# INTERGRID SECURITY POLICY INTEGRATION FRAMEWORK BASED ON UCON TOWARD FEDERATED GRID ACCESS CONTROL

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

[1] Technical Support Department,

Malaysian Nuclear Agency, 43000 Kajang, Selangor.

[2] Faculty Of Computer Science and Information Technology,

University Putra Malaysia, 43400 Serdang, Selangor .

(maizura, nurbahyah)@nuclearmalaysia.gov.my

(hamidah,azizol,rohaya)@fsktm.up.edu.my

## ABSTRACT

Research in grid computing access control is focused on improving the scalability and enhancing the expressiveness of the security policy while keeping the security overhead as low as possible. Implementation of UCON model in grid computing authorization system is one of the best ways to enhance the expressiveness of grid security policy. However, there are still a lot of enhancement need to be done to improve the expressiveness and performance of grid authorization system. This paper proposes a combination of UCON with semantic technology to enhance the expressiveness and improve performance of intergrid authorization system.

## KEYWORDS

Grid computing; Access Control; Authorization; UCON; Policy Integration

## 1 INTRODUCTION

Intergrid (also known as global grids or multi-grid) is a collection of small grids that cross organizational boundaries to create a very large virtual system that can be accessed from anywhere in the world. The nature of intergrid environment that consists of very large, dynamic, and distributed user populations sharing resources in heterogeneous environment introduces challenging security issues. The resource pools that are shared are also very large, dynamic, and distributed worldwide. Resource sharing in grid computing may involve direct access to resources such as remote software, data which included safety critical data, sensors, and instrumentations. These resources need to be protected from unauthorized access. Security policy is used to define the access rules stating ‘who can do what and to whom’.

Security policy is defined as a set of rules which define the security subjects, security objects, and the relationship among them [1]. In the context of policy-based grid computing, these rules are stated in the VO security policy and local/resource level security policy. Security policy is referred by grid authorization system to evaluate every request submitted by a VO subject to access VO objects in determining whether the request should be allowed or denied.

In grid, when a user request a permission to access remote resources, numbers of security policies maintained by different Source of Authorities (SoAs) must be evaluated. Each one of different resources may be controlled by a different security policy officer in a different security domain. Each policy officer is a Source of Authority for an authoritative point. As the grid expands and its application traverses more administrative domains and become more virtual, the protection of these resources become more critical due to increasing number of users and resources. In addition, the users and resources become more dynamic, and more distributed too. As the consequences, the number of different security policies that must be evaluated and enforced increases [2], the security policies become larger and more complex in order to specify the access rules accurately. The time needed to evaluate and enforce the policies increases, hence decrease the overall grid performance in authorizing a user. Thus, there is a need to find a new method to minimize the effect of increasing numbers, size, and complexity of security policies over the grid authorization performance.

Recently, research is more focused on improving the expressiveness of security policy to accommodate the need of resource providers to precisely stating the access rules they want to enforce in a large, dynamic, distributed and heterogeneous environment. Moreover, grid communities are currently looking toward grid federated access control, it is important to do a detail study on the effect of these parameters over the grid performance because implementing federated access control involves integration of large number of users and resources. Large number of users and resources will definitely involve big number of security policies, size and complexity and affecting grid performance in authorizing users. However, none of the previous research describes the effect of increasing the numbers, size, and complexity of the security policy over the authorization performance in intergrid environment.

In this paper, we proposed a framework to improve grid authorization performance by simplifying the policy evaluation and enforcement process. The VOs security policies and local security policies are combined and filtered using semantic technique to provide only the relevant security policy to be evaluated hence reduce the numbers of policy to be checked and enforced by the grid authorization system. This method is also benefit in preserving privacy of data being shared in grid environment. Our model is based on the usage control model (UCON) [3] because our literature analysis shows that UCON is more expressive than other traditional access control model such as Discrete Access Control Model (DAC), Mandatory Access Control Model (MAC) and Role Based Access Control Model (RBAC)

This paper is organized as follows. The next section is the review of the related works. In Section 3 we present the proposed framework. Section 4 discusses about the advantages of our framework and finally we conclude the paper and our future works is explained in Section 5.

