User Revocation Based Anonymous Access Provision for Efficient Cloud User Privacy

[1]M. R. Kavitha Rani [2]S. Brindha
[1]M. E Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]K.L.N.College of Engineering, Pottapalayam, Sivagangai 630612, India

Abstract

Cloud computing is a recent technology provides a flexible, on-demand and low cost feature of computing resources. The Main issue in Cloud Computing is user identity privacy and data content privacy. The User Privacy in Cloud Computing is achieved by various data access control Schemes. Existing Fully Anonymous Access control scheme with decentralized attribute authority provides data content privacy and also prevents full user identity leakage by using N-oblivious transfer and multi-authority ciphertext-policy attribute based encryption scheme. But user attribute revocation is not implemented for better security. Supporting user revocation over Anonymous Multi-authority Ciphertext-policy attribute based encryption (MA-CP ABE) is an important issue in the real application. We Propose a Revocable Anonymous Access Control with Multi-authority cloud storage system to enhance the security and to solve revocation problem, Here Each Individual Attribute Authority is able to issue the attributes and keys independently. Our Revocable Anonymous Access Control Scheme for Multi-Authority Ciphertext-Policy Attribute Based Encryption can achieve both forward and backward security. Our security analysis and performance analysis shows that our scheme is more secure and more efficient than previous work.

Keyword- CP-ABE, Anonymity, Multi-Authority, Cloud Storage, Access Control, Attribute Revocation

I. INTRODUCTION

In Recent years, Cloud Computing is a technology has many features like access anywhere from anywhere and at any time. There are some access controls and authentication schemes are provided to avoid the unauthorized access to the cloud data. The main issue in cloud computing is data security. Because the cloud server may not trustworthy all time and the malicious user may collude with each other to get the data stored in cloud storage. CP-ABE is the one of the most important technique used for access control in the cloud storage. By using this technique the data owner have their own control over data stored in cloud server. The data security in cloud is ensured by using CP-ABE scheme.

A. Cloud Storage:

The Cloud server is the main service of cloud computing. This can provide services for data owner to upload their data into the storage cloud. Here the main issue is data access control scheme with data hosting and data access service, because malicious user may misuse their rights and collude with each other to get the data from the cloud storage server. Hence the cloud server is not reliable and it will affected from collusion attack and also sometimes it compromises when a security breach happens.

B. CP-ABE

The most preferable technology for data access control in cloud storage server is CP-ABE. The CP-ABE Provides the cloud data owner to direct control over the data stored in the cloud server. Here the authority is responsible for the key generation and attribute key management.

There are two types of CP-ABE scheme they are Single Authority CP-ABE and Multi Authority CP-ABE.

Single Authority Ciphertext-Policy Attribute Based Encryption: In this only one centralized authority which manages all the key generation and attribute keys.

Multi-Authority Ciphertext-Policy Attribute Based Encryption: In this scheme N number of Decentralized Authorities are works independently to generate key and attributes.

C. User Revocation:

User Revocation is a process of removing the access right of users. This is done by the attribute Authority. Here the revoked users are maintained in the revocation list and this list is available in the cloud.

II. RELATED WORKS

[1] In 2011, S.J.Hur and D.K.Noh, worked on 'Attribute – Based Access Control with Efficient Revocation in Data Outsourcing System' in this paper a new access control mechanism based CP-ABE is proposed to execute the access control policies with more powerful attribute and user revocation mechanism. Major technique used here is dual encryption scheme to achieve fine grained access control. Merits of this paper are selective group key distribution in each attribute group and it manages the outsourced data securely. Major problem in execution of authorization policies and policy update support.

[2] In 2014, Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak , worked on 'Decentralized Access Control with Anonymous authentication of Data Stored in Cloud', In this Paper a new privacy preserving authentication access control scheme is introduced to provide secure cloud storage without knowing the user identity before storing the data. Key Distribution Center is used for the Decentralized Architecture. User Revocation methodology is used to revoke the user and it also restricts the user to access the data from cloud storage. Merits of user revocation scheme are prevention of replay attack and also this scheme is collusion secure and protests privacy of the user. Cloud server knows the access policy for each record stored in the cloud and it doesn't hide the attribute and access policy of a user.

