ISSN:0975-9646

Multi-Level Encryption Mechanism for Access Control Over Cloud Data

T. Kavitha B. Narendra C. Sushama S. Shiva Prakash

Dept. of CSSE, Sree Vidyanikethan Engineering College, A. Rangampet,
Tirupati, AP, INDIA

Abstract- Data storage and accessibility through remote places is becoming the challenging task in the recent days. The amount of data need to be stored is increasing day to day, number of people to be allowed to use the information and locations are also increasing. Cloud computing is the well and emerging technology used by the individuals, entrepreneurs and organizations for this purpose. Cloud technology provides virtual storage of data and it can be accessed by the data owner or any others with the privileges of the data owner. With the traditional methods of information storage accessibility of data is very less. Cloud data storage has taken a revolution in the information storage and accessibility from remote places with less infrastructure. However the issues concern with cloud data storage mechanism are: data privacy, data loss and threats. Here we proposed a secured multi-level encryption mechanism for privacy preserved access control over cloud data.

Key Words: cloud server, Access control policy, Encryption, Fine-grained access

I. INTRODUCTION

Data storage and accessibility through remote places is becoming the essential part of the current world. Cloud storage mechanism is the emerging technology people are using now a days for this purpose. Using the cloud data storage information can be stored and viewed when required from any place with less infrastructure, sometimes even with mobile phones also. Security and privacy of information are the major concerns with the cloud data storage. However we have so many encryption mechanisms to protect our data, these encryption mechanisms can assure the confidentiality of the data, but the use of general traditional encryption mechanism may not sufficient. Most of the organizations now a days are enforcing access control policies (ACP's).

In traditional data privacy mechanism the entire system has to depend on the cloud server for protection by which, any unexpected privilege growth may expose all the data. In a shared cloud storage mechanism data will be stored in one physical storage but virtually it will be stored in different machines. Coming to availability of data we have a number of cryptographic mechanisms through which a third party will take care of data security by providing files to the data users without loss of data or without loose of data owners privacy. Data sharing is the major functionality of cloud computing. The thought-provoking task here is that how data owners will provide access rights to different kinds of data owners to view the encrypted data. The general method is users can download the files, decrypt them then share the data with others, but it losses the value of cloud storage mechanism. For this reason we should provide a mechanism for directly accessing the data from the cloud based on the access rights given to the data user. Of course providing partial access to the cloud data by providing different kinds of access right is not a simple task.

One mechanism to provide access to data users is to use fain-grained encryption mechanisms in which data items with similar kind of access control polices will be encrypted with a group of symmetric key. Now data owners will share these keys with the users based on the data items they are allowed to use. Drawback with this approach is maintaining several number of keys for the data items. However enhanced mechanism have been proposed to reduce the number of keys to be distributed by establishing the relationship between data items. It has some drawbacks such as, whenever a data user is revoked the owner has to download the complete data, decrypt it, re-encrypt and upload to the cloud, in order to distribute new encryption keys through the users owner has to establish a private secured connection with the users, all these issues reflect the cost inefficiency of the mechanism. In the recent days some broadcast key management schemes were proposed which will resolve some of these problems, which we used to refer as single level encryption mechanisms. A better mechanism for this is proposed in the form of multi-level encryption mechanism in which the data owner will perform a coarse-grained encryption at the owner level before hosting the data on to the cloud environment. The cloud server will perform fine grained encryption over the encrypted data received from the owner. Here the approach we used is the existing one only but the novel interesting thing here is how we applied the encryption mechanism at the cloud by identifying the relationship between various attributes of the data received.

A typical thing in implementing the multi-level encryption is how to decompose the access control policies (ACP's) to establish relationship among the data to provide new encryption mechanism without losing the data secrecy at the cloud level. While decomposing the access control policies (ACP's) it should be noted that the confidentiality of the data from the cloud environment should be maintained with less number of attributes. The decomposition should be done such that the union of all the sub access control policies (ACP's) should give the original access control policy (ACP). The data owner will encrypt the data first at owner level with one set of access control policies (ACP's), then cloud server will perform all other encryptions based on the relationship among the various attributes with the other set of access control policies (ACP's). At the user level the data user has to apply two decompositions one for the encryption performed by the cloud server another one for the encryption performed by the data owner. Advantage with this mechanism is that when the data user changes owner side encryption need not be redone, only cloud side encryption need to be changed with a new set of keys. No data transmission is needed between the data owner and the cloud server. Another advantage with this mechanism is that no need to distribute the secret keys among the users, it's enough to make teach them how to generate the secret key.

