AUDITING SERVICE AND REVOCABLE-ROLE BASED ACCESS CONTROL

Manendra Sai Dasari
Research Scholar
MUIT University
Lucknow

Dr. B.D.K.Patro
Professor
MUIT University
Lucknow

ABSTRACT

Cloud storage is an important service of cloud computing, which offers services for data owners to host their data in the cloud. This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Cipher text-Policy Attribute-based Encryption (CP-ABE), is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution. The authority can be the registration office in a university, the human resource department in a company, etc. The data owner defines the access policies and encrypts data according to the policies. Each user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes satisfy the access policies. The major part of this paper is Revocable Role Based Access Control model which can assign different roles to tenants means cloud users and later based on the privacy and security concerns the same model can revoke the access control polices from the tenants. And auditing services of different models are explained.

KEYWORDS: *CP-ABE, ABE, Auditing, Access Control*

I. INTRODUCTION

This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Cipher text-Policy Attribute-based Encryption is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies. In CP-ABE [3] scheme, there is an authority that is responsible for attribute management and key distribution. In a multi-authority cloud storage system, attributes of users can be changed dynamically. A user may be join some new attributes or revoked some current attributes. In [5,6], worked on Attribute Based Data Sharing with Attribute Revocation. This paper use semi-trustable on-line proxy servers. This server enables the authority to revoke user attributes with minimal effort. This scheme was uniquely integrating the technique of proxy re-encryption with CP-ABE, and also enables the authority to delegate most of laborious tasks to proxy servers. The advantages of this scheme is More Secure against chosen cipher text attacks. Provide importance to attribute revocation which is difficult for CP-ABE schemes.

Role Based Access Control Models

[11] lists the problems with the role based access control such as role explosion. The work states that RBAC is suitable for only an organization which has well defined hierarchy of roles and organizational

structure. [10] in their work implies that the role based access control is not suitable for distributed applications. This work emphasis the usage of adding attributes to the roles. [8] Proposed a Generalized temporal based Access control model based on the basic temporal model which adds time constraints to the role based Access control model. This work states the importance of the transient nature of permissions for a static role. [9] Introduces the administrative model of the role based access control to ease the management of RBAC. In some application domains like mobile computing, the location of the user is considered as a parameter for providing access rights. [1, 2] proposed an access control model by adding the location to the role based access control. But such model is suitable only for specific applications.

[3] Proposed an access control model for cloud based on RBAC, this model takes in to consideration the user and the owner of a object. The user acquires permission from the owner and access the cloud service. This model is not suitable for enterprise or an organizational set up. This model may be considered as the basic of the models that are in wide use now which asks permission from the owner to access certain services. Example would be some application asking for authentication to view some data of the user through email login. [5] Combined the cryptography method with the formal RBAC to provide security in the cloud systems. This paves a way for a new architecture where the sensitive data can be stored in the private cloud and other data can be stored in the public cloud. The authors concentrate on providing another layer of security to the data by encrypting it based on Roles. [6] proposed a method of RBAC that suits the multitenant characteristics of the cloud. Access control is based on the trust relations of the user in one tenant to the other. There were also many other works that modifies the RBAC with spatial and temporal parameters.

II. Attribute Based Access Control Models

The problem with the role based access control is many persons in an organization are assigned with a same role, but all the persons cannot be provided with same set of rights. So an extended model called ABAC is introduced, in addition to the roles assigned to the user some other attributes are also assigned to achieve more fine grain access control. Byungrae cha et al. (2012) presents a model of attribute based access control that is suitable for cloud computing environment.

[11] Proposed cryptographic attribute based access control mechanism with added user revocation technology in it. Though there are various works based on the Attribute based Access control, [10] provides a detailed view of the Attribute based access control and its variants. There are also different variants of Attribute based Access control Mechanisms. The problem that persists with the access control mechanism is accountability and administrative constraints with the increased number of Attributes.

Other Access Control Models

Zhang et al. (2006) proposed an access control model to enhance the basic RBAC model to meet the scenario of business to business and business to consumers where various organizations are involved. A work proposed by sejong oh &seog park (2003)

extends the role based access control model to include the tasks in the organization. Access is provided based on the unit of work referred as task to be done by the requestor. Role based access control at certain cases is lacking in expressing the access control rules. In order to overcome this issue Jeffrey Fischer et al. (2009) introduced a model based on business objects. This model is suitable for object oriented languages.

