Evaluation of Access Control Techniques in Cloud Computing

Devyani Patil
Asst. Prof.
Arihant College of ACS
Camp, Pune-01

Nilesh Mahajan, PhD
Prof
Bharti Vidyapeeth's
IMED, Pune

ABSTRACT
Cloud Computing is an advanced evolving technology. It is a technology in which authorised user can store, retrieve and delete data from cloud computing environment. Mostly it is used for storage of data because now a day's storage of data in safe space is a critical problem. Data kept in cloud can be retrieved any time and at any place, if you are legitimate user and having internet access. Main benefit of use of this technology is you don't worry about the data storage capacity, equipment purchasing and access speed. Even with of this technology data sharing is very easy. According to use of this technology cloud computing is categorised into service models as SaaS, PassS and IaaS. As data security is depends on user authentication it is also depends on access control.

Keywords
Cloud Computing, Authentication, Data Storage and Access Control

1. INTRODUCTION
Cloud Computing is on growing technology in IT sector. This technology is mostly used for data storage, data updating and retrieving of data. Storing and use of data is very easy in this technique you just have to login with your authenticate account and then you will be in cloud environment. [1][5] According to use of cloud computing this technology is categorised into its service level models as shown in **Fig. a**:

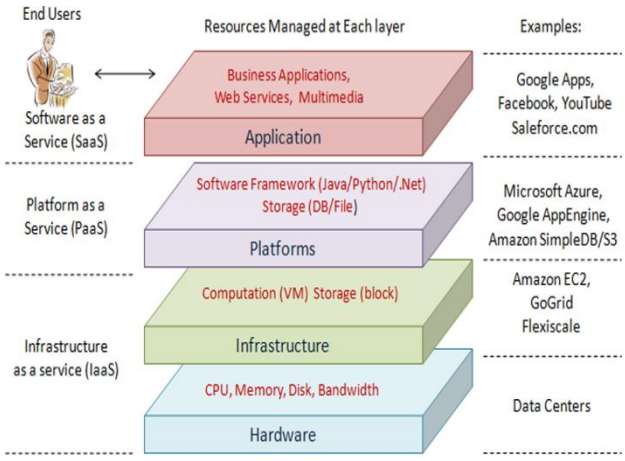

Fig. a: Categories of Cloud Computing according to service models.

As mentioned in above figure a SaaS is an end user application software service users are using only applications in this type. This is Pay-as –you –go model Applications used by end user are running on a particular cloud service provider. Many users can use these applications on multiple devices at same time by using their accounts.[2]

PaaS is next category in which user is using cloud platform. This category works as middle man between SaaS and IaaS. CEnd User cannot manage anything in this category as network, server or OS etc. PaaS providers offer predefined combinations of OS as WAMP, LAMP etc. This is done for security purpose.

IaaS is a platform virtualization. Ability of this category is providing storage, networks and other fundamental computing resources where the end user is capable to install and run software. Instead of purchasing servers, software, data centre and network equipment's this resource is fully outsourced and controlled by service provider. One important part of hardware is also covered in this category. This includes all type of hardware related to the whole cloud service infrastructure.[4]

As user is using whole infrastructure managed by third party then a big question of security is arises here. User authentication and access control are an important terms in cloud computing. Through this paper we will discuss some access control methods which are available nowadays. [3][5]

Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security. Some of these methods are: Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Discretionary Access Control (DAC), Fine-Grained Access Control (FGAC), Hierarchical Attribute-Based Access Control (HABE) and Attribute-Based Encryption Fine Grained Access Control (ABE FGAC).

Mandatory Access Control (MAC) raised when DAC is not efficient in terms of security. The fullness and confidentiality of the system are the most important features. Thus, it is high in security and low in flexibility. Because of high security and complete privacy it is used in government and military system [10]. While MAC performs operations, it does not consider the relationship it has with the users into consideration, user has to strictly follow all the permissions and roles assigned to him. MAC allows system administrative to perform operations according to the introduced policies [11]. Thus, it is much better in terms of logical comparisons when compared with DAC explained in Fig. b

