Received: February 25, 2017

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Secure Access Control with Dynamic Policy Updating for the Data in Cloud System

Pooja Choudhary[1]* **Jaisankar Natarajan[1]**

[1]*Computer Science and Engineering, School of Computer Science and Engineering, VIT University, Vellore, India*
* Corresponding author's Email: choudhary.pooja.23@gmail.com

Abstract: It is always an effective option for storing the data on cloud as it has advantages such as processing huge volume of data on user's request. But policy updating is one of challenging issue when attribute based encryption method is used for constructing schemes such as access control. Many techniques have been proposed for achieving secure data access control in any cloud storage system, but policy updating is always a problem. In this paper, a novel scheme is proposed to enable to access control by using method known as dynamic policy updating for the data in cloud. The focus of this paper is to develop dynamic policy updating method for the data which is stored in the cloud. This method will help the data owners to update the policy for the data which is stored in the cloud. The features of this method are that data owner can update the policy on his data and data will be encrypted according to the new policy and user will be able to download only if he has new policy which is not possible in existing methods. The drawback of traditional method was removed such as user revocation and method is made more efficient access control scheme policy update based on attribute. The results show that policy can be updated for the data stored in the cloud and revoked user cannot download the file. Only the data owner can update the policy for his data in the cloud other than data owner cannot do this.

Keywords: Cloud, Policy update, Signature generation, Signature verification, User revocation.

1. Introduction

The objective of the policies in cloud is to make sure that the providers of cloud services is according with the security requirements, business, related regulations and laws. Cloud consists of huge amount of data and it is difficult to process this data using hand database management tools. While hosting any data on cloud the data security will be one of the major concerns as service providers and this will not be fully trusted by owners of data. Attribute based encryption is emerged which is promising technique for data security end to end in cloud. And dynamic policy update method allows data owners for defining new access policies and for encrypting data under that policies, such that only data users whose attributes that satisfies the access policy can able to decrypt the data. Now days many organizations and enterprises migrate their data on cloud, the policy updating has become an important issue for data access policy can be changed by data owners dynamically. The policy updating issue has not been considered attribute based schemes in existing systems.

Attribute based encryption (ABE) which has been emerged as one of the promising technique for maintaining security from end to end in cloud. Nowadays more number of organizations and enterprises are outsourcing their data in cloud. The policy updating is one of the problems in the cloud and this issue is not considered in the existing systems. There are different challenges involved while updating the access policies for the data which is stored on cloud. The different challenges are explained as above and the method was implemented which satisfies all of these challenges.

Correctness: Data users having enough privileges having attributes can decrypt the data

which has been encrypted under the new access policies which has been provided by data owners.

Completeness: The system should be able to update the data under any new updating policy given by the data owners

Security: The system should not break any security constraints when data is encrypted under new access policy.

In the cloud system we have seen that policy update is always a problem in the cloud based system and key policy structure is discussed [1] and even cipher based text policy structure has been discussed [13]. Whatever the methods which are discussed in the above two papers will not satisfy the completeness property. But this is important which is used for delegating the key the data which was encrypted under the new access policy and also it does not satisfy the security requirements.

The proposed system features are as policy update has made possible, authorized user only can update the policy ,authorized user can upload or download the files same things are not possible for revoked user. Access policy is sent through the mails to the user in encrypted format or it is available to the user by just clicking on get access policy tab which is also in encrypted format. The results show that policy can be updated for the data stored on the cloud which was not possible in the existing methods. Many of the paper have used Attribute based encryption method but policy update was the main problem for that method which has been solved. Revoked users cannot download the file even though they have access policy which was one of the disadvantages of existing methods.

Next section gives us details about the different papers and the method which has been proposed by them. Section 3 describes about proposed architecture, modules in the project and different methods which were used to implement the system, detailed architecture diagram and different algorithms used for policy updating in cloud, section 4 includes the results of the implementation which also describe why our policy updating method is good than conventional methods and finally section 5 provides overview and then it concludes.

2. Literature survey

In this paper a new method cryptosystem was been proposed to share fine grained data which is in encrypted format which is called as Key-Policy Attribute-Based Encryption . In this system cipher texts are labelled by the group of attributes and which are associated with some private structures which are used to access and are used to control which cipher texts will be able to decrypt by a particular user. Even they have demonstrated the construction to sharing of audit-log information and broadcast encryption, the construction is used to support the private keys which are delegated by using subsumes Hierarchical Identity-Based Encryption. Problem of the proposed method is giving other party private key [1].