Tahminaahmed et al. (2006). Proposed an access control model based on the object relations that exist between the objects in object oriented programming. But the relations specified are taken in its general form. Canngo et al. (2015) provides a new method of access control mechanism suitable for multitenant nature of the cloud environment based on attribute based access control. The access control is combined with the information model of the cloud infrastructure. The performance results shows that the time for providing an access token is slow due to the overhead created during digital signing of the tokens. Banyal et al. (2014) introduces a access control mechanism for cloud which depends on the trustworthiness of the user. The trustworthiness is based on user's credentials, behaviors and reputation. The work acts as a method of detecting the unauthorized access and does not prevent it. Chang choiet. al. (2014) proposed an access control model based on context ontology. It eliminates the limitations imposed by some characteristics of cloud computing, this model is also based on RBAC.

[8] enhances the traditional Role Based Model with trust added to it. A layer for checking the trust credentials of the user is introduced before assigning the policies to the roles. Since the model is based on the role based access control, the problems associated with RBAC persist in this model also. Jun Luoet. al. (2016) introduces a novel role based access control model suitable for the cloud environment based on the factors such as security state of the user and server, the network availability of the user host, etc.,

Limitations of Existing Access Control Mechanisms

How the various access control models that are currently being in use are used to solve the scenario described and discussed. There is a list of access control mechanism that are in use and each have their own pros and cons. The latest of these mechanisms is Relation based Access control (ReBAC). Mechanisms that precede ReBAC are access control list, Mandatory Access Control, Discretionary Access Control; Role based Access control (RBAC), Attribute Based Access control (ABAC). RBAC and ABAC are the predominant Access control mechanisms that are in use now.

Limitations of RBAC Role based access control earlier used only in domains such as databases (R.W Baldwin 1990) in the form of named protection domain is later used in organizations after David Ferraiolo (1992), emphasis the suitability of role based access controls for the organizations. Sandhu et al. (1996) discusses the various other models based on RBAC suitable for access controls in organizations. Roles are created based on the business requirements of the organization and each role is assigned with a set of access control rights based on the access policies of the organization. Individual users are assigned

to the roles, so the access rights provided for a role is applied to the user to which the role is assigned. The general method of RBAC is depicted from the following Figure 4.1.

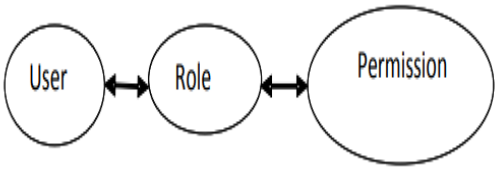

Fig 2 Role based access control model

In the example scenario considered, the Role Faculty Advisor will be assigned to a person, and the access control policy is, if a person is a Faculty Advisor then he or she can access the Student record. It should also be noted that the roles are common and there are many persons in an educational system with the role of Faculty Advisor. But all Faculty Advisors are not supposed to view the records of all students. Imagine, a Faculty advisor of computer science Department accessing the personal data of the student belonging to the mechanical Department. But, the requirement is that faculty advisor can access only the record of the student who is assigned to him. This example clearly illustrates the problem pertaining with RBAC. The next Access Control Mechanism that came in to use is ABAC.

Limitations of ABAC

Attribute based access control model had its beginning with the work of Mohammed kahtain, Ravi & Sandhu (2002), in which the attributes of the subjects are used to assign the users dynamically to the roles. ABAC can be considered as the extension of RBAC, in addition to the Roles assigned to the users, attributes are also added Vincent Hu (2015). For example, the Department of a person can be added as an attribute to the Faculty Advisor Role. This can be used as an access control policy as follows; Faculty Advisor belonging to a particular department to which the student belongs only can access the student record. The attributes considered here is of both the subject attributes and the object attributes. The General Architecture of the ABAC given by National Institutes of Standards and Technology (NIST) is given in figure 4.2.