## 2 RELATED WORK

There is a wealth of work on grid authorization systems which can be classified into three classes based on the basic model or technology used, which are *traditional access control based authorization system*, *UCON based authorization system*, and *semantic based authorization system*. Traditional access control based authorization system uses traditional access control model such as Access Control List (ACL), Mandatory Access Control Model (MAC), Discrete Access Control Model (DAC), and Role Based Access Control Model (RBAC) as the basis of the system. The second used UCON as the basis, and the later used semantic web technology in the system.

### 2.1 The Traditional Access Control Based Authorization System

The first grid authorization system used ACL in specifying security policy. It was developed by [1] to address the need to coordinate diverse access control policies in large, dynamic, and high performance computing environment, as well as to operate securely in heterogeneous environments. Using the security policy as a context, the corresponding grid security architecture called the Globus Security

Infrastructure (GSI) is proposed. The core component of the GSI is a correct mapping between a global subject and a corresponding local subject called the globusmap file in a form of access control list. The correct mapping is achieved by converting a global name (e.g., certificate) into a local name (e.g., login name or user ID) using a mapping table in the resource proxy. The simplicity of the globusmap file provides the required high performance computing. However, this architecture only covers authentication process which is when a user proves that he/she hold credentials for both a global and local subject, he/she will be allowed to access all resources. This architecture does not provide method to explicitly define in detail what a user can do to a certain resources or in other word, the authorization part. Moreover, it is very coarse grained, inflexible, and not scalable which had caused bottleneck in the growth of grid [4], [5].

Then, researches are focused on proposing security architecture towards fine-grained access control, scalability, and flexibility in authorization process. External authorization systems were proposed to integrate with the GSI such as PERMIS [4], [6], Akenti [7], VOMS [8], CAS [9], and [10]. PERMIS enhances grid authorization by incorporating a role based access control and stores the users' roles in X.509 certificate, while Akenti is proposed to produce a usable authorization system for distributed resources used by geographically and administratively distributed users. However, all of these works based on traditional access control have limitation in encoding the expressiveness of the security policy.

The authorization model in Akenti consists of resources that are being accessed by users via policy enforcement point (PEP) called the resources gateway. Akenti server acts as Policy Decision Point (PDP) where it responsible in finding all the relevant certificates, verifies that each one is signed by an acceptable issuer, evaluates them and returns the access decision to the PEP. Akenti facilitates the use of user identity via X.509 public key certificate and facilitates setting of access policy by multiple independent stakeholders remote from actual resource gateway. In order to reduce certificate search time for the subsequent requests, caches technique is used to store the entire certificate when it is found for the first time. It also caches authorization decision, so that the subsequent requests for the same resource by the same user require no repeated decision. However, caches method only effective if the users attribute, use-condition, and resources attribute are assumed to be static. In real grid environment, users' attributes, resources' attributes, and use-condition are dynamic in very large grid environment making this technique not effective enough in current pervasive grid environment. More recently, research has focussed on applying Usage Control Model, UCON [3] to enhance the expressiveness of grid access control.

## 2.2 The UCON Based Authorization System

The usage control model (UCON) is the extended model of traditional access control model that introduces a new access control paradigm. In addition to traditional access control, UCON cover authorization, obligations, conditions, continuity (ongoing controls), and mutability of attributes. UCON not only dealt with authorizations as the basis for its decision making process, but it utilizes subject attributes and object attributes making it more flexible than traditional access control model. UCON also includes obligations and conditions as well as authorizations as part of usage decision process, providing richer and finer decision capability compared to traditional access control model. The UCON flexibility, richer and finer decision capabilities, and strong expressivity to specify modern access control makes it very suitable for pervasive computing environment like grid where users and resource pool are very large and dynamic.

