2L-RBACG: a New Framework for Resource Access Control in Grid Environments

Hakimeh Alemi Baktash
Islamic Azad University-Qazvin branch,
Qazvin, Iran
alemi_ha@yahoo.com

MohammadReza Meybodi
Amir Kabir University
Tehran, Iran
mmeybodi@au.ac.ir

MohammadBagher Karimi
Islamic Azad University-Tabriz branch,
Tabriz, East Azerbaijan, Iran
m_karimi@iaut.ac.ir

Asgarali Bouyer
Faculty of Computer Science and Information Systems, UTM
81310, Johor, Malaysia
basgarali@sidwa.utm.my

Abstract

With the increasing complexity of dynamic and collaborative computing environments in Grid, access control has become a critical factor. Several approaches have been proposed in grid environment for scalable and efficient authorizations that are either VO-centric or Resource-centric. Reviewing different kinds of proposed authorization systems, we find out that VO-level and Resource-level authorization systems look at two different aspects of the grid authorization. Indeed, they complement each other, and can be implemented together to provide a holistic authorization solution. For this purpose, we propose a new access control framework which uses an extended two level RBAC model in Grid computing environments. By separating the administrations of users by VO level policies and mapping these policies to resources by resource or service providers, our scheme provides decentralized, autonomous, and fine-grained security management. The art of this approach is support of high flexibility in policy configuration, dynamically modifying authorization policies and reducing the cost of policy management.

1. Introduction

Grid computing has been becoming a general platform for automatic, transparent and pervasive collaborations between various Resource Providers (RPs) and consumers which are typically grouped towards a common goal into virtual organizations (VOs) [1, 4]. As a fundamental problem, access control (particularly authorization) is a critical factor for many applications where sensitive operations need to be granted to only authorized entities (subjects) from different organizations (or domains). Particularly, in a Grid-based application, a resource or service provider wants to specify who can access its shared objects. However, heterogeneity and dynamicity of such environments make the definition and management of policies complicated. Since usually, (1) access requests come from different domains or organizations within a VO and users can join or leave the VO community dynamically, and (2) a domain or organization has its own policies determining who can access resources shared by other domains in the community, and (3) these policies can be changed without notice of other domains [3]. Frequently, an authorization decision may require security policies from multiple resources, typically from resource providers and VO. Therefore, authorizations should ensure the ultimate control of resource owners, and autonomous authorization administration in distributed communities.

Obviously, traditional identity-based authorization mechanisms become infeasible in grid environments. Because a provider of resources can't determine subject identities when define policies. Supporting role-based access control (RBAC) [7, 8, 9] is desirable in Grids. RBAC shows clear advantages over traditional access control models. The essential concept of RBAC is to define roles which are assigned to a collection of permissions that can be invoked to access protected resources. A user is assigned to a set of roles to obtain the permissions of the roles.

Several approaches have been proposed in grid environment for scalable and efficient authorizations that most of them have used RBAC as their access control model. Often these grid authorization systems are either VO-centric or Resource-centric. Reviewing different kinds of proposed authorization systems, we find out that

VO-level and Resource-level authorization systems look at two different aspects of the grid authorization. Indeed, they complement each other, and can be implemented together to provide a holistic authorization solution.

In this paper we present a two-level role-based access control framework in grid environment. 2L-RBACG framework provides two aspects of grid authorization management. One aspect assumes grid to be composed of one or more VOs from several users and resource providers (or services), and another aspect treats whole grid as a series of independent, interrelated and dynamic resource groups which are provided to users of a VO. Thus, administration of access control is done in two levels: management of resource independent RBAC polices in VO-level and mapping of Resources to these policies which done in resource-level.

The paper is organized as follows. Section 2 addresses some related works and compression them. Two-level authorization schema and administration framework are illustrated in section 3. An architecture design and evaluation of 2L-RBACG is provided in section 4 and 5, respectively. Section 6 has some conclusion.

