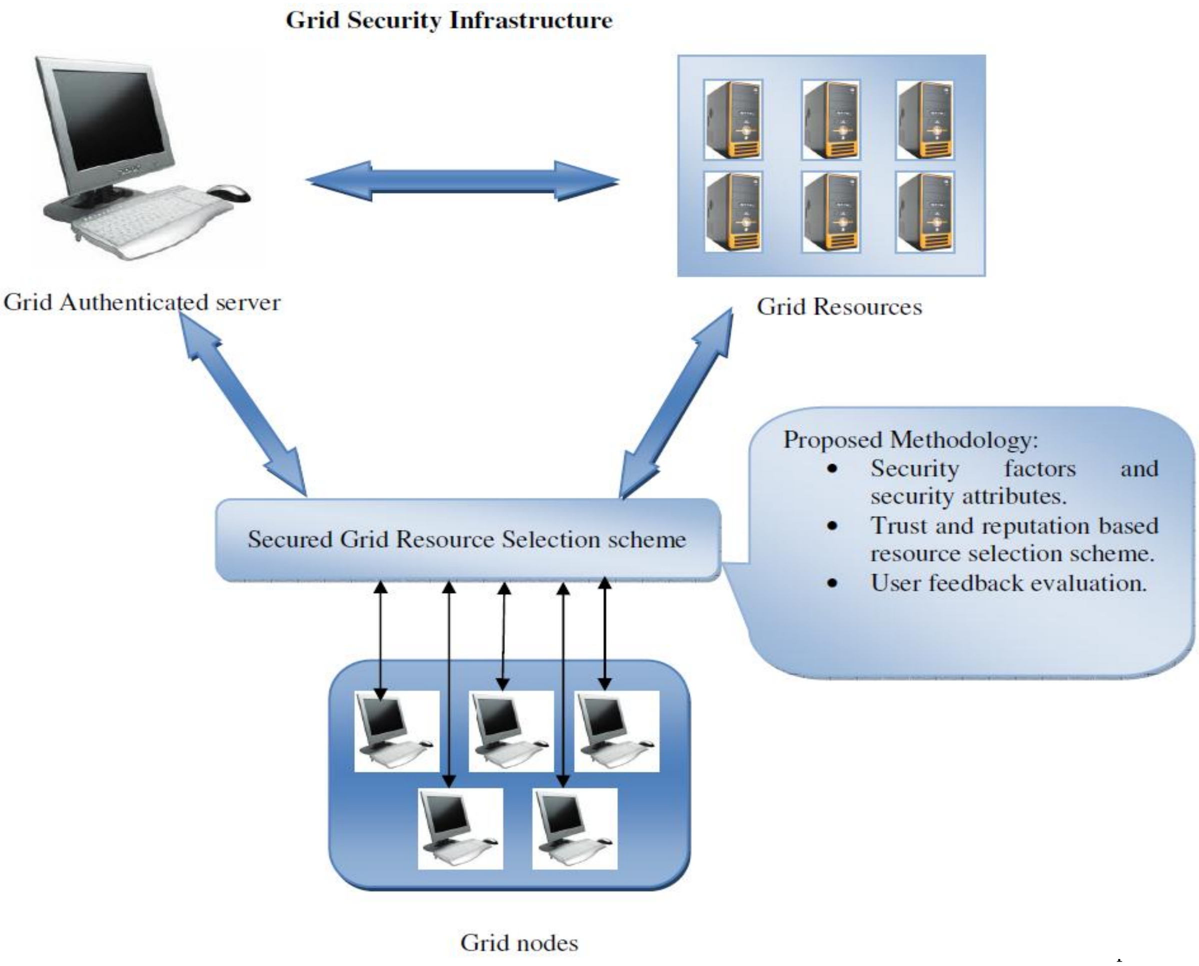
Grid Security Infrastructure
Grid Authenticated server
Grid Resources
Secured Grid Resource Selection scheme
Proposed Methodology:
• Security factors and security attributes.
• Trust and reputation based resource selection scheme.
• User feedback evaluation.
Grid nodes

Fig 1: Proposed model of our research

Besides, a novel approach is proposed for evaluating user's feedback. The feedback given by a user about an entity is evaluated on the basis of the aggregated feedback available about that entity.

