Methods for Managing Access Control in Virtual Organizations

Hassan Kurdi

06/02/2015

Abstract: The management of the access control is one of the challenges that face virtual organizations (VOs). There are many approaches have been used to manage and govern the access control of the resource. This paper shows two extensions of Role-Based Access control (RBAC) that could rival other common approaches (such as Community Authorization Service (CAS) or Virtual Organization Management Service (VOMS)) in achieving access control properties (such as scalability, flexibility and security) in virtual organizations. The aim of this paper to clarify that there is possibility to develop RBAC to achieve the essential requirements and properties of the access control in VOs. However, before explaining the extensions of RBAC, this paper will clarifies the general requirements of access control in virtual organizations. In addition, explaining the concept of RBAC including the advantages and disadvantages. One of the most interesting points in this paper is, indicating to the essential requirements that are not achieved by RBAC. In other words, the factors needed by the RBAC in VOs to achieve effective administration of the resources.

1- Introduction

Dynamic virtual organizations are temporary consortia of heterogeneous, independent and perhaps geographically dispersed organizations that work together to achieve a common goal. This collaboration is executed by sharing the resources among all organizations but, each organization has its own resources that are provided to other organizations depending on requirements of achieving the goal. The purpose of this collaboration is to achieve specific task that cannot be achieved individually, because an organization may not have the resources or the capability to achieve the goal on its own. Thus, all the organizations work together to complement each other. This collaboration will terminate when the required goals are achieved. One of the most fundamental mechanisms for sharing resources and establishing a virtual organization is the Grid environment, **[2, 3]**. The term "Grid environment" refers to a compilation of computers that are linked together to provide combination of resources from different administrative organizations.

Virtual organizations (VOs) face several challenges which are related to the security aspects, because virtual organizations deal with different kinds of entities (resources, services and users) from different domains. One of these aspects is, protecting the resources and information from unauthorized access. In other words, Due to heterogeneity and dynamicity of virtual organization, the management of the access control could be slightly complicated, **[4]**. This because that the users of the organization demand different kinds of access to the resources in VO and some of these users are changed continuously from time to time. Second reason is that some organizations can change the policies of the access control without informing other organizations. Thirdly, each organization in the consortia has its own policies to access the resources, so they specify who can access their shared resources.

Although the access control of the resources in VOs is a relevant factor, it does not provide complete security. This is because the accesses of the resources require additional security aspects such as building the trust and providing the authentication. All of these aspects should be provided in VO to

achieve sufficient security. This paper will focus on the model which can enforce and manage the access control in VO, and the requirements that is related to control and govern the access to the resources. There are many models can be used to manage the access control of the resources in VO. Role based access control (RBAC) is one of the models which can be employed to manage the access control in VO, **[15]**. RBAC is an easy and flexible model to manage the access control in virtual organization, **[3]**. RBAC is a preferred model to be used in distributed systems because it provides high features to manage and administrate access control moreover, it is claimed to be a scalable and efficient access control model, **[1]**.

In this paper, the research will be divided into six main sections. Section 1 clarifies the requirements of the access control in virtual organization. Section 2 defines the access control model (RBAC) which will be used in VOs moreover, providing description of how this model works. Section 3 explains the advantages and disadvantages of Role based access control (RBAC) in VO. Section 4 indicates some of the essential factors of VOs that are not provided by RBAC. Section 5, the paper discusses the extension of RBAC to address the issues that have been mentioned in section 4. Finally, shows the properties that are achieved by the extended RBAC.

2- Requirements for access control in virtual organizations

According to **[5]**, there are four main requirements for access control in virtual enterprises. These requirements develop the access control and address information security issues.

2.1 Security policy specification approaches.

It is the approaches that protect the security requirements of individual systems which are associated with virtual organization. The purpose of these approaches is to determine various access control policies that adapt with the complete system of VOs. There are different models of security policy specification approaches could be enforced in VO. One of these approaches is Authorization Specification Language (ASL). A further approach is the Language for Security Constraints on Objects LaSCO.