2. Related works

In this section, we will discuss some authorization systems that have been used in popular grid implementations and other distributed systems. The grid authorization systems can be mainly divided into two categories: VO-level systems and resource-level systems. VO-level systems have a centralized authorization system which provides credentials for the users to access the resources. Resource-level authorization systems, on the other hand, allow the users to access the resources based on the credentials presented by the users [3].

In the next subsections we will discuss in detail about some grid authorization systems which operation focus is one of these levels.

2.1. VO-Level authorization systems

VO-level grid authorization systems are centralized authorization for an entire Virtual Organization (VO). These types of systems are necessitated by the presence of a VO which has a set of users, and several Resource Providers (RP) who own the resources to be used by the users of the VO. Whenever a user wants to access certain resources owned by a RP, he/she obtains a credential from the authorization system which allows certain rights to the users. The user presents the credentials to the resource to gain access to the resource. In this type of system, the resources hold the final right in allowing or denying the access to the users.

In Community Authorization Service (CAS) [3], the owners of resources grant access to a community account as a whole. The CAS server is responsible for managing the policies that govern access to a community's resources. It maintains fine-grained access control information and grant restricted GSI [17] proxy certificates to the users of community. CAS completely removes access control from local resource or service. CAS also has scalability problem because of central management.

Virtual Organization Membership Service (VOMS) [11] is a grid access control system similar to CAS. VOMS integrates the role concept. VOMS server signs an attribute certificate that includes role information (in contrast to direct permission in CAS) and dispatches to each user. Just like CAS, VOMS is also centrally managed and has the limitation of scalability.

Enterprise Authorization and Licensing Service (EALS) [12] has been developed in Software Engineering Technology Labs. The EALS system has been built with the focus on enterprises and authorization required to cater to the users there. The design of EALS is based on some principles which make it different from CAS and VOMS systems. Unlike CAS or VOMS, EALS is based on the pull based model where the credentials are pulled from the EALS system. Other difference arises from integration of EALS with Standards. EALS uses SLAM for transferring authorization credentials. Finally, as VOMS, EALS allows access to certain resource based on the role a user has, and the permission the role has for the set of resources.

2.2. Resource-Level authorization systems

Unlike the VO-level authorization systems, which provide a consolidated authorization service for the virtual organization, the resource-level authorization systems implement the decision to authorize the access to a set of resources.

Akenti [13] is an access control architecture where all the resources are controlled by multiple authorities (stakeholders). In Akenti, stakeholders [18] create and sign user-condition certificates [19] that define conditions which must be satisfied by the user before giving access permission to a resource. Attribute authority creates and sign attribute certificates defining the user attributes that must be asserted. Certificate authority creates and signs identity certificates. Akenti is a success attempt to create and manage policy certificates [19] and use these certificates to make secure policy-based access decisions. But in Akenti, the management of certificates is burdensome, and it cannot provide large scalability because of the centralized management of policies.

Privilege and Role Management Infrastructure Standards (PERMIS) [13] is a policy driven RBAC Privilege Management Infrastructure (PMI). The policy is written in XML and stored in X.509 attribute certificates (AC) [8] in the local LDAP [20] directory. The

credentials may be widely distributed. The access decision is made centrally by the ADF (Access Decision Function) module of PERMIS. How to combine different participant domains' policies has not been solved.

GridMap [2] is the earliest authorization system used in Globus [21]. Though more sophisticated systems like Community Authorization Service (CAS) and other authorization systems discussed in this paper have been developed, GridMap is still one of the most widely used authorization system is Globus mainly due to its simplicity. In a GridMap system, the static policies of which user can access the resource and how is placed in each local resource. The decision to grant access to a resource is based on the information present in the GridMap file. As mentioned earlier, this authorization system is simple to implement and does not require too much overhead. However, lack of scalability really hampers the use of GridMap system in a wide scale.