Based on our analysis, a numbers of studies have been done to enhance the UCON model in order to adopt it in grid computing environment. The analysis from these studies shows that different types of grid require different UCON modification and enhancement. There are three types of grid which are data grids, service grids, and computational grid [11]. For data grid, [12] adapted UCON for the case of distributed systems with multiple authoritative points. This study proposed an enhancement of UCON for data grid called the distributed usage control model. The goal of this study is to facilitate resource sharing in data grid with more flexible and high control capabilities over who is authorized to view or modify data in grid environment. With the UCON novelty of providing continuity of decisions making and policy enforcement process, the solution proposed in this study ables to provide data grid with an access control improvement in term of richer security policy expression. However, this study only covers the theoretical part of the model. A part from that, this study mentioned about the need for advance study on the method of controlling the policy granularity in UCON based model which becomes one of the focus of our study.

Martinelli & Mori [13] introduced a formal model, architecture and prototype implementation for usage control on grid computational services. In this study, they adapt the original UCON model to develop a full model for usage control specific for grid system. Policy language based on process algebra (POLPA) is used in this study in order to specify security policy. Using the POLPA, they are able to provide continuous policy control and other UCON peculiarities such as mutability of subject's and object's attributes, and inclusion of obligation and condition as well as authorization in the access decision process. The experiment done with the prototype shown that the overhead introduced is acceptable. However, the model assumed that the PDP reads the policy resulting from the merging of local and VO policies where the resolution of possible conflict was assumed executed in the previous step. In current grid environment, the security policy evaluated before the access decision may be very large and may affect the performance of the authorization process. However nothing was mentioned about how the increasing numbers of security policies affect their proposed model. Therefore, there is a need to investigate the effect of large security policy into this model.

### 2.3 The Semantic Based Authorization System

Recently, [14] proposed a grid authorization architecture based on semantic web. In this architecture, grid security policies are represented using the combination of Semantic Web Rule Language (SWRL) and Web Ontology Language 2 (OWL 2). Utilization of semantic web concepts and technologies give added value features such as separation between domain description and policy description, reasoning capabilities about domain description and policy description, and interoperability. The proposed architecture provides higher expressiveness for policy and domain definition hence reducing the gap between abstraction and reality, aiding security administrators in authorization management. This work also proposes towards the automatic management of security services, advance conflict detection and resolution techniques that can provide semi-automated answer when conflict appears, advanced privacy and trust management as the future work. However, the architecture did not cover the requirement of mutability of subject and object attributes and continuous access monitoring. Therefore, we proposed a framework that covers mutability of subject and object attributes, continuous access control monitoring, and included new method to simplify policy evaluation and enforcement process.

## 3 THE PROPOSED FRAMEWORK

We propose the use of semantic technique in our framework to facilitate policy integration. We use UCON as the basis of our framework in order to enrich the subjects, objects and right flexibility by incorporating attributes into each. Additionally, beside authorization, our framework also includes obligation and condition in the decision process to improve the correctness of access decision being made. Our model consists of two parts: 1) Intra VO 2) Inter VO.

### 3.1 Intra VO

The intra VO model is depicted in figure 1. It covers the requirements of capturing organization's subjects, objects, subjects' attributes, objects' attributes, authorization rules, obligations, and conditions. These elements will be recorded and will be used to build the organization's ontology. The organization ontology will act as the input to the VO ontology after the filtration process.

The semantic policy filter acts as the engine to check the semantic similarity of the security policy between organizations, simplify and merge them to the respective VO ontology. The filter may also cover the process of conflicts detection, resolution and reconciliation of the security policies. When a user requests to access resources in the VO, instead of checking both global policy and local policy, system may only refer to the consolidated policy in the VO ontology.