2.2 Distributed security architectures.

These architectures are the responsible to “deploy access control policies within distributed communities”, **[5]**. Distributed security architectures protect the objects (information and resources) from unauthorized access. These requirements govern and manage the access of the resources. There are many approaches could be used to control the access in distributed systems, and these approaches manage the access control in different ways. For example, Open Grid Service Architecture (OGSA) which determines architectural level of the software of grid computing. This architecture aims to “facilitate the rapid development of interoperable Grid services by extending and leveraging the existing security technologies and assets of participating organizations”, **[5]**.

2.3 Policy management architecture.

Policy is high level statements that protect the resources of the organizations from unauthorized access. Policy management is the requirement that determines the scope of access control to the resources moreover, defines the roles and the responsibilities that should be followed by the users. The techniques that could be enforced in this architecture are policy decision point (PDP) and policy enforcement point (PEP).

2.4 Security standards

Security standards are the aspects that specify the obligatory requirements that help executing and supporting the policies. In other word, the aim of the standards is to manage the policies and make the access decision. Security standards maintain the consistency of the security in organization and provide security controls that associated with the implementation of specific technology, hardware or software. There are several standards could be used in VOs such as Security Assertions Markup Language (SAML) or eXtensible Access Control Markup language (XACML).

3-The concept of Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) is one of the models that can be used in the Grid environment. The concept of RBAC is that each user of the system is assigned to specific roles and the permissions to access to any objects (resource) are assigned to these roles. Users obtain permission to perform any operation (function), through the roles which are assigned to them. Therefore, the users will not obtain the resources directly, unless through their roles. In addition, the users will not exceed the privileges and authorities that have been given to them to access to the sources.

The RBAC contain of four main entities, [6]:

1- **user:** the person who is a member of the staff of the organization for example, John, Peter and Hassan.

2- **role:** the name of the job (job function) of the user in the organization such as doctor, assistant and nurse. This describes the granted authority for each user based on their job in the organization. For example, the privileges which are granted to the doctor differ from the privileges which are granted to the nurse or the assistant. One of the features of this model is that the user can be associated with several roles, and the roles can represent many users.

3- **permission:** The access right to the resources. In other word, it is the operations which should be conducted for each resource and for each user. For example, doctors can read and write on the patient's file, while the nurse can just read the file. One of further feature of this model is that the role can be assigned to several permissions, and the permission can be associated with many roles. 4- **session:** an activation operation of the role(s) that belong to each user. Therefore, the permissions available to the user depend on the role(s) which are activated in that session. Each session is associated with a single user. However, the user may have multiple sessions at the same time, if the tasks (access to the resources) are performed in different windows on a workstation screen.