In this paper they have realized the present system for accessing complex data which controls the encrypted data which is known as Cipher text-based -Policy-Attribute-Based Encryption. It uses the technique which uses encrypted details protected even if the storage server is not safe. Attributes are used in describing the user credentials, and the other party which encrypts there data which uses some policy and same policy is used for decryption of data. The methods were proposed earlier and these are the traditional methods used for policy update access methods which were used to control data known as Role-Based Access Control which is necessary to protect the data from unauthorized access (RBAC). The drawback of this method is that encrypting data sharing is possible at coarse grained level. In proposed system we can update the policy for the data and data will be re encrypted according to new policy [2].

In this paper a Multi-Authority Attribute-Based Encryption was been proposed. The system which was designed consisted of that any party may become authority and no global coordination was required. But here the authors have created an initial set of common reference parameters. A party can be an authority provider after creation of public key and issuing particular private keys to particular users which were used to reflect as their attributes. No central kind of authority has been created. A new technique was been proposed which was used to prevent the collusion of attacks between different users which uses global identifiers. The drawback of this method is that it requires central authority [3].

A fully secure attribute-based encryption scheme and a fully secure (attribute-hiding) predicate encryption (PE) scheme have been proposed. To adapt the dual encryption methodology introduced by waters the results have used the novel strategies. They have constructed a scheme in composite order bilinear groups, and also it has proved the security through static assumptions. The scheme was used to support arbitrary monotone. A new approach was been proposed which uses the bilinear pairings of the notion .The bilinear paring of the notion were used for dual pairing vector spaces which was been proposed by Okamoto and Takashima .In this method there is security drawback. And the

drawback related to security constraints were resolved only authorized data owner can update policy and revoked user cannot download the files [4].

The method called Cipher text based Policy Attribute-based Encryption and this method is considered as one of the best and well known technology used for data access control in cloud. This method gives the data owners the direct access on different policies which is used to store data on cloud. Now a day it has become difficult to use CP-ABE schemes for data access control usually stored in cloud storage .As attribute based revocation is one of the major challenge. The revocable, expressive and an efficient data access control scheme have been proposed for multi-authority cloud storage systems. Here the system consist of multiple authorities exists and each authority uses attributes independently. This method was been proposed for both forward as well as backward security. The paper analysis and simulation results show that the proposed data access control scheme is secure. And in any the random oracle model it was more efficient than other methods which have been proposed previously [5].

In this paper, they have proposed a multi-authority based cipher text-policy attribute-based encryption-method which uses data access control for cloud storage. In this paper the authors had said that the proposed scheme which was used for dealing revocation which is based on attribute based revocation was used to achieve both forward as well as backward type of security. The investigation and further analysis shows that the work has adopted both bidirectional re-encryption methods while updating cipher text .So vulnerability on security appears. The method which has been proposed attack method demonstrates that the user which has been revoked can decrypt new cipher texts .The cipher text have which requires the newly secret keys for decrypting the data which is stored on cloud. In this paper for addressing the challenge of traditional methods the data owner usually does the encryption of data and then he delivers the encrypted data along with decryption keys to authorized particular users. Due to this it is difficult to manage the key involvement and complicated key management with overload on data owner's side. Authors have designed the framework to access data control usually stored in cloud. Using the proposed methodology called as Cipher text-Policy Attribute-based Encryption (CP-ABE) approach the data owner can store data on cloud safely. In the proposed scheme which consist of attribute revocation method which was been is proposed for dynamic changes of users' access privileges used in large scale systems. The analysis shows that the proposed scheme is safe and revocation is possible. It is very costly to re encrypt data under new access policy [6].

This paper characterizes different privacy problems in emerging scenarios with respect to cloud. It has discussed the various risks involved, solutions for them and open problems to ensure privacy of users who are using cloud to store data and to access the resources. The drawback this method is that it is decomposable for certain attribute [7].With the help of backward and forward derivation function a comparison based encryption was implemented. It was used to compare time in attribute based access policy. This method cannot be directly applied to the PHR which are based on cloud which has different reasons such as encryption cost grows linearly according to the attributes present in it and high communication overhead with high cost for computation. They have proposed hierarchical comparison-based encryption with improved encryption performance and has implemented policy update scheme for avoiding transmission of cipher texts and minimize overhead due to computation at data owner side. The updating cost increase linearly with the increase in number of attribute based system while in proposed system the problem of linearity has been solved [8].

