Enhancing Cloud Security through Access Control Models: A Survey

Chirag Langaliya
Research Scholar,
Department of C.E
School of Engineering,
R.K. University, Rajkot.

Rajanikanth Aluvalu
Associate Professor,
Department of C.E
School of Engineering,
R.K. University, Rajkot.

ABSTRACT

Cloud computing is a new computing paradigm in which an application can run on connected Cloud Server instead of local server. Cloud computing provides efficient data storage, resource sharing and services in a distributed manner with great ease. However Cloud computing is having issues like security and privacy of data when sensitive data is stored under third party cloud service providers. Various access control models have been proposed to resolve the security issue in cloud computing. So in this paper we have discussed various access control models starting from the traditionally DAC (Discretionary Access Control), MAC (Mandatory Access Control), RBAC (Role Based Access Control) and ABAC (Attribute Based Access Control) to the latest ABE (Attribute Based Encryption) models like CP-ABE (Ciphertext Policy - Attribute Based Encryption), KP-ABE (Key Policy Attribute Based Encryption), HABE (Hierarchical Attribute Based Encryption) and HASBE (Hierarchical Attribute - Set Base Encryption).

Keywords

ABE based Access control models, Cloud computing, HASBE, Traditional Access Control Models

1. INTRODUCTION

Cloud computing is a new computing model that provides services and access to resources stored on distributed service – oriented architecture called Cloud. The cloud service providers manage a cloud to offer data storage service and resource access. Data owners encrypt their files and store them on the cloud, and that encrypted files can be shared with the data consumer. Data customers download encrypted data files of their interest from the cloud and then decrypt them**.** So basically Cloud provides a platform to store, retrieve, and utilize multiple users' data. Benefits of using cloud computing involve reduced cost, easy and better operational facility, efficient database use and immediate response time. Though cloud is having multiple advantages, security in cloud is still a major area of concern, as Data owner and Data consumer are not on same trusted domain [12]. Data confidentiality is not the only security requirement, Flexible, scalable and fine-grained access control are also the characteristics that we need to have on our Cloud. Various access control models have been proposed for cloud computing, but most of them can't offer characteristics like flexibility, scalability and fine-grained access control efficiently.

The second section includes survey of various access control models with their advantages and disadvantages as well as comparison table of traditional access control models and ABE based access control models. The third section includes the conclusion of the review paper.

2. ACCESS CONTROL MODELS

As cloud computing provides on-demand access to resources and services, we need to have proper security arrangement in terms of authentication and authorization. Access control model does exactly the same work to monitor, control and limit the access to cloud users on the set of resources and services [1]. Access control increases security of a system and gives predefined access to the resource. Access control is a policy or procedure that allows, denies or restricts access to a system [2].Access control in cloud depends on the cloud storage and its data security and the access option becomes very necessary option in cloud. Access control is very important part in the data center of government and business.

DAC (Discretionary Access Control), MAC (Mandatory Access Control), RBAC (Role Based Access Control), and Attribute Based Access Control (ABAC) are traditional access control while Attribute Based encryption (ABE) schemes are advance access control models which introduces the concept of encryption. Access control mechanisms are used to restrict particular user based on the access privileges given by the system [3]. All these mechanisms are discussed below.

2.1 Discretionary Access Control (DAC)

DAC is the traditional access control mechanism in which user is given complete control over all the programs or resources. DAC allows access on the base of user identity and authorization which is defined for open policies. DAC is the mechanism which manages who can access what. In DAC owner of the resource grants the access permission to the end user. DAC mainly deals with Inheritance of permissions, User Based Authorization, Auditing of system Events and Administrative privileges [3].

Advantage of DAC: flexibility in usage by maintaining the authorization database which consists number of authorized user.

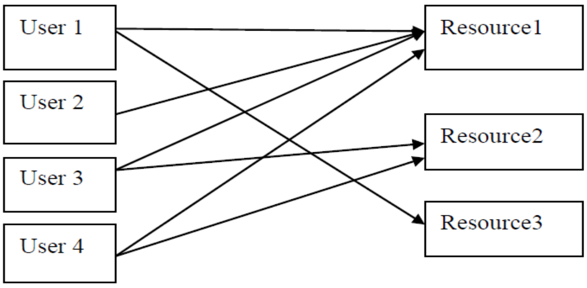

Figure 1. Discretionary Access Control [11]

Disadvantage of DAC: it can be easily attacked by third parties and there might be the chance to steal the copy of original message without owner's permission.

