Journal of Computer Science 10 (12): 2576-2583, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.2576.2583 Published Online 10 (12) 2014 (http://www.thescipub.com/jcs.toc)

ENHANCING THE PERFORMANCE OF ADVANCED FINE-GRAINED GRID AUTHORIZATION SYSTEM

[1,2]Maizura Ibrahim, [2]Hamidah Ibrahim, [2]Azizol Abdullah and [2]Rohaya Latip

[1]Department of Technical Support, Malaysian Nuclear Agency, 43000 Kajang, Selangor, Malaysia
[2]Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

Received 2014-08-18; Revised 2014-11-04; Accepted 2014-12-29

ABSTRACT

Grid computing is a system that coordinates distributed resources using standards, open, general purpose protocols and interfaces to provide nontrivial quality of services. Usage Control model (UCON) is a new emerging authorization framework that combined features of traditional access control, trust management and digital right management in one abstraction. Adoption of UCON improved the fine-grain of grid authorization policy. The major problem of the UCON based authorization is the finer-grain the authorization, the higher overhead will be impacted to the system. This is because fine-grained authorization required very complex policies to define rules accurately. To evaluate complex policies is very time consuming as the system needs to check rules by rules in each policy for each resource in order to produce the access result, resulting in lower authorization performance. This limitation is crucial for large collaborative environment like grid where user and resource keep increasing year by year. Therefore, a mechanism to reduce the number of checking during authorization process is needed. In this study we propose a mechanism to reduce the number of rules checking by eliminating irrelevant set of rules. The irrelevant rules are determined by the dependency of rules model. Our simulation result shows that our technique able to further reduce the number of rules checking in grid authorization system compared to previous method. The checking process also can be skipped for certain rules using our method.

Keywords: Grid Computing, Grid Authorization, Security Policy, UCON

1. INTRODUCTION

Grid computing aimed to enable resource sharing for large project collaborations to solve one big problem. Foster and Kesselman (2004) defined a grid as a system that coordinates distributed resources using standards, open, general purpose protocols and interfaces to provide nontrivial quality of services. The Virtual Organization (VO) concept makes the resource sharing in grid became possible. A VO is a group of individuals and associated resources and services located within multiple administrative domain but united by a common purpose (Welch *et al*., 2003). The need to support and manage users and resources within VOs introduces challenging security issues (Foster *et al*., 1998). While scalability, performance and heterogeneity are the objectives for any distributed system, the nature of VOs in grid demands a fine-grained authorization system to manage the usage of resource (Keahey *et al*., 2003). Authorization in grid can be defined as the act of providing and checking the authority of a user or a job on a specific set of resources (Chakrabarti, 2007).

A traditional mode of security operation demand users to have a user account (i.e., username and password) to establish direct relationships with resources they want to use but did not own. In grid, both resource pool and user pool are large and dynamic, thus implementing traditional model becomes unmanageably complex (Keahey *et al*., 2003). Grid security requirements are different from a common distributed

Corresponding Author: Maizura Ibrahim, Technical Support Department, Malaysian Nuclear Agency, 43000 Kajang, Selangor, Malaysia

environment, hence it needs the adoption of a complex security and trust model (Foster *et al*., 1998). Some of the requirements mentioned in (Foster *et al*., 2001; Welch *et al*., 2003; Foster and Kesselman, 2004; Humphrey *et al*., 2005) included naming and authentication, authorization, privacy, trust, intrusion detection, security policy exchange and enforcement. To address those requirements, various grid security solutions have been proposed. Pearlman *et al*. (2002) introduced the Community Authorization Service (CAS) to address the problem of scalable representation and enforcement of access policy within distributed virtual communities. CAS stores a database of VO policies and issues proxy certificates that embed CAS policy in it to the grid users. However, CAS policy is coarse-grained because it only specifies which local services can be accessed by the grid user. The Virtual Organization Membership Service (VOMS) proposed by (Alfieri *et al*., 2005), the Privilege and Role Management Infrastructure Standards Validation (PERMIS) (Sinnott *et al*., 2005) and Akenti (Thompson *et al*., 2003) enhanced the solution by incorporating roles and capability. However, the access rights produced by those solutions are still considered static because the same user will have the same access rights at each access. To update the access right, administrator intervention is required. Moreover, no further access controls are executed by the system once the standard authorization service granted the access right to a user. All the previously mentioned solutions adopted the traditional access control model such as Discrete Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC). The shortcomings of the traditional access control model are they cannot support ad hoc collaboration, dynamic collaborative environment and continuity enforcement of security policy (Zhang *et al*., 2008).

