An Analysis on Access Control Mechanisms in Cloud Environment

Mrs. J. Persis Jessintha
Assistant Professor, Department of Computer Science
Bishop Heber College
Trichy
India

Dr. R. Anbuselvi
Assistant Professor, Department of Computer Science
Bishop Heber College
Trichy
India

***Abstract*-Cloud Computing is an evolutionary outgrowth of prior computing approaches, which builds upon existing and new technologies where resources are available pay as you go basis. The storage capacity in cloud technology provides a large pool of storage to the users. Securing the data thus stored is the major concern. As the sensitive data are moved into the cloud data centers, it is often outsourced to be stored at the cloud service providers (CSP) and the data may be exposed to unauthorized parties. This paradigm brings forth many new challenges for securing data and access control while outsourcing sensitive data in cloud. So security can be enhanced by providing access control to the authorized user. As far as cloud security is concern, the access control policies play the major role in securing data from unauthorized user. This paper deals with various access control mechanisms in cloud computing. And a detailed analysis for the same is given.**

Keywords: Discretionary Access Control, Mandatory Access Control, Role Based Access Control, Attribute Based Access Control, distributed RBAC, Cloud Optimized RBAC.

I INTRODUCTION

Recently cloud has become one of the hot topics in IT environment. This model of computing has made a tremendous change in the computing field. The three main service models of cloud computing are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).Also, Cloud Computing has four deployment models:Private Cloud, Public Cloud and, Community Cloud and Hybrid Cloud[1].

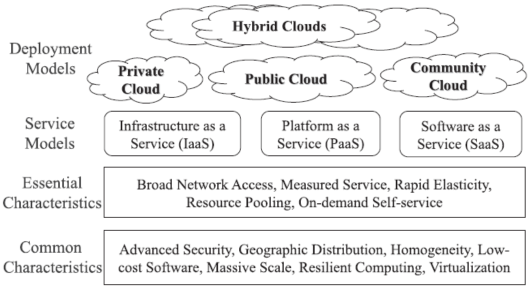
Hybrid Clouds
Deployment Models
Private Cloud
Public Cloud
Community Cloud
Service Models
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Essential Characteristics
Broad Network Access, Measured Service, Rapid Elasticity, Resource Pooling, On-demand Self-service
Common Characteristics
Advanced Security, Geographic Distribution, Homogeneity, Low-cost Software, Massive Scale, Resilient Computing, Virtualization

Figure.1: NIST framework for cloud Computing

One of the important factors that the business organizations adopt in cloud is that it offers service on demand basis. Cloud storage is one of the services that cloud offers. Cloud provides a large pool of data storage. As the sensitive data are moved to the cloud storage, the owner of the data is unaware of where the data actually resides. This may be the vulnerable point that the data may be exposed to some unauthorized parties. This brings forth many new challenges for securing data in cloud. The user can access the data through web enabled devices. Providing access control to the data through web is the major concern in data security. Many traditional access control mechanisms have been followed to secure data. The purpose of introducing access control mechanisms is used to identify the authorized user. The access control is very important in data accessing in cloud environment [1]. Providing access control alone to the authorized user is not only the solution, it is also very important to encrypt the stored data. The most commonly used access control methods are based on user identity.

The various types of access control mechanisms are discussed in the section II.

II VARIOUS ACCESS CONTROL METHODS

A. Discretionary Access Control (DAC)

This method is a traditional method in which the user has the complete control over the system. In a system, every object has an owner. With DAC, access control is determined by the owner of the object who decides who will have access and what privileges they will have. In DAC, the access control flexibility is good where as the Permission Management in DAC is very difficult to maintain; furthermore, DAC does not scale well beyond small sets of users [2].

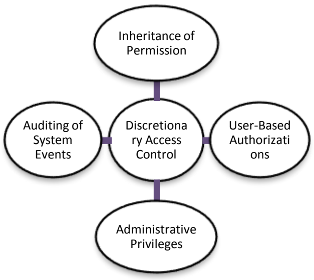
Inheritance of Permission
Auditing of System Events
Discretionary Access Control
User-Based Authorizations
Administrative Privileges

Figure.2:DAC

In DAC, each system object (file or data object) has an owner, and each initial object owner is the subject that causes its creation. Thus, an object's access policy is determined by its owner. A typical example of DAC is UNIX file mode.