[3] In 2011, Hur and Noh, worked on 'Attribute Based Access Control with Efficient Revocation in Data Outsourcing System' in this paper a new access control mechanism based CP-ABE is proposed to execute the access control policies with more powerful attribute and user revocation mechanism. Major technique used here is dual encryption scheme to achieve fine grained access control. Merits of this paper are selective group key distribution in each attribute group and it manages the outsourced data securely. Major problem in execution of authorization policies and policy update support.

[4] In 2014, Liu Zhenpeng, Zhu Xianchao,Zhang Shouhua, 'Multi authority attribute based encryption with attribute revocation' ,this paper improves revocation in the Multi authority attribute based encryption by using agent re-encryption technology, decryption outsourcing technique and time division revocation technique. The revocation can be achieved by embedding the revocation list in the cipher text and adding revocation list to authority. Decryption outsourcing methodology will reduce the user calculation. The Advantage of this scheme is resistant to collusion attack, reduces computational overhead. Multi-Authority CP-ABE Protocol needs the help of Central Authority to decrypt the ciphertext.

[5] In 2013,Xingxing Xie, Hua Ma, Jin Li, Xiaofeng Chen , worked on 'An Efficient Ciphertext-policy Attribute-based access control towards revocation in cloud computing' , In this paper a new attribute based access control scheme is used to provide secure and efficient attribute revocation with new ciphertext-policy Attribute based encryption deployment with efficient attribute and user revocation. The efficient secret sharing methodology is used to provide security. The advantage of this paper is collusion resistant, data confidentiality and also provides both forward and backward security. Main issue is method of copying with collusion attack will lack of efficiency.

III. EXISTING SYSTEM

The data confidentiality in cloud storage, less importance is given to protect users' identity privacy during those interactive protocols. It cannot tolerate arbitrarily many users collusion attack. Their solutions do not prevent the attribute disclosure in the key generation phase. This paper presents a semi anonymous privilege control scheme AnonyControl to solve both the data content privacy problem and user identity privacy issues in existing access control schemes. The usage of multiple authorities in cloud computing system, this scheme achieves oblivious cloud data access control and fine-grained user privilege control. In addition, this existing system tolerates the compromise attack towards attributes authorities. In this work encryption policy is described with a tree called access tree. Each leaf node is described by an attribute. Supporting user revocation is an important issue in the real application, and this a great challenge in the application of Anonymous Multi-Authority CP-ABE scheme.

IV. PROPOSED SYSTEM

A. Problem Formulation

1) System Models

In our proposed scheme there are four entities: They are Revocable Multi-Authority, Cloud Storage Server, Data consumer and Data owner.

Revocable Multi-Authority is responsible to revoke a user and also issue of attribute key. Each Whole Attribute set is split into N-Disjoint sets then each individual attribute is managed by N-Attribute Authority. So Each Attribute Authority only knows a part of detail.

Cloud Storage server is a storage platform which maintains the file upload and download history of each user without user identity. Cloud User is both Data Owner and Consumer of data stored in Cloud storage.

2) Threat Models

We assume that the Cloud Storage server is sometimes may not be honest so they collude with the malicious user and get the benefit of illegal data file access.

Assume sometimes the N-Attribute Authority is not trustworthy. Data consumers also not honest sometimes, they will collude with each other to get illegal access of data.

3) *Security Model*

a) Construction of Anonycontrol Scheme

This construction involves five steps

1) Setup (P_k,MK_K)

In this algorithm takes input and execute the public parameter and master key for each authority.

2) Key generates (PK, MK_k, A_u) → SKu)

Here the Algorithm allows the user to communicate with each attribute authority using public key and masterkey to produce the secret key.

3) Encrypt (PK, M, {Tp}p∈{0,...,r−1}) → (CT,VR)

This algorithm takes the input of Public key and Message and also the privilege tree set to generate the cipher text and verification set. if the user satisfies the privilege tree only able to read the file.

4) Decrypt ((PK, SKu , CT) → M

This algorithm takes public key, secret key and cipher text as input and generates the Message. if the data consumer who satisfies the verification set only can able to modify the content of the file.

To achieve full anonymity we are using Full AnonyControl scheme over normal AnonyControl scheme. In addition to that we are using the revocation concept over AnonyControl-F scheme to gain enhanced security.

Revocation AnonyControl-F scheme achieved through one out of n-oblivious transfer and making use of Multi-authority CP-ABE scheme and also through additional revocation scheme.

