ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

A Hierarchical Approach to Access Control – A Review

Sunita Rani Jindal, Sahil Vasisth, Rajwinder Singh
M TECH Student, CGC Landran , Punjab, India
Asst. Professor, CGC Landran , Punjab, India
Asst. Professor, CGC Landran , Punjab, India

ABSTRACT*:* Cloud Computing is an emerging platform which supports all the three arenas of the services namely IAAS , PAAS and SAAS .The future aspects of cloud system would definitely consider a mechanism which controls the flow of data and the access limitations. Role Based Controls Access Provides a way to limit the burden of the server by restricting users from accessing the contents out of their zone. There has been a lot of models of RBAC launched at cloud since ever it has been introduced. This paper briefs about the RBAC mechanism and focuses on the internal architecture of RBAC.

KEYWORDS*:* Cloud Server , RBAC , User Limitation

I. INTRODUCTION

Cloud Platform is a new technology which tries to provide the entire scenario of the development and other services to the user. There are different slots or sections of a cloud service. They are as follows

a) IAAS
b) PAAS
c) SAAS

IAAS stands for infrastructure as a service where as PAAS stands for Platform as a service and SAAS stands for Software as a service. All of the three paradigms are necessary for any cloud computing data centre. It is assumed that in future days the entire services will be provided by the cloud itself and the user will have to pay for each and every kind of service which the user uses .[1]

Figure1 represents the utilities of cloud

The above figure represents the basic services provided by the cloud data centre. The figure clearly states that the data centre provides mailing services, accounting services, software services and etc.

As the cloud computing platform is a complete platform where every kind of users would be there hence there must be a mechanism which prevents the data from the unauthorized uses. A mechanism called ROLE BASED ACCESS CONTROL is available for such kind of application [2] .

WHAT EXACTLY IS RBAC:

RBAC stands for role based access control. In this system there are roles and users are created according to the roles. Permission is applied to the role and they automatically get applied to every user related to the category. There are several models of RBAC which are presented below [3].

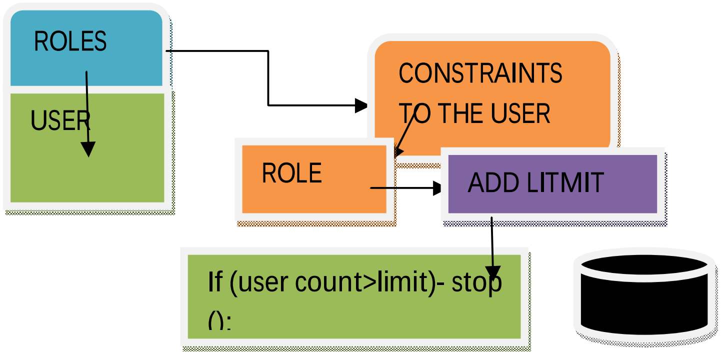
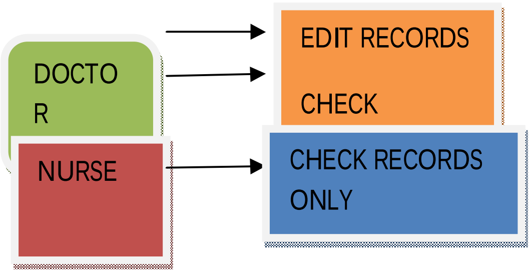


Figure (2) The above figure represents the role hierarchy of the roles and their users . The above figure represents the general architecture service of the RBAC model in which there would be roles and users. The constraints would be applied to the roles and their respected users. If the user count increases of the predefined threshold value then the user limit exceeds and the server stops the functionality.

The first model of RBAC is RBAC 0

RBAC 0: The RBAC0 model is the simplest architecture of the role based access control in which there are users according to the role and the constraints are applied to the roles not on the users. To understand the RBAC0 a simple example is illustrated below [3 4].

Let us suppose there is system in which doctor is a role then its constraint are defined as follows.



The above diagram shows two categories namely doctor and nurse. In this architecture the doctor category has been assigned with two permissions namely edit records and check records and hence the doctor can check the records and edit the records where as another role called nurse can only check the records and she cannot edit the records.