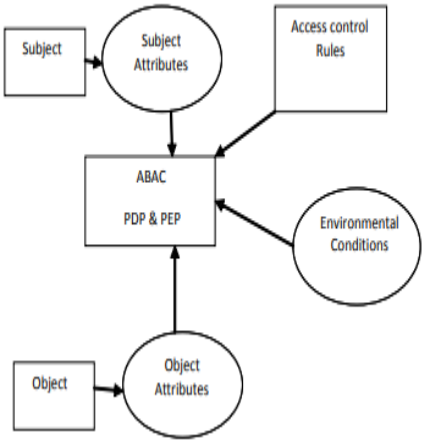

Fig 3 Attribute based access control model

The extent to which the RBAC and ABAC satisfies the example scenario can be understood with the following rules that are framed based on the RBAC and ABAC.

III. Significance of the Problem

In this paper, they first offer a revocable multi-authority CP-ABE scheme, where an efficient and secure revocation strategy is advised to take care of the attribute revocation issue in the framework. This attribute revocation technique is proficient as it brings about less correspondence cost and calculation cost. Additionally, is

secure as in it can accomplish both in backward security (The renounced user can't decrypt any new cipher text that requires the revoked attribute to decode) and forward protection (The recently joined user can likewise decrypt the beforehand distributed ciphertexts1, on the off chance that it has adequate properties). Their scheme does not require the server to be trusted entirely because the vital upgrade authorized by each quality specialist, not the server. Regardless of the possibility that the server is not semi-trusted in a few situations, their scheme can even now ensure the backward security. At that point, they apply their proposed revocable multi-authority CP-ABE system as the fundamental methods to build the meaningful and secure data get access control scheme for multi-authority cloud storage frameworks.

The proposed system conquers the issue exists in the existing system. The author suggested another algorithm named as Improved Security data Access Control. This algorithm enhances the security of the framework. The data owner when stores the data into the cloud server he encrypts it and afterward stores it. The regarded authorities give keys to the authorized authorities. So, when the user tries to access the data to which he is not having the desirable attribute the demand gets rejected, and the user gets blocked by the authority. Also, the administration will likewise produce a message about the attack to the data owner so thatdata owner can make additionally move. On the off chance that the user has done it by error the authorized user can contact the data owner to unblock him. On the off chance that the user has not done it then likewise the user can communicate the data owner and can guarantee greater security by requesting the data owner to change the login credentials. This new algorithm similarly gives data integrity. It educates about the attack by the unauthorized user to data owner when data owner verifies it. That is the point at which the data owner needs to check the files stored in the cloud often. Assuming any adjustments are found in the file on the server by any unauthorized access then this algorithm notifies the data owner that the document not protected, it changed.

There are five entities in the system as, a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud (server) and data consumers (users). A global trusted certificate authority in the framework is CA. CA sets up the system and furthermore acknowledges the registration of the considerable number of users and also AAs in the structure. For each legitimate user in the structure, the CA assigns a unique user identity to it and furthermore creates a single public key for that user. Nonetheless, the CA do not engage with attribute administration and formation of secret keys that are related to attributes. For instance, the CA might be the Social Security Administration, a free office of the United States government. Each user is issued unique Social Security Number (SSN) as its standard attribute. Each AA is an independent attribute authority that oversees entitling and renouncing client's characteristics agreeing to their part or identity in its area. In this proposed scheme, each property associated with a single AA. However, every AA can deal with a personal number of semantics of its characteristics. Each AA is in charge of producing a public attribute key for each

quality it oversees and, a secret key for every client mirroring their attributes.

To start with, let us consider what trait based encryption is and why this might be valuable. In standard crucial open cryptography, a document encrypted under a client's public key. The relating mystery key (and that key alone) would then be able to be utilized to decrypt the ciphertext. Presently, accept users each have different credits related to them. For instance, Alice might be in gathering called internal affairs, she is female and situated in the USA office of her association. Along these lines, they relegate her traits interior issues, female and USA. On the off chance that Bob needs to encode a file, so it decrypted by everybody who is an individual from the inner issues gathering, he could make an encryption of the archive for each client in this group utilizing their open key. Notwithstanding, consider the possibility that Bob does not know who is in the gathering. Imagine a scenario in which users are added to this collection later. In this circumstance, they cannot utilize standard public key cryptography, in this manner; they swing to quality based encryption (ABE).

