Towards achieving scalability and interoperability in a Triple-Domain Grid-Based Environment (3DGBE)

Nureni A. Azeez, Isabella M. Venter
Department of Computer Science,
University of the Western Cape
Private Bag X17, Bellville, 7535, South Africa

Email: 3008814@uwc.ac.za, iventer@uwc.ac.za

***Abstract*—The adoption of grid computing has posed challenges regarding access control, interoperability and scalability. Although several methods have been proposed to address these grid computing challenges, none has proven to be completely efficient and dependable. To tackle these challenges, a novel access control architecture framework, Triple-Domain Grid-Based Environment (3DGBE), modelled on role-based access control, was developed. The architecture's framework assumes three domains, each domain with an independent Local Security Monitoring Unit and a Central Security Monitoring Unit that monitor security for the entire grid. The architecture was evaluated using the G3S, a grid security services simulator and Java Runtime Environment 1.7.0.5 for implementing the workflows that define the model's task. The simulation results show that the developed architecture is reliable and efficient if measured against the observed parameters and entities. A further benefit is the reduction in the cost of policy management. This proposed framework for access control has proved to be interoperable and scalable within the parameters tested.**

Keywords: authorisation, grid, role-based access control, scalability, interoperability

I. Introduction

This paper aims at finding a solution to the problem of scalability and interoperability which poses security challenges in a grid based environment. It raises the following research question:

How should information on a grid be secured without compromising accessibility, interoperability and scalability. This can be revealed by answering the following questions:

- How should a common security policy for various domains on the grid be determined? and
- How should the security of the grid be managed to ensure accessibility of resources in an interoperable and scalable grid based environment?

Grid computing is an environment that provides unhindered access to computational infrastructure across various domains in academia and industry. It allows the porting, running, sharing and distribution of applications [1]. Since grid computing involves many users from different organizations and domains, sensitive and classified information may be vulnerable if no control policy for regulating and securing all the domains on the grid, is present [2], [3].

The concept of a grid system is analogous to a "water grid system". The facilities of a water grid system make it possible for anyone in his home to open a tap to collect water without knowing exactly where such water is being processed [4]. Similarly grid computing is able to provide endless and ubiquitous access [5] to high quality computing resources without having to know exactly where the data is being processed [1].

Buyya [4], defined a grid as follows:

> The "grid is a type of parallel and distributed system that enables the sharing, selection, and aggregation of resources distributed across multiple administrative domains based on their (resources) availability, capability, performance, cost, and users' quality-of-service."

The South African Grid (SAGrid) is a typical example of a functional grid. It is a group of South African tertiary institutions (Universities, laboratories and also the Meraka Institute) that are collaborating in the sharing of resources [6].

A. Why secure a grid?

To prevent sensitive and important information from being copied, altered, divulged to unauthorized users or manipulated, has brought about the need for security on a grid system [7].

Without security a grid cannot be considered to be dependable. However, security models on the grid are difficult to implement and to sustain, due to the complexity of the grid environment [8]. Traditional access-based control models are based on recognized inadequacies and there is thus a need to replace them with more flexible [9] models which are relevant to distributed environments [10].

B. Security challenges

Scalability: Scalability caters purposely for future expansion [11]. For a grid environment to be scalable, a centralized administration as well as regular update of the security policies is necessary [12]. In other words, scalability simply means the capability of a grid system such that it can efficiently handle both a small or large number of nodes and users [13].

Interoperability: This can be simply defined as the ability of various systems on the grid to exchange, share and utilize information across platforms. It is a security challenge due to disparate and unequal security policies.

The characteristics of an interoperable grid-based environment include:

- the presence of a central authority for security and trust;
- heterogeneous resources, service discovery and management as well as;
- the interdependence of security infrastructures [14], [15].

The remaining part of the paper is organised as follows. In Section II, a summary of related work is presented. A brief analysis of the various security requirements on the grid is explained in Section III. Section IV gives a stratum of the proposed architecture with Subsections A and B presenting the stages of the archiXIectural model. Section V provides a comprehensive overview of the components of the architecture. Section VI gives an operational overview of the model while Section VII gives an approach for evaluating security in a triple-domain grid-based environment (3DGBE). Section VIII deals with the implementation and evaluation. Finally, the paper is concluded in Section XI.

