International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

Reducing Overhead Costs to Data Owners with Data Confidentiality in Cloud Computing Using Encryption Technique

Geetanjali Dadi [1], Amarendra Kothalanka [2]

[1]*Student, computer science and engineering, Dadi Institute of Engineering & Tech, Andhra Pradesh, India*
[2]*Vice Principal, Department of computer science, Dadi Institute of Engineering & Tech, A.P, India*

Abstract - *Cloud computing is to place an important role for sharing data through a group of members. While sharing data with a group of people, privacy and security of shared data is of more concern. To provide security and privacy of data the cloud technologies provides encryption of stored data. However, whereas encryption assures the confidentiality of the data against the cloud, the use of conventional encryption approaches is not sufficient to support the enforcement of fine-grained organizational access control policies. In this paper we have proposed secret key share signature schema for the verification of users and prime order Xor group key generation is used for the generation of group key. For the purpose of data encryption and decryption we are using advanced encryption standard. By implementing those concepts we can provide authentication of users and also provide data security in the cloud.*

Key Words: **Privacy, identity, cloud computing, encryption, access control.**

1. INTRODUCTION

To provide security of data in the cloud, technology place an important role. So that many approaches are mitigate these concerned for using the concept of cryptography. In the cryptography approach, we are performing encryption and decryption of cloud storage data. So that to provide security and privacy of cloud data, there are too many techniques available. By improving sharing of data through the network we can provide more efficiency. By using those techniques we can provide more security and privacy of cloud storage data. However so many encryption approaches are not sufficient to provide confidentiality of cloud data. Some of the encryption approaches are not sufficient to support the cryptography technology policies. In the cloud storage service encrypted data is of critical requirement in order to utilize selective data sharing among the users. So, by implementing the identity based technique we provide more secure data in the cloud storage.

Approaches based on encryption of shared information are the main concepts in cloud technology for providing security and privacy of cloud technology for stored data. By implementing encryption process in cloud technology we can improve the performance of cloud storage. We provide security of data by implementing encryption process of cryptography technique. Basically the cryptography technique can be categorized in to two types i.e., symmetric key and asymmetric key cryptography technique. By implementing those concepts we can improve the security and privacy of cloud storage data. In the symmetric key cryptography, we are using single for the encryption and decryption of cloud storage data. In the asymmetric key cryptography technique, private key is used for the encryption process and public key for the decryption process. In this paper, we are implementing symmetric key cryptography technique for performing encryption and decryption of data in the cloud.

Authentication of users is crucial in a cloud. In this authentication process, each user can be extensively authenticated by the cloud.So, to perform the authentication process we are implementing signature generation process. By implementing signature generation process each user will be extensively authenticated by the cloud, and then we can perform the data encryption and decryption process. In this paper, we are implementing sharing of keys between the cloud and users. By using those keys the trusted centre will generate signature by using message digest one way- hash function. After that, trusted centre will send those signatures to individual users in the cloud. Each user will retrieve that signature and again generate signature. After generating a signature each user will compare both the signatures and verify them, hence allowing only authenticated users in the cloud. So, by implementing signature generation process the cloud contains only the authenticated group member.

By implementing the encryption approach in cloud technologies, there have been proposed some fine grained access control over encrypted data. So, by implementing those approaches we can group the data items and perform the encryption of those data items. By performing

the encryption of data items we are using different type of symmetric keys. By using those symmetric keys users can only perform the encryption and decryption of cloud data. There are many techniques available in the information technology for the generation of symmetric keys. In this paper, also used one of those techniques for the generation of symmetric key to encrypt and decrypt the cloud data.

The rest of the paper is organized as follows. Section 2 describes in detail related work of proposed system. Section 3 is to provide details of existing system. In Section 4 provides a detailed description of proposed system for the generation of signature, generation secret key of group members and file encryption, decryption process.. Section 5 is used to specify the result analysis. Section 6 describes the conclusion of our paper. Section 7 describes reference of the proposed system.