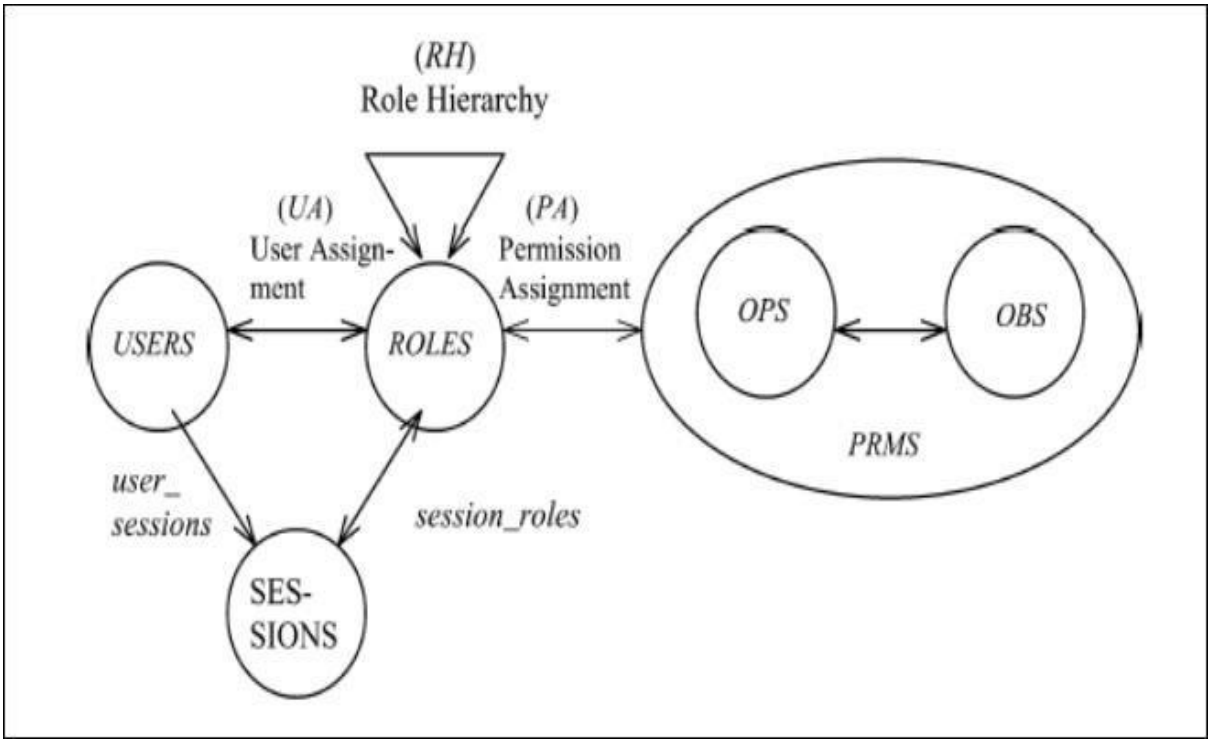

Figure1. Core Role-Based Access Control, [7].

4- Advantages and disadvantages of RBAC

There are many advantages of RBAC. Firstly, the separation of duty (SoD) principle can be enforced in RBAC to "avoid role conflict among subjects and restrict the subjects in acquiring conflicting roles at the same time" **[7]**. In other words, the user is unable to execute more than one operation at the same time. The purpose of this principle is to prevent fraud and errors because the execution of any operation will be distributed among different users, **[8]**. Therefore, that reduces the possibility of occurrence of fraud or error by the users. For example, the procedure of purchasing a product can be executed by four users. User 1, order the product and record the details, user 2, verify the details and the invoice of the ordered product and user 3, compare the details and the invoice of the received product with the product that has been ordered by user 1. User 4, takes inventory the products of the stock. Therefore, the error and fraud can be detected by any of the four users. A second advantage is that RBAC is supported by the least privilege principle which specifies the only required privileges of achieving the goal for each user, **[16]**. In other words, the users will be restricted to perform the operations that are necessary to complete the goal. This principle able to reduce and define the damages that are caused by any error or accident. In addition, it decreases the number of the process on the resource, **[9]**.

On other hand, there are some disadvantages in RBAC. One of these disadvantages is, in the existence of least privilege and SoD principles, the role hierarchy in RBAC infringe (trespass) the concept of inheritance in the hierarchy, **[10]**. In other word, the concept of role hierarchy is that a higher role inherits all access right of the lower roles which can be sub-roles (children) for the higher roles. However, this concept cannot occur for several reasons. First reason, SoD disallow that two similar roles (that has the same parent) execute at the same time. Therefore, the two roles will not have the same parent. Second reason, higher role cannot inherit all access right of the lower role because least privilege principle prevent any role to have unnecessary access right. In other word, if lower role have

some access right which some of them are necessary and unnecessary for higher role, the higher roles will only able to obtain the necessary privilege.

