Optimization of Dynamic Access Control Mechanism in Grid Computing

[1] Johnson Durai .A.R, [2] Chidambaranathan.S
[1] Research Scholar, [2] Associate Professor
[1]Manonamaniam Sundaranar University, [2] St.Xaviers College,
[1] johnsonduraiar@rediffmail.com
[1,2] Tirunelveli, Tamilnadu, India

Abstract:

Grid Computing Services are now reliable and plays its vital role in our day today world of collaborative Information Technology .Since the scalability of users and their accessing nature are Enhanced in the electronic communication medium towards the multiplicity mode of interaction, static request and response guaranteed is never an achievement until the dynamic quality of communication must be ensured by both the customers and the service providers. Nowadays the dynamic access control mechanism in Grid defines the Grid Service Provider to survive in this competitive corporate culture which proves it in the recent years with the improved methodologies compared earlier. This paper deals with the optimization of dynamic access control mechanism in Grid computing services environment. The proposed optimization method is an augmented approach with the unique individual implementation towards the fine tuning of Dynamic access control mechanism improvements. The results and discussions of our proposed method lead to the implementation of Scalable Dynamic Access control mechanism for the Grid computing environment services.

Index Terms: *Grid, Dynamic access, Optimization, Access control, and Enhancement*

1.Introduction

The Grid is an emergent technology that can be defined as a system able to share resources and provide problem solving in a coordinated manner within dynamic, multi-institutional virtual organizations[8]. This definition depends mostly on the sharing of resources and the collaboration of individual users or groups within the same or among different virtual organizations, in a service oriented approach[5].

The Grid's unique characteristics, such as its highly distributed nature and the heterogeneity of its resources, require the revision of a number of security concepts Trust, authentication, authorization and access control are some of the security concepts met in Grid systems[9]. Access control is of vital importance in a Grid environment since it is concerned with allowing a user to access a number of Grid resources. This is mainly due to the partially or weak fulfillment of the access control requirements in Grid systems[3].

The process of access control in any computer system guarantees that any access to the resources of the system conforms to its access control policy. The application of the abstract concept of the reference monitor is capable of providing the requirements that are posed from the access control process[1].

The reference monitor operates as an access mediator between the User's access requests and the Grid Service Response objects. The accesses comply with the system's security policy[2]. The reference monitor can be informed for the security policy of the computer system from an access control database. Moreover, all the security relevant transactions are kept into an audit file for security and traceability reasons [6].

The Grid access control architecture and dynamic access control mechanism are represented in Figure 1 and Figure 2 respectively.

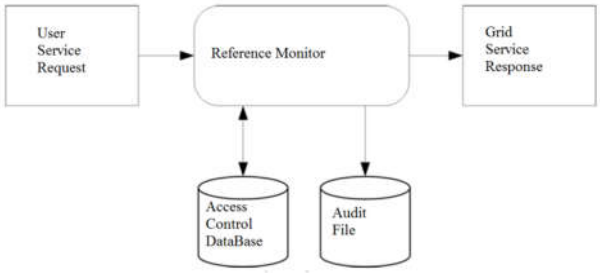

Figure 1. Grid access control Architecture

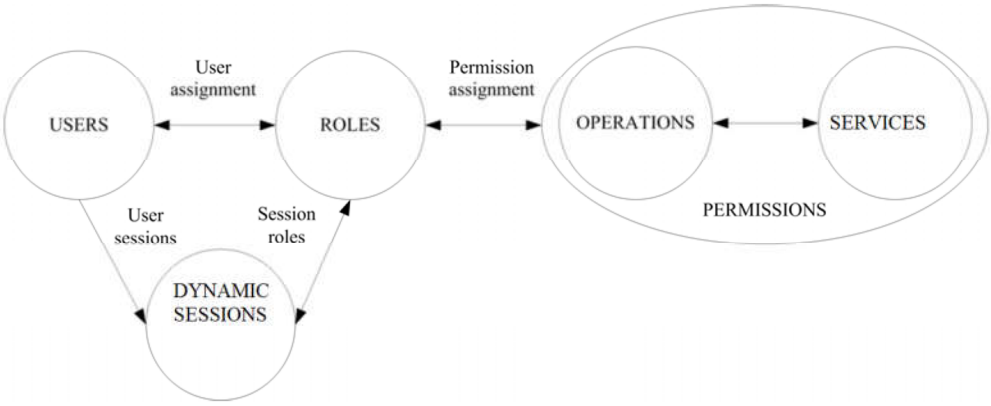

Figure 2: Dynamic Access Control Mechanism in Grid Computing

2. Methodology Requirement

The backbone of Dynamic Access Control Mechanism depends on two entities, the role and need in accessing Grid computing services. They are as follows [2],

