Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review on Cloud Computing Security Measure – Role-Based Access Control

Sanjay Tiwari*, Khushbu Sharma
Computer Science& RTU, Kota
India

Abstract— Cloud Computing is an emerging technology. It is receiving significant attention by both research community and industries. Cloud computing security is an important issue due to increasing scale of users. Therefore, series of security concepts are required to be revised such as Role-Based Access Control (RBAC) proposed by the National Institute of Standards and Technology (NIST) which promises to become a more prominent security model today. The aim of this article is to describe Access Control, RBAC model, its drawback and to identify proposed research work to reduce security risk.

Keywords— Cloud Computing, Security, Access Control, Role-based Access Control model.

I. INTRODUCTION

Earlier, In the developing stage, we used to create applications and data storage on the local servers. If local server or local system crashes, the entire system, applications and related data crashes automatically. It was becoming a huge problem all over the world. To overcome this problem, the concept of cloud computing was brought out into action. But due to increasing scale of users many security related problem arises and then security issues became most common in the interest of researchers. Security models such as Mandatory Access Control and Discretionary Access Control have been the means by which information's were secured and access was regulated. But due to the inflexibility of these models, the rather new security concept of Role-Based Access Control (RBAC) was proposed by the National Institute of Standards and Technology (NIST) which promises to become a more prominent security model. But due to increasing scale of users providing significant security has become bottleneck [1].

This paper describe access control, concept of RBAC (Role-based Access Control) model, its drawback and at last we conclude to describe proposed research work to reduce security risk.

II. ACCESS CONTROL

Privacy, trust and Access Control are some of security concept required to meet in Cloud platform. Access Control's role is to control and limit the action or operation in cloud systems that are performed by user on set of resources [2]. In brief, it enforces the access control policy of the system, and at the same time it prevents the access policy from subversion. We can also consider access control as access authorization of resources means to say it specifies how user may access specific resource and when.

The access control model bridges the existing abstraction gap between the mechanism and the policy in a system. According to TCSEC there two types of access control mechanism namely the Mandatory Access Control policies (MAC), the Discretionary Access Control policies (DAC) [3]. Later new access control policy use in practice such as the Role Based Access Control policies (RBAC).

A. Discretionary Access Controls(DAC):

In Discretionary access Control (DAC) model access to resources is based upon user's identity means of restricting access to objects based on the identity of subject and/or groups to which they belong. In discretionary access control (DAC) user/subject with certain permission is capable of passing that permission (perhaps indirectly) on to any other subject to be left upon user willing without the intercession of a system administrator [3]. So, when user (or group) is the owner of an object in DAC model it has permit to grant and revoke access privileges to other user and groups. User is granted permissions to resource by being placed on access control list (ACL) associated with resource. With access control list (ACL) lists that specify which users can access a particular piece of data, DAC consists of a set of rules that specify which users are allowed to access the data. DAC does not impose any restrictions on data access for a particular user. Once users can access data, they can change or pass that information onto any other user without the security administrator's knowledge as shown in figure (1) [4].

B. Mandatory Access Control(MAC):

In Mandatory access Control Model (MAC) users are given permission to resource by an administrator. Only an administrator can grant or revoke permission to an object/resource. Permission access to resource is based on a resource security level clearance. Basically it is based on hierarchical security labels and assigns each user and each piece of information or application a particular security level (e.g., classified, secret, top secret) as shown in figure 2. Two

common principles are then applied to determine if a user has access to a particular piece of information: read down access and write up access.

