A HIGH PERFORMANCE UCON AND SEMANTIC-BASED AUTHORIZATION FRAMEWORK FOR GRID COMPUTING

[1]Maizura Ibrahim, [2]Hamidah Ibrahim, [2]Azizol Abdullah &
[2]Rohaya Latip
[1] Malaysian Nuclear Agency, Malaysia
[2]Universiti Putra Malaysia, Malaysia

maizura@nm.gov.my; hamidah.ibrahim@upm.edu.my;
azizol@upm.edu.my; rohayalt@upm.edu.my

ABSTRACT

Authorization infrastructures are an important and integral part of grid computing which facilitate access control functions to protect resources. This paper presents an authorization framework that combines the usage control (UCON) model with semantic web technology. To our knowledge, an authorization framework that combines both the UCON and semantic web technology in one framework has not yet been previously proposed. As the UCON model combines traditional access control, trust management and digital rights management in a grid authorization infrastructure, its adoption enhances the capability of the authorization. However, UCON-based authorization presents a problem in controlling the policy granularity and minimizing the authorization overhead due to complexity in the policies inherited from the UCON model. The growing number of users and resources in the grid makes this problem even worse. We use the semantic web technology to provide a way to automatically manage the rules in the policies, hence keeping the granularity under control. To minimize the authorization overhead, a new mechanism to reduce the number of policy checks is proposed in this paper. Our simulation result shows that the proposed mechanism provides a 63% reduction in rule checking compared to previous methods.

Keywords: Grid computing, UCON, security policy, ontology, semantic web, grid authorization.

INTRODUCTION

Grid computing is concerned with geographically distributed computers composed of heterogeneous resources that are owned, shared and coordinated by multiple administrative domains to provide nontrivial quality of services (Foster & Kesselman, 2004). The virtual organization (VO) concept makes the resource sharing in a grid possible. A VO is a group of individuals and associated resources and services located within multiple administrative domains, but united by a common purpose (Welch, Siebenlist, Foster, Bresnahan, Cjajkowski, Gawor et al., 2003). The massiveness, dynamism and heterogeneous nature of the grid demand a fine-grained, high performance and scalable authorization system. Authorization can be defined as the act of providing and checking the authority of a user or a job to access a specific set of resources (Cakrabarti, 2007). The requirement for fine-grained authorization and high performance makes grid authorization a major challenge. Fine-grained authorization is composed of two factors. First, the selected authorization model must support as many parameters as possible in order to satisfy the need to describe the dynamic and heterogeneous rules in grid authorization. Second, the language used to write the security policy must be as high-level and expressible as possible so that it can describe the rules specifically and accurately as demanded by the grid stakeholders, the grid's users and the resources' behaviors.

The use of UCON in grid authorization systems provides a good solution for describing the dynamic and heterogeneous in the grid authorization (Zhang, Parisi, Sandhu, & Park, 2005). The mutability of the users' and resources' attributes and the continuity of the access monitoring in the UCON model provide a fine-grained authorization for the grid. However, UCON-based grid authorization presents a problem in controlling the granularity of grid resources' security policies. In order to provide dynamic and continuous monitoring, many parameters must be used to describe the users and resources in the grid authorization; thus, a very high level of data granularity is required. The large number of users and resources in a grid makes it impossible for humans to control the granularity of grid security policies manually. A growing number of users and resources adds to the risk that the grid authorization system's granularity will burst out of control. Thus, the implementation of UCON in the grid authorization system requires a mechanism to keep the granularity under control. This paper attempts to solve the granularity control problem using ontology and semantic web technology. A new grid authorization framework that stores the UCON-based grid security policies in the form of ontology is presented. In the framework, the ontology web language (OWL 2) (W3C, 2012) and the Semantic Web Rule Language (SWRL) (Horrocks, Schneider, Boley, Tabet, Grosof & Dean, 2004) is used to perform the authorization query and access the request processing. The advantages of using a combination of OWL and SWRL compared to other technologies are that they allow automated reasoning and at the same time can perform formal validation and verification of the domain constraints specified in the ontology to ensure these constraints are fulfilled (Pérez, Bernabe, Calero, Clemete, Perez & Gomez, 2011). To minimize the authorization overhead caused by the complex rule checking in the policies inherited from the UCON model, a new irrelevant rule elimination procedure based on the dependence rules model is used in the framework

LITERATURE REVIEW

Since the invention of grids, intensive research has been done to improve the grid authorization system in terms of the level of the grain, the scalability and the performance of the access control because the native access control provided by the Grid Security Infrastructure, namely, the grid map file (Foster et al., 1998), is based on the access control list concept that is very coarse-grained and not scalable.

The Virtual Organization Membership Service (Alfieri, Cecchini, Ciaschini & Agnello, 2005), Akenti (Thompson, Essiari, & Mudumbai, 2003), PERMIS (Chadwick & Otenko, 2003) and Community Authorization Service (Pearlman,Welch, Foster, Kesselman, & Tuecke, 2002) focus on improving authorization functionalities based on the traditional access control concept through methods such as discrete access control, mandatory access control and role-based access control. However, these approaches have limitations in coping with the mutability of users' and resources' attributes and continuous access monitoring for pervasive environments like a grid computing environment.

The UCON model is an enhancement of the traditional access control models which not only deals with authorizations as the basis of its decision-making process, but also counts obligations and conditions in the process. In addition, the UCON features of continuous access monitoring and mutability of attributes provide richer and more dynamic decision-making capabilities than traditional access control. The UCON flexibility and finer decision capabilities make it very suitable to use in pervasive computing environments like the grid where the user and resource pools are very large and dynamic.

