International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 4– No.2, September 2012 – www.ijais.org

Analysis of Different Access Control Mechanism in Cloud

Punithasurya K
Post Graduate Scholar
Department of Information Technology
Karunya University, India

Jeba Priya S
Lecturer
Department of Information Technology
Karunya University, India

ABSTRACT

This paper deals with various access control mechanisms that are present in cloud computing. Cloud computing is the emerging technology where resources are available pay as you go basis. Cloud storage technology provides the large pool of storage capacity to the cloud users. Providing security to the data stored in cloud is the major concern. So Security can be enhanced by providing access control to the authorized users. Access control gives the authorization to the users which gives the access privileges on data and other resources. Access control can be enabled in most of the computing environment such as Peer to Peer, Grid and Cloud. Cloud storage services are accessed through a cloud storage gateway. We present various types of access control mechanisms that are used in cloud computing environment.

General Terms

Cloud Computing, Access control.

Keywords

Discretionary access control, Mandatory access control, Role Based Access control , Conventional RBAC, dRBAC, Cloud Optimized RBAC.

1. INTRODUCTION

Cloud computing is said to be usage of computing resources such as hardware and software that can be delivered as a service over the internet. There are various number of resources available such as SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service).

End users can access the resources through a web enabled desktop and mobile. Giving access to those resources through the web is major concern and it enhances the security. Access control gives the authorization to the users to access resources that are publicly available to the users. In the earlier there was various access control mechanisms has been introduced for the secure data access. Access control relies on the security of the system and gives the access to the object.

Traditional access control mechanisms are DAC (Discretionary Access Control), MAC (Mandatory Access Control), RBAC (Role Based Access Control) .The purpose of access control in cloud is to prevent the access on object in cloud by unauthorized users of that particular cloud which will enhance security in the cloud environment. Accesscontrol mechanisms used to mediates the each and every attempt of particular users to the object based on the access privileges given to the system. Traditional access control considers reference monitor that has the authorization database. This database considers the authorization of user [1]. It can be widely used especially in computer science and automation. However the security of information is major concern in cloud. The security of information system directly or indirectly affects the organizations.

Access control is generally said to be policy or procedure that allows, denies or restricts access to a system [2]. It also identifies when the unauthorized users trying to access the system. The mostly used access control methods are identity based access control models [2]. Access control in cloud depends on the cloud storage and its data security and the access option becomes very necessary option in cloud. Access control is very important part in the data center of government and business. It is also important to understand that access control alone not a solution for securing data so the encryption of data also important. There will be a difference between policy decision and mechanism. Access policies are an always high level decision that determines how access are controlled and access decisions are made.

The various types of access control mechanisms are discussed below. In section 2.1 we will discuss Discretionary access control and its performance and in section 2.2 we will discuss Mandatory access control and its performance metrics and in section 2.3 we will discuss about role based access control and dRBAC, coRBAC , ABAC also discussed further.

2. ACCESS CONTROL METHODS

2.1 Discretionary Access Control

This is the traditional access control in which user has the complete control over all the programs. DAC is based on giving access to the user on the basis of user identity and authorization which is defined for open policies.

DAC owns and executes and also it determines permissions to the particular user to the object. DAC policies considers the access of users to the object which is based on the user's identity and authorization that specifies for each user's access method and object that is requested by user. Each individual request to access an object that has been checked. In DAC access method flexibility will be good. In this method most of the authorization is specified explicitly and also authorizations of individual user is closed. And also when authorizations are open then it is said to be open policies.

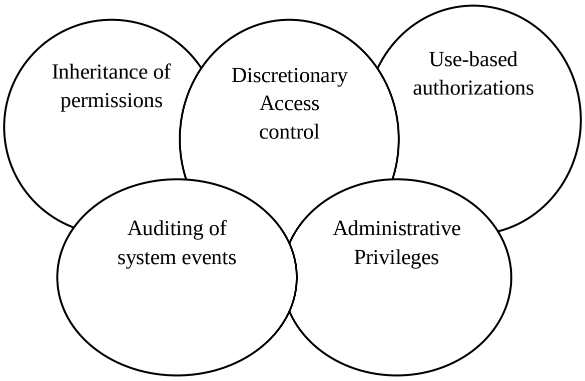
Inheritance of permissions
Discretionary Access control
Use-based authorizations
Auditing of system events
Administrative Privileges

