ISSN:2229-6093

Anjali Soni et al , International Journal of Computer Technology & Applications,Vol 8(5),595-601

# A Survey on Access Control Mechanism Used In Cloud Computing

**Anjali soni**
**(UIT) RGPV Bhopal, India**
anjali.07soni@gmail.com

**Dr. Sanjay Silakari**
**(UIT) RGPV Bhopal, India**
ssilakari@yahoo.com

**Prof. Uday Chaurasia**
**(UIT) RGPV Bhopal, India**
udaychourasia@rgtu.net

***Abstract—*** This paper deals with numerous access control mechanisms that square measure present in cloud computing. Cloud computing is that the rising technology wherever resources square measure offered pay as you go basis. Cloud storage technology provides the big pool of storage capability to the cloud users. Providing security to the info keeps in cloud is that the major concern. Thus Security is increased by providing access control to the approved users. Access control provides the authorization to the users which supplies the access privileges on knowledge and different resources. Access control is enabled in most of the computing atmosphere like Peer to look, Grid and Cloud. Cloud storage services square measure accessed through a cloud storage entryway. We have a tendency to present numerous kinds of access control mechanisms that square measure utilized in cloud computing atmosphere.

Keywords—Access control, DAC, MAC, RBAC, ABE and HABE.

## 1.INTRODUCTION

Cloud computing is alleged to be usage of computing resources like hardware and software package that may be delivered as a service over the web. There are varied range of resources accessible like Software as a Service (SaaS)[20], Platform as a Service (PaaS)[20], Infrastructure as a Service (IaaS)[20].
End users will access the resources through an online enabled desktop and mobile. Giving access to those resources through the online is major concern and it enhances the protection. Access control offers the authorization to the users to access resources that are in public accessible to the users. Within the earlier there was varied access control mechanisms have been introduced for the secure information access. Access control depends on the protection of the system and provides the access to the thing. Traditional access control mechanisms are Discretionary Access Control (DAC)[6], Mandatory Access Control (MAC)[1], Role based Access Control (RABC)[3] .The motive of access control in cloud is to stop the access on object in cloud by unauthorized users of that exact cloud which can enhance security within the cloud atmosphere. Access control mechanisms want to mediate the every and each try of specific users to the thing supported the access privileges given to the system. Ancient access control considers reference monitor that has the authorization information. This information considers the authorization of user [1]. It will be wide used particularly in engineering science and automation. But the protection of data is major concern in cloud. The protection of data system directly or indirectly affects the organizations. In the field of physical and information security, access control is selective restriction of access to a place or other resources [2]. It additionally identifies once the unauthorized users making an attempt to access the system. The mainly used access control technology square measure identity based access control models [2]. Access control in cloud relies on the cloud spare and its info security and additionally the access alternative becomes really compulsory alternative in cloud. Access control is foremost component inside the knowledge center of administration and employment. Access control is extremely necessary half within the information center of state and business. It's conjointly necessary to know that access control alone not an answer for securing information that the encoding of knowledge conjointly necessary. There'll be a distinction between policy call and mechanism. Access policies square measure perpetually high level call that determines however access square measure controlled and access choices square measure created. The assorted varieties of access control mechanisms square measure mentioned below. In section 2.1 we are going to discuss Discretionary access control and its performance and in section 2.2 we are going to discuss mandatory access control and its performance metrics and in section 2.3 we are going to discuss regarding role based access control and ABAC, ABE, HABE conjointly mentioned further.

ISSN:2229-6093



## 2. ACCESS CONTROL METHODS

### 2.1 Discretionary Access Control

This is the standard access control during which user has the entire management over all the programs. DAC is predicated on giving access to the user on the scheme of user distinguishes and permission that is determine for open strategy. DAC owns and executes and conjointly it determines permissions to the actual user to the thing. DAC policies considers the access of users to the thing that is predicated on the user's identity and authorization that specifies for every user's access technique and object that's requested by user. Every individual request to access associate object that has been checked. In DAC access technique flexibility are sensible. During this technique most of the authorization is fixed expressly and conjointly authorizations of individual user is closed. And conjointly once authorizations are open then it's aforementioned to be open policies. DAC consists of access rules and access attributes .The access attributes permits the system to outline many distinct level of authorization, and therefore the access rules give the mechanism for the cloud to stop unauthorized access of sensitive data. DAC provides controlled sharing of objects among varied subjects. DAC is alleged to be the mechanism of "who will access what". In DAC the owner of associate object will prefer to grant access permissions to alternative users. Access control list is related to every object's classification system. a straightforward style of Discretionary access control will be file passwords and giving access to the approved users. DAC primarily deals with the subsequent that are legacy of authority, User-Based permission, survey of system occurrences, and executive right [6].