3. Overview of 2L-RBACG system design

In this section we describe a design of a new authorization framework which aim is leveraging the operation of legacy one-level systems by using a two-level approach.

Figure 1 provides a high-level overview of 2L-RBACG system using numbered arrows to represent a general sequence of actions. In step 1, VO-administrator creates RBAC policies. This level of administration includes defining roles and role-permission assignments. Then these roles (or privileges) are granted to grid users. Also, the granted privileges can be delegated among and between grid users, administrators and other entities (step 2 and 3, respectively). Step 4 shows that grid users holding privileges can manage the use of their privileges by selecting a subset of them for use with a specific access. In this level, the access control policies are resource-independent and globally accessible with resource administrators. As shown in step 5, Resource administrators map their resources to these policies autonomously. For example, a resource provider (RP1) may select a policy which assigns 'update' permission to 'student' role; while RP2 is free to don't this selection. In step 6, the grid users can create a specific grid resource request by supplying subset of selected privileges.

4. 2L-RBAC model and administrations

4.1. 2L-RBAC model

In contrast with RBAC96 model, 2L-RBAC eliminates all resource dependencies from RBAC policies. Similar to classic RBAC model, in 2L-RBAC there are three basic concepts: users, roles and permissions. Users are assigned to roles, and the roles grant/deny permissions to/from specified tasks. In a session, user activates a subset of assigned roles and obtains the permissions assigned to these roles. By configure permission-role and user-role assignments, many security objectives can be achieved efficiently. Other concepts such as role hierarchy and constraints are supported in our model, too.

