International Journal of Pure and Applied Mathematics
Volume 118 No. 24 2018
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

AN IMPROVED WAY FOR SECURING CLOUD DATA STORAGE

Ilaiyathasan S [1] (PG scholar),Prabu kanna G [2](AP/IT)
Information Technology
Kalasalingam University
Virudhunagar, India
thasan234@gmail.com,gpkanna@klu.ac.in

May 22, 2018

Abstract

Cloud computing is a computing pattern which allows user to store and access data through virtual network with convenient feasibility, elasticity and integrity towards stored data in cloud. Currently every data are accessed from cloud via internet. The data stored in cloud should be provided with a high security. To reduce security issues data are stored in cloud by encrypted format. In our proposed scheme an encryption type is used on behalf of identity basis. Along with that a technique is to be followed to have improved security over data in cloud. In our proposed system, functional encryption concept is used for making the key to be enhanced for data in securing manner. So that no hackers would be able to get rid of secret key that are shared. A technique is implemented called Group signature in which data stored in cloud are signatured in a way that no one is able to view the content of the data which is stored publically. It will most probably improve the security of the data that are stored in the cloud.

***Key Words*:**cloud computing, functional encryption, AES, RSA, quick sort, group signature.

1 Introduction

In this world, no one is their without internet. More number of multiple mobile devices like smart phones , laptops are grooming up in the fields which helps to access their own data from anywhere they are needed via internet. For that purpose all are in need of cloud computing infrastructure to store and access those data. Cloud computing is the boomed up field for storing the data on internet in secure manner. So the data fetched in the cloud should be secured and also made to have a easier way of attempting upload and download activities from everywhere when we needed. Storing the data in cloud provide more benefits such as accessibility, reliability, integrity. Trending web companies like Amazon web services, Google are focusing on the storage capacity to be served to the users. This is the deterministic approach for the cloud storage. Only proper structured data are found in the cloud. Thus the arrangement of data is going to be a tough task in it. Many of the opportunities are given for the development of infrastructure in cloud. Blooming business owner are given a chance of storing their own data in cloud for a free of cost given by the cloud providers. In which security is the big issue while storing the data in cloud. The following illustrates about basic security measures: Access management (AM) is the process of accessing the control of the specified user by tracking their moves and activities. It is a vast concept that comprises of all policies, methodologies and tools to have access within an IT environment. Each and every user is provided with a proper way for accessing their own data from the cloud. No eavesdropping of secret way of access to the data is done. By doing so we could have data security in cloud. Identity management (ID) is the process of giving authentication and authorization for a particular individual in that group with own identity provided by user. Identity management thus focus on authentication process, while access management will follow authorization as well. All the users are given an unique identification so that it would stop the misleading of information from the cloud. Controlling and monitoring privileged access is extremely important to stop the risks possessed by the attackers. Methods of protecting the corporate or business network where the remote devices access their file or data through that network. All the remote devices connected to the

networks will have a individual potential point for security threats. Endpoint security is formed to secure each endpoint on network created by those devices. Here the endpoint security is got to be maintained because the usage of mobile devices on corporate network is allowed by the company for their own employees on their own workspace. Designed to safeguard the usability and integrity of data and network to prevent the unauthorized access. The admin of network should adopt the preventive measures to avoid security threats. Such as government or business centre are in need of security while working on computer networks. The simplest way of protecting the network is to have an unique password along with their own identity. Cloud provider offers encryption services to encrypt data before it is transferred to the cloud. The sensitive data were encrypted end-to-end while uploading into cloud. In this model, cloud provider will be given appropriate key to the user, due to that user would be able to have a safe decrypt of data from cloud. Cloud encryption is the best approach for securing the data which are stored in system; file or any databases which could be decipher using keys. By providing encryption key management, a person of a company could decipher sensitive data only with the help of encryption key. If the key is lost the attacker will not be able to access that data using that key because each data is provided with an individual encryption key. Communication encryption: A way in which encrypted data in cloud are processed from one to another in a secure manner. Encryption is meant for securing data when stored on devices. The sensitive information will not be affected even if it is loss or theft. By doing so all the data stored in cloud will be secured for future use. Challenges: The only primary challenge in encryption is efficiency of data should not be lost. In encryption bandwidth is founded to be big constraint to avoid such thing every data uploaded in cloud could be got encrypted. Benefits: Only authorized persons of the particular cloud are allowed to access data which could be stored in that cloud. The data should be ensured that in case of loss of data occurs no one is able to view that data because key could be changed accordingly.