In this paper a cipher policy based on attributes proxy re-encryption method was been proposed which is regarded as a notion for pre encryption. It employs the technology based on pre in attribute based encryption setting. Here proxy can change an encryption under an access policy for other encryption which is under new access policy. This method was applicable to many applications based on network such as data sharing in the network. It eliminates the problem of integrating dual system based encryption technology which has used selective proof technology. It supports any monotonic access structures which were built in a bilinear group of Composite order and improvement was done re-encryption key generation and its different phases. The problem of attribute based encryption is setting where user credential can change and cipher text is stored by third party and this problem was solved in proposed system [9]. In this paper an access control policy was enforced by giving various cryptographic key in the collaborators. Many times access policy need an update which leads to various cost at owner of data or different parties side for re-encrypting data with new key in order to verify with the new key. To remove the policy updating problem new method

known as dual header structure proposed and batch revocation because it leads to overhead for privileges that should be granted independently. And for the improvement in efficiency lazy revocation was applied to privilege revocation in a certain group where revocation request was arrived. It has efficiently managed frequent policies updating [10].

In this paper, a method for computation of signature of the encrypted message with its claim policy for the verification of claim policy has been proposed. Due to this user can modify data. In the system allows modifying the data for the users which has claimed policy and even they have not disclosed the policy to cloud service providers. The outsourced data integrity can be verified by data owner for ensuring the intact with him as well as validation is possible which was been updated by providing the new signature. The problem here was centralized storage within an organization where different users may have access to the varying level of sensitive data and problem of security constraints were resolved in proposed system [11].An Attribute based method has been approached in this paper. Policy update has always has been always a challenging issue. In this trivial implementation which allows data owners retrieve the data and even we can re-encrypt the data under the new policy. Novel scheme was been proposed in this paper which enables for efficient with an access control. The analysis always shows that the policy update is correct and secure. The problem of this method it will not allow revocation of private keys and also the ability to reflect cipher text for the most recent updates [13].

In this paper policy based attribute encryption method was been proposed. There are two issues in policy update for the data which is stored in the cloud but in this method the revocation and policy updating is always a problem. This scheme has supported a large number of attributes which will make efficient data on cloud and this scheme has proved it is statistically secure nay other scheme which has been proposed earlier [14]. A NTRU method was been proposed in this paper which is secure and as well as it verifiable scheme for any NTRU cryptosystem. And also new NTRU based decryption algorithm has been proposed which has solved the problem failure of existing NTRU method. This scheme is used for updating cipher text for the data in cloud for the policy which has been provided. The policy updating should not break security of access control system which will lead to new security constraints. In Proposed system only authorized user can update the policy for data and if the user has been revoked then he cannot download the file from the system [15]. In this paper cipher text based attribute based encryption method has been proposed to remove the problem of attribute based encryption method which has supported the user revocation as well as it has taken into consideration proxy server which can be trusted. The scheme was proved fine grained as well as secure for storing the data in cloud comparing to the other methods which has been proposed. It has the drawback of availability that is granularity for user access control between user level and system level [16].

3. Proposed arcgutecture

To remove the problem of attribute based encryption, new method has been proposed for updating the policy for the data stored in the cloud. Traditional methods had revocation and efficiency problem and even policy updating was problem of attribute based encryption. To overcome this problem new method has been proposed which is efficient for access control scheme for user revocation and update based on attribute.

Here we have considered a cloud storage where are multiple authorities are there and is in Fig.1. This architectural model consist of different things such as cloud server(server), owners of data (data owners, authorities and data consumers of data known as users.

Authority: The authorities in this system are independent of any other authorities and who are responsible for giving or defining attributes among the different users of the system. They are responsible for generation of keys (public key pair) for the other attributes and also used for generating the secret key for the various users based on the attributes.

