Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
15th April 2011. Vol. 26 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RECENT TRUST MODELS IN GRID

[1]P. SURESH KUMAR, [2]P. SATEESH KUMAR, [3]S. RAMACHANDRAM

[1]Kakatiya Institute of Technology & Science, Warangal, India,

[2]Vaagdevi College of Engineering, Warangal, India,

[3]Member, IEEE, Osmania University, Hyderabad

ABSTRACT

A grid is a framework providing services to access and manage distributed hardware and software resources. A thorough authentication is required before any requested access or operation is allowed on any resource of the grid. In particular, much risk is involved when the grid is used for e-commerce where it is necessary to share resources with unknown parties. It is difficult for a resource user on the grid to identify the quality of the resource providers. Trust is one mechanism with which one can identify the quality of the resource provider. Various models are proposed in the literature on the use of trust mechanisms in grid. This paper presents a survey on various models proposed recently on trust management in grid computing.

Keywords – *Grid, security, trust, grid computing, trust models, recommendation trust, and behavior trust.*

1. INTRODUCTION

Grid Computing [1] is the distributed computing capability of a powerful self managing virtual computer made up of a large set of heterogeneous systems connectivity for sharing various resources. Grid computing makes use of an idle machine present on the grid for an application, if the regularly used machine is unusally busy due to the peak activity. This is the simplest use of the grid. This simplest scenario enforces at least two prerequisites. One, the application must run on a remote machine without any excessive overhead. Other, the application must be sufficiently provided with all the required resources such as special hardware and software. Much of the survey indicates that most desktop systems are underutilized in most of the organizations. Around 95% of the time is idle and only less than 5% of the time is busy for computations in desktop systems. Grid computing increases the efficiency of these systems by providing a framework for better utilizing the resources. A simple grid is depicted in Fig.1.

Another function of the grid is to better balance resource utilization. An organization may have occasional unexpected peaks of activity that demand more resources. If the applications are grid-enabled, they can be moved to underutilized machines during such peaks. In general, a grid can provide a consistent way to balance the loads on a wider federation of resources. This applies to CPU, storage, and many other kinds of resources that may be available on a grid.

2. TRUST

In grid computing, the applications are run of the remote machines rather than simply transferring data on to the machines. There is a high probability of attack of viruses and Trojan horse programs on the systems if the grid is not configured for securing the applications. In fact, there is a need for enforcing high levels of security in grid computing to prevent from such attacks. Security is a much more important factor in planning and maintaining a grid than in conventional distributed computing [1], where data sharing comprises the bulk of the activity. For this reason, it is important to understand exactly which components of the grid must be rigorously secured to deter any kind of attack. Furthermore, it is important to understand the issues involved in authenticating users and properly executing the responsibilities of a certificate authority.

Grid security builds on well-known security standards and fundamental services such as authentication, authorization, and encryption. A grid resource must be authenticated [2] before any checks can be done as to whether or not any requested access or operation is allowed within the grid. Once the grid resources have been authenticated within the grid, the grid user can be granted certain rights to access a grid resource. Furthermore, encryption mechanisms are required to prevent data in transit between grid resources from being captured, spoofed, or altered.

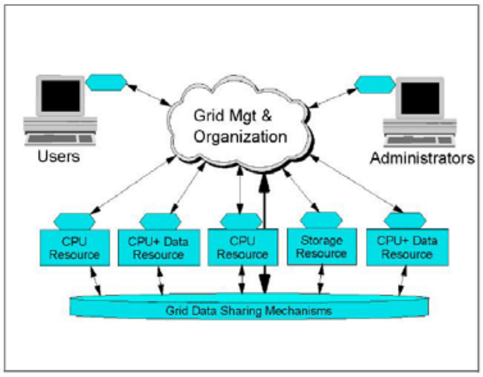

Figure 1. A Simple Grid (Courtesy: IBM RedBook)

This section analyses the concept of trust and its relation with security. There is a vast source of information on the theory and application of trust, For instance [3],[4],[6],[7]. In the Internet world, trust has been recognized as an important aspect of decision making for electronic commerce [8],[9]. The Grid was initiated as a way of supporting scientific collaboration, where many of the participants knew each other sharing the resources. In this case, there is an implicit trust relation, all partners have a common objective - for instance to realize a scientific experiment- and it is assumed that resources would be provided and used within some defined and respected boundaries. However, when the Grid is intended to be used for business purposes, it is necessary to share resources with unknown parties. Such interactions may involve some degree of risk since the resource user cannot distinguish between high and low quality resource providers on the Grid. The inefficiency resulting from this asymmetry of information can be mitigated through trust mechanisms. Trust is specified in terms of a relation between a trustor, the subject that trusts a target entity, and a trustee, the entity that is trusted. Based on the relation between trustor and trustee, trust is classified into following categories [8]: Service Provision Trust, Resource Access Trust, Delegation Trust, Certification Trust, and Context Trust. In Service Provision, the trustor trusts the trustee to provide a service that does not involve access to the trustor's resources. In Resource Access Trust, a trustor trusts a trustee to use resources that he own or controls. In Delegation Trust, a trustor trusts a trustee to make decisions on his behalf, with respect to a resource or service that the trustor owns or controls. Certification Trust is based on the certification of the trustworthiness of the trustee by a third party. Context Trust refers to the base context that the trustor must trust.