#### 2.1.1 Advantages of DAC

The DAC mechanism provides the plasticity of usage on info. This technique can maintain the authorization information that consists variety of approved user.

#### 2.1.2 Disadvantages of DAC

In DAC there's no assurance on flow info or data or knowledge and additionally there's no restriction on the usage of data this can build the confusion on the usage of data and additionally information are going to be lost. It is simply attacked by third parties. There's no consistency on info. There may well be the probability to pirate the duplicate of genuine memo while not owner's authority. Generally owner might amendment the DAC policies by inserting Trojan horse.

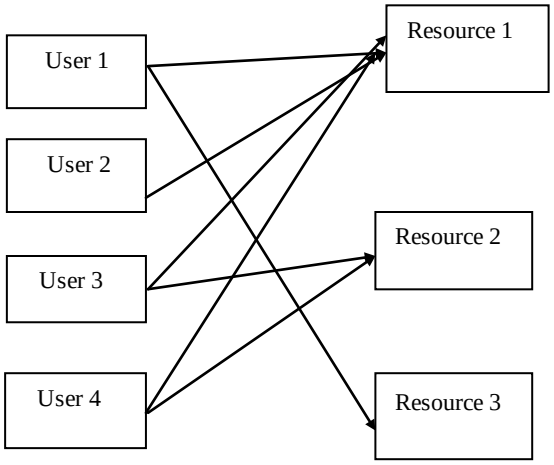


**Figure 1: Discretionary Access Control [19]**

### 2.2 Mandatory Access Control

Mandatory access control relies on the access of objects to variety of subjects. Necessary access control is especially supported the safety level. During this individual cannot amendment the access. Ancient MAC mechanism is especially not to mention some security thought. This follows the subsequent 2 principles [1]. Those are, browse down (users current security level should dominate the access of the item being read) and write up (users current security level should dominate the access of the item being write)

MAC supported the classification of objects and subjects available within the cloud setting. Access to a selected object is allowed provided that some relationship is fulfilled. Every object and subject present in cloud setting assigned some security level. This security level helps to spot the present access state of the item. Security level related to user conjointly referred to as clearance [1]. MAC won't to defend network and filing system, block users from accessing while not acceptable authorization. In MAC the users won't be allowable to alter the access control and its security level. MAC label is alleged to be security attribute which can be applied to subjects and objects throughout the system.

#### 2.2.1 Advantages of MAC

In MAC info integrity can increase and additionally it prevents the ensue low objects to high objects. This info dominant can win the integrity. MAC largely employed in military and government applications.MAC provides construction security.

Prevents from unauthorized users from creating changes. Once we think about the flow of data within the vertical order it'll give the multilateral security. In MAC each access to the user are mediate that the info that's accessed through cloud is safer. Here access is permitted or restricted to things supported the time of day reckoning on the protection level on the resource and user written document. Measurability in MAC is lower and additionally it won't be adapt to any or all form of applications.

**2.2.2 Disadvantages of MAC**

The major disadvantage in MAC is that when the safety level is known to explicit subject within the hierarchy it won't modify the safety level.