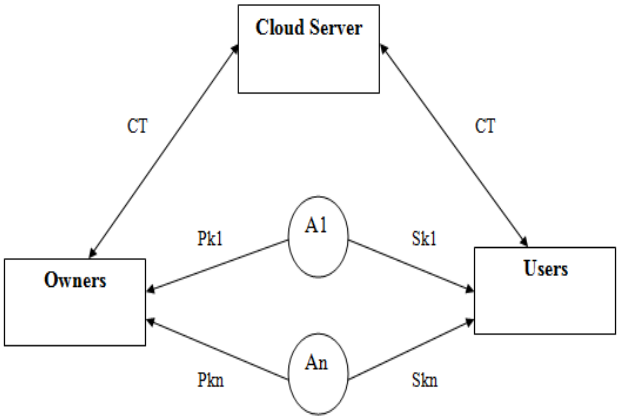

Figure.1 Architecture Design

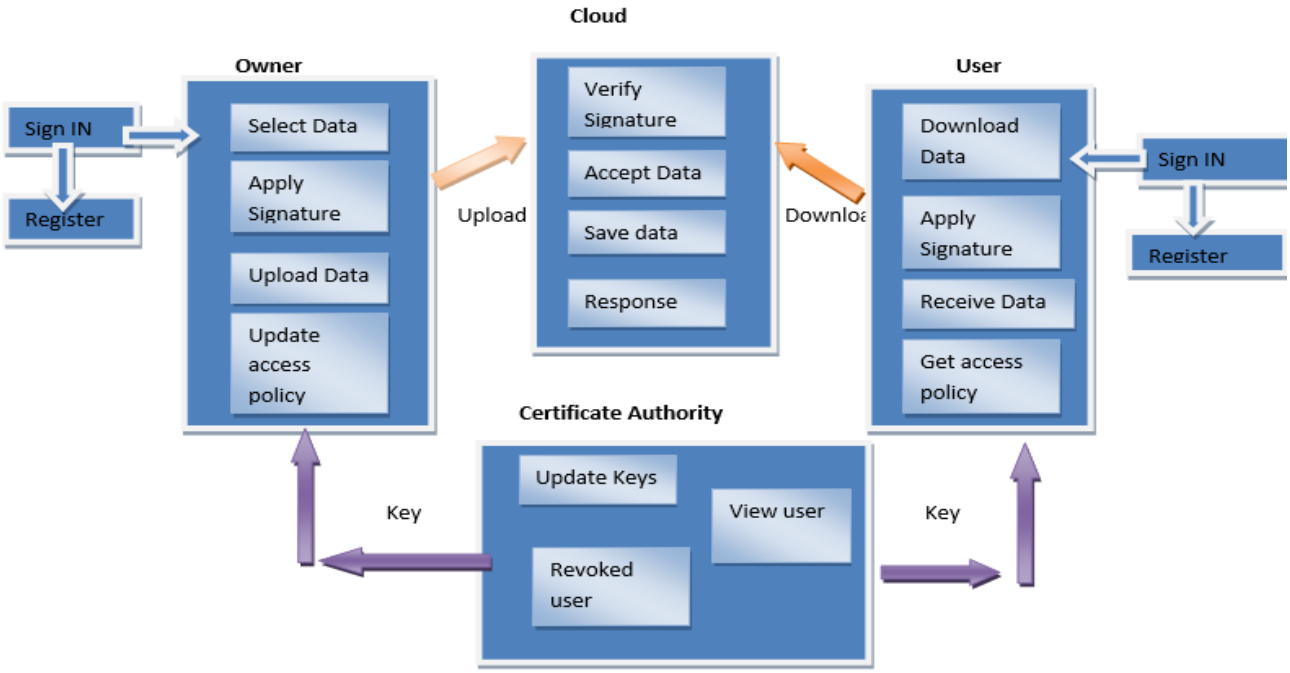

Figure.2Detailed architecture diagram

Server: It is used to store the data provided by data owners and also it gives access of the data among the different users in the system. Server can also update the cipher text from the old policies of the data to the new polices. For the same data

Data Owners: The owner's data is stored in cloud and he can define the different access policies according to his feasibility and even he can encrypt the data under any polices before storing is his data in the cloud. Only the right owner can update the policy for his data in the cloud and accordingly it updates the policy for the data which is stored in the cloud

Data Users: In this system, each user has given an identity and accordingly he can get the cipher texts from the cloud server. The decryption of data can be done using the cipher text if and only if theattributes satisfies whatever they are defined under the access policy of the cipher text.

Here user can get access policy through mail or get access policytab that is in encrypted format then that access policy is decrypted and used to download the file that is stored in the cloud.Revoked user neither can store data in cloud on can download the file from the cloud.

Figure 2 Represents the detailed architecture diagram involves various components such as data owner, data user and cloud server and administrator. Both user and owner need to register with the system and owner can select the data from his system and then he applies signature and will upload the data in the cloud according to some policy and cloud will verify the signature and it will save the data. The user can download the data only if he has the policy after the signature verification Admin can revoke the user as well as data owner, if user is revoked then he cannot download the file and if owner is revoked then he cannot upload the data to the cloud.

The steps which were followed to implement the policy update method in the cloud are as follows: All of the existing system which was been proposed earlier uses attribute based encryption method to encrypt the data but policy updating method was notimplemented. So improve this shortcoming the policy update method has been proposed to update the policy for the data which is stored in the cloud. The policy can be updated by the data owner itself. Other data owner cannot update the policy of the file which is owned by other owner. The admin can revoke the existing users. The revoked user cannot download the file through the get access policy method. Once the policy is updated by the data owner the user cannot download the file through the get access policy method. The policy will be received to the user in encrypted format. He can get the policy through get access policy method or through the mail. The signature generation and verification algorithms are used to while updating the policies to the specific file in the cloud and dynamic update policy update method has been implemented. So above are the some of the algorithms which are used to implement the Dynamic access policy update in the cloud.

