Secure Cloud Storage using Multi Attribute Authority with Multi Central Authority

Minakshi V.Shinde
Computer Science & Engineering
JSCOE ,Hadapsar
Pune, India
Chavanminakshi14@gmail.com

Prof.H.A.Hingoliwala.
Computer Science & Engineering
JSCOE ,Hadapsar
Pune ,India
Ali_hyderi@yahoo.com

***Abstract*—** Cloud Computing plays a main role in present day to day life. Security & privacy of data is major task in cloud. It is required to protect data from hackers & introdures . To provide more security this paper present multi attribute authority Cipher text Attribute Based Encryption (CPABE)technology with multi Central Authority(CA). Due to untrusted cloud server data access control becomes challenging task in cloud computing. Current data access control scheme is no longer applicable to cloud storage system, because it can't provide fully trusted cloud server. We call it as a central authority. This single CA did not manage any attribute but responsible for issuing user unique id (UID).This CA must have capacity to decrypt any Cipher Text(CT) on the cloud. To overcome such a drawback here we can replace single CA to multi CA.in this paper we design secure cloud storage by providing access to the files using CPABE scheme. This system achieve forwarded & backward security . Also in this paper revocation technique is used related with file,user and attribute.

Keywords-*Access Control,forward and backward security,revocation,muliattribute authority,multi central authority*

*****

I. INTRODUCTION

Cloud storage typically refers to a hosted object storage which provide service for data owner to inject their data into cloud storage and provides users with immediate access to a broad range of data .Every owner can upload their data into cloud storage. Cloud server provides "24/7/365" data access to user .Because of data outsourcing user cannot be fully trusted on cloud server for data access control service. Existing server based methods 1) DAC-MACs method 2)Revocable data access control for multiauthority cloud storage was proposed by Kan Yang. These 2 methods are no longer applicable to cloud storage system .Because in both methods single Central authority(CA) is used.Which is responsible for providing id to user & Owner & Attribute Authority.Because of that this single CA can easily decrypt any Cipher Text on to cloud. To overcome such a drawback we have replace the single CA to multi CA.

CPABE is one of the most suitable technology for data access control in cloud storage .In this scheme CPABE, the receiver has the access policy in the form of a tree , with attributes as leaves monotonic access structure with AND,OR and other threshold gates. This method gives data owner to control on access structure policy and does not require data owner to distribute key with data user for downloading file from cloud .In this scheme there is an Attribute authority i.e AA responsible for attribute management and key distribution .Data owner defines the attribute set and access structure policy over these attribute set and encrypt data under these policy .A user can decrypt CT from cloud if and only iff it's attributes satisfy the access policies. Due to inefficiency of computation previous CPABE proposed by Kan Yang technique can not directly applied to data access control system in terms of security.

In this paper we first replace single CA to multi CA with multi AA. For each AA there is separate AA according to their attribute set.

The main contribution of this work can be summarized as follows.

1. We propose DAC multi AA –multi CA ,an effective and secure data access control scheme for trusted cloud storage system. This system has good performance than DAC MAC & efficient, expressive DAC MAC by Ken Yang scheme.
2. We construct new multi CA Multi AA CPABE scheme with efficient revocation and decryption.
3. We also construct revocation method for Multi AA Multi CA CPABE regarding attribute, file & user revocation which is used for achieving forward and backward security.

The remaining of this paper is described as follows .We first define system related work in I section .In section II system model ,frame work ,Then we propose Experimental set up for a new MA CPABE with multi CA .In section IV we analyze multi AA multi CA in terms of both security and performance. Finally conclusion is given in last section.

II. RELATED WORK

A. Attribute Based Encryption (ABE)

Sahai & Waters in 2005 proposed a system in which data is encrypted at the fine grained level & named as ABE([5],[8]). In ABE a owner can encrypt data specifying attribute set & number d as a access control over attribute

set, such that only a user with at least d of given attribute can decrypt message.

B. *Key Policy Attribute Based Encryption (KPABE)*

V.Goyal ,O. pandey , Sahai & Waters proposed a KPABE scheme [8].In this method type of public key encryption, the secrete key of a user & the Cipher Text (CT) are dependent upon attributes. In such a system, the decryption of CT is possible only if the set of attributes of the user key matches the attributes of CT.