The rest of the paper is organized as follows: In Section 2, a concise review of the recent researches related to the proposed approach is presented. An experimental analysis of the proposed approach with the previous approach to prove the efficiency is provided in Section 3 and Section 4 concludes the paper.

2. RELATED WORK

A proper clarity of both trust and reputation was offered and a model for incorporating trust into Grid systems was discussed by Farag Azzedin and Muthucumaru Maheswaran [3]. The Overview of an open source Grid toolkit known as Grid bus, the structural design of which is deeply driven by the requirements of Grid saving was carried out by Rajkumar Buyya and Srikumar Venugopal [4].

rthiness
s based
ust was proposed by Baolin Ma et al. [1]. Zhiguo Shi et al. [9] described a novel unidentified coordination authentication development capable of providing efficient and reliable mysterious identity authentication and remote platform substantiation for Grid computing systems.

Vijayakumar et al. [10] proposed a trust model by considering both trust and reputation with the user's feedback and also the other entities feedback in providing the secured resources for the users to submit their job in the grid environment.

3. EXPERIMENTAL ANALYSIS

This section presents the experimental analysis of the proposed approach [5] with the previous approach to prove the efficiency. Initially, the simulation set up and then the comparative analysis with respect to the trust and evaluation accuracy is presented. Finally, the effects of trust integration for secured selection of grid resources are reported.

3.1 Simulation Setup and Performance Metrics

For the experimentation, we have simulated 50 entities in a grid environment and the "*n*" number of user is allowed to select the secured grid resources. Then, the malicious nodes are simulated to identify the efficacy of the approaches in selecting the secured grid entities. Here, two sets of experiments are performed in which, the first set of results are obtained once n=50 users are used for the simulated grid environment and the second set of experiment is conducted once n=100 users are used for the simulated grid environment. Then, two sets of evaluation are conducted to compare the proposed approach with the previous approach such as, trust and the trust evaluation accuracy.

3.2 Comparative analysis of the proposed approach

In the simulation setup, the trust model is compared with the previous approach [1] that presented a trust model, which is utilized to compute and compare the trustworthiness of entities in the same autonomous and different domains. Here, they proposed a trust model that computes node's reputation using the trust score based on past quality and reliability of interaction records. To accurately evaluate the trustworthiness of a node, this trust model contains three parameters: the quality of a node's historical transaction, the feedback score provided by feedback source and the credibility of feedback source. Along with this previous approach, the proposed approach are also performed their experimentation in the simulated grid environment and the corresponding trust and the trust evaluation accuracy is computed to plot the graphs. Then, two set of experiments are used to evaluate the accuracy of the approaches and show how the malicious node behaviors affect the selection problem in grid system and its performance.

3.2.1 Trust index

Initially, the grid environment is simulated and the list of user is allowed to select the secured grid resources. After selecting the grid resource, every user enters feedback values about the grid entity. These values are stored in the corresponding table with regards to the technique used in both the approaches. After getting the updates from 50 users, trust values generated for the new user is plotted as graph shown in figure 2.

The graph shows that the trust values computed for the 50 entities of both the approaches. From the graph, we can identify that the trust values of the proposed approach is deviated very well so that the selection of secured grid resources is not a challenging task. Similarly, the graph shown in figure 3 is plotted once 100 users utilized the simulated grid environment. This graph is also more similar to the first one in behavior but, the trust factor is continuously increased if more number of users utilized the grid environment.