2 RELATED SURVEY

The following are the issues regarding security are briefly explained in [1], by ihshan jabbar. In this paper, the use of homomorphic encryption to encrypt the clients data in cloud server and it also enables to execute required computations on encrypted data. [2], by anusha bilakani, they have developed a scheme based on fully homomorphic encryption that can perform operation directly on encrypted images. [3], by peidong, a simple modification torwads RSA algorithm is made in FHE. [4], by ping zhu, in which the combination of both assistive and multiplicative homomorphism is performed to have advanced security. [5], by chen, it will make possible for users to fetch information from search engines without exposing the content of the request which greatly promotes the development of security in cloud storage. [6], by ayantika, propose a sorting technique called lazy sort with reduced recrypt operation, which give better result when compared to comparison sort. [7], by neetu, in this work authors have used the merge, count and insertion sort separately over the buckets and results are compared with each other. [8], bykedar, this paper gives about the data sharing in cloud on the basis of identity based encryption along with cipher text. [9], by wei, they propose a notion called revocable-storage IBE which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text updates simultaneously. [10], by libing, two way of security scheme is followed one is on cipher-text scheme and another one is on identity basis is done to have efficient security. [11], by quasy, the proposed scheme provide integrity and confidentiality as well as the ability to protect communication between devices against possible attacks. [12], by ali, they uses signcryption scheme to provide the efficiency of the cloud computation.

3 EXISTING WORK

Fully Homomorphic Encryption

A fully homomorphic encryption system delegates the processing of data without giving access to it. This type of cryptosystem will provide security, privacy and also preserve computations over many areas. Suborning of data in cloud is the difficult task. It is

the best solution for securing the user data in encrypted format and also fetch the data without decrypting it . The data is encrypted with FHE before fetching the data in cloud. Both while uploading and downloading file or data the data should be transferred securely. Every user is given with the appropriate login and password for accessing the cloud. Keys are provided for every individual user. Public keys are used for uploading the data in cloud in public group so that everyone alive in that group is able view the file. As well as private key is used to the make data to be more confidential. The main gimmick of this existing system is time complexity.

Demerits

a. Less security system.

b. Takes more time for both encryption and decryption.

4 PROPOSED WORK

In this paper, we propose a new data access control scheme for multi-authority cloud storage system. The proposed scheme provides the protection mechanism to enhance the confidentiality of cloud data. A technique called sorting is meant for quicker access of data from the cloud both for uploading and downloading data. The functional encryption brings out the identity based encryption to have a unique identity towards the users for the security purpose. If a user wants to recover the data from the cloud, the user is provided with attribute secret key with respect to policy access and also authorized key are to be given. In our work the size of the cipher text and number of arithmetic operations are founded to be in constant. So that it leads to have cost computation overhead of the system.

Fig.1 Proposed model overview

Cloud admin: The cloud admin has the access control of activation and deactivation of user account. Backing up of files, log files

are managed. All the users in the cloud are controlled by admin. Auditing of files and users is got to be done by them. They are mainly meant for monitoring and managing the services. Thus the cloud admin is also a member of the group.

User management: Will establish the user rights to information within an organization. First every user should register by giving their own details in the system. The authentication for every user of the system is provided with his/her own identity key. With that identity key all the messages could be shared among other users. Thus user should define the particular identities of other users to access files. User identity encryption: All the identity keys of every user are stored in meta-data file which got to be stored as a file in the storage. Activated email and also active mobile numbers are to be given for the registration process if that seemed to alive only then the registration of every user got completed. File stored in cloud are encrypted using secret key along with identity keys for the secure access.

Key management: A technique is followed to improve the security of the system is the periodic key management. The generation of the secret key is done along with the private key not to be ensured by intruder. Secret key is got to be changed for every periodic session. Those key are transferred only through the private communication via email. Thus the shared secret key are founded to done to the user along with their own identity keys.

Algorithm Steps

AES Encryption Algorithm

AES is a symmetric block cipher which consists of N-rounds depends on key length. It is founded to have a faster execution time and reduces the cost for implementation purpose. AES algorithm is used for data encryption and decryption, since it is faster and secure than other algorithms.

```
Cipher (byte inner [16], byte outer[16],
Key_arrayroundkey[Nr+1])
begin
byte x[16];
state = inner;
Addroundkey(x, roundkey [0]);
for i=1 to Nr-1 stepsize 1 do SUbbytes(x);
Shiftrows(x);
```

Mixcolumns(x);
Addroundkey(x, round key[i]);
End for subbytes(x);
ShiftroWs(x);
addroundkey(x, round_
key[Nr]);
End
Funtional Encryption

A way of public key encryption scheme which allows to decrypt the data by secret key without revealing any other information. In the functional encryption system, a decryption key allows a user to learn a function of the encrypted data.

Two types

(i) Attribute based encryption

(ii) Identity based encryption

Identity based encryption: An identity based encryption (IBE) scheme is a public key cryptosystem where any string is a valid public key. The email address and dates can be public keys. The users active email and mobile number is provided for security purpose. Now in the functional encryption the identity based encryption will give a secured data storage in cloud .identity based encryption is a type of public key encrypting in which the public key of a user is used with some unique information about the identity of the user. Where the identity given by the user should be in live state. E.g.: mail address, OTP.

