Data Security for Cloud using Multi Key Cryptosystem

Sajjan R.S.
Computer Science and Engg Department
VVP Institute of Engg & Technology, Soregaon
Solapur, Maharashtra, India

Vishvajit Dalimbkar
Computer Science and Engg Department
VVP Institute of Engg & Technology, Soregaon
Solapur, Maharashtra, India

ABSTRACT
Cloud computing is group of services for example software system storage, network and hardware these type of services are provided to user. Cloud storage is easily access anywhere anytime of the data because cloud is work in remote location. It uses the storage service provided by the cloud provider. Data is not secure in the cloud because the unauthorized user can try to use of the private data. So providing the data security it uses the different encryption method to protect the data. The proposed system assures security for data stored in cloud by using key aggregate cryptosystem (KAC). Initially the data is divided into multiple chunks each chunks is encrypted using encryption algorithm and generate different keys. Those keys are aggregated into a single master key which is used for decrypting retrieved cloud data.

Keywords
Cloud Computing, Data Security, Key Aggregate Cryptosystem

1. INTRODUCTION
The definition of cloud given by National Institute of standard and Technology (NIST) says that:"Cloud computing is a model for enabling convenient on demand network access to a shared pool of configurable computing resources.(e.g networks,servers,storage application and services)that can be rapidly provisioned and released with minimum management effort or service provider interaction [1].In the cloud computing there is no need to store data in the desktop or fixed location computer. You can store the data in a server and you can access the data in any remote location using of the internet topology. Cloud computing provides a large amount of data can be easly stored in the cloud. The advantages of using cloud computing are: i) reduce hardware and maintenance cost ii) accessibility around the glob iii) flexibility and highly automated process. Cloud computing is a computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. Clouds can be classified as public, private or hybrid. From initial concept building to current actual deployment, cloud computing is growing more and more mature. Nowadays many organizations, especially Small and Medium Business (SMB) enterprises, are increasingly realizing the benefits by putting their applications and data into the cloud. The adoption of cloud computing may lead to gains in efficiency and effectiveness in developing and deployment and save the cost in purchasing and maintaining the infrastructure [2].

Cryptography is technique applied for encryption and decryption. Encryption means the plain text is converted into the cipher text or some coded form using of the different encryption algorithm. For the purpose of data security and decryption is opposite of encryption. In the decryption the cipher text is converted into the plain text r original text using the decryption algorithm. Conventional cryptography is also referred as symmetric encryption or single key encryption. Same key is used for encryption and decryption. Public key cryptography is referred as asymmetric encryption or public key encryption. Separate keys are used for encryption and decryption. The encryption process consists of an algorithm and a key. The key is a value independent on the specific of the plain text. The algorithm will produce a different output depending on the specific key being used at that time. Changing the key changes the output of the algorithm. Once the cipher text is produced, it may be transmitted to cloud storage. Upon reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm with the same key that was used in encryption [3].

2. LITERATURE SURVEY
To secure the cloud security goals of the data include three points namely. Confidentiality, Integrity and availability (CIA).Encryption is used two types of algorithm symmetric and asymmetric algorithm. In the symmetric algorithm it uses private key for encryption and the same key is used for decryption. And asymmetric it uses the public key for encryption and private key is distributed to all using of the private key decrypt the data [4].

Table 1. Comparisons among Different Algorithms

	AES	**RSA**	**BLOW FISH**	**DES**	**ECC**
Key size	128,192,256 Bits	1024 bits	32-448 bits	56 bits	135 bits
Block size	128 bits	Variants	64 bit	64 bit	Variants
Introducer	Rijman Joan	Rivest Shamir	Bruce Schneier	IBM 75	Neal Koblitz,
Data ency capacity	Encrypt large amount of data	Encrypt small amount of data	Encrypt avg amount of data	Encrypt avg amount of data	-
Execution Time	Faster	Require maximum time	Lesser time to execute	Faster	Fastest

In cloud, data sharing plays an important role. This study explains how to securely, efficiently and flexibly. These existing systems which produce a constant size cipher text.

