A Noval Approach Key Aggregate Cryptosystem for Resizable Data Sharing in Cloud Storage

Shivadatt D Chame[1], Anil Kumar[2]

[1]*Mtech Student, Computer science and Engineering, Arkay college of Engineering and Technology, T.S, India*

[2] *Assistant Professor, Computer science and Engineering, Arkay college of Engineering and Technology, T.S, India*

Abstract—gigantic research has been done on Cloud computing security and a large number of papers have been published on this topic during the last few decades. Very few worked on Secured data sharing in cloud storage using Key Aggregate Approach. In the new technology of cloud computing platform introduces the distributed cloud resources. This Paper explains how to securely, distribute the data with others in cloud in [1]. This Paper gives a public key cryptosystem, which produces constant size Cipher texts [1]. In this paper implemented the new methods how efficiently shares the data with others in Cloud storage [2][6]. The proposed Approach gives the new techniques for Aggregate Key Cryptosystem for Resizable data on cloud storage [1].

Keywords— Public Key Encryption, Proposed Key Aggregate System.

Introduction

Cloud computing (CC) has grew a lot of attention in current years as cloud computing is characterized as a style of computing abilities delivered and utilizing the internet technology [1]. Cloud computing basically stores all cloud computing app and databases which are put at Remote areas. Because of this development of software, data and services are not trustworthy. Hence, this leads to challenges like virtualization vulnerabilities, availability vulnerabilities.

Cloud computing is Internet positioned cultivation and use of computer technology. It is an approach of computing in which dynamically [1] scalable and often resources are provided as a service over the Internet. The actual term "cloud" borrows from telephony in that telecommunications companies, Cloud service provider offering "(VPN)" services at a lower cost. Cloud computing is a better way to run your business. They run on a shared data center instead of running your apps yourself. Any user are able to access information from anywhere [3][6] and at any time instead of having to use dedicated machine [3] [4].

METHODS

Cryptanalysis Key for Hierarchical Approach

We take the tree structure Alice can first classify the cipher text classes like Figure 3. Each node in the tree represents a secret key [1], while the leaf nodes represents the keys for individual cipher[1] text classes [1][2]. Black circles represent the keys for the classes to be delegated [2] and circles circumvented by dotted lines [1] represent the keys to be granted.

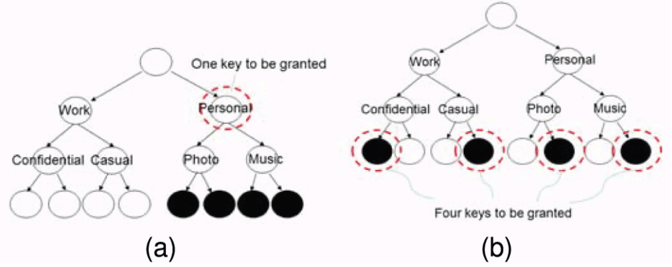


Fig 2.1 Cryptographic Keys for Predefined Hierarchy

In Figure 3(a), if Alice wants to share files in the "personal" category [1][2], she needs to grant the key for the node personal category [2], which automatically grants the delegate [4] the keys of all the descendant nodes(photo and music)[1]. This is the ideal case, where most classes to be shared [6] belong to the parent key of them is sufficient.

However, As shown in Figure 3(b), if Alice shares her demo music at work (work→casual→demo and work→confidential→demo) in [1] [3] who also has the rights to see some of her personal data, which leads to an increase in the total key size [3]. This approach is not flexible when the classifications [5] are more complex and she share different sets of files to different people [6]. On average, the number of keys increases with the number of branches.

Symmetric Key Cryptography

Benaloh proposed an encryption scheme, where a huge number of keys can be sent rapidly. The Procedure is as follows. Initially pick two prime [6] numbers p and q for a module. Master secret key will be chosen and prime numbers will be allied with the class. The outcome of this is a constant size key. So here the sender should encrypt files with secret keys [2] which will not be feasible.

Algorithm:

1. Read Input File data
2. Using single key produce cipher texts from plain text file.
3. Send this key to the receiver for decryption

Fig 1: ALGORITHM TO PROPORTIONATE KEY ENCRYPION

Numerous Private Key Encipher Algorithms Available as AES and DES etc [6]. Symmetric-key structure is simplest and faster, but the main disadvantage is that both share the same key for encryption and decryption. Asymmetric encryption averts this problem because the public key send on a network and the private key is never transmitted. Symmetric-key cryptography [8] also called *secret-key cryptography*. The most popular symmetric-key system is the *Data Encryption Standard (DES)*.