C. *Cipher Text Attribute Based Encryption(CPABE)*

Sahai et al suggest new modification in this in existing ABE called CPABE ([3],[8]) .In this method user secret key related with a set of attribute & ach CT embedded with an access structure. It removes the need for knowing the identity of the user's-ABE improves the disadvantages of KP-ABE that the encrypted data cannot choose who can decrypt it. But it is difficult in user revocation.

D. *Identity Based Encryption (IBE)*

M.F ranklin, D. Bonch in 2001 introduced an identity based encryption scheme ([8],[9]). In this data is encrypted using ID of user by owner. Decryption takes place by using secrete key for relevant ID which have been used during encryption. This secrete key is received by user from key generation center (KGC). Main drawback of such a system is that, KGC have power to decrypt all CT over cloud. Another version of IBE is Hierarchical identity based encryption (HIBE).It is hierarchical form of IBE.

E. *Multi Authority Attribute Ciphertext Based Encryption(MA-CPABE)*

MA-ABE is introduced by Chase[1] .It consist of single central authority ,which is responsible for issuing secrete key to user and there are multi attribute authorities, from which, each AA is responsible for monitoring attribute and issuing it to user for decryption CT. But main drawback of such a system that single CA has power to decrypt any CT on cloud. Hence user cannot fully trusted on cloud server because this single CA issue UID & AID to user & attribute authority respectively. By using this UID &AID CA can decrypt any CT on cloud.

The comparisons above discussion Encryption techniques are shown in Table1

Table1 Comparisons Between different Technique

Sr. no	Technique	Algorithm	Scalability	Efficiency	Security
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	Proposed System	RSA	High	High	High

III. SYSTEM MODEL

As shown in figure we consider a cloud storage system with multi AA multi AA.This system model consists of 5 main entities.

1)Central Authorities(CAs)2)Attribute Authorities(AAs) 3)Owner 4)User 5) Cloud Server

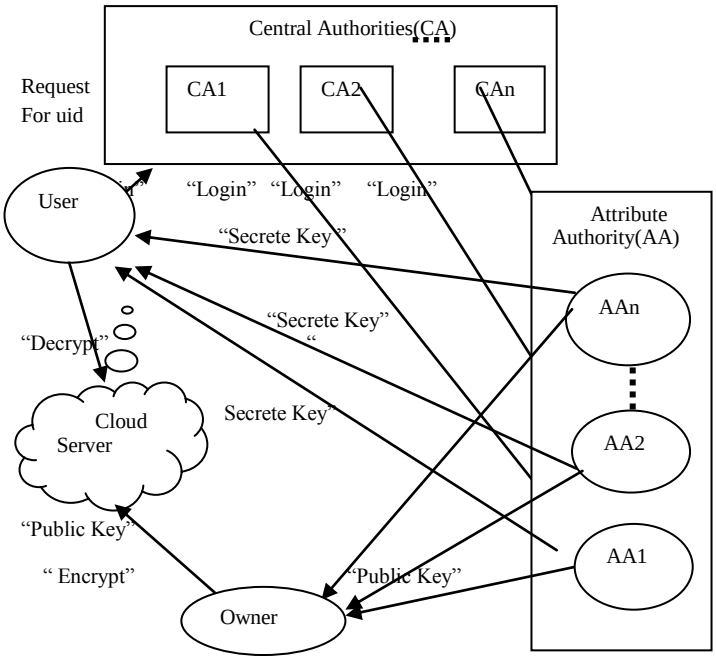

Fig.1 System model for MA-ABE with multi CAs

A. *Central Authority(CA)*

In this system there are multiple CAs. Who set up the system according attributes in the system. For each attribute set 1 CA is allocate .Each CA accept registration of 1 AA number and number of users according to there attributes. The CA is not involved in managing attributes but responsible for assigning unique ID to AA & user .By using that ID single CA can decrypt any CT on to cloud. To overcome such drawback here replace single CA top multiple CA. Ex .In Pune University there are different departments like Engineering ,Management …and so on. For each department single CA is used.

B. *Attributel Authority(CA)*

Every AAi in this system is first register to respective CAi in the system. And receive ID. Every AA is responsible for a managing attributes and attributes revocation ,user revocation ,file revocation. Every AA has full control over structure. AA generate public key for owner for uploading her file on to cloud. Also AA generate secrete key for user for downloading her file iff users attribute policy match with owners attribute policy.