II. Related research

The research that has been done in this area can be divided into three main categories: security-policy aggregation, access control and reliability in grid security.

A. Security-policy aggregation

In a bid to ensure aggregated security policy across different domains [16] proposed Global Access Control for enforcing an aggregated security policy. A distributed object kernel security service was provided for enforcing and aggregating local and general security policies on the grid. In order to allow control of data aggregation, they provide a security framework Federated Logic Language (FELL) and a logic-based language [16]. The security constraint was enforced by mapping state-transition graphs which model different nodes on the grid. This approach is good and enforces various security measures but it is not scalable since it does not allow more nodes to be added to the grid [6]. Security-policy aggregation in terms of scalability and interoperability still needs to be addressed.

B. Access control

In the work of [17], a model was developed based on a public-key and double-identity authentication on a grid. The model was developed to ensure both authenticity and confidentiality. For the implementation of this model, they applied an RSA cryptosystem. Furthermore, a double identity authentication approach was employed, to include a *time parameter* on the server side. Finally, both the server and client produce passwords which change over time.

However, this model is not scalable and dynamic as provision was not made for adding users [17].

Some Attribute-Based Access-Control systems such as Akenti and PERMIS have been in use for several grid applications [18]. These authorization systems apply their own rules. As a result, a dynamic attribute based access control is required for the grid computing environment [19]. In this model, there is no room for interoperability across various domains on the grid.

John McLean [20] came up with a framework in which Mandatory Access Control (MAC) models, allow for changes in security to be formalized. He employed algebra to construct his model that paves the way for the discretionary access control for n persons. This model is good but does not handle the problem that emanates from the separation of duties and cyclic redundancy as a result of roles and hierarchy among participants on the grid.

C. Reliability in grid security

Laccetti and Schmid [21] came up with a framework for reliable grid security infrastructures using Grid Security Infrastructures (GSI) and Community Security Policy (CSP). Their analysis captured the policies and rules upon which GSI and CSP were based. Trust relationship based on a cryptographic key was used as a guiding principle. It was finally revealed that authentication implemented at grid levels develop a trust relationship that is transitive which is not the case when authentication is used at operating system tier. A formal model algebra was adopted in developing the security of the grid [21]. This model is not flexible as it has limited application.

III. Security requirements in a grid environment

The security requirements defined by the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU) are ITU-T Provision X.805 and X.800 [22].

A. Authorization

For any organization to allow its resources to be jointly shared between all parties involved there is need for authorization as per who should have access to any particular resource and who should not [23]. It allows permission only to authorize nodes on the network [18]. Globus Toolkit Gridmap files [24], Community Authorization Service (CAS) and Virtual Organization Membership Service (VOMS) are authorization measures usually adopted in grid computing [25].

B. Authentication and Access Control

Impersonation has been identified as a threat [11] in grid environments. Authentication is thus important to prevent illegal access [26]. The main purpose of authentication is solely to confirm that the user is who he claims to represent and not any other person. In both the shared and personal computer system, authentication is usually carried out with the use of a password and username. It has been established that when a password is used to log into the system [4], the authenticity of a user is usually fully guaranteed. However a password can be stolen hence the information on the system can be vulnerable. Digital certificates, verified by a Certificate Authority [26], are taken as the best way to ensure authentication on the internet.

C. Data Confidentiality

The purpose of data confidentiality is to protect data from being divulged to the wrong or an unintended party [27].

Two steps can be used to achieve data confidentiality; data encryption and data decryption. Also, two main types of cryptography can be used to provide data confidentiality [28], they are: symmetric and asymmetric.

IV. Stratum of the proposed architecture

The architecture is presented as two stages, each of which involves two phases—see Figure 1.

1) In the first phase, security is monitored by the local security monitoring unit (LSMU);
2) In the second phase, the central security monitoring unit (CSMU) interacts directly with all the domains of the first phase;
3) The third phase is a processing phase. All activities which result in the granting of resources are carried out in this phase;
4) The fourth phase is the grid environment (GE) phase where many resources are available. Based on a decision made in the third phase, a user is allowed access to the available resources.

