SECURED ARCHITECTURE FOR MULTI-CLOUD USING KEY AGGREGATION TECHNIQUE

Suruchi Narote[1], Lokesh Bijole[2]

[1]*ME (Student), Department of Computer Engineering, Padm. Dr. V. B. Kolte College of Engineering Malkapur, Maharashtra, India*

[2]*Asst. Professors, Department of Computer Engineering, Padm. Dr. V. B. Kolte College of Engineering Malkapur, Maharashtra, India*

Abstract

Data storage and data sharing is the most important aspect in cloud computing, so sharing data and storing it in a secure way is the biggest task when adopting cloud services. In this paper, we will discuss how to share and store data effectively which will prevent the third party to access the secure data in cloud storage. This article provides a survey of using multiple clouds to achieve a security. In this we are introducing a public-key encryption known as Key-aggregate Cryptosystem (KAC). Cryptography is a technique which encodes a data using some key and produces unreadable data so that only a desired party is able to decode that data. KAC produces a constant size ciphertexts (unreadable data) such that decryption right for any set of ciphertexts are possible, means one can aggregate any set of secret keys and make them as compact as single key, but encompassing the power of all the keys being aggregate. This aggregate key is sent to other via secure channel (or via email) for decrypting the ciphertext set and remaining files outside the set are remains secret.

Keywords: *Cloud, multicloud, key-aggregate encryption, data storage, data sharing and security.*

----------***----------

1. INTRODUCTION

In today's world Cloud computing is the most emerging technology used in the scientific and industrial workgroup. Cloud computing provides scalable resources and services over the internet which the third party can access as per their requirement and have to pay rent for using these services as per their usage, which is very cost effective as well as expenditures for hardware and software. [1]Cloud can be divided into 2 types based on their physical location from the viewpoint of the user: *public cloud* and *private cloud*. A *public cloud* is a cloud which is provided by the third party and involves resources outside the user's office and in contrast to public cloud; *private cloud* is installed within the user's office. This article will concentrate on public cloud due to highest security demand. Cloud provides various types of Services. In this paper we are focusing on the following two services provided by the cloud:

1. Software as a Service (SaaS): This allows cloud user to access the provider's application running on a cloud using various client devices via interface such as web browser.
2. Platform as a Service (PaaS): This allow cloud user to upload his own application and data on to the cloud without installing any tools or platform on their local machine.

Data from various clients are stored on the single physical machine, so there are various cryptographic techniques which will allow unauthorised user to access data on behalf of the owner without leaking anything about the data, or without compromising the data owner's anonymity [4]. The cloud user don't have the full faith on the cloud server or cloud provider that they will not leak their data with the others, so before uploading the data on the cloud server, the cloud user encrypt their data using their own key. Sharing of data is most important in cloud storage. For example, you can let your friend so see some of your photos in which he is present from your private pictures; an organization granted an access rights to their employee to access some sensitive data. The challenge is how encrypted data is to be shared effectively.

1.1 Data Sharing in Cloud

For an example Alice keeps her private data i.e. photos on Dropbox and she doesn't want to share it with everyone. Due to the possibility of data leakage, Alice does not fell to only depend on the privacy preserving mechanism provided by Dropbox, so before uploading the photos she encrypts them by her own key. Some day Alice wants to share photos to Bob in which he is present. Alice can share the photos by using the share function of the Dropbox, but the problem is how to share the decryption rights with the Bob. One option is Alice sends an email to Bob in which the private key is ivolved.There are 2 possible ways: [3]

1. Alice can encrypt all photos with one key and send to Bob securely.
2. Alice encrypts each photo with different keys and sends Bob the keys for each photo which she wants to share.

The first way is not proper method because all the photos of Alice may be leaked to Bob. For the second way efficiency is the major concern because it needs as many keys as the number of photos she want to send to Bob. So transferring these keys securely and storing them requires very expensive secure storage, which is very heavy and expensive. For the above problem the best solution is that

Alice encrypts files with different public key but sends a single constant size aggregate key to Bob for decrypting the file.

