SCALABLE CRYPTOGRAPHIC COMMUNITY OF DATA SHARING IN CLOUD

R. Anjaneyulu[1], M. Raghavendrarao[2]

[1]PursuingM.Tech (CSE), [2] Assistant Professor (CSE)

Holy Mary Institute of Technology and Science (HITS), Bogaram Village, Keesara Mandal,
Ranga Reddy (D), Telangana (India)

ABSTRACT

The main functionality of cloud storage is Data sharing. In this paper we discuss about how to share data with others in cloud storage, provide with securely, flexibly and efficiently. We introduce new technique is "Public Key Crypto systems ".This generates fixed size cipher texts that help efficient decryption for any different sets of cipher text as possible. The new method is one can that combined any set of different secret keysand make them form as a single key. But expand the power of all the keys being aggregated (combined)to explain in other words the secret key user can release fixed size aggregate key for convenient choice cipher text set in cloud storage, remain encrypted files stored in confidential. This key flexibly sent to other users or with small secure storage, the secure key to be stored in smartcard. In the standard model provide formal security analysis of our schemes.In our schemes provide for flexibly hierarchy gives first efficient public encryption scheme.

I. INTRODUCTION

In enterprise settings, different organizations cloud storage was more popular. In cloud data out sourcing,this gives strategic management of corporate data. In cloud storage upload different files and user can access files through mobile, emails at any place in world wide.In cloud data can upload different users/clients host data on separate virtual machines on single physical machine. Destination virtual machines connect with another virtual machine. Based on availability of files there are a series of cryptographic schemes allowing third party users data without releasing information about the data. Sharing user's data is the main advantage of cloud.In internet user create blogs, post ads and sharing the data like etc in social networking. If user share his files with some peoples and security encrypt files with help of security key. In big enterprises and organizations employs share and download secure files. The main problem is how to transfer data effectively in share encrypted data. However, recognize an efficient and secure way to transfer temporary data in cloud storage is not a difficult.

In cryptography the main problem we often think about strong the security for apiece of knowledge, into ability perform different cryptographic functions like encryptions and authentication for number of times.In this paper now we study to generate a decryption key more powerful in sense decryption of a multiple cipher texts without changing its size.In existing system have a problem is to develop an more efficient encryption scheme for public key which belongs to a subset of different cipher texts is decrypt able by fixed size decryption key.It generated based on the master secret key to overcome this problem we introduce a special future is public key encryption, is called Key aggregate crypto system (KAC).

II. KEY AGGREGATE CRYPTO SYSTEM (KAC)

In normal encryption key encrypted in this KAC, users encrypt message not only public key, but also under an identifier of cipher text called class. Cipher texts are can be divided into different classes. The key user save a major secret called master –secret key, this can be utilized to separate secret keys for different classes. Most importantly the separated key have aggregated key which is as generate a compact secret key for a single class. But combined the power of many such keys, i,eMost importantly, the separated key have can be an aggregate key which is as 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. The size or length of the secret key, master key, cipher text and KAC schemes are equal size.