3. TRUST MODELS

Vivekananth [10] proposed a behavior based trust model which shows the behavior conformity. In this model author concentrated on behavior of entities in different domains, in different contexts. The total trust will be calculated by direct trust and indirect trust. Both the trust will be evaluated by reputations. There will be tracking module, which will keep track of behavior. Based on experiences with the entities, an entity trust level will be increased or decreased. There can be a penalty factor, which can be levied for malicious behaviors. The trust factor between two entities may depend on penalty, context and time. The penalty will be higher if the misbehavior creates heavy harm. Other wise the penalty will be low. Based on this experience the trust will be updated. The penalty factor can be a number between 0 & 1. If the total trust is greater than the required trust then the resource is allocated. This model is still under revision. Srivaramangai et al [11] proposed a trust model to improve reliability in grid. According to their model, reputation based systems can be used in grid to improve the reliability of transactions. To achieve reliable transactions mutual trust must be established between the initiator and the provider. Two types of trust have been taken, namely direct trust and indirect trust. Indirect trust is measured from the reputation score of other entities. The authors aim to provide a model by eliminating the feedbacks using rank correlation method. Further, applies two way test criteria for initiator and provider. It also includes new expression for measuring direct trust.

Wang Meng et al [12] proposed a Dynamic Grid Trust Model named DyGridTrust which is based on recommendation credibility. This model suggests a way to distinguish honest and dishonest recommendation and adjust the weight of trust evaluation dynamically. This model categorizes the participating nodes as three kinds: sponsor node, goal node and recommended node. Further classification is made on trust relationships as direct, indirect and recommended trust relationship. As per the model, there is only one sponsor node in the process acting as main node meant for trust evaluation. The resulting node in the process of trust evaluation is goal node. And the recommended node is the node to more separate nodes. The trust relationship between sponsor node and goal node is termed the direct trust relationship. Sponsor node is provided with the set of recommended nodes due to recommended trust relationship. Indirect trust relationship is held between sponsor node and goal node with the assessed feedback from recommended nodes. This model evaluates the trust as the continuous real number in range [0, 1], where 0 expresses unbelievable while 1 means believable. Hongmei Liao et al [13] proposed a new behavior trust model based on fuzzy-logic. This model focused on the behavior trust that varies with time. Because of the fuzzy nature of trust, it is more appropriate to adopt fuzzy logic to express and compute trust than adopt probabilities approach. By variable weighted fuzzy comprehensive evaluation, Direct Trust can be gotten; by derivation and combination of trust, Reputation can be obtained. Expert's experience is used to set and simplify fuzzy rules. Malicious recommendation in trust transmission process are also be removed and punished in this model.

Gao Ying et al [14] proposed a layered trust model based on behavior to enhance grid security and extensibility. This model is based on the problem in open service grids to establish trust relationship among different domains. According to this model, there are two layers: upper layer and lower layer. The upper layer establishes and maintains recommendation trust relationships between different domains in grid whereas lower layer acts as in-charge of evaluating trust value of entities in that domain. The authors have proposed an algorithm to adjust trust relationships between domains based on entities interactions and also proposed a technique to process recommendation trust. Kai Wei Shaohua Tang [15] proposed a multi-level trust evaluation model based on direct search. According to this model, the grid becomes large as the user increase and direct search is suitable to solve such large scale problems. The model insists that Grid Service Providers (GSPs) need to evaluate and manage the trust of all users effectively. In accord with the architecture for grid, this model restrains the attacks such as Whitewash, and provides better protection for the GSPs. Changsong Ding et al [16] proposed a trust model considering user's QoS constraints. Two new concepts, namely Trustworthiness of Service and Satisfactoriness of Service, are introduced into the model, which are used to describe the resources' capabilities and users' satisfaction respectively. This trust model applied Bayesian Network to evaluate services' trustworthiness that takes into account users' multiple QoS metrics. Tie-Yan Li et al [17] proposed a two-level trust model and the corresponding trust metrics evaluation algorithms. In this model, the upper level defines the trust relationships among Virtual Organizations (VO) in a distributed manner. The lower level justifies the trust values within a grid domain. This model provided an integrated trust evaluation mechanism to support secure and transparent services across security domains. The authors claim that this model is flexible, scalable and interoperable. The design of the model also included the embedding the trust scheme into Grid Security Infrastructure (GSI).