A. Identity Bases Encryption (IBE) IBE is a type of a public-key encryption. Identity-string is set for encryption which is nothing but user's public key. In IBE, master secret keys are generated by the private key generator and here the secret key is provided based on user's identity. Sender wants to share files. So sender will encrypt the files by making use of user identity and public parameter and sends the files. Receiver will decrypt these files by making use of his secret key. Guo et al. [5][6] tried to develop IBE with key aggregation. But out of key-aggregation and IBE, only one assumes random oracles. Key aggregation is inhibited as keys to be aggregated will come from various "identity".

Advantages

- Encryption type is public-key encryption.
- This scheme has a reliable party which will hold secret key.
- Based on the identity, secret key will be provided.
- The size of decryption key is constant.

Disadvantage

- Cipher text size is non-constant.
- Cost of storing cipher text and transmitting it expensive.

B. Symmetric Key Encryption Benaloh et al. [7] proposed an encryption scheme, where a huge number of keys can be sent rapidly in a broadcast scenario. The key origin is as follows. Initially choose two prime numbers p and q for a composite module. At random, master secret key will be chosen. Dissimilar prime numbers will be allied with each class. A public system parameter is considered for which all the prime numbers will be put. The outcome of this is a constant size key. This method is designed for symmetric-key setting. So here the sender should encrypt files with corresponding secret keys which will not be feasible. Advantages

- Ciphertext size is constant.
- Decryption key size is constant
- Requires less space to store ciphertext and keys.
- Construction is simple.

Disadvantages

- Both encryption and decryption is done by same key.
- Encryptor should get corresponding key to encrypt files.

C. Attribute Based Encryption (ABE) In Attribute Based Encryption method an attribute will be linked with ciphertext. From master secret key, the secret key will be derived. This secret key is used to decrypt the files merely if all its connected attributes go after the rules. Before Attribute Based Encryption method was introduced, the user who wanted secret key must go to third party and proving he is real by providing his identity and then he was capable to decrypt the file. Later in ABE scheme the secret key of user was not allowed to a single centre. Instead it was authorized by independent authorities. But still this scheme has drawback i.e. no solidity on secret key. Here in this scheme there is linear increase in key size, with the increase in attributes. Advantages

- Encryption type is public key encryption.
- Ciphertext size is constant.

Disadvantages

- Decryption key size is non-constant.
- Requires more space to store keys.
- Decryption key size increases linearly.
- Managing keys is expensive

3. PROPOSED STUDY

The confidentiality and integrity of the data cannot be assured if it is uploaded as such to the cloud. It depends on many cryptographic schemes to overcome this issue. Cryptographic schemes don't assure complete security but prevent the absolute revealing of the secret data. One method is that the user has to provide the permission to access the complete data since the selected data permission can't be granted. Another method is that separate encryption has to be done the selected data one-by-one separately and send the private keys to the one who request. This is practically impossible when we consider the time, cost, and complexity. Data can be so shared by encrypting all the selected data with its attributes and secret key converting it to a single aggregate key(private key) and this key can be sent over any communication channel like email, message etc. This mechanism not only saves the space, but also the execution time, cost, complexity etc[8] The aggregate key can be used only to decrypt the data with which it was encrypted which means all the other data outside this set remains safe and hidden to the one to whom the aggregate key is being sent.

The size of master-secret key, cipher text, public-key, and aggregate key in our KAC schemes are all are kept constant size. KAC scheme is flexible in the sense that there is, no special relation is required between the classes. The key aggregation property is especially useful when the delegation key to be efficient and flexible. It is easy to key management.