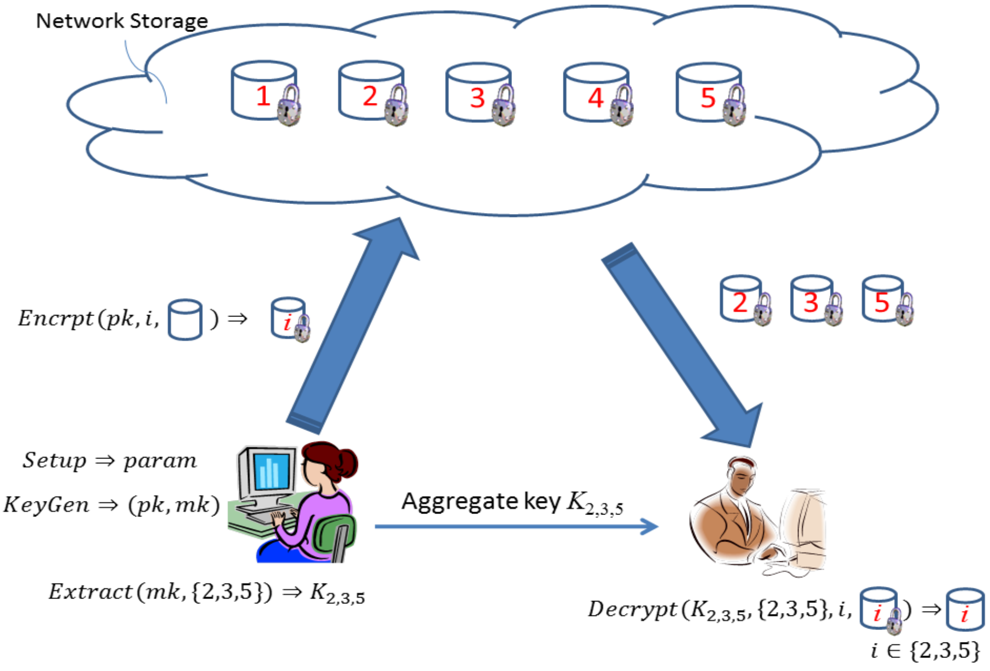
Frame work: A key aggregate encryption scheme follows steps

- User of the data owner discovered the public system variable through setup.
- Generate a public and master secret key pair using KeyGen.

Messages can be encrypted through encrypt by anyone user also decides which message was associated of cipher text with normal text message to be encrypted. The user can generate the aggregate decryption key with help of master secret key for different set of cipher text though extract now generated keys can be passed to other users securely via secure mail or secure devices. In the last phase user with the help of aggregate key can decrypt any cipher text's class is contained in the cipher text provided that cipher text aggregate key through the decrypt.

2.1 Sharing Encrypted Data

An accepted application key Aggregate crypto system is sharing the data. The aggregation of a key propriety is useful when we expect the references to be flexible and efficient. The main aim of this scheme is content share data in a secure and confidential way along with a little bit size of cipher text expansions, by sending to each authorized user with a single aggregate key.


Network Storage
1
2
3
4
5
$Encrpt(pk, i,$ $) \Rightarrow$ i
2
3
5
$Setup \Rightarrow param$
$KeyGen \Rightarrow (pk, mk)$
Aggregate key $K_{2,3,5}$
$Extract(mk, \{2,3,5\}) \Rightarrow K_{2,3,5}$
$Decrypt(K_{2,3,5}, \{2,3,5\}, i,$ i $) \Rightarrow$ i
$i \in \{2,3,5\}$

Now we discuss the main objective of data sharing in cloud storage with the help of key aggregate crypto system. Let see one example of sharing encrypted data in cloud, suppose data owner have share photos show in the above figure, a1,a2,a3,a4,a5…….On the server. First generate to public key, master secret key, cipher text and encrypted key, now generate Setup to get a parameter and execute after gen KeyGen and pair generated that is public key and master secret key(pk,msk).The system generated parameter and param public key and master secret key should be save in dataowner. If any person wants to encrypt by each shared photo then using encryption of master key, public key and encrypted data uploaded to the server, with public key and parameter. User'shelps to the user upload data on the server. Once user share data in cloud of other users who aggregate the shared key by performing the extract of master secret and fixed size this is sent to another shared person through secure mail.In the next step user got an aggregate key, now he download the authorized files for each file decrypt the code and download files.

III. COMPARE OF KAC WITH ADJUSTED KEY ENCRYPTION SCHEME

In this section compare with Key aggregate crypto system with other adjusting possible solutions for sharing a secure data in cloud storage, like those are

- Compact key in symmetric – key encryption.()
- Compact key in identity based Encryption.(IBE).
- Attribute –based encryption.(ABE)

IV. CRYPTOGRAPHIC KEYS FOR A PREDEFINED HIERARCHY

The aim of the cryptographic or security of the data in cloud provide the security of a user data.In cryptographic system is to reduce the cost of a storing the key and managing the security. Secrete key for the purpose of cryptographic.In basic structure of tree hierarchy containing nodes and sub nodes.Granted permissions of a main node then share files in descent nodes.