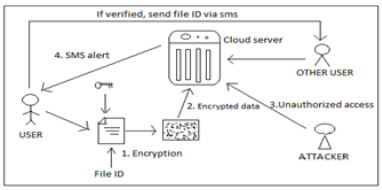

Fig 2. IBE model

4 phases

Setup phase: creates a public key and master secret key. The public key is meant for storing the data in public which could be

viewed by everyone. The master secret key is used to have a separate key holded b the group admin.

Key generation: use master key to generate new user specific keys. By using the individual group admin master key it helps to generate a specific key to the new users.

Encode: use public key to encode any message to be public or private keys to be confidential. The usages of keys are on the basis of user choice the data to be uploaded in the cloud.

Decode: use secret key to calculate specific function on cipher text .Here a secret key is meant for decoding the data which are in secured format.

Sorting Technique

Sorting is arranging the objects in the form of list. Two types of sorting had taken place one is internal sorting and another is external sorting. Internal sorting is performed only for the small amount of data. For vast amount of data external sorting is performed. Sorting plays a role of ordering or arranging of the data stored in the cloud. Sorting technique is an opted to overcome the time complexity. By sorting we would be able to have secured data in cloud for faster access from cloud database in an authorized way.

Quick sort: In all other sorting algorithm quick sort is the fastest one. On the average, it has O (n log n) complexity; it is suitable for sorting big data in amount. This algorithm is simple to write and also realize too.

The following are algorithm steps for quick sort:

Initial a pivot value - First step is to choosing a pivot value by taking the centre element which could be founded out by taking average value among the data stored in database .

Partitioning It will be got rearranged in such a way that, lesser valued data will be moved to the left array as well as greater valued data will be moved to right side. The equal value data will remain as a pivot.

Sorting from both parts We have to apply quick sort algorithm to both left and right parts.

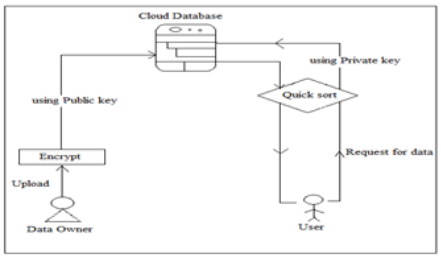

Fig 4. Quick sort

The i and j are two indices found in the quick sort. i takes the first element in the data where j takes last element in that one. Now i moves forward and j comes from bottom. I get stops when the value is founded to have greater value to pivot asa well as j will stop until value gets lesser to pivot. If i j swapping occurs and i moves to the next position (i + 1), j moves to the previous one (j - 1). Once the algorithm get stopped, only when i ¿ j. After all the i-th value gives values lesser than pivot and the j-th give values greater than pivot.

Merits:

- Large amount of data can be processed.
- Reduces time complexity.

Group Signature Technique

A Group signature is a technique which allow a member of the group to sign the data on behalf of that group . To achieve authenticity and privacy it should be publically verified by providing unique identifier sign. Group based authentication is a suitable approach for achieving an individual users privacy. Each member of the group should have a membership certificate provided by the group manager.

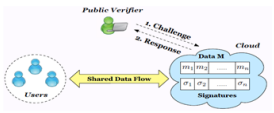

Fig 5. Group signature

This certificate provides the secret signing key of the respective group member. Each member of group can use it to produce group signatures on arbitrary messages. Using public key anyone in the group could validate issued group signature. Thus group signature confirms that signer is founded to be in that group only.

The following steps are used for implementing the group signature technique

1. Choose the file and a key whether it is made to be publicly available or only viewed by the user alone privately.
2. Now the file is stored as a private file in the database.
3. The process is founded to be repeated for all files stored in database and based on the key the files are arranged.
4. Now the file is signed by the user on behalf of group signature mentioned for that group.
5. Now the verification of sign is done then the private key for that file is shared and finally, the content of file is viewed.

The user has to choose the file and encrypt that file. The appropriate key which is necessary for the user is given. Then for both encrypt and decrypt of that file the same key is used. For each and every session the key value is changed to have a secure data transfer. According to the key, rearranging of file is done in database. Adding to that each and every data stored in the database is signed individually by the user whom belongs to the group. Finally, using the private key shared by user he/she will able to view the file and also able to have a notice on the sign by user whether the data is founded to be original data.

5 RESULTS AND COMPARISON

TABLE 1. Processing time between AES and RSA

File size (3mb)	FE using AES	FHE using RSA
Encryption time in sec.	1.2	2.4
Decryption time in sec.	2.8	3.6

Table I shows the comparative analysis of encryption algorithms. This study between them is done based on stimulated time foe encryption and decryption process. Based on their experiments they concluded that AES algorithm consumes least encryption and RSA consume longest encryption time. Now a day an important problem faced by all organization and providers is that fastest and secure delivery of services to the customer. Hence the proposed system provided security to user through encryption before uploading on the cloud.