2. RELATED WORK

In encryption approach have proposed broadcast key management schema [1][2][3] address some of the limitations i.e., as the data owner does not keep a copy of the data, whenever user dynamic change, data owner needs to download the cloud data and again re-encrypt the data items by using a new key. So, this process must be applied to all data items in cloud encrypted with the same key. This is inefficient when it contains large set of data. Another approach based on the data encryption have propose the fine grained access control [4][5] of encrypted cloud data. By implementing fine-grained access control we can encrypt a group of data items and also use the symmetric key approach. So that users only give those keys to perform the encryption and decryption of cloud data.
Another approach of encryption process is a two layer encryption [6] that is used to perform the encryption of a group of data items in cloud. By implementing this approach the data owner will perform coarse-grained encryption over data in order to provide confidentiality of cloud data. So, the two- layer encryption is not a new concept but it combines both the concepts of fine-grained encryption and symmetric approach. However the way to perform coarse and fine-grained encryption is a novel concept and provides better solution than the existing solution based on two-layer encryption. In this section, we first introduce broadcast encryption (BE) schemes [7], [8] and oblivious commitment based envelope (OCBE) protocols [9]. We present an abstract view of the Fig. 1. Traditional approach.

Main algorithms of those protocols and then describe how we use them to build our privacy-preserving attribute based group key management (PP AB-GKM) scheme [10].

3. EXISTING SYSTEM

In the existing system, sharing data among a group of people through cloud is difficult for the data owners. Under such approaches, data owners are in charge of encrypting the data before uploading them on the cloud and re-encrypting the data whenever user credentials change. Data owners thus incur high communication and computation costs. The implementation of this approach has several limitations. Following are the some of the limitations:

1. As the data owner does not keep a copy of the data, whenever user dynamics change, the data owner needs to download and decrypt the data, re-encrypt it with the new keys, and upload the encrypted data. The user dynamics refers to the operation of adding or revoking users. Notice that this process must be applied to all the data items encrypted with the same key. This is inefficient when the data set to be re-encrypted is large.

2. In order to issue the new keys to the users, the data owner needs to establish private communication channels with users.

3. The privacy of the identity attributes of the users is not taken into account. Therefore the cloud can learn sensitive information about the users and their organization.

4. They are either unable or inefficient in supporting fine-grained ABAC policies.

4.PROPOSED SYSTEM

Now-a-days, security and privacy are of great concern in cloud technology for data storage. So, in the implementation of the existing approach, encryption of stored data can be a difficult task. However implementation of an encryption process assures confidentiality of data in a cloud these conventional approaches are insufficient to support the enforcement of fine-grained organizational access control policies. That is, if there is any change in the user credentials, the data owner will have to create a new key and re-encrypt the data. So, this approach incurs the data owner high communication and computation cost. So, this problem can be overcome by implementing the proposed system. The proposed system mainly contains three concepts i.e., signature generation, group key generation and encryption of the stored data. The implementation procedure of those concepts are as follows:

Secret key share signature schema:

In this process, the user and the trusted centre will communicate with each other. By implementing this approach the trusted centre will generate signature for each user for the purpose of authentication. After performing authentication each user will get one secret key for the decryption process and secret key common for all group members. The implementation process secret key share signature schema as follows:

1. Each user select two prime number that is P, G and choose one private key a.

2. Each user calculate public key base on this formula pub=g^a mod P

3. After calculating public keys the users will send those public keys to trusted center.

4. The trusted center randomly choose P_i, g_i and private keys of each users i.e .,a_i.

5. After choosing the values the trusted center will generate public key of each users by using this formula.

   Pub=g_i^{ai} mod P_i

6. After generating public keys of each user the trusted center will send those keys to individual users.

7. The users retrieve the public key coming from the trusted center and calculate shared key by using this formula.

   Shared key=pub^a mod P

8. After generating shared key of individual users, it will be sent to trusted center.

9. The trusted center will retrieve those shared key and calculate group key by using this formula.

   Secret key=$sharedkey_1$ ^$sharedkey_2$^….. ^$sharedkey_n$.

10. Before sending secret key the trusted center will generate signature for individual users by using this formula.

    Val=secret key ^ shared key_i
    Sig=hash (Val)

11. After generating signature the trusted center will send to individual users.

12. The users retrieve signature and again generate signature compare both signatures.
    If both are equal user will get the secret key.

13. The trusted center will also send that secret data owner.

Prime order Xor group key generation schema:

After completion of authentication process the trusted center again generate group key by using the following process:

1.After the completion of authentication, each user randomly generate secret id(P_i), secret share(S_i) and those values sent to trusted center.

2.The trusted center will retrieve those value from the user and randomly generate a group key.

3.After generating a group key the trusted center will generate shared values of each users by using following formula.

$x_i = k / (P_i \wedge S_i)$
$y_i = k \bmod (P_i \wedge S_i)$

4.The generated secret shares(x_i,y_i) of sent to individual users .