5- The essential factors required by RBAC in virtual organization:

Access control requires several factors that help to manage and organize the access control in virtual organization. These factors are not provided and supported in RBAC model. However, the RBAC could be extended and developed itself to achieve these factors. There are three factors:

1- One of the challenges that face virtual organization is the administration of the access control of resources. In RBAC the mechanism of the administration of the access control is centralized which is not suitable in virtual organization because the nature of the autonomous and dynamic in VO requires that the administration should be decentralized, **[11]**. Whereas the resources of the organization should be provided to other organizations independently. This facilitates the process of achieving autonomy and avoid the occurrence the failures. Also, each organization has to be able to share their resources without the intervention the administrator, and this reduces the burden on administrators.
2- One of the most important factors that are not provided by RBAC is fine-grained access control mechanism, **[12]**. Fine-grained access control is required in VO to fulfil the complicated requirements of the access control, **[13]**. The aim of the fine grained is to allow the resources' provider to determine and change the access right policies which limit and grant the user's access to the resources under any operation could be executed on the resources. In addition, fain-grained access control enables the users to be divided in specific groups (roles) to determine their own policies and this lead to restriction of their own shared resources.
3- Contextual model is one of the approaches that improve the security policies of the access control, **[3]**. This approach is used to make the decisions of the access to the resources. Some decisions are based on the location of the user, the time of the access to the resources or the purpose of the access. For example, some resources can be accessed by the users from specific location with limited time. In fact, RBAC provide limited contextual model which is insufficient in virtual organization. RBAC decisions based on three aspects “(1) which user can perform (2) what operation (3) on which object ". However, RBAC can be extended to make additional decisions.

6- Extended RBAC

This section clarifies an extension of RBAC which provides the essential factors required by virtual organization.

6.1 Two-level role-based access control framework in grid environment (2L-RBACG)

First extension is two-level role-based access control framework in grid environment (2L-RBACG) which divides the management of access control into two levels (Virtual organization (VO) and resources administration), **[4]**. In VO level, the administrator determines the general resource independent RBAC policies moreover, defines roles, user-role and role-permission assignments. VO administrator grants the privilege to the specific users who can manage and select the required privileges for their resources. In addition, these users can delegate the granted privileges to other users without the intervention of the administrator. On the other hand, in resource level, the resources are assigned to the policy of RBAC by resources administrator. In other word, the decisions of authorization to access to the resources are implemented in resource level.

It is obvious that 2L-RBACG framework achieves decentralization because the privileges are managed by the users without the intervention of administrator. Furthermore, this framework provides fine-grained because the policies of the access to the resources can be modified in resource level.