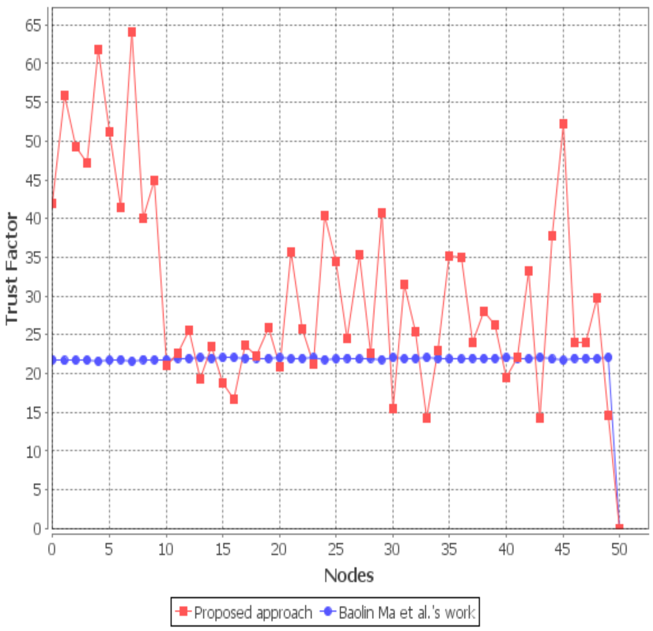

Fig 2: Graph plotted for the trust values once 50 users used the simulated grid environment

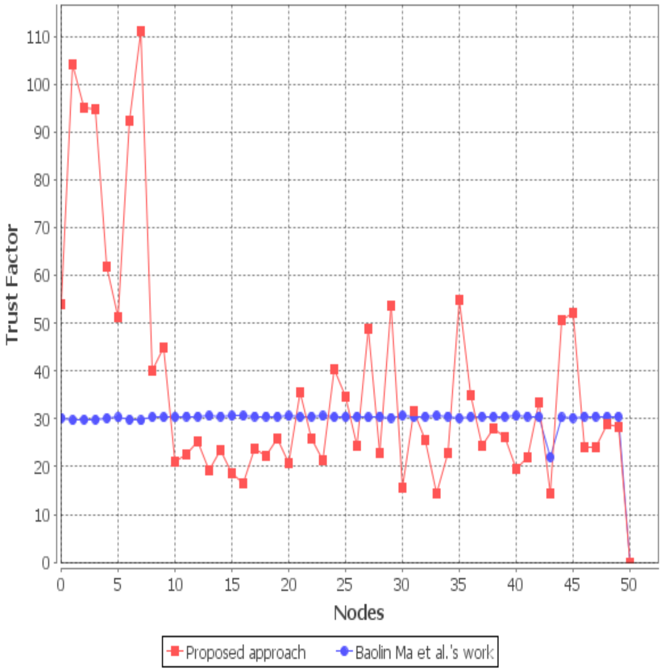

Fig 3: Graph plotted for the trust values once 100 users used the simulated grid environment

3.2.2 Trust Evaluation Accuracy

Trust evaluation accuracy is computed for both approaches and the accuracy of the resource selection is compared by plotting the graphs. By fixing the malicious nodes, number of grid entities is selected to execute the job and then the accuracy of selection is computed whether all the selected grid nodes are secured one or malicious nodes.

This procedure is repeated for varying number of malicious nodes and the accuracy is calculated. Using the computed values, the graph is plotted under two different level of updating happened. The accuracy graph shown in figure 4 is plotted after updating the feedback values of 50 users.

This ensures that the proposed approach provides better results for large number of malicious nodes compared with the previous approach. But in second experiment, the proposed approach outperformed completely than the previous approach. The accuracy graph shown in figure 5 is plotted after updating the feedback values of 100 users.