2.1 Role of Dynamic Access Control Mechanism

Dynamic access control represents the access control mechanism that dynamically adjusts *role assignments* to users based on their context information. Dynamic separation of duty relationships handles conflict of interest policies in the context of a session. In this case, the user is actively logged into the system and a set of the user's assigned roles is activated. These constraints are described during the design time, as it happens with the static separation of duty relationships. However, they are applied during the run-time, in the context of a session, and they prevent the simultaneous activation of two or more conflicting roles. In case of role hierarchies, the same as in static separation of duty relationships applies with the difference that they are enforced only on the activated user's roles.

2.2 Needs for Dynamic Access Control Mechanism:

The necessities to implement dynamic access control mechanism for the grid computing environment are as follows,

1. User to User collaboration-User with different sessions change dynamically.

2. Component to Component Interaction-Service access feasibility.

3. Users collaborate access resource-User access service mode.

3. Implementation

This paper deals with the proposed methodology for optimizing the Dynamic access control mechanism in terms of reducing the ambiguity by providing the solutions or alternates for the issues in effective Grid services consumption .

3.1 Proposed Methodology:

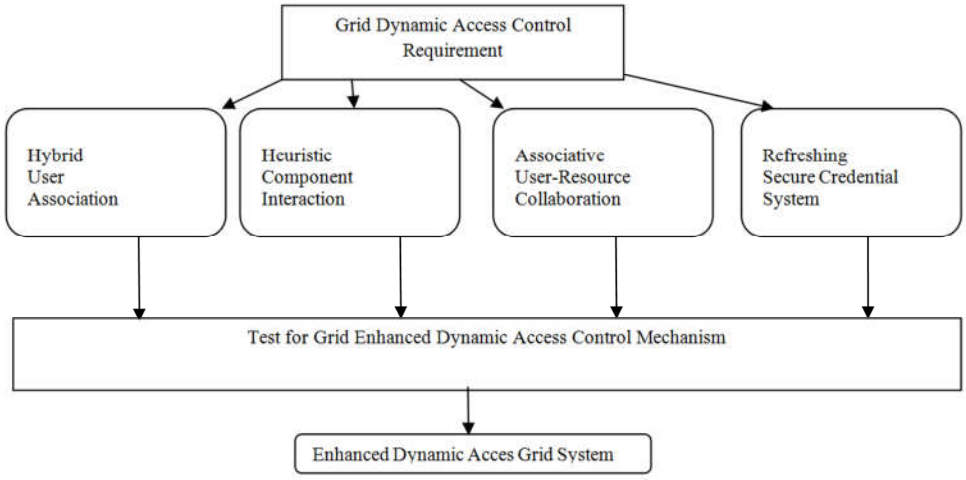

Figure 3. Proposed Dynamic Access Control Mechanism for Grid Services

3.2 Hybrid User Association

A multiple user environment or a single user with different access nature equates the users from different domain will associated to access the grid services. The identity of the user is not the only credential to make access control decision but also focusing on the location, network usage and environment to grant permission. As this information is dynamic and will change from time to time, observably, dynamic access control mechanism is necessary. The solution to this issue can be implemented by developing a Fuzzy membership based model as Fuzzy f(x).f(x) is in [0, 1] such that hierarchical descending values from Genuine to infeasible components. The resultant membership assignments are represented in the following table 1,

Table 1. Hybrid User Association Membership assignment

Device/Gain	Type	Membership values f(x)
Location	Non Secure	0.1
	Unknown	0.3
	Public Isolated	0.5
	Secured	0.7
	Privacy	0.9
Network Bandwidth	>10 MBps	0.9
	1- 5 MBps	0.7
	Upto 1 MBps	0.5
	<512 KBps	0.3
	<64 KBps	0.1
Local policy	Centralized	0.3