Adoption of advanced access control called the Usage Control model (UCON) (Park and Sandhu, 2002; Park, 2003; Park and Sandhu, 2004; Zhang *et al*., 2004; 2005) in grid are proposed by (Zhang *et al*., 2008; Stagni, 2009; Martinelli and Mori, 2010). UCON is a new emerging authorization framework that combined features of traditional access control, trust management and digital right management in one abstraction (abstraction mean it is independent of any specific existing language, policy or model, which is a major design of UCON). Zhang *et al*., (2008) specify the UCON policies using the eXtensible Access Control Markup Language (XACML) whereas Martinelli and Mori, (2010) create a specific UCON policies language based on process algebra called POLPA. Apart from that, Stagni (2009) proposed the enforcement of UCON policy model using theoretically goal-based approach. All of them focus on improving the fine-grained of the authorization. In this context, fine-grained authorization means the security policy can describe authorization rules which exist in grid stakeholders' mind specifically and accurately using very high expressive language. In (Ibrahim *et al*., 2012) we have proposed a conceptual framework to facilitate intergrid policy integration based on UCON with semantic elements.

The major problem of the UCON based authorization is the finer-grained the authorization, the higher security overhead will be impacted to the system. This is because fine-grained authorization required very complex security policies to define rules accurately. To evaluate complex security policies is very time consuming as the system needs to check rules by rules in each policy for each resource in order to produce the access result, resulting in lower authorization performance. This limitation is crucial for large collaborative environment like grid where user and resource keep increasing year by year. Therefore, a mechanism to reduce the number of checking during authorization process is needed. In this study we propose a mechanism to reduce the number of rules checking by eliminating irrelevant set of rules. The irrelevant rules set are determined by the dependency of the rules to other rules.

We have given the overview of our research in section 1. Section 2 will discuss about the related work. Section 3 describes a methodology of how we model rules dependency base on some examples. In section 4 we present the result of our performance testing and discuss the result. In section 5 we conclude the paper and mention our future work.

2. RELATED WORK

Some solutions have been proposed to solve the problem of high security overhead in fine-grained grid authorization system. Most of current grid authorization systems use the Brute Force Approach (BFA) during the authorization process which consumed a very high authorization overhead due to redundancy and repetition in security policy checking (Hoheisel *et al*., 2006). Due to that, most of grid VO only deployed a very simple policy whereby if a user's identity is verified during authentication then the user is allowed to access all resources in grid.

The Primitive Clustering Mechanism (PCM) (Kaiiali *et al*., 2008), Hierarchical Clustering

Mechanism (HCM) (Kaiiali *et al*., 2010a) and Grid Authorization Graph (GAG) (Kaiiali *et al*., 2013) are proposed to reduce redundancy and repetition in security policy by arranging the resources' security policy using a tree structure. However, they only assume small number of resources and security rules. Moreover, the security policies used in their study are too simple which cannot model the complex security policy like UCON based security policy. A part from that, for a large grid such as the EGEE grid, the previous mechanisms do not give a significant performance reduction. In every security policy there may exist rules that depend on other rules whereby if the rules are treated independently they become irrelevant to the authorization context and increase the total set of rules that must be checked. As the grid size grows, the number of security policies increases, the irrelevant set may increase and further degrade the authorization performance.

Thus, to overcome the limitations, in this research the rules dependency in UCON based policy for grid is modeled. Then we introduce mechanism to eliminate the irrelevant sets to reduce the number of rules checking.