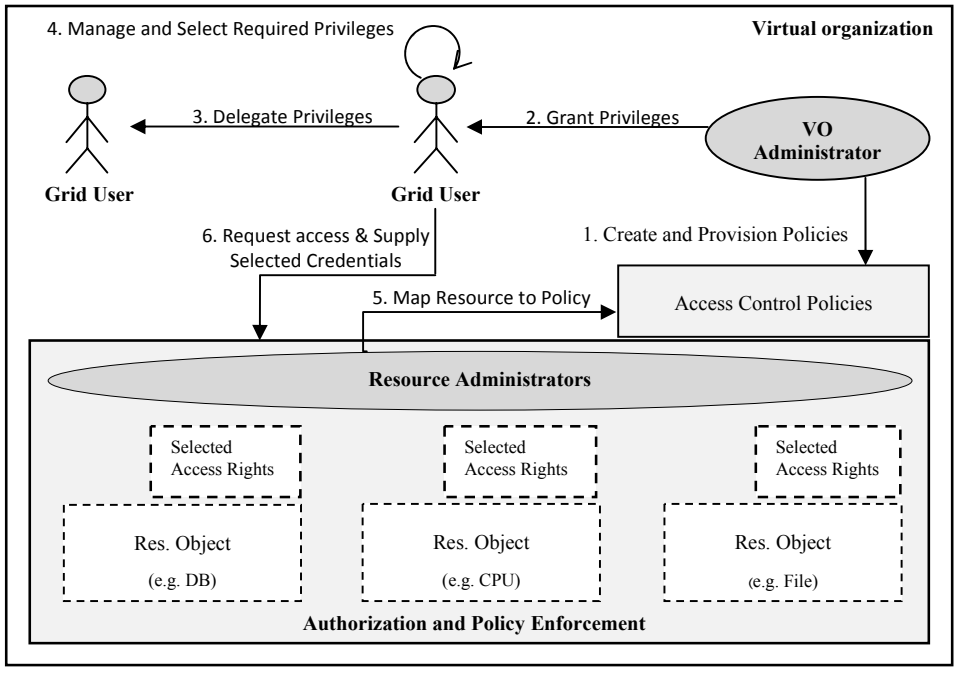

Figure 1. **2L-RBACG system overview**

4.2. Administration of 2L-RBAC policies

2L-RBAC distributes authorization policy management among VO and resource administrators. In VO-level, Global resource-independent RBAC policies are defined by VO-administrator. These policies include role definition and user-role and role-permission assignments which are determined by organization and application requirements. At the other hand, mapping of resources to these policies is done in resource-level. We choose PKI/PMI infrastructure for implementation of this model. Thus, we developed our system with x.509 ACs. The ACs can be classified into two categories; namely role ACs that store the users' roles and policy ACs that store the authorization policies. The authorization policies specify which roles have what rights. Access rights are not directly associated with specific target resources. In fact, policies are completely resource-independent; in our schema resource information including resource DNS name and applied policies' ID (subject of policy ACs in this schema) is centrally maintained in (or hierarchically distributed among) LDAP server(s). LDAP entries express mapping of resources to VO-level policies. Configuration of these LDAP servers (e.g. select or remove policies from LDAP) is left to resource administrators.

Multi-level administration provides an autonomy mechanism that is so vital to grid. However, local administrators should adhere to RBAC policies which are globally defined by VO administrator. This provides a unified view of VO policies and authorization decisions can be made consistently across a VO.

The main benefits of such model are Decentralized policy administration, Resource Provider and VO Independence, and Consistent View and Flexibility of Policy Infrastructure.

5. 2L-RBACG system architecture and authorization schema

The 2L_RBACG system architecture and authorization process is illustrated in Figure 2. This framework is based on a centralized authentication system which validates the user credential and sends an authentication token back to the grid entry point. The grid entry point can be any interface which redirects the request to the centralized authentication system. The authenticated request is bundle with the subset of user selected privileges and is passed to authorization system.

The authorization and enforcement part of this architecture has four primary components. Policy Enforcement Point (PEP), Policy Decision Point (VO-level PDP and Resource-level PDP), and Policy Repositories (VO-level and resource-level LDAP servers). The access request including subject DN (x.509 Distinguished Name), target URL, and operation name are pushed to PEP. Also, Users' role ACs are obtained in push mode as access privileges. PEP then validates the privileges accompanying the request and requests an authorization decision during the following sequence of actions: The central PEP asks Resource-level PDP to determine which RBAC policy set applied to the