### 3.2 Inter VO

The inter VO model is depicted in figure 2. It act as the first layer of intergrid access control which interact with users request. The intergrid semantic usage control service acts as the policy enforcement point (PEP). The semantic usage control service consecutively gets the ontologies update from every VO and updates the intergrid security policy so that the intergrid security policy is always in updated form. When a user request to access grid, he/she will only interact with the semantic usage control service and will instantly get the access decision.

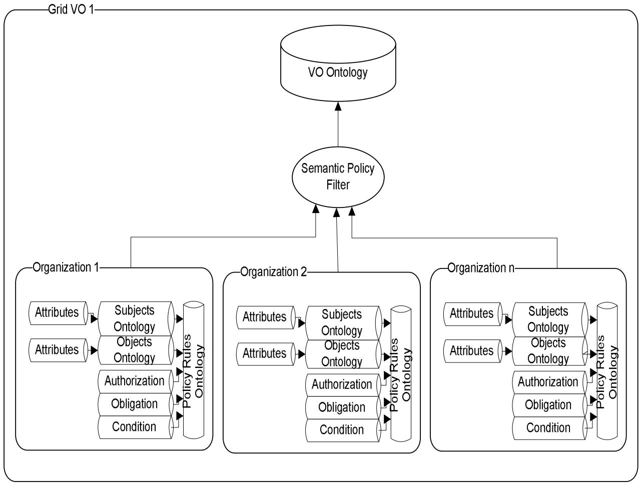

**Figure 1.** Intra VO Model

.

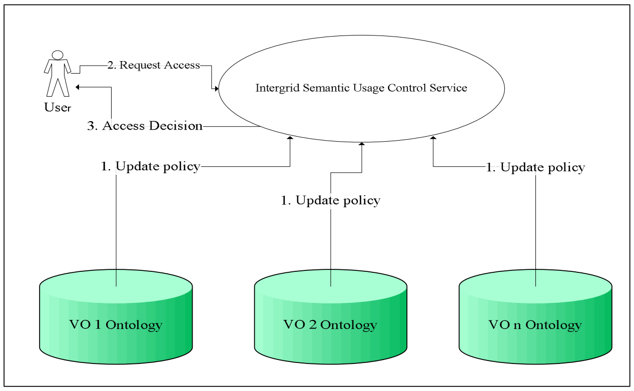

**Figure 2.** Inter VO Model

## 4 DISCUSSION

In this section we will discuss the advantages of the propose framework in term of framework features and performance subjectively.

The advantages of our framework compared to the previous work with respect to features are depicted in Table 1. Subject and object attribute is considered as one of the key features of UCON embedded in this framework which make the access decision for a subject is not static, but depend on dynamic factors. The subject is the entity that executes access operations on objects.

**Table 1.** Frameworks features comparison

| Features | Subject & Object Attributes | Obligation | Condition | Continuous policy monitoring | Policy Integration | Policy Ontology |
|---|---|---|---|---|---|---|
| **Martinelli & Mori** [15] **2010** | √ | √ | √ | √ | | |
| **Perez, J., et al** [14] **2011** | | | | | √ | √ |
| **Our framework** | √ | √ | √ | √ | √ | √ |

For example, subject could be a user and object could be a file that a user wants to access to perform a write or read operation. Both subjects and objects are paired with attributes in order to describe their features, and define the subjects and the objects instances. To further enhance the expressivity, attributes is categorized into mutable and immutable attributes. Mutable attributes is the dynamic attributes which will be change as the consequences of the access performed by subject, such as credit. Subject's credit is updated every time the user accesses resources with charge. Immutable attributes instead, are fix attributes. It will not change after the access is performed. It is a classical attributes such as user distinguish name (DN) for a subject, and memory size, CPUs speed, or disk size for an object.

To further enhance the framework, we added conditions and obligations to authorization in the decision making process. Conditions are dynamic factors that do not depend upon subjects or objects. Conditions are environmental or system-oriented decision factors which are evaluated at runtime, when the subject attempts to perform the access. Obligations are decision factors that are used to verify whether the subject has satisfied some mandatory requirements before performing an action. All the factors are evaluated before the access, during the access, and after the access to provide the continuous policy monitoring functionality.