A number of studies have adopted the UCON model in a grid computing environment. There are three types of grid, namely, data grids, service grids, and computational grids (Cody, Sharman, Rao, & Upadhyaya, 2008). For data grids, the UCON model has been adapted for the case of distributed systems with multiple authoritative points (Stagni, 2009). That study proposed a theoretical methodology (i.e. the goal-oriented approach) to formally validate the UCON policy enforcement. A formal model for the architecture and prototype implementation of UCON in grid computational services was proposed by Martinelli and Mori (2010). In their model, the policy language based on process algebra (POLPA) is used to specify security policy. Using the POLPA, continuous policy control and other UCON peculiarities such as the mutability of users' and objects' attributes, and inclusion of obligations and conditions as well as authorization in the access decision process, are able to be provided. A usage-based authorization framework for collaborative computing was proposed by Zhang, Nakae, Covington, & Sandhu (2008). They used extensible access control markup language to specify UCON policy in their prototype. In their framework, a sensor program is used to detect changes in users' attributes in the user platform. All of these UCON-based authorization solutions assume a small number of users and resources so that the granularity of the security policy can be updated and maintained manually by the security officers in an organization. They lack the semantic-aware component element that can assist in controlling the granularity of the security policy for the large-scale scenario. The numbers of users and resources in a grid keep on increasing year by year. For example, the Enabling Grid for E-Science project holds about 17,000 identities of users, the management of which required around 336,000 policy statements in 2011 (Pérez et al., 2011). It is impossible to manually control the granularity of data for such large numbers of users. Therefore, we propose a framework that uses ontology to store the UCON-based security policies and process the evaluation of authorization using a combination of OWL 2 and SWRL.

Apart from the need for richer features to accommodate authorization policy specification and autonomous management, grid computing also needs a high performance authorization system, especially as grids become larger and larger in the future. The performance testing results of previous grid authorization systems show that the authorization request time exponentially increases when the number of individuals in a VO increases (Martinelli & Mori, 2010; Pérez et al., 2011). The number of individuals refers to the number of grid users in a VO. These results indicate that the performance of the grid authorization system will exponentially decrease when the number of users of the grid increases. The impact of this overhead will be greater in a large-scale grid environment because the large-scale grid environment involves more subjects, objects and operations compared to an ordinary grid environment. The use of the UCON as a policy model adds complexity to the policy representation. The number of policy statements and the complexity of the authorization policy become very high, making the process of authorizing a user more time-consuming and reducing the overall grid authorization performance. Thus, there is a need to find a new method to minimize the effect of increasing numbers, size and complexity of security policies on the grid authorization performance.

Modeling Resource and Security Policy in the Grid VO

Let us consider a grid VO that deploys *j* resources in its environment. There will be *j* resources that can be requested by a subject (s):

Definition 1

$\mathbf{R} = \{r_1, r_2, r_3,...,r_j\}, j = 1, ..., k$ where **R** is the set of grid resources in a VO.

For each resource $r_j \in O$ there will be a corresponding security policy $\mathbf{SP_j} \subseteq \mathbf{SR}$ where **SR** is defined as:

Definition 2

$\mathbf{SR} = \{sr_1, sr_2, sr_{,..},sr_k\}, k = 1, ...,l$ where **SR** is the set of security rules for the VO.

A user who wants to access resource r_j needs to satisfy all the security rules of $\mathbf{SP_j}$. Most of the existing grid authorization systems adopt an inefficient structure for storing security policies for the available resources. Many systems use the brute force approach (BFA) during the authorization process which consumes a very high authorization overhead due to redundancy and repetition in the security policy checking (Hoheisel & Mueller, 2006). Due to that reason, in most cases, the grid VO only deploys a very simple policy whereby if a user's identity is verified during the authentication process, then the user is allowed to access all the resources in the grid. The BFA is modeled by the rule mapping (**RM**) group as expressed in the following definition:

Definition 3

$\mathbf{RM} = \{(r_j, \mathbf{SP_j})\} \mid r_j \in O_{,} sr_j \subseteq \mathbf{SR}$ where $j = 1,...,k$

In a grid VO every resource has its own security policy which contains rules that might be similar or almost similar to some other resource's security policy. For example, if a grid VO consists of *j* resources deployed by *j* numbers of security policy, SPj, that consist of *k* security rules, similarity of rules in the security policy will occur if:

$\mathbf{SP_1} = \{sr_1, sr_2\}$, $\mathbf{SP_2} = \{sr_1, sr_2\}$, $\mathbf{SP_3} = \{sr_1, sr_2, sr_3\}$ and $\mathbf{SPj} = \{sr_1, sr_2, sr_k\}$
The **RM** of BFA for this scenario gives:

$\mathbf{RM_{BFA}} = \{(r_1, \{sr_1, sr_2\}), (r_2,\{sr_1, sr_2\}), (r_3,\{sr_1, sr_2, sr_3\}),\ldots, (r_j,\{sr_1, sr_2, sr_k\})$
The process of checking the security rules using the BFA for this scenario is illustrated in Figure 1 which gives a sequential complexity of O(k*j); where k is the maximum number of rules in each security policy and j is the number of resources in the grid VO.

r_1 sr_1, sr_2	r_2 sr_1, sr_2
r_3 sr_1, sr_2, sr_3	r_j sr_1, sr_2, sr_k

Figure 1. Brute force approach mechanism for rule checking.