A. Stage 1 of the architecture

This stage involves the interaction between various users. In Figure 2, a theoretical framework of the interaction between the user and the LSMU of three domains, as well as its interaction of the three domains and the CSMU is depicted. To explain the process of the architecture presented in Figure 2, let us assume the following scenarios:

1) Adam who is a grid user (GU) in domain A where his authorisation is verified and confirmed. Adam's status (eligibility as a user) is thus determined. This phase makes Adam's access right to the intended domain known;
2) The LSMU then sends Adam's request to access a resource in any intended domain to the CSMU to reconfirm his authorisation right in his own domain and his rights to access resources of any other domain. CSMU verifies whether Adam qualifies

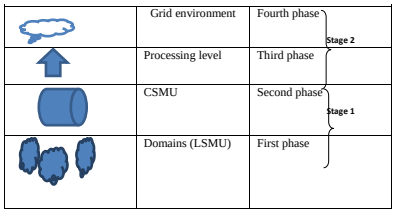

Fig. 1. Phases involved in the proposed architecture

Algorithm 1 Algorithm describing the working relationship of components in Figure 2

required by Domain A, Domain B, Domain C, LSMU, CSMU
Begin:
feedback [authorisation] = "Yes or No";
GU(Domain A,B,C) requests authorization from LSMU
if authorisation = "No"
then : terminate (process)
else:
if authorisation = "YES"
Then: LSMU forwards request to CSMU
CSMU :{(GU (role))}:
Verifies
If CSMU [permission(decision)]: = "yes"
then: CSMU moves to stage 2;
Stop

to access the required resource. There are two outcomes; YES (acceptable) or NO (not acceptable);

3) If NO, the process (request) terminates and a reject message is sent to the user;
4) If YES, a clearance certificate will be given to the user (Adam) by the LSMU of the intended domain and the user can proceed to Stage 2;
5) If there is a successful processing in Stage 2, the user will proceed to access resources in the grid environment.

B. Stage 2 of the architecture

This stage deals with the interaction between the processing phase and grid environment. This stage comes into play if and only if there is a positive feedback during Stage 1. See Figure 3 where the operation of the architecture is presented.

1) Through the grid entry link, the user requests access (with the role-authorisation certificate) from the Grid User Authentication Service (GUAS). The request is either granted or not.
2) If the feedback is negative, the entire process will be terminated immediately.
3) However, if the feedback is positive (YES), then the request will be forwarded to the Policy Information Point (PIP) (a protocol of XACML for access control). This is to source detailed information about the user. The request will further be directed to the Policy Decision Point (PDP) another XACML protocol for access control. PDP is responsible for deciding on whether the user may access the requested domain. The feedback of the PDP will either be positive (YES) or negative (NO). If the feedback is negative, the entire process stops;
4) If the feedback is YES the request is conveyed to the Policy Enforcement Point (PEP);
5) PEP will demand an updated version of the user permission certificate from the PDP (Grid VO-PDP);
6) A certificate validation/update will be transferred to the central resource database server (CRDS) from the PDP (Grid VO-PDP);
7) Finally, a message will be sent to the user to proceed and access resources on the grid.

The procedure is applicable from either of the domains available on the grid. That is, either domain A to domain B or from domain A to domain C and vice versa.

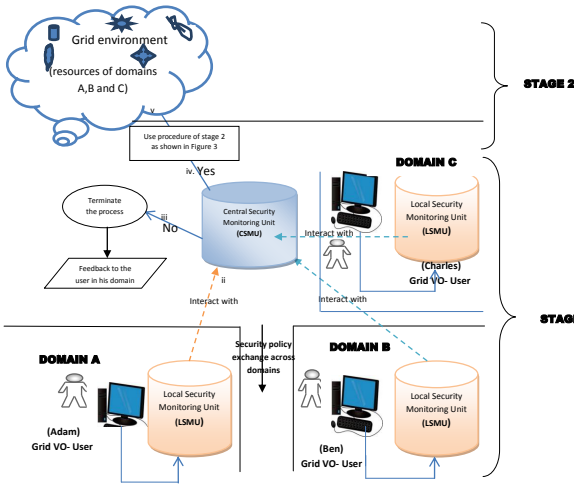

Fig. 2. A 3-domain role based access control (rbac) architecture showing interaction between users, CSMU and LSMU