2.2 Mandatory Access Control (MAC)

MAC is mainly concerned with confidentiality of information. MAC is centrally controlled by a security policy administrator; users do not have the ability to override the policy [4].MAC policy takes decision based on network configuration. Each object present in cloud environment assigned some security level, which helps to identify the current access state of the object. MAC structure is as shown in the figure 2[11].

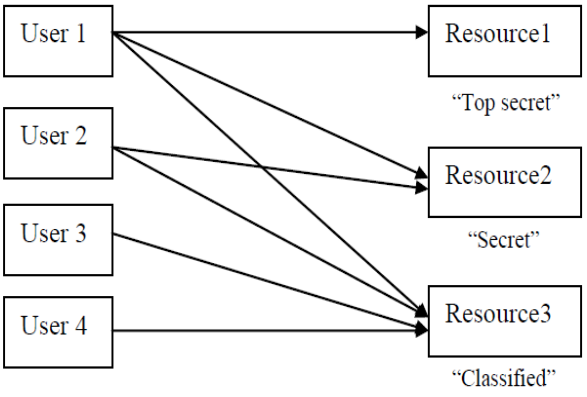

Figure 2. Mandatory Access Control [11]

Advantages of MAC: in MAC information integrity will increase and it prevents the flow from low objects to high objects. It is mainly used in military and government applications.

Disadvantage of MAC: once the security level is identified to particular subject in the hierarchy it will not modify the security level.

2.3 Role based Access Control (RBAC)

In RBAC access decisions are based on the individual's roles and responsibilities within the cloud environment. It identifies the user role and based on this it manages the access of a user. Role is a set of objects or policies related to the subject. Role may vary from user to user. RBAC provided web based application security. It allows users to execute multiple roles at the same time. RBAC decides what permission should be assigned to which user [3]. Working model of RBAC scheme is shown in the Figure 3 [11].

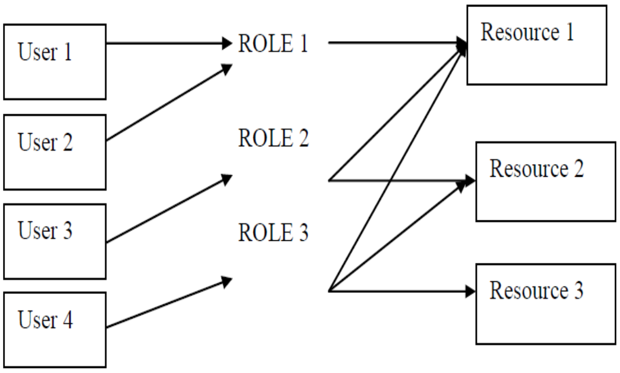

Figure 3. Role Based Access Control [3]

Advantages of RBAC: it minimizes the damage of information by intruders. It provides classification of user based on their roles.

Disadvantage of RBAC: permissions associated with each role can be deleted or changed based on the privilege of role change.

2.4 Attribute based Access Control (ABAC)

ABAC works with identification, authentication, authorization and accountability. RBAC had a problem of assigning privileges to the user, which is solved by ABAC. It considers attributes of user request. In attribute based access control the attributes are considered based on the user's request and the type of access user wish to access and the needed resources of user. ABAC is more secure and flexible and scalable and it provides hierarchical structure. Set of user attributes will be maintained individually as shown in the Figure 4 [3].

Advantages of ABAC: Since ABAC has interference of attributes it provides better security than other access control models. ABAC is more secure and flexible and scalable and it provides hierarchical structure.

Disadvantages of ABAC: ABAC doesn't offer the user role assignment concept.

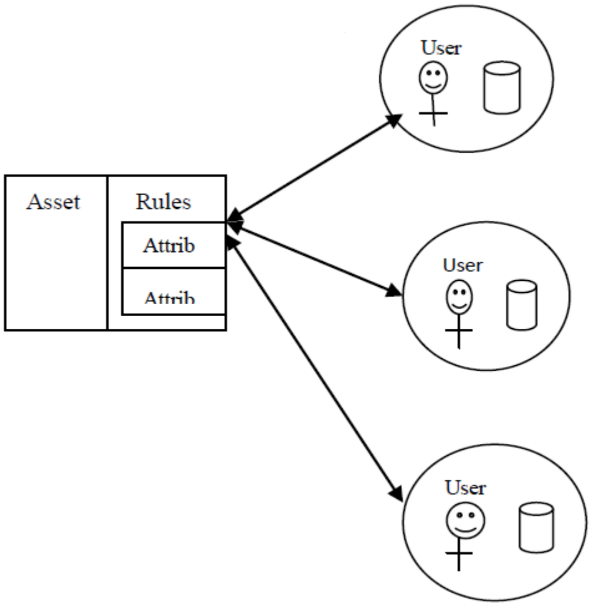

Figure 4. Attribute Based Access Control [3]

