CC ASSIGNMENT-01

Name-Vishal Singh
Roll No.-1905704
Branch-CSE

Q. What is cloud access control mechanism ? Discuss some of algorithm for it.

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. 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.

ACCESS CONTROL METHODS -

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.

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.

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

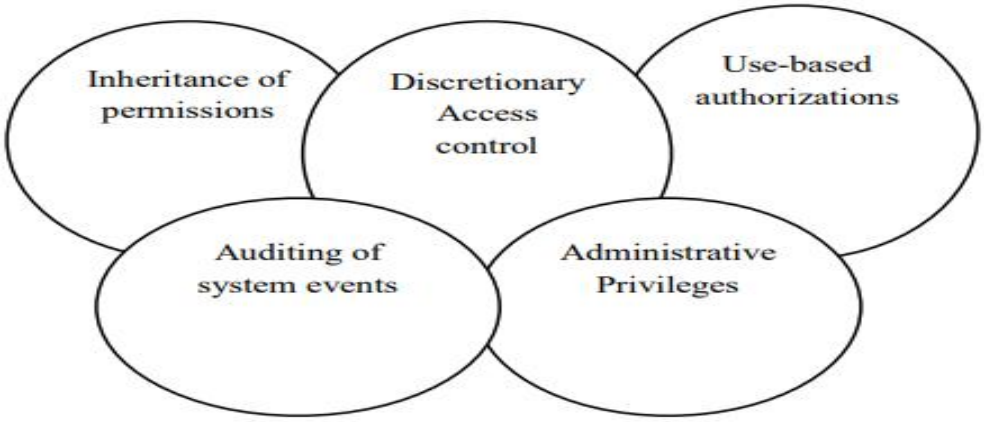

Figure 1. Discretionary Access Control

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.

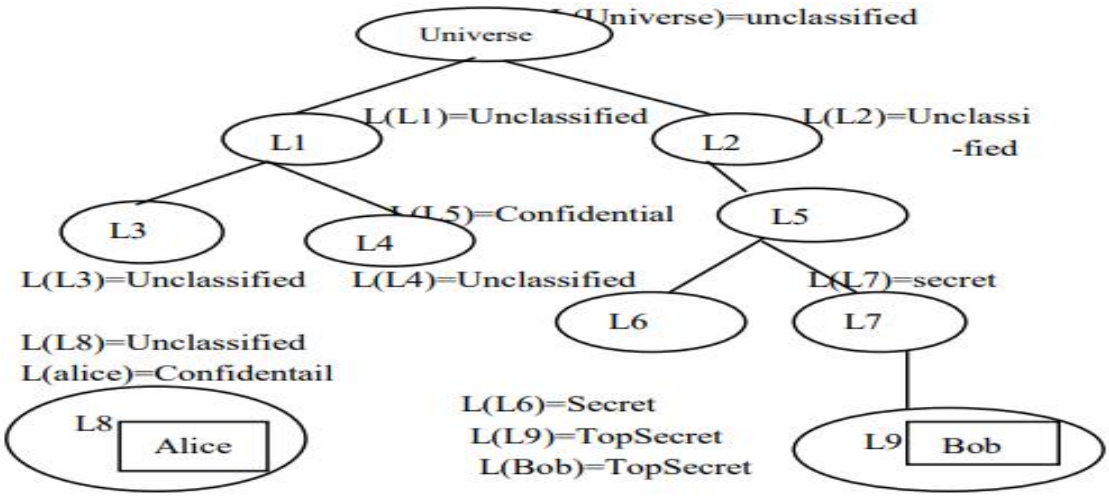

Figure 2. Example Mandatory Access Control Model

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.

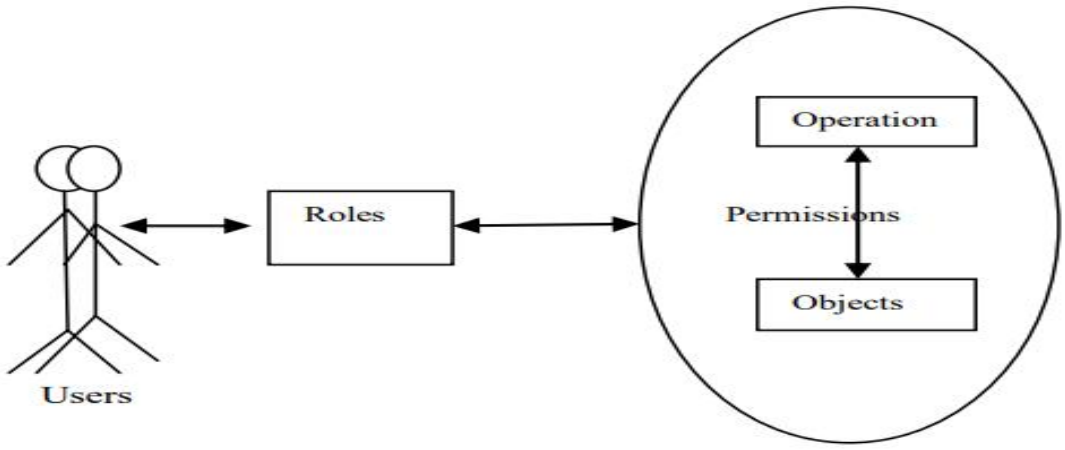

Figure 3: Role-Based Access Control

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-

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

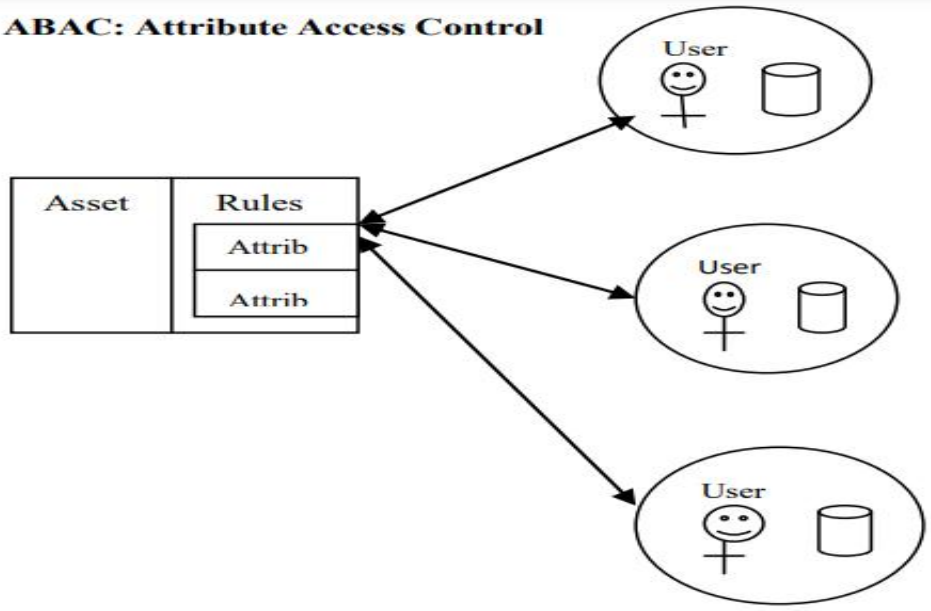

Figure 4: Attribute Based Access Control