II. OVERVIEW

The existing traditional single level encryption policy uses broadcasting mechanism and group key management. The broadcast encryption is simply the process of generating some public keys broadcasting those among all the registered users along with the secret of generating private keys. Here transfer of keys is public and it is easy for the data owner to provide the keys. No need to replicate the secret key generation mechanism to the users whenever the data is modified. Broadcast encryption consists of several phases such as establishing secure connection, transfer of keys, broadcasting encrypted data, key decryption, and decryption of original data.

In the group key management process whenever a particular data user is revoked or some data is altered it is not necessary to change all the data content, re-encrypt it and distribute among the data users. Simply it is sufficient to broad-caste the public key among all the data users, they will generate the secret key from the information they are provided at the beginning itself with the help of secured connection. The main advantage with this mechanism is less cost of establishing and maintaining secured connection among the data owner and the users for key transfer. This group key management needs the attribute information and the various access control policies (ACP's) applied on those attributes. Similar to broad-caste encryption it also follows several steps such as establishing the connection between the data owner and the server through a trusted third party to access data from the cloud environment. The public key generation, secret key generation with access control policies (ACP's), key distribution, data decryption, and rekey management when the user dynamics are changed.

Loss less join decomposition of ACP

In group key management scheme, at the owner level itself access control policy (ACP) will be decomposed in to multiple sub groups such that the union of all the sub groups should produce the original access control policy (ACP). Another issue here is the decomposition should be such that the owner should have some attribute which preserves the data confidentiality and provides security for the data from unauthorized accesses from the cloud, also the attributes it maintains should be as minimum as possible so that majority of the data modifications should be done at the cloud server level itself, without intervention of the owner every time.

Conventional encryption:

The conventional mechanism consists of four entities such as the data owner, trusted third party, the cloud server and the data user.

- Data owner will produce the data and defines access control policies (ACP's) for the data based on the user requirements also encrypts data with public key mechanism.
- Cloud server will stores the data it should be honest but curious such that the data should be secured and privacy preserved, it hosts the encrypted data provided by the owner.
- Trusted third party plays a major role in this process it establishes a secured connection between the owner and the user through the cloud server, it transfers identity keys and secret information between the owner and the user for information exchange.
- Finally the user uses the identity keys gathered from the trusted third party to access the required data from the cloud environment which is supplied by the owner in encrypted format.

In the conventional single level encryption the system undergoes the following phases.

Initially the trusted third party issues identity token among users based on their attributes.

The data users has to register all their identity token with the data owner so that they will receive the secret information which is necessary to decrypt the data which is hosted to the cloud server by the data owner with encryption.

Now the data owner will encrypt its data based on the access control policies (ACP's) issued with the relevant attributes. The data owner encrypts the data using keys which will be generated by using the group key management scheme which we discussed earlier, and uploads to the cloud server.

User has to download the encrypted data available with the cloud environment, generates secret key with the help of information provided initially with trusted channel, and decrypt the data uses it.

During the process of using data in this way data users may revoke, some data items may be modified, further encrypted data may undergo some alterations. In all these situations the data owner is responsible to perform re-encryption. The owner has to download all affected data items from the cloud, decrypt, then encrypt again and upload to the cloud.

III. IMPLEMENTATION METHODOLOGY

Observe that in the conventional single level encryption approach the data owner has to pay large communication and computational cost because, whenever the user dynamics changes, owner has to alter the related data items as the encryption mechanism related to those attributes is with the owner. If the access control related encryption is assigned to the cloud server owner can get relaxation from re-encryption of the source data. Hence to reduce the computational cost on the owner it is better to transfer the authorization related encryption to cloud server keeping the confidentiality related encryption with the data owner. The proposed mechanism is having two levels of encryption say the owner level and the cloud level encryption.