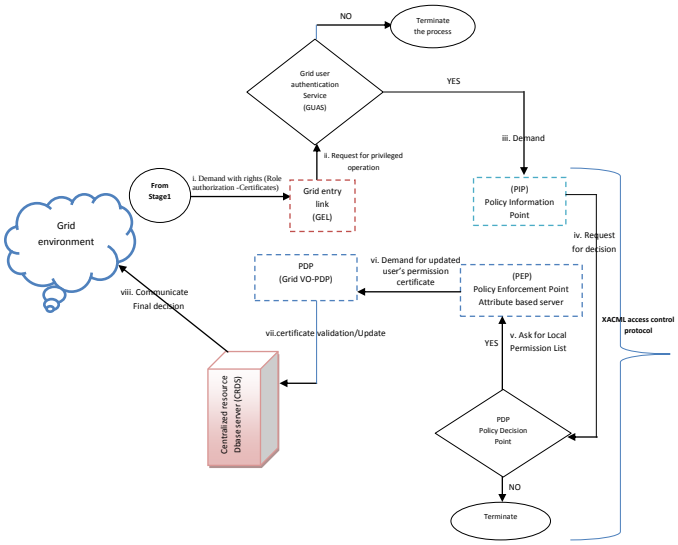

Fig. 3. A 3DGBE with RBAC architectural framework of the proposed model

In order to ensure a smooth and efficient access control mechanism on the grid and also to improve the performance of the architecture, the LSMU cooperates with the CSMU. That is, there is smooth correspondence between the local security units of all the domains with the central security unit for the entire grid. They both communicate, and work hand-in-hand to achieve a flexible, interoperable and scalable grid environment.

V. Overview of the Basic Components of the Architecture

In the proposed model, each of the domains available in the virtual organisation (VO) has an LSMU saddled with the responsibility of the domain's local security access control and management. The CSMU is an advanced access control and management system that handles access control and authorisation for the various grid entities across the three domains of the model. The CSMU along with the LSMU ensure interoperability, scalability, flexibility and secure access control for various grid entities across multiple administrative domains through inter-domain interaction; application independence as well as its

ability to accommodate additional grid entities. For any access request by a grid user, the LSMU would verify the user's access privilege. The model is based on the adoption of the XACML's (eXtensible Access Control Markup Language) request-response protocol which makes use of four basic components. The components are: PEP, PDP, PIP and PAP. However, in this model, only PEP, PDP and PIP are used because of their relevance, usefulness and application in the proposed architecture.

A. Assumptions

The following were assumed:

1) A user from Domain A (Adam) may intend to access a resource in Domain B and a user in Domain B (Ben) may also be interested in accessing resources from Domain A;
2) A user in Domain A (Adam) may wish to access resources in Domain C while a user that is in Domain C (Charles) may equally be interested in resources of Domain A.

These are two possible scenarios when a three domain based architecture is being considered. Scenario 1 is illustrated in Figures 2 and 3 and it is equally applicable to other scenarios. Adam, Ben and Charles are users in the domains A, B and C respectively. Each of them is bound with the security and access framework in their respective domains. There are six ways in which access could be requested: request can come from Domain A to Domain B, from Domain A to Domain C, from Domain B to Domain C, etc.

VI. Operational overview of the model

The security of the individual domains is quite dependable and efficient; because each of the domains has its own access control and monitoring policy which is monitored by the LSMU. If a user, however, wishes to access resources in another domain, the user from the designated domain will first need to be verified by his domain. This is achieved by translating the certificate of his domain to the domain in which he wishes to access resources. The translation (or conversion) targets the access privileges and the identities in other domains on the grid. CSMU is mainly in charge of monitoring and overseeing access and security relationship from one domain to another domain depending on where an entity requires access. Also, CSMU is equally responsible for maintaining the information for mapping interactions between domains. See Figures 2 and 3.

VII. Determination of security in a 3-domain grid VO

A. Definition of simulation parameters

In order evaluate the effectivity of the security of the domains; the following parameters defined below were taken into consideration.

