International Journal of Engineering & Technology, 7 (1.1) (2018) 322-325

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Different access control methods with revocation in multi-authority cloud

K. V. V. Satyanarayana [1] *, J. Mahathi [2], V. V. R. Srikar [2], Sk. Sai Babu [2]

[1] *Professor Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India-522502*

[2] *Student Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India-522502*

**Corresponding author E-mail: mahathilalitha@gmail.com*

Abstract

Now-a-days, usage of cloud is getting more popular and for the safety the security is being enhanced every day from time to time. Multiple security techniques are being implemented. Attribute based security is one of the concepts especially for basics of the cipher-text based, but the user's attributes were given by the multiple authorities. So, the multi-authority with cipher-text encryption is emerging at present. In this, we will see why the cipher-text based is important and different security models with the multi-authority with the revocation in the different levels in the security models.

Keywords: *Multi-Authority; Revocation; Encryption; Attributes.*

1. Introduction

Cloud Computing in present days is a paradigm which attracting the attention in present society. Cloud is being used by many different people in multiple ways such as the storage purposes, providing access for the data stored to the other people using methods. One of the main concern or the problem facing is about the security concern, because the data that stored in the cloud maybe the sensitive (or) personal type which is sensitive type. So, security is one of the concern for the Cloud computing aspects. The Cloud Service Providers (CSP) can be the semi-trusted and they maintain, operate the storage in the cloud. So in order to provide the security and also to avoid the unauthorized people from accessing the sensitive data, encrypting the data and uploading it into the cloud. For this purpose there many encryptions that exists. One of the type is the usage of the Identity based encryption (IBE), there are some disadvantages in this method. So the new versions depending on the attribute-based type of the encryption methods are being developed and implemented. Depending on the attribute based, the revocation and the access to the multi people by multi-authorities is being secured with the necessity for the revocation.

2. Literature survey

CP-ABE is trusted cryptographic approach for fine grained get to control. The underlying multi-expert ABE (MA-ABE) was given by pursue in which a few AAs and one focal authority (CA). Other CP-ABE conspire was given by T. Herranz with consistent size figure content which works for edge case. The denial issue is vital in quality based frameworks. Other CP-ABE plans that help characteristic level disavowal are additionally proposed.

3. About the attribute base encryption

Before knowing about the different methods depending on the attribute based, we need to know Identity based encryption, as it is used before the ABE, we now see about IBE usage and why attribute based is using not identity based is using.

Identity Based Encryption is about the encryption of the data depending on the identity who are going to use the data. Let us see an example of the mail sending. In this X sends an email with the encryption to the Y using the identity of her, which results in the accessibility of the mail content only to Y, which means a single user can only decrypt and uses the data. This leads to the fall of the flexibility and in the data access control because that encrypted data may need to be used by multiple users. This is a disadvantage in using the identity based encryption.

So, the attribute based encryption (ABE) is being implemented to solve the problem of the IBE. The problem in the IBE is overcome by using ABE, which provides the multiple attributes to the user, the cipher-text of the user is being associated with some set of attribute. The decryption of the data is only possible only if the set of the attributes. With respect to attribute based there are two composes: Key-policy attribute based encryption (KP-ABE) and cipher-text policy attribute based encryption (CP-ABE).

In the key based policy the secret key will be with the associated with the policy of access and cipher-text will be having a set of the attributes.

In the cipher-text policy every cipher text will be associate with policy of access and key will having the set of the attributes. Comparing the KP-ABE with the CP-ABE, CP-ABE is much more effective than the KP-ABE because in the CP-ABE there will be much flexibility for the data owner to enforce access policy on the data.

Copyright © 2018 K. V. V. Satyanarayana et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

So, in this we will be concentrating about the CP-ABE encryption policies. Using the cipher based, there are many problems present, one of the problem is that in cipher based there is one attribute authority (AA) which is responsible for the allocation of the attributes to the users. If there users that in need for the attributes then the work will be delayed with the single AA. So in order to overcome these problems we are going with the multiple-authority ABE (MP-ABE). After this we need to know about the revocation of the attributes to the users.

Revocation is an important process in the cloud and also for the access of the data. Let us consider an example of an office in which the employees in the office can be hired / fired (or) promote/demote. So there is a need to change or revoke the attributes to the users, for the accessibility of the data. In order for the success for the attribute revocation we consider two requirements:

1) Backward security: If a employee is demoted then the attributes will be revoked such that they can't decrypt the new cipher-texts(high level data or the previous access able data).
2) Forward security:-If the employee is newly hired then he will be given access to previous data, if he is promoted then the attributes provided must have sufficient credentials for access of high level data of the company.

