Cross-Domain Role Mapping in Grid Computing Environment

Kaustav Roy* and Avijit Bhowmick†
Department of CSE, Dr. B.C. Roy Engg. College, Durgapur, WBUT, India

Lack of proper authorization techniques in grid computing technologies is a matter of much concern. The concept of virtual organizations which is at the core of computational grids further complicate the matter. Role-based access control (RBAC) is a security technology that is gaining importance now-a-days. It is used a lot in network security and can be effectively applied in grids too. Here a cross-domain policy mechanism for authorization is outlined based on the research of RBAC model at present, whereby equality is achieved between a local and a global role. The future work is to realize the model and implement it in practice.

PACS numbers:

I. INTRODUCTION

The dynamic and multi-institutional nature of grid computing environment[1] has produced challenging issues related to its security[2]. Grids are generally employed in high computation oriented tasks which needs secure collaboration among the various autonomous domains geographically dispersed at various places. A lot of research has been done on authorization in distributed systems but not much work has been done in real life distributed applications such as grids. The identity based authorization which was initially put into practice maps a users global identity(distinguished name) to a local account that has to be setup at every grid site. This is maintained in a list called Grid-mapfile. In a scalable grid infrastructure this should not be a likable solution for authorization purposes. The evolution of role based access-control mechanism is thus a natural choice in such a scenario[3][4].

A grid involves many management domains[1][6] and each domain is distributed in the network, so grid access control will be implemented in global management and local autonomy. The grid access control policy allots different access permissions and range to various global user in every local area. Users will be given roles according to his/her duty and permission. The user has to be restricted by access permission.

There is no standard solution for authorization in case of cross domain architectures. A service request may originate from one domain and may span several domains to accomplish its task. Thus the local role of the user has to be mapped to a global role and a proper authorization policy has to be envisioned for accepting or denying access rights to the user. In such a scenario, the model described in the following section comes in handy to put to practice.

*Email: kaust_1984@yahoo.co.in
†Email: avijit.bhowmick@gmail.com

II. CROSS-DOMAIN AUTHORIZATION MECHANISM

Cross-domain authorization[5] is a critical factor in multi domain access control policy. Generally the grid environment is composed of several domains and subdomains having different roles and responsibilities. The role of a node in one domain will vary greatly in some other domain. So the need is of some policy that could result in some equality of roles in various domains. Here the approach which has been taken is of a weighted tree. By combining the role of a node with that of its parent a global ranking has been established for access control purposes.

Role based access control has gained significance for authorization and for providing RBAC, some sets of policies are to be created for the Grid computing environment with the corresponding virtual organizations. In this paper we have developed a novel architecture and cross-domain policy mechanism for authorization in Grid which is based on RBAC, where access control is attained through global-local role of users and resource providers. The cross-domain architecture consists of the following components :

- Two domains A and B have been taken.
- Domain A consists of sub-domain A_u and A_r having user nodes and resource nodes respectively.
- Domain B consists of sub-domain B_u and B_r having user nodes and resource nodes respectively.
- There is an user authorization server1 for grid nodes from domain A_u and a resource authorization server1 for resource nodes from domain A_r.
- The user authorization server2 and resource authorization server 2 plays a similar role for domain B_u and B_r respectively.
- Rating servers 1 and 2 for two domains A & B store the rating of the sub domains.
- Global rating server is used for redirection purposes.