B. *Algorithm 1-Out-of-n Oblivious Transfer*

1) Bob randomly picks n secrets s1, . . . , sn and calculates ti as follows:

∀i ∈ {1, . . . , n} : ti = s1 ⊕· · ·⊕si−1 ⊕ Mi

2) For each i ∈ {1, . . . , n}, Bob and Alice are engaged in a 1-out-of-2 OT where Bob's first message is ti and the second message is si . Alice picks ti to receive if she wants Mi and si otherwise.

3) After Alice receives n components, she has ti = s1⊕· · ·⊕

si−1 ⊕ Mi for the i she wants and sk for k ≠ i , she can recover the Mi by

Mi = ti ⊕ si−1 ⊕ si−2 ⊕· · ·⊕s1

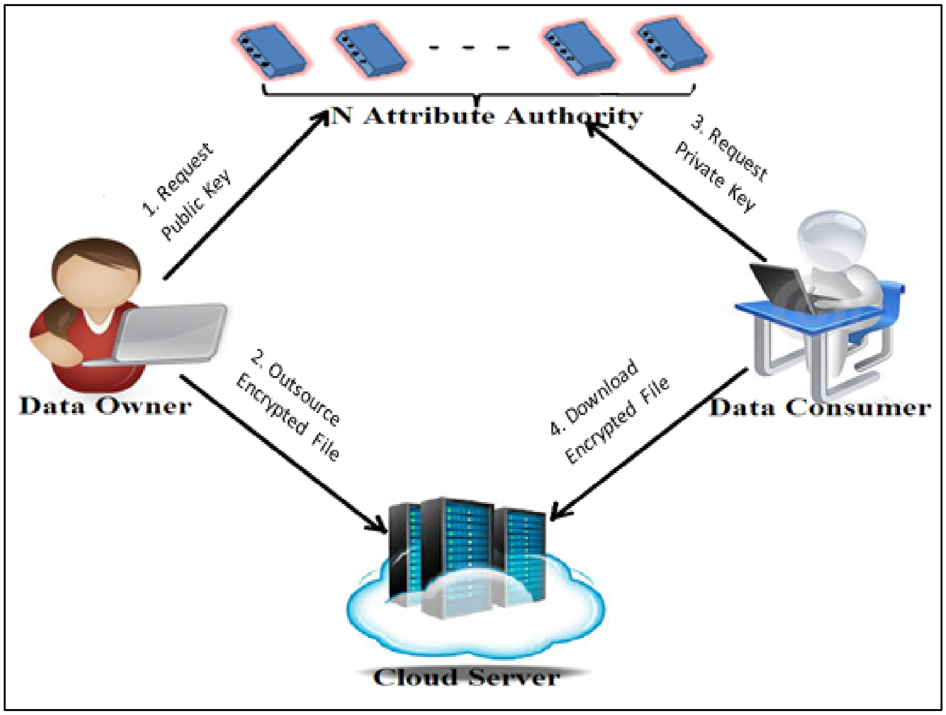
C. *Revocable Anonymous Multi-Authority-CP ABE*

A Revocable Multi-authority CP-ABE scheme is secure against static corruption of authorities. The attribute revocation problem can be solved only we need to assign a version number for each individual attribute. An attribute revocation happens when those elements associated with the revoked attribute in secret keys and Ciphertext need to be updated. When an attribute of a user is revoked from its corresponding AA, the AA generates a new version key for this revoked attribute and thus the AA generates an update key. With the update key, all the users, except the revoked user with revoked attributes can be updated its secret key thus provides a Backward Security. By using the update key, the elements associated with the revoked attribute in the Ciphertext can also be updated to the current version. Improved efficiency can be achieved only we delegate the workload of updated Ciphertext to the server by using the proxy re-encryption technique, such that the new user can also able to decrypt the previously published data, which are encrypted with the previous public keys, if they have sufficient attributes (Forward Security). Moreover, while by updating the Ciphertext, all the users need to hold only the latest secret key, rather than to keep records on all the previous secret keys.

Attribute Revocation consist of three steps they are: i. Update key Generation which is done the attribute authority. The input for the Update KeyGen Algorithm is User attribute.

1) Secret key update for non-revoked user can be done upon the usage of the update key to generate new secrete key update.
2) Ciphertext update by cloud server is done proxy re-encryption method. The cloud server takes the input of user attribute and update key from attribute authority to generate new Ciphertext for the revoked attribute.