2.5 Attribute based Encryption (ABE)

ABE model was proposed by Sahai and Waters[5] in 2005. ABE allows users to encrypt and decrypt data based on user attributes. The secretkey of a user and the ciphertext are dependent upon attributes. The decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. ABE enforces access control through public key cryptography. The main goal for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, and this can be achieved only when user and server are in a trusted domain [12]. Another problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. So various ABE based access control schemes have been proposed to overcome this problem.

2.5.1 Key Policy Attribute based Encryption (KP-ABE):

KP-ABE was proposed by Goyal et al.[6] in 2006 which is the modified form of classical model of ABE. In KP-ABE ciphertext is associated with a set of attributes and user's decryption key is associated with a monotonic tree access structure. Only if the attributes associated with the cipher texts satisfy the tree access structure, can the user decrypt the cipher texts.

Advantages of KP-ABE: The KP-ABE scheme can achieve fine-grained access control and more flexibility to control users than ABE scheme.

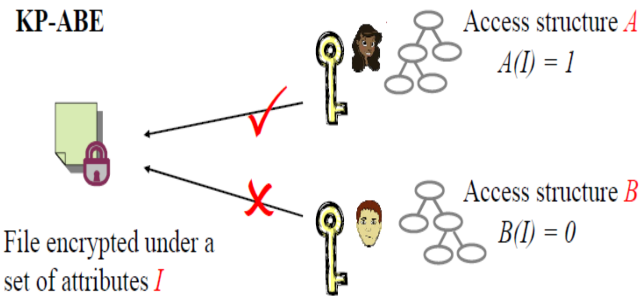

Figure 5: Key Policy Attribute Based Encryption

Disadvantages of KP-ABE: The problem with KP-ABE scheme is the encryptor cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data, it is unsuitable in some application because a data owner has to trust the key issuer.

2.5.2 Ciphertext Policy Attribute based Encryption (CP-ABE)

CP-ABE is another modified form of ABE called introduced by Sahai[7]. CP-ABE is used to encrypt the data which can be kept confidential even if the storage server is untrusted. A random number of attributes expressed as strings a primary key is associated. On the other hand, when a data owner encrypts a message he/she specify an associated access structure over attributes. If the data consumer's attributes pass through the ciphertext's access structure then only user can be able to decrypt a ciphertext. Access structures in this system are described by a monotonic access tree structure.

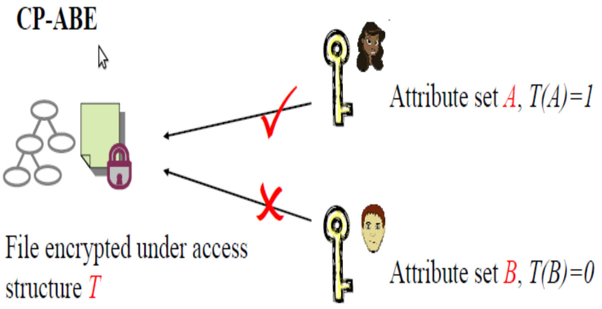

Figure 6: Ciphertext Policy Attribute Based Encryption

Advantages of CP-ABE: It overcome the problem of KP-ABE of choosing who can decrypt the data. In CP-ABE user's private key is a combination of a set of attributes, so an user only use this set of attributes to satisfy the access structure in the encrypted data.

Disadvantages of CP-ABE: CP-ABE still not fulfilling the enterprise requirements of access control which require considerable flexibility and efficiency. CP-ABE has limitations in terms of specifying policies and managing user attributes. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set.

2.5.3 Hierarchical Attribute based Encryption (HABE):

The HABE model was derived by Wang et al [8]. HABE model has the hierarchical structure consisting of root master at the top, followed by multiple domain masters which consists of set of users and users have the set of attributes as shown in the Figure 7 [3].