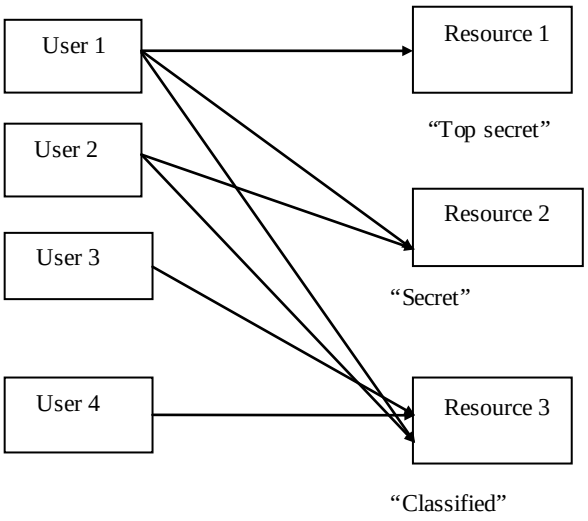


**Figure 2: Mandatory Access Control [19]**

## 2.3 Role-Based Access Control

RBAC allows access based on the job designation. RBAC largely remove discretion when giving access to objects. It construct the user's access to the system supported the activities that the user has been dead within the cloud. It needs the identification of roles of users on the system. Role is set of objects or actions related to the topic. Role might vary depends on the user's priority. RBAC provides the net primarily based application security. Roles square measure assigned supported the actual cloud structure with their security policies. Every role within the organization's profile includes all approved users, commands, group action and allowable data access. Roles is assigned supported the smallest amount privilege. These known roles is transferred and used supported the acceptable procedures and security policies. Roles are managed centrally. RBAC enforced in 3 ways supported the look constraints that square measure, RABC0, RBAC1, RBAC2, RBAC3 [3]. RBAC0 is predicated on the smallest amount privileges and separation of roles. It doesn't contain hierarchy and permissions to the actual object are assigned directly [3]. RBAC1 is predicated on the employment of hierarchies and RBAC2 is predicated on the hierarchy inside the RBAC1 [3]. RBAC3 is predicated on the each constraints and hierarchy [3]. RBAC permits users to execute multiple roles at constant time and roles square measure the helpful approach to organizations like cloud, grid and peer to look atmosphere. In some cases the sole one role is assigned to 1 user and it acknowledge constant roles to alternative users conjointly. When the DAC and MAC Mechanism RBAC has been tried because the economical access controls mechanisms. Thus securing data on the cloud is analogous to securing information on the net. RBAC on the net is user-pull design [4]. RBAC is accustomed give service and assigns roles to every user's supported the user identity and its role supported the execution atmosphere in cloud. RBAC on the net is enforced with server pull design [4]. RBAC permissions square measure related to roles and users square measure assigned to acceptable roles. System directors solely are ready to produce roles and granting permissions to those roles. While not RBAC it's troublesome to work out what permission has been assigned to that user.

**2.3.1 Advantages of RBAC**

It provides hierarchy roles of access supported several applications. Roles square measure allotted supported the smallest amount privilege for the actual object, therefore this may minimize the harm of knowledge by intruders. Separations of roles are going to be maintained therefore there's no likelihood of misuse of knowledge as a result of every user allotted to individual roles. These separations of roles are often either static or dynamic. RBAC provides the classification of user supported their capital punishment atmosphere.

Role primarily based Access control has following body policies. Those square measure Centralized, class-conscious, Cooperative, Ownership, and localized. In giant distributed system centralized access right isn't acceptable.

**2.3.2 Disadvantages of RBAC**

Sometimes it's tough to achieve that privilege to that user it's been related to a selected role. Permissions related to every role will be deleted or modified supported the privilege of role modification. Job roles square measure assigned supported the smallest amount privilege however still modification of role of user might need some confusion once considering the permissions of every user related to that role.

ISSN:2229-6093



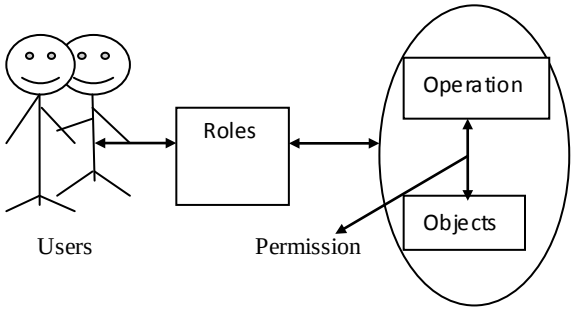


**Figure 3: Role - Based Access Control [3]**

## 2.4 ABAC (Attribute Based Access Control)

ABAC is one of the access control mechanism in which access privileges are allowed to users through the use of policies which merge attributes jointly. User identity is that the crucial part in access control means then it is called to be Identity primarily based Access control (IBAC). However IBAC is problematic once implementing it in massive distributed system.

RBAC has drawback| of assignment privileges to the user ABAC solves this problem supported the set of user attributes. In ABAC access relies on the set of user attributes. It may also be named as authentication primarily based access control. It extends RBAC supported the subsequent [5].