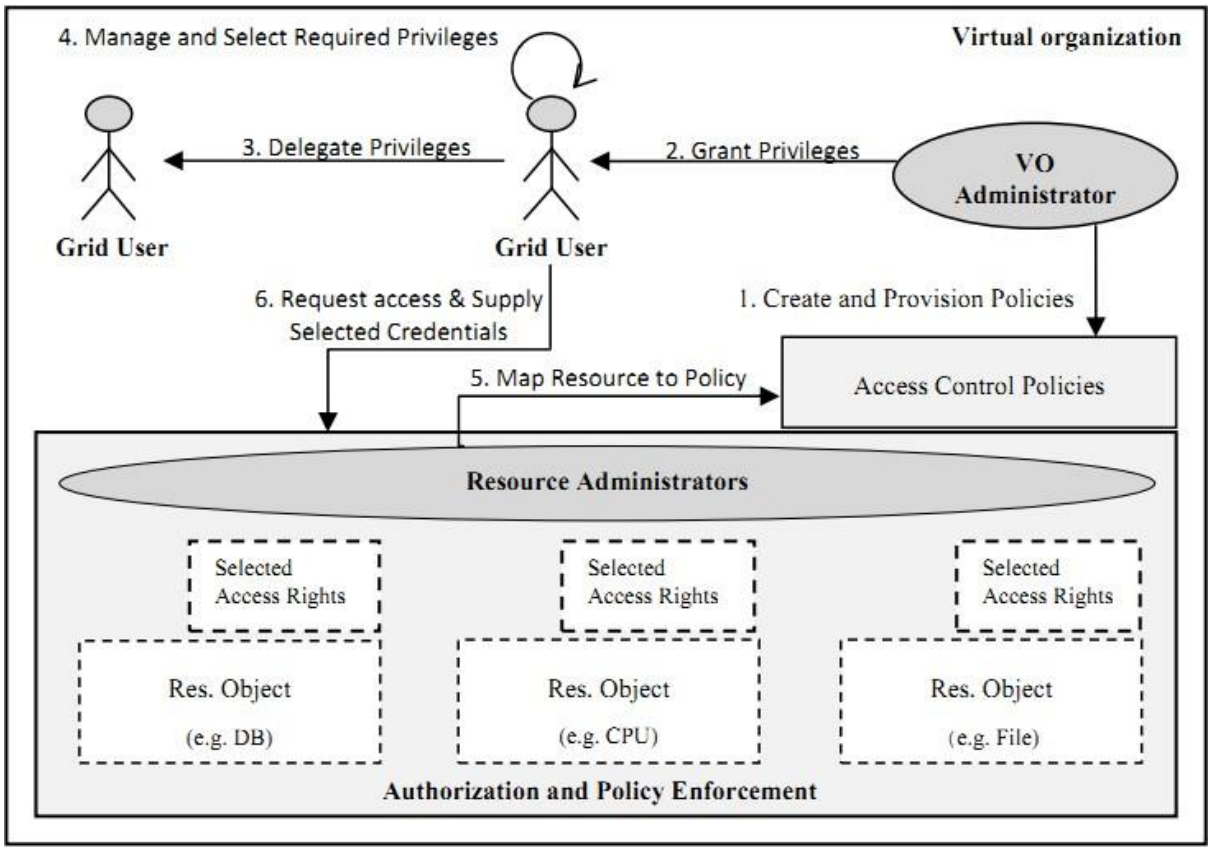

Figure2. Two-level role-based access control framework in grid environment (2L-RBACG), [4].

6.2 Contextual role based access control model (C-RBAC)

The contextual model in access control is the approach which makes additional decisions to the access to the resources. The contextual model which is selected in this paper is C-RBAC. C-RBAC is an extended model to traditional RBAC, **[7]**. C-RBAC model is based on four decisions to access to the resources. These decisions contain the three RBAC decision including the purpose of the access decision. The three RBAC decision are, which user can perform (e.g. doctor, nurse) what operation (e.g. read, write) on which object (e.g. file.doc, file.exe). Whereas, the purpose of the access decision indicates to the intention of the user in accessing to the resource.

For example, if there is a research which require a collection of doctors from a hospital and university. The research demands the only doctors whose domain is in e.g. (toxins analysis). Therefore, C-RBAC allows granting the access to the research for only the doctors whose domain is in toxins analysis from the university and hospital. In fact, the contextual model is unconfined on the four decisions which are mentioned above. There is a contextual model that has been provided which is based on location of the users including the three main decision of RBAC, **[14]**.