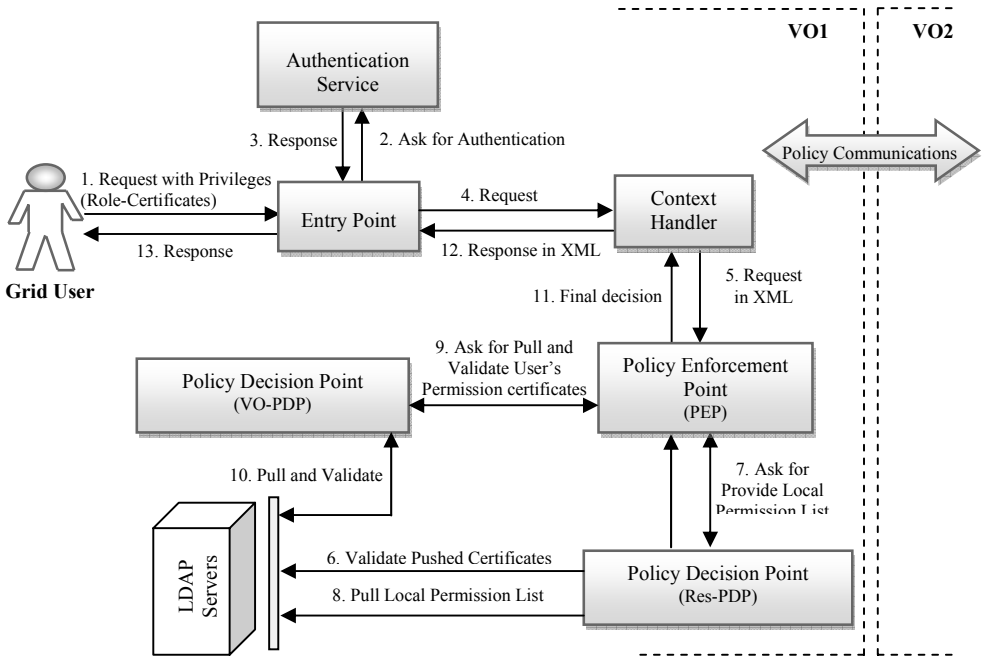

Figure 2. **2L-RBAC system architecture and authorization process**

requested resource. Resource-level PDP queries hierarchical distributed LDAP server(s) to provide local policy list. Finally, associated policy IDs (permission AC's SNs in this infrastructure) is send back to the PEP. Receiving local policy list, PEP sends a token including this list and requested action to VO-level PDP. VO-level PDP pulls related RBAC policy sets or permission certificates form LDAP server(s). VO-level PDP then makes a response including a yes/no decision. After receiving VO-level response, PEP sends back to the entry point the requested action result or an exception.

Passing of security Tokens between PEP and entry point is done via a Context Handler component. Context Handler is an entity that converts access requests in native request format to XML form and converts access decision in XML form to native response format.

Policy communication relationships are considered to handle secure policy communication among policy administrators in different domains or virtual organizations. It ensures that the communication is confidential, authenticated, integrated and reliable. Policy communications provide defining cross-VO or cross-resource policies, too.

6. Evaluation

In order to evaluate the operation of 2l-RBACG system, we inspect the framework based on some major issues that are important in grid environments such as scalability, security, interoperability, and response time.

Scalability: there are two different types of scalability: performance scalability and administrative scalability. Number of users is the primary measure for the former type of scalability. The authorization system should not be a bottleneck in the grid infrastructure and should scale even if the number of users increase significantly. In case of performance scalability, 2L-RBACG is relatively scalable, since it has a hybrid push/pull architecture where role credentials are pushed to the PEP and other policy certificates are pulled by the PDPs. Therefore, it scores higher than fully pull-based models. Systems with centralized administration have high administrative scalability. Modifying authorization policy in 2L-RBACG system requires two steps: updating the RBAC policies in the policy store, and updating the mapping of resources to those policies. In our system, the modification of authorization policy is inexpensive. The RBAC policies can be updated by VO-level authorization manager. Updating of policies which are applied to a specific resource is left to the resource providers. The worst case cost of policy modification (that affects every user, every role and every resource) in our infrastructure is (U * P) + R, while in other one-level authorization system the modification cost is U * P * R in worst case (where U is the number of users, P is the number of permissions and R is the number resources, in the VO). The vast majority of policy changes, however, only require modifications along one of these three dimensions.

In large Grid environments, many resources are not static, but they change dynamically. In our system, resources and policies that govern them are maintained separately. Resource administrators can freely update information about by changing the information stored in LDAP server(s). The resource-independent policies in the VO-level policy store will be unaffected by these resource changes. In contrast to this architecture, other authorization systems such as PERMIS, Akenti, and CAS all store policies that contain resource information directly. In these systems, there is no upper bound on how many policies will be affected when a resource changes.

Putting all results together we can rank the introduced systems as figure 3 and 4.

Security: Because of using public key infrastructure, 2L-RBACG system have high immunity against masquerade attacks. However, it because of using push model for receiving user privileges, a DoS attack can easily bring our authorization system down. It is possible by sending a lot of authorization requests to the 2L-RbACG. Each request may flow over a SSL channel which authenticates the user. However, that does not stop a malicious user from sending thousands of connection requests per second. By similar analysis the ranking of