Definition 1: Let $\text{DSR}(A, B)$, $\text{DSR}(A, a)$, denote the *direct security rate* which is determined and evaluated when the CSMU finds and grants permission and access privilege of a user from Domain B to Domain A or from an entity $a \in$ Domain A to Domain A depending on from where the access is requested. $\text{DSR}(A, B, C)$ denotes the DSR between the three designated domains.

Definition 2: Similarly let $\text{SR}(A, B)$ or $\text{SR}(A, a)$ denote the *security rate* for accesses from Domain B to Domain A or for an access from entity $a \in$ Domain$A$ to Domain A. $\text{SR}(A, B, C)$ denotes the SR between the three designated domains.

Definition 3: Let $\text{Assess}(a_i \dots a_j)^m$ denote *assessment* for entities $a_i \dots a_j$ when $a_i \dots a_j$ terminate at time step m, and $-1 \leq \text{Assess}(a_i \dots a_j)^m \leq 1$ shows either rejection or satisfaction during the assessment of the entites involved. While '-1' indicates the rejection which will reduce the value of SR, '$+1$', however, indicates satisfaction which will increase the value of SR.

Definition 4: Let $\text{DSR}(a_i \dots a_j)$ stands for *direct security rate value* in a grid for entities $a_i \dots a_j$

Definition 5: Let $\text{Rep}(A, a)$ denote *reputation and status* of entity a in Domain A on a grid.

Definition 6: Let $\text{Approv}(a_i \dots a_j)^m$ stand for the *approval* in the service request for $a_i \dots a_j$ after m time steps.

VIII. Security evaluation in a 3DGBE

Determining or evaluating the security rate in a multi-domain grid-based environment is completely different from what is obtainable in a single-domain environment. The main reason for this is the interaction and relationship between the grid entities involved. Unlike in a single-domain environment, a multi-domain grid environment has more entities from one domain to another to interact with. Hence, to handle the complexities that arise from the user's accessibility to different domains resources, the SRs for the entities of each domain is useful for quick and accurate evaluation of the security within different domains. The approach adopted for determining the inter-domain security rate value is simple and provides the benefit of feedback that is flexible and dynamic in nature. $\text{Rep}(C, a_i)$ yields status/repute of entity a_i to Domain C in a virtual organisation (VO) considered that a_i is not an entity in Domain C. It is worth mentioning that A, B, and C represent three different domains being considered while a_i , b_i and c_i are entities in the three domains. Hence,

$$\text{SR}(A, B, C) = \lambda_1 \text{DSR}(A, B, C) + \lambda_2 \text{Rep}(A, B, C) \tag{1}$$

Equation 1 is used to evaluate the SR in the three domains A, B, C with Rep where the weight λ_1 and λ_2 are positive and $\lambda_1 + \lambda_2 = 1$.

$$\text{DSR}(A_i, A_j) = \frac{\sum_{a \in A_j} \text{DSR}(A_i, a)}{|A_j|} \tag{2}$$

where a is an entity from the Domain A. Given two different domains A_i and A_j with $i, j \in [1..n]$, where $i \neq j$, and n is the number of domains.
Therefore,

$$\text{DSR}(A, C) = \frac{\sum_{c \in C} \text{DSR}(A, c)}{|C|} \tag{3}$$

When considering any domain, either A, B or C, Equation 2 is generic and can therefore be used to compute DSR between them. The same is applicable to Equation 3 where domains A and C were only and specifically considered.

IX. Repute and status across domains

For Domains A_i to A_j with $i \neq j$, the status of entities is determined as follows:

$$\text{Rep}(A_i, A_j) = \sum_{a \in A_j} \theta_a \text{Approv}(A_i, a) \text{Rep}(A_i, a), \tag{4}$$

where $\theta_a > 0$ is the weight given to $\text{Approv}(A, a)$ for $a \in A$ and $\sum_{a \in A} \theta_a = 1$. Equation 4 implies that the Rep can be determined from any desired domain and can be extended to any number of domains.