Advantages of proposed system

They alter the structure of the scheme and make it more down to earth to cloud storage formworks, in which data owners not included in the key generation.They significantly enhance the effectiveness of the property revocation technique. Our system not just gives forward and backward security. However, it additionallygives increased security by providing access control to authorized users.The algorithm proposed by us improves the safety by notifying about the attack to the data owner. They provide the data integrity. The data owner identifies the verification of the data storage when he checks the file.

Table 1Comparisons between Different Techniques

SR. no	Techniq ue	Algorit hm	Scalabi lity	Efficie ncy	Secur ity
1	ABE	DES	high	low	low
2	CPABE	DES	low	high	low
3	KPABE	DES	low	high	low
4	IBE	AES	low	low	high
5	MA-CPABE	AES	high	high	low
6	PROPO SED MODEL	RSA	high	high	high

IV. Proposed Methodology

As the number of users in cloud computing is expanding, security issues are additionally expanding accordingly. The primary security issue can be on how to control the unauthorized data access in the cloud. In this paper, they proposed an efficient data access control scheme with enhanced security. Their plan restricts the unauthorized access as well as guarantees secure access by the approved users. Alongside that data, integrity likewise provided. This scheme proposed for multi-authority cloud storage formwork. This project can connect to social networks which are on the web and furthermore in the remote storage formworks. Java is the

language used to implement the algorithms, and it is the most powerful language regarding security.

System Architecture

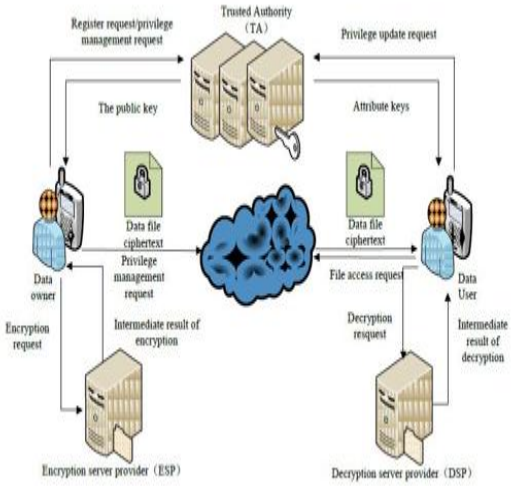

Figure 4: The figure demonstrates the system architecture

The number of records accessible by a single user within an organization is another metric which would depict the separation of the duties of the individual roles and hence the associated users. The following Table gives these details. The data is derived from the Access control policies enforced on the educational institution scenario, considering all the records that are available in the organization. The table also shows the action allowed for individual records, either both read and write or only read is allowed. The same record in the format of graph and the same data in terms of the percentage of records accessible by the individual user.

Table 2 Number of records accessible

	ABAC	RoBAc	TSP-RRBAC
Managing Director(R&W)	375	375	375
CEO(R&W)	369	123	118
Manager(R&W)	120	35	35
Team Leader(R&W)	350	38	20
Executive Staff(R&W)	10	8	4

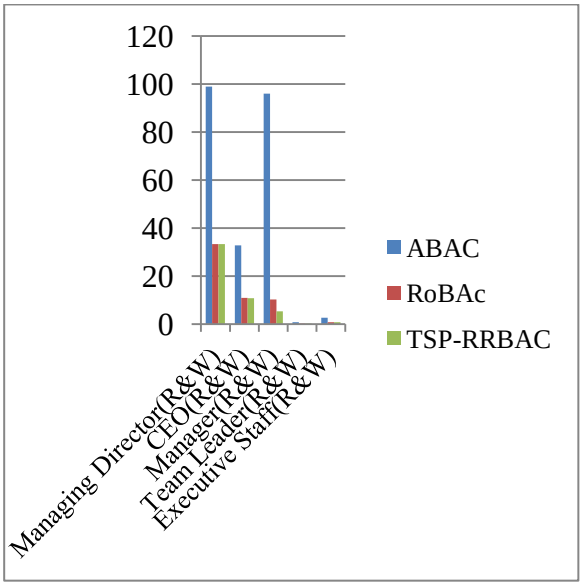

Figure 5: Number of records accessible by individual users

Table 3 Percentage of records accessible by individual users

	ABAC	RoBAc	TSP-RRBAC

Managing Director(R&W)	99	33.3	33.3
CEO(R&W)	32.7	10.83	10.81
Manager(R&W)	96	10.2	5.23
Team Leader(R&W)	0.7	0.23	0.23
Executive Staff(R&W)	2.56	0.7	0.7