The steps that were followed to implement the system are as follows:
Step1: Generate File
Select File from local system f={f1,f2,f3,…fn}.
Step2: Encrypt File
Using Encryption for file (C_f),=(E_c,key,f).
Step3: Generate Access policy
Generate Access policy (A_{cc}) for each file (f).
Step4: Upload
Upload Encrypt file (C_f) and Access policy (A_{cc}) upload by data owner.
Step5: Update Access policy
Generate Update access policy (A_{ccup})and Select File (C_f) from cloud
Update access policy defends on file
Step6: Update and change access policy
Update Access policy ($A_{ccup,}$ C_f)

Signature generation
Select any random variables a, rM1, rR1, ms1,mx1, mP, mT, mEand pseudo code is given below
start
A1 ← rE gg*
*A2 ← (rE * hT1)+ hT*
A3 ← (rE hT2) + hT*
St1 ← rM1 (EPri + keT)*
*ACX1 ((a2^rM1) *A mod N).mod N*
*BCX1 ((w^ rR1 mod l) *B) mod l*
*Tt2 ← rR1 * EPri*
Y1 ← mE gg*
Y2 ← (mx1 gg)+(hT1 * mE)*
Y3 ← (mx1 gg)+(hT2* mE)*
*Vrv ← ((BCX1^~mP mod l) *(w^mT mod l))))mod l*
*Vpk ← ((a2^ms1 mod N) *(a1^mx1 mod N)).mod(N))*(ACX1^~mP mod N)).mod(N))*
V ←Y1+Y2+Y3
E ← A1+ A2+A3
reste ←ACX1+ BCX1+ Vrv V + Vpk and then set the value of c as follows
c ← f(msg+ E + reste)
Construct the numbers as following
*us1 ← (s+ms1) *c*
*tat1 ← (t+mT) *c*
*ux1 ← (x +mx1) * c*
tE3 ← (rE+mE) c) mod(o)*
*tauP ← (EPri + mP) *c*
All these values are returned
as(tauP,tat1,tE3,ACX1,BCX1,A1,A2,A3 ,c,ux1,us1
End

Signature verification
Input to the algorithm are as follows which includes system parameters are as follows
A1,A2,A3,ACX1,BCX1,c,ux1,us1,tauP,tat1,tE3 and output generated may be true or false.
Compute the following values
a0a1 ← ((a0^c mod N)(a1 ^ ux1 mod N))mod N*
a2A ← ((a2^us1 mod N)(ACX1^ ~tE3 mod N)mod N*
tE3 ← (c(expKe+tauP);*
tauEG ← tE3 gg*
*Vpk ← (a0a1 * a2A)mod N*
Bw ← ((b^c mod l)(w^tat1 mod l))mod l*
Vrv ← (bw(BCX1^~tauP mod l)) mod l*
E ← A1+ A2+A3
V ← Y1+Y2+Y3
rem ← ACX1+ BCX1+ V + Vpk+ Vrv
if (c ← f(E + rem + msg))
Return True
else
Return False
End
Modules
1. Data owner
2. Data user
3. Certificate Authority
4. Cloud server

Data owner:
This module uses for upload data to cloud using certificate and access policy. This module helps to encrypt the file using algorithm.
Data user:
Download file with adding access policy and apply signature
Certificate Authority:
Giving authorized certificate to all data owner and data user. Revoke user.
Cloud server:
- Check certificate or security
- Accept file from authorized data owner

Response to data user and data owners.

4. Results and discussion

We have seen that policy updating has been always a problem in Attribute based encryption system so we have developed the new method to remove this problem. Group Signature algorithm is used for user creation and user revocation. In proposed system only authorized user can update or change the access policy and for revoked user it is not possible to upload or download the file from cloud. Authentication provide for both user and owner. Access policy is used by both data owner and data user. Dynamic access policy method is used for update access policy.