Efforts have been made to improve the brute force mechanism, such as the primitive clustering mechanism (PCM) (Kaiiali et al., 2008), hierarchical clustering mechanism (HCM) (Kaiiali et al., 2010) and grid authorization graph (GAG) (Kaiiali, Wankar, Rao, Agarwal, & Buyya, 2013). These mechanisms aim to reduce the redundancy and repetition in security policy checking.

The Primitive Clustering Method

PCM reduces the redundancy of checking using a clustering method that depends on the similarity of the security policy. It is modeled using a rule mapping group called reverse rules mapping (**RRM**):

Definition 4

Let $r_j \subseteq \mathbf{R} = \{r_i | r_i \in \mathbf{R}, (r_i, \mathbf{SP_j}) \in \mathbf{RM}\}$ be the set of all resources that share the same security policy $\mathbf{SP_{j.}}$ Then,

$\mathbf{RRM} = \{(\mathbf{SP_j}, \mathbf{R_j}) \mid \mathbf{SP_j} \subseteq \mathbf{SR}\}$ is the set of security policies relevant to a group of resource assignments.

Using the same example as above and j=3 yields:

$\mathbf{RRM} = \{(\{sr_1,sr_2\}, \{r_1,r_2\}), (\{sr_1,sr_2,sr_3\},\{r_3, r_4\})\}$

Rather than doing four rounds of checking, PCM only does two rounds of checking for the same scenario. The illustration of PCM for this scenario is depicted in Figure 2.

sr_1, sr_2 r_1, r_2	sr_1, sr_2, sr_3 r_3, r_4

Figure 2. Primitive clustering mechanism for rule checking.

Primitive clustering removes the redundancy of checking the identical security policies, but the redundancy of checking identical security rules still exists. This limitation is overcome in the HCM.

Hierarchical Clustering Mechanism

HCM further reduces the redundancy in checking the security rules by arranging the resources' security policy using a hierarchical tree structure. The HCM building algorithm was developed based on the depth-first search algorithm using the data in the security table (ST).

The ST is a simple table that represents the **RM** group of rule-checking mechanisms. In ST, the security rules are considered as attributes and the resources are considered as objects. The ST entry is a Boolean value of 1 or 0. If the *l*-th security rules are elements of the *j*-th resource, the entry of the (*j,l*)th cell of the ST is 1 and vice versa.

Grid Authorization Graph

One limitation of the HCM is that it cannot describe the OR-based security policies. The GAG enhances the HCM by overcoming this limitation. By introducing special types of edges, namely, the correspondence edge and the discrepancy edge, the GAG can totally eliminate the redundancy of checking and can handle the cases where the sets of security rules are mutually exclusive. In every security policy there may be 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 and the number of security policies increases, the number of irrelevant sets may increase and further degrade the authorization performance.

In the proposed UCON and semantic-based authorization framework we introduce policy filters as components in the framework. The policy filters are responsible for reducing the number of rules checked during the authorization process. This results in a reduction in the time taken to authorize grid users in very large-scale grid computing.

METHODOLOGY

The UCON and semantic-based authorization framework is developed using the policy enforcement implementation (PEI) method (Sandhu, 2006). We follow the method used by Zhang et al. (2008) in developing our framework. The early literature (Park, 2003) assumed the policy layer would be rigorous and well defined; however, in reality, the highest level policy is very informal and fuzzy. Modern systems like grids are distributed and have multiple trust and service dependencies, thus it is very hard to close the gap between policy and mechanism in such a complex environment. The PEI framework introduces a realistic approach through which it can accommodate an informal policy layer at the top and hence close the overall gap between informal policy and concrete code in multiple steps. Figure 3 illustrates the PEI framework.

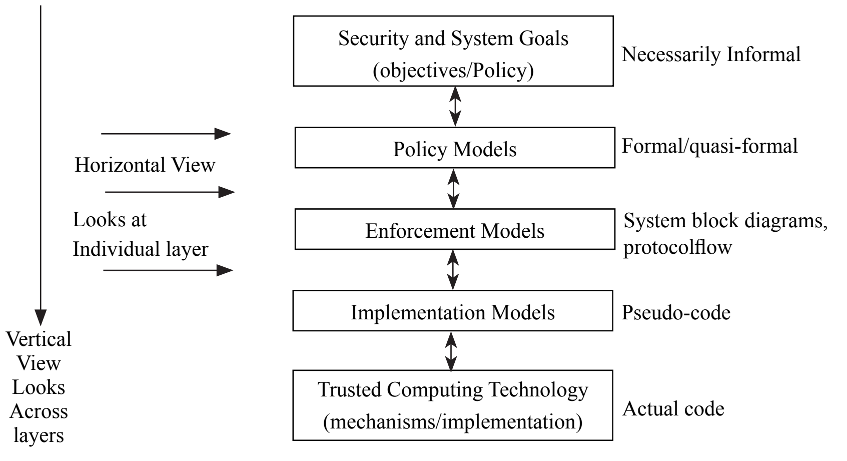

Figure 3. Policy enforcement implementation framework.

The top layer of the PEI framework defines the security and system goals. In this layer, we define the security and system requirements informally. This layer is necessarily informal. It is a mistake to try to formalize this layer as in the traditional security system design approach. The purpose of the second layer is to take informal high-level objectives and flesh out rigor and detail using formal or quasi-formal notation. In this stage, the subjects, objects, administrator roles, groups and other requirements are specified in an ideal setting. In this layer, we use the UCON policy model (Zhang et al., 2005) as our model.

