ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2016**

# A Survey on Key Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage

S. M. Bhandare, P. P. Devkar, A. T. Divekar, R. B. Shinde, Prof. A. H. Pawar

Student, Dept. of Information Technology, SVPM's College of Engineering Baramati, Pune, Maharashtra, India

Student, Dept. of Information Technology, SVPM's College of Engineering Baramati, Pune, Maharashtra, India

Student, Dept. of Information Technology, SVPM's College of Engineering Baramati, Pune, Maharashtra, India

Student, Dept. of Information Technology, SVPM's College of Engineering Baramati, Pune, Maharashtra, India

Assistant Professor, Dept. of Information Technology, SVPM's College of Engineering Baramati, Pune, Maharashtra, India

**ABSTRACT**: In cloud storage Data sharing is most important. Nowadays, Cloud Computing is widely used. Using which data can be easily outsourced on cloud can access easily. User can access the remote services provided by cloud in any corner of the world. So, there is need to share the data securely. In cloud storage main need is securely storage of user's data. The important thing is authentication is necessary to provide the secure storage of the data. Anyone can share the data on cloud as the want. Data owner can share the data safely using cryptosystem. Cryptosystem provides the encryption of the data. So, data owner can easily upload the data on cloud. The encryption and decryption key are generated for different data. The decryption keys are generated and shared for only the data which is selected by user for decryption. Master secret key is generated for encryption of the data. For decryption the constant size aggregate key is generated. While performing the generation of aggregate key, the secret keys are extracted and formed in single compact key. This compact aggregate key can efficiently and securely send to the user via secure channel or via email.

**KEYWORDS**:Cloud Computing, Cloud Storage, Data Sharing, Key Aggregate Encryption.

## I. INTRODUCTION

Nowadays, the most popular and widely used technology is cloud computing. And it is also used as a core technology for private applications. Data can be stored on remote server rather than hard disk or any physical storage. Cloud provide the huge number of applications and services to the customers. This services and applications are shared among customers with good qualities. As the large number of functionality provided by cloud, the cloud computing perform the management of data. Nowadays, it is easy to apply for free account of photo album, email, file sharing. The maximum storage size is provided is more than 25GB.

The user as well as enterprise can store the data on cloud with flexibly and with minimum cost. It is necessary to focused on the security concern which is insider attack, to avoid this problem data can be encrypted before upload it on cloud. Different users data can stored on single cloud in encrypted format. In cloud there is chances of leakageof private data which is stored on cloud. So to encrypt the data before uploading on cloud. And use the constant size key.

The main problem is how to share the data securely and efficiently. The solution is cryptography. The main concern how to encrypt the data before sharing. The important thing is to encrypt the data and give the right access to the other user for decrypt the data. This decryption key is send via secure channel or email. For example, John wants to share his private data on drop box. But he doesn't want to share his data with everyone. But one day his friend Jenny asked his to share his private photos taken over the last year. But John doesn't want to share his all photos to Jenny. It is possible for hacker to hack the data. He can encrypt data by using his own key before upload on cloud. There are two possibility of encryption, either john can encrypt the all data with single key or encrypt the data with distinct key for different data. In first method, if the key is leaked then all data which is encrypted with that single key may leaked. In second method, using distinct key encryption increases the complexity and cost. Because, if number of files and thousands of photos are encrypted then number of keys needed to encrypt them. This decreases the efficiency.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2016**

A new technique of encryption and decryption is implemented which provide the more efficiency than the existing one. i.e. Key Aggregate Cryptosystem(KAC). In key aggregate cryptosystem the encryption is performed using identifier of cipher text which is known as class. So that cipher text are categorized into different classes. The key owner holds the master secrete key which is useful for extracting the key. After that John send key to the jenny via secure channel or email. Using this key Jenny can be easily download data from drop box and decrypt it, which is shown in fig1.