To remove the problem of existing systems such as the data which is newly encrypted should not be decrypted by user's key that has been revoked from

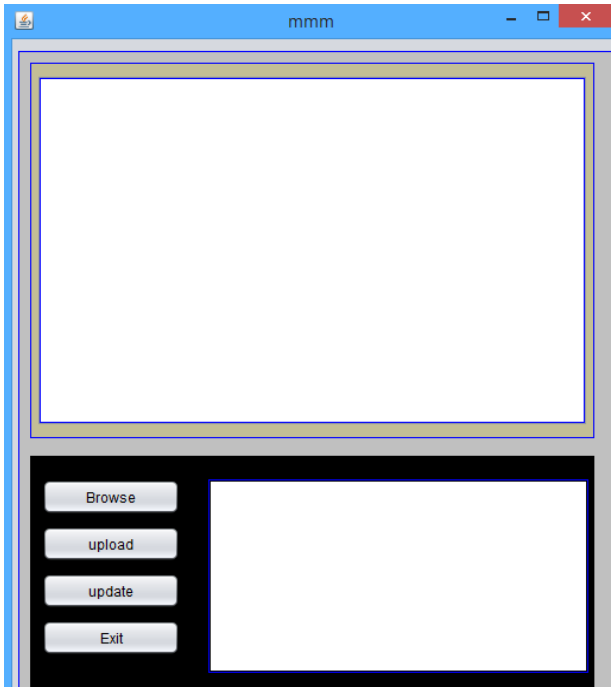

Figure3 Data owner storing file into cloud

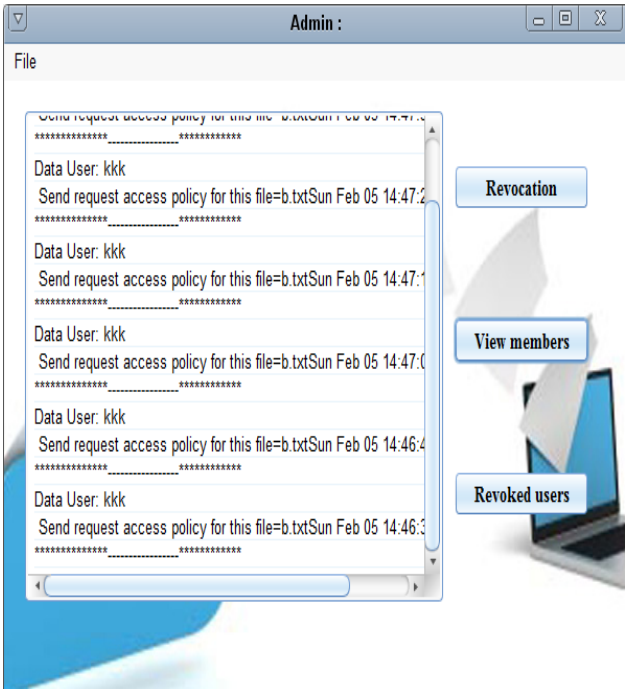

Figure.4 Admin can view and revoke members

the system. So problem of revocation has been solved. No central Authority is required and updating cost does not increase linearly as in attribute based encryption methods. Data owner can update their data under new policy if he wants any type of access restrictions to be applied on his data for the user who can access their data.

The problem of attribute based encryption is setting where user credential can change and cipher text is stored by third party and this problem was solved in our method. Previous work proposed were having security problems such as revoked user can be able to download the file or unknown data owner can update the policy which was breaking the security constraints .So this problem is solved in our system constraints. The problem of granularity was been solved on level of access on data for user level and system level.

Some of the screenshots has been added. In the proposed system both user and data owner has to register. After registering with the system data owner can store the data on the cloud, Fig.3 shows how the data owner will browse the file from laptop and store that file in cloud. Firstly, data owners used to sign in with the cloud after that itself they can store the files on the cloud. While storing the file on cloud it will ask for policy need to enter that policy and the data will be stored in encrypted format in the cloud. He can update the policy for the data whenever required; only authorized owner can update the policy for the data stored on cloud

Admin can view the list of data owners and data users. Figure 4 shows the list of files stored in the