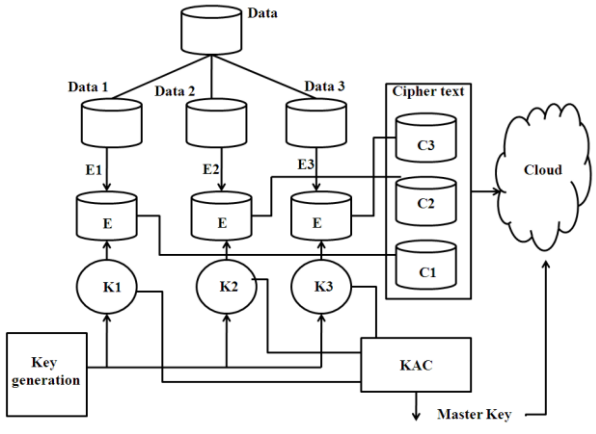

Figure 1 System design for Proposed System

The public cloud space is used in which various data are stored and access by the various users. In order to make the data secure encryption algorithm is used that generates secret key to prevent the data from the attacker .The methodology include initial data which as to be divide into the multiple chunks by using Fragmented block storage (FBS) and key

generator act as the common mediator among the multiple chunks. The key generator generates the key for each multiple chunks these chunks are the encrypted data consisting of respective secret key for each multiple chunks. The multiple keys are generated from those chunks these multiple keys are accumulated forming the master key as key aggregate cryptosystem this master key is essential key for the each multiple chunks and the initial data also.

For performing the encryption and decryption process using the Advanced Encryption Standard (AES) algorithm. AES uses a symmetric key cryptography scheme called Rijndael, a block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The algorithm can use a variable block length and key length. The latest specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits.

Algorithm for Encryption

```
Cipher(byte in[16], byte out[16], key array round key[Nr+1])
begin
        byte state[16];
        state = in;
    AddRoundKey(state, round_key[0]);
    for i = 1 to Nr-1 stepsize 1 do
    Sub Bytes (state);
    Shift Rows (state);
    Mix Columns (state);
    AddRoundKey(state, round key[i]);
    End for
    Sub Bytes (state);
    Shift Rows (state);
    AddRoundKey (state, round key[Nr]);
    End
```

Cryptography is an amazing technique with which veils the veracity of the message from superfluous users. The Key-Aggregate Cryptosystem (KAC) [8] provides an outstanding performance reducing the computational complexity of the overall algorithm. The KAC aggregates various cipher texts into cipher text classes and every class holds a secret key from which the aggregate key will be generated. This generated aggregate key holds the decryption power of any subset of cipher classes.

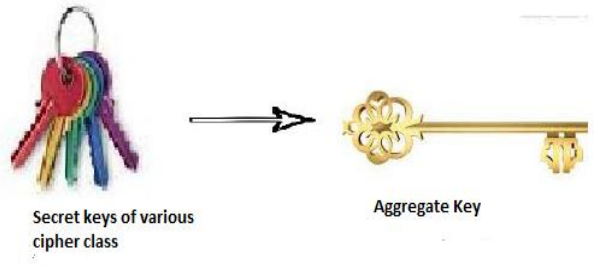

Fig 1.1 Multiple Secret Keys to Single Powerful Aggregate Key

Another advantage of this scheme is that the size of cipher text, aggregate key and the master secret key remains constant. KAC is a flexible work that the cipher text classes need not establish a relationship between each other [8].

4. KEY-AGGREGATE ENCRYPTION

The key-aggregate encryption process comprises of five polynomial-time algorithms as follows.[13] The data owner generates the public system parameter with the Setup algorithm and engenders a public/master-secret3 key pair through the KeyGen. Encryption of the messages to be stored on to the cloud can be done with the Encrypt algorithm. The master-secret key thus generated can be used to form the aggregate key in the Extract process. The generated aggregate key can be sent to delegate securely as an email or through portable devices. Finally, any client with an aggregate key can decrypt the data associated with this key receive though the process called Decrypt.

1. Setup: This is a randomized algorithm that takes no input other than the implicit security parameter.
2. KeyGen: randomly generate a public/master secret key pair (pk,msk).
3. Encrypt (pk,i,m): performed by anyone who is the owner of the data. Encrypts the data m using the public key and the index i of the cipher class and outputs C.
4. Extract (msk,S): this process results an aggregate key when we input the set of indices of the cipher class along with the master secret key.
5. Decrypt : decrypt is the process done by the one who receives the aggregate key obtaining the message m iff i ε S.