Yuan Lin et al [18] designed a model by adding an asymmetric users' behaviors reflecting users' characteristics (both the subjective and objective). Trust based on user behavior not only can reduce or avoid the contact with the malicious user, but also can reduce additional costs from monitoring and prevention for mutual trust between different users. According to this model, a user has different trust evaluation result because of different transaction and behaviors. They have proposed different behaviors of user in transaction, a recommender trust model based behavior. Huang Wenming et al [19] studied the characteristics of the two classes of true and false recommendation. This model identifies the baleful entities that provide false recommendations in grid system, thus increasing the veracity of trust rating, based on the analysis of the feature set. Tatyana Ryutov et al [20] proposed a trust model based on trust negotiation. The model is named as Adaptive Trust Negotiation and Access Control (ATNAC) framework. This model addresses the problem of access control in open systems by protecting itself from adversaries who may want to misuse, exhaust or deny service to resources. This model provided a mechanism for adaptive access control capturing dynamically changing system security requirements. This model promises for establishing a trust between the negotiating participants, based on the sensitivity of the access request and a suspicion level associated with the requester. A federated security context allows Grid participants to communicate their security appraisal and make judgments based on collective wisdom and the level of trust among them.

Wu Xiaonian et al [21] tried to quantify the entity's trust according to the entity's behaviors. This behavior trust computation model is based on risk evaluation. This model includes asset identification, threat identification and trust relationship identification. Shashi Bhanwar et al [22] proposed a trust model for establishing and evaluating trust by computing reputation and trustworthiness of the transacting domain on the basis of number of past transactions and rated feedback score. Farag Azzedin et al [23] proposed a model in which trust is built by verifying the identity and authorization of an entity, and monitoring and managing the behavior of the entity. The trust in this model focused on behavior and reputation, instead of identity alone. This model tried to discuss the behavior trust management architecture that models the process of evolving and managing of behavior trust. Woodas W.K. Lai et al [24] viewed trust in two aspects – identity trust and behavior trust. Issues on grid context and trust tree structure are addressed to help in managing, evolving and interpreting trust. Huu Tran et al [25] proposed a trust model based on recommendation. This approach preserves the grid's decentralized structure and participant's autonomy, but also enables secure service exchange. S.ThamaraiSelvi et al [26] proposed a model based on affordability, success rate and bandwidth in commercial grids. Paul D Manuel et al [27] introduced a trust model to evaluate the grid and cloud resources by means of resource broker. The resource broker chooses appropriate grid/cloud resource in heterogeneous environment based on the requirements of user. This model considered metrics suitable for both grid and cloud resources. Trust enhanced resource broker evaluates the trust value of the resources based on the identity as well as behavioral trust. Junwei Huo et al [28] proposed a model in which trust management is combined with trust negotiation mechanism. This model provides the authorization and access control for the scientific data grid and aimed to enhance the grid security. This framework takes into account the aspects related to negotiations such as the policy language, negotiation protocol, and strategy to algorithms. This model presents features, such as trust ticket that can speed up the negotiation, supporting different negotiation protocols to carry on a negotiation, the enhanced policy language for credentials and policies, as well as the trust management strategy and the optimal negotiation strategy.

4. CONCLUSIONS

This paper presents various trust models proposed in recent years and analyzed the strategies of the models after introducing the concept of grid and trust. Much of the research is focused on trust based on recommendation, behavior and identity. The target of all the models is to provide the services qualitatively, uninterrupted manner and with trust. These models are experimented for various grid environments. This paper tried to provide a comprehensive survey and analysis of various models and related issues.

REFERENCES

[1] IBM Red Boo, "Fundamentals of Grid Computing", REDP-3613-00

[2] D. Chadwick. "Authorization in Grid Computing", Information Security Technical Report, Elsevier, 10(1)33:40, 2005.

[3] C. Castelfranchi, R. Falcone, B. Sadighi, Y-H Tain. Guest Editorial. Applied Artificial Intelligence, 14(9), Taylor & Frances, 2000.

[4] M. Waidner (editor). Ercim News, Special Theme: Information Security. No 49, 2002.

[5] P. Nixon, S. Terzis (editors). First International Conference on Trust Management. Lecture Notes in Computer Science, vol. 2692, Springer, 2003.

[6] C.D. Jensen, S. Poslad, T. Dimitrakos (editors). Second International Conference on Trust Management. Lecture Notes in Computer Science, vol. 2995, Springer, 2004.