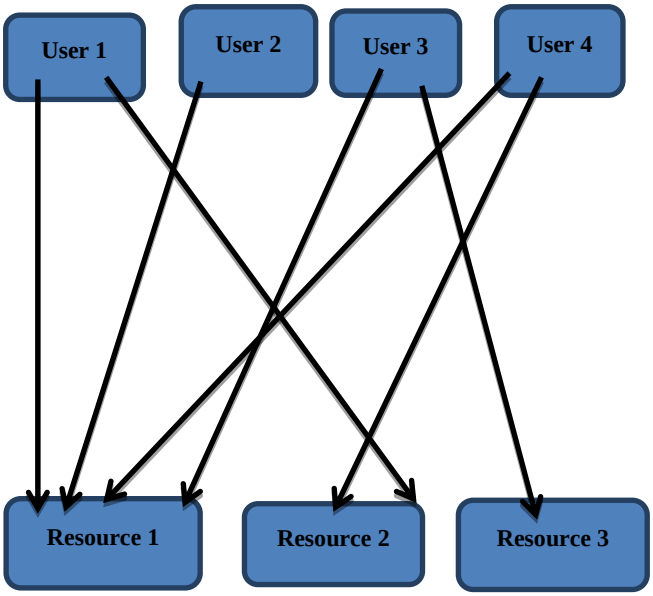

Fig. b: Mandatory Access Control (MAC)

2. ROLE-BASED ACCESS CONTROL (RBAC)

In this method users are allocated with different roles and the necessary permissions, limitations and authorizations are performed because of these roles [6]. Working structure of RBAC is as: one user is assigned with one or more than one roles. Two roles of different users can give permission to access one resource. Also at one time user can give permission to two different roles and to two different resources [6] [7]. Diagrammatical description of this is as shown in Fig. c

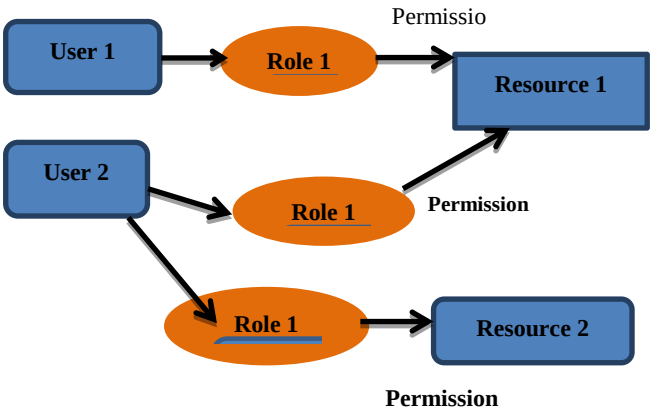

Fig. c: Role Based Access Control (RBAC)

Uncategorized Universe Private

3. ATTRIBUTE BASED ACCESS CONTROL

In the usage of Attribute-Based Access Control (ABAC), the user attributes play an important role. Attributes are like Name Age, Designation and Personal Information. These attributes can update according to change. These attributes can be categorise into many groups as Subject Attributes, Environment Attributes and Resource Attributes Aim of this grouping is to avoid complexity. Same as RBAC, ABAC demands the permissions and limitations to action when they are needed. Additionally, logical comparisons, and controls are important features. The set of user attributes will be conserved distinctly as shown in Figure d.

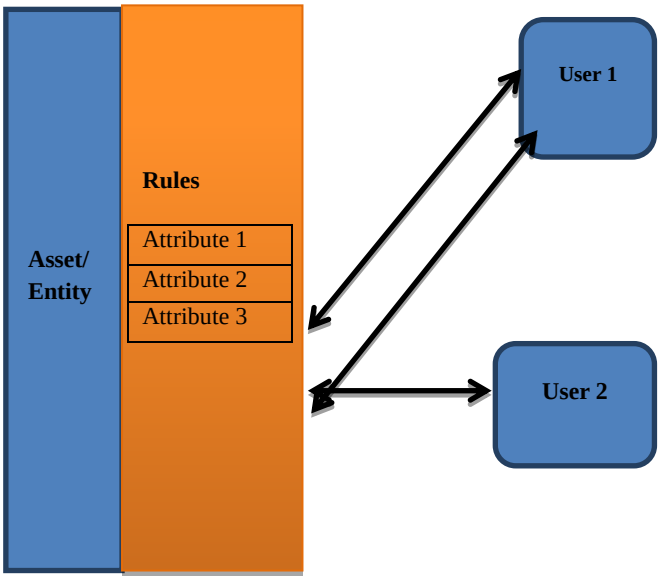

Fig. d: Attribute Based Access Control (ABAC)

For working of ABAC two models are developed: One is Policy model that defines the policies and Second model is the Architecture model that provides the web service access control. Attributes of these models are determined by the experts and they are dynamically altered constantly. Because of this change in access control become easier.[8] But this flexibility increases the occurrences of policy conflicts and makes the maintenance and administration of the policies difficult. After some time period because of this reason developers decided that ABA is not efficient. The reason behind this is access permissions given according to the attributes of the users became insufficient and unproductive. So ABAC is newly introduced as ARBAC with combination of ABAC and RBAC. Time period of this conversion was very less so no more experiments are available on ABAC.[9]