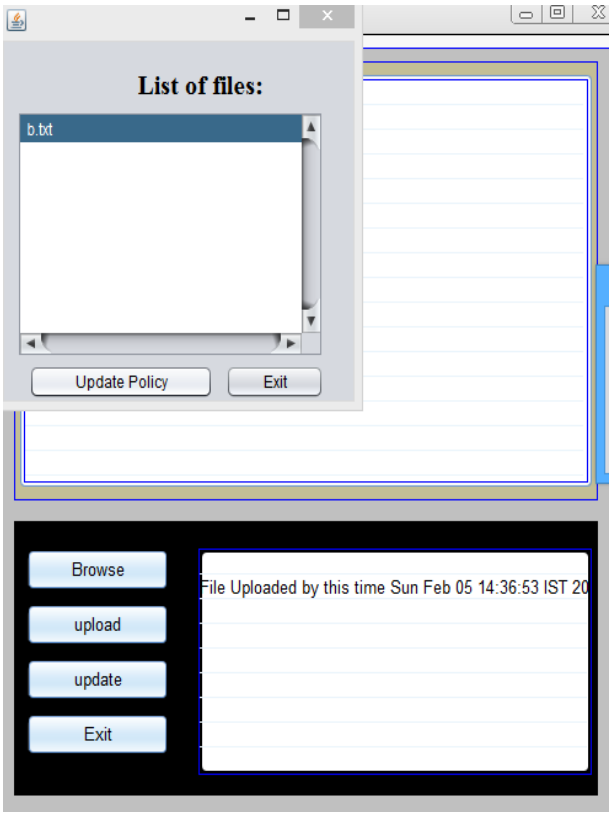

Figure.5 Admin can view and revoke members

cloud, admin is able to revoke the both data owner as well as data user. Revoked user doesn't have permission to get access policy to update the access policy in the cloud. The message will be displayed that this user has been revoked. Admin will get all the details whatever is done on the data stored in the cloud, we

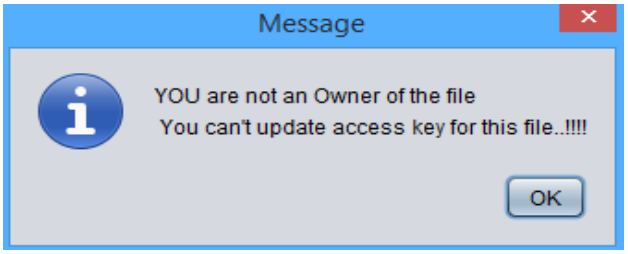

Figure.6 Other than data owner tries to update the access key

Figure.7 Data user can get access policy and download the file from cloud

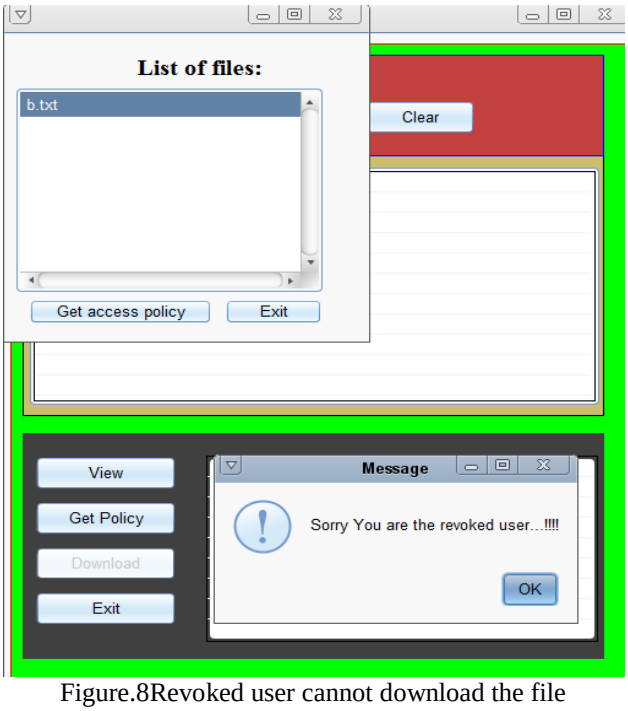

Figure.8Revoked user cannot download the file

can see that in Fig.4 users has sent request to get access for the policy so that he can download the data stored on cloud.

Figure 5 shows that data owner can update the policy for the data which is stored on the cloud with new access policy and only the right data owner can do this update. When he tries to update the access policy for the file then he is able to see all the files which are stored in the cloud. After that he has to select his file and then click on update policy tab and then he has to specify the policy for the file. It also shows that whenever data owner store the file on the cloud, after uploading the file it will show message that the file has been successfully updated.

If other than data owner updates policy then it will display message that you are not owner of this file as shown in Fig.6. So here we have solved the problem related to security, only authorized user can update the policy for his data.

Figure 7 shows how to get the policy from the data owner and download the file. The policy will be encrypted format and data user can get from the above screenshot as well through mail. So whenever data user wants to download the file stored on cloud he can download the file only if he has the new policy in case if policy is updated by the data owner.And the content of the file will be visible to him as well as he can see message that file is downloaded from the cloud.

Figure 8 shows that revoked user cannot get an access policy he will get the message that you are revoked from the system and now he cannot download the file as admin has revoked that user from the system.

So admin can revoke both data users as well as data owner, in this way problem of revocation has been solved in the proposed system.

5. Conclusion and future enhancement

From this paper we have seen that policy updating was always a problem in the cloud. So to overcome this problem a new method was implemented. In many of the paper we have seen that attribute based encryption method was used but has the policy update problem. Through the implemented system model we can update the policy for the data stored in the cloud and it also ensures that no other cloud owner can update the policy for the other file i.e. only data owner can update the policy. The Administrator can revoke the users and he will become unauthorised user for the data and even he cannot download the data with the old access policy. Even one more method has been

proposed which enable the data owners to check the integrity and cipher text updating is done properly.