The enforcement and implementation layer address how the desired policy model can be enforced in the chosen environment. It addresses the big picture of the "how" question, at the level of the system block diagram and protocol flow. The protocol flow can be formalized and analyzed in order to establish the various security properties of the system. However, certain levels of detail are left unspecified, and these are elaborated on in the implementation model. At this layer, the approximated policy is realized using the system architecture (with trusted servers, clients etc.). In the implementation model, we focus on the specific issues identified in the enforcement model. These issues are focused on in detail up to the pseudo-code level of detail precision.

The adjacent layers have many-to-many relationships with each other. For example, a single policy model can be enforced by a multiple enforcement model. However, there are certain different trade-offs between security, trust, performance, cost, convenience and other factors. On the other hand, a single enforcement model may be supported by the multiple policy model. The relationship between the enforcement model and the implementation model is similar. At the layer of the implementation model, a specific issue identified in the previous layer will be resolved in sufficient detail.

THE UCON AND SEMANTIC-BASED AUTHORIZATION FRAMEWORK

The UCON and semantic-based authorization framework consists of three different levels, as illustrated in Figure 4. Each level caters for different grid authorization requirements.

Level 1: Multi-Domain Grid Infrastructure

Level 1 of the framework caters for the authorization process with a combination of multi-organizational grid infrastructures to form a federated grid. In the grid, each of the different resources may be contributed by different organizations. Each resource in an organization may have its own security policy. At this level, the inter-grid policy integration is implemented using the mechanism proposed by Ibrahim, Hamdan, Ibrahim, Abdullah & Latip (2012). This level also caters for the multiple authorities' security points (Lorch, Cowles, Baker, Gommans, Madsen, McNab et al., 2004), as depicted in Figure 5.

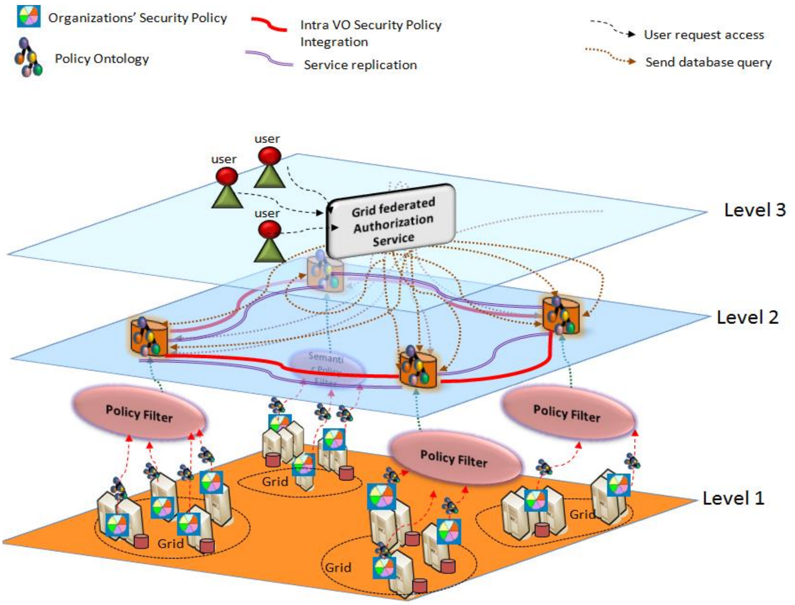

Figure 4. UCON and semantic grid authorization framework.

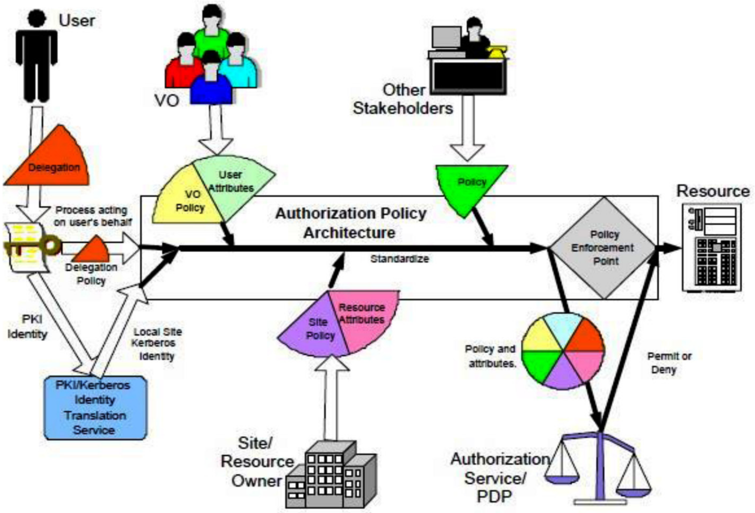

Figure 5. Multiple authorities' security points (Lorch et al., 2004).

The security policy of each resource in the grid is input and updated by a policy officer. Each policy officer is a Source of Authority (SoA) for an authoritative point in the grid. The site or resource policy officer defines and updates the rules related to the resources' policies and resources' attributes. The VO policy officer inputs and updates the rules in the security policy related to the VO policy and users' attributes. The grid stakeholders define and update the rules regarding the stakeholder policy. All the rules are combined to represent the security policies required by that particular grid in the form of an ontology. Figure 6 illustrates the first three class levels of the security policy ontology based on the UCON attributes.