3. METHODOLOGY

This section discusses the technique we use to identify the first level dependencies of rules, eliminate the irrelevant rules set and simulate the UCON based authorization policies. We define entities related to our study as below Equation 2:

$$O = \{o_1,\ o_2,\ o_3,\ \ldots,\ o_j\} \quad (1)$$

$$AR = \{ar_1, ar_2, ar_3, ..., ar_k\} \quad (2)$$

Where:
O = The set of grid resources
AR = The set of authorization rules

For each resource $o_j \in 0$ there will be a corresponding authorization policy $AP_j \subseteq AR$. A user who wants to access resource o_j needs to satisfy all the authorization rules of AP_j. AP_j is defined based on UCON policies and scheme as in definition 1 and definition 2. A permission in UCON is a tuple (s, o, r) where s is the requesting subject, o is the target object and r is the access right. A UCON policy specifies the authorizations, obligations and conditions requirement before and during a usage process.

Definition 1

A UCON policy maps a permission of (s, o, r) to a tuple (P_{pre}, P_{on}, OB_{pre}, UP_{pre}, UP_{on}, UP_{post}).

Where:
P_{re} = A set of attribute predicates needs to be satisfied before a usage process
P_{on} = A set of attribute predicates needs to be satisfied during a usage process
OB_{pre} = A set of obligations need to be satisfied before a usage process

UP_{pre}, UP_{on} and UP_{post} are sets of update actions that are performed on the attributes of s and o before, during and after usage process, respectively.

The parameters of the policy are s and o, whereas r is a right. P_{re} and P_{on} are conjunctions predicates built whether on s's and/or o's attributes or on the system attributes. If the conjunction predicates are built on s's and/or o's attributes, it is regarded as authorization predicates. If the conjunction predicates are built on system attributes, it is regarded as condition predicates. The prefix $_{pre}$ indicates that the components are pre-decision component, whereas $_{on}$ are ongoing decision components. A predicate obtains one or more attribute values and constants and returns boolean values.

Definition 2

A UCON scheme is a 6-tuple (ATT_a, ATT_c, R, P, OB, C).

Where:
ATT_a = A fixed set of subject and object attributes names
ATT_c = A fixed set of system attributes names
R = A fixed set of generic rights
P = A fixed set of predicates built on ATT_a and ATT_c
OB = A fixed set of obligation actions
C = A set of policies

In UCON scheme, an attribute is considered mutable if it appears in UP_{pre}, UP_{on} or UP_{post}. Otherwise, it is immutable. All policies in a UCON scheme are defined for positive permission. For an access request, if there is no policy to enable the permission according to the predicates, the access is denied by default (Zhang *et al*., 2008).

Let us consider the following grid scenario. A federated grid environment is performed called the

'*AcademicVO'* by three organizations. Each organization contributes two resources each. Based on this scenario Equation 1 gives:

$$O = \{o_1, o_2, ..., o_6\} \quad (3)$$

Each resource has authorization policy. Since there are two resources from the same organization, authorization policy is considered being the same for each two resources. So we consider six UCON based authorization policies.

3.1. Authorization Policy 1: Consumable Resource Management

Resources o_1 and o_2 are contributed by organization A which has a policy regarding consumable resource management. The AP_1 and AP_2 stated that internal users are allowed to use 500 MB of storage in each resource o_1 and o_2 whereas users from other organizations only allowed using 250 MB each.

3.2. Authorization Policy 2: Credit or Reputation Management

Resources o_3 and o_4 are contributed by organization B which has a policy regarding credit or reputation management since organization B share an incentive-based content sharing. AP_3 and AP_4 require that user from other organization to have maximum limit of 1 GB downloading quota per day.

3.3. Authorization Policy 3: Status of Shared Objects and Collaborative Tasks

Resources o_5 and o_6 are contributes by organization C. Policy regarding status of shared objects and collaborative task in AP_5 and AP_6 state that when a user from a project (for example project X) is doing write operations on resources, other collaborative users from the same project cannot write or modify the object in order to preserve its integrity.