DAC attributes include:

- User may transfer object ownership to another user(s).
- User may determine the access type of other users.
- After several attempts, authorization failures restrict user access.
- Unauthorized users are blind to object characteristics, such as file size, file name and directory path.
- Object access is determined during access control list (ACL) Authorization and it is based on user identification and/or group membership.

DAC is easy to implement and intuitive but has certain disadvantages, including:

- Inherent vulnerabilities (Trojan horse)
- ACL maintenance or capability
- Grant and revoke permissions maintenance
- Limited negative authorization power

B. Mandatory Access Control (MAC)

Mandatory access control (MAC) is a security strategy that restricts the ability individual resource owners have to grant or deny access to resource objects in a file system. MAC criteria are defined by the system administrator, strictly enforced by the operating system or security kernal, and are unable to be altered by end users[2].

In government and military facilities, mandatory access control works by assigning a classification label to each file system object. Classifications include confidential, secret and top secret. Each user and device on the system is assigned a similar classification and clearance level. When a user or device tries to access a specific resource, the OS or security kernel will check the entity's credentials to determine whether access will be granted. While it is the most secure access control setting available, MAC requires careful planning and continuous monitoring to keep all resource objects' and users' classifications up to date.

As the highest level of access control, MAC can be contrasted with lower-level discretionary access control (DAC), which allows individual resource owners to make their own policies and assign security controls.

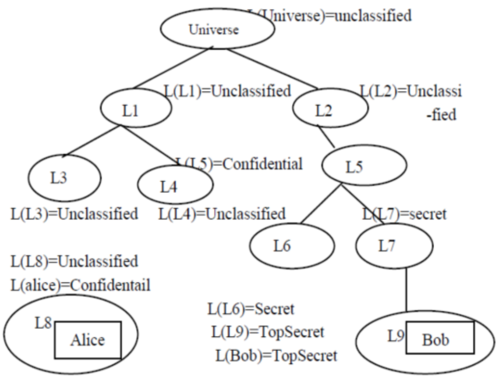

Figure.3: MAC

The information about location is sensitive in nature. The location information of a user or an object should not be disclosed in an uncontrolled way due to privacy and security. For instance, the information about the location of weapons should not be disclosed to everyone. Alternately, if several top secret clearance users are in a top secret location and this information is revealed then this may cause a security breach.

Advantages of MAC:

- MAC is mainly used in military and intelligence agencies.
- It is straight forward and good for commercial systems.
- Scalability is very low and never supports all types of applications.

Disadvantages of MAC:

- Once the security level is fixed for an object it won't be modified.

C. Role Based Access Control (RBAC)

Access policy is determined by the system. MAC access is based on subject trust or clearance, with RBAC access is based on the role of the subject. A subject can access an object or execute a function only if their set of permissions—or role—allows it. In this access mechanism, the access decisions are based on the role of the user. So every user has to take an assigned role [3].

Access rights are grouped by the role name and the use of the resources are restricted to that particular authorized user. The role of the user is based on the competencies and the responsibilities.

The NIST RBAC Model uses a limited set of concepts to define an RBAC system as depicted in Figure 4.

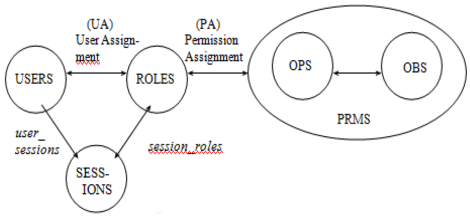

Figure.4:RBAC

The RBAC model contains 6 main entities:

user: contains all the user data

session: contains the session data for all currently logged on users

role: contains all the roles that are defined

permissions: contains all the permissions based on objects and operations

object: objects are the items that require protection

operation: operations are the actions that are performed on the objects

Advantages of RBAC:

- It is used to manage large number of users securely.

- It is mainly used in financial institutions and insurance companies.
- It is Centralized, Hierarchical, Cooperative, Ownership and Decentralized.

Disadvantages of RBAC:

- Sometimes it is difficult to find to whom the privilege is to be given.
- The change of role sometimes creates ambiguity.

III CLOUD RELATED ACCESS CONTROL TECHNOLOGIES

There are some access control mechanisms mainly used in cloud computing environment, they are ABAC, dRBAC, coRBAC.