A policy update algorithm has been designed for different types of access policy. The method has enabled the data owners for checking the cipher text correctness for policy updating. The scheme was analysed in various terms such as correctness, performance, completeness and in security. As compared to other methods its efficiency of access control scheme for user revocation and update based on attribute. We can outsource the policy update to the cloud server to minimize the communication overhead and computation overhead.

Acknowledgments

The project is completed successfully under the guidance received from my quarters. I would like to thanks and gratitude to VIT University for giving me this opportunity.

My very first thanks is to Prof. Jaisankar Natarajan (Professor Scope) for his guidance and support during the completion of my project. His valuable advices helped me a lot to overcome the difficulties which I faced when I was doing project. With his advices and my dedication towards the project made the project to complete successfully. Finally I want to thanks to whole VIT University for giving me opportunity to study and complete my M.Tech from such a good University under the guidance of good faculty.

References

[1]V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute based encryption for fine grained access control of encrypted data", In: P*roc. 13th ACM Conference Computer and Communication*, pp. 89-98, 2006.

[2]A. Sahai, J. Bethencourt, and B. Waters, "Cipher text policy attribute based encryption", In:*Proc. IEEE Symp. Security privacy*, pp.321-34, 2007.

[3]B. Waters and A.B. Lewko, "Decentralizing attribute based encryption", In *Proc. 30th Annual International Conference*, pp. 568-588, 2011.

[4]T. Okamotp, A.B. Lewko, K. Takashimaand, and B. Waters, "Fully secure functional encryption: Attribute based encryption and inner product encryption", In: *Proc. 29th ANNU. International Conf. Theory Appl. Cryptographic Tech.*, pp.62-91, 2010.

[5]X. Jia, K.K. Ren, K. Yang, B. Zhang and R. Xie, "DACMACCS: Effective data access control for multi authority cloud storage systems*", IEEE Trans. Informs Forensics Security*, Vol 8, No. 11,pp.1790-1801, 2013.

[6]X. Jia, K. Ren and K. Yang, "Attribute based fine grained access control efficient revocation in cloud storage systems", In: *Proc. 8th ACM SIGSAC Sympony Information, Computer and communication Security*,pp.523-528,2013.

[7]S. De Captani di Vimercati, S. Foresti, and P. Samarati, "Managing and accessing data in cloud: Privacy risks and approaches", In: *Proc.*7th*International Journal on Risks and Security of Internet and System (CRISIS)*, pp 1-9, 2012.

[8]X. Liu, T. Peng, and J. Wu, and Q. Lin, "Dynamic access policy in cloud based personal health record (PHR) systems", *Information Sciences*, Vol 379, pp. 62-81,2017.

[9]K. Liang, M.H. Au, K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, "A secure and efficient cipher text policy attribute based proxy re-encryption for cloud data sharing", *Future generation Computer Systems*, Vol. 52, pp. 95-108,2015.

[10]J. Weiyu, W. Zhan, L. Limin, and G. Neng, "Towards efficient update of access control policy for cryptographic cloud storage", In *China Communications*, Vol.12, No. 12,pp.43-52,2015.

[11]S. R. Krishnan, A. Krishna, and P. Laxmi, "Efficient framework for verifiable access control based dynamic data updates in public cloud", In: *Proc. of the International Conference ICDCIT*, 2017.

[12]A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic crendentials and cipher text delegation for attribute based encryption", In: *Proc. of the International Cryptol Conference*, pp.199-217, 2012.

[13]K. Yang, X. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud", *IEEE Transactions on Parallel and Distributed Systems*, Vol 26, No. 12, pp.3461-3470, 2015.

[14]Z. Liu, Z.L. Jiang, X. Wang, S.M. Yiu, C. Zhang, and X. Zhao, "Dynamic attribute based access contol in cloud storage systems", *IEEE Trustom/BigDataSE/ISPA*, pp.129-137, 2016.

[15]C. Hiu, W. Li, X. Cheng, J. Yu, S. Wang, R. Bie, "A secure and verifiable access control scheme for big data storage in cloud", *IEEE Transactions on Big Data*, Vol PP, No.99,pp 1-14, 2017.

[16]N. Vaanchig, W. Chen and Z. Qin, "Ciphertext-policy attribute-based access control with

effective user revocation for cloud data sharing system," In *Proc. of the International Conference on Advanced Cloud and Big Data (CBD*), pp. 186-193, 2016.