All policies are based on UCON conceptual or formal model proposed in previous work by Park and Sandhu (2004; Zhang *et al*., 2005). For simple policies example, two dimension policy table is adequate to model all rules and their relationship as done by Kaiiali *et al*., (2013) in their studies. However, two-dimension policy table is not enough to model UCON based policies because UCON policy treats the user and resource attributes as predicates. Multi-dimension authorization policy tables must be built for UCON based policies. However in this study we only want to investigate the first level structure of rules dependency exist in this type of policies, so we assumed that user and resource only have one attribute.

Thus, we combined the subject (i.e., user) and the object (i.e., resource) with their respective predicates because we only use one attribute for each subject and object. Equation 3 base on our assumption gives:

$$O = \{o_{1orgA}, o_{2orgA}, o_{3orgB}, o_{4orgB}, o_{5orgC}, o_{6orgC}\} \quad (4)$$

o_{1orgA} is resource o_1 with attribute ^{orgA} because it is contributed by organization A and so on. Further, we derive Equation 4 to incorporated attribute storage limit of 500MB for resources o_1 and o_2 and so on.

Each organization has i grid user. Similarly we denote user, S as Equation 5:

$$S = \{S_1, S_2, \ldots, S_i\} \quad (5)$$

Then we incorporated user attribute to each users Equation 6:

$$S = \{S_{1orgA}, S_{2orgB}, \ldots, S_{iorgC}\} \quad (6)$$

Extraction of rules from policy 1, 2 and 3 gives:

- ar_1 required the user to be a member or *"AcademicVO"*
- ar_2 required the user to be from organization A
- ar_3 required the user to be from organization B
- ar_4 required the user from organization C
- ar_5 allowed the user from organization A to use 500MB of storage
- ar_6 allowed the user from organization B to use 250MB of storage
- ar_7 allowed the user from organization C to use 250MB
- ar_8 allowed the user from organization A to download maximum 1GB/day
- ar_9 allowed the user from organization C to download maximum 1GB/day

We adopt method proposed by (Kaiiali *et al*., 2010b; 2013) to generate authorization rules Vs. resources table based on the extracted rules as depicted in **Table 1**.

Note that there are intangible dependencies exist between rules which cannot be shown in the table. For example rules 250 MB depend on rules organization C in ar_6 and this dependency must be count in the rules checking during authorization in order to make it relevant to the context of authorization scenario.

We modeled rules dependency in a hierarchical manner as depicted in **Fig. 1**.

Default rules checking process is done by generating all possibility of set containing combination of rules. l authorization rules can represent 2^l authorization policies. We show some values of possible set generated in our scenario in **Table 2**.

Line number 1 shows the possible policy is AP = {AcademicVO}. This policy is considered relevant because there are situation where resource provider could deploy an authorization policy that require checking VO membership only. For the line 5 of the **Table 2**, authorization policy AP = {500 MB} is considered irrelevant because deployment of policy require to check only storage of 500 MB give no meaning. Because this rule depends on rules Org.B or Org.C and it should be combined with the parent rules in order for it to give meaningful function in this context. This kind of set will be eliminates.

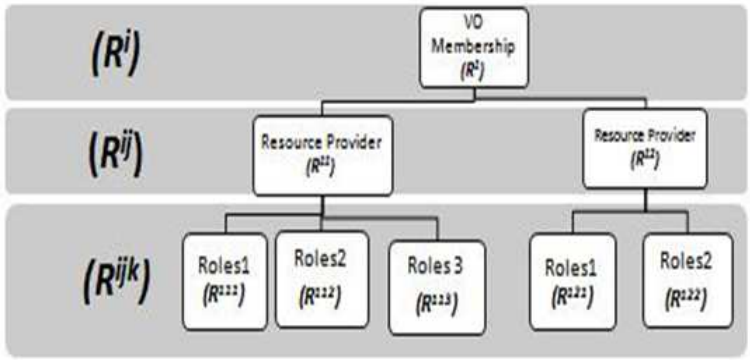

Fig. 1. Rules dependency model

Table 1. Authorization rules vs. resources tables

	1st level extracted rules						
O_j	AcademicVO	Org.A	Org.B	Org.C	500 MB	250 MB	1 GB/day
o_{1orgA}	1	1	1	1	1	1	0
o_{2orgA}	1	1	1	1	1	1	0
o_{3orgB}	1	0	1	0	0	0	1
o_{4orgB}	1	0	1	0	0	0	1
o_{5orgC}	1	0	0	0	0	0	0
o_{6orgC}	1	0	0	0	0	0	0