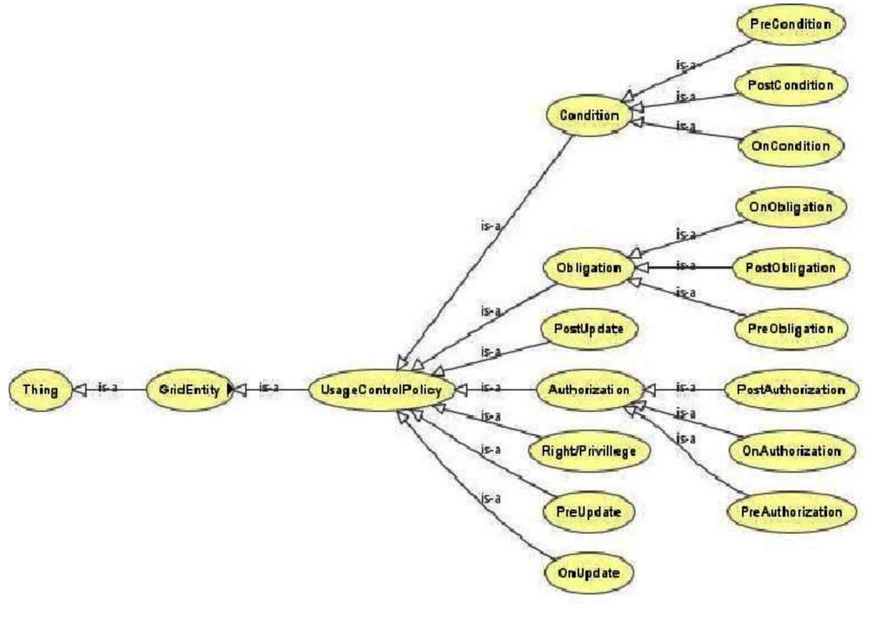

Figure 6. First three class levels of the UCON-based security policy ontology.

The ontology is designed in such a way that it can store rules to provide the UCON peculiarities during the user request evaluation process. In UCON, the existence of a right for a user does not depend on authorizations only: obligations and conditions are also considered. This ontology also supports the UCON feature of ongoing monitoring of the user's request. The ontology is designed so that, for each user request, the authorization, obligations and conditions are checked before, during and after the usage of the resources. This makes the authorization very dynamic and enables it to be continuously monitored tailored to the UCON peculiarities. The policy filter is used to reduce the number of checks during the authorization. A mechanism to eliminate sets of irrelevant rules is used in order to reduce the number of checks. To determine the irrelevant rules, the rules are modeled based on their dependencies on other rules. The example of the proposed rules dependency model is shown in Figure 7 which is based on European Grid Initiative (EGI) grid environment security policies analysis. Yuhanis, Madi, & Hassan (2012) simulate a dependency model for the same grid environment by calculating dependency level using file weight. We used a different approach. Our dependency model is based on hierarchical tree. A detailed explanation of our method was published in Ibrahim et al. (2014).

Level 2: Distributed Databases

Level 2 of the framework consists of components to cater for the requirements of the distributed authorization databases that store the federated grid's security policies. Each grid infrastructure owns a database that models the rules concept and domain concept of that particular grid. In order to model the grid domain concept, we enhance the existing core grid ontology (Xing et al., 2006) on the policy model to make it suitable for modeling the UCON policy model.

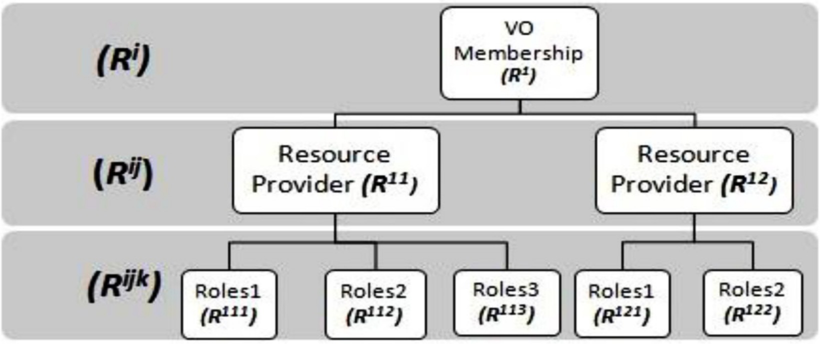

Figure 7. Rules dependency model.

The core grid ontology is suitable because it more closely models the grid environment used in Malaysia (i.e. based on the European grid) compared to the common information model (Bumpu, Sweitzer, Thompson, Westerine, & Williams, 2000) and the standard ontology for ubiquitous and pervasive applications (Chen, Perich, Finin, & Joshi, 2004). The architecture used to embed this framework in each resource is shown in Figure 8. The modified part of the core grid ontology is shown in Figure 9.

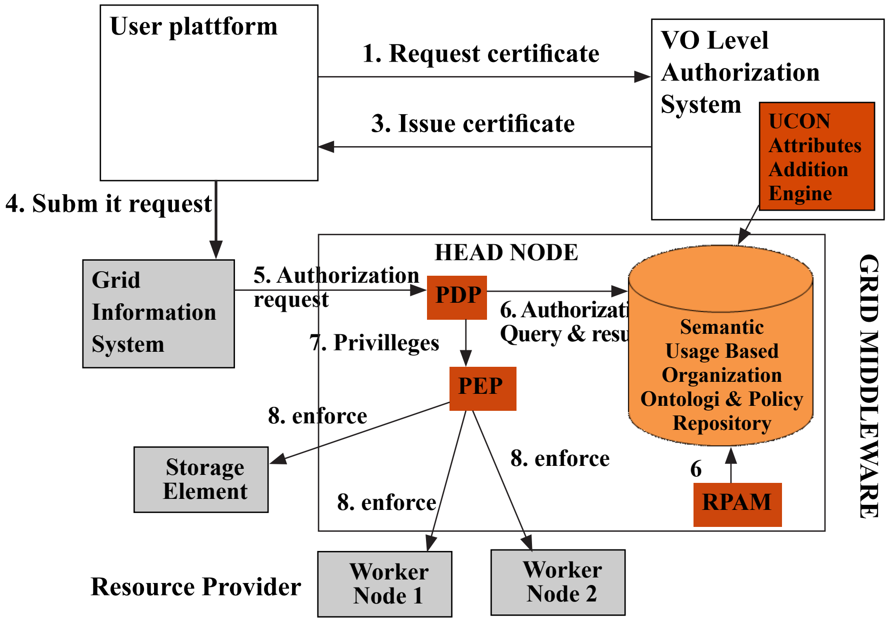

Figure 8. UCON and semantic implementation architecture.