C. *Owner*

Each owner has a unique id in the system Owner submit attribute set and policy structure over this attribute to the system. These attribute come from AA .Then respective AA generate public key for that attributes.Then owner submit text file size up to 1 MB that is a encrypted file to system as a CT.

D. *User*

Each user has a globalunique id in the system.User submit attribute policy structure to system.Respective AA check if these attribute policy structure is match with owner policy .Then generate secrete key and user successfully download that file.

E. *Server*

In our system server is fully trusted cloud server.This store data from owner and provide access to the user.Also help to owner for update CT when user,file,attribute revocation happens.

IV. FRAMEWORK

A. *Phase 1 :System Initialization*

1. CA SETUP

The CA setup the system by running the CA set up algorithm. Each CAi accept both user & AAi registration for particular attribute domain.Ex. Engineering university domain for Engineering user (student, staff, H.O.D) and Engineering attribute authority which holds all Engineering attributes like Engineering syllabus, branches, seats and so on.

- *User Registration.*

CAi first assign uidi to user. Also generate 2 random number uidi, uidi' using RSA algorithm, .Then generate global secrete keys are

GSKi= uidi and GSK'i=aidi

Then global public keys are

GPKi= uidi and GPK'i=aidi

CAi also generate certificate(uidi) for user.CAisend global public key and global secrete key & certificate to user, that is set of (GSKi, GPKi, uidi).

- *AAi Registration*

Every AAishould register to respective CAi, during system initialization. If AAi is legal authority in the system, then CAi first assign a global attribute authority id aidi to this AAi. Then CAi send the global public /secrete key of each user(GSKi, GPKi) to AAi, which can be used to verify the certificates of users issued by CAi..

B. *Phase2:Data encryption by owner*

Owner send request to AAi for upload data by submitting ID, file, attribute set and policy structure ,then AAi check for legal owner. If he is valid owner then AAi send public key to the user according to its role or identity.

C. *Phase3:Data decryption by user*

User send request to CAi using secrete public key pair GPKi, GSKi, UIDi.By submitting this certification (UID) to AAi,then AAi check for legal user. If he is valid user then AAi send attributes to the user according to its role or identity.

V. SECURITY ANALYSIS

We prove that our data access control is secure under the security model we defined, which can be summarized as in the following theorems.

A. *Theorem 1:*Our system achieve high security than previous schemes like DAC MACS[1] and Expressive ,efficient DAC[2].

Proof*:* . Due to untrusted cloud server , data access control schemes becomes challenging task in cloud computing. Current access control scheme DAC MACS[1] and Expressive ,efficient DAC[2] are no longer applicable to cloud storage system, because it cannot provide fully trusted cloud server we called it as a Central authority (CA).This single CA did not manage any attribute but responsible for issuing user unique id (UID).This CA must have capacity to decrypt any Cipher Text (CT) on the cloud. To overcome such drawback, here we replace Single CA to multi CA.In this paper we design secure cloud storage by providing access to the files using Attribute Based Encryption (ABE) scheme.Because of that Our system achieve high security

B. *Theorem 2:*Our system achieve both Forward and Backward Security

Proof*:* . 1)Forward security :Whenever user attribute revocation takes place, AA send request to owner for update that revoked attributes.In this way user cant download any CT in future from cloud by using that revoked attributes.

2)Backward Security:During the secret update,respective AA generates an update key for each non revoked user.This update key is associated with user id.Revoked user cant use update key of non revoked user to update its own secret key.

VI. PERFORMANCE ANALYSIS

In this section ,we analyze the performance of our scheme By comparing with the Kan Yang DAC-MAC [1]& Expressive, efficient DAC[2] in terms of storage overhead & computation efficiency.

A. *Storage Overhead*

The storage overhead is special issue of the access control scheme in cloud storage system. We compare storage overhead on each entity in system.

1) Storage overhead on Each CA: Each CA need to store information about user id uid,attribute id according to there attributes.

2) Storage Overhead on Each AA:Each AA need to store information about all attributes in its domain.Also each AA need to store public key & secret key for encrypting and decrypting file from cloud respectively.

3) Storage Overhead on Each Owner:Every owner hold the set of attributes & attribute policy.Also owners are required to hold original file & public key for every CT in the system.

4) Storage Overhead on Each User:Every user hold the set attribute policy.Also users are required to hold separate secret key for every CT in the system.

5) Storage Overhead on Server:All CT are stored on to cloud.