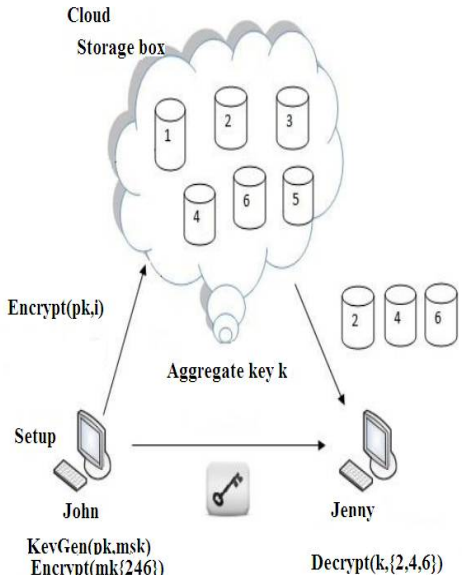


Fig .1 File sharing between John and Jenny

## II. LITERATURE SURVEY

In daily life generation cloud computing is visualizes architecture. The risk of attacker can attack the private data on user and leak the user identity. While the need is authentication is necessary for cloud user and service provider. The service provider and users both are not compromised then issue will be arises. The need of user is accessing data locally that present on remote side with flexible use of cloud storage. There is need to inspect the data set on cloud. There is many cloud users that wants to upload data without using its personal information.

The Attribute-Based Encryption (ABE) is another way to sharing encrypted data. Encrypting each part of data is worse than equivalent user attribute to encrypt data. The attribute decrypt the cipher text is matched only a particular key in Attribute-Based Encryption. For Decrypting a particular Cipher text the user key and attribute must be match.

A hierarchical access control accomplished by Multi group key management by applying multiple group authorities with handling group keys for different user and also integrated key graph. Tree structure is used by centralized key management plan to minimize Storage overload, Communication and Processing of Data. It updates and also maintain keying related things. For every users an integrated key graph is accomplished.

A vital primary things of Identity based Cryptography is Identity-Based Encryption. Different information of user's identity is contained by the public key of user. The Domain name or textual value can be Key. The public Key infrastructure is deployed using IDE. For public key encryption identity of the user is used as identity string .In IBE another name of trusted party is private key generator which gives according to user identity master secrete key and secrete key. The identity of user to encrypt data and public value collaborated by data owner. By using secrete key decrypt the cipher text.

The user must get a particular key related to attribute while decrypting a message in multi attribute authorities number of attribute are analyzed regarding the decryption key. The user those who have attribute identity without interaction between each other are allocated independently decryption keys. Real time deployment attribute which is based on privileges is allowed by multi authority attribute based encryption as different attribute are issued by different

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2016**

authority. Confidentiality is maintain by central authority due to attribute authority ensure the honesty of user privileges.

## III. PROPOSED SYSTEM

A Key Aggregate Encryption technique consist of five polynomial time algorithm which given below. This polynomial time algorithm which is used for encryption of data.

The data owner which generate setup parameter using setup and generate the master secrete key which is used for encrypt the data using key gen. Encrypt function is used for encryption of message also it defines cipher text classes. Extract function is used for extracting the secrete key to generate the aggregate key and this aggregate key is used for decryption of data. After that Decrypt function is used. This Decrypt function uses the aggregate key for decrypting the data.

### *A. Setup Phase*

Using setup phase data owner can create account on untrusted server. This setup phase takes only the security parameters which is use for performing setup operation.

### *B. KeyGen Phase*

The data owner is execute the keygen phase for generating the private key master secrete key (pk, msk).

### *C. Encrypt Phase*

Anyone can execute encrypt phase who wants to store encrypted data on server. Encrypt function takes the actual original massage, private key and index (pk,m,i). The encryption algorithm takes the input message m and produces output cipher text c. Only the users who has set of attributes which are used for decryption.

### *D. Extract Phase*

The extraction phase is executed by the data owner, who gives the delegating power to the delegatee for the certain set of cipher text classes.