Figure 1. Discretionary Access Control

DAC consists of access rules and access attributes .The access attributes allows the system to define several distinct level of authorization, and the access rules provide the mechanism for the cloud to prevent unauthorized access of sensitive information. DAC provides controlled sharing of objects among various subjects. DAC is said to be the mechanism of “who can access what”. In DAC the owner of an object can choose to grant access permissions to other users. Access control list is associated with each object’s file system. A simple form of Discretionary access control can be file passwords and giving access to the authorized users. DAC mainly deals with the following that are Inheritance of permissions, User-Based Authorizations, Auditing of System Events, and Administrative Privileges.

2.1.1 Advantages of DAC

The DAC mechanism provides the flexibility of usage on information. This method will maintain the authorization database which consists number of authorized user.

2.1.2 Disadvantages of DAC

In DAC there is no assurance on flow of information and also there is no restriction on the usage of information this will make the confusion on the usage of information and also information will be lost. It can be easily attacked by third parties. There is no consistency on information. There might be the chance to steal the copy of original message without owner’s permission. Sometimes owner may change the DAC policies by inserting malicious program.

2.2 Mandatory Access Control

Mandatory access control is based on the access of objects to number of subjects. Mandatory access control is mainly based on the security level. In this individual cannot change the access. Traditional MAC mechanism is mainly coupled with some security consideration. This follows the following two principles [1]. Those are, read down (users current security level must dominate the access of the object being read) and write up (users current security level must dominate the access of the object being write)

MAC based on the classification of objects and subjects present in the cloud environment. Access to a particular object is allowed only if some relationship is satisfied. Each object and subject present in cloud environment assigned some security level. This security level helps to identify the current access state of the object. Security level associated with user also called clearance [1]. MAC used to protect network and file system, block users from accessing without appropriate authorization. In MAC the users will not be permitted to change the access control and its security level. MAC label is said to be security attribute which may be applied to subjects and objects throughout the system.

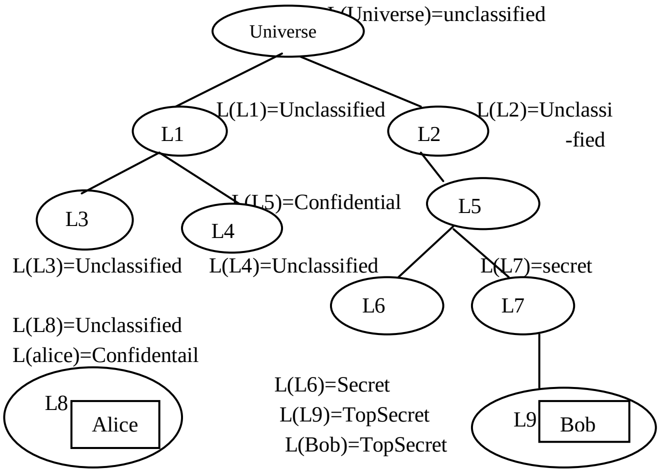

Figure 2. Example Mandatory Access Control Model

In Figure 2 it mentions the mandatory access control based on the security level identified. The security level is hierarchical based on the security level from the top most security level. Here alice and bob are in the security level based on the classification of mandatory access control. This hierarchical classification consists of the following TopSecret (TS), Secret(S), Confidential(C) and Unclassified (U) [1]. In figure 2 the security level for alice and bob is identified from the confidential and top secret level. User alice has the permission to access information from the cloud where it can be mentioned as confidential level. But Alice has no permission to read down the data of Bob because bob is associated with security level TopSecret (TS). Here the hierarchical security level is associated with the objects and subjects. Alice and Bob is said to be subjects and the information that they request is called as objects.

Users can be associated with the object based on the degree of trust and its security level. MAC normally takes the hierarchical approach to control the access of cloud data. This hierarchical approach depends on the security level. Normally MAC consists of security label. This security label is assigned to all subjects based on the requesting object. The security label is consists of two information that are a classification and category. Classification consists of top secret and confidential information. Category is based on the security level. Before accessing the data from cloud MAC will check the user’s identity based on the classification and category. It enforces the organizational security policies. It has been found that MAC is more secure than DAC.