VII. COMPUTATION EFFICIENCY

We implement our scheme on a Win XP/Win 7 with an Intel Core 2 DuO CPU at 3.16GHZ and 4.00 GB RAM.We compare the computation efficiency of both encryption & decryption in terms of time. As compared to previous scheme[1][2],our system require less time for encryption and decryption.

VIII. ADVANTAGES

A. *Security*

Without secrete key, any user can not access any CT on the cloud. Also CA does not encrypt any CT on the cloud..The data is highly secured by using MA-CPABE, because before outsourcing data in the cloud it is encrypted using secrete key and set of attributes and access structure over attributes.

B. *Storage*

Whole information is stored in the cloud. Like data, attribute access structure over attributes.The encrypted data is stored on the cloud for security purpose.

C. *Portability*

User can access data on the cloud at any time and from anywhere as the encrypted data stored in the cloud. It can reduce the cost for accessing the information as it can be accessed from any where and any time.

D. *Data Integrity*

This is fundamental requirement in the cloud system. Our system can provide data integrity means that without owner permission data cannot be updated.

E. *Control*

In the cloud system controlling is important thing. It indicate that amount of data is to be visible to legal user should be controlled. In our system data is visible to only those users whose attributes can satisfy attribute access structure which has used during encryption.

IX. CONCLUSION

The key objective of our framework is to provide security cloud data using Multi Attribute Authority- Attribute Based Encryption using multi central authority, that can support efficient attribute, file , user revocation. These systems also provide backward and forward security. Main goal of this system is to provide security against decrypting every cipher text by single central authority in Multi Attribute Authority - Attribute Based Encryption with single Central Authority system. In which different attribute authorities are managed by central authority according to their attribute domain. And no authority can independently decrypt any Cipher Text. And this can achieve more security as compared to Multi Attribute Authority Attribute Based Encryption single CA.

ACKNOWLEDGMENT

I would like thanks to Prof. H. A. Hingoliwala professor of Computer Engineering at J.S.P.M .Hadapsar ,who guided through this paper.

REFERENCES

[1] Kan Yang, "DAC-MACS: Effective Data Access Control for Multi Authority Cloud Storage"in IEEE ,vol.8,Nov 2013.

[2] Kan Yang, " *Expressive, Efficient, and Revocable Data Access Control for Multi Authority Cloud Storage"* ,in IEEE,vol .7,Jul 2014

[3] J. Bettencourt, A. Sahai,B .Water "Cipher text Policy Attribute Based encryption"in IEEE vol .7,200s7.

[4] S .Yu, C. Wang, K ,Ren " Achieving secure, scalable ,and fine grained data access control in cloud computing"in IEEE INFOCOM 10,2010.

[5] S .Yu, C. Wang, K ,Ren ," Attribute based data sharing with attribute K. Elissa, "Title of paper if known," unpublished.

[6] S .Yu, C. Wang, K ,Ren ," Attribute based data sharing with attribute based revocation",I n IEEE ,2010.

[7] Muller, S. Katzenbeisser and C.ekert " Distributed Attribute Baseed Encryption " 2008.

[8] Gitesh Sonawane "Enhansing securities for cloud storasgse using file encryption"2010.

[9] Sharmila Rajsudhan "A study on cryptographic methods in cloud storage"injournal,vol 02,Mar 2014.

[10] Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel

"*Securing Broker-Less Publish/Subscribe systems Using Identity-Based Encryption" in IEEE ,vol 25,Feb* Article in a conference proceedings:

[11] Debajyoti Mukhopadhyay,"Enhanced security for Cloud storage using file Encryption",2011.

[12] Shani Raj" Multi owner data sharing in cloud storage using policy based encryption"vol 4 Issue 5,may 2014.

[13] Sharmila Rajasudhan"Study on cryptographic methods in cloud storage"Vol 02,Issue 02,Mar 2014.

[14] Allamaprabhu G.Rudraxi"A novel patient centric framework for data access control in semi trusted cloud servers "vol 03,Issue 6 Jun 2014.

[15] Rajesh L Guikwad "Implementation of network security model in cloud computing using encryption technique" vol 1,Issue 02,2013.

[16] Sharmila C"Multiuser access control and key management mechanism for personal health records"vol 03,Issue 04,Mar 2014.

[17] Vibha Mittal"Enhanced security for cloud storage using file encryption."

[18] Kan Yang "DAC-MACS:Effective data access control for multiauthority cloud storage storage" vol 8 ,No 11,Nov 2013.