4. DISCRETIONARY ACCESS CONTROL

DAC is mostly used in area where computer security is very important. Access permission given to a particular user is called as Authenticate User or Owner. These users gives the necessary authorization to individuals in the system and limits their access to the system according to his own requirements. The most important feature of this method is the fact that it has a high level of security, it cannot distinguish between the subjects and object domains and has security leaks [13]. This access control is based on the user or group control so there are many chances of security leaks. Even in this type one owner can share his access with another user and if the another user is not trustworthy then a data security problem will arises. To avoid this you can create a group and assign permissions to only one parson so if anybody is misusing shared access that will be controlled by that one person only. You can call him access admin [14]. This type of access control is highly flexible. Detailed description of this method in diagram format is shown in Fig. e

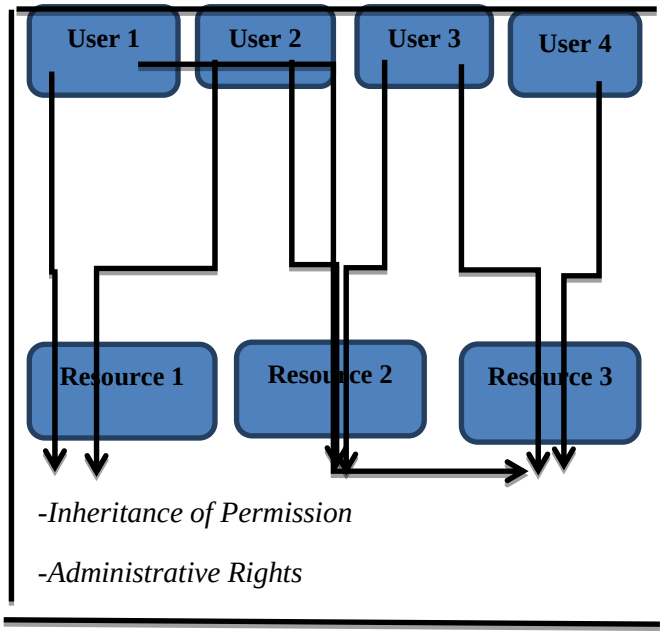

Fig. e: Discretionary Access Control (DAC)

5. HIERARCHICAL ATTRIBUTE BASED ACCESS CONTROL

Hierarchical Attribute Based Access Control (HABE) is operated in a hierarchical structure, and according to this structure, the system is made up of a root master (RM) and multi-layer domain masters that consist of the set of users, and users have the set of attributes as shown in Fig. f. This growing authenticates by allowing the admin to assign their function keys to other admins. HABE is the best control mechanism that provides the best scalability and flexibility. The most important feature of this access control is that it gives the information user, in a secure way, belongs to which class [15].

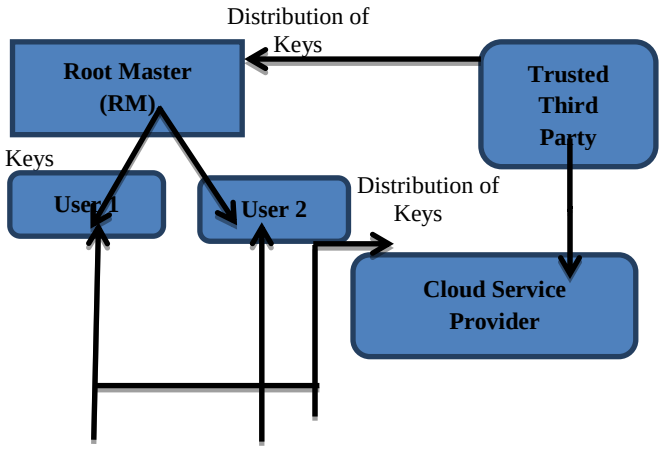

Fig. e: Hierarchical Attribute Based Access Control (HABAC)

6. FINE GRAINED ACCESS CONTROL

The advantage of this mechanism is it has the flexibility to determine the access rights and in which mode they can work for each user. In this type of access control user have the right to decide their policies as per their own requirements. In FGAC different hybrid models are used to reach the mechanism. Most important disadvantage of this system is it does not create problems in the systems that work on their own. FGAC has problems in identifying and distinguishing between the operations produced when cooperating with complex structures. Fig f shows structure of tis access control[12][15].