Table 2. Possible generated authorization policies

	1st level extracted rules						
O_j	AcademicVO	Org.A	Org.B	Org.C	500 MB	25 0MB	1 GB/day
o_{1orgA}	1	0	0	0	0	0	0
o_{2orgA}	0	1	0	0	0	0	0
o_{3orgB}	0	0	1	0	0	0	0
o_{4orgB}	0	0	0	1	0	0	0
o_{5orgC}	0	0	0	0	1	0	0
o_{6orgC}	…	…	…	..	…	…	…

4. RESULT AND DISCUSSION

Figure 2 shows simulation result of a grid environment consists of 12 resources and 4 authorization rules. The objective of this experiment is to compare the result with a result that we calculated manually in order to verify that our simulation is producing a correct result. We initiated 100 different authorization processes with randomly generated authorization rules input. A graph comparing GAG with our method is plotted. X axis for the number of initiated authorization process (Experiment No) and Y axis for the authorization complexity (No of checked security rules).

Based on **Fig. 2** we can realize that maximum number of checked authorization rules for GAG (represent by the dash line in the graph) is equal to the number of authorization rules exist in the system. This result is in agreement with the result obtained by (Kaiiali *et al*., 2013). It proof that our simulation result is correct. Note that the average minimum number of checked rules for GAG is equal to 2 compared to 0 by our method. This is true because while GAG checked all possible authorization policies, the checking process is sometimes can be skipped in our method (represent by the graph solid line) due to irrelevances of the containing rules.

Figure 3 shows a significant reduction in number of checking using our method in larger grid environment. Note that larger grid environment consist of big number of resources and rules, thus the combination set of irrelevant rules increased. Elimination of those sets gave big impact of reducing complexity checking to the larger grid environment. All experiments are done by enhancing the Grid Authorization Simulator developed by (Kaiiali *et al*., 2013).

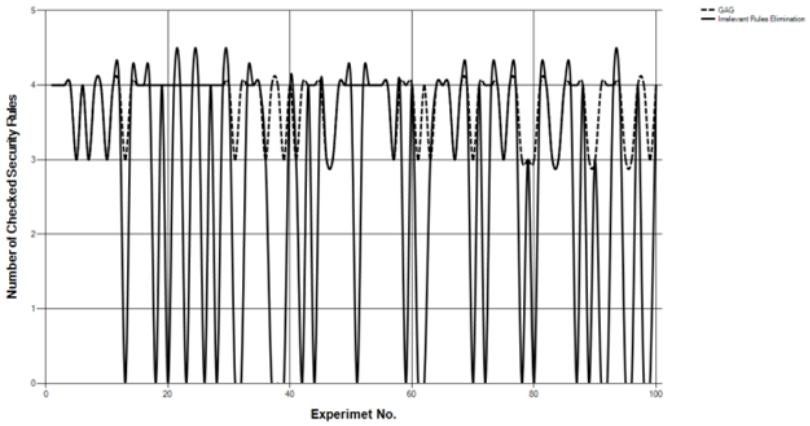

Fig. 2. Graph of complexity checking for 100 initiated authorizations for 12 resources with 4 authorization rules

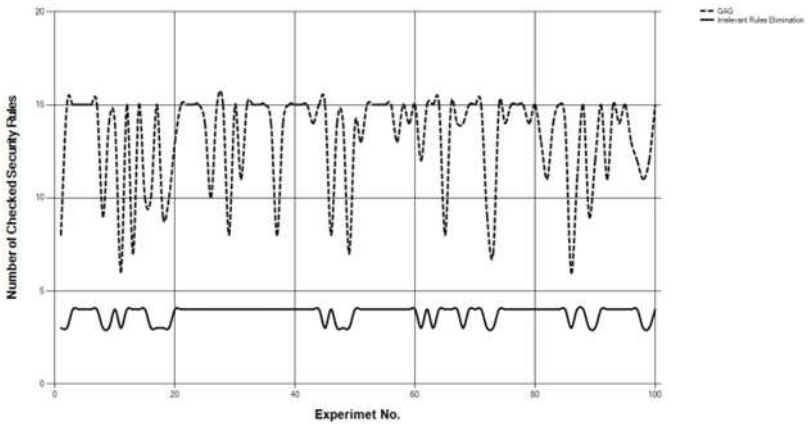

Fig. 3. Number of complexity checking for 100 initiated authorizations for grid consist of 200 resources and 15 security rules