For these two requirements to complete there will be a high overhead because there will be much data to r-encryption.

4. Models regarding the CP-ABE based encryption

There are many people who proposed many different methods regarding the multi-authority CP-ABE and the revocation process in these methods.

Some of the models are:-

1) DAC-MACS (Data Access Control for Multi-authority Cloud Storage).
2) TFDAC-MACS (Two - Factor Data access control for the Multi-Authority Control Systems).

In all the above models mentioned we need to know about the components in them

- Data Owners.
- Users.
- AA (Attribute Authority).
- Cloud Authority.
- Cloud Storage providers.
- Server.

Cloud Authority: It is the global trusted party in the system which sets and do the registrations for the Attribute authority and the users. For the every user that is considered as legal will provide a unique identity along with the public key for the user. It doesn't involve in any kind of secret key generation and along for the attribute management.

Attribute Authority:-In the system there will be many no of the AA's which will be independent of one another, its responsibility is allocation, updating, revocation of the user level attributes depending on their identity or role. AA for each attribute produce the public-key and for each user, produce secret-key

Users: Each user will be having a unique identity given by the CA in order to query the Cipher texts and then submit the secret keys which were given by the AA's. He can decrypt only when he satisfy the access policy by using the secret key and the decryption token and the cipher text.

Data Owners:Before sending the data into the cloud or outsourcing the data, they encrypt the data with the assistance of content keys. The owner defines the access policy over the attributes from multiple AA's

When the user can satisfy the attributes over the access policy then only he can decrypt the data.

Cloud Storage Providers: The data that the user encrypts and stores the data in the cloud, Sometimes the cloud storage providers can also act as the servers which will give the information to the clients using the AA's for the legal check and whether the attributes satisfy the access policy.

These are the basics or the terminology of the components that need to be known.

5. DAC-MACS

In this we are going to discuss about the DAC-MACS and it's working.

In this there will be many phases

1) System Initialization:

There are two steps:-CA setup and AA setup

a) setup of CA:

SA will be the set of attribute authorities.

Su will be about the set of the users.

Input will be security parameter.

Output will be the pair of signatures and the verification key

Using the random number it will generate the master key to compute the system parameter. This will accept the user registration and the AA registration.

Registration of User: For the every user he must be registered

Inputs will be: System parameters , user information.

Output will be: Both the global secret, global public key along with the user certificate to the user.

Registration of AA: Each AA must register to the CA.

Inputs to CA will be info of the AA

Outputs will be global authority identity, verification key, system parameter to AA.

b) Setup of AA:

Each AA chooses the three random numbers as the input

Output will be the public attribute key and the public authority key.

2) AA's Secret key generation:

In this the users and the AA will authenticate by the verification key. Then it will take the following as the inputs to generate the user's secret key

The inputs will be the secret authority key, system parameters, secret key certificate of the user along with a random number.

3) Data encryption by the owners:

Before the data is stored in the cloud the data is encrypted and it is stored in the cloud.

Inputs will be the system parameters, set of public keys given by the authority set, group of public keys, data and access structure of the selected attributes.

4) Data decryption by the users (using the cloud): First the user authentication will be done and can access the data only if he can satisfy the access structure to get the data.

There are two steps in this phase

a) Token generation by the Cloud Servers:
b) Data decryption by user.

Token generation by server: In this user asks the server by sending secret key for the token which is responsible for the decoding, possible when only the attributes possessed by the user is valid

For this the inputs will be the access structure, global public key and the secret key of the user, using them the output which is token of decryption will be send to user.

Data decryption by user: By receiving the decryption token along with the global secret key, along with this user will be using the content key for getting the data.

5) Revocation by using the efficient attributes:

For the revocation purpose there are three phases that includes:-AA's update the Key generation, Updating the secret key of the non-revoked-users, Updating the cipher text by the cloud server. Using this secret key updating can be useful in the Backward security and the cipher text updating will be useful in the forward security.

AA's updating the key generation:

The responsible AA can run the update secret key algorithm

Inputs will be secret authority key, the current attribute version key and the user’s global public keys.

Output will be the new update User's key and the cipher text.

The AA will update the public attribute key of the revoked person and broadcasts the key to the owners that are updated.
Updating the secret key of the non revoked-users: For the non-revoked users who are having the attributes which are revoked will be having the user's key update key, using this the user runs the update key algorithm to update the secret key.
Updating the cipher text by the cloud server:-
In this corresponding AA will sends the cipher update key to server to run the update cipher key algorithm for the updating all the cipher texts which are related to the revoked attribute
Inputs will be the Cipher text and the cipher text key
Output will be the new cipher text.
This is all about the DAC-MACS, which is required to update the components which are associated with revoked attribute.