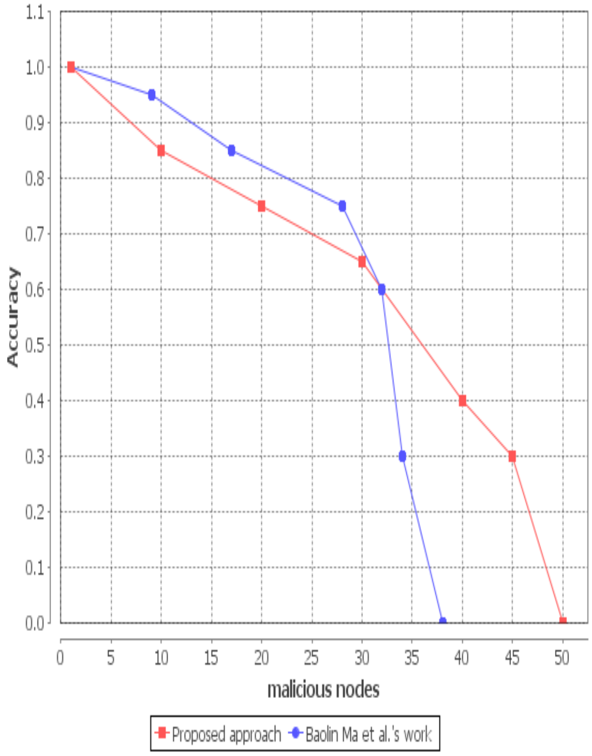

Fig.4. Trust evaluation accuracy once 50 users used the simulated grid environment

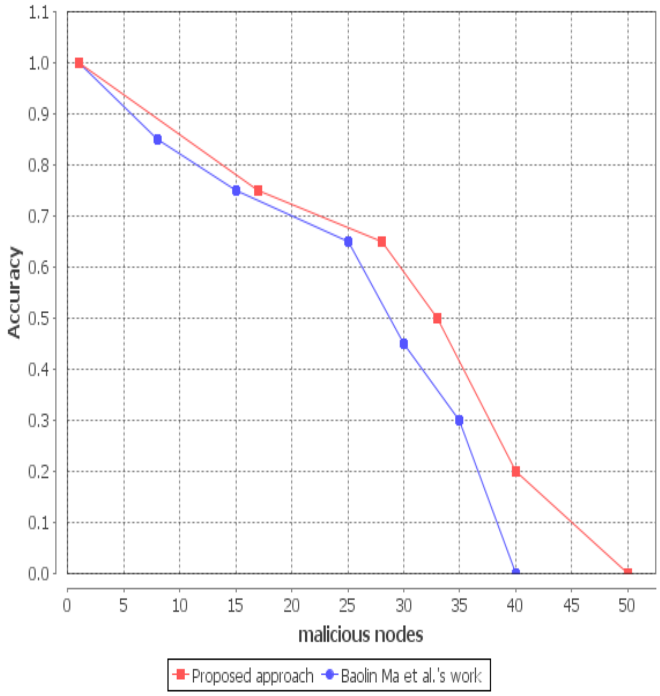

Fig.5. Trust evaluation accuracy once 100 users used the simulated grid environment

4. CONCLUSION

The comparative analysis of the proposed approach with the previous approach to prove the efficiency is carried out in the simulated grid environment. Trust and the trust evaluation accuracy are computed for both the approaches to evaluate the performance of the approaches. Along with, the malicious node behaviors in the selection problem and its performance are compared for both the approaches.

5. REFERENCES

[1] Baolin Ma, Jizhou Sun, Ce Yu, "Reputation-based Trust Model in Grid Security System", Journal of Communication and Computer, Vol. 3, No.8, August 2006.

[2] V.Vijayakumar and R.S.D.Wahida Banu, "Security for Resource Selection in Grid Computing Based On Trust and Reputation Responsiveness", International Journal of Computer Science and Network Security (IJCSNS), Vol.8, No.11, November 2008.

[3] 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.

[4] R. Buyya and S. Venugopal, "The Grid bus 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.

[5] V.Vijayakumar and R.S.D.Wahida Banu, J. H. Abawajy, **"**Novel Mechanism for evaluating feedback in the Grid

Environment on resource allocation ", Proceedings of the 2010 International Conference on Grid Computing Applications, GCA 2010.

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

[7] 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.

[8] 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.

[9] 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.

[10] V.Vijayakumar, R.S.D.Wahida Banu and J. H. Abawajy, "An efficient approach based on trust and reputation for secured selection of grid resources", International Journal of Parallel, Emergent and Distributed Systems, Sep 2011.