Level 3: Federated Authorization Application Service

The federated authorization application service serves the function of interacting with the user. It collects the attributes of the user that requests the grid services and sends the attributes to the policy decision point (PDP) via the grid information system as shown in Figure 8. The PDP then interacts with the semantic usage-based organization ontology and policy repository that stores the authorization rules for all the resources in the federated grid to obtain the answer regarding the user's privileges.

The PDP then pushes the privilege to the policy enforcement point (PEP) to enforce the decision to all the worker nodes and storage elements involved in the federated grid. The resource provider attributes management (RPAM) interacts with the grid information system to collect the resource attributes and updates the repository so that the PEP can use the information to enforce the privilege.

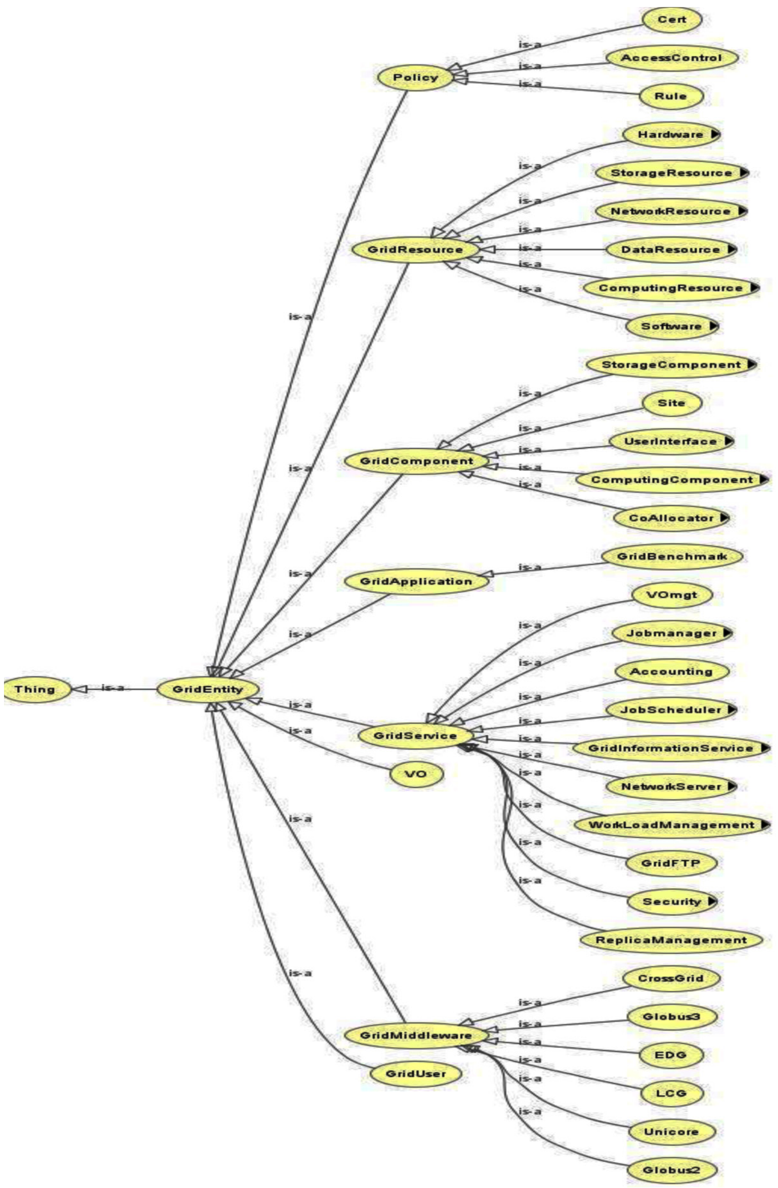

Figure 9. Modified part of the core grid ontology (Xing et al., 2006).

EVALUATION

A quantitative evaluation was performed by simulating the rule checking process used in our framework and comparing the result to the GAG

(Kaiiali et al., 2013). All the experiments were done by enhancing the grid authorization simulator (GAS) developed by Kaiiali et al. (2013). The GAS was run on a Windows 7 machine with Intel Core i7 CPU at 2.10 GHz with 12 GB of RAM. First, we validated our simulator by initiating 100 different authorization processes with the input of randomly generated authorization rules. After that, we ran our simulator using 100 initiated authorizations for a grid consisting of 200 resources and 15 security rules. Then, a graph comparing GAG with our method was plotted. The X axis ("Experiment No.") was for the number of initiating authorization processes, and the Y axis ("Number of Checked Security Rules") was for the authorization complexity. Figure 10 is a graph of the complexity checking for 100 initiated authorization processes for 12 resources with four authorization rules, while Figure 11 is a graph of the complexity checking for 100 initiated authorization processes for 200 resources with 15 authorization rules. The dotted line represents the GAG and the non-dotted line represents the proposed method.

