A Study on User Authorization for Grid Resources

Seoung-Hyeon Lee, Won-Goo Lee and **Jae-Kwang Lee,** *Member, KIMICS*

Abstract—We suggest resource authorization system based on RBAC admitting someone to access resources. In existing grid environment, The authorization mechanism on user's resource is to give users an authority on the basis of DN(Distinguished Name) of proxy certificate and map file mapped in local system ID by one-to-one. In this case, it is difficulty in resource management such as each accounting management, memory resource, and disk resource, if the number of users, who want to use them is increased. To solve this problem, we specify the role of user's task in extension fields of his proxy certificate instead of the authorization mechanism of user's ID and propose resource authorization system being able to access his resource.

Index Terms—Grid, Resources, Authorization, RBAC, Certificate, User level

I. INTRODUCTION

As it partly and locally locates each resources in which grid provide security services such as authenticating users, giving the use of resources to authenticated user, and giving security against communication channel[1].

Currently, middleware of variety version developed to provide grid security service, but most populate Globus, using X.509 based certificate to provide for authentication and authorization service for computing resources. Because Globus provides authentication and authorization service for users through certificate and local system ID, easily and efficiently provides authentication and authorization service without modification in existing systems, but security service in Globus is only authentication for user, there is a today need for research of each authorization to authenticated subjects.

So, In this paper we analyzed problems about authentication and authorization for user on the basis of standard documents[2][3][4] and proposed new authorization system based RBAC mechanism.

This paper is divided into five parts as the followings. Chapter 2 discuss the requirements of security infrastructure to provide user authentication and authorization service in grid and middleware to provide service. Chapter 3 describes authorization system applying RBAC mechanism proposed this paper. Chapter 4 discuss implementation list to be used to our system, then compare a proposed security service to an existing services. Chapter 5 is conclusions.

Manuscript received May 10, 2004.

Seoung-Hyeon Lee is with department of computer engineering, Hannam University, Daejeon, 306-791 (phone : 042-629-7559, E-mail : shlee@netwk.hannam.ac.kr)

Won-Goo Lee is with department of computer engineering, Hannam University, Daejeon, 306-791 (phone : 042-629-7559, E-maile : wglee@netwk.hannam.ac.kr)

Jae-Kwang Lee is with department of computer engineering Hannam University, Daejeon, 306-791 (phone : 042-629-7559, fax : 042-629-7658, E-mail : jklee@netwk.hannam.ac.kr)

*This research was supported by the Program for the Training of Graduate Students in Regional Innovation which was conducted by the Ministry of Commerce, Industry and Energy of the Korean Government.

II. RELATED WORKS

A. GSI(Grid Security Infrastructure)

The prosperity of grid security has a big effect on security in distributed system. That is the goal of grid security mechanism focus on protecting system from user in traditional distributed system. That system security service is an important part in grid application services, especially grid environment includes special requirements to protect users data to be used in application and calculation, and because execution code can be begun in several places of network, means that potential, request of powerful method to verify disclose the source, authentication of code and its execution rapidly that code that is attacker can be executed are is required[5][6]. Also, grid resources have each engine security requirement and security policy collision possibility because is managed by different institution.

Security management in grid environment is giving much trouble by these reasons[7]. Is discussing about GSI solution in grid maintenance of public security working group that study security in grid and progress standardization process in reply to solve such problem. GSI is an alternative approach to inter-site security. We began developing it under the Globus research project4 to support distributed computing environments, or computational grids 5 which are similar to virtual organizations. GSI deals with inter-domain operations, bridging the different local security solutions of constituent sites.

B. Grid Middleware

Grid middleware or its software that worm that do so that can inflect resource had scattered to environment on a single computer like having belonged resource be. There is Globus, Legion, Condor with middle ware used mainly current[8]. Specially, Globus offers software infrastructure that do to use different resource scattered geographically like resource that belong to one virtual computer. And not that most feature of Globus adopts

staid programming methodology offers security, fundamental point service of communication and only resource management with object oriented model and in application programmer purpose necessary service selection and that being doing to support application program of various form by mixing be[9].

