Enhancement of Scalable 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, Manonmaniam Sundaranar University
[1,2] Tirunelveli, Tamilnadu, India

Abstract: Nowadays the impact of Grid services through Grid Systems are a considerable phenomenon due to our online accessing features and capability through feasible providers. Grid systems are a composition of autonomous domains, which are most probably open and dynamic. Grid systems handle large number of users, who are frequently changeable, and different domains have their own policies. The existing identity based models are closed and inflexible. Scalability and the capacity for distributed control have unfortunately not extended well to resource access-control policies and mechanisms.This paper deals with the issues raised by scaling up of measures such as number of users, protocols, applications, network elements in a grid topological constraints, and functionality expectations. The proposed enhancement method is a unification approach with the unique individual implementation towards the fine tuning of scaling improvements. The results and discussions of our proposed method lead to the implementation of enhancement of scalable access control mechanism in grid computing.

Index Terms: **Grid, Scalable, Access Control, Unification, Enhancement**

I.INTRODUCTION

A *service* is an implementation of well defined functions that are able to interact with other functions. The *service oriented architecture* (SOA) is comprised of a set of services that can be realized by technologies such as the web services [4].

A *domain* can be defined as a protected computer environment, consisted of users and resources under an access control policy. The collaboration which can be established among domains leads to the formation of a virtual organization.

A *user* in a Grid environment can be a set of user identifiers or a set of invoked services that can perform on request one or more operations on a set of resources. Furthermore, we identify two types of users. These are the resource requestor and the resource provider [9]. The former type of user acts like a resource access or usage requestor, and the latter type of user acts like a provider of its own sharable resources. All users are restricted by the policies enforced in their participating domains and virtual organization [6].

A *resource* in a Grid environment can be any sharable hardware or software asset in a domain and upon which an operation can be performed [5].

Access control's role is to control and limit the actions or operations in the Grid system that is performed by a user on a set of resources. In brief, it enforces the access control policy of the system, and at the same time it prevents the access policy from subversion. Access control in the literature is also referred to as access authorization or simply authorization [2].

A Grid *access control policy [3]* can be defined as a Grid security requirement that specifies how a user may access a specific resource and when. Such a policy can be enforced in a Grid system through an *access control mechanism.* The latter is responsible for granting or denying a user access upon a resource. Finally, an *access control model* can be defined as an abstract container of a collection of access control mechanism implementations [8], which is capable of preserving support for the reasoning of the system policies through a conceptual framework. The Grid service architecture is represented in Figure 1.1.

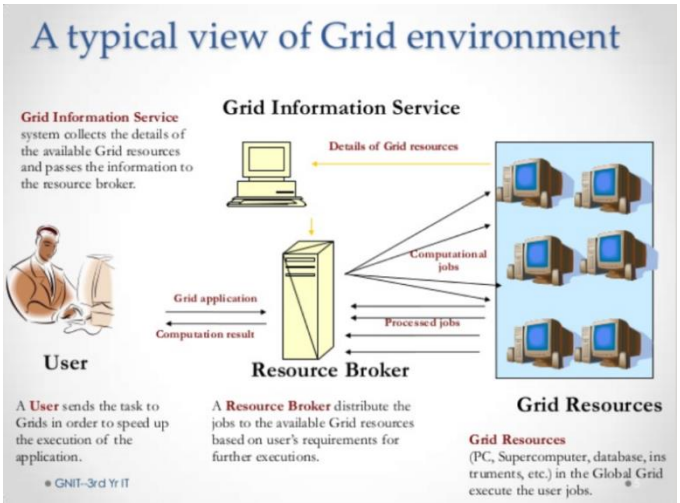

Figure 1.1: Grid Service Architecture [10]

II. METHODOLOGY REQUIREMENT

Scalability Issue:

Scalability does not focus on the size alone but also improving the local autonomy by delegating functionality to end nodes has led to scalable Grid systems. Scalability and service distribution control are not enhanced well in the past for resource access-control policies and mechanisms. Moreover security management is becoming an increasingly challenging problem, due to

scaling up of measures such as number of users, protocols, applications, network elements, topological constraints, and expected functionalities. The upgraded scalable system must be implemented, deployed and applied in a manner such that the management, maintenance and operational costs do not increase as the number of system components (users, applications, policies and enforcement points) increases.