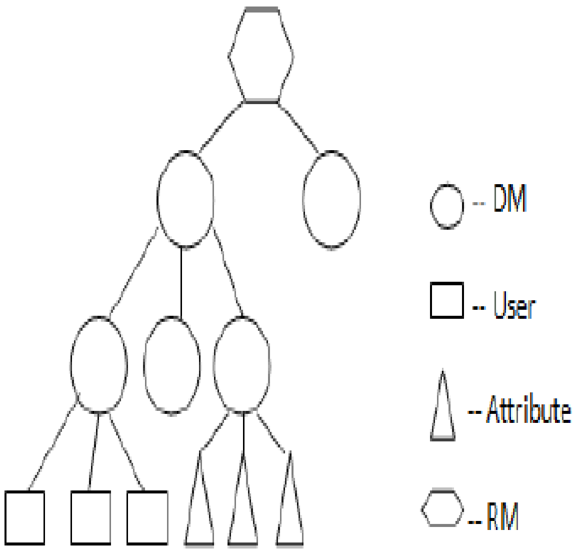

Figure 7: Hierarchical Attribute Based Encryption [3]

Advantages of HABE: This scheme can satisfy the property of fine grained access control, scalability and full delegation. It can apply to achieve proxy re-encryption [8].

Disadvantages of HABE: In practice, it is unsuitable to implement HABE, since all attributes may be administered by the same domain authority, the same attribute may be administered by multiple domain authorities.

2.5.4 Hierarchical Attribute-Set based Encryption (HASBE):

HASBE is extended from ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. In HASBE each data owner/consumer is managed by a domain authority. A domain authority is directed by its parent domain authority or trusted authority. Data owners, Domain authorities, Data consumers, and the trusted authority are prearranged in a hierarchical structure as shown in the fig. 8[9].

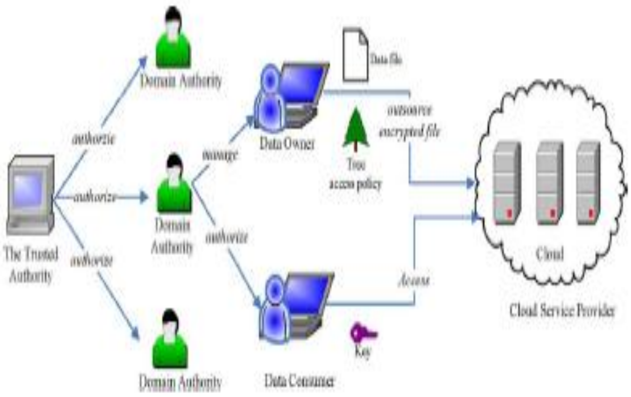

Figure 8: Hierarchical Attribute-Set Based Encryption [9]

HASBE uses Bilinear Mapping system for encryption and decryption. Data encryptor specifies an access structure for a ciphertext policy. Only users with decryption keys whose attributes are linked with the specified key structures and fulfill the access structure can decrypt the ciphertext [9]. The Figure 9 [13] shows the working architecture of the bilinear mapping technique.

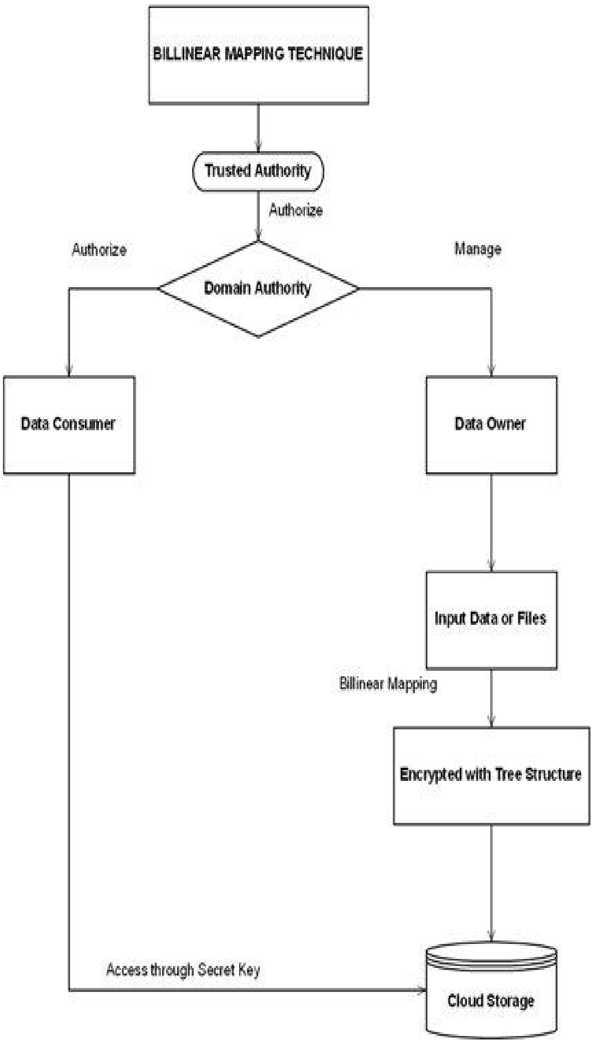

Figure 9: Bilinear Mapping [13]

HASBE works on recursive set based key structure [10] where all elements of the attribute set is a set or an element of an attribute corresponding to it.