V. SYSTEM ARCHITECTURE



A. *Modules Description*

1) *Setup*

This algorithm takes nothing as input except implicit inputs such as security parameters. Attributes authorities works together to execute the algorithm and compute a system-wide public parameter PK as well as an authority-wide public parameter y_k , and to individually compute a master key MK_k

B. *Key Generation with Revocation*

In which, Multi-Authority CP-ABE are involved for key generation. Where the user entered attribute are taken as a string and is encrypted for key. For secure encryption a key length should be length as compared with others. In which our system, the name of both consumer and data owner is taken as an attribute for key generation. Then the hash value of an attribute is taken for authority key generation. Both encrypted key and attribute hash value on generated for secure file transfer between owner and consumer. Here the attribute authority can also able to revoke an attribute.

C. *File Encryption*

In this module the ECC are involved for file encryption using generated key from previous module. The encrypted key is taken as a symmetric key for file encryption and the file were encrypted. Because of involvement of encrypted key the encryption could be more security. Here the key was generated by attribute authority. When data owner is need to upload a file into a cloud server the user will request for key for encryption. In which data owner will encrypt a file and upload it into cloud server.

D. *File Decryption*

In which the above encrypted file should be decrypted by using the same key that was used when encryption. The Encrypted file downloaded from the cloud server and is taken for decryption process. In our System there is consumer who will decrypt a file using file decryption key. Consumer will get a key by sending a file download request to authority unit. The Attribute authority will sends a file decryption key for a particular requested file.

VI. Result Analysis

A. Performance Measures

1) Time

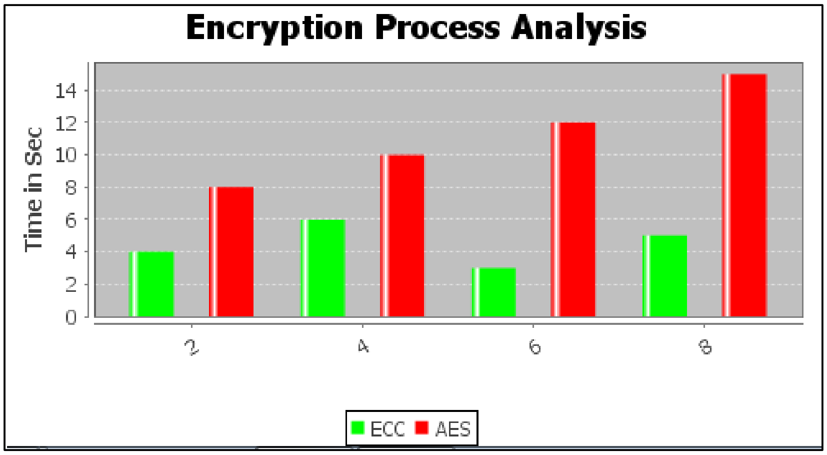


Fig. 4.1: Encryption time

Here the Encryption time of the proposed scheme using Elliptic curve cryptography algorithm with revocation method gives less time for Encryption than the existing scheme using Advance encryption standard algorithm without revocation.

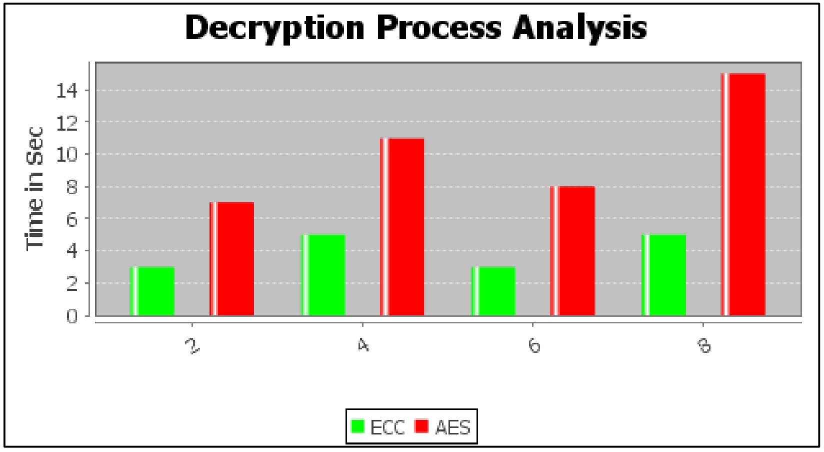


Fig. 4.2: Decryption time

Here the Decryption time of the proposed scheme using Elliptic curve cryptography algorithm with revocation gives less time for decryption than the existing scheme using Advance encryption standard algorithm without revocation method.