C. RBAC

RBAC is center concept is authorization that display rule, user who is constituent of role, and involved action in dynamic side.

Each constituents have the many-to-many relation among them. One user of this can be involved with one or more role and one role means having one or more user constituent. Role and authorization are similar with this. In this way, can add in role easily or remove user because have been allocated in role that user is not authorization. And authorization can amend easily operation without necessity to correct user when function of role changes or is deleted because connect with role only. Rule and involved authorization constituent of role decided limited[10].

III. PROPOSED AUTHORIZATION SERVICE

A. Local ID-Based Authorization Services

Current Globus is doing local system ID and mapping and give authorization to user draws subject DN (Distinguished Name) in grid user certificate with figure 1.

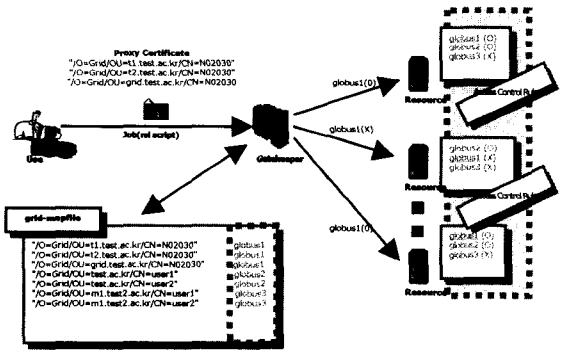


Fig. 1 Authorization Service based Local ID

User runs job in grid, in relevant system to deliver jobs file and proxy certificate to relevant system proxy certificate subject-DN local system of searching in '/etc/grid-security/grid-map', draw ID that conform and by ID of local system resource access is authorization.

Access for this resource LSF as well as access limited on OS dimension, PBS, job management program such as LoadLeveler depend apply can. Can be based on user ID to job management program and limit number of available CPU, memory capacity, run time.

B. Proposed Role-Based Leveled Authorization Services

Suffer much difficulty in system ID management problem and memory resource, management of disk resources that augment user proxy certificate subject-DN and ID of local system if there are many users when do mapping by one-to-one in old Globus user authorization system.

By these reason, existent Globus is wearing form that several subject-DN share one local ID. However, problem that happen keeps irrational cotton to apply all requirement of great many grid user when share single local ID.

In this paper, ID base is not, proposed user authorization system of certificate base that apply RBAC as show in figure 2.

Did so that add user authorization grade to extension field in certificate instead of authorization system of existent ID mapping way that explain before, and decide access authorization about resource of grid based on access policy defined by authorization grade and RBAC given.

Authorization Model for Resources. Role that user associates with user level to acquire permission for grid resource acquisition process need. User who connects in grid environment requests achievement of work, and make out this to RSL file. RSL file includes information related with user level, and use about resource in execution of this is used acquiring authority after flow RBAC module.

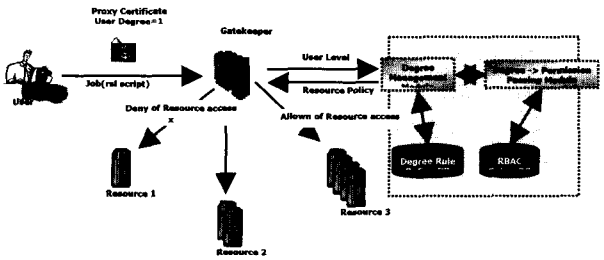


Fig. 2 Authorization Service based User level

Table 1 Units for Magnetic Properties

Component	Explanation
Degree Management Module	It is module that management user level.
Degree Rule Define DB	It is repository which store information about user level and link a policy rule.
Passing Module	User level and RBAC Rule function that change mapping achieve .
RBAC Policy DB	It is repository that store necessary contents in operation of RBAC system such as user role, operation, inheritance, duty separation, and restriction condition.

Figure 3 is show that express process that acquire access privilege for resource through RBAC module.