5.Each user will retrieve secret share and get secret key by using following formula

Secret key=$x_i * ((P_i \wedge S_i) + y_i$

By performing this process all users will get the same secret key. Before sending secret shares the trusted center will also send secret key to data owner for the purpose second time encryption data.

File upload and encryption: The data owner will upload the file into cloud service. Before uploading file the data owner will retrieve all secret keys from the trusted centre. Here the data owner will encrypt the uploaded file two times. thereby improving the security and privacy of the stored data. For performing encryption process the data owner will use advanced encryption standard for getting cipher data. After performing encryption process the data owner will store the data in the cloud service.

File download and decryption: If user wants to retrieve any file from the cloud service and get the selected file in the form of cipher data, After retrieving the file content the user will perform decryption process for two times and get the original plain text. By performing decryption

process the user will use advanced encryption standard decryption process and get the plain text.

5. EXPERIMENT RESULT

In this section we first present experiment result of the proposed system. The implementation of proposed system is done using the java language. By using that language we specify the functionality of proposed system. The following screenshot specify the implementation procedure of proposed system.

The above screenshot shows the registration process of each user in the cloud. By entering the personal details of each user, one can be registered. Once the user is registered, all his/her details are stored in the database. All the registered users can login using the username and password given at the time of registration. Provide username and password of each user. Once signed-in, the user can perform the functionalities of the proposed system.

The above screenshot shows the generation of public key. By using the values of p, g and private keys we can generate public key. Here p and g are prime numbers. After calculating public key that key is sent to the trusted centre.

The above screenshot shows the retrieval of public keys. The trusted center will retrieve all public keys sent by group members in the cloud.The above screenshot shows the generation of public key for users. The trusted center will retrieve public keys from the users and generate public keys for users by using the those public keys.

The above screenshot shows the generation of shared key. Each user will generate a shared by using the public key sent by the trusted center. By using that public key, each user will calculate shared key and send it to the trusted center.

The above screenshot shows the generation of shared key once the shared key is generated it is sent to the user

The screenshot shoes the authentication of user.once the user is authenticated ,will be allowed to upload a file after creating a few keys.

The screenshot shows the generation of shared id and secret share. Each user will generate secret id and secret share randomly and send to trusted center.

The screenshot shows the retrieval of secret ids and secret shares. The trusted center will retrieve the secret ids and secret shares from the users.

The above screenshot specifies the generation of secret points of individual users. The trusted center will retrieve the secret ids and secret share from the users. By using those value we can generate secret points of individual user.

The above screenshot specifies the upload process of a file. The data owner will upload the stored file and encrypt that file. After the encryption of the file, the data owner will store it cloud.

The above screenshot shows the successful encryption of the file and data storage in the cloud.

The above screenshot specifies the successful encrption and decryption of the file and stoage lolcation of the file.

6. CONCLUSION

The proposed system is used to provide security and privacy of cloud stored data and also perform the access credential of users. By performing that functionality we have mainly proposed three concepts i.e., secret key share signature schema, prime order xor group key generation and advanced encryption standard for encryption and decryption of data stored in cloud. So, by implementing those concepts we can perform authentication of users in group and also generate group keys. we are using advanced encryption standard for the process of encryption and decryption. Here the file upload and encryption process can be done by data owner and file download and decryption process can be done by users. By implementing those concepts we can provide more security and privacy of cloud data.

REFERENCES

[1] N. Shang, M. Nabeel, F. Paci, and E. Bertino, “A Privacy-Preserving Approach to Policy-Based Content Dissemination,” Proc. IEEE 26th Int’l Conf. Data Eng. (ICDE ’10), 2010.

[2] M.Nabeel, E. Bertino, M. Kantarcioglu, and B.M. Thuraisingham, “Towards Privacy Preserving Access Control in the Cloud,” Proc Seventh Int’l Conf. Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom ’11), pp. 172-180, 2011.

[3] M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Trans. Knowledge.

[4]. E. Bertino and E. Ferrari, "Secure and Selective Dissemination of XML Documents," ACM Trans. Information and System Security, vol. 5, no. 3, pp. 290-321, 2002.

BIOGRAPHIES

Geetanjali Dadi
Student of M.Tech,
Dadi Institute Of Engineering & Technology,
Anakapalli.AndhraPradesh,India.

Amarendra Kothalanka,
Vice Principal & Professor,
Department of CSE,
Dadi Institute of Engineering & Technology, NH-5, Anakapalle,
Visakhapatnam-531002,
Andhra Pradesh, INDIA