Finally, we note that there are schemes which try to reduce the key size. However, sharing of decryption power is not a concern in these schemes. The disadvantage of this Symmetric Key Algorithms it shares the same key for sender and receiver. Due to this reason the security will be break sometimes.

Identity Based Encryption (IBE)

It is a type of Asymmetric encryption in which the public key of a user is information about the identity of the user (e.g. a user's email address)[8]. IBE is a type of a public-key encryption [4]. It is set for encryption which is nothing but user's public key. In IBE, secret keys are generated by using third party private key generator(PKG) and here the secret key is provided based on identity. Sender wants to share files using identity key. So sender will encrypt the files by making use of user identity and Receiver will decrypt these files by making use of his secret key. But out of key-Accumulated and IBE, only one divine casual oracles. Key aggregation is restrain as keys will be come from various identity.

There is a third party called private key generator (PKG) in IBE holds a master-secret key in [8][10] and issues a secret key to each user with respect to his identity. The encryptor user can take the public criterion and user integrity to encrypt a message. The recipient can decrypt this cipher text by his secret key. Integrity-based encryption (IBE) is a type of asymmetric encryption the key of a user can be determined as an selfhood-string of the user e.g., an email address in [1]. In this Approach one single compact secret key can decrypt Encoded texts encrypted under many identities.

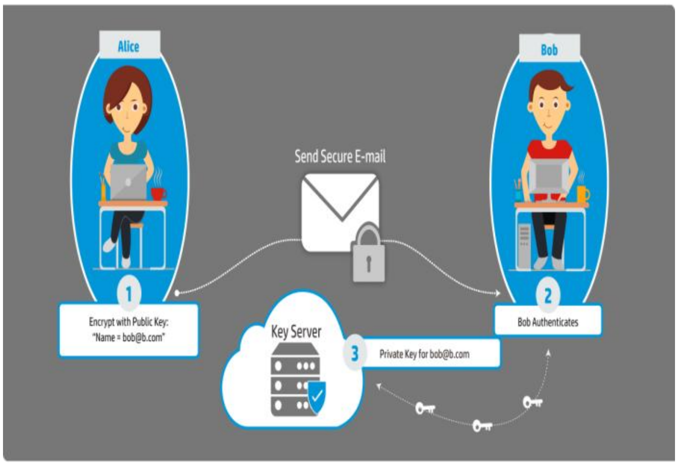

Alice
Bob
Send Secure E-mail
1
Encrypt with Public Key: "Name = bob@b.com"
2
Bob Authenticates
Key Server
3
Private Key for bob@b.com

Fig 3: Identity Based Encryption

HP Identity-Based Encryption dramatically simplifies the process of sensitive communications. For example, how Alice send a secure Email to Bob using HP IBE.

Another Way IBE:

- Alice's e-mail id alice@gmail.com is Asymmetric key.
- Alice validates myself to an "authority" and generates the private key for this id.
- Bob adopt alice@gmail.com and few civic parameters of the expert to encode a message to Alice.
- Alice decrypts message using own private key.

Advantages:

- Encryption type is public-key encryption.
- This scheme has a secure key approach.
- Based on the identity, secret key will be provided.

Disadvantages:

- Cipher text size is non-constant.
- Cost of storing cipher text and transmitting it expensive.
- Sending Alice Private Key Require Secure Channel.

Our contribution: Cryptography is an amazing technique with which veils the veracity of the message from superfluous users. The Key-Aggregate Cryptosystem (KAC) [1] affords an outstanding performance reducing

The estimation intricacy of the overall algorithm. The KAC assemblages diversified cipher texts into encode text classes and every class keeps a secret key from which the aggregate key will be generated.