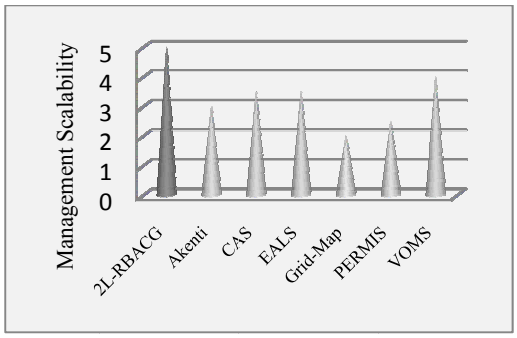

Figure 3. **Management scalability of 2L-RBACG towards other systems**

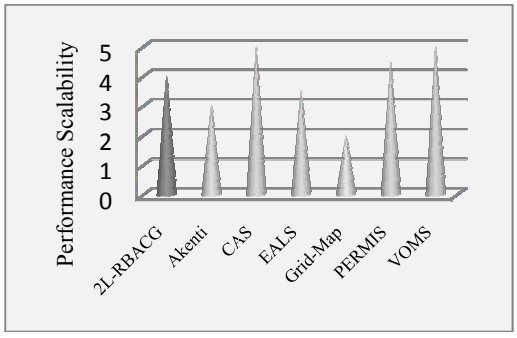

Figure 4. **Performance scalability of 2L-RBACG towards other systems**

proposed system security toward other systems is estimated as figure 5.

Interoperability: One of the ways that most systems try to tackle interoperability issues is through standardization. Systems that use SAML or XACML as policy expression or security tokens format, have high degree of interoperability. The proposed system doesn't be integrated with such standard infrastructure. However, in contrast with systems as Akenti and VOMS that use own certificate formats, 2L-RBACG uses standard X.509 certificates for policy expression. So, our system scores relatively well in case of interoperability (figure 6).

Response Time: Simulation and comparison of 2L-RBACG system with other one-level authorization systems is done based on similar qualifications of Markov chains which supposes one server for each operating stage. Also, λ and μ are defined as arrival and service rates, respectively. We assume that PDP operations to be as main service and comparison point in these authorization systems. The basic mathematical simulation of a one-stage operation with dispatched queues of user queries will be as which are expressed in equations (1) and (2); Where, Pn is The probability of being n entities in the system and E(T) is the average response time.

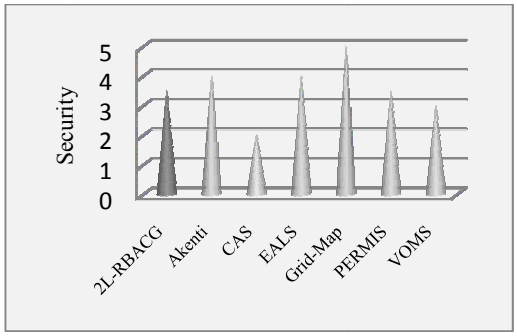

Figure 5. **Security of 2L-RBACG towards other systems**

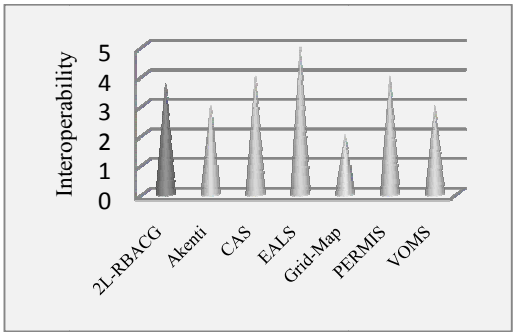

Figure 6. **Interoperability of 2L-RBACG towards other systems**

$$Pn = \left(\frac{\lambda}{\mu}\right)^{n}\left(1-\frac{\lambda}{\mu}\right) \quad (1),$$

$$E(T) = \frac{\left(\sum_{n=0}^{\infty} n \times Pn\right)}{\lambda} = \frac{1}{\mu \times \left(1-\frac{\lambda}{\mu}\right)} \quad (2).$$