[7] P. Hermann, V. Issarny, S. Shue (editors). Third International Conference on Trust Management. Lecture Notes in Computer Science, vol. 3477, Springer, 2005.

[8] T. Grandison, M. Sloman. A Survey of Trust in Internet Applications. IEEE Communications Survey and Tutorials, 3, 2000.

[9] A. Josang, R. Ismail, C. Boyd. A Survey of Trust and Reputation Systems for Online Service Provision. Decision Support Systems, 43(2), pp 618-644, 2007.

[10] Vivekananth.P "A Behavior Based Trust Model for Grid Security", International Journal of Computer Applications (0975 – 8887) Volume 5– No.6, August 2010, Published by Foundation of Computer Science.

[11] Renagaramanujam Srinivasan and Srivaramangai P. "A Comprehensive Trust Model for Improved Reliability in Grid.", *International Journal of Computer Applications* Volume5-No.7:1–4,

August 2010. Published By Foundation of Computer Science.

[12] Wang Meng; Hongxia Xia; Huazhu Song , "A Dynamic Trust Model Based on Recommendation Credibility in Grid Domain" , International Conference CiSE,2009 , Page(s): 1 - 4

[13] Hongmei Liao; Qianping Wang; Guoxin Li, "A Fuzzy Logic-Based Trust Model in Grid ", International Conference NSWCTC '09. 2009, Page(s): 608 - 614

[14] Gao Ying; Zhan Jiang, "A layered trust model based on behavior in service grid", 2nd International Conference ICACC, 2010 , Page(s): 511 - 515

[15] Kai Wei; Shaohua Tang, "A Multi-level Trust Evaluation Model Based on D-S Theory for Grid", International Conference CIS '09. 2009, Page(s): 411 - 415

[16] Changsong Ding; Yi Fu; Zhigang Hu; Peng Xiao, "A Novel Trust Model Based on Bayesian Network for Service-Oriented Grid" , Eighth IEEE/ACIS International Conference ICIS 2009, Page(s): 494 – 499

[17] Tie-Yan Li, Huafei Zhu, Kwok-Yan Lam: A Novel Two-Level Trust Model for Grid. ICICS 2003.

[18] Yuan Lin; Siwei Luo; Zhan Gao, "A Recommender Trust Model Based Behavior in Grid", Second International Conference FITME '09, 2009, Page(s): 568 - 571

[19] Wenming Huang; Peizhi Wen; Xianli Zeng; Zhenrong Deng, "A Trust Rating Model of Recommendation in Grid", Fifth International Joint Conference NCM '09, 2009, Page(s): 1982 - 1985

[20] Ryutov, T.; Li Zhou; Neuman, C.; Foukia, N.; Leithead, T.; Seamons, K.E, "Adaptive trust negotiation and access control for grids", The 6th IEEE/ACM International Workshop on Grid Computing, 2005.

[21] Wu Xiaonian; Zhang Runlian; Zhou Shengyuan; Ma Chunbo, "Behavior Trust Computation Model Based on Risk Evaluation in the Grid Environment", WRI World Congress WCSE '09, 2009, Page(s): 392 - 396

[22] Bhanwar, S.; Bawa, S, "Establishing and Evaluating Trust in a Grid Environment", 10th International Symposium ISPAN'09, 2009, Page(s): 674 - 678

[23] Azzedin, F.; Maheswaran, M., "Evolving and managing trust in grid computing systems", CCECE 2002, Page(s): 1424 - 1429 vol.3

[24] Woods W.K. Lai, Kam-Wing Ng, Michael R Lyu, "Integrating Trust in Grid Computing Systems", LNCS, vol.3251/2004, pg.887-890

[25] Tran, H.; Watters, P.; Hitchens, M.; Vijay Varadharajan, "Trust and authorization in the grid: a recommendation model", Proceedings. International Conference ICPS '05, 2005, Page(s): 433 – 436.

[26] Selvi, S. Thamarai; Balakrishnan, P.; Kumar, R.; Rajendar, K., "Trust Based Grid Scheduling Algorithm for Commercial Grids", International Conference on Conference on Computational Intelligence and Multimedia Applications, 2007, Page(s): 545 – 551.

[27] Manuel, P.D.; Thamarai Selvi, S.; Barr, M.I.A.-E., "Trust management system for grid and cloud resources", First International Conference on Advanced Computing (ICAC)-2009, 2009, Page(s): 176 – 181.

[28] Junwei Huo; Tingtang Ming; Hao Xu, "TTN: Towards Trust Negotiation for Grid Systems", International Conference on Computational Intelligence and Software E gineering (CiSE-2009), 2009, Page(s): 1 – 7.