IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-10 E-ISSN: 2347-2693

A Secure and Scalable Data Sharing using Key Aggregate Crypto System

Bharati A. Patil

Dept. of Computer Engineering, SITRC, SPPU University, Nashik, India

*Corresponding Author: bharati.patil@sitrc.org

Available online at: www.ijcseonline.org

Received: 15/Sep/2017, Revised: 28/Sep/2017, Accepted: 19/Oct/2017, Published: 30/Oct/2017

***Abstract*—** Today, gaining popularity privacy for accessing outsourcing data stored on cloud is a major issue in cloud computing. In cloud storage data is stored on single physical machine and this stored data may shared by multiple users from different machines. User doesn't have control on accessing outsourced data. For identification of leaked data to everyone data access security or privacy for data is a challenging section. To store as well for sharing data securely Cryptosystem is used. In cryptosystem before storing data on cloud user firstly encrypt data then placed it on cloud. And then data decryption is performed when user want to access it. This task may require multiple keys for data encryption as well as data decryption. In proposed system key-aggregation is implemented on concept on merging or aggregating the encryption and decryption key into single one in cryptosystem for sharing of scalable data. It is very compressed formed of aggregation of key. In proposed approach unique key can hold multiple keys that are required. In proposed system concentrate on sharing data securely, efficiently among multiple users. Sharing data and delegation of data is possible as fixed sized of data blocks are created. In this proposed system implements Shamir secret sharing algorithm for securely, sharing aggregate key for multiple users.

Index Terms—Cloud storage, data sharing, key-aggregate encryption, patient-controlled encryption.

I. INTRODUCTION

This outsourcing of data is increasingly demanded in enterprise settings. In outsourcing of data there are chances of stolen data from virtual machine. On separate virtual machine is used to access the data of cloud stored on single physical machine. Previously, ABE scheme is used for pairing operations that is required for decryption of data. This ABE scheme is a very expensive because it requires n-number of pairing for decryption of data. The proposed system helps to solve the challenges occurred in the previous systems. The proposed system provide compressed from of secret key. In proposed system key owner have master key which contains different keys required for encryption as well decryption of different cipher text class. Proposed system supports KAC scheme which contains various security levels. It has compressed form. Data encryption can be done using encryption keys. But there is an issue of key management. N-number of such keys needed to shared data. For transformations of such secret keys needs safe channel,and also its storage is more Hence there is a chances of growth in costs as well as evaluation complexities as the number of keys are in-creased. In short, it is very heavy and costly to do that. Therefore, the best technique to solve this is that owner encrypts files with distinct public-keys, but only sends receiver a single decryption key. There is a need of a secured channel for sending decryption key and kept secret, small key size is always desirable in this case which is achieved in proposed approach. Hence, proposed approach works on to create decryption key more secured and inertial in the way that it supports multiple decryption of cipher texts, without increasing its size. Hence in the proposed model promotes the public key encryption scheme. In this scheme owner will encrypt the data with the master key and supplementary delegation is to be done in way that further data can decrypted with constant size decryption key. As explained above KAC can achieve this at great extend. This paper further discussed about related work in section II, then proposed system architecture and its working flow in section III. Moving forward we define algorithm and system mathematical model for our system in section IV. Finally, we conclude our system in section V.

II. RELATED WORK

Cheng-Kang Chu, Sherman S. et al.[1], represent the solution known as public-key encryption for KAC i.e. key-aggregate cryptosystem. In this system, user is able to encrypt messages under any class of cipher-text, in this scheme, data owner have key known as master key. This key is in the compressed form. It holds all the other keys required for encryption and decryption and provides security levels as well as it provides flexible hierarchical key assignment. D. Boneh, C. Gentry, B. Lynn, and H. Shacham[2] introduced an aggregate key or a signature approaches. An aggregate key is build from short signature scheme. It is implemented using bilinear maps. To reduce certificate chains and it also reduces message size in secure way for routing protocols. This system,mainly verifies