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

In attribute primarily based access control the attributes are considered based on user's need and also the type of access user want to access and also the requested services of user.

**2.4.1 Advantages of ABAC:** Since ABAC[5] has involvement of attributes it offer better security than various access control models. ABAC is higher secure and adaptable and climbable and it provides perpendicular design.

**2.4.2 Disadvantages of ABAC:** ABAC[5] doesn't give the user role detail notion.

## 2.5 Attribute based Encryption (ABE)

ABE model was introduced by Sahai and Waters[8] in 2005. ABE[8] permits users to inscribe and decode information supported user attributes. The confidential key of a user and also the cipher text are relying upon attributes. The confidential writing of a cipher text is feasible as long as the set of attributes of the user key matches the attributes of the cipher text. ABE enforces access control through public key cryptography. The major aim for these models is to given confidentiality and access control. The major features are to given adaptability, compatible and fine grained access control. In classical model, and this may be achieved only user and server are in a very trusty environment [12]. Another drawback with attribute based mostly confidential writing (ABE) strategy is that information owner must use each approved user's public key to inscribe information.

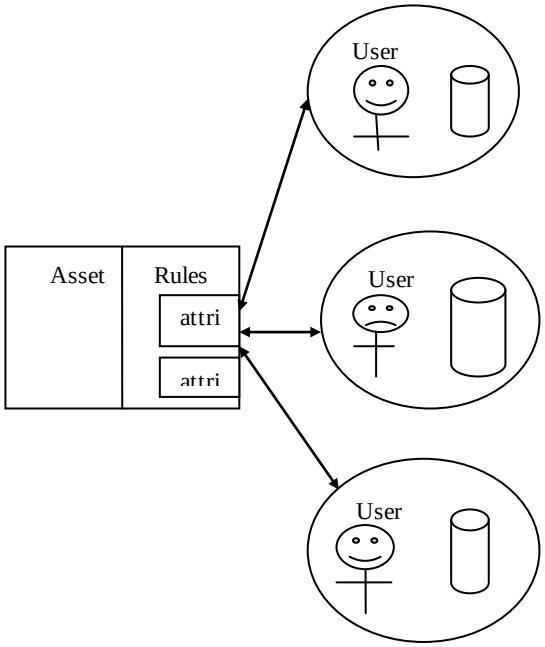


**Figure 4: Attribute Based Access Control [6]**

**2.6 Hierarchical Attribute based Encryption (HABE)[9]**

The HABE model was introduced by Wang et al [9]. HABE[9] model has the vertical design containing of origin master at the highest, proceed by numerous field masters that collection of set of users and users have the set of properties as shown within the Figure seven [6].

**2.6.1 Advantages of HABE**

This strategy will contented the feature of rear access control, compatible and deputation. It will concern to realize proxy re-encryption [9].

**2.6.2 Disadvantages of HABE**

In exercise, it's incompatible to perform HABE, since all attribute could also be operate by similar environment authority; similar attribute could also be operated by many environment authorities.

Table 1. Differentiation between Various Access Control Mechanisms

| Access Control | DAC[6] | MAC[1] | RBAC[3] | ABAC[5] | ABE[8] | HABE[14] |
|---|---|---|---|---|---|---|
| User's Ease | Good | Diverse | Good | Good | Good | Good |
| Transformable | Many | Not remark | Many | Many | Many | Many |
| Single point collapse | Permission collapse | Small | Small | _ | Small | Good |
| Permission Collapse | Small | Rely on distributed scenario | Rely on position allocate | Small | Good | Small |
| Job allocation | Not remark | Single node allocate | Many | Not remark | Not remark | _ |
| Performance | Less | Based on reliability level | Good | Good | Median | Good |
| Node overhead | Small | Many | Small | Diverse | Not remark | Diverse |
| Scalable | Good | No | Small | No | Small | Good |
| Efficient | Adaptable | Not adaptable | Adaptable | Good | Median | Adaptable |
| Fine grained access control | Small | Good | Good | Median | Short | Good |

## 3.CONLUSION

Access control in cloud is major analysis space which is able to enhance the safety on user's information that area unit hold on in cloud surroundings Guaranteeing access control in cloud enhances the safety. We've got analyzed varied access contro mechanism that area unit utilized in previous and current. A comprehensive and outline and analysis o DAC, MAC and RBAC give the importance of access control in cloud to confirm the safety of user's data.