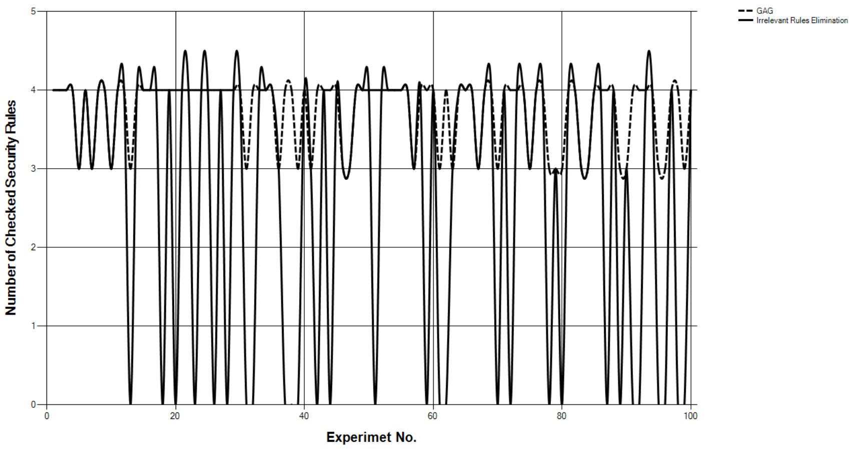

Figure 10. Complexity of rule checking for 100 initiated authorization processes for a grid consisting of 12 resources and four authorization rules using the GAG and proposed method.

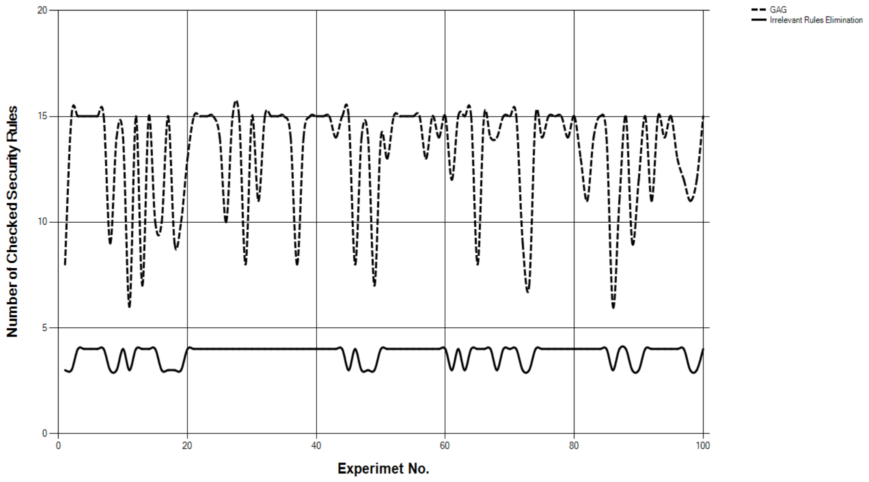

Figure 11. Complexity of rule checking for 100 initiated authorization processes for a grid consisting of 200 resources and 15 security rules using the GAG and proposed method.

DISCUSSION

From the results presented above in Figure 10, we can realize that the maximum number of checking authorization rules for the GAG is equal to the number of authorization rules existing in the system. This result is in agreement with the result obtained by Kaiiali et al. (2013). It proves that our simulation result is correct. It is noted that the average minimum number of rule checks for the GAG was equal to 2, compared to 0 for our method. This is true because while the GAG checked all the possible authorization policies, the checking process is sometimes skipped in our method due to the irrelevance of the rules. The results presented above in Figure 11 showed that there was a significant reduction in the number of checks using our method in a larger grid environment. It is noted that a large grid environment consists of a large number of resources and rules including a large number of irrelevant rule sets. The elimination of those sets has a significant impact on reducing complexity checking in the larger grid environment.

To further compare the result between our method and the GAG, the percentage of the total reduction of rule checking was calculated based on the average number of rule checks. The result is presented in Table 1.

Table 1

Percentage Comparison of the Average Number of Security Rule Checks for 100 Initiated Authorization Processes for a Grid Consisting of 200 Resources and 15 Security Rules

Method	Average number of security rule checks	$\frac{\textbf{Average number of security rule checks}}{\textbf{\textit{Total Security Rules}}}\ \boldsymbol{X}\ \mathbf{100\%}$
Irrelevant Rule Elimination (our method)	3	20
GAG	12	83
Total reductions =		63%

CONCLUSION AND FUTURE WORKS

To briefly summarize, we have proposed a new solution for facilitating federated grid authorization. This solution enhances the previous approaches by combining UCON features and semantic technology in order to improve the methods of controlling the granularity of the security policy to support the grid authorization requirements for a large grid environment. In the framework, we create the policy filter that uses a new mechanism to reduce the complexity of the access control policy. From the results of our simulation, our mechanism is shown to gain a 63% reduction on complexity checking compared to the GAG. We believe this work contributes to the enhanced performance of federated grid authorization systems. For future work, we plan to adopt the idea and method used in Yuhanis et al. (2012) which calculate file dependency using file weight parameter and evaluate this framework based on the that performance metric. We also plan to prove the feasibility of this concept by implementing this framework in a real grid test bed for more advanced and accurate evaluation.

ACKNOWLEDGMENT

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

REFERENCES

Alfieri, R., Cecchini, R., Ciaschini, V., & Agnello, L. (2005). From gridmap-file to VOMS: Managing authorization in a grid environment. *Future Generation Computer Systems*, *21*(4), 549–558. doi:10.1016/j.future.2004.10.006

Bumpu, W., Sweitzer, J., Thompson, P., Westerine, A., & Williams, R. (2000). *Common information model: Implementing the object model for enterprise management*. John Wiley & Sons.