Architecture	Semi Centralized	0.5
	Decentralized	0.7
Secured environment	Non-Secured	0.1
	Unknown	0.4
	Secured	0.7

3.3 Heuristic Component Interaction

High preferences user has higher priority to use the resource by changing the low accessed. Similarly no trust relationship with the user component restricts other components to access the critical service. Also in order to maintain congestion control only limited resource accessing will be permitted. The solution to this issue can be implemented by developing a Fuzzy membership based model as Fuzzy f(x).f(x) is in [0, 1] such that hierarchical descending values from Genuine to infeasible components. The resultant membership assignments are represented in the following table 2,

Table 2. Heuristic Component Interaction Membership

Device/Gain	Type	Membership values
Privilege preferences	Best	0.9
	High	0.7
	Average	0.5
	Low	0.3
	Least	0.1
Trust Relationship	Distrust	0.1
	Suspect	0.2
	Normal	0.5
	Good	0.7
	Trust worthy	0.9
Simultaneous Access	Free Access	0.9
	Yet to Full	0.5
	Congestion	0.1
Autonomy	Self-Configure	0.5
	Self-Heal	0.6
	Self-Operative	0.7
	Self-Optimize	0.8
	Self-Protection	0.9

3.4 Associative User Resource Collaboration

The network topology will be dynamically updated, the new resource will be dynamically included, and the user who accesses the resource can be anyone. In such a dynamic and heterogeneous environment, if the user moves to another site which is not secure, the delegate application will possible be denied to continue access some resource because the potential risk of leaking information to malicious user. The solution to this issue can be implemented by developing a Fuzzy membership based model as Fuzzy f(x).f(x) is in [0, 1] such that hierarchical descending values from Genuine to infeasible components. The resultant membership assignments are represented in the following table 3,

Table 3. Associative User resource Collaboration Membership

User Access	Type	Membership values
Application	Same Location	0.1
	Different Location	0.3
	Mobile Data	0.5
	Self-Wifi	0.7
	Public-Wifi	0.9
Simulation	Distrust	0.1
	Suspect	0.2
	Normal	0.5
	Good	0.7

3.5 Refreshing Secure Credential System

Short Term Time division credentials consist of an access key ID and a secret access key, but they also include a security token that indicates when the credentials expire. Long-term credentials are remaining valid until the customer manually revokes them. However, temporary security credentials expire after a short period of time provides the optimal security [7].

Also Implement different access keys for different services for the same user also enhances the security. A customer can separate the permissions and revoke the access keys for individual applications if an access key is exposed [4].

4. Results and Discussion

Consider the case studies of a single user want to access dynamically the grid computing resources which is YET TO FULL for our proposed methodology as follows,

Case-1: Privacy User having 1 MBps speed resides on semi centralized policy architecture within a secured environment. The user is a prime user with trust worthy and self configurable, able to access through application or simulation.

Case-2: Public isolated location having more than 10 MBps speed ,moving towards unknown environment of decentralized policy architecture with average privileges, normal trust and self configurable , able to access through application or simulation in mobile data .

Case-3: Non secured location having <64KBps speed, resides on a centralized policy architecture within a distrust region, able to access through application or simulation using public Wifi.

The three cases access permission assessment is illustrated in the following tables Table 4, Table 5, Table 6 and Table 7.

Table 4. Hybrid User Association Access Permission Assessment

Device/Gain	Type	Membership values	Access Permission
Location	Non Secure	0.1	Case-3
	Unknown	0.3	
	Public Isolated	0.5	Case-2
	Secured	0.7	
	Privacy	0.9	Case-1
Network Bandwidth	>10 MBps	0.9	Case-2
	1- 5 MBps	0.7	
	Upto 1 MBps	0.5	Case-1
	<512 KBps	0.3	
	<64 KBps	0.1	Case-3
Local policy Architecture	Centralized	0.3	Case-3
	Semi Centralized	0.5	Case-1
	Decentralized	0.7	Case-2
Secured environment	Non-Secured	0.1	Case-3
	Unknown	0.4	Case-2
	Secured	0.7	Case-1

