A Review On Different Access Control Mechanism In Cloud Environment

B Sankaraiah
Asst. Professor
SVIT.

D. Bhadru
Ph.D Scholar
JJTU.

G Shravan Kumar
Asst. Professor
SVIT.

ABSTRACT:

These days in IT industry cloud computing are most popular paradigms and it provides various services to the customers with price as pay for use such services are Infrastructure as a service (IaaS), Platform as a service (PaaS), software as a service (SaaS) and Data base as service (DaaS) like so many services. And all these services providing needful facilities and various benefits to its customers, but there are still Many challenges existed with cloud services such as data confidentiality, malicious inside and outside attack and lack of access control policies, so among all the challenges access control is one of the major challenge why because in order to avoid un authorized access of data and to protect sensitive data of owner. Access control grants the permission to the users which gives the right to use rights on data and other resources. Access control can be allowed in mainly of the computing setting. So in this paper we present various types of access control mechanisms that are used in cloud computing environment. Some of the access control models are Mandatory Access control models (MAC), Role Based Access control (RBAC), Attribute Based Encryption model (ABE), Identity Based Encryption model (IBE).

Keywords: Control Policy, Encryption, data confidentiality, access control.

INTRODUCTION:

In cloud computing Access control is an essential feature of data security that is directly applied to the outsourced data and individuality such as confidentiality, integrity and availability. Cloud computing service providers must offer the following basic functionalities from the perception of access control: (i) Control access to the service features of the cloud based on the specified policies and the level of service purchased by the customer. (ii) Control access to a consumer's data from other consumers in multi-tenant environments. (iii) Control access to both regular user functions and privileged administrative functions. (iv)Maintain accurate access control policy and up to date user profile information. Access control models can be traditionally categorized into three types: (1) Discretionary (2) Mandatory and (3) Role-based. In the discretionary access control (DAC) model, the owner of the data will decides its access permissions for other users and sets them accordingly. The UNIX operating system is a classical example for discretionary access control model. For example, the subject (i.e., owner of an object) can specify what permissions (read/write/execute) members in the same group may have and also what permissions all others may have. DAC models are usually used only with legacy applications and will incur considerable management overhead in the modern multi-user and multi-application environment, characteristic of distributed systems such as cloud. The Mandatory access control (MAC) models abstract the need for resource-user mapping and hence are more adaptable for distributed systems, compared to DAC models. The MAC model is normally worn in multi-level protection systems. Here, the access permissions are determined by the administrator of the system, and not by the subject. In a multi-level MAC model, each subject as well as object is recognized with a defense level of categorization (e.g., Unclassified, Classified, Secret and Top Secret). In a Role-based access control model (RBAC), a user has access to an object based on his/her assigned role in the system. Roles are defined based on job functions. Permissions are defined on job authority and responsibilities of the job. Operations on the object are invoked based on the permissions. RBAC models are more scalable than the discretionary and mandatory access control models, and more suitable for use in cloud computing environments, especially when the users of the services cannot be tracked with a fixed identity.

Access control Methods:

(1) Discretionary Access Control:

Discretionary access control is one of the access control method in which owner has the complete control over his outsourced data in cloud storage. DAC is support on generous 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 decides set of 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 entity applies for to access an object that has been tartan. 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. DAC is supposed to be the method of "who can access what". In DAC the owner of and data can prefer to grant access permissions to other users.

(2) Mandatory Access Control

Mandatory access control (MAC) is based on the access of data to number of users. Mandatory access control is mostly based on the protection level. In this entity cannot change the access. Traditional MAC mechanism is mainly coupled with some security consideration. This follows the following two principles. 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). Using MAC data integrity will increase and it will give priority to low objects to high objects, this will achieve data integrity, MAC mostly will applied for government and military applications.

(3) Role Based Access control:

Role based access control access (RBAC) defined based on the individual's users roles and responsibilities within the cloud environment. RBAC map the user's access to the system based on the activities that the user has been executed in the cloud environment. 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 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.

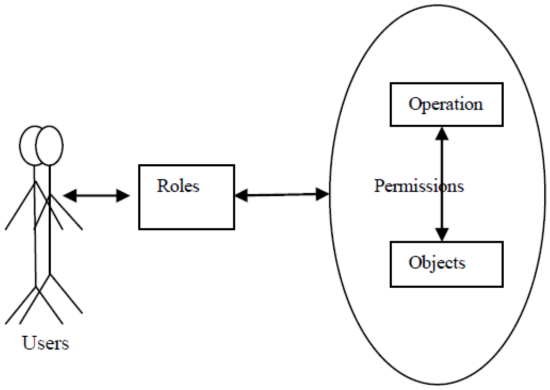

Fig: Role Base Access control

ATTRIBUTE-BASED ENCRYPTION (ABE) MODEL:

Attribute-based encryption (ABE) is best fit to protect the privacy and secrecy of data in a cloud. ABE is helpful when the resource of the facts recognize neither the identity of the recipient nor their public key but only knows certain attributes of the recipient. For example, imagine user Alice wishing to communicate with her former classmates, but she does not know their email addresses. ABE identifies a user with a set of attributes.

CONCLUSION:

Access control method in cloud is main study area which will augment the protection on user's data that are stored in cloud computing. Make sure 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 consequence of access control in cloud to make sure the security of user's information.

REFERECES:

[1] L. Popa, M. Yu, S. Y. Ko, S. Ratnasamy and I. Stoica, "CloudPolice: Taking Access Control out of the Network," Proceedings of the 9th ACM Workshop on Hot Topics in Networks, October 2010.

[2] S. Oh and S. Park, "Task-role-based Access Control Model," Information Systems, vol. 28, no. 6, pp. 533-562, September 2003.

[3] H. A. J. Narayanan and M. H. Gunes, "Ensuring Access Control in Cloud Provisioned Health Care Systems," Proceedings of the IEEE Consumer Communications and Networking Conference, 2011.

[4] S. Sanka, C. Hota and M. Rajarajan, "Secure Data Access in Cloud Computing," Proceedings of the 4th IEEE International Conference on Internet Multimedia Services, December 2010

[5] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proceedings of the 29th IEEE International Conference on Information Communication, pp. 534-542, 2010.

[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.