A Hybrid Approach using RBAC and ABAC models

Kunj Amrutbhai Patel
Department of Computer Science Engineering,
University of Texas at Dallas
Kxp180035@utdallas.edu

Abstract—

Protecting resources from unauthorized users is a huge problem for cloud computing. The Role Based Access Control (RBAC) model is a common framework for managing access to data. Access control is widely deployed on many cloud systems. If the number of roles increases, the complexity of the roles increases. In order to get rid of the drawbacks of RBAC, the attribute base access control (ABAC) model has been adopted, which is more versatile. Here permissions are directly connected to roles. This paper being inspired by 3 reference papers introduces such hybrid way by integrating both RBAC and ABAC, a more scalable and dynamic hybrid access control scheme can be developed.

Keywords— Hybrid access control; Role Based Access Control; Attribute Based Access Control.

I. Introduction

Cloud storage provides easy, on-demand network access to a shared pool of configurable computing services (networks, servers, storage, applications and services). Computer owners have small storage space to store all the data. People are now storing their data in the cloud because it is more stable and safer in nature and can provide high processing capacity and many technological applications without any extension of the device over the internet. The private cloud is suited to protect classified documents. As a result, the protection of the private cloud is very critical, several researchers have proposed strategies for data security in private cloud. Two very important strategies for safe access to data are based on the RBAC and ABAC models. The following sections address the Role Based Access and Attribute Based Access Control systems for private cloud computing. A new innovative hybrid scheme using both the RBAC and ABAC models for private cloud protection is proposed.

II. BASIC RBAC MODEL

RBAC (Role-based access control) as explained in **Paper-1** was invented for on-line multi-user and multi-application schemes. The author of RBAC is a security professional from the National Institute of Standards and Technology. The simple RBAC model, consisting of four segments: participants, Tasks, Session and Authorization. Typically, an user is considered a human being. Role is known to be permissions to perform an operation on an object, i.e. an action, function or task that the user may perform. The policy of access control is fully framed around this semantic framework. It is a function within the organisation that represents the authority and the responsibility assigned to the role of the user. It is a set of transactions that the user or a set of users can perform in an organisation. System administration assigns transitions to roles. Session is the method of connecting an user to one or more roles. Next, the user starts a session where a subset of the functions of which the user is a part of the double-headed arrow of the session is running.

Permission and user assignments are many to many relationships. As a result, many permissions are given to a role, and permission can be extended to many roles. The RBAC model is capable of creating a relationship between roles, permissions and roles, and between users and roles. The basic RBAC structure is shown in Figure 1.