Table 5. Hybrid Component Interaction Access Permission Assessment

Device/Gain	Type	Membership values	Access Permission
Privilege preferences	Best	0.9	Case-1
	High	0.7	
	Average	0.5	Case-2
	Low	0.3	
	Least	0.1	Case-3
Trust Relationship	Distrust	0.1	Case-3
	Suspect	0.2	
	Normal	0.5	Case-2
	Good	0.7	
	Trust worthy	0.9	Case-1
Simultaneous Access	Free Access	0.9	
	Yet to Full	0.5	Case-1,2,3
	Congestion	0.1	
Autonomy	Self-Configure	0.5	Case-1,2,3
	Self-Heal	0.6	
	Self-Operative	0.7	
	Self-Optimize	0.8	
	Self-Protection	0.9	

Table 6. Associative User Resource Access Permission Assessment

User Access	Type	Membership values	Access Permission
Application	Same Location	0.9	Case-1
	Different Location	0.7	
	Mobile Data	0.5	Case-2
	Self-Wifi	0.3	
	Public-Wifi	0.1	Case-3
Simulation	Distrust	0.1	Case-3
	Suspect	0.2	Case-2
	Normal	0.5	Case-1
	Good	0.7	

Table 7. Access Permission computation Table

Cases	Hybrid User Association	Heuristic Component Interaction	User Resource Collaboration Application	User Resource Collaboration Simulation
Case-1	Avg(0.9+0.5+0.5+0.7)=0.65	Avg(0.9+0.9+0.5+0.5)=0.7	**0.9**	**0.5**
Case-2	Avg(0.5+0.9+0.7+0.4)=0.625	Avg(0.5+0.5+0.5+0.5)=0.5	**0.5**	0.2
Case-3	Avg(0.1+0.1+0.3+0.1)=0.15	Avg(0.1+0.1+0.5+0.5)=0.3	0.1	0.1

The Final result is the User with Case-1 and Case-2 scenario using Application based dynamic accessing will be permitted. But Case-2 with Simulation based Dynamic Grid accessing will not be permitted. Moreover User with Case-3 Scenario will not be permitted for dynamic access of resources in Grid computing environment. The proposed methodology yields the summarized improvement as follows,

1 out of 3 cases restricted =>33% efficiency (Case-3 elimination)

Case-2 restriction for simulation=>33/2=16.5 % efficiency.

Our proposed methodology yields the efficiency gain of nearly 50 % towards optimized enhancement in Dynamic Access control in Grid Computing environment.

The resultant graph for Optimized Dynamic access Permission in grid Services is as follows,

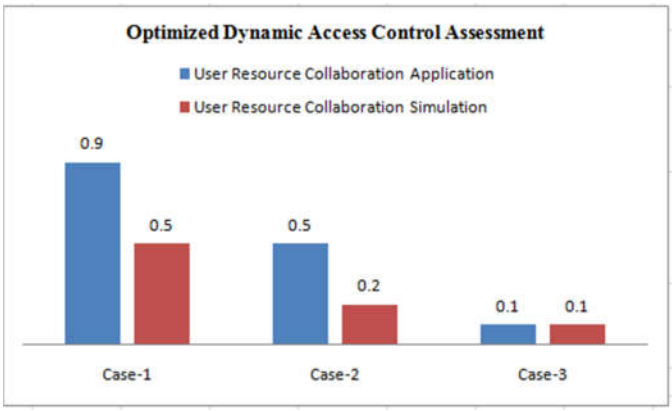

Figure 4. Resultant graph for Optimized Dynamic access Permission in grid Services

Coding for Maple Soft tool using C# script [10]