A. ABAC (Attribute Based Access Control)

ABAC considers identification, authentication, authorization and accountability. User identity is the major element in providing access control to the user and this type is called as Identity Based Access Control (IBAC). But it is not suitable for large distributed system [4].

ABAC is based on the set of user attribute and this solves the problem in assigning privilege, which is the major problem in RBAC.ABAC is more secure, scalable and flexible. The set of user attributes are maintained individually.

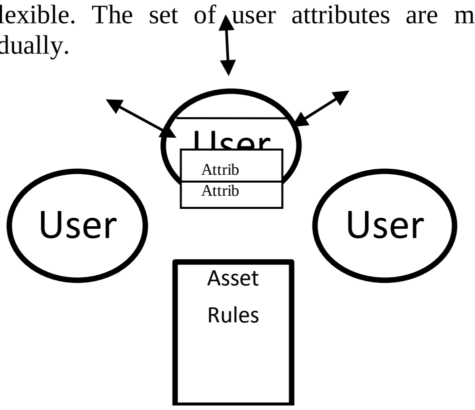

Figure.5:ABAC

B. dRBAC(distributed RBAC)

dRBAC supports large distributed systems. dRBAC solves the problem occurs while giving access control in multiple organization .dRBAC has some problem like high time complexity and high space complexity. Also the sequential accessing of the cloud resources cause redundancy and inconsistency.

C. coRBAC(Cloud Optimized RBAC)

RBAC supports the management of data across a large scale, so the security is high but roles cannot be maintained properly. Therefore, RBAC does not support web so user mobility is low.

coRBAC acquires the functionality of both dRBAC and RBAC to improve the certification process. Here, the time complexity and space complexity are also reduced. The time taken for authentication and login is considerably reduced comparing to RBAC. This method improves the overall efficiency.

There are some disadvantages also, user has to get access certificate from the third party instead of getting it from the server administrator. It is not easy to change the certificate according to the users' wish, if an attempt is made so, it leads to unnecessary cost and confusion.

IV LITERATURE SURVEY

Role Based Access Control is elaborately discussed in paper [3]. In [5], attribute based access control mechanism is used to ensure organizational security policies. Here the author talks about the importance of Provenance of the data, which plays a vital part in finding the authorized user.[8] explored on data protection, here it is stated that to ensure data protection, encryption alone is not sufficient. Role-based access control framework combined with trust degree in multi-domain is given. Access control in local domain directly applies RBAC model combined with trust degree. Multi-domain contains the conception of role translation. Papers, [8][10] explored the Trust based access control mechanism to ensure user authorization. In [11], the problem stated is that giving access rights to an authorized person is a difficult task. This paper focused on semantic interoperability for integration of various information systems. Semantic Access Control (SAC) is used and it is extended with RBAC (Role Based Access Control).A Contextual role-based access control authorization model aiming to increase the patient privacy and the confidentiality. Paper [14], proposed an authorization re-cycling approach along with role based access control mechanism in order to improve giving rights to authorized person. In [15], the Data security is focused and provides an access control technique which is based on user privileges and also introduces a new type of key called "Group Key" for encryption purpose. Kalaichelvi et al. [18] presented a framework of User Access control in Cloud Computing and the proposed framework is based on role based access control mechanism. In [19], the access control mechanisms are based on username, user IP. The main disadvantage of following the above system alone is that the provider does not know to whom the access should be restricted. A negative authorization should be followed to reduce the data theft by some fake users.

V DISCUSSION AND ANALYSIS

Attribute based access control mechanism is well suited for provenance based access control mechanism with little change in it. While talking about Trust based access control mechanism, the traditional role based access control mechanism is well suited. Moreover, a negative authorization should be taken in to account to find the unauthorized user to whom the service must be avoided.

Issues and Challenges:

- ➢ Encrypting data at rest, data at transit and data in process may cause the key management more difficult.
- ➢ Fixing threshold for Trust, based on user behavior alone is not sufficient because behavior trust is dynamic.
- ➢ Maintenance of database for data provenance in cloud in very cumbersome.

VI CONCLUSION

Providing access control to an authorized user to access cloud based data is the major problem. The main aim of this work is to understand various access control mechanisms. In this paper, a brief description about various access control mechanisms was discussed and an analysis of the same is given. The advantages and disadvantages of the traditional and related access control technologies were also discussed. This analysis ensures the need of security, the authentication of user and also the importance of access control. Though many changes were made on the traditional access control mechanism to improve the security standard, still there is a big room of research in that area.