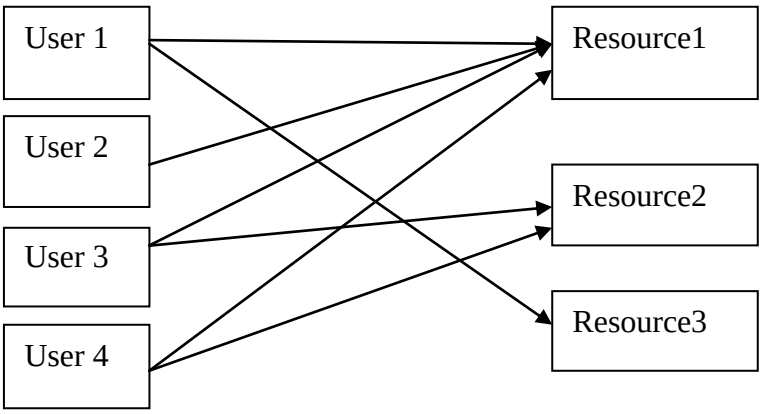

Fig 1 Discretionary Access Control

Read down access gives users the ability to access any piece of information that is at or below their own security level. If a user has a secret security level, they are able to access secret and classified material but not top secret material. Write up access states that a subject's clearance must be dominated by the security level of the data or information generated [4].

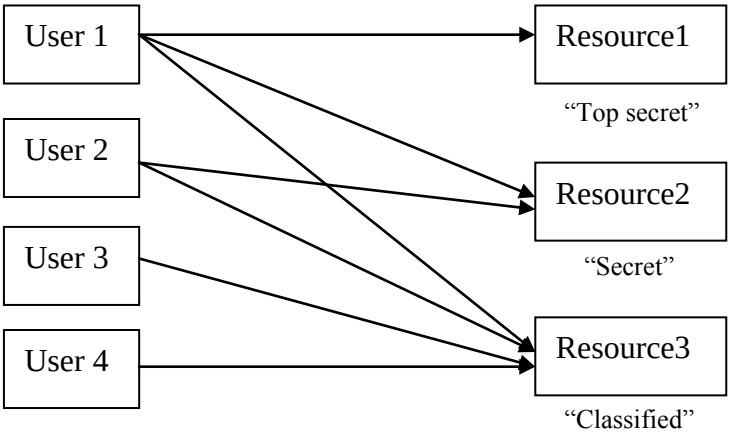

Fig 2 Mandatory Access Control

C. ***Role-based Access Control(RBAC):***

The central notion of RBAC is that permission are associated with roles and users are assigned to appropriate roles [5] or we can say RBAC in a system architecture provide an access to roles and user associated with them as shown in figure 3[4]. In this architecture administrator has the privilege to modify the access granted to roles and to delete a particular role.

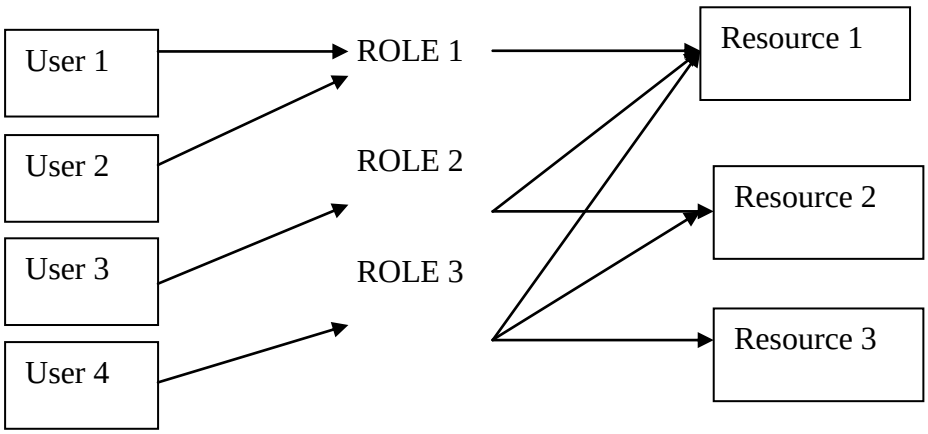

Fig 3 Role-based Access Control

III. ROLE –BASED ACCESS CONTROL MODEL

Due to the need for a better security the National Institute of Standards and Technology (NIST) began a project simply titled as "RBAC Project". Role Based Access Control is an architecture which provides the authority to restrict the user if he is not allowed to access particular content .It is affective in lot of manners. This architecture saves data from unauthorized access. Admin panel has all the rights to restrict user to access data and to edit access rights of the user.

RBAC system has two phases in assigning a privilege to a user: in first phase, user is assigned to one or more roles or role can have many users; here role represent a specific job function within organization with responsibilities associated with it; and in second phase, the roles are checked against the requested operation [1]. In RBAC permissions are assigned to roles rather than user; here permission is an approval of particular mode of access/operation to one or more objects in the system [5].