Grade defined to user certificate acquires part defined that flow role passing module, and search this in database. Role that acquire passes through process of object selection, and acquisition of permission about resource acquires final authority through the query that search objective/role/authorization database.

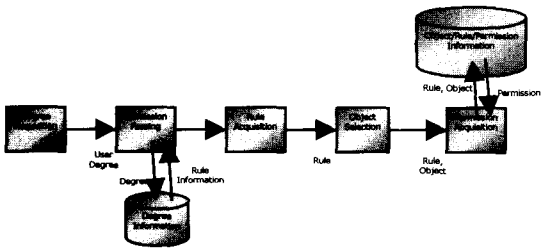


Fig. 3 Authorization processed by RBAC

User Level Field Application. In this paper, must define in certificate extension field area and add field that can mark user level in user proxy certificate to use user authorization system of role base that propose. If user transmits job file and proxy certificate to local system to run jobs, it has drawn user level in proxy certificate in local system. Examine that job file that user submits examining resource and policy each kind system resource amount used defined depending that access is possible can execute this deservedly searching authorization policy database about role of local predefined and decide execution availability of job.

Figure 4 is show adds user level item involved to certificate extension field.

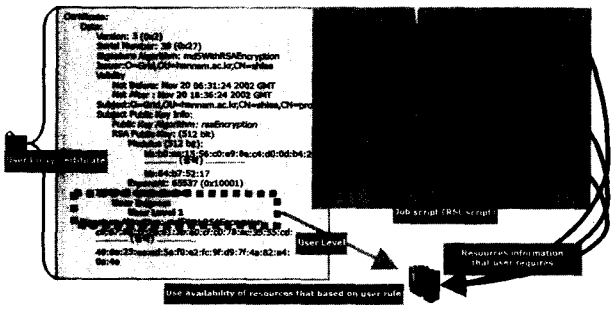


Fig. 4 User level in Certificate

IV. IMPLEMENTATION AND FUNCTIONAL COMPARISON

A. Implementation of Proposed System

Point of authorization system that propose in this paper adds extension field that mark access privilege for each resource in grid user certificate, and set in role that this is stored to database and give permission for different resource to process with grid user.

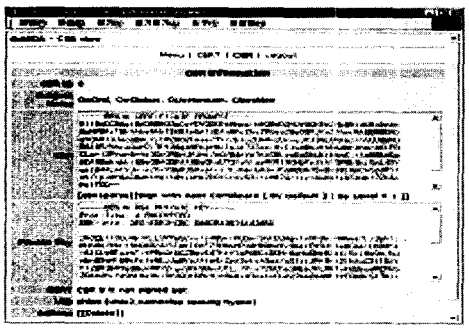


Fig. 5 Interface Screen Applying Authorization Service

Figure 5 is show screen that change development and certificate issuance system(GridCA V1.0) that distribute according to system proposed in a super computer center. Above screen can be screen that create actuality certificate about user certificate issuance request, and issue certificate that grade is given according to policy that predefine after certificate issuance manager confirms user certificate request to user.

B. Functional Comparison

Research to grid actively proceeding and, according to its realization effort actively proceeding in industrial, academy, and research, grid middleware that can use grid resource advanced, various middleware tools were developed. Globus, Legion, Condor are representative to these tool. In this paper, that being utilized most much current among various middleware for grid, likely Globus of standardization to base grid CA authorization service module embody. Table 2 is comparison with module embodied in paper that sees with authorization module had included in existent Globus.

Table 2 Comparison with an Existing Authorization Service Module

System Function	An existing system	Proposed system
Middleware	Globus 2.0	Globus 3.0
Grid CA	OpenSSL	KGrid v1.0 & CryptoAPI
User Authentication	authentication through certificate	authentication through certificate
User Authorization	Grid-mapfile based ID	Access policy database that have fetters in user level field of certificate
Server/Client	None	Grid CA and link a certificate management client

As shown in table 2, existing authentication services module to user authentication certificate problem that system proposed although took policy that apply local system ID and grid map-file to authorization can inflected authentication and authorization certificate, and apply RBAC and offered efficient side of user authorization, and happen in old system solve.