These equations can be extended to a multi-stage operation with one server for each operation. According to figure 7, the simulation results of a two-stage operation in this simulation bed are as equations (3) and (6); where Pn,m is the probability of being n and m entities in system queues and q is the probability of failed requested in first queue.

$$Pn,m = \alpha^{n} \times (1-\propto) \times \beta^{m} \times (1-\beta) \quad (3)$$

$$\text{Where } \alpha = \frac{\lambda}{\mu 1} \quad (4),$$

$$\text{And } \beta = \frac{(1-q)\mu 1}{\mu 2} \quad (5).$$

In consideration of equation (3) and independency of queues in two stages, the average response time of this system, E(T), will be computed as follow:

$$E(T) = \frac{\sum_{n=0}^{\infty} n \times Pn \times \sum_{m=0}^{\infty} m \times Pm}{\lambda} = \frac{1}{(\mu 1-\lambda)} \times \frac{(1-q)\mu 1}{\mu 2-(1-q)\mu 1 \mu 2} \quad (6).$$

Final results of 2L-RBACG system simulation and comparison with existing one-level systems show that our system can claim a closing competition with resource-level systems such as PERMIS or Akenti but Average response time of this system is greater than VO-level centralized systems such as VOMS or CAS. This is illustrated in figure 8.

7. Conclusion and Future Work

We propose a 2-LRBAC model and apply it in authorization administration of Grid environments. The main feature of the model is to leverage the control of user management by a VO, while preserve the final control of permissions to shared resources by resource providers. The benefits of our approach are decentralized security management and fine-grained permission control. As a result, our model can support dynamically modifying authorization policies and consistent view and flexibility of policy infrastructure.

We are extending our model and authorization schema in different aspects. First of all, mapping of global roles to local roles will be included in our future work. Secondly, we will extend our schema to support dynamic contest-aware permissions. Thirdly but not finally, we will explore authorization management in a fully service-oriented environment, which gains increasing interest since Grids have been becoming service-oriented architectures.

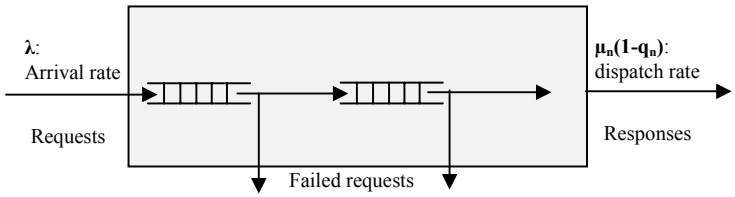

Figure 7. **Basic bed for response time simulation**

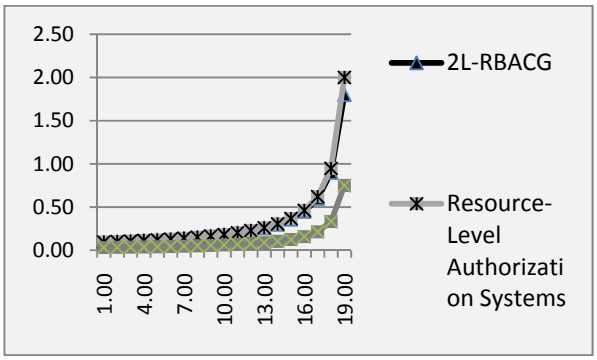

Figure 8. **Average response time of 2L-RBACG towards one-level and two-level authorization systems**

8. References

[1] I. Foster, "The Grid: A New Infrastructure for 21st Century Science", Physics Today, vol. 55, no. 2, pp. 42-47, 2002.

[2] I. Foster and C. Kesselman, "The Grid: Blueprint for a New Computing Infrastructure", Morgan-Kaufman, pp. 2-48, 1999.

[3] I. Foster, "What is the Grid? A Three Point Checklist", GridToday, 2002.

[4] A. Chakrabarti, "Grid Computing Security", Springer Berlin Heidelberg, pp. 77-114, 2007.