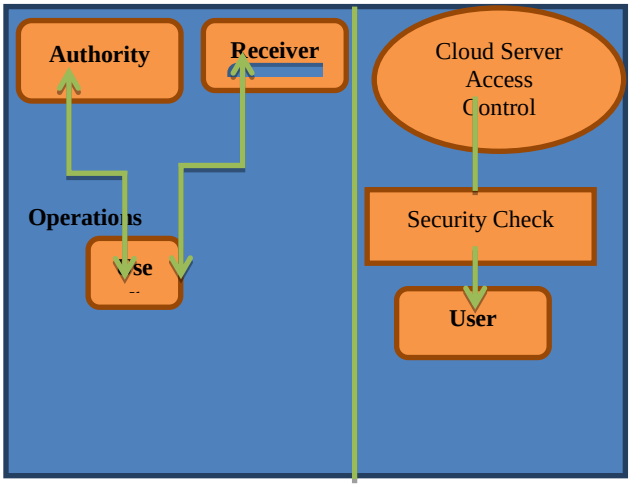

Fig f: Fine Grained Access Control (FGAC)

7. CONCLUSION

Security is one of the most important topics in Cloud Computing, and access control is a important part about user identification, Access permissions and use of proper roles and resources.

In this paper, we have discussed some access control techniques as RBAC, ABAC, DAC, MAC, FGAC and HABE with their characteristics. Some techniques like RBAC and DAC are having better advantages as compare to others , but we cannot neglect some important features of other techniques as FGAC and HABE which allow us to create hybrid model of access control. Access Control administrator also play very important role in this. According to situation and data security you can decide which access control Technique is useful for you. And according to situation you can use any one of theses or can make a hybrid combination of this.

8. REFERENCES

[1] https://en.wikipedia.org/wiki

[2] Y.G.Min, Y.H.Bang, "Cloud Computing Security Issues and Access Control Solutions", Journel of Security Engineering, vol.2, 2012.

[3] A.R.Khan, ARPN "Access Control in Cloud Computing Environment," Journal of Engineering and Applied Sciences, vol 7, no 5, MAY 2012.

[4] Almubaddel, M., and Elmogy, A. M. (2016). "Cloud computing antecedents, challenges, and directions".International Conference on Internet of things and Cloud Computing

[5] Ahmadi, M., Chizari, M., Eslami, M., Golkar, M. J., and Vali, M. (2015). "Access control and user authentication concerns in cloud computing environments." International Conference on Telematics and Future Generation Networks (TAFGEN)

[6] http://www.cio.com/topic/3024/Cloud_Computing

[7] Khan, M. F. F., and Sakamura, K. (2015). "Fine-grained access control to medical records in digital healthcare enterprises." International Symposium on, Networks, Computers and Communications (ISNCC), 2015

[8] Msahli, M., Chen, X., and Serhrouchni, A. (2014). "Towards a fine-grained access control for cloud." IEEE 11th International Conference on, e-Business Engineering (ICEBE), 2014

[9] Bhatt, S., Patwa, F., and Sandhu, R. (2016). "An attribute-based access control extension for openstack and its enforcement utilizing the policy machine." IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)

[10] Heitor Henrique de Paula Moraes Costa, Aletéia Patrícia Favacho de Araújo, JoaJosé Costa Gondim, Maristela Terto de Holanda, and Maria Emília Machado Telles Walter. "Attribute based access control in federated clouds: A case study in bioinformatics". 12th Iberian Conference on Information Systems and Technologies

[11] Wang, R., Azab, A. M., Enck, W., Li, N., Ning, P., Chen, X., and Cheng, Y. (2017). SPOKE: "Scalable Knowledge Collection and Attack Surface Analysis of Access Control Policy for Security Enhanced Android". In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security

[12] Lei, Z., Hongli, Z., Lihua, Y., and Xiajiong, S. (2011). "A mandatory access control model based on concept lattice." International Conference on Network Computing and Information Security (NCIS)

[13] Taubmann, B., Rakotondravony, N., and Reiser, H. P. (2016). "Cloudphylactor: Harnessing mandatory access control for virtual machine introspection in cloud data centers." Trustcom/BigDataSE/I SPA, IEEE

[14] Punithasurya, K., and Jeba Priya, S. (2012). "Analysis of different access control mechanism in cloud." International Journal of Applied Information Systems (IJAIS)

[15] Wang, G., Liu, Q., Wu, J., and Guo, M. (2011). "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers."computers & security