REFERENCES

[1]Mauro Jose A.de Melo,Zair Abdelouahab,"A Study of Access Control in Cloud Computing Environment", International Journal of Computers & Technology,Dec 2012.

[2] Dipmala Salunke, Anilkumar Upadhyay1, Amol Sarwade, Vaibhav Marde, Sachin Kandekar ,"A survey paper on Role Based Access Control", International Journal of Advanced Research in Computer and Communication Engineering, March 2013.

[3].Zhuo Tang et al. "A new RBAC based access control model for cloud computing" GPC'12 Proceedings of the 7th international conference on Advances in Grid and Pervasive Computing, Springer-Verlag Berlin, Heidelberg, 2012. [4].Chandana.V.R' Radhika Govankop'Rashmi N and R.Bharathi,"GASBE: A Graded Attribute-Based Solution for Access Control in Cloud Computing", International Conference on Advances in Computer and Electrical Engineering,November 2012.

[5].Adam Bates, Ben Mood,Masoud Valafar and Kevin Butler, "Towards Secure Provenance-Based Access Control in Cloud Environments", CODASPY'13, Feb 2013.

[6].Chia-Hui Liu,Tzer-Long chen,Han-Yu Lin,Fong-Qi Lin,Chih-Ming Liu,En-Ping Wu,Yu-Fang Chung and Tzer-Shyong Chen, "Secure PHR Access Control Scheme in Cloud Computing", May 2013.

[7].Daniel Ricardo dos Santos, Carla Merkle Westphall,Carlos Bcker Westphall, "Risk-based Dynamic Control for a Highly Scalable cloud Federation", 7th International Conference on Emerging Security Information, Systems and Technologies,2013.

[8].Guoyuan Lin, Yuyu Bie, Min Lei, "Trust Based Access Control Policy in Multi-Domain of Cloud Computing", Journal of Computers, May 2013.

[9].Ming Li,Shucheng Yu,Yao Zheng,Kui Ren,Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in cloud Computing Using Attribute-Based Encryption", IEEE Transactions on Parallel and Distributed Systems, January 2013.

[10].Mustapha Ben Saidi, Anas Abou Elkalam, Abderrahim Marzouk,"TOrBAC:A Trust Organization Based Access Control Model for Cloud Computing Systems",International Journal of Soft Computing and Engineering,September 2012.

[11].Nithyasri .G and Ramya .G, "E-Health System using International Journal of Information and Electronics Engineering, g SAC in Cloud Computing", International Journal of Research in Engineering & Advanced Technology,March 2013.

[12].B. Raj Kumar, S. Satyanarayana, "Secure Sharing of Personal Health Records in Cloud Computing", International Journal of Science and Research, March 2013.

[13].M V Rajesh, Soma Sekhar T and Siva Rama Krishna T," Enhanced Secure Data Access Model for Public Clouds", International Journal for Research in Science & Advanced Technologies, August 2012.

[14].Reeja S L,"Role Based Access Control Mechanism in Cloud computing Using Co-operative secondary Authorization Recycling Method", International Journal of Emerging Technology and Advanced Engineering, October 2012.

[15].Sonam Chugh,Sateesh Kumar Peggoju," Access Control Based Data Security in Cloud Computing", International Journal of Engineering Research and Applications,June2012.

[16].Sultan Ullah, Zheng Xuefeng and Zhou Feng," TCLOUD: A Multi – Factor Access Control Framework for Cloud Computing **",** International Journal of Security and Its Applications Vol. 7, No. 2, March, 2013.

[17].Tien Tuan Anh Dinh and Anwitaman Datta, "Streamforce: Outsourcing Access Control Enforcement for Stream Data to the Clouds",May 2013.

[18].R.Kalaichelvi and Dr.L.Arockiam, "Enhanced User Access Control Architecture for Cloud Storage", International Journal of Advanced Research in Computer Science and Software Engineering, March, 2014.

[19].Xiaohui Li, Jingsha he, Ting Zhang, "Negative Authorization in Access Control for Cloud Computing", International Journal of security and its Applications, April 2012.

[20].S. Ullah,Z. Xuefeng and Z. Feng,"TCloud: Challenges and Best Practices for cloud Computing",International Journal of Engineering Research and Technology,2012.