### *E. Decrypt Phase*

The decryption phase is executed by delegatee after receiving the aggregate key which is used for decryption of data (Ks, S, i, c).

## IV. METHODS AND ALGORITHMS

### *A. AES Algorithm*

*AES* is a new cryptographic algorithm which is used for protecting data. It is block cipher technique which generate the size of 128 bit, 192 bit, 256 bit.

Several steps are included in AES algorithm:

Step 1: Key Expansions

For each round AES needs a different 128-bit block of round key also one more.

Step 2: Initial Round

Add Round Key with a block of the round key, each byte of the state is combined using

Bitwise xor.

Step 3: Rounds

- Sub Bytes in this step each byte is replaced with another byte.
- Shift Rows for a certain number of steps, the states last three rows are moved cyclically.
- Mix Columns on the columns of the state a mixing operation operates, in each

Column combining the four bytes.

Step 4: Add Round Key

Step 5: Final Round (no Mix Columns)

- Sub Bytes
- Shift Rows
- Add Round Key.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2016**

*B. MD5 Algorithm*

MD5 algorithm is used to find the message digest. When the input is variable size then MD5 takes input and produces the output as fixed size output.

Following are the steps which is performed in MD5-

- Append the padding bit

Append the bit to message so its length is congruent to 448, modulo 512.

- Appending length

A b bit with 64 bit representation is appended to the result of previous step.

- Initialization of MD buffer

To compute the message digest a four word buffer (A,B,C,D) is used.

These four word registers are initialized with following values in hexadecimal-

First word A: 01 23 45 67

Second word B: 89 ab cd ef

Third word C: fe dc ba 98

Fourth word D: 76 54 32 10

- Process message in 16 word blocks

In this step the three 32-bit word input is used by four auxiliary function which produces the output in one 32-bit word.

- Output

This algorithm produce the output in A, B, C, D.

## V. CONCLUSION

TData sharing is an important thing in cloud storage. End user upload there data on a cloud with different user using encryption scheme. Using encryption can provide the secure sharing of the data to users. The decryption key i.e. aggregate key can be shared easily via email or any other secure channel. This plays very important role. In cloud storage cryptosystem provides delegation of decryption key for different cipher text classes. It provides the aggregate key of constant size.

## REFERENCES

1. B. S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.
2. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans.Computers, vol. 62, no. 2, pp. 362–375, 2013.
3. 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
4. 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" IEEE Transactions On Parallel And Distributed System, Vol 25, No. 2 February 2014.
5. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data,"in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp. 89–98.
6. Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," in Proceedings of the 23th IEEE International Conference on Computer Communications (INFOCOM '04). IEEE, 2004.
7. D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proceedings of Advances in Cryptology – CRYPTO '01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229.
8. M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in CM Conference on Computer and Communications Security, 2009, pp. 121–130.
9. D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.
10. 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.
11. 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.
12. W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Transactions on Knowledge and Data Engineering (TKDE), vol. 14, no. 1, pp. 182–188,2002.
13. A. Brink, "Thresholding of digital images using two-dimensional entropies," Pattern Recognit., vol. 25, no. 8, pp. 803–808, 1992.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Vol. 4, Issue 3, March 2016

**BIOGRAPHY**

**Miss. S. M. Bhandare**, is Student at Information Technology. Dept. SVPM's College of Engineering Baramati, Maharashtra

**Miss. P. P. Devkar**, is Student at Information Technology. Dept. SVPM's College of Engineering Baramati, Maharashtra

**Miss. A. T. Divekar**, is Student at Information Technology. Dept. SVPM's College of Engineering Baramati, Maharashtra

**Miss. R. B. Shinde**, is Student at Information Technology. Dept. SVPM's College of Engineering Baramati, Maharashtra

**Prof. A. H. Pawar** is Assistant Professor, at Information Technology. Dept. SVPM's College of Engineering Baramati, Maharashtra