[5] I. Foster, C. Kesselman and S. Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organization", International Journal of Supercomputer Applications, vol. 15, no. 2, 2001.

[6] X. Zhang, "Flexible Authorization with Decentralized Access Control Model for Grid Computing", 10th IEEE High Systems Engineering Symposium, 2007.

[7] R.S. Sandhu, E.J. Coyne, H.L. Feinstein and C.E. Youman, "Role-based Access Control Models", IEEE Computer, vol. 29, no. 2, pp. 38-47, 1996.

[8] B. Bouwman, "Rights Management for Role-Based Access Control", 5th IEEE CCNC, 2008.

[9] D.W. Chadwick and A. Otenko, "RBAC Policies in XML for X.509 Based Privilege Management", Proceeding of the 17th International Conference on Information Security, 2002.

[10] L. Pearlman, V. Welch, I. Foster, C. Kesselman and S. Tuecke, "A Community Authorization Service for Group Collaboration", Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, Monterey (CA), pp 50-59, 2002.

[11] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Frohner, A. Gianoli, K. Lorentey and F. Spataro, "VOMS, an Authorization System for Virtual Organizations", 1st European Across Grids Conference, Santiago De Compostella (Spain), 2003.

[12] D. Chadwick and S. Otenko, "A Comparison of the Akenti and PERMIS Authorization Infrastructures in Ensuring Security in IT Infrastructures", Proceedings of the ITI First International Conference on Information and Communications Technology, 2003.

[13] M.R. Thompson, A. Essiari, K. Keahey, V. Welch, S. Lang and B. Liu, "Fine-Grained Authorization for Job and Resource Management Using Akenti and the Globus Toolkit®", Lawrence Berkeley National Laboratory, Paper LBNL-52976, 2003.

[14] D. Chadwick and O. Otenko, "The PERMIS X.509 Role Based Privilege Management Infrastructure", ACM SACMAT, Lake Tahoe (CA), pp. 135-140, 2002.

[15] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Gianoli and F. Spataro, "Managing Dynamic User Communities in a Grid of Autonomous Resources", Computing in High Energy and Nuclear Physics, La Jolla, California, 2003.

[16] 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", Proceedings of the 12th IEEE International Symposium on High Performance Distributed Computing, 2003.

[17] D.A. Haidar, N. CuppensBoulahia, F. Cuppens and H. Debar, "An Extended RBAC Profile of XACML", Proceeding of the 3rd ACM workshop on Secure Web Services, Workshop On Secure Web Services, pp. 13-22, 2006.

[18] Y. Deng, X. Guo and X. Niu, "A New Design Scheme of Role-Based Access Control Based on PKI", Proceeding of the First IEEE International Conference on Innovative Computing, Information and Control, ICICIC, vol. 3, pp. 669-672, 2006.

[19] M. Lorch and D. Kafura, "The PRIMA Grid Authorization System", International Journal of Grid Computing, vol. 2, no. 3, pp. 279-298, 2004.

[20] S. Fugkeaw, P. Manppanpanich and S. Juntapremjitt, "Exploiting X.509 Certificate and Multi-Agent System Architecture for Role-based Access Control and Authentication Management", Proceedings of 7th IEEE International Conference on Computer and Information Technology, 2007.

[21] D. Zou, L.T. Yang, W. Qiang, X. Chen and Z. Han, "An Authentication and Access Control Framework for Group Communication Systems in Grid Environment", Proceeding of 2[1st] IEEE International Conference on Advanced Networking and Applications, 2007.

[22] H. Jin, W. Qiang, X. Shi and D. Zou, "RB-GACA: a RBAC based Grid Access Control Architecture", International Journal of Grid and Utility Computing, vol. 1, no. 1, pp. 61-70, 2005.

[23] A.L. Pereira, "Role-Based Access Control for the Open Grid Services Architecture - Data Access and Integration (OGSA-DAI)", A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, 2007.