In this study we've got analyzed the assorted access control technique that area unit popularly utilized in cloud surroundings like DAC, MAC, RBAC, ABAC, ABE, HABE. Access control of cloud relies on the on top of mechanism essentially and performance conjointly compared supported the user satisfaction However within the giant distributed system like cloud and grid desires a lot of versatile and climbable access control. The advantage and disadvantage o varied access control technology mentioned with their performance. The normal access control is DAC, MAC and RBAC and connected access contro technologies conjointly mentioned more. This survey ensures would |the requirement of security of user and authentication need of user and security of cloud data by providing increased access contro technology. The most contribution of this paper is to grasp the assorted access control methods in cloud.

## 4.REFERENCES

1. Ravi S., Sandhu and Pierangela Samarati,(1994) Access Control: Principles and Practice IEEE Communications Magazine.
2. Yingjie Xia, Li Kuang and Mingzhe Zhu,(2010) A Hierarchical Access Control Scheme in Cloud using HHECC : Information Technology Journal, 9 (8): 1598-1606.
3. Hazen A.Weber,(2008) Role Based Access Control: The NIST solution San Institute of Info Reading Room., October 3.
4. Joon S.Park., Gail-Joon Ahn, Ravi Sandhu Role-based Access control on the web using LDAP ACM Transactions on Information and System Security., Volume four ,, No. 1, February 2001.
5. Abdul Raouf Khan Access control in cloud computing Environment ARPN Journal of Engineering and Applied Science., volume seven, No.5 May 2012.
6. Younis A. younis, kashif kifayat, madjid merabti,(2014) an access control model for cloud computing journal of information security and applications.
7. Manoj V. Thomas; K. Chandra sekaran,(2013) an access control model for cloud computing enviorment advanced computing, networking and security 2nd international conference on 15-17 Dec.
8. A. Sahai and B.Waters,(2005) Fuzzy identity-based encryption in Proc. Eurocrypt., pp. 457473..
9. Q. Liu, G. Wang, and J. Wu,(2012) Time based proxy re-encryption scheme for secure data sharing in a cloud environment, Information Sciences., In Press.
10. N.krishna, L.Bhavani,(2013) HASBE: A Hierarchical Attribute Set Based Encryption For Flexible, Scalable And Fine Grained Access Control In Cloud Computing International Journal of Computer & Organization Trends –Volume three: Issue 9 ,, Oct.
11. Armbrust, M., A. Fox, RGriffith, A.D., Joseph and R Katz et al,(2010). A view of cloud computing Commun. ACM., 53: 50-58..
12. Vouk, M.A.,(2008). Cloud computing-issues research and implementations. J., Comput. Inform Technol.,,4: 235-246 ;
13. Tolone, W.G, Ahn, T. Pai and S Hong, (2005) Access control in collaborative systems, ACM Comput.,37: 29-41.
14. Zhiugo wan, Jun'e Liu, Robert H., Deng,(2012). HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing IEEE Transaction on Information Forensics and security.
15. Ramadan Abdunabi, (2010) Extensions to the Role Based Access Control Model for Newer Computing paradigms :October 26.
16. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang, Shanbiao Wang,(2012). Towards Temporal Access Control in Cloud

Computing IEEE conference on computer communication.

17. Lorenzo Cirio., Isabel F Cruz., Roberto Tamassia,(2007). A Role and Attribute based Access Control System using Semantic Web Technologie nov. 25.

18. Mariana Raykova., Hang Zhao., Steven M. Bellovin,(2012). Privacy Enhanced Access Control for Outsourced Data sharing financial cryptography and data security: 16th international conference pp: 223-238.
19. Abhishek majumder Suyel Namasudra and Samir Nath,(2014) "Taxonomy and classification of access control models for cloud environment" journal of Springer;

20. https://en.wikipedia.org/wiki/Cloud_computing.

21. Bibin K Onankunju "Access Control in Cloud Computing" International Journal of Scientific and Research Publications, Vol. three, Issue 9, September 2013.
22. Prasad. V.potluri "access control in cloud computing based on broadcast group key management" international journal of scientific engineering and technology research volume four, issue January 02-2015.