TABLE I
SIMULATION PARAMETERS WITH THEIR CORRESPONDING VALUES

Parameter	Corresponding value
λ_1	0.25
λ_2	0.25
DSR$(a_i \ldots a_j)$	0.34

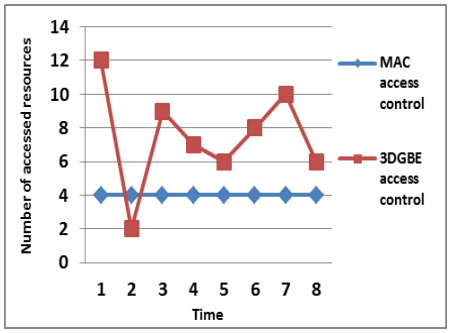

Fig. 4. Number of available resources in the two access control policies 3DGBE and MAC

X. IMPLEMENTATION AND EVALUATION

Various simulation experiments have been carried out using different simulators. In this case, Grid Security Services Simulator (G3S) was used [29]. To carry out empirical evaluation of the access control architecture, our simulation was developed in Java by making use of Jbuilder. There are three different domains in our experimental grid based environment; domains A, B and C. Domain A was made up of a Cluster of computers (which comprised 7 nodes) while the other two domains were LANs (Local Area Network) with 13 computers each. The simulated grid environment was developed using the Globus toolkit 5.0.5. All the hardware of the testbed was embedded in Linux Ubuntu 12.04. A computer hosted a database with the information of all users and acted as the LSMU for each domain while a computer server with a static IP address was chosen as the CSMU for the experimental grid. For efficient and reliable evaluation, we considered resources and entities which were accessible when a grid user requests their services. The result of our experiment revealed efficiency in terms of interoperability and scalability.

A. Access control

In the experiment, we compared 3DGBE access control and MAC, which is a popular access control method. Table I provides the detail of the parameters used in the simulation experiment. Users were provided and assigned with both a MAC-based and 3DGBE access control simultaneously. The number of resources was varied over different time periods. It was noted that the number of available resources varied over time in the 3DGBE access control architecture whereas it remained unchanged in the MAC-based access control system. See Figure 4. From this, it can be deduced that access to resources would be flexible when deploying a 3DGBE architecture.

Equations 4 was used to evaluate the security without considering any weights. Entities in either Domain A, B or C will request resources from any desired domain and such requests will be evaluated by the destination domain. The result of SR was thereafter obtained. The result is shown in Figure 5.

Equation 2 was used for calculating the SR between the domains. The security rate value will vary if there are no weighted values for θ_j. Table II gives a summary of the required parameters.

TABLE II
SIMULATION PARAMETERS FOR λ_1, DSR, REP FOR DOMAINS A, B, AND C ALONGSIDE THE NUMBER OF ENTITIES OF EACH DOMAIN

Parameter	Corresponding value
λ_1	0.60
Initial value of DSR(A, B, C)	0.58
Initial value of Rep(A, B, C)	0.44
Entities in Domain A	20
Entities in Domain B	15
Entities in Domain C	23

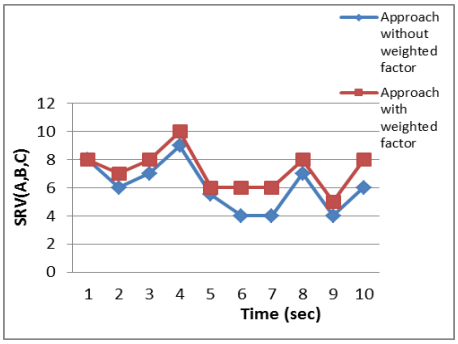

Fig. 5. Secure rate comparison using two approaches

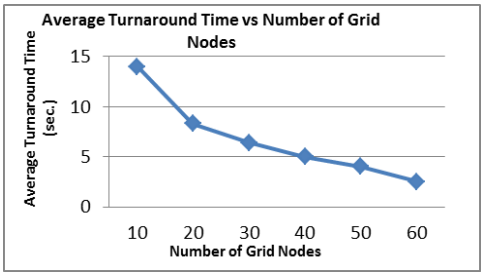

Fig. 6. Average turnaround time versus number of grid nodes

Our simulation result revealed that the available number of grid nodes has a direct influence on the turnaround time as shown in Figure 6. This implies that as the number of grid nodes increase the average turnaround time reduces and thereby increases the number of service requesters (grid users) on the grid. To further prove and sustain the argument that the model developed and implemented is scalable, Figure 7 shows that as the number of service requesters increases, there is little and slight effect on the turnaround time which does not impact on the users' services and request time.