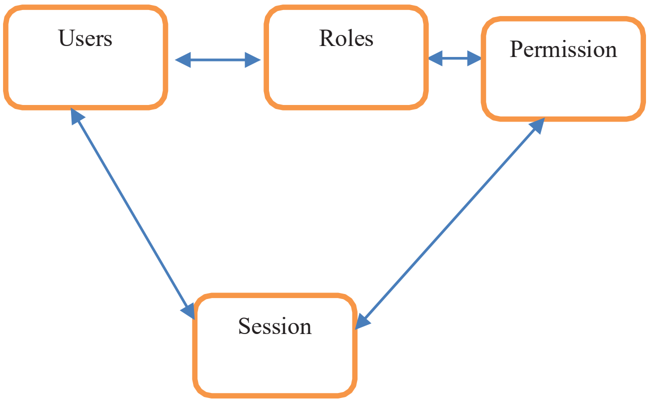

Figure 1 Basic concept of Role Based Access Control

III. BASIC ABAC MODEL

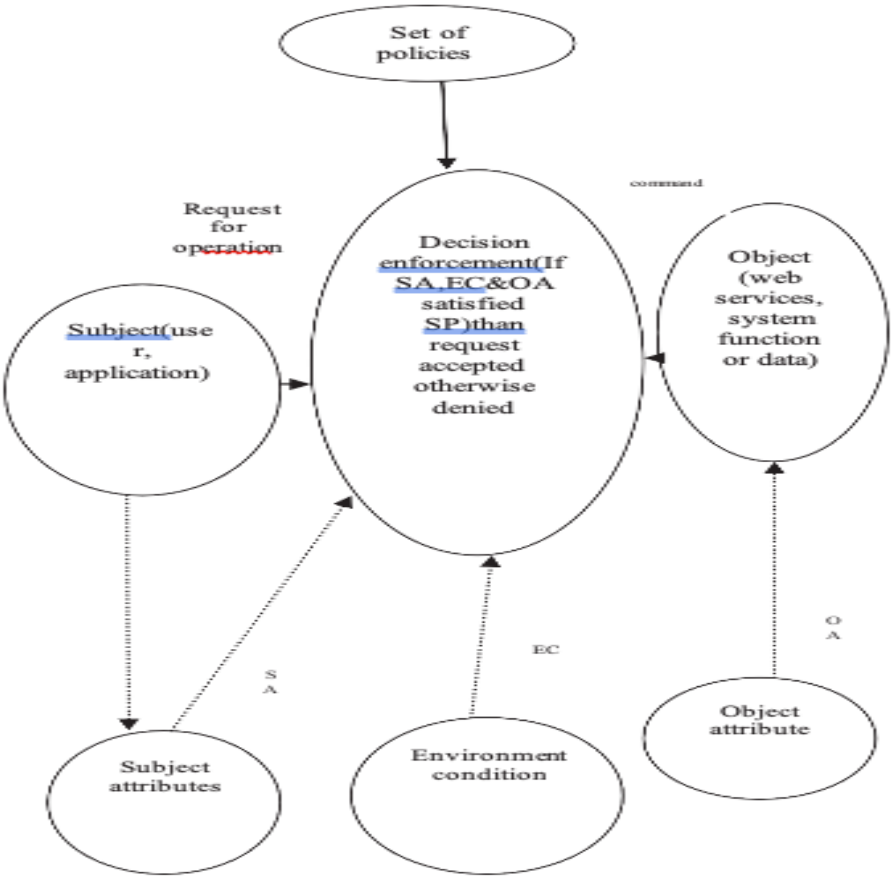
Set of policies
command
Request for operation
Decision enforcement(If SA,EC&OA satisfied SP)than request accepted otherwise denied
Object (web services, system function or data)
Subject(user, application)
O A
EC
S A
Object attribute
Subject attributes
Environment condition

Figure 2 Basic concept of Attribute Based Access Control

The ABAC (Attribute based Access Control) as described in **Paper-2** is based on the various attributes of subjects, objects and environmental conditions. Where these attributes and environmental conditions comply with the policy set, the subject may carry out an operation on the subject. Access is then granted [2]. The policy set is based on the object-based attributes. Object is an entity that can be an application for the user process which can manage objects. It has a lot of attributes for identification. The object is an entity operated by subjects. It has a lot of attributes. For example: -resources such as a web server or document, etc.In short, the ABAC subject and the objects are represented by a set of attributes and the permissions are granted based on the combination of these attributes as described in the policy set. Basic ABAC structure is as shown in Figure 2.