Introducing a special type of public-key encryption which calls key-aggregate cryptography system (KAC). In KAC, users encrypt a message not only under a public key, but also under an identifier of ciphertext called class. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes. More importantly, the extract key can be an aggregate key which is compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of ciphertext classes.

Framework:

Following are different framework activity perform for executing KACS encryption;

Step1: The data owner establishes the public system parameter via Setup.

Step2: It generates a public/ master-secret key pair via KeyGen.

Step3: Messages is encrypted via Encrypt .

Step4: Cipher text class is associated with the plaintext message which is to be encrypted.

Step5: The data owner uses the master-secret to generate an aggregate decryption key for a set of ciphertext classes via Extract.

Step6: The generated keys is passed to delegates securely through secure e-mails or secure channels.

Step7: Receiver with an aggregate key decrypts any ciphertext provided that the ciphertext‟s class is contained in the aggregate key.

5. CONCLUSION AND FURURE WORK

In this paper the key-aggregate cryptosystem approach is flexible as by using single key is able to decrypt multiple files. To store the aggregate key, less space is required. Through this KAC scheme, key management becomes easy. KAC reduce network bandwidth. This KAC support delegation of secret keys for different cipher text classes in cloud storage. Our approach is more flexible than other. The compressed key can only save spaces if all key-holders share a similar set. This scheme enable a content provider to share data in a confidential and selective way, with a fixed and small cipher text extension, by distributing small aggregate key.

In cloud storage, the number of ciphertexts usually grows rapidly. So we have to reserve enough ciphertext classes for the future extension. Otherwise, we need to expand the public- key.

6. REFERENCE

[1] P. Mell and T. Grance, The NIST Definition of Cloud Computing, version 15, October 7, 2009, National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov).

[2] Uma Somani,Kanika Lakhani,” Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing.”IEEE PDGC-2013.

[3] William Stallings, Cryptography and Network Security: Principles and Practices, Fifth edition, Prentice Hall, ISBN-13: 978- 0136097044, 2010.

[4] Amazon Web Services: Overview of Security Processes, may 2011.

[5] F. Guo, Y. Mu, Z. Chen, and L. Xu, “Multi-Identity Single-Key Decryption without Random Oracles,” in Proceedings of Information Security and Cryptology (Inscrypt ’07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384–398.

[6] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” in Proceedings of Advances in Cryptology - EUROCRYPT ’05, ser. LNCS,vol. 3494. Springer, 2005, pp. 457–473.

[7] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records, ” in Proceedings of ACM Workshop on Cloud Computing Security (CCSW ’09). ACM, 2009, pp. 103–114.

[8] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, Senior Member, IEEE,” Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage”.

[9] L. M. Kaufman, "Data security in the world of cloud computing,"IEEE Security & Privacy Magazine, vol. 7, pp. 61-64, July2009.

[10] K Hashizume et al., An analysis of security issues for cloud computing, Journal of Internet Services and Applications, a Springer open journal, pp 1-13, 2013.

[11] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, Ensuring Data Storage Security in Cloud Computing.

[12] K. Dubey, M. Namdev, S. Shrivastava, “Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment”, IEEE sixth international conference, 2012.

[13] Prakash G. L , Dr. Manish Prateek, Dr Inder Singh, ,“Efficient Data Security Method to Control Data in Cloud Storage System using Cryptographic Techniques ”,IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India .

[14] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records, ” in Proceedings of ACM Workshop on Cloud Computing Security (CCSW ’09). ACM, 2009, pp. 103–114.

[15] R.S.Sajjan,V. Ghorpade,V.Dalimbkar,” Key Aggregate Cryptosystem: A Different Approach for Cloud Data Security”(Paper accepted in AIM Conference).

[16] Sandha, M.Ganaga Durga,” Study on Data Security Mechanism in Cloud Computing”,IEEE conference no-33344.

[17] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, “C loud security issues” In ServicesComputing, 2009. IEEE International Conference on, page 517520, 2009.