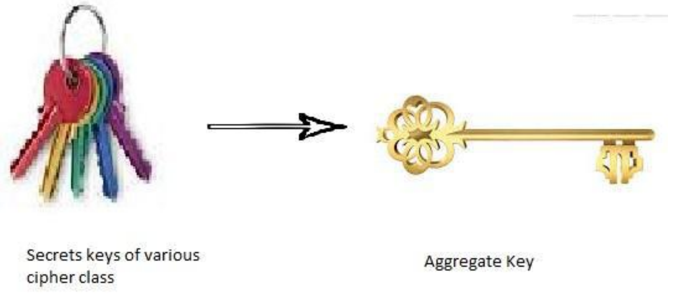


Fig 1.3 Multiple secret keys to single powerful Aggregate Key

Alice can send to bob the aggregate key as an email so that

Bob can decrypt the set of data which is being encrypted using The aggregate key and the set outside this encryption remain Hidden to bob. 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[1].

Proposed Approach – Key Aggregate Cryptosystem

The key-aggregate encryption process comprises of five polynomial-time algorithms as follows.[1]

1. Setup: This is a randomized algorithm that takes no input other than the implicit security parameter.

2. KeyGen: alternately create 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 text class file and outputs C.

4. Extract (msk,S): A process result generates set of secrete keys forms an Aggregate Key when we input the set of indices of the cipher class with secret key in [1].

5. Decryption : decryption is the procedure who receives the aggregate key obtaining the message m iff i ε S.

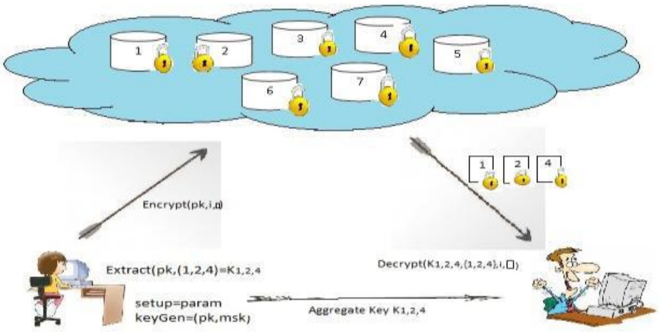


Fig 2.1 Data sharing in clouds

The above figure shows data is being shared in the cloud. Suppose a user A wants to share the data 1, 3, 5 to

Another user B, then the user A generates an aggregate key using the attributes of 1, 3, 5 and sends it to the user B. The user B thus decrypts the required data by performing the setup to generate the param, and then the keys are generated followed by the encryption process. The extract process generates the aggregate key with which the user B decrypts the data. In the traditional methods the key assignment will be providing separate keys for every data to be decrypted. Process improves key generation process as well as consumes space.

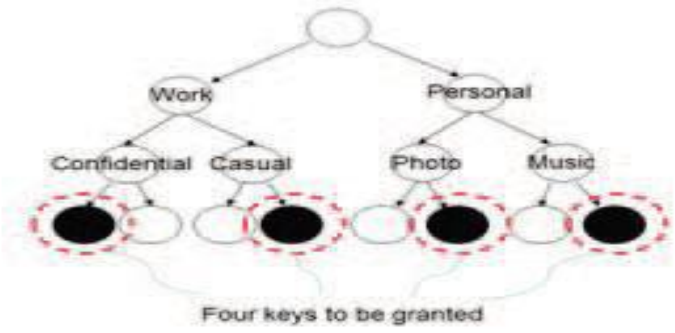


Fig 2.2 Key assignment for traditional cryptographic scheme

Here in the above figure four separate keys are to be granted for the availability of these files. The KAC uses only half the no.of keys than in the traditional cryptographic schemes. For example, consider the figure.