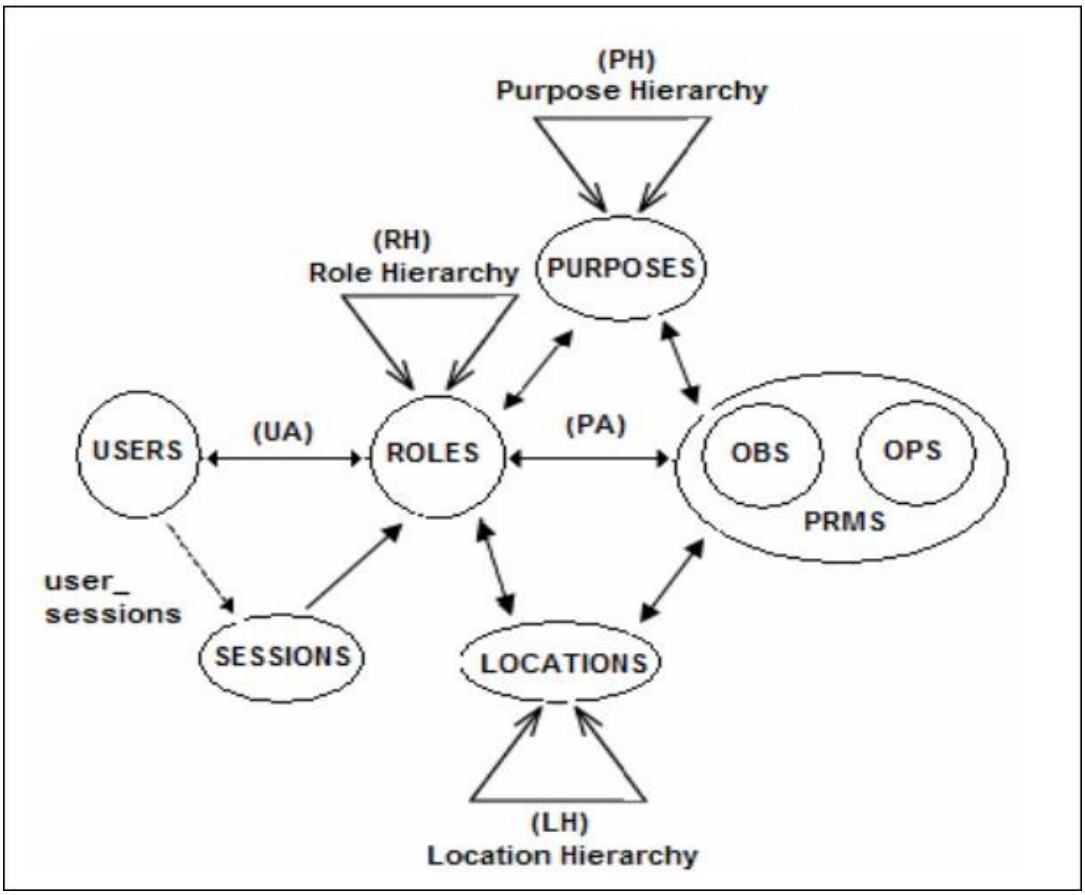

Figure3. Contextual Role-Based Access Control (C-RBAC), [7].

7- Properties of extended RBAC

It can be said that the extension of RBAC has achieved three important properties.

1- Scalability: the extended RBAC interacts with increased amount of operations while maintaining the cost of administration. In addition, it has the ability to be enlarged to accommodate the increased numbers of users and operation.

2- Flexibility: the policy of roles and permission assignment and access right to the resources can be changed continuously.

3- Autonomy: VOs is self-managed because the resources and VO administration are managed in two levels. Therefore, each level has the responsibility to be administrated individually without the intervention of administrators.

8- Conclusion

RBAC model is one of the most appropriate models that can be enforced in virtual organization. In this paper, It has been explained the concept, advantages and disadvantages of Role-Based Access Control. In fact, it has been found that there are three important factors that are not provided by RBAC. These factors are decentralization, fine-grained and sufficient context permission. However, the extension of RBAC (2L-RBACG and C-RBAC) has addressed these issues and has provided the three requirements that needed to control the resources. In addition, the extension of RBAC has achieved some important properties of access control. These properties are scalability, flexibility and autonomy.