Family of RBAC model as shown in figure 4 defines in [5] as: RBAC0 is a base model with minimum requirement, RBAC1 and RBAC2 include RBAC0 with their own independent features. RBAC1 include concept of role hierarchies and RBAC2 include constraints and RBAC3 includes RBAC1 and RBAC2 and, by transitivity RBAC0.

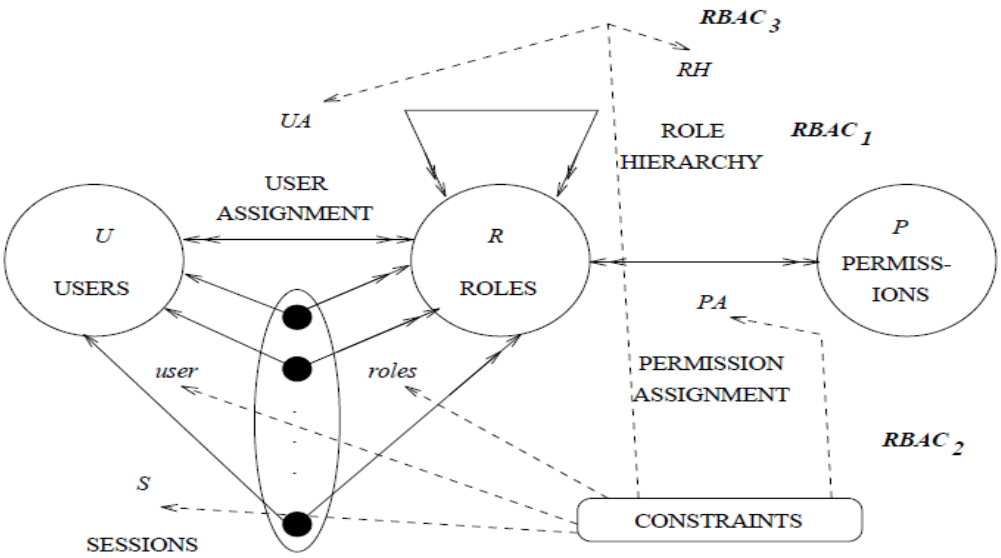

Fig 4 Family of RBAC model

A. ***Users:***

Users are both employees and network mechanisms and entities that require access to a specific resource object.

B. ***Permission:***

Permission is an approval of particular mode of access/operation to one or more objects in the system.

C. ***Role hierarchy (RH):***

Role hierarchy is natural way of organizing roles to reflect the organization's lines of authority and responsibility. By convention, junior role appear at bottom of hierarchic role diagrams and senior role at the top so, hierarchic diagrams are partial order (means reflexive, transitive and anti symmetric) [5].

D. ***User assignment (UA):***

It is many-to-many relation between users and roles means multiple users can be a member of many roles; and roles can have many user.

E. ***Permission assignment (PA):***

It is also many-to-many relation between roles and permissions; means role can have much permission, and the same permission can be assigned to many roles.

F. ***Session:***

Session is a mapping of one user to possibly many roles. Each session is associated with single user and the permissions available to user are the union of permission from all roles activated in that session.

G. ***Constraints:***

Constraints are predicates which, applied to these relations and functions, return value of "acceptable" or "not acceptable". We can view it as in most organization the same individual will not be permitted to be a member of both roles so, here we use constraints to prevent possibility of committing fraud.

RBAC supports three well known security principles: Least privilege, separation of duty (static and dynamic), and data abstraction. Least privilege is also known as least authority. In RBAC least privilege is assignment of minimum set of privileges to user associated with role according to their job necessities. Separation of duties is require for particular set of transactions where no single individual be allowed to execute all transactions within the set.

Separation of duty can be either static or dynamic. Static separation of duty define as, two or more role that cannot be assigned to same user at any time. Restriction is made upon assignment of individuals to roles and allocation of

transactions to roles. Example: no individual who can serve as payment initiator could also serve as payment authorizer. Dynamic separation of duty define as, same individual allows to access two or more roles but exception is that they are not allowed to activate at same time or in same user session.