In DAC the flow of information will not be proper but in MAC it is controlled based on the security level assigned and also it assigns security clearance to each user. All users can read from lower hierarchy only if the owner gives permission and also users have permission to write to the higher hierarchy based on the authorization.

2.2.1 Advantages of MAC

In MAC information integrity will increase and also it prevents the flow from low objects to high objects. This information controlling will achieve the integrity. MAC mostly used in military and government applications.MAC provides multilevel security. Prevents from unauthorized users from making changes. When we consider the flow of information in the vertical order it will provide the multilateral security. In MAC every access to the user will be mediated so the information that is accessed through cloud is more secure. Here access is authorized or restricted to objects based on the time of day depending on the security level on the resource and user credential. Scalability in MAC is lower and also it won't be adapt to all type of applications.

2.2.2 Disadvantages of MAC

The major drawback in MAC is that once the security level is identified to particular subject in the hierarchy it won't modify the security level.

2.3 Role-Based Access Control

In role based access control access decisions are based on the individual's roles and responsibilities within the cloud environment. It formulates the user's access to the system based on the activities that the user has been executed in the cloud. It requires the identification of roles of users on the system. Role can be set of objects or actions associated with the subject. Role may vary depends on the user's priority. RBAC provides the web based application security. Roles are assigned based on the particular cloud organizational structure with their security policies. Each role in the organization's profile includes all authorized users, commands, transaction and allowable information access. Roles can be assigned based on the least privilege. These identified roles can be transferred and used based on the appropriate procedures and security policies. Roles can be managed centrally.

RBAC implemented in three ways based on the design constraints that are, $RABC_0$, $RBAC_1$, $RBAC_2$, $RBAC_3$ [3]. $RBAC_0$ is based on the least privileges and separation of roles. It does not contain hierarchy and permissions to the particular object is assigned directly [3]. $RBAC_1$ is based on the use of hierarchies and $RBAC_2$ is based on the hierarchy within the $RBAC_1$ [3]. $RBAC_3$ is based on the both constraints and hierarchy [3].

RBAC allows users to execute multiple roles at the same time and roles are the useful approach to organizations such as cloud, grid and peer to peer environment. In some cases the only one role can be assigned to one user and it recognize the same roles to other users jointly. After the DAC and MAC

Mechanism RBAC has been proven as the efficient access control mechanisms. So securing information on the cloud is similar to securing data on the web. RBAC on the web is user-pull architecture [4]. RBAC can be used to provide service and assigns roles to each user's based on the user identity and its role based on the execution environment in cloud. RBAC on the web is implemented with server pull architecture [4]. RBAC permissions are associated with roles and users are assigned to appropriate roles. System administrators only can be able to create roles and granting permissions to those roles. Without RBAC it is difficult to determine what permission has been assigned to which user.

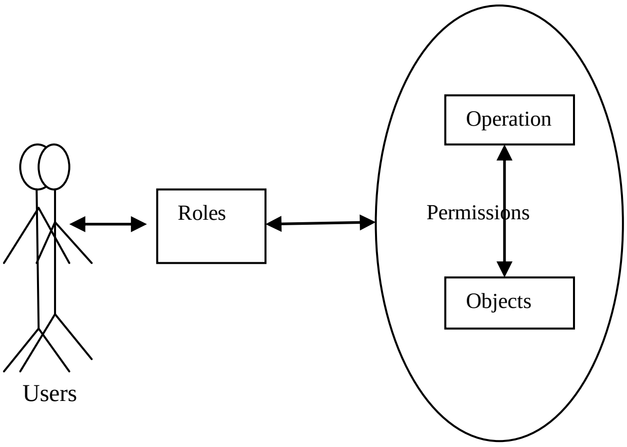

Figure 3: Role-Based Access Control

RBAC can be implemented based on the user-pull architecture and server-pull architecture [4]. User-pull architecture means user pulls their roles from server and server-pull architecture means web server pulls their roles from the server[4]. These two methods can be used in the RBAC model.

2.3.1 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.

2.3.2 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 .

3. RELATED TECHNOLOGIES

There was traditional access control methods which are DAC,MAC and RBAC and also some access control methods that are used in cloud that are dRBAC,ABAC and coRBAC

3.1 ABAC (Attribute Based Access Control)

ABAC is attribute based access control normally considers identification, authentication, authorization and accountability. User identity is the major element in access control means then it is said to be Identity Based Access Control (IBAC). But IBAC is problematic when implementing it in large distributed system.