The following sample code in C# script for Grid Maple Soft Tool is used to implement dynamic access control mechanism for student data table towards St.Xaviers College Tirunelveli in order to attain the access permission for a genuine user session.

```
Using System;
Using System. Data;
Using System.Collections.Generic;
Using System.Linq;
Using StXaviersCollege.Data;
namespace StXaviersCollege.Rules
{

public partial class DynamicAccessRules : StXaviersCollege.Data.AccessRules

 {

     protected override void EnumerateDynamicAccessControlRules(string
controllerName)
     {
        RegisterAccessControlRule(
           "UserID", AccessPermission.Allow, "JOHNSON", "DURAIAR");
        RegisterAccessControlRule (
           "UserID",
           "[Location] =@Location and [Policy] = @Policy",
           "Select UserID from Students" +
           "Where Location=@Location and Policy=@Policy",
           AccessPermission.Allow,
           new SqlParam ("@Location", "Privacy"),
           new SqlParam ("@Policy", "Decentralized"));

        RegisterAccessControlRule(
           "UserID",
"[Preference]=@Preference and [Trust] = @Trust",
           "select UserID from Students " +
           "where Preference=@Preference and Trust=@Trust"
           AccessPermission.Allow,
           new SqlParam("@Preference", "Best"),
```

```
            new SqlParam("@Trust", "Worth"));

          RegisterAccessControlRule(
            "UserID",
"[Autonomy]=@Autonomy and [Application] = @Application",
            "select UserID from Students " +
            "where Autonomy=@Autonomy and Application=@Application",
            AccessPermission.Allow,
            new SqlParam("@Autonomy", "Self Protection"),
            new SqlParam("@Application", "Mobile Data"));
      }
   }
}
```

The proposed methodology yields the optimization in Dynamic Access Control mechanism by minimum 50 % for Grid computing services.

5.Conclusion

The optimized dynamic access control mechanism for grid computing services are in essential need for the surplus amount of augmentation in technical user access, which lead to the safety necessity for efficient grid accessing services to all the requestors. The dynamic access control focuses on the user association, component interaction, resource collaboration and safety service access throughout the transaction and protection. In this paper we deal with optimization methods which comprises several component enhancement fusion of hybrid user association, Heuristic component interaction, Associative resource collaboration with multiple access keys in short term mode of refreshment basis are used for security Upgradation which yields a specific level of guaranteed service for the user side to enhance the access control mechanism for grid computing services in dynamic mode. The stage by stage wise fuzzy membership based implementation produces minimum 50% optimization in the proposed research methodology. The fine tuning of security in grid computing services can also be enhanced by identifying the specific amount of guaranteed short term tokens between the user and the policy enhancer through Grid services. In near future this proposed methodology will be extended to deal with Dynamic access control mechanism using Neural networks concepts.

REFERENCES

[1] Alfteri. R, R. Cecchini, V. Ciaschini, L. Dellagnello, A. Frohner, A. Gianoli, K. Lorentey,and F. Spataro VOMS, An Authorization System for Virtual Organizations, In 1st European Across Grids Conference, Santiago de Compostable, **(2003)**.

[2] Barton. T, J. Basney, T. Freeman, T. Scavo, F. Siebenlist, V. Welch, R. Ananthakrishnan, B. Baker, M. Goode, and K. Keahey. Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, Gridshib, and My Proxy. In *5th Annual PKI R&D Workshop*, **(2006)**.

[3] Chadwick. D. Authorization in Grid Computing. Information Security Technical Report, 10(1):33-40, **(2005)**.

[4] Foster. I, C. Kesselman, and S. Tuecke. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International J. Supercomputer Applications, **(2001)**.

[5] Frey. J, Foster. I , S. Graham, S. Tuecke, K. Czajkowski, D. Ferguson, F. Leymann, M. Nally, T. Storey, and S. Weerawaranna. Modeling Stateful Resources with Web Services. Globus Alliance, **(2004)**.

[6] ISO/IEC 10181-3:**(1996)**, Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Access Control Framework.

[7] Otenko. A and Chadwick. D. The PERMIS X.509 Role based Privilege Management Infrastructure. Future Generation Computer Systems, 19(2):277-289,**(2003)**.

[8] Welch. V, R. Ananthakrishnan, S. Meder, L. Pearlman, and F. Siebenlist. Use of SAML for OGSA Authorization (work in progress), Global Grid Forum, **(2004)**.

[9] Welch. V, T. Barton, K. Keahey, and F. Siebenlist. Attributes, Anonymity, and Access: Shibboleth and Globus Integration to Facilitate Grid Collaboration. In 4th Annual PKI R&D Workshop,**(2005)**.

[10]www.maplesoft.com/path=grid/support/En