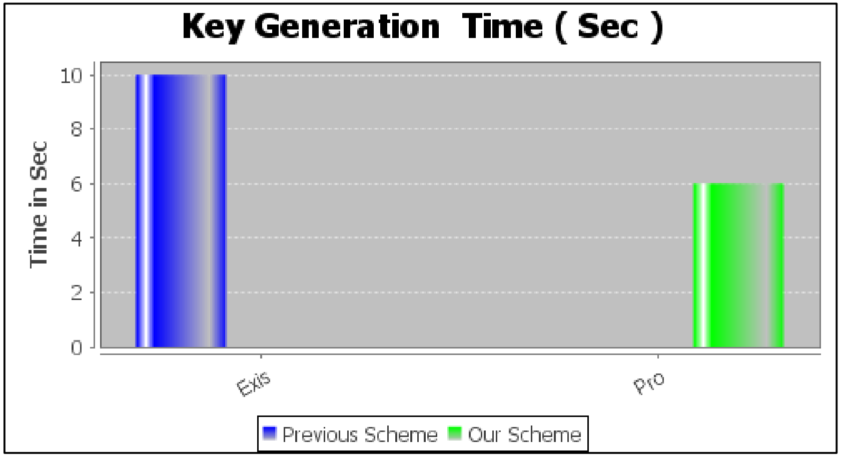


Fig. 4.3: Key Generation time

Here the Key Generation time of the proposed scheme using Elliptic curve cryptography algorithm with revocation gives less time for key generation than the existing scheme using Advance encryption standard algorithm without revocation method.

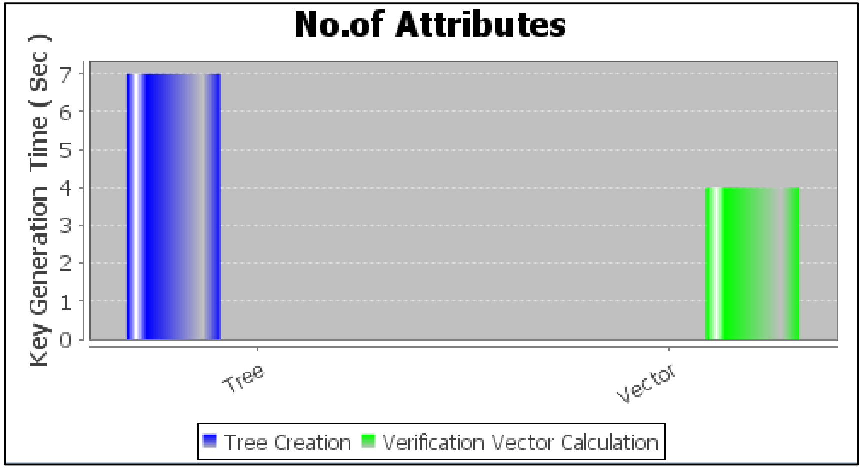


Fig. 4.4: Methodology

Here the Vector calculation of the proposed scheme using Elliptic curve cryptography algorithm with revocation gives less time for key generation than the tree calculation of the existing scheme using Advance encryption standard algorithm without revocation method.