The final Upgradation for the Enhanced Scalable Grid System consists of the following requirements,
1. Feasible architecture for extension and maintenance.
2. Handling Administrative Complexity [7].
3. Modifications, Grants and revokes in Policy Management.
4. Safety and Secured Credential Management System for proper utilization of resources [1].

III.PROPOSED IMPLEMENTATION

We consider scalability at the architectural level, *i.e.*, whether it is possible for the system to be implemented, deployed and used in a manner where management, maintenance and operational costs do not increase as the number of system components (users, applications, policies and enforcement points) increases

3.1 Proposed Methodology:

The proposed methodology for the enhancement in Grid scalability implementation diagram is as follows,

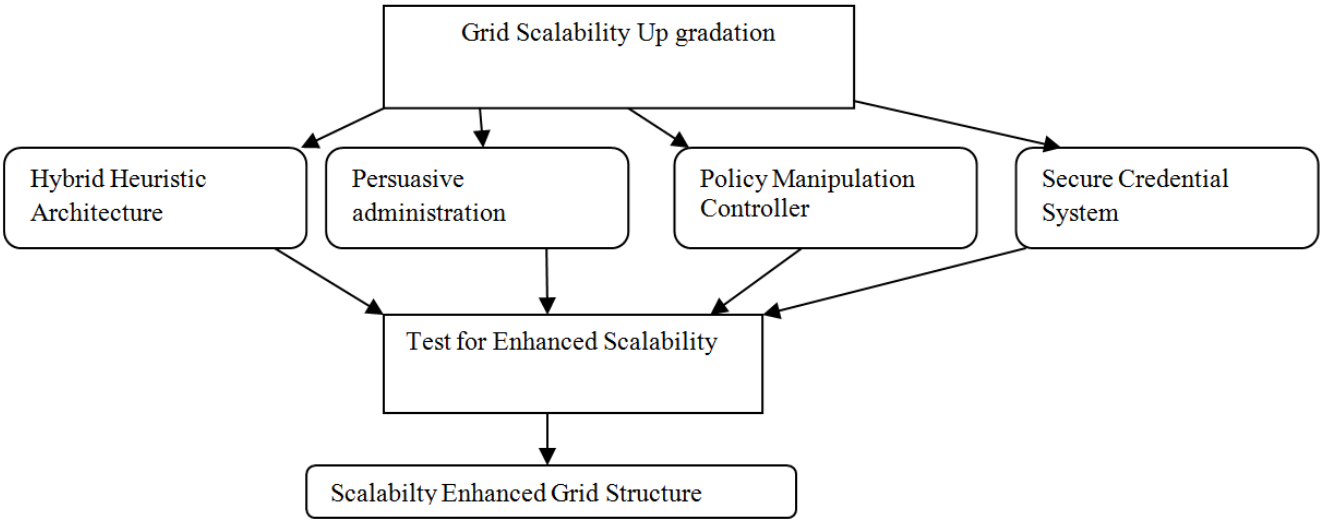

Figure 3.1: Proposed Methodology for Grid Scalability Enhancement

3.2. Proposed Hybrid Heuristic Architecture

The development of Hybrid architecture is based on the Service type categories. The services are divided into three types based on its preferences to the customer value system and features on grid server system services. They are,

3.2.1. Exclusive Services:

These services are decentralized services opt for the most valuable users with more cost expensive services, so that the scalability enhancement will not be affected with proper preference based system and dedication servers.

3.2.2. Prime Services:

These services are Semi centralized services opt for the optimal valuable users with more featured services, so that the side effect of scalability enhancement will be reduced by choice based allocation servers.

3.3.3. General Basic Services:

These services are centralized services opt for the generic valuable users with more basic fundamental services; the scalability enhancement will not be affected by proper queue based time token system.

The following Figure 3.2 represents the proposed Hybrid architecture.