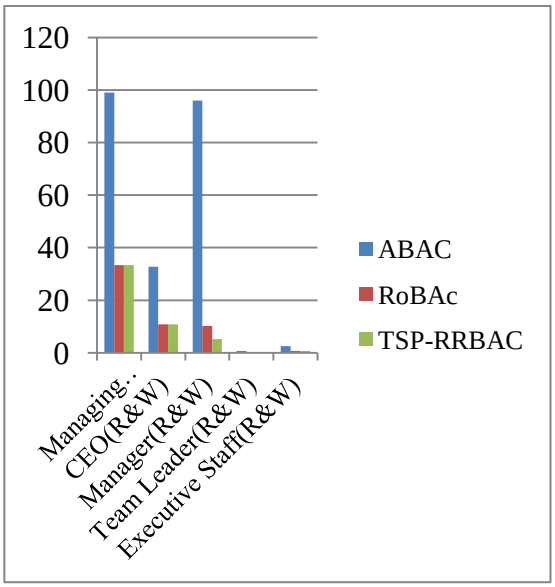

Figure 5: Percentage of data accessible by individual employee

V. CONCLUSION

The amount of records reachable with way of a single user within a business is just another metric which represented the remainder of the duties of the individual functions and hence the users. The following Table 4.4 gives those specifics. The data comes from the Access control policies imposed over the educational institution scenario, considering all of the records which can be found in the company. The table also shows that the actions enabled for individual recordings, both read and write or read is enabled. Figure 27 shows the exact identical listing in the arrangement of this chart and Figure 28 shows exactly the exact data in regard to the proportion of files reachable by the individual user.

REFERENCES

1. *Basri, S. R., &Rashmi, K. (2015, May). Attribute based revocable data access control for multi authority cloud storage. International Journal of Advanced Research in Computer Engineering &Technology, 4(5), 1887-1890.*
2. *Chen J, Dai S, Song Z. Efficient decentralized attribute-based access control for cloud storage with user revocation[C]. IEEE International Conference on Communications. IEEE, 2014:3782–3787.*
3. *Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]. ACM Conference on Computer and Communications Security. ACM, 2006:89–98.*
4. *Han Y, Di J, Yang X. The Revocable Attribute Based Encryption Scheme for Social Networks[C]. International Symposium on Security and Privacy in Social Networks and Big Data. IEEE, 2016:44–51.*
5. *Jahid, S., Mittal, P., &Borisov, N. (2011). Easier: Encryption-based access control in social networks with efficient revocation. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp. 415-425, Hong Kong, China, March 22-24, 2011.*
6. *Lai J, Deng R H, Li Y. Expressive CP-ABE with partially hidden access structures[C]. ACM Symposium on Information,*

Computer and Communications Security. ACM, 2012:18–19.

7. *Prasadu Peddi (2016), Comparative study on cloud optimized resource and prediction using machine learning algorithm, ISSN: 2455-6300, volume 1, issue 3, pp: 88-94.*
8. *SushmitaRuj, 2014, "Attribute based access control in clouds: A survey", ISSN: 2165-0608, 2014 International Conference on Signal Processing and Communications (SPCOM), PP: 1-6.*
9. *Younis A. Younis ;KashifKifayat ; MadjidMerabti, 2015, "A novel evaluation criteria to cloud based access control models", 2015 11th International Conference on Innovations in Information Technology (IIT), PP: 68-73.*
10. *Prasadu Peddi (2018), Data sharing Privacy in Mobile cloud using AES, ISSN 2319-1953, volume 7, issue 4.*
11. *Prasadu Peddi (2020), "Public auditing mechanism to verify data integrity in cloud storage", vol 8, issue 9, pp: 5220–5225.*