Cakrabarti, A. (2007). *Grid computing security*. New York, New York, USA: Springer-Verlag Berlin Heidelberg.

Chadwick, D. W., & Otenko, O. (2003). The PERMIS X. 509 role based privilege management infrastructure. *Future Generation Computer Systems*, *19*(2), 277–289.

Chen, H., Perich, F., Finin, T., & Joshi, A. (2004). SOUPA: Standard ontology for ubiquitous and pervasive applications. In *Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04)* (pp. 258–267).

Cody, E., Sharman, R., Rao, R. H., & Upadhyaya, S. (2008). Security in grid computing: A review and synthesis. *Journal Decision Support Systems*, *44*(44), 749–764. doi:10.1016/j.dss.2007.09.007

Foster, I., Kesselman, C., Tsudik, G., & Tuecke, S. (1998). A security architecture for computational grids. In *The 5th ACM Conference on Computer & Communication Security (CCS'98)* (pp. 83 –92). San Francisco, CA USA: ACM Press. doi:10.1145/288090.288111

Foster, Ian & Kesselman, C. (Eds.) (2004). *The Grid: Blueprint for a new computing infrastructure* (2nd ed.). San Francisco, CA USA: Morgan Kaufmann Publishers.

Horrocks, I., Patel-Schneider, P. F., Boley, H., Tabet, S., Grosof, B., & Dean, M. (2004). *SWRL: A semantic web rule language combining OWL and RuleML. W3C*. Retrieved from http://www.w3.org/Submission/SWRL/

Ibrahim, M., Hamdan, S. N., Ibrahim, H., Abdullah, A., & Latip, R. (2012). Intergrid security policy integration framework based on UCON toward federated grid access control. In *Proceedings of the International Conference on Informatics and Applications (ICIA2012)* (pp. 205–212).

Ibrahim, M., Ibrahim, H., Abdullah, A., & Latip, R. (2014). Enhancing the performance of advanced fine-grained grid authorization system. *Journal of Computer Science*, *10*(12), 2576–2583. doi:10.3844/jcssp.2014.2576.2583

Kaiiali, M., Wankar, R., Rao, C. R. R., Agarwal, A., & Buyya, R. (2013). Grid authorization graph. *Future Generation Computer Systems*, *29*(8), 1909–1918. doi:10.1016/j.future.2013.04.010

Lorch, M., Cowles, B., Baker, R., Gommans, L., Madsen, P., McNab, A., … Thompson, M. R. (2004). *GFD-1.038 Conceptual Grid Authorization Framework and Classification. Global Grid Forum.*

Marín Pérez, J. M., Bernabé, J. B., Alcaraz Calero, J. M., Garcia Clemente, F. J., Pérez, G. M., & Gómez Skarmeta, A. F. (2011). Semantic-based authorization architecture for Grid. *Future Generation Computer Systems*, *27*(1), 40–55. doi:10.1016/j.future.2010.07.008

Martinelli, F., & Mori, P. (2010). On usage control for GRID systems. *Future Generation Computer Systems*, *26*(7), 1032–1042. doi:10.1016/j.future.2009.12.005

Pearlman, L., Welch, V., Foster, I., Kesselman, C., & Tuecke, S. (2002). A community authorization service for group collaboration. In *Proceedings of Third International Workshop on Policies for Distributed Systems and Networks (POLICY'02)* (pp. 50–59). doi:10.1109/POLICY.2002.1011293

Sandhu, R. (n.d.). The PEI framework for application-centric security. In *Proceedings of 5th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Crystal City, Virginia.* (pp. 1–5).

Stagni, F. (2009). *On usage control for data Grids: Models, architectures, and specifications control*. University of Ferrara, Italy.

Thompson, M. R., Essiari, A., & Mudumbai, S. (2003). Certificate-based authorization policy in a PKI environment. *ACM Transactions on Information and System Security*, *6*(4), 566–588. doi:10.1145/950191.950196

Welch, V., Siebenlist, F., Foster, I., Bresnahan, J., Czajkowski, K., Gawor, J., … Tuecke, S. (2003). Security for Grid services. In *Proceedings of the 12th IEEE International Symposium on High Performance Distributed Computing, 2003* (pp. 48–57). IEEE Comput. Soc. doi:10.1109/HPDC.2003.1210015

W3C OWL Working Group. (2012). OWL 2 web ontology language: Document overview. *W3C*. Retrieved from http://www.w3.org/TR/owl2-overview/

Xing, W., Dikaiakos, M. D. M. D., & Sakellariou, R. (2006). A Core Grid Ontology for the Semantic Grid. In *Proceedings of the Sixth IEEE International Symposium on Cluster Computing and the Grid (CCGRID'06)* (pp. 178–184). Ieee. doi:10.1109/CCGRID.2006.3

Yuhanis, Y., Madi, M., & Hassan, S. (2012). Dynamic replication strategy based on exponential model and dependency relationships in data Grid. *Journal of Information and Communication Technology*, *11*, 193–206.

Zhang, X., Nakae, M., Covington, M. J., & Sandhu, R. (2008). A usage-based authorization framework for collaborative computing systems. *ACM Transactions on Information and System Security*, *11*(1(3), 1–36. doi:10.1145/1133058.1133084

Zhang, X., Parisi-Presicce, F., Sandhu, R., & Park, J. (2005). Formal model and policy specification of usage control. *ACM Transactions on Information and System Security*, *8*(4), 351–387. doi:10.1145/1108906.1108908