Table 3. Percentage comparison of average number of checked security rules for 100 initiated authorizations for grid consist of 200 resources and 15 security rules

	Average number of checked security rules	%
Our Method	3	20
GAG	12	83
	Total reduction =	63%

However, this technique is limited to modeling two-dimension rules dependencies only (**Table 3**). Most of UCON based policies are multi-dimension rules dependencies, such as Policy 3 that contain rules about status of shared objects and collaborations.

5. CONCLUSION

In this study, a novel technique to reduce the number of complexity checking for UCON based grid authorization policies is proposed. The technique used a novel dependency rules model proposed in this study to identify irrelevant authorization policies. By eliminating the irrelevant authorization policies, 63% reduction of average number of complexity checking is made. Result shows that this method gives a big impact to a large grid environment. Our future work is to study the multi-dimension rules dependency in UCON based policy and to develop the multi-dimension dependency model so that we will be able to simulate complete authorization process of UCON and semantic based grid authorization system.

6. ACKNOWLEDGEMENT

The first author would like to thank the Malaysian Government, the Ministry of Science Technology and Innovation (MOSTI) for financial support throughout her studies in Universiti Putra Malaysia.

6.1. Author's Contributions

All authors equally contributed in this work.

6.2. Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved

7. REFERENCES

Alfieri, R., R. Cecchini, V. Ciaschini, L. Agnello and Á. Frohner *et al*., 2005. From gridmap-file to VOMS: Managing authorization in a Grid environment. Future Generat. Comput. Syst., 21: 549-558. DOI: 10.1016/j.future.2004.10.006

Hoheisel, A., S. Mueller and B. Schnor, 2006. Fine-grained security management in a service-oriented grid architecture. Fraunhofer Institute for Computer Architecture and Software Technology.

Chakrabarti, A., 2007. Grid Computing Security. 1st Edn., Springer Berlin Heidelberg, New York, ISBN-10: 3540444920, pp: 331.

Foster, I. and C. Kesselman, 2004. The Grid: Blueprint for a New Computing Infrastructure. 1st Edn., Morgan Kaufmann Publishers, ISBN-10: 1558609334, pp: 748.

Foster, I., C. Kesselman and S. Tuecke, 2001. The anatomy of the grid: Enabling scalable virtual organizations. Int. J. High Performance Comput. Applic., 15: 200-222. DOI: 10.1177/109434200101500302

Foster, I., C. Kesselman, G. Tsudik and S. Tuecke, 1998. A security architecture for computational grids. Proceedings of the 5th ACM Conference on Computer and Communication Security, Nov. 02-05, ACM Press, San Francisco, pp: 83-92. DOI: 10.1145/288090.288111

Humphrey, M., M.R. Thompson and K.R. Jackson, 2005. Security for grids. Proc. IEEE, 93: 644-652. DOI: 10.1109/JPROC.2004.842776

Ibrahim, M., S.N. Hamdan, H. Ibrahim, A. Abdullah and R. Latip, 2012. Intergrid security policy integration framework based on ucon toward federated grid access control. Proceedings of the International Conference on Informatics and Applications, (CIA' 12), pp: 205-212.