RBAC has the problem of assigning privileges to the user ABAC solves this problem based on the set of user attributes. In ABAC access is based on the set of user attributes. It can also be named as authentication based access control. It extends RBAC based on the following [5].

i) Delegation of attribute authority
ii) Decentralization of attributes
iii) Interference of attributes

In attribute based access control the attributes are considered based on the user's request and the type of access user wish to access and the needed resources of user. ABAC is more secure and flexible and scalable and it provides hierarchical structure. Set of user attributes will be maintained individually.

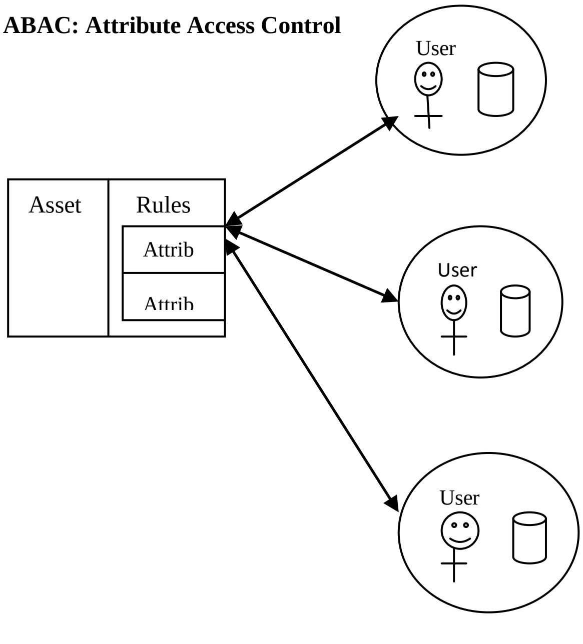

Figure 4: Attribute Based Access Control

3.2 dRBAC (distributed RBAC)

dRBAC is distributed role based access control which supports large distributed system. For multiple organizations dRBAC is mainly used. dRBAC solves the problem of giving access control in multiple organization. dRBAC has the following problems:

This dRBAC method has the high time complexity and high space complexity. Due to the increasing nature of cloud users and sequential access of resources which will cause the redundancy and inconsistency of information access and also this will cause the complex cross domain problems.

3.3 coRBAC (Cloud optimized RBAC)

RBAC enforcing the management of data across large-scale enterprise so the security is higher but still roles cannot be maintained properly. So when considering RBAC on web there is no high user mobility.

CoRBAC inherits the functionality of dRBAC and RBAC [6] here coRBAC improves the certification process. CoRBAC reduces the following [6].

i) Unnecessary process of establishing secure connection
ii) There is no need of setting up multilevel cache
iii) Space and time complexity of access control system is reduced.

Similarly conventional RBAC provides scalability but it fails when having large number of users in the system. The major drawback of conventional RBAC is excess time of authentication and login time. But coRBAC improves the overall efficiency.

3.3.1 Disadvantages of coRBAC:

coRBAC produces the CA from the third party instead of managing by the server administrator. When user arriving to access the resources it will be difficult to issue CA by server admin so in coRBAC third party authorization is implemented. But here certification management is major issue. When user willing to change their certificate it will lead to confusion and unnecessary cost also be increased.

4. NEGATIVE AUTHORIZATION IN CLOUD

Access control in cloud should not lead spreading of fragmented information access to users. So negative authorization is needed when there is need of restricting the access of user to the undesired information.

Normally access is based on the username, user IP, address and requested type [7]. The disadvantage of this particular method is how the provider will identify this particular information is undesired to the particular user. But providing negative authorization reduces the stealing of information of other users.