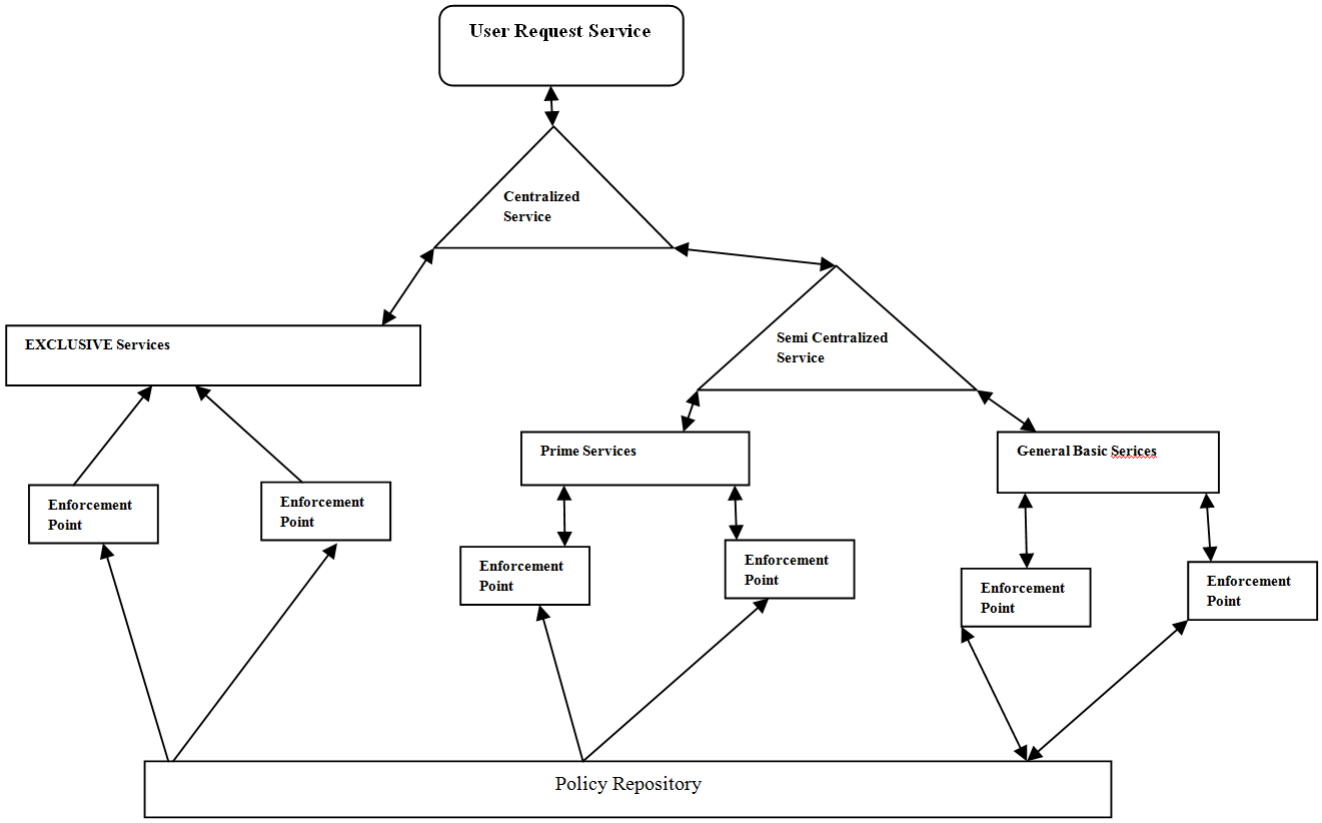

Figure 3.2: Proposed Hybrid Architecture for Grid Scalability Enhancement

3.3. Proposed Persuasive Administration Structure:

The enhanced Grid scale affects the ability of human administrators to maintain its complexity. The proposed methodology to tackle this issue by assigning proper responsibility by the approach of Hungarian assignment problem solution by reducing the cost. The following Table 3.2, Table 3.3 and Table 3.4 are the assignment solution for the sample Cost Matrix Table 3.1.

Table 3.1: Service Administrators Task assignment Cost Matrix

Service/Admin Cost Matrix	Admin-1	Admin-2	Admin-3
Exclusive	8	7	3
Prime	6	2	5
Generic	9	1	6

Table 3.2: Step-1 for Row Reduction

5	4	0
4	0	3
8	0	5

Table 3.3: Step-2 for Column reduction

1	4	0
0	0	3
4	0	5

Table 3.4: Step-3 for Test for Optimality

1	4	**0**
0	-	3
4	**0**	5

Result:
Exclusive service by Admin-3 Cost Expenditure=3
Prime service by Admin-1 Cost Expenditure=6
Generic service by Admin-2 Cost Expenditure=1
Total Cost=10 units
Proposed Persuasive Administrative structure reduced the total cost of 10 units.