encrypted signatures are used through aggregation. M. J. Atallah, M. Blanton, Frikken, et al.[3] provide methodology for theproblem of access control in an arbitrary hierarchy. It accessed a descendants key from its parent key which required hash functions. Thissystem also modifies Cramptons extensions of the standard hierarchies to limited depth and reverse inheritance. J. Benaloh, M. Chase, E.Horvitz, and K. Lauter [4] described concrete PCE to form an efficient system. It allows patients to perform searches and to share partial access rights with others, over their records. In this system, if server has been compromised then security is still guaranteed. For producing a root secret key DirKeyGen algorithm is used. FormDirEntry is required to make secret key as private and DecDirEntry is used for decryption. A CCA-secure Hierarchical Identity Based Encryption (HIBE) scheme is implemented to provide data security. F. Guo, Y. Mu, Z. Chen, and L. Xu [5] introduced, identity- based set encryption (IBSE), and described IBTT scheme 2 from IBSE and fingerprint codes based on the Boneh-Naor paradigm. IBTT scheme is short and more secure for random oracle model for both private key and cipher-text. They described MISKD scheme, this is mostly secured than previous one. V. Goyal, O. Pandey, A. Sahai, [6] suggested a Key-Policy Attribute-Based Encryption (KPABE) cryptosystem is proposed. It is used for fine-grained sharing of encrypted data. In this cryptosystem ciphertexts are high lighted with a set of attributes as well as private keys are generated with access structures. It is used to enable a user for the decryption. This new construction supports all MSP based access structures. In fine grained access control, data is stored on the server in an encrypted an user can be decrypting various pieces of data using defined security policy. To contribute a secret with different parties or group Secret-sharing schemes (SSS) are used. S. G. Akl and P. D. Taylor [7], represents a scheme known as cryptosystem for controlling data access. In this, organization data used POset. This scheme is useful in distributed system. This scheme is hosted on different operating of security and further communicates through csn. Encrypted messages are broadcast into the network of cloud security. G. C. Chick and S. E. Tavares [8], providing representation of master key system based on modular exponentiation. It is required for improve access to an intent of services in cryptographic system. To derive keys neededfor accessible services master key is used. W. G. Tzeng [9], describes a time-bound crypto graphic key assignment scheme. For each time period, different cryptographic keys of a class are required in this system. Bilinear order is preferred for partially ordered classes. It contains multiple time-dependant keys that are correspond to time-period. They describes two schemes for broadcasting an authorized user in multilevel. CA scheme is implemented to assigns key in hierarchy of the classes..

III. METHODOLOGY

In proposed system the algorithm used is Aggregate key generation Algorithm, AES algorithm, Shamir secrete sharing. For the creation of the aggregate key the Aggregate key generation algorithm is used. The aggregate key is created by using master key, class and secret code. AES Algorithm is use for Encryption at the time of uploading and Decryption purpose at the time of downloading. Shamir Secrete Sharing algorithm is used for sharing aggregate key securely with user.

1. Aggregate Key Generation Algorithm:

Aggregate key generation algorithm use the inputs such as Master Key, Class, Secrete code and create aggregate key. Aggregate key is used for securely transfer the data or files over the big network.

Input:-k1=Master Key, k2=Class, k3=Secrete CodeOutput:-Secure Aggregate key

Processing:-

1) First Set the Data

2) Initially all keys like k1, K2, k3 are in string format then it will convert into bytes i.e. in number using Byte Encoder.

3) Then every string converted in string to

number like,

k1=234

k2=567

k3=891

4) All set key combine then it can give separator for that different key like, 234 0 567 0 891 here no value consider as separator.

5) Secrete Aggregate Key i.e., S.

6) Key convolution: we are use the quadratic equation,

f(x) = (n 1 x + n 2 x 2 + S) here the x is consider as 2 or any number.

7) Secure Aggregate Key = f(x) XOR S

8) Key is Created.