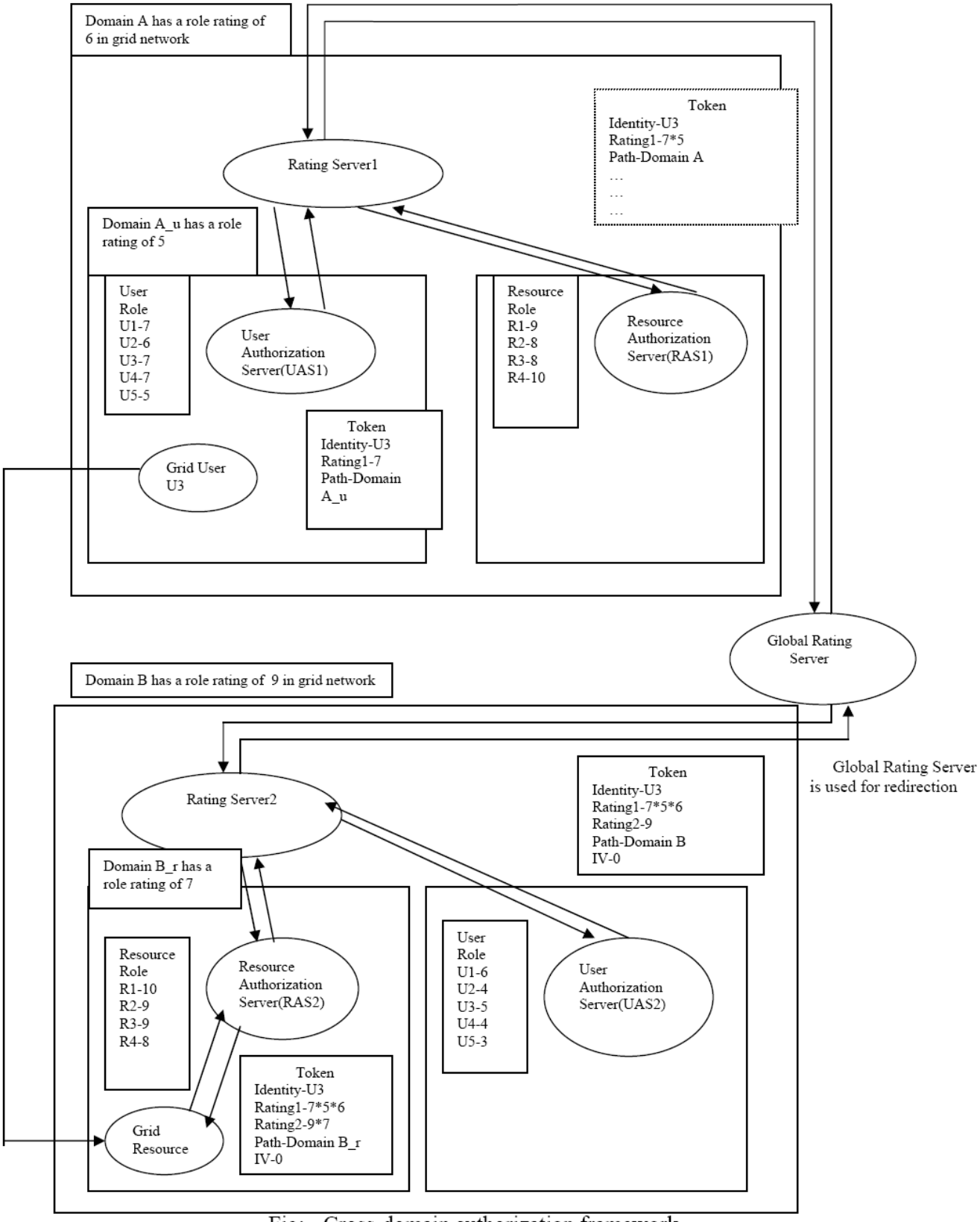

Fig:- Cross-domain authorization framework

U1,U2,….Un : Users
R1,R2,…..Rn : Resources
UAS1 : User Authorization Server of users at domain A
UAS2 : User Authorization Server of users at domain B
RAS1 : Resource Authorization Server of resources at domain A
RAS2 : Resource Authorization Server of resources at domain B

FIG. 1: Cross-domain authorization framework.

Using the concept of role ranking, local role of a node is mapped to a global role ranking[4] so that authorization can be effected seamlessly across multiple domains or virtual organizations.

The proposed cross-domain architecture consisting of several sub-domains, user nodes, resource providers, rating servers etc as components are shown in the diagram illustrated below in Fig-1.