Figure 3 shows the relationship scenario of the subject, object, authorization, condition, and obligation in continuous decision process of giving right to a subject in accessing an object.

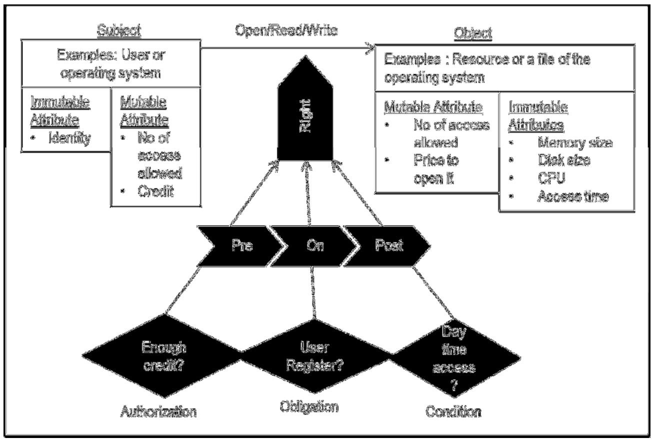

**Figure 3.** Relationship scenario of the entities in UCON

A part from the need for richer features to accommodate security policy specification, intergrid environment also needs a high performance authorization system. The performance testing result of grid authorization system depicted in figure 4 shows authorization request time of a grid exponentially increase when the number of individuals in a VO increase. Number of individual refers to the grid users in a VO. This result indicates the performance of grid authorization system will exponentially decrease when users of the grid increase. The impact of this overhead may be greater in the intergrid environment. Intergrid environment involves more subjects, objects, and operations compared to a grid. As a complication, the number of policy statements and the complexity of intergrid security policy is very high, making the process of authorizing a user more time consuming, hence may reduce the overall grid authorization performance.

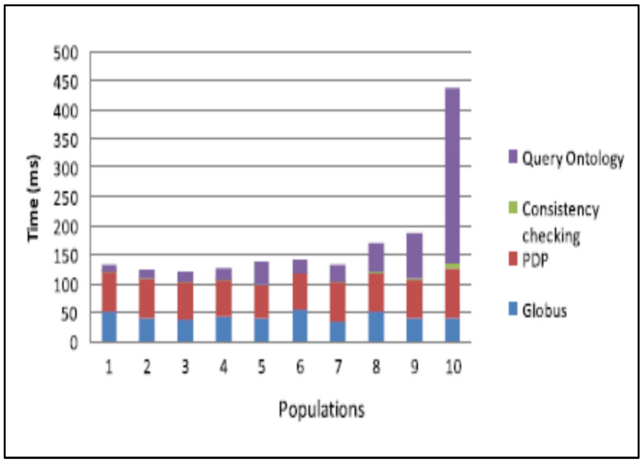

**Figure 4.** Authorization request time of semantic based authorization system for 1000 requests [14]

Usually, a VO consists of different individuals and/or organization which share resources in a coordinated manner. Each resource provider may define its own security policy to specify the access to it resources (local/resource level policy). Meanwhile, the VO itself may define some common policy which governs the resource sharing behaviour in the specific VO (global policy). This situation leads to the problem where different organizations use different term or syntax to define the same entity.

For example, Organization 1 defines their users using *Researcher*, while Organization 2 using *Research Officer* and Organization 3 using *Scientist*. Even though the concept of *Researcher*, *Research Officer*, and *Scientist* refer to the same entity i.e. user, the simple join of their security policy may not work. This is because the use of different syntactic representation will be considered as different concept by the system. A part from that, in a usual manner, the system may read the policy line by line, starting from global policy to each of the local/resource policy which may consume a lot of time before the access decision is made.