Process of Generating the Aggregate Key with Example

Let k1=234, K2=567, k3=891

By applying the zero as separator we get one

number 23405670891.

S=23405670891.

Key Convolution: use following quadratic Equation

F(x) = (n 1 x + n 2 x 2 + S),

Where n 1 =66, n 2 =192

Where x=number of files selected for sharing.

F(x) = (66*3) + (192*3*3) +23405670891Key = f(x) XOR S

1.AES Algorithm:

AES Algorithm is use for Encryption and De-cryption purpose at the time of uploading and downloading the document by the user. Advance Encryption Standard is a symmetric key block cipher. AES is a non-Feistel cipher that encrypt and decrypts 128-bits block of the data. The size of the key can be 128,129 or 256-bits. It depends on the number of rounds The number of the rounds:

10 rounds for 128-bits,

12 rounds for 192-bits,

14 rounds for 256-bits.

Input:- Secret Aggregate Key k, Message M

Output:- Encrypted Message EM

Processing:

1) Key Expansions Round:

Keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2) Initial Round:

Add RoundKey each byte of the state is combined or added with a block of the round key using bitwise XOR.

3) Rounds:

-SubBytes: a non-linear substitution is performed where each byte is replace with another according to a lookup table.

-ShiftRows: a transposition of byte is done where the last three rows of the state are shifted cyclically at a certain number of steps.

-MixColumns a mixing operation is performed in which the columns of the state is combining the four bytes in each column.

-Add Round Key

4) Final Round (no Mix Columns)

-S-Sub Bytes.

-Shift Rows.

-Add Round Key

Shamir secret sharing:

1) In cryptography, secret key sharing is method for distributing a secret key amongst a group of participants, each of which is allocated a share of the secret

2) Key is to divided into n pieces K1, ..., Kn in such a way that

IV. SYSTEM OVERVIEW

ABE scheme is used to encrypt and decrypt data. This operation is expensive for resource limited devices because of pairing feature. As number of pairing operation grows the complexity of system also increases. Pairing operations are dependent on access policies. Along with this secure key sharing is important aspect. Data encryption is achieved in proposed system. For this AES algorithm is used. While doing this encryption process number of keys are generated this generates the issues of sharing and key management overheads. In proposed system this issue can be handled using aggregate key technology. Aggregate key is shared on email hence to make it more secure Shamir Secret Sharing process is involved in sharing activity as part of contribution.

The above observation motivates us to work with aggregate key generation as well as the secure key sharing.

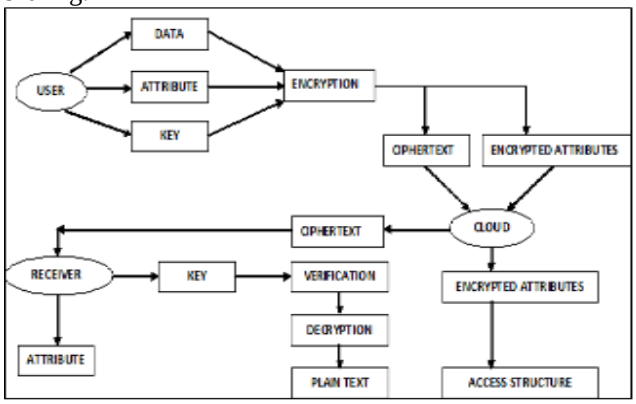

Fig. 1. System Architecture

V. SETUP PHASE

Initially the setup algorithm does not take any input. This algorithm only required a implicit security parameter. And the output s of this algorithm will be a public key parameters and master key MK parameters

2 ENCRYPT PHASE

Encrypt(PK,M, A). Here the encryption algorithm takes input as the public parameters PK which are created in setup phase, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt message M and produce a ciphertext CT. This generated ciphertext conains acess policy attributes such that the user only possesses a set of attributes which satises the access structure that will be able to decrypt the message. We will assume that the ciphertext implicitly contains A

KEY GEN PHASE

Key Generation(MK,S).In the key generationalgorithm user takes input as the master key MK which are generated in setup phase and a set of attributes S that describe the key.By using this key generation algorithm user creates its own private key SK

SHARE KEY

Shamir secret sharing mechanism is used to share data among multiple users. This technique is useful to securely transfer data.