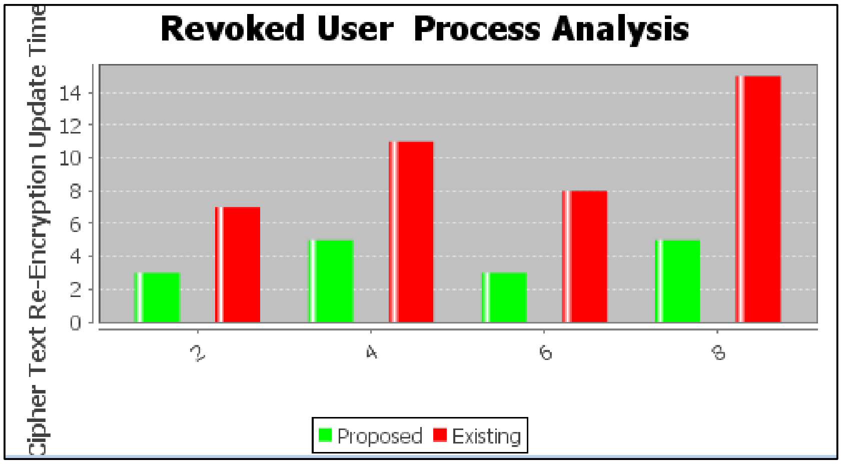


Fig. 4.5: Revocation Process time

Here the Revocation time of the proposed scheme using Elliptic curve cryptography algorithm with revocation method gives less time for Encryption than the existing scheme using Advance encryption standard algorithm without revocation.

B. Security Analysis

1) Theorem 1

Our Proposed Scheme using Elliptic curve cryptography algorithm with revocation method achieves both forward and backward security.

2) Proof

Actually the forward and backward securities are the two requirement of the attribute revocation Process.

3) Theorem 2

Our access control scheme achieves fully anonymity and collusion resistance

4) Proof

In our scheme Authority generates a set of random key parameter and shares across other authorities via secure channel.

VII. CONCLUSION

This paper proposes a revocable anonymous multi-authority CP-ABE scheme to enhance the security and also provides effective attribute revocation. The construction of our access control scheme is effective for the cloud storage environment.

ACKNOWLEDGEMENT

This work was supported in part by grants from the Dr.A.V.Ram Prasad, Principal of K.L.N.College of Engineering and also supported by grants from Dr.N.Lakshmi Narasimman, Professor & Head of Computer Science and Engineering and Ms. S.Brindha Project Guide, K.L.N.College of Engineering ,Who had helping us during preparation and also provided valuable feedback for guidance.

REFERENCES

[1] Jun beom hur and dong kun Noh(2011),"Attribute-Based Access Control with Efficient Revocation in Data Outsourcing systems", IEEE Transactions on parallel and Distribute systems, Vol:22 no.7 PP:1214-1221.

[2] Kan Yang,Xiahoua jia,(2013),"Expressive, Efficient and Revocable Data Access Control for Multi-authority cloud storage", IEEE Transaction on Parallel and Distributed Systems Vol:25,Issue:7,PP:1735-11744.

[3] Liu Zhenpeng, Zhu Xianchao, Zhang Shouhua (2014), "Multi authority attribute based encryption with attribute revocation",IEEE 17th International Conference on Computational Science and Engineering, DOI:10.1109/CSE.2014.343,PP:1872-1876.

[4] S.Yu, C.Wang, K.Ren and W.Lou,"Attribute Based Data Sharing with Attribute Revocation" (2010), Proc.5th ACM Symp. Information, Computer and Comm. Security (ASIACCS'10), pp: 261-270.

[5] Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak (2014), "Decentralized Access Control with Anonymous authentication of Data Stored in Cloud", IEEE Transactions on Parallel and Distributed Systems, 2014 VOL. 25, NO. 2, PP: 384-395.

[6] S.J.Hur and D.K.Noh (2010), "Attribute – Based Access Control with Efficient Revocation in Data Outsourcing System", IEEE Transactions on Parallel and Distributed System, DOI:10.1109/TPDS.2010.203 PP: 1045-1221.

[7] S.Jahid, P.Mittal and N.Borisov (2013), "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute Based Encryption", IEEE Transaction on Parallel and Distributed Systems Vol:24,Issue:1,PP:131-143.

[8] Tacho Jung, Xiang-Yang Li, Zhiguo Wan and Meng Wan. (2015). "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute Based encryption". IEEE Transaction on Information Forensics and Security, vol: 10 no.1, pp: 190-198.

[9] Xingxing xie,Hua ma,jin li xiaofeng chen(2015), "Multi-Authority Attribute Based Encryption scheme with revocation", (ICCCN) 24th Internal Conference on computer communication and Networks,DOI:10.1109/ICCCN.2015.7288431,PP:1-5.

[10] Yong cheng,Zhi ying wang Jun ma,Jiang-Jiang Wu,Song-zhu Mei(2013), "Efficient Revocation in cipher text- policy attribute based encryption based cryptographic cloud storage", Journal of Zhejiang University-Science (Computers & Electronics), vol:14,No:2 PP:85-97.