Kaiiali, M., R. Wankar, C.R. Rao, A. Agarwal and R. Buyya, 2013. Grid authorization graph. Future Generat. Comput. Syst., 29: 1909-1918. DOI: 10.1016/j.future.2013.04.010

Kaiiali, M., R. Wankar, C.R. Rao and A. Agarwal, 2008. Design of a structured fine-grained access control mechanism for authorizing grid resources. Proceedings of the 11th IEEE International Conference on Computational Science and Engineering Workshops, Jul. 16-18, IEEE Xplore Press, San Paulo, pp: 399-404. DOI: 10.1109/CSEW.2008.42

Kaiiali, M., R. Wankar, C.R. Rao and A. Agarwal, 2010a. Enhancing the hierarchical clustering mechanism of storing resources' security policies in a grid authorization system. Proceedings of the 6th International Conference on Distributed Computing and Internet Technology, Feb. 15-17, Springer, Bhubaneswar, India, pp: 134-139. DOI: 10.1007/978-3-642-11659-9_13

Kaiiali, M., R. Wankar, C.R. Rao and A. Agarwal, 2010b. New efficient tree-building algorithms for creating HCM decision tree in a grid authorization system. Proceedings of the 2nd International Conference on Network Applications, Protocols and Services, Sept. 22-23, IEEE Xplore Press, Kedah, pp: 1-6. DOI: 10.1109/NETAPPS.2010.8

Keahey, K., V. Welch, S. Lang, B. Liu and S. Meder, 2003. Fine-grain authorization policies in the GRID: Design and implementation. Proceedings of the 1st International Workshop on Middleware for Grid Computing, (MGC' 03).

Martinelli, F. and P. Mori, 2010. On usage control for GRID systems. Future Generat. Comput. Syst., 26: 1032-1042. DOI: 10.1016/j.future.2009.12.005

Park, J. and R. Sandhu, 2002. Towards usage control models: Beyond traditional access control. Proceedings of the 7th ACM Symposium on Access Control Models and Technologies, Jun. 03-04, ACM Press, New York, pp: 57-64. Doi: 10.1145/507711.507722

Park, J., 2003. Usage control: A unified framework for next generation access control. PhD Thesis, George Mason University.

Park, J. and R. Sandhu, 2004. The $UCON_{ABC}$ usage control model. ACM Trans. Inform. Security, 7: 128-174. DOI: 10.1145/984334.984339

Pearlman, L., V. Welch, I. Foster, C. Kesselman and S. Tuecke, 2002. A community authorization service for group collaboration. Proceedings of 3rd International Workshop on Policies for Distributed Systems and Networks, Jun. 5-7, IEEE Xplore Press, Monterey, CA., pp: 50-59. DOI: 10.1109/POLICY.2002.1011293

Sinnott, R.O., A.J. Stell, D.W. Chadwick and O. Otenko, 2005. Experiences of applying advanced grid authorisation infrastructures. Proceedings of the European conference on Advances in Grid Computing, Feb. 14-16, Springer, Netherlands, pp: 265-274. DOI: 10.1007/11508380_28

Stagni, F., 2009. On usage control for data grids: Models, architectures and specifications. PhD Thesis, Università degli studi di Ferrara.

Thompson, M.R., A. Essiari and S. Mudumbai, 2003. Certificate-based authorization policy in a PKI environment. ACM Trans. Inform. Syst. Security, 6: 566-588. DOI: 10.1145/950191.950196

Welch, V., F. Siebenlist, I. Foster, J. Bresnahan and K. Czajkowski *et al*., 2003. Security for grid services. Proceedings. 12th IEEE International Symposium on High Performance Distributed Computing, Jun. 22-24, IEEE Xplore Press, pp: 48-57. DOI: 10.1109/HPDC.2003.1210015

Zhang, X., M. Nakae, M.J. Covington and R. Sandhu, 2008. A usage-based authorization framework for collaborative computing systems. ACM Trans. Inform. Syst. Security, 11: 1-36. DOI: 10.1145/1133058.1133084

Zhang, X., F. Parisi-Presicce, R. Sandhu and J. Park, 2005. Formal model and policy specification of usage control. ACM Trans. Inform. Syst. Security, 8: 351-387. DOI: 10.1145/1108906.1108908

Zhang, X., J. Park, F. Parisi-Presicce and R. Sandhu, 2004. A logical specification for usage control. Proceedings of the 9th ACM Symposium on Access Control Models and Technologies, Jun. 02-04, ACM, Yorktown Heights, pp: 1-10. DOI: 10.1145/990036.990038