DECRYPT PHASE

Decrypt (PK, CT, SK).This algorithm will be used to create a original message from cipher text. The decryption algorithm takes input as a cipher text CT, which contains an access policy A, the public parameters PK, and a private key SK, which is a private key for a set S of attributes. If the set Sofattributes satises the access structure A then the algorithm will decrypt the cipher text and return a message

VI. ANALYTICAL ANALYSIS

UF3 = download document
The proposed system is a novel approach
UF4 = generate aggregate key using k shares
to provide confidentiality and authentication

UF4P1,P2,..Pk→O2

Following is the

UF5 = decrypt document

Mathematical Model

UF5(O2,I3)→O1

S = O, U, C WHERE,

UF6 = Save document

O= Owner system

U= Users System

C = CI, CO, CF Cloud system

C= Cloud system

CI= I1, I2,I3,I4 WHERE,

I1= User Details

O = OI, OO, OF Owner system

I2 = D1, D2.,Dn Set of encrypted document

OI = I1, I2, I3, I4, I5 WHERE,

I3 = Class name

I1 = User Details

I4 = Access Rights

I2 = Master Key

I3 = Document class

I4 = document

I5 = Sharing Rights

OO = O1, O2,O3 WHERE,

O1 = User Account

O2 = Encrypted document

O3 =Aggregate key

CO= O1,O2 WHERE,

O1 = User Account

O2 = file storage

O3 = Set of class filesD1, D2.,Dn

CF= CF1, CF2, CF3, CF4 WHERE,

CF1 = Register user

CF1(I1)→O1

OF=OF1,OF2,OF3,OF4,OF5,OF6,OF7WHERE,
CF2 = Validate user

OF1=User Registration

CF3 = Save document

OF1(I1)→O1

CF3(I2, I3,I4)→O2

OF2=Login

CF4 = download document

VII. CONCLUSION

Data encryption is achieved in proposed sys- tem. For this AES algorithm is use. While doing this encryption process number of keys are generated this generates the issues of sharing and key management overheads. In proposed system is issue can be handled using aggregate key technology. Aggregate key is shared on email hence to make it more secure Shamir Secret Sharing process is involved in sharing activity as part of contribution. So, proposed approach constructs good solution for data privacy and sharing segments.

REFERENCES

[1] Chu, C. K., Chow, S. S., Tzeng, W. G., Zhou, J., & Deng, R. H. (2014*). Key-aggregate cryptosystem for scalable data sharing in cloud storage*. IEEE transactions on parallel and distributed systems, *25*(2), 468-477.

[2] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, *Dynamic and Efficient Key Management for Access Hi-erarchies*, ACM Transactions on Information and SystemSecurity (TISSEC), vol. 12, no. 3, 2009. 416432.

[3]J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, *Patient Controlled Encryption:*, in Proceedings of ACM Work-shopCloud Computing. ACM, 2009, pp. 103114.

[4] F. Guo, Y. Mu, Z. Chen, and L. Xu, *Multi-Identity Single-Key Decryption without Random Oracles*, in Proceedingsof Information Security and Cryptology (Inscrypt 07), ser.LNCS, vol. 4990.Springer, 2007, pp. 384398.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, *Attribute-Based Encryption for Fine-Grained Access Control of En-crypted data*, in Proceedings of the 13th ACM conferenceon Computer security. ACM, 2006, pp. 8998.

[6] S. G. Akl and P. D. Taylor, *Cryptographic Solution to aProblem of Access Control in a Hierarchy*, ACM Trans-actions on Computer Systems (TOCS), vol. 1, no. 3, pp. 239-248, 1983.