6. TFDAC-MACS

The proposed system will be the TFDAC-MACS. In this the main problem will be making the two factors into the integration.
In this there will be many 6 phases which will be having different roles.
1) Initialization of the system:
In this there will be 3 steps:
a) Setup of the CA.
b) Setup of the AA.
c) Setup of the DO's.
a) Setup of the CA:
CA runs the setup algorithm for the setup of the system. It choose two multiplicative groups G and Gt which are being useful for a generator g

e: G×G → GT.

Each AA should register with the CA to provide the unique global identifier to the AA.

GPP= (p, g, G, GT, e, H)

b) Setup of the AA:
The input that AA takes will be Global Public Parameters and Attribute Domain.
The output will be the Public key and its related master secret key.
Public key will be

PKaid= (APK aid = e (g,g)x aid, {UPK aid i,j = g yaid i,j |u aid i ∈ U aid ∧ v aid i,j ∈ Said,i})

Master secret key will be

SK aid= (ASK aid = xaid,{USK aid i ,j =y aid i,j | u aid i ∈Uaid ∧ v aid i,j ∈S aid ,i}).

c) Setup of the DO(Data Owners):
The id of the Data owners will be unique DO uid which will be taking the GPP as the input and creates the public/secret pairs of pairs which are used for authentication.
Data owner choose some random number as the authentication secret key (OSK aid) for computing the public ket (OPK aid)
2) Secret key and Authorization generation:
a) Key generation of the AA's:
The user first request the AA for the attribute generation, AA will first check for the user identity using the certificate of the user, then AA will assign the user with a list of the attributes.
In this the inputs will be the Global public parameters and master's secret key.
Using the inputs the AA will generate set of the attributes secret keys for the data user.
b) Authorization:
In this the user asks the data owners for the permission or the authorization request. The authorization is done using the Certificate of the user, if valid then owner takes the authorization secret key as the input and generate the authorization key for the user

SKuid, oid =H (uid) α

3) Data Encryption:
In this the data owner first encrypts the data which needs to update to the cloud by using the access policy and also with the set of attributes along with public keys (U aid ∈IA W APK aid, U v aid i, j∈ W U PK aid i,j) and the authorization secret keys. (OSK oid).
The data owner choose some random number and sets

$$CT_w = (W, C_1, C_2, C_3), \text{where}$$

$$C_1 = m.(\prod_{aid \in I_W^A} e(g,g)^{x_{aid} n_W^{aid}})^s \; C_2 = g^s$$

$$C_3 = (\prod_{v_{aid_i,j} \epsilon W} g^{y_{aid_i,j}})^{s+\alpha}$$

Then the owner selects the unique label and sends the (oid,IDW,CTW) onto the CSP.
4) Data decryption:
On receiving the data from the cloud server, then user checks for the U (L uid, aid)! = W. If correct then data consumer uses the global unique identifier, secret key U (SKuid, aid) and the authorization key SKuid, oid.
Then the data (m) recovered is

$$m = \frac{C_1 . e(H(uid), C_3)}{e(C_2, SK_W) e(SK_{uid,oid}, UPK_W)}$$

5) Revocation in Attribute level: When an user's attribute is revoked the AA asks the query from the CSP for cipher text components using this the AA will generate the cipher text component and also compute the attribute update key for the every non revoked user. there are some algorithms that need to be followed.
a) key Update:
The AA will takes the non-revoked list, secret key, master secret key, cipher text components, public key as the inputs in this algorithm.
The output will be the new user public key, attribute keys, new cipher text component updates
After this the AA sends all the output to the Cloud Service provider and the non-revoked users.
b) SKUpdate:
After receiving the update attribute key the users updates the attribute secret key
c) CTA Update:-This is used to update the cipher text components.
The CSP choose randomly and gets the cipher text as

$$C_1' = C_1 . (\prod_{aid \epsilon I_W^A} e(g,g)^{x_{aid} n_W^{aid}})^r$$

$$= m.(\prod_{aid \epsilon I_W^A} e(g,g)^{x_{aid} n_W^{aid}})^{(s+r)}$$

$$C_2' = C_2 . g^r = g^{s+r} \; C_3' =$$

$$C_3 . CUK_{v_{aid_i,j}}^{ID_w} . \left(\prod_{v_{aid_t,j} \in W, v_{aid_t,j} \neq v_{aid_i,j}} g^{y_{aid_t,j}}\right)^r . g^{y'_{aid_i,j} r} =$$

$$(\prod_{v_{aid_t,j} \in W, v_{aid_t,j} \neq v_{aid_i,j}} g^{y_{aid_t,j}})^{(s+\alpha+r)} . (g^{y'_{aid_i,j}})^{(s+\alpha+r)}$$