IV. HYBRID ACCESS MODEL

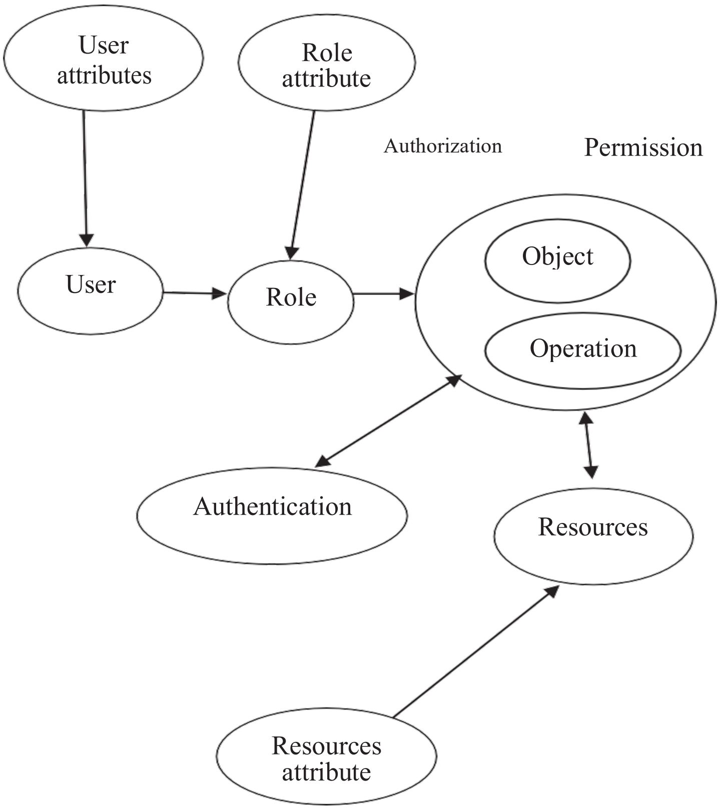

Figure 3 Basic concept of Hybrid Access Model

RBAC has centralised control over various resources and scalability. Roles and permissions are limited in this situation. In Attribute Based Access Control, a single function based on the attribute may be granted different permissions. Some resources can only be accessed by users who perform roles and others who satisfy all roles and attributes.Thus, by integrating all access control schemes, a dynamic situation can be accomplished, and the system can be more flexible. Specific configuration of the Hybrid Access Control as seen in Figure 3.

V. COMPARITION OF ALL MODELS

Merits and Demerits of different access control models:

Mandatory Access Control

- *Merit:* It gives greater security to access the resources.
- *Demerit:* It has a less open environment for the processing of access rights. It's hard to implement.

Discretionary Access Control

- *Merit:* The data owner is in charge of the data access policies. It also has more flexibility than the MAC.
- *Demerit:* It's offers less security.

Role Based Access Control

- *Merit:*
  1) Simple and it's easy to use.
  2) Major RBAC-based cloud computing is open stack, AWS and Microsoft Azure.
  3) The policy specifications are simple.
  4) It's simple to manage.
  5) Trust is global.

- *Demerit:*
  1) Role explosion.
  2) It is not possible to have access to a particular entity without changing the rules.
  3) It has issues related to administrative, data abstraction.
  4) No environmental attribute considerations.
  5) Not well suited to a highly distributed environment.

Attribute Based Access Control

- *Merit:*
  1) It has fine grained access controls.
  2) It is very flexible and expandable, with the potential to increase the number of higher users.
  3) There is no Role Explosion and Role Permit Explosion Problem.

- *Demerit:*
  1) The policy specifications are complex.
  2) The ability to manage is complex.
  3) Trust is local.
  4) Sometimes the attributes of subjects do not match those of objects.

Hybrid model (RBAC + ABAC)

- *Merit:*
  1) It's a more fine-grained access model.
  2) It limits the number of attributes required in the process. This simplifies the user's – permission relations.

VI. CONCLUSION

This paper presented the Role Based Access control and the Attribute-based access control models. RBAC has three separate components: users, role and permissions. Access to services relies on the authorization assigned to the functions. It makes the authorization process quick, since the same permission can be granted to multiple users to play the same role. The attribute-based access control remove user– role assignments. It focuses on the attributes of the user that are necessary to grant access. The drawbacks of these two methods can be solved by integrating both the RBAC and ABAC models which is the hybrid model. In the end, three models are compared.

VII. REFERENCES

[1] V. Nirmalarani, “Protection of Resources using Role Based Access with multilevel Authentication,’ 2014 ISSN, volume 9, November 11.

[2] Xin Jin,Ram Krishnan , “A Unified Attribute Based Access Control Model Covering DAC, MAC, and RBAC,”IFPT International Federation for Information Processing :2012:pp41-55.

[3] Sonu Verma, “Hybrid Access control Model in semantic Web, “International Journal of Information Technology, ISSN, Volume - 1, August 2012, pp 43-50.