The use of grid middleware has been identified as one of the ways for solving the challenge of interoperability among multiple administrative domains. Since our model adopted the XACML access control protocol, it has the highest level of interoperability when compared to others.

We compared 3DGBE which uses X.509 certificates with MAC, CAS, AKENTI and PERMIS that use own their certificate formats and the result is presented in Figure 8. The result shows that 3DGBE has highest degree of interoperability when compared to others.

XI. CONCLUSION

It has been established that the full scale benefits of using and maximizing grid computing can only be realized when a secured access control framework is in place. It on this premise that various

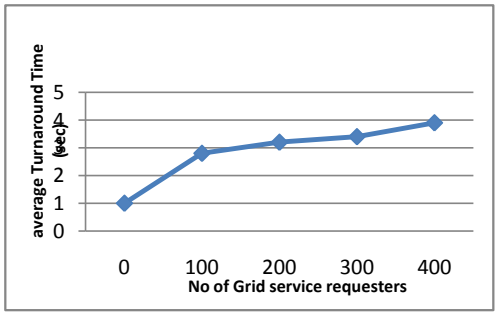

Fig. 7. Average turnaround time versus number of service requesters

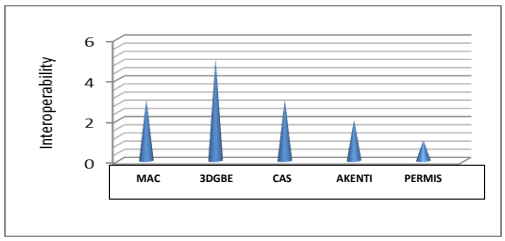

Fig. 8. Comparative evaluation of interoperability of 3TDGE with the existing system

methods in use were examined and studied. Having realized the importance of scalability and interoperability for any grid environment, we succeeded in proposing and implementing a 3DGBE architecture to handle these challenges. From the foregoing, it is clear that role-based access control can be used to monitor, regulate and authorize users on any high performance computing specifically on the grid.

Based on the simulation results and their analysis, it can be deduced that the objectives for carrying out the experiment have been achieved. From the simulation results and the parameters used for the practical evaluation of the model, it is evident that, the results prove the model's desired features of interoperability and scalability. It is therefore, the belief of the authors that a full scale implementation of this model on a real grid system will ensure a secure, scalable and interoperable grid-based environment.

A. Acknowledgement

The authors thank the Research Committee of the University of the Western Cape for funding.

References

[1] N. A. Azeez, T. Iyamu, and I. M. Venter, "Grid security loopholes with proposed countermeasures," in *ISCIS 2011*. Springer Verlag, London, 2011, pp. 411–418.

[2] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems*, vol. 18, no. 2, pp. 106–112, 2009.

[3] M.-S. Hwang and W.-P. Yang, "A new dynamic access control scheme based on subject-object list," *Data and Knowledge Engineering*, vol. 14, no. 1, pp. 45–56, 1994.

[4] R. Buyya, "Economic-based distributed resource management and scheduling for grid computing," Ph.D. dissertation, Monash University, Melbourne, Australia, 2002.

[5] H. Baktash, M. B. Karimi, M. R. Meybodi, and A. Bouyer, "2L-RBACG: A new framework for resource access control in grid environments," in *2010 Fifth Int. Conf. on Digital Information Management (ICDIM)*. Thunder Bay: IEEE Computer Society, 2010, pp. 359–366.

[6] GStat, "Grid gstat 2.0," 2010, http://gstat.gridops.org/gstat/sa-gr.

[7] Z. Mao, N. Li, H. Chen, and X. Jiang, "Trojan horse resistant discretionary access control," in *in SACMAT 09: Proc. 14th ACM Symp. on Access Control Models and Technologies*. Stresa, Italy: IEEE Computer Society, 2009, pp. 237–246.

[8] B. Bouwman, S. Mauw, M. Petkovic, and E. Philips Res.-Ordina, "Rights management for role-based access contro," in *Consumer Communications and Networking Conference, CCNC*. Las Vegas, N: IEEE Computer Society, 2008, pp. 1085 – 1090.