Data abstraction define as it abstract permissions such as credit and debit for an account object, rather than the read, write and execute permissions typically provided by the operating system[5].

There are many key benefits of using RBAC model:

1) RBAC is policy neutral which enables it to support different security policies and system administrator is responsible for enforcing policy.
2) In RBAC system administrator has authority for granting, revoking and updating membership to set of specified named roles with in system.
3) RBAC model provides more flexibility than DAC and MAC due to many-to-many relation between role and user unlike the access control list in DAC and do not restricting objects based on sensitivity as in MAC.
4) RBAC model implementation is challenging task but once implemented it is easy to scale and require minimal maintenance.
5) Access privileges are handled by assigning permissions in a way that is meaningful, because every operation has specific pre defined meaning with in operation.

IV. PROBLEMS IDENTIFIED

There are several key benefits of using RBAC but among various business and commercial key benefits, it has some drawbacks.

The drawbacks are as follows.

A. Cardinality constraints:

The existing architecture does not implement any restriction over the number of users per role. Therefore, chances of getting hacked in terms of data increases as the administrator does not have any information about how many users are there in each role. Example: In INFORMIX Online Dynamic Server, there is no concept of cardinality constraints to maximize and minimize number of user per role [6].

B. No restriction over transaction:

In existing RBAC model there is no restriction over number of transaction per user. If someone hacks an existing id then it can make multiple transactions from that existing id. It could be a disaster if hacking persists. Example: In Online money transactions, there is no concept of number of transactions allowed per day to minimize loss of being hacked.

V. CONCLUSION & FUTURE SCOPE

Role Based Access Control is a model that provides an architecture in which system administrator has privilege to assign/grant, revoke and edit role to users. RBAC offer as an alternative to traditional Discretionary Access Control (DAC) and Mandatory Access Control (MAC) policies and provide improved security mechanism but with all benefits of RBAC, it has some limitations as:

There is no constraint over role/ user relationship to maximize or minimize number of user per role.

There is no constraint of number of transaction per user.

Hereby, it is understood that attending these limitation will restrict unauthorized access. This in turn will increase scalability and efficiency of system.

REFERENCES

[1] Wei-Tek Tsai, Qihong Shao, "Role-Based Access-Control Using Reference Ontology in Clouds," in *Proc. Tenth International Symposium on autonomous Decentralized Systems (ISADS)*, 2011, p. 121-128.

[2] Gouglidis Antonios, "Towards new access control models for Cloud Computing Systems," in *Proc. Kaspersky – IT Security for the Next Generation – European Cup*, 2011.

[3] David F. Ferraiolo and D. Richard Kuhn, "Role-Based Access Controls," in *Proc. 15th National computer Security Conference, 1992*, p.554-563.

[4] Michael P.Gallaher, Alan C.O' Connor, Brian Kropp, "The Economic Impact Of Role-Based Access Control," National Institute Of Standards & Technology, Gaithersburg, RTI project No 07007.012, March 2002 .

[5] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feintein and Charles E. Youman, "Role-Based Access Control Models," *IEEE Computer.*, vol. 29, no 2, pp. 38-47, Feb 1996.

[6] R. Chandramouli, R. Sandhu, "Role-Based Access-Control Features in Commercial Database Management Systems," in *Proc. 21st National Information Systems Security Conference , Crystal City, Virginia*, Oct 1998.

[7] Dong Xu, "Cloud Computing an Emerging Technology," in *Proc International Conference On Computer Design And Application, Qiahuangdao,* June 2010.

[8] D. Richard Kuhn, "Mutual Exclusion Of Roles as Means Of Implementing Seperation Of Duty In Role-Based Access Control System," in *Proc Symposium on Access Control Models and Technologies , ACM NewYork, USA*, 1997, p. 23-30.

[9] Ravi. Sandhu, David Ferraiolo, Richard Kuhn, "The NIST Model For Role-Based Access Control: Towards a Unified Standard," in *Proc Symposium on Access Control Models and Technologies , ACM NewYork, USA*, 2000, p. 47-63.