6) User level revocation:
If the owner wants to change the access of his data, he chooses the new secret authorization key and its corresponding public keys. He generates the update key of authorization for non-revoked users along with the cipher text components.
There are some algorithms that need to be followed.
a) DA Auth update:
Owner takes the old authorization key, non-revoked list, public parameters from each AA as the input.

Then generates the new authorization key and the public key as the output and sends for the non-revoked users.

b) Auth-Update: Each non revoked user on receiving the new update generate the authorization key

SK'uid', oid =SKuid', oid· AUKuid', aid =H (uid') β.

c) CTO Update:

This is used to update all the outsourced data or the cipher texts. For the each cipher text the CSP computes:

$$C_1' = C_1 \cdot (\prod_{aid \epsilon I_W^A} e(g,g)^{x_{aid} n_W^{aid}})^{r'}$$

$$= m \cdot (\prod_{aid \epsilon I_W^A} e(g,g)^{x_{aid} n_W^{aid}})^{(s+r')}$$

$$C_2' = C_2 \cdot g^{r'} = g^{s+r'}$$

$$C_3' = C_3 \cdot \prod_{v_{aid_i,j} \epsilon W} UAU_{aid_i,j} \cdot (\prod_{v_{aid_i,j} \epsilon W} g^{y_{aid_i,j}})^{r'}$$

$$= (\prod_{v_{aid_i,j} \epsilon W} g^{y_{aid_i,j}})^{(s+\beta+r')}$$

Then the Cipher text will be updated with the new one.
This is the process that happens in the TFDAC-MACS.

7. Differences between the different policies

We need to know some terms for the comparisons

Notation	Descriptions
p	The bit size of an element in Z_p,G and G_T with prime order p.
N	The bit size of an element in the group Z_N with composite order $N=p_1p_2p_3$.
n_A	The number of AAs involved in the system
n_{uid}	The number of attributes values held by the DC_{uid}
l	The number of roe of the access structure M
F_{uid}	The index set of the AAs the DC_{uid} attributes related
T_e	Computation of one exponentation operation

Scheme	Access Policy	Parameter Size Secret key	Cipher text	Encryption cost	Decryption cost CSP	USER	Revocation Attribute level	User level
DAC-MACS	LSS	$(3n_A+n_{uid}+1)p$	$(3l+3)p$	$(3l+3)t_e$	$(2n_A+3n_{uid})t_e+ (n_A+n_{uid})t_e$	t_e	yes	no
TFDAC-MACS	ANDm	$(n_{uid}+1)p$	3p	$3t_e$	-	$3t_p$	Yes	yes

Scheme	Aganist user	Against CSP	Collison Resistance	Backward Security	Forward Security	Secure Channel Revocation
DAC-MACS	No	Yes	No	No	Yes	Yes
TDFAC- MACS	Yes	Yes	Yes	Yes	Yes	No

8. Conclusion

From the above comparisons we can say that the TFDAC-MAC is more efficient than the DAC-MACS or other policies in terms of the security and in the comparisons of the encryption and the decryption times along with the overhead that is present when reading the data for the encryption or the decryption timings
The Attribute revocation is present best in the TFDAC-MACS when comparison to the other models
The levels of the revocation is best in the TFDAC-MACS. There is provision for the revocation in the user levels which is not present in the previous models.
The TFDAC_MACS will provide the two-factor access for the security in the cloud security management.

References

[1] DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems Kan Yang, Associate Member, IEEE, Xiaohua Jia,IEEE, Kui Ren, Senior Member, IEEE, Bo Zhang, Member, IEEE, and Ruitao Xie, Student Member, IEEE.

[2] On the Security of Data Access Control for Multiauthority Cloud Storage Systems Xianglong Wu, Rui Jiang, and Bharat Bhargava, Fellow, IEEE.

[3] Two-Factor Data Access Control with Efficient Revocation for Multi-Authority Cloud Storage Systems Xiaoyu Li, Shaohua Tang, Lingling Xu, Huaqun Wang, and Jie Chen.

[4] D. Boneh and M. Franklin, ‘‘Identity-based encryption from the Weil pairing,’’ in Proc. CRYPTO. https://doi.org/10.1007/3-540-44647-8_13.