Our framework proposes semantic policy integration in order to merge the organizations' policy in a VO as well as VOs policies when two or more grid collaborates with each other. The policy filter may reduce the number of policy statement hence may also reduce the time taken to execute the query in access decision process. Additionally, instead of checking both global policy and local policy, system may only refer to the consolidated policy in the VO ontology to make the access decision, which may shorter down the path for policy checking, hence may reduce the grid authorization request time.

## 5 CONCLUSION AND FUTURE WORKS

To briefly summarize, we have proposed a conceptual framework to facilitate intergrid collaboration access control. This framework enhances the previous one by combining UCON features and semantic technology in order to improve the expressiveness of specifying grid security policy.

This framework also proposes a semantic technique to integrate the security policy of the organizations in a VO and inter VO in order to simplify the security policy checking and enforcement process. The next stage of this work is to investigate the grid policy mapping mechanism using semantic technique, and to investigate the correctness and the completeness of the proposed framework with respect to inconsistencies. A part from that, we plan to simulate our framework implementation in intergrid environment and test the performance of our framework. We believe this work is laying a foundation toward high performance grid federated access control.

## 6 ACKNOWLEDGEMENT

The first author would like to thanks Ministry Of Science Technology and Innovation (MOSTI) for financial support throughout her studies in University Putra Malaysia.

## 7 REFERENCES

1. Foster, I., Kesselman, C., Tsudik, G., Tuecke, S.: A

Security Architecture for Computational Grids. In : 5th Conference on Computer & Communications Security, San Francisco CA, pp.83-92 (1998)

2. Foster, I., Kesselman, C.: The Grid: Blueprint for a New Computing Infrastructure 2nd edn. Morgan Kaufmann, Carlifornia (2004)
3. Park, J., Sandhu, R.: The UCON_ABC Usage Control Model. ACM Transaction on Information and System Security 7(1), 128-174 (2004)
4. Chadwick, D., Otenko, A.: The Permis X.509 role based privilege management infrastructure. Future Generation Computer System 19, 277-289 (2003)
5. Jie, W., Arshad, J., Sinnot, R., Towned, P., Lei, Z.: A Review of Grid Authentication and Authorization Technologies and Support for Federated Access Control. ACM Computing Surveys 43(2), 1-26 (2011)
6. Laccetti, G., Schmid, G.: A Framework Model for Grid Security. Future Generation Computer Systems 23, 702-713 (2007)
7. Thompson, M., Essiari, A., Mudumbai, S.: Certificate-Based Authorization Policy in a PKI Environment. ACM Transactions on Information and System Security 6(4), 566-588 (2003)
8. Alfieri, R., Cecchini, R., Ciaschini, V., Agnello, L., Frohner, A.: From gridmap-file to VOMS: managing authorization in Grid environment. Future Generation Computer Systems 21, 549-558 (2005)
9. Pearlman, L., Welch, V., Foster, I., Kesselman, C., Tuecke, S.: A Community Autorization Service for Group Collaboration. In : Proceedings of the Third International Wokshop on Policies for Distributed System and Networks (POLICY'02)
10. Koshutanski, H., Lazouski, A., Martinelli, F., Mori, P.: Enhancing grid security by fine-grained behavioral control and negotiation-based authorization. International Journal of Information Security 8(4) (2009)
11. Cody, E., Sharman, R., Rao, R., Upadhyaya, S.: Security in grid computing: A review and synthesis. Journal of Decision Support System 44, 749-764 (2008)
12. Stagni, F., Arenas, A., Aziz, B., Martinelli, F.: On Usage Control in Data Grids. In : IFIP, pp.99-116 (2009)
13. Martinelli, F., Mori, P.: On usage control for grid systems. Future Generation Computer System 6(7), 1032-1042 (2010)
14. Perez, J., Bernabe, J., Calero, J., Clemente, F., Perez, G., Skarmenta, A.: Semantic-based authorization architecture for grid. Future Generation Computer Systems 27, 40-55 (2011)