Main issue with the multi-level encryption is that how to distribute the encryption among the owner and the server. We have different methods for this such as the first one is data owner will encrypt the data using a symmetric key first, then cloud server will perform access control related encryption. Advantage with this approach is there will be less work for the owner once he has encrypted the complete data using symmetric key. Another approach is both the owner and server will collaboratively perform the encryption related to access control. The draw back with this approach is it is somehow similar to the conventional method in which, there will be computational overhead on the owner.

IV. MULTI-LEVEL ENCRYPTION

In the proposed multi-level encryption mechanism all the access control policies (ACP's) will be decomposed in two different sub components such that the loss less join condition is preserved. Here the partition of access control polices at the owner level will be such that the attributes related to confidentiality of the data will come under one sub set all the remaining comes under another set. At the cloud server level again the decomposition will be performed such that users requirement of various data attributes will be satisfied, common requests from various users will be grouped as single entity, all the related attributes access control encryption will be same, another group of attributes will be having another encryption with a different key, like this the method follows with a group of keys generated at the cloud level. Whenever the user dynamics changes, any data is modified, or a user is revoked only the related attributes encryption at the cloud level need to be re done. This reduces the burden on the owner and assigns access control related privileges to the cloud server without loss of confidentiality of the data.

Token Issue:

Trusted third part issue identity tokens to the data users based on the attribute request of the users.

Primary Decomposition of ACP:

Initially data owner will decompose access control policies (ACP's) into two sub groups such that the first group consists of confidentiality related attributes, second group consists of other attributes of the data items.

Secondary Decomposition of ACP:

Cloud server will group the attributes in to sub groups based on the user registration of various tokens. Cloud is responsible for encryption of the data items based on the access control policies (ACP's) of various data items.

User Registration:

Users has to register with their identity tokens so that they will get the secrets about how to generate the private key to decrypt data at later point of time. The user registration has to be done in two phases i.e., all the attributes related to confidentiality of the data has to be registered with the owner, all other attribute tokens related to access control has to be registered with the cloud server.

Encrypt and Upload data:

First, owner has to perform confidentiality related encryption of all the data items, each data item should have at least one attribute related to confidentiality. The sub group of access control polices related to confidentiality plays major role in this process. After the owner level encryption is done the data items will be encrypted again with other sets of access control policies (ACP's) at cloud. Both owner and cloud will use different symmetric keys for encryption.

Now the data is uploaded in to the cloud environment, along with the public information. The secret of key generation will be communicated separately to the users with the help of trusted third party. Cloud handles group key management and access control based encryption.

Decryption at User:

In order to access the original data, the data user has to decrypt the retrieved data twice, first decryption is done with the help of public information provided by the cloud server to generate key for access control related attributes, second level of decryption is done with the public information provided by the owner, it will give another secret key, by using both the keys the user can access original content of the data files.

Re-encryption Management:

Once the initial encryption is done, all the data items which are altered, added, or revoked has to be re-encrypted. Here the re-encryption is performed on those data items for which attributes are altered. This is done by the cloud server without involvement of the owner. Re-encryption can be taken care by the cloud server until unless access control policies (ACP's) are not altered. If the access control related attributes are modified again the owner has to decompose the ACPs perform re-encryption of those data items and upload to server which is similar to the conventional method. In this case both owner and cloud has to perform re-encryption of the data items.

V. ANALYSIS

Conventional Verses Proposed:

We aware that, in the conventional single level encryption mechanism the owner has to perform all the access control encryptions with a fine-grained mechanism. Here the cloud simply acts as a data storage place, it is not responsible for any access control related issues. The main advantage with this approach is that access control policy related information can be hide from the cloud server. If any user is trying to get unauthorized access from the cloud the data cannot be accessed by him. Major drawback with this approach is that owner has to pay high computational and communication overhead whenever the user dynamics changes, he has to download corresponding data items, decrypt them re-encrypt with a new symmetric key, and distribute the secure information among the users with the help of third party and upload the data files onto the cloud.

Whereas the multi-level encryption mechanism reduces the burden on the owner. He has to perform encryption only at the initial stage with only those attributes which consists access control related to confidentiality of the data. Here most of the key management tasks will be taken care by the cloud itself. Whenever any identity attributes are altered, the owner will change the access control policies related to cloud, such that re-encryption can be handled by the cloud itself.