3.4 Proposed Time Division Credential System:

In a credential-based access control system, new user registration or Access grant modification are equal to issuing a new credential with same set of operations. The use of credentials has many features in terms of flexibility. But the focus is on for distributing them with proper scalability and correctness of the system.

A short term Time division credential system is an alternate solution for proper user verification and KYC updation of the system in which nowadays most of the governments are concentrating, the customer with long-term credential has to periodically retrieve a short-term credential that must be used in conjunction with the long term one. They can do this by simply contacting the issuer of the credential.

For Example:

Profile Password acts as a Long term valid one whereas the login Passwords is expired with certain interval of time.

3.5 Proposed Safety 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

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.

IV.RESULTS AND DISCUSSION

By applying the proposed methodology for the enhancement in Grid scalability implementation we obtained the following results,

Test for Enhanced Scalability:

Table 4.1: Proposed Methodology for Enhanced Grid Scalability

Proposed Model Features	Type	Contention Ratio	Gain %
Architecture Contention	Hybrid (3 Components)	1: ((1-1/3)*100)	67%
Persuasive Administration Structure	Assignment Model	Avg-Exc:Avg-Pri:Gen:Opt (6+4.3+5.3):10=**15.6:10**	66%
Enhanced Gain %=(100-66% of (100-67%))			79%

The following graph represents the Test for optimality in the implementation of proposed methodology for scalability enhancement in Grid access control mechanism.

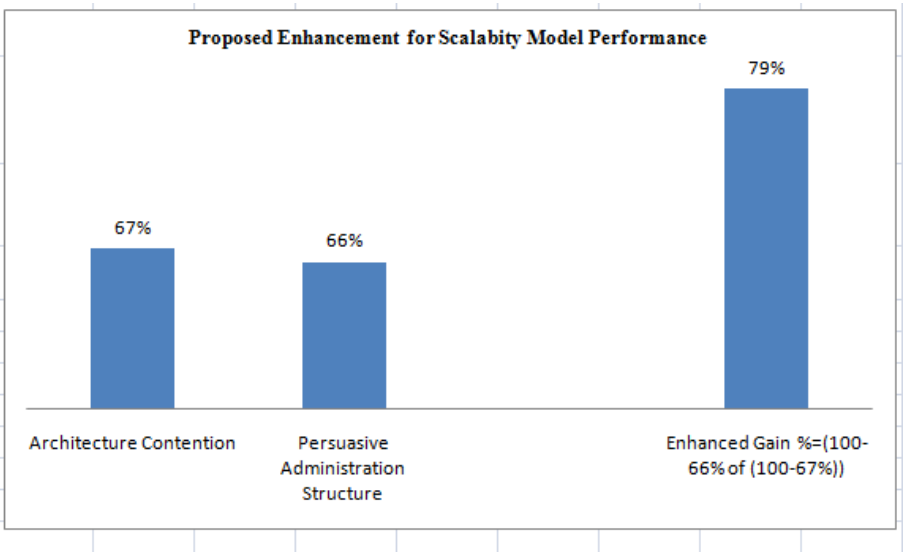

Figure 4.1: Proposed Enhancement Scalability in Grid Access control mechanism performance

The proposed Time division credential system and safety measures are qualitative measures for the supporting system rather than quantifying in terms of units. The proposed methodology provides the gain in scalability by nearly 79% for Grid access control mechanism.

V.CONCLUSION

The enhancement of scalable access control mechanism in Grid computing systems comprises the Upgradable construct for the architectural design, administrative structure, and Time division credential system along with the safety constraints. This paper provides the novel composition of Hybrid architecture, Persuasive administration. Time division credential and Short term and different access key for different services towards safety with proper care on service guarantees for different role of users. Our proposed methodology focuses on the each individual components and enhance the Grid access control mechanism system by the efficiency rate of 79%.In near future the usage of high end 128 or 256 bit THz processors utilization along with the Fuzzy

logic based Grid service allocation methodology will make this entity an admirable one for the different category of customers with simultaneous access of different level of multiple services.

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, February 13-14,2003.
[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*, April 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, 15(3):200-222, 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, February 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, May 14, 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, April 2005.
[10]https://www.slideshare.net/pramit9836/grid-computing-32947751