In future work, it can be suggested that the extensions of the RBAC could be linked to provide the complete requirements of access management. In other word, instead of using different approaches (such as CAS, VOMS or other approaches) to perform the management of access control, the RBAC can be extended and this extensions can be linked together as a one approach to perform all the characteristics of access control management. On the other hand, the level of the properties (such as scalability, flexibility, security) in different models (Such as CAS, VOMS or other models) has not been measured. Therefore, it would be an interesting topic to measure the level of the properties of the different models to determine which model can provide better properties.

References

[1] Ferraiolo, D.F., Kuhn, D.R., Chandramoul, R. Role-Based Access Control (Second Edition). Artech House Publishers, United States, 2007.

[2] Pearlman, L., Welch, V., Foster, I., Kesselman, C., Tuecke, S. A community authorization service for group collaboration. *Policies for Distributed Systems and Networks, 2002. Proceedings. Third International Workshop on*, pp.50-59, 2002.

[3] Nasser, B., Laborde, R., Barrère, F., Benzekri, A., Kamel, M. Grid Virtual Organization: Access Control management. *Gres*, Luchon, France, Mars 2005.

[4] Baktash, H.A., Karimi, M.B., Meybodi, M.R., Bouyer, A. 2L-RBACG: A new framework for resource access control in grid environments*. Digital Information Management (ICDIM), 2010 Fifth International Conference on*, pp.359-366, 5-8 July 2010

[5] Coetzee, M., Eloff, J.H.P. Virtual enterprise access control requirements. *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists (SAICSIT '03)*, PP. 285-294, 2003.

[6] Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E. Role-based access control models. *Computer* , vol.29, no.2, pp.38-47, Feb 1996.

[7] Tahir, M.N. C-RBAC: Contextual role-based access control model. *Ubiquitous Computing and Communication Journal*, Vol.2, No. 3, 2007.

[8] Hassan, T., Morteza, A., Rassol, J. Separation of Duty in Role-Based Access Control Model through Fuzzy Relations. *Third International Symposium on Information Assurance and Security*, Vol. 29, No. 31, pp.125-130, 2007.

[9] Saltzer, J.H., Schroeder, M.D. The protection of information in computer systems. *Proceedings of the IEEE* , vol.63, no.9, pp. 1278- 1308, Sept. 1975.

[10] Oh, S., Park, S. Task–role-based access control model*1. Information Systems Journal, Vol.28, pp.533-562. Elsevier Science Ltd. Oxford, UK, UK, 2003.

[11] Jin, H., Qiang, W., Shi, X., Zou, D. VO-Sec: An access control framework for dynamic virtual organization. *Lecture Notes in Computer Science*, Vol. 3574, pp. 370-381, 2005.

[12] Periorellis, P., Parastatidis, S. Task-Based Access Control for Virtual Organizations. *Lecture Notes in Computer Science*, Vol. 3409, pp.38–47, 2005.

[13] Zhang, N., Yao,L., Nenadic, A., Chin, J., Goble, C.A., Rector, A.L., Chadwick, D.W., Otenko, S., Shi, Q. Achieving fine-grained access control in virtual organizations. *Concurrency and Computation: Practice and Experience,* John Wiley and Sons Ltd, Chichester, UK, Vol. 19, pp.1333-1352, 2007.

[14] Tahir, M. N. Hierarchies in contextual role-based access control model (C-RBAC). *International Journal of Computer Science and Security (IJCSS)*, Vol.2, pp.28-42, 2008.

[15] Benzerki,A. Virtual Organization security policy: specification & deployment (V1). *Value Improvement through a Virtual Aeronautical Collaborative Enterprise (VIVACE)*, 2006, from World Wide Web: www.vivaceproject.com/content/3rdtier/vosp_full.pdf

[16] Ferraiolo, D. F., Cugini, J. A., Kuhn, D.R. Role-Based Access Control (RBAC): Features and Motivations. *National Institute of Standards and Technology,* 11th Annual Computer Security Applications Proceedings, 1995, from world wide web: http://hissa.ncsl.nist.gov/rbac/newpaper/rbac.html