Open access Journal International Journal of Emerging Trends in Science and Technology
Impact Factor: 2.838 DOI: http://dx.doi.org/10.18535/ijetst/v3i03.06

Secured Data Sharing In Federated Cloud Environment

Authors
G.Kavitha[1], R.Priya[2]
[1]MCA, Mphil, Research Scholor, Vels University, Pallavaram, TamilNadu, India
Email: *giridharan.kavitha@gmail.com*
[2]MCA, Mphil, PhD, Assistant Professor, MCA Dept, Vels University, Pallavaram, Chennai, Tamil Nadu, India
Email: *priyaa.research@gmail.com*

Abstract
Cloud storage is an important area in cloud computing. This involves lot of process like storing large amount of data, encryption of data and securely communicating encrypted keys with the users. Nowadays large amount of secured data are shared in the cloud environment. Hence it is very important to maintain the privacy of secured data. Thus the secured data is encrypted and the large numbers of keys are shared with the users. But sometimes the user will not be able to maintain large amount of secured keys. In this journal a secured key aggregate searchable encryption is proposed which is used for sharing a single aggregate key to the user for sharing large number of documents in a federated cloud environment. Also the number of keyword trapdoors send to the cloud environment by the user is also minimized in this approach.
Keywords – *Aggregate key, Trap door, searchable encryption, Federated cloud.*

Introduction

Cloud is an important storage environment used for storing large amount of outsourced data. Mostly it includes secured, personal data and business related data. Hence privacy of the data are very important and to ensure the privacy the data are encrypted and uploaded in the cloud. In addition to that authentication for every user also provided. So that the data can be accessed by authorized users. There may be chance for data leakage by the user or by an ineffective cloud owner. Also an unexpected privilege leak will lead to data leakage.

A common approach to overcome data leakage is that all the data are uploaded only after encryption and the data will be decrypted by those who have decryption keys. These clouds are named as cryptographic cloud storage. But in these encryption schemes only selected data are retrieved by using the given specific keywords. This makes it very challenging for the users to retrieve the data stored. A general solution to this is that the data owners will encrypt the potential keywords and upload them in the cloud along with the encrypted data. This process is called searchable encryption in which for retrieving the data the user has to send the corresponding keyword trapdoor to the cloud for getting the data. By combining searchable encryption with cryptographic cloud storage the basic necessity of security is achieved. But for millions and millions of data implementing such a system will leads to a tedious process and hence it is impractical. This is because sharing of encrypted data with users generally needs different encryption keys for different files. So the number of keys to be distributed to the user will be proportional to the number of files distributed. Also these keys have to be distributed in a secure way and also the user has to manage the keys securely. Also a large number of trap doors have to be generated and send to the cloud for the user to perform search operation.

To overcome this a Key aggregate searchable encryption is proposed. This scheme supports searchable group data sharing functionality in which the user may share a group of selective files with a group of selective users and also allow them to perform search over the data. There are two requirements for achieving this. The first one is that the data owner has to share a single aggregate key instead of multiple keys for sharing number of files. Secondly the user has to submit a single trap door instead of multiple trap doors to the cloud for searching in a number of files. These are performed in a federated cloud rather than in a single cloud.