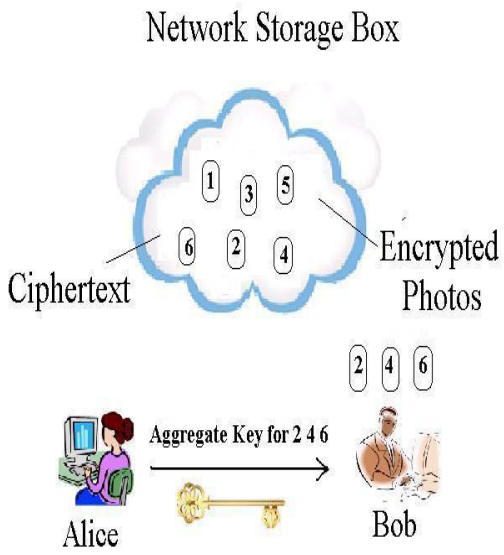

Fig 1 Alice shares files with identifiers 2, 4 and 6 with Bob by sending him a single aggregate key.

One way of reducing the threat and proving security to the data and application in a public cloud is to use multiple clouds simultaneously, one for storing the application and the other for storage of the data. This triggered a lot of research activities, resulting in various approaches which differ in technologies, partitioning, encryption techniques and distribution patterns as well as security levels. Public key encryption requires different key both for encryption and decryption. In this paper we are using multiple clouds one for application and one for storage and a key aggregation encryption for encrypting the data.

2. LITERATURE SERVEY

In 2013 Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Lacono and Ninja Marnau, "Security and Privacy-Enhancing Multicloud Architectures", one idea on reducing the risk for data and applications in a public cloud is the simultaneous usage of multiple clouds. Several approaches employing this paradigm have been proposed recently this paper provides a servey on different security by multicloud adoption approaches. It provides four distinct models in form of abstracted multicloud architectures. These developed multicloud architectures allow to categorize the available schemes and to analyze them according to their security benefits.[1]

In 2014 Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng," Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" In this paper, we study how to make a decryption key more powerful in the sense that it allows decryption of multiple cipher texts, without increasing its size.

"To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the ciphertexts (produced by the encryption scheme) is decryptable by a constant-size decryption key (generated by the owner of the master-secret key)?" [2]

To ensure data integrity and security in cloud computing this proposed architecture uses a primary cloud and a secondary cloud to incorporate a multi cloud system, these are as follows[5]:

1. Primary cloud: The primary cloud can be created using centrally built software to fall under the category of SaaS (software as a service) cloud computing model. The primary cloud consists of a group of systems which are interconnected through LAN which in turn forms the primary cloud. The internal users can access the primary cloud through the same LAN whereas the external users can access the primary cloud through devices supporting a web browser using GPRS services. This model thus enables multiple users to access the primary cloud simultaneously. The primary cloud where application resides also maintains security of data by authentication of the user who are using the application. So only an authorized user can access data .This is done by the cloud administrator and hence a user is allowed to access only data relevant to him not the data of others which is also stored in primary cloud.

2. Administrator: The cloud administrator is the most important part of this architecture and is responsible for proper working of both primary and secondary cloud. The data so retrieved from the secondary cloud is in an unreadable encrypted format. For the file to be back in its original form data decryption takes place. The data retrieved from the secondary cloud is uploaded to the administrator who in turn performs decryption code to get the data in its original form. This is then sent to the user. The data sent is user specific and can only be sent to authenticated users. The user authentication is done by the administrator to maintain integrity of data.

3. Secondary cloud: The Secondary cloud falls under the same SaaS (software as a service) cloud model similar to the primary cloud. Secondary cloud is used for storing a backup of the data stored in the primary cloud in an encrypted form. This is done after the administrator performs data encryption and segmentation on the data taken from the primary cloud. The secondary cloud can only be controlled by the administrator to ensure integrity of data. Each segmented data known as chunks are stored in separate systems in the secondary cloud. In case data is being retrieved from secondary cloud, the encrypted and segmented data is sent to the administrator for data decryption and de-segmentation before sending it to the user. Thus, the proposed system ensures security and integrity to the data saved in the cloud and also provides an architecture which is secure and reliable through the use of Linux as the OS.

3. PROPOSED WORK

Our main aim was to develop an encryption/decryption program which will generate an encryption key. In today's world most of the application uses the concept of cryptography. For example, if we have to protect confidential data then this concept of cryptography provides very high level of security to the data of individual or group. Cryptography not only provides confidentiality service but also provides many services like, data integrity, data authentication etc. Cryptography is a method which securely transfer data only to the relevant user not allow other to access the data, in other words it is a way that allow access to data only to the user who has a decryption key provided by the sender to the receiving user via secure medium.