Three parameters have been chosen to assign a role value to a user node-computation, storage & data transfer. Combining the values of these three parameters, eight different values can be generated,000111 in binary & converted into decimal, thus 7 denotes a node which can perform all the three functions. The ratings are given on a scale of 10. The sub-domains are also given a role ranking based on importance & hierarchy on a scale of 10. The resource nodes have been classified into three categories namely cluster systems, mainframes & dedicated storage devices having roles of 10,9 and 8 respectively. The requested resource upon receiving the request asks for authorization of the requestor to its local authorization server which thereby redirects it to the global rating server to fetch user credentials. The global server passes the request to the authorization server of the domain in which the user resides. The authorization server creates a token and sends its reply through the same path in reverse direction, in every step the role rating of the parent domains get weighted into the global rating of the user. After getting the final token, rank of the user is normalized on a scale of 1. An interaction value(IV)is also contained in the token which has a value 1 if there was an earlier interaction between the two or 0 in case of no interaction. The authorization server executes the algorithm described below and takes the final call to deny or grant the request. The whole procedure is as follows:

1. Grid user U3 from domain A_u seeks a resource from domain B_r sending his identity, path & requested operation.
2. The requested entity asks the resource authorization server RAS2 for its decision.
3. The authorization server implements the authorization algorithm for checking user credentials.
4. As the user is from a different domain, RAS2 takes the help of the global server and redirects it to the user authorization server UAS1 of the domain in which user resides.
5. The users role, rating etc are collected and UAS1 issues a token containing all those items. An interaction value IV is also given which has a value of 0 or 1. 1 signifies earlier interaction between the two and 0 signifies no interaction.
6. The token follows the same path in reverse direction and at every stage, the ranking of the parent domains get weighted, thus continuously modifying the global ranking.
7. RAS2 ultimately receives the token and normalizes the user rating on a scale of 1,obtaining the value 7*5*6/1000
8. RAS2 finds the minimum role to access the resource. It is equal to the role of the domain in which the user resides which is 5. Normalization is done in this case also to get the value 9*7*5/1000
9. Interaction value(IV) is then ascertained from the token.
10. Algorithm is being executed to take final call. Some fine-grained access control policy may also be included thereafter to further strengthen the authorization policy.

Some fine-grained access control policy may also be included thereafter to further strengthen the authorization policy.

III. ALGORITHM

1. Procedure for role mapping is executed(credentials).
2. Normalized global rating of user(NGU) is calculated from the value received in the token.
3. Minimum rated role to access resource in the domain is calculated, which is the role ranking of the domain in which user resides.
4. Normalized global rating(NGR) of that role is determined.
5. Interaction value(IV) is checked from the token.It is 0.1 for earlier interaction or 0 for no interaction.
6. If NGR + IV >= NGU,
   Accept user as authorized
   else
   return unauthorized user.

The procedure for mapping role is as under :

1. Accept token seeking user credentials.
2. Rating of domain is added to the global rating of the entity in the token.
3. Return the token.

IV. CONCLUSION

Access control is most vital parameter in Grids and thus it is of critical importance to introduce access control to impose Grid system security. The proposed role mapping authorization architecture will make it possible to practically authorize users at time of collaboration

TABLE I:

Serial No	Requestor & resource	Initial model proposed by us	Modified model proposed by us
1	U3(7) from domain A_u(5) seeks resource from domain B_r(7)	NGU NGR 0.21 0.31 Accept	0.21 0.31 Accept
2	U5(5) from domain C_u(6) seeks a resource from domain A_r(5)	NGU NGR 24. 0.18 Reject	24. 0.18 Reject
3	U4(3) from domain C_u(6) seeks a resource from domain D_r(5)	NGU NGR 14. 0.21 Accept	14. 0.21 Accept
4	U1(7) from domain E_u(8) seeks a resource from domain C_r(6)	NGU NGR 56. 0.38 Reject	56. 0.38 Reject
5	U2(4) from domain B_u(7) seeks a resource from domain D_r(5)	NGU NGR 24. 0.24 Reject	0.25 0.24 Reject
6	U2(4) from domain B_u(7) seeks a resource from domain C_r(6)	NGU NGR 0.25 0.33 Accept	0.25 0.33 Accept
7	U4(4) from domain B_u(7) seeks a resource from domain D_r(5)	NGU NGR 0.25 0.24 Reject	0.25 0.24 Reject
8	U1(7) from domain E_u(8) seeks a resource from domain C_r(6)	NGU NGR 56. 0.38 IV=1 to be added to NGR Accept	NGU NGR 0.56 0.38 IV=0.1 to be added to NGR Reject
9	U3(7) from domain A_u(5) seeks resource from domain B_r(7)	NGU NGR 0.21 0.31 IV=1 to be added to NGR Accept	NGU NGR 0.21 0.31 IV=0.1 to be added to NGR Accept
10	U2(4) from domain B_u(7) seeks a resource from domain D_r(5)	NGU NGR 0.25 0.24 IV=1 to be added to NGR Accept	NGU NGR 0.25 0.24 IV=0.1 to be added to NGR Accept

among multiple domains. The interactions once established can be used repetitively in future endeavors also in the form of interaction value. More fine grained access control policies can also be formulated in future. The future work is to realize the model and apply it in practice.

[1] I. Foster and C. Kesselman (eds.), The Grid 2: Blueprint for a New Computing Infrastructure, Morgan Kaufmann Publishers, 2003.

[2] Marty Humphrey , Mary R Thomson and Keith R Jackson, "Security for Grids", Proceedings of the IEEE, Vol 93, No 3, pp 644-652, March 2005.

[3] Hong Fan, He Xubin, and Xu Zhiyong, " Role-Based Access Control", Mini-Micro Systems,Vol. 21, pp. 198-200, February 2000.

[4] Ravi Sandhu, David Ferraiolo, D. Richard Kuhn, "The NIST Model for Role-Based Access Control: Towards a Unified Standard", ACM Workshop on Role-Based Access Control, 2000, pp47-63.

[5] G. Geethakumari, Dr. Atul Negi, Dr. V.N. Sastry, "A cross-domain role mapping and authorization framework for RBAC in Grid systems", International journal of Computer Science and Applications, Vol. 6 No. 1, pp. 1-12.

[6] Ian Foster, Carl Kesselman, Steven Tuecke, "The anatomy of the Grid: enabling scalable virtual organizations", 1st IEEE International Symposium on Cluster Computing and the Grid, Brisbane, Austalia, pp 6-7, May 2001.

[7] Jin Wu, Chokchai Box Leangsuksun, Vishal Rampure,"Policy-based Access Control Framework for Grid Computing", Proceedings of the Sixth IEEE International Symposium on Cluster Computing and the Grid, 2006.

[8] Rafae Bhatti, Elisa Bertino, Arif Ghafoor, "A Trust-based Context-Aware Access Control Model for Web-Services", Proceedings of the IEEE International Conference on Web Services, 2004.

[9] Pearlman, L., Welch, V., Foster, I., Kesselman, C. and Tuecke, S., A Community Authorization Service for Group Collaboration. IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.

[10] R. Alfieri et al. (EDG Security Co-ordination Group), "Managing Dynamic User Communities in a Grid of Autonomous Resources", Proceedings of Computing in High Energy and Nuclear Physics (2003).

[11] J. Vollbrecht, et.al. "AAA Authorization Framework" IETF RFC2904 http://www.ietf.org/rfc/rfc2904.txt?number=2904

[12] M. Lorch, D. Adams, D. Kafura, M. Koneni, A. Rathi, and S. Shah. The prima system for privilege management, authorization and enforcement in grid environments. In Proceedings of the 4th Int. Workshop on Grid Computing - Grid 2003, Phoenix, AZ, USA, Nov. 2003