RBAC 1: The RBAC 1 model is an extension of the RBAC 0 model in which constraint over the number of transactions to a user has been limited according to the services used by the users

RBAC 2 : The next version of RBAC is RBAC2 .In this version of RBAC constraints overs the user limits have been applied . This model enhances the RBAC 1 Model and put the restriction over the limit over the number of users per role for the safety purpose [6].
The below diagram can explain how it goes

RBAC 3: Another advanced version of RBAC is RBAC three which enhances the concept of RBAC 2. In this concept another constraint over the number of transaction of the users has been applied to the architecture. In this scenario, if there are ten roles then accordingly how much transactions a user can make would be classified in this arena. RBAC 3 can be termed as the most efficient role based access control model till now .Its algorithm can be defined as follows[9]

1) Start
2) Create roles
3) For i=1: n
4) If role[i].usercount.limit
5) Notify the server about user limit where n=number of users
6) For i=1:p
7) Transaction occurred /role
8) Transaction++
9) If transaction .currentrole >transaction limit
10) Noitify server
11) Stop

COMPARITIVE ANALYSIS OF THE RBAC

FEATURE	RBAC 0	RBAC 1-2	RBAC 3
USER CREATION	YES	YES	YES
ROLE CREATION	YES	YES	YES
RESTRCITION OVER USER LIMIT	NO	YES	YES
RESTRICTION OVER TRANSACTION OF USERS	NO	NO-YES	YES

Three primary rules defined for RBAC

12) Role assignment:- A person can exercise a permission only if the person has selected or been assigned a Role.
13) Role authorization:- A person's active role must be authorized for the person. This rule ensures that users can take on only roles for which they are authorized.
14) Permission authorization:- A person can exercise a permission only if the permission is authorized for the person's active role. With rule1 and rule2, this rule ensures that users can exercise only permission for which they are authorized.

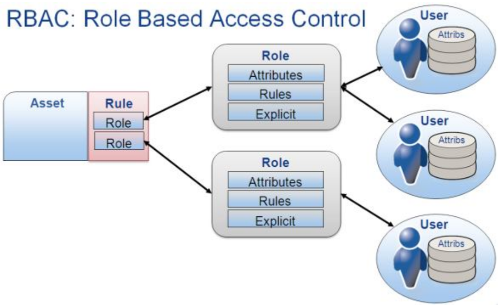


Figure represents the general RBAC MODEL

The above figure represents the RBAC MODEL which clearly defines the role alignment model and the user creation process. The users can be categorized only on the basis of the roles made to them.

Advantages of RBAC It provides hierarchy roles of access based on many applications. Roles are assigned based on the least privilege for the particular object, so this will minimize the damage of information by intruders. Separation of roles will be maintained so there is no chance of misuse of information because each user assigned to individual roles. This separation of roles can be either static or dynamic. RBAC provides the classification of user based on their executing environment. Role Based Access Control has following administrative policies. Those are Centralized, Hierarchical, Cooperative, Ownership, and Decentralized. In large distributed system centralized access right is not appropriate.

Disadvantages of RBAC Sometimes it is difficult to reach which privilege to which user it has been associated with a particular role. Permissions associated with each role can be deleted or changed based on the privilege of role change. Job roles are assigned based on the least privilege but still change of role of user might have some confusion when considering the permissions of each user associated with that role.

CONCLUSION

With the above context we conclude that there are several models of rbac namely rbac0 , rbac1 and rbac2,rbac 3. Each access control mechanism has their own features which has been discussed through the tabular structure. We also conclude that the rbac3 mechanism is one the finest role based mechanism which includes the limitation over number of transactions per user and the restriction over the generation of number of users per role. Future research works can add swapping methods for user so that if some user does not need more number of transactions in a day, he can swap his transactions with other users

REFERENCES

[1] Reeja S L ROLE BASED ACCESS CONTROL MECHANISM IN CLOUD COMPUTING USING CO – OPERATIVE SECONDARY AUTHORIZATION RECYCLING METHOD International Journal of Emerging Technology and Advanced Engineering october 2012

[2] Dancheng Li H-RBAC: A Hierarchical Access Control Model for SaaS Systems I.J.Modern Education and Computer Science, 2011, 5, 47-53 Published Online August 2011 in MECS (http://www.mecs-press.org/)

[3]Yan Zhuongxin Huy, Gail-Joon Ahny, Dijiang Huangy, and Shanbiao WangTowards Temporal Access Control in Cloud Computing ieee 2010

[4] ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT VOL. 7, NO. 5, MAY 2012 ISSN 1819-6608 ARPN Journal of Engineering and Applied Science

[5] J. Carneiro, J. Laranjeira, G. Marreiros, C. Freitas, and R. Santos. A context-aware model to support ubiquitous group decision making, 2012.

[6] A. Corradi, R. Montanari, and D. Tibaldi. Context-based access control for ubiquitous service provisioning. In Proc. of the 28th Annual International Computer Software and Applications Conference (COMPSAC'04), Hong Kong, China, pages 444–451. IEEE, September 2004.

[7] D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli. Role-Based Access Control. Artech House, 2003.
[8] K. Fukushima, S. Kiyomoto, and Y. Miyake. Towards secure cloud computing architecture - a solution based on software protection mechanism, 2011.
[9] W. Han, J. Zhang, and X. Yao. Context-sensitive access control model and implementation. In Proc. of the 5th International Conference on Computer and Information Technology (CIT'05), Shanghai, China, pages 757–763. IEEE, September 2005.