Table 1. Comparison Of Various Access Control Methods

Access Control	DAC	MAC	RBAC	dRBAC	ABAC	coRBAC
User's Convenience	High	varies	High	Medium	High	High
Performance	Low	Based on security level	High	Depends on subjects	High	Depends on user
Reusability	Multi	Not mentioned	Multi	Multi	Multi	Multi
Role Assignment	Not Mentioned	Single Node assignment	Multi	Multi	Not mentioned	Multi
Single Point Failure	Authorization failure	less	Less	High	-	-
Node overhead	less	less	Less	High	varies	-
Authentication failure	less	Depends on distributed environment	Based on job role assigned	High	less	less

5. CONCLUSION

Access control in cloud is major research area which will enhance the security on user's data that are stored in cloud environment. Ensuring access control in cloud enhances the security. We have analyzed various access control mechanism that are used in previous and current. A comprehensive and description and analysis of DAC, MAC and RBAC provide the importance of access control in cloud to ensure the security of user's information.

In this study we have analyzed the various access control technique that are popularly used in cloud environment such as DAC, MAC, RBAC, ABAC, dRBAC, coRBAC. Access control of cloud is based on the above mechanism basically and performance also compared based on the user satisfaction. But in the large distributed system like cloud and grid needs more flexible and scalable access control. The advantage and disadvantage of various access control technology discussed with their performance. The traditional access control is DAC, MAC and RBAC and related access control technologies also discussed further. This survey ensures the need of security of user and authentication need of user and security of cloud information by providing enhanced access control technology. The main contribution of this paper is to understand the various access control mechanisms in cloud.

6. REFERENCES

[1] Ravi S. Sandhu and Pierangela Samarati "Access Control: Principles and Practice" IEEE Communications Magazine, September 1994.

[2] Yingjie Xia, Li Kuang and Mingzhe Zhu "A Hierarchical Access Control Scheme in Cloud using HHECC" Information Technology Journal 9 (8): 1598-1606 , 2010

[3] Hazen A.Weber "Role Based Access Control: The NIST solution" San Institute of Info Reading Room, October 3 ,2008.

[4] Joon S.Park, Gail-Joon Ahn, Ravi Sandhu "Role-based Access control on the web using LDAP"

[5] Abdul Raouf Khan " Access control in cloud computing Environment" ARPN Journal of Engineering and Applied Science,vol 7, No.5 May 2012.

[6] Zhu Tiayni, Liu Weidong, Song jiaxing "An Efficient role based access control system for cloud computing" 2011 11th IEEE International Conference on Computer and Information Technology.

[7] Xiaohui Li, Jingsha he, Ting Zhang "Negative Authorization in Access Control for Cloud Computing" International Journal of security and its Applications. Vol. 6, No.2 April 2012.

[8] Armbrust, M., A. Fox, R.Griffith, A.D. Joseph and R.Katz et al,2010. "A view of cloud computing Commun. ACM., 53: 50-58

[9] Vouk, M.A., 2008 Cloud computing-issues, research and implementations. J.Comput. Inform Technol.,4: 235-246

[10] Tolone, W.G, Ahn, T.Pai and S Hong, 2005 "Access control in collaborative systems", ACM Comput.Surv.,37: 29-41.

[11] Zhiugo wan, Jun'e Liu, Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" IEEE Transaction on Information Forensics and security, April 2012.

[12] Ramadan Abdunabi, " Extensions to the Role Based Access Control Model for Newer Computing paradigms", Oct 26,2010

[13] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang, Shanbiao Wang, "Towards Temporal Access Control in Cloud Computing",

[14] Lorenzo Cirio, Isabel F. Cruz, Roberto Tamassia, "A Role and Attribute based Access Control System using Semantic Web Technologie".

[15] Mariana Raykova, Hang Zhao, Steven M. Bellovin, "Privacy Enhanced Access Control for Outsourced Data Sharing".

[16] V.Sathya Preiya, R.Pavithra, Dr.Joshi, “Secure Role Based Data Access Control in Cloud Computing” International Journal of Computer Trends and Technology, may 2011.

[17] Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou, “ Achieving Secure, Scalable and Fine-Grained Data Access Control in Cloud Computing”

[18] Amanda Crowell, University of Maryland. “ A Survey of Access Control Policies”.

[19] Yongdong Wu, Vivy Suhendra, Huaqun Guo, “A Gateway- Based Access Control Scheme for Collaborative Clouds” Institute for InfoComm Research.

[20] Sushmita Ruj, Amiya Nayak, Ivon Stojmenovic, “DACC: Distributed Access Control in clouds” 2011 International Joint Conference of IEEE TrustCom-11/IEEE-ICESS-11/FCST-11.