But rather than these advantages, now days there are various methods to break an encryption through cryptanalytic attacks. This is the main reason why we need strong encryption algorithm. Cloud users will not have full faith on the cloud service provider that they will not share their confidential data with their competent or himself(service provider) use his(users) data for own benefit. For this reason we will use multiple clouds one for accessing the services and one for storing data, so only relevant user can access his data. For providing more security we are using Key-aggregation Cryptography (KAC).

4. KEY-AGGREGATE CRYPTOSYSTEM (KAC)

In KAC, users not only encrypt a message under public key, but also under an identifier of ciphertext called as class. Ciphertext are divided into different classes. To extract the corresponding secret key for different classes, a master secret key is used which is hold by the key owner. More importantly the extracted key is the aggregate key which is as compact as the secret key for a single class, but combining the power of many keys to decrypt the subset of any ciphertext classes. In KAC the size of all the keys (public key, master secret key and aggregate key) and ciphertext are all constant. [2]

4.1 Framework

Key aggregate encryption schemes consist of five polynomial time algorithms as follows:

1. Setup (1λ, n): The data owner establishes public system parameter via Setup. On input of a security level parameter 1λ and number of ciphertext classes' n, it outputs the public system parameter param.

2. KeyGen: It is executed by data owner to randomly generate a public/ master-secret key pair (Pk, msk).

3. Encrypt (pk, i, m): It is executed by anyone who wants to encrypt the data. On input a public key, index I indicating the ciphertext class and message m, to provide the ciphertext C as output.

4. Extract (msk, S): It is executed by data owner for delegating the decrypting power for a certain set of ciphertext classes. On input the master secret key (msk) and a set S indices corresponding to different ciphertext classes and it output the aggregate key for set S denoted by Ks.

5. Decrypt (Ks, S, I, C): It is executed by a delegate who received, an aggregate key Ks generated by Extract. On input Ks, set S, an index i denoting the ciphertext class ciphertext C belongs to and output is decrypted result m.[6]

4.2 Properties of KAC

1. Decryption key size: - constant.
2. Cipher text size: - constant.
3. Encryption type: - public-key

5. ADVANTAGES

1. It allows decryption of multiple cipher texts, without raising its size.
2. The size of master-secret key, cipher text, public-key, and aggregate key in our KAC schemes are all are kept constant size.
3. KAC scheme is flexible in the sense that there is, no special relation is required between the classes.
4. The delegation of decryption can be efficiently implemented with the aggregate key.
5. Particular Member can view their messages.
6. We can provide rigorous security analysis, and extensive performance.

6. CONCLUSION

Data privacy is the major question regarding cloud storage. In this survey, we study how to compress secret keys in public key cryptosystem which supports delegation of secret keys for different cipher text classes in cloud storage. A limitation in our work is the predefined bound of the number of maximum ciphertext classes. In cloud storage, the number of ciphertexts usually grows rapidly. So we have to reserve enough ciphertext classes for the future extension. In this paper we study the concept of multicloud which provides extra security for the storage of data.

REFERENCES

[1]. Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Lacono and Ninja Marnau, "Security and Privacy-Enhancing Multicloud Architectures", IEEE Transactions on Dependable and Secure Computing, VOL. 10, NO. 4, JULY?AUG 2013

[2]. Cheng-Kang Chu ,Chow, S.S.M, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng , "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014.

[3]. Arun Kumar S, S.Dhanasekar , "A Literature Survey On Key Aggregation System for Secure Sharing of Cloud Data", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 3, Issue 12, December 2014

[4]. B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Dataon the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.
[5]. Nikhil Dutta , Himanshu Bakshi , Mujammill Mulla , Viraj Shinde, "Multi Cloud Architecture to Provide Data Security And Integrity", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 10, October 2013)
[6]. Mrs. Komal Kate, Prof. S. D. Potdukhe, "Data sharing in cloud storage with key-aggregate cryptosystem.", International Journal of Engineering Research and General Science Volume 2, Issue 6, October-November, 2014