Security and Privacy:

Coming to security concern both the conventional method and proposed method provide data security and privacy. In the earlier one as the owner is doing the complete encryption users can get access to the data only if it has the correct information about the decryption. Here all attribute based encryption will be performed by the server by considering access control policies. In the later one as encryption is performed at multiple levels user has to perform decryption two times first at the cloud level to get identity related data, next owner level to access the complete data. Privacy is provided in both the cases as the identity tokens will be issued based on the identity attribute through trusted third party. Here both owner and the cloud are unaware of the identity attributes of the user.

VI. CONCLUSION

Conventional approaches for secured and privacy preserved access control policy encryption for cloud data storage incur high computational and communication cost for the owners, as they has to re-encrypt the data whenever any user dynamics changes, in the proposed method we provided a better approach for privacy preserved fine-grained access control encryption by decomposing the ACP's into different sub groups, in this encryption will be done both at owner level and cloud level, the owner level encryption is to preserve the data confidentiality by maintaining related attributes encryption with owner, and access control privileged encryption will be done by the cloud by which encryption over head on the owner is reduced.

REFERENCES

[1] M. Nabeel and E. Bertino, "Privacy Preserving Delegated AccessControl in the Storage as a Service Model," *Proc. IEEE Int'l Conf.Information Reuse and Integration (IRI)*, 2012.

[2] G. Miklau and D. Suciu, "Controlling Access to Published DataUsing Cryptography," *Proc. 29th Int'l Conf. Very Large Data Bases (VLDB '03)*, pp. 898-909, 2003.

[3] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A Privacy-PreservingApproach to Policy-Based Content Dissemination," *Proc. IEEE26th Int'l Conf. Data Eng. (ICDE '10)*, 2010.

[4] M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving PolicyBased Content Sharing in Public Clouds," *IEEE Trans. Knowledge and Data Eng., vol. 25, no.* 11, pp. 2602-2614, Nov. 2013.

[5] S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-Encryption: Management of Access Control Evolution on Outsourced Data," *Proc. 33rd Int'l Conf. Very Large Data Bases (VLDB '07)*, pp. 123-134, 2007.

[6] M. Nabeel and E. Bertino, "Towards Attribute Based Group Key Management," *Proc. 18th ACM Conf. Computer and Comm. Security*, 2011.

[7] A. Fiat and M. Naor, "Broadcast Encryption," *Proc. 13th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '93)*, pp. 480-491, 1994.

[8] M. Nabeel and E. Bertino, "Attribute Based Group Key Management," to appear in *Trans. Data Privacy*, 2014.

[9] S. Coull, M. Green, and S. Hohenberger, "Controlling Access to an Oblivious Database Using Stateful Anonymous Credentials," *Proc. 12th Int'l Conf. Practice and Theory in Public Key Cryptography*, pp. 501-520, 2009.

[10] K.P.N. Puttaswamy, C. Kruegel, and B.Y. Zhao, "Silverline: Toward Data Confidentiality in Storage-Intensive Cloud Applications," *Proc. Second ACM Symp. Cloud Computing (SOCC '11)*, pp. 10:1-10:13, 2011.

[11] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure Attribute-Based Systems," *Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06)*, pp. 99-112, 2006.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," *Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06)*, pp. 89-98, 2006.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute- Based Encryption," *Proc. IEEE Symp. Security and Privacy (SP '07)*, pp. 321-334, 2007.

[14] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," *ACM Trans. Information System Security, vol. 9*, pp. 1-30, Feb. 2006.

[15] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute Based Proxy Re-Encryption with Delegating Capabilities," *Proc. Fourth Int'l Symp. Information, Computer, and Comm. Security (ASIACCS '09)*, pp. 276- 286, 2009.

[16] J.-M. Do, Y.-J. Song, and N. Park, "Attribute Based Proxy Re-Encryption for Data Confidentiality in Cloud Computing Environments," *Proc. First Int'l Conf. Computers, Networks, Systems and Industrial Eng.*, pp. 248-251, 2011.