Existing System

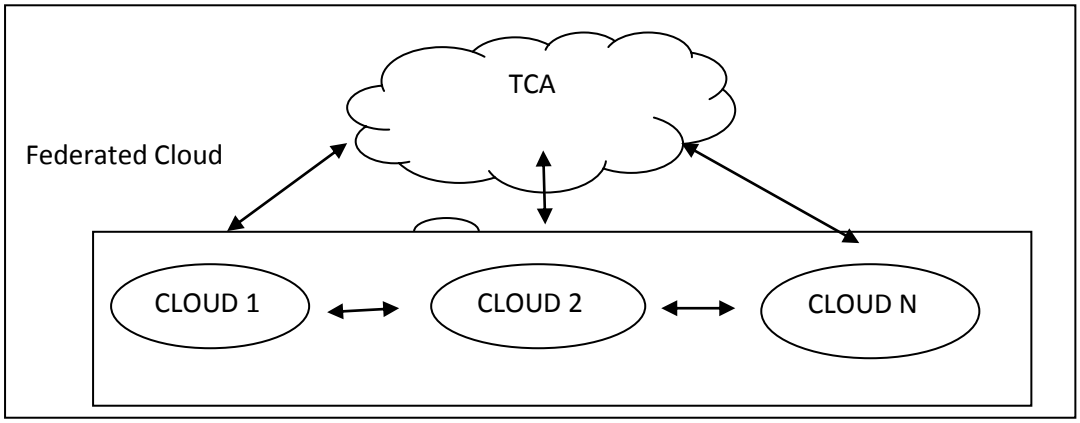
The existing system uses a searchable encryption scheme in which the user will share a group of selective files with the group of selective users. This will allow the group of users who have access to the group of files to search and access the data. In this the data owner will share a single aggregate key with the user instead of multiple keys to perform the search. Also the user will submit a single trap door instead of multiple trap doors to the cloud for searching the files. But if the user wants to access the documents possessed by multiple owners then the number of trap door increases. Also the existing process is performed in a single cloud environment.

Proposed System

The proposed system uses a key aggregate searchable encryption in which the data owner will provide a single encrypted key to the user for sharing group of files. By using these key the user will able to access a group of selected files to which it has access and also it provides access to group of users. The user will send a single trap door to the cloud for searching the selected data. If the files are owned by multiple owners then multiple trap doors are used. To overcome this aggregated trap doors are proposed to reduce this. Also instead of single cloud environment federated cloud environment is used and these schemes are applied on that.

Federated Cloud

A federated cloud is the combination of multiple external and internal clouds services. Union of smaller parts that perform a common action is called federation. In this way businesses will use local cloud providers to connect with customers, partners and employees anywhere in the world. Using federated cloud the end users gain promise of the cloud. And, it's how data center operators and other service providers will finally be able to compete with, and beat, today's so-called global cloud providers.



MODULES

Uploading of data in cloud

Generally large amount of data are uploaded in cloud by service providers. These data has to be securely stored in the cloud environment to protect it from hacking.

Data Encryption

Encryption converts the data in to other form called cipher text. This cipher text cannot be easily understood by users except those are authorized. The primary purpose of encryption is to protect the confidentiality of data stored on computer systems and those data that needs to be transmitted via the internet. Modern encryption algorithms play a vital role in the security they not only provide data confidentiality but also provides authentication and integrity.

Searchable encryption

For accessing the encrypted data the data owner has to provide a single encrypted key to the users. The user has to securely store and by using the key the user will be able to access the group of files to which it has access. The user will also provide access to the group of other user to the access is given.

Creation of Trap door

For accessing the group of files the user has to send a trap door to the cloud. For accessing multiple files multiple trap doors are used. Hence an aggregated multiple trap doors are used.

Conclusion

These modules are used to share the data to group of users in federated cloud environment by reducing the generation of n.umber of trap doors

Reference

1. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.
2. X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multiowner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 11821191.
3. P. Van,S. Sedghi, JM. Doumen. "Computationally efficient searchable symmetric encryption", Secure Data Management, pp. 87-100, 2010.
4. C. Bosch, R. Brinkma, P. Hartel. "Conjunctive wildcard search over encrypted data", Secure Data Management. LNCS, pp. 114127, 2011.
5. B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud", Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507525, 2012.
6. R. A. Popa ,N. Zeldovich. "Multi-key searchable encryption". Cryptology ePrint Archive, Report 2013/508, 2013
7. K Venkatramana "A threshold secure data sharing scheme for federated clouds"
8. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing", Proc. IEEE INFOCOM, pp. 534-542, 2010.
9. Thiruselvan Subramanian∗ and Nickolas Savarimuthu† A study of optimized resource provisioning in federated cloud.
10. Dr. Atulbhai Patel, Kalpit Soni Cloud computing security using federated key management
11. Thiruselvan Subramanian∗ and Nickolas Savarimuthu† A Study on Optimized Resource Provisioning in Federated Cloud
12. Riddhi Solani Kavita Singh Rathore B. Tech. Student B. Tech. Student Department of Information Technology Department of Information Technology Institute Of Technology, Nirma University Institute Of Technology, Nirma University Federation of cloud computing infrastructure.