V. COMPACT KEY IN SYMMETRIC –KEY ENCRYPTION

Compact key symmetric key encryption problem is supporting hierarchy flexible delegation power of decryption. Benalohwas proposed an encryption scheme it mainly apply for trans mitting large number of keys in broadcast of telecommunication. In compact key encryption is try to minimize the size of symmetric encryption in authentication.

VI. COMPACT KEY IN IDENTITY BASED ENCRYPTION (IBE)

It is the one type of public key encryption is identity based encryption.Inthis a user can send identity string through secure mail. In middle adjust a trusted party is called private key generator.In identity based encryption user holds a secure master secrete key, secrete key issue based on the trustee authentication, user encrypt the public key with message and receiver decrypt the cipher text with help of secrete key.

6.1 Attribute Based Encryption

In attribute based encryption user encrypt the code cipher text and along with one attribute, master secrect key user separate a secret key based on a policy of this attributes, so cipher text decryption can be based on the related attribute conforms of the method.

VII. PUBLIC KEY EXTENSIONS

If user wants to divided is cipher text into more than one class user can register more than one public key and more than one master secret key that is number of pairs . Now cipher text in each class index in each class and increase the number of added classes, because public key is single and it is treated for only single user. If that key is shared to another user is not possible, but we need achieve shorter and strong key. In public key extension we achieve local aggregation that means the secret key and aggregation key belongs to the same branch.

In the last node of a tree for better illustration of change feature.In that advantage is still manage when differeciate between quaternary trees in hierarchical method which is increase references the decryption power node for all nodes if the key is adjusted for parent node is delegated, also number of classes will be equal to number of keys .

VIII. FUTURE IMPLEMENTATION

In key aggregate crypto systems limited that is predefined bound of more number of a cipher text classes is limited. In cloud daily number of users login and upload data so that number cipher text increase rapidly day by day. So in future extension developing and reserved the maximum cipher classes. In the present project cipher text, encrypted data is limited fixed size, so if anyone knows size remaining also has a same size. So in future implementation independent length for all cipher text, another problem is secure sending delegates sending secure with sending mail and another secure device. If one key is broken automatically code will be change so use secures in future extensions.

IX. CONCLUSION

In cloud storage the main question is how to protect and provide secure of the user data in cloud with the help of mathematical operations and encrypted methods and cryptographic system methods. Different key and multiple times decryption the code in user‘s data in cloud. In this project using KAC is key aggregate crypto system in that equal size of cipher text in decrypting code with the using of public key, master secret key and one fixed size code will be sent into the users through secure mail transaction. This is help for provide the security of user’s data in cloud with a fixed size of cipher text , public key ,master secret key.

REFERENCES

[1]. L. Hardesty, “Secure computers aren’t so secure,” MIT press,2009, http:// www.physorg.com/news176107396.html.

[2]. 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.

[3]. T. Okamoto and K. Takashima, ―Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption,‖ in Cryptology and Network Security (CANS '11), 2011, pp. 138–159.

[4]. Data sharing in cloud storage with key-aggregate cryptosystem. Mrs. Komal Kate, Prof. S. D. PotdukhePG Scholar, Department of Computer Engineering, ZES COER, pune, Maharashtra Assistant Professor, Department of Computer Engineering, ZES COER, pune, Maharashtra.

[5]. R. Canetti and S. Hohenberger, "Chosen-Ciphertext Secure ProxyRe-Encryption," in Proceedings of the 14th ACM Conference onComputer and Communications Security (CCS '07). ACM, 2007, pp. 185–194.

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

AUTHOR DETAILS

R.ANJANEYULU pursuing M.Tech (CSE) from Holy Mary Institute of Technology and Science(HITS)	
M. RAGHAVENDRARAO working as Assistant Professor(CSE) from Holy Mary Institute of Technology and Science(HITS)., is a young, decent, dynamic Renowned Educationist and Eminent Academician, has overall 07 years of teaching experience.	