[9] Z.-D. Shen, F. Yan, W.-Z. Qiang, X.-P. Wu, and H.-G. Zhang, "Grid system integrated with trusted computing platform," *Computer and Computational Sciences, International Multi-Symposiums on*, vol. 1, pp. 619–625, 2006.

[10] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[11] R. Lakshmish, L. Ling, and I. Arun, "Scalable delivery of dynamic content using a comprehensive edge cache grid," *IEEE Trans. on Knowl. Data Eng.*, pp. 614–63, May 2007.

[12] O. Rahmeh and P. Johnson, "Towards scalable and reliable grid networks," in *IEEE/ACS International Conference on Computer Systems and Applications (AICCSA-2008)*. Doha, Qatar: IEEE Computer Society, 2008, pp. 253–259.

[13] A. Detsch, L. Gaspary, M. Barcellos, and G. Cavalheiro, "Towards a flexible security framework for peer-to-peer based grid computing," in *2nd Workshop on Middleware for Grid Computing*, Toronto, Canada: ACM, 2004, pp. 52–56.

[14] S. Basit, B. James, B. Elisa, and G. Arif, "Secure interoperation in a multidomain environment employing rbac policies," *IEEE Trans. Knowl. Data Eng.*, pp. 1557–1577, 2005.

[15] G. Pankaj, "Application of a distributed security method to end-2-end services security in independent heterogenous cloud computing environment," in *IEEE World Congress on Services*. Washinsgton, DC: IEEE Computer Society, 2011, pp. 379–384.

[16] Z. Tari and A. Fry, "Controlling aggregation in distributed object systems: A graph-based approach," *IEEE Trans. Parallel Distrib. Syst.*, pp. 23–32, December 2001.

[17] H. Yanxiang, L. Fei, and H. Wensheng, "The design and implementation of security communication model in grid networks," in *Int'l Conference on Computer Science and Information Technology, IEEE, ICCSI*, 2008, pp. 421–424.

[18] A.-B. Ali, Z. Hussein, and S. Francois, "Access control mechanism for mobile ad hoc network of networks (MANoN)," Software Technology Research Laboratory, De Montfort University, Leicester, Tech. Rep., 2009.

[19] H. Mohteshim, "Passive and active attacks against wireless LAN," in *IASTED, 2004. Int. Assoc. of Sci. and Technology for Development*, 2005. [Online]. Available: http://www.iasted.org/conferences/2004/Innsbruck/pdcn.htm

[20] J. McLean, "The algebra of security," in *IEEE Symp. on Security and Privacy*. Naval Research Laboratory, Washington, D.C.: IEEE Comput. Soc., 2008.

[21] G. Laccetti and G. Schmid, "A framework model for grid security," *Future Generation Computer Systems*, vol. 23, no. 5, pp. 702–713, June 2007.

[22] NHSE, National HPCC Software Exchange, pp. 4–8, 2009. [Online]. Available: http://wotug.org/parallel/nhse/

[23] A. Imine, A. Cherif, and M. Rusinowitch, "An optimistic mandatory access control model for distributed collaborative editors," INRIA, Tech. Rep., 2009.

[24] I. Foster and C. Kesselman, "Globus: A metacomputing infrastructure toolkit," *The International Journal of Supercomputer Applications and High Performance Computing*, vol. 11, pp. 115–122, 1997.

[25] D. Chadwick, "Authorisation in grid computing," *Information Security Tech.*, vol. 10, pp. 33–40, 2005.

[26] C. Rongxing, Lu; Zhenfu, "A simpler user authentication scheme for grid computing," *International Journal of Network Security*, vol. 7, pp. 202–210, 2008.

[27] Z. Weide, W. David, D. V.and Glenn, and H. Marty, "Flexible and secure logging of grid data access," in *7th IEEE/ACM Int. Conf. on Grid Computing, (Gridn 2006)*. Barcelona, Spain: IEEE/ACM Computer Society, 2006, pp. 1–8.

[28] MSDN, "Data confidentiality," 2005. [Online]. Available: http://msdn.microsoft.com/en-us/library/ff650720.asp

[29] N. Syed and R. Michel, "Grid security services simulator (G3S)—a simulation tool for the design and analysis of grid security solution," in *Proc. First Int. Conf. on e-Science and Grid Computing (e-Science '05)*. IEEE Computer Society, 2005, pp. 421–428.