Advantages of HASBE: hierarchical structure of system users, to achieve scalable, flexible and fine-grained access control. It achieves efficient user revocation.

Disadvantages of HASBE: It supports compound attributes, but as there are multiple domain masters and each of these domain masters have list of attributes and each attribute is administrated by each domain masters. HASBE scheme can be extended to sustain any depth of the key structure and system can be improved by putting the attributes that has same attribute set with multiple values.

Analysis: - In Table 1 and Table 2, I have analyzed traditional access control models like DAC, MAC, RBAC and ABAC as well as ABE based access control models like CP-ABE, KP-ABE, HABE and HASBE consequently in terms of security measure and characteristics of access control mechanism.

Table 1: comparison of various traditional access control models

Access Control	**DAC**	**MAC**	**RBAC**	**ABAC**
User’s Convenience	High	varies	High	High
Performance	Low	Based on security level	High	High
Reusability	Multi	Not mentioned	Multi	Multi
Role Assignment	Not Mentioned	Single Node assignment	Multi	Not mentioned
Single Point Failure	Authorization failure	less	Less	-
Node overhead	Less	Less	Less	varies
Authentication failure	Less	Depends on distributed environment	Based on job role assigned	less

Table 2: comparison of various ABE based access control models

Parameters	ABE	KP-ABE	CP-ABE	HABE	HASBE
Fine grained access control	Low	Low, High if there is re-encryption technique	Average realization of complex access control	Good access control	Good

Efficient	Average	Average, High for broadcast type system	Average, not efficient for modern enterprise environment	Flexible	Flexible but Not Enough
Computati-nal overhead	High	Most of computational overhead	Average computational overhead	Some of overhead	Compound Attribute Problem
Collision resistant	Average	Good	Good	Good	Good

3. CONCLUSION

In this paper, we have analyzed different access control models like DAC, MAC, RBAC, ABAC, ABE, KP-ABE, CP-ABE, HABE, and HASBE with their characteristics, advantages and disadvantages. CP-ABE and KP-ABE are the basic access control models from which multiple access control models can be derived and implemented. HASBE is extended from ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. HASBE scheme supports compound attributes. But as there are multiple domain masters and each of these domain masters have list of attributes and each attribute is administrated by each domain masters. That's why HASBE suffers from the problem of efficient compound attribute issue. So in our proposed system HASBE scheme can be extended to sustain any depth of the key structure and system can be improved by putting the attributes that has same attribute set with multiple values as a single attribute set.

4. REFERENCES

[1] Mavridis Ioannis "Towards new access control models for cloud computing systems"

[2] Rajanikanth aluvalu, lakshmi Muddana "A Survey on Access Control Models in Cloud Computing" Springer International Publishing, Advances in Intelligent Systems and Computing 337, DOI: 10.1007/978-3-319-13728-5_7.

[3] Punithasurya K, Jeba Priya S "Analysis of Different Access Control Mechanism in Cloud", International journal of Applied Information Systems, Vol. 4, September 2012

[4] Parmindar Singh, Sarpreet Singh "Cross Bread Role based Acces Control for Exteded Security at Azure in Cloud Computing" Internatonal Journal of Application or Innovation in Engineering and Management, Vol, 2, February 2013

[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption," inProc.EUROCRYPT, 2005, pp. 457473

[6] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

[7] J. Bette ncourt, A. Sahai, and B.Waters"Ciphertext-policy attribute based encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.

[8] Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences .In Press, 2012.

[9] Zhiguo Wan, Jun'e Liu, and Robert H. Deng "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012

[10] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.

[11] Sanjay Tiwari, Khushbu Sharma **"**Review on Cloud Computing Security Measure – Role-Based Access Control**"** International Journal of Advanced Research in Computer Science and Software Engineering

[12] N.krishna, L.Bhavani **"**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 3 Issue 9 – Oct 2013

[13] John Bethencourt, Computer Sciences Department Carnegie Mellon University," Intro to Bilinear Maps"