In this paper, in our proposed system the results are discussed on the basis of both performance and time by evaluating two algorithms such as AES and RSA. By doing so, AES has the best result than RSA algorithm with the reduced time consuming in addition to that security is founded to be stronger in AES.

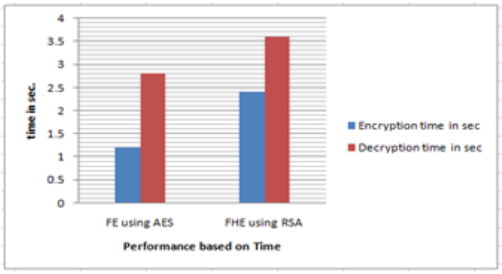

Fig 6. Comparison between existing RSA and proposed AES algorithm

The above comparison graph represents that the proposed functional encryption algorithm is giving better result when compared

to the existing fully homomorphic encryption algorithm based both on performance and time.

6 CONCLUSION

In this paper, we have studied to secure the data stored in cloud while it got accessed by multiple authorized users. The main problems are security and time complexity. By increasing the security and also reducing time complexity we would be able to get rid of the cloud consumers for longer term. Encryption of cloud is handled using fully homomorphic encryption which leads to have desirable security. Thus , to overcome that a simple and effective methods are proposed in this paper for data encryption using group signature technique. The implementation is carried out in cloudsim. Thus the result is compared with fully homomorphic encryption algorithm and proved to have a better result based on both performance and time complexity.

References

[1] Using fully homomorphic encryption to secure cloud computing, ishan jabbar, saad najim, Internet of things and cloud computing, 2016.

[2] Secure computation over cloud using fully homomorphic encryption, anushka, anjana, 2016.

[3] The modification of RSA algorithm to adapt fully homomorphic encryption algorithm in cloud computing peidong sha, zhixiang zhu, proceedings of CCIS, 2016.

[4] A algorithm of fully homomorphic encryption, guangli xiang, benzhi yu, ping zhu, International conference on fuzzy systems and knowledge discovery (FSKD) , 2012.

[5] Cloud storage third-party data security scheme based on fully homomorphic encryption, junjian CHEN, International conference on network and information systems for computers, 2016.

[6] Sorting of fully homomorphic encrypted cloud data: can partitioning be effective?, ayantika chatterjee , indranil sengupta, 2017.

[7] The detailed experimental analysis of bucket sort, neetu faujdar, shipra saraswat, 2016.

[8] Reliable data sharing using revocable-storage identity based encryption in cloud storage, kedar g pathre, International conference on recent trends in electrical, electronics and computing technologies, 2017.

[9] Secure data sharing in cloud computing using revocable storage identity based encryption, jianghong wei, wenfen liu, xuexian hu, 2015.

[10] Efficient identity based encryption scheme with equality test in smart city, libing wu, yubo zhang, 2017.

[11] An efficient and secure scheme for smart home communication using identity- based signcryption, yosef ashibani, qusay H. mahmod, 2017.

[12] S-Mbank: secure mobile banking authentication scheme using signcryption, pair based text authentication, and contactless smart card, 2016.

[13] Survey of various homomorphic encryption algorithms and schemes, payal, padhar, patel, International journal of computer applications, 2014.

[14] Multi-party protocol with access control on symmetric fully homomorphic encryption scheme, wamda, siti, Journal of therotical and applied information technology, 2016.

[15] Study on data security policy based on cloud storge, diao zhe, wang, International conference on big data security on cloud, 2017.

[16] Parallelizing fully homomorphic encryption, ryan, chiang, International symposium on computer, consumer and control, 2014.

[17] Enhanced RSA algorithm with varying key sizes for data security in cloud, world congress on computing and communication technologies, 2015.

[18] Pairing free and implicit certificate based signcryption scheme with proxy re-encryption for secure cloud data storage, braken, shabisha, 2017.

[19] Mututal heterogenous signcryption schemes for 5G network slicing, liu, zhang, 2107,

[20] Known plain text attack and improvement of PRNG based text encryption, ahmad amo, and sayed, International conference in information and communication systems, 2016.

[21] Development of a secure system for distributed data storage and processing in the clouds based on the concept of active security in RNS, cherviakov, babenko, 2017.

[22] Data storage security algorithms for multi cloud environment, ashaltha, jayashree, International conference on advances in electrical, electronics, information, communication and bio-informatics, 2016.

[23] Enhancing data storage security in cloud using certificateless public auditing, swathi, 2017.

[24] The detailed experimental analysis of bucket sort, neetu, shipra, 2017.