Also, through resources assignment policy of detailed role base, offered environment that can run various job.

V. CONCLUSION

In this paper we analyzed problems about authentication and authorization for user on the basis of standard documents and proposed new authorization system based RBAC mechanism to solve authorization problems on grid resource allocation. Features of our system can be summarized as following.

First, Our system decides resource allocation to its request by each user by relating user level defined in certificate with RBAC policy to authorize users. Second, Our system minimizes or reduces the difficulty in management of local ID or memory/disk waste. Third, Our system satisfies a variety of requirements of users by dividing the use of resources into each role.

We will research multi-level delegation of role authorization applying RBAC, design and implement system with role-based delegation of authorization for grid resources included authenticate by applying to real system.

REFERENCES

[1] Randy Butler Von Welch, Douglas Engert, Ian Foster, Steven Tuecke, John Volmer, Garl Kesselman, "A National-Scale Authentication Infrastructure", IEEE, December. 2000. pp. 60-6.

[2] IETF, "GSS-API Extensions", Internet Draft, February 2002.

[3] IETF, "Internet X.509 Public Key Infrastructure Proxy Certificate Profile", RFC 2459, August 2001.

[4] IETF, "Internet X.509 Public Key Infrastructure Certificate Management Protocol", RFC 2510, March 1999.

[5] Czajkowski, K., Fitzgerald, S., Foster, I. and Kesselman, C. "Grid Information Services for Distributed Resource Sharing", 2001.

[6] Gyung-Woo Kang, Hyung-Woo Park, "A Trends of Research and Implementation in Grid", Communication of the Korea Information Science Society, Vol 20, No. 2 pp.27, 2002. 2.

[7] Foster, I., C. Kesselman, and S. Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," International Journal of Supercomputer Applications, 2001.

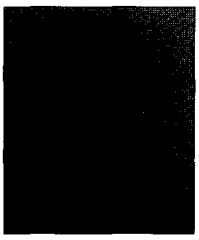
[8] http://www.gridforum.org/2_SEC/SEC.htm

[9] http://www-unix.globus.org/toolkit/

[10] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman "Role-Based Access Control Models", IEEE Computer, vol. 29, no. 2, Feb. 1996.

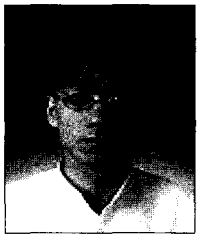
[11] Ravi S. Sandhu, "Role-Based Access Control Features in Commercial Database Management Systems", Proceedings of NISSC, 1998.

[12] Ravi S. Sandhu, "Role-Based Access Control Features in Commercial Database Management Systems", Proceedings of NISSC, 1998.



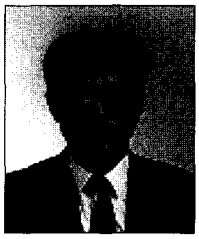
First A. Seoung-Hyeon Lee

He received the B.S degree in the Dept. of computer engineering from Hannam University, Korea in 2001. He received the M.S. degree in computer engineering from Hannam University, Korea in 2003. He is currently working towards the Ph.D. degree in Computer Engineering at Hannam University. His research interests are in grid computing and public key infrastructure.



Second A. Won-Goo Lee

He received the B.S degree in the Dept. of computer engineering from Hannam University, Korea in 2000. He received the M.S. degree in computer engineering from Hannam University, Korea in 2002. He is currently working towards the Ph.D. degree in Computer Engineering at Hannam University. His research interests are in network security and active network.



Third A. Jae-Kwang Lee

He received the B.S. and M.S. and Ph.D. degree in computer science from Kwangwoon University, Korea in 1984, 1986 and 1993, respectively. He was a Professor in the Department of Computer Science from 1986 to 1993 at Kunsan University He was a visiting Professor from 1997 to 1998 at University of Alabama. Since 1993, he has been with Hannam University, where he is currently a Professor in the Department of Computer Engineering. His research interests are Computer Network, Network Security, Public Key Infrastructure and Grid Computing.