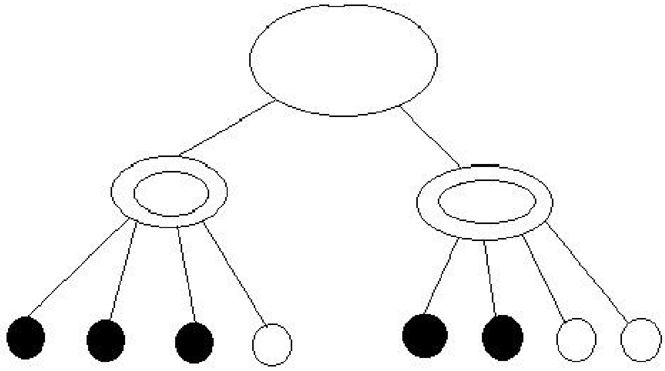


Fig 2.3 Key assignment in KAC

Only two different keys has to be provided for the access of

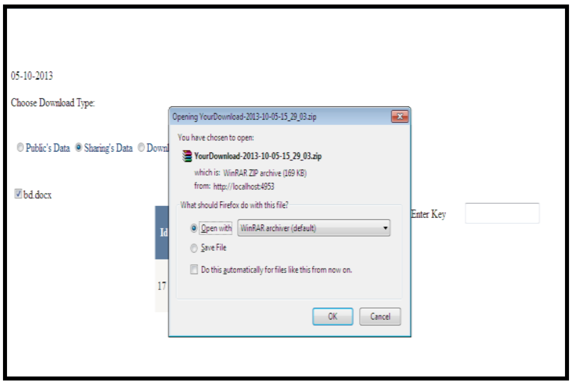
five data. Hence hierarchical level of classification of data

has a more advantageous level than the data arrangement in

class level.

The Key Aggregate Cryptosystem allows the users to upload files, share their files and to download and access the files. Uploading files into cloud requires all the files need to be encrypted and then stored. The Fig 2 shows the uploading of files into cloud. Sharing files among cloud users is done by using the aggregate key. The files are downloaded from cloud and then decrypted for accessing the files. Fig describes the sharing of data to other cloud users.

1. First Encrypt the Data file using Public Key Encryption and Upload on Cloud Server
2. Login the User Account and Share this data with other users using Key
3. Download File:



05-10-2013

Choose Download Type:

○ Public's Data ● Sharing's Data ○ Downl

☑ bd.docx

Opening YourDownload-2013-10-05-15_29_03.zip

You have chosen to open:

YourDownload-2013-10-05-15_29_03.zip

which is: WinRAR ZIP archive (169 KB)

from: http://localhost:4953

What should Firefox do with this file?

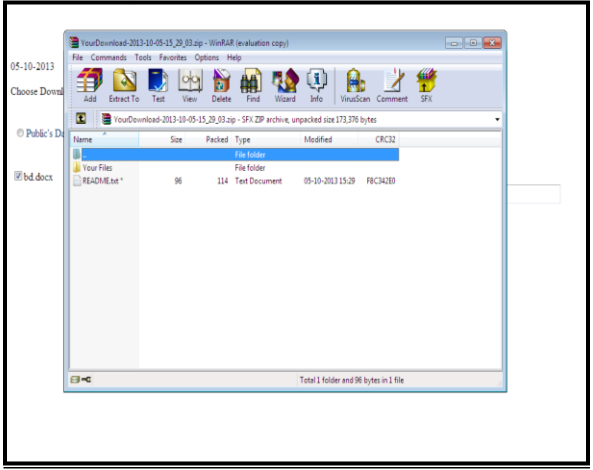
● Open with WinRAR archiver (default)

○ Save File

□ Do this automatically for files like this from now on.

Enter Key

4. Key Sent to Email ID



YourDownload-2013-10-05-15_29_03.zip - WinRAR (evaluation copy)

YourDownload-2013-10-05-15_29_03.zip - SFX ZIP archive, unpacked size 173,376 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Your Files			File folder		
README.txt *	96	114	Text Document	05-10-2013 15:29	F8C342E0

Total 1 folder and 96 bytes in 1 file

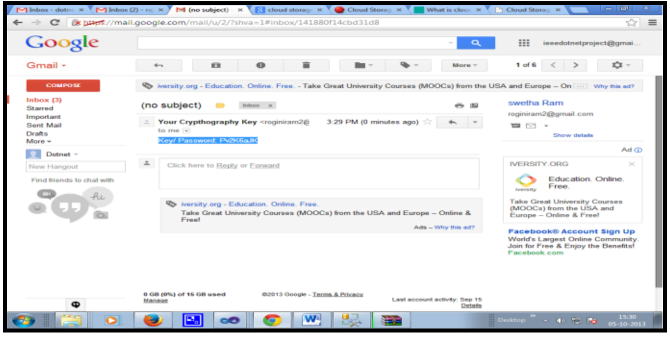
05-10-2013

Choose Downl

○ Public's Da

☑ bd.docx

5. View the original data using Aggregate key



https://mail.google.com/mail/u/2/?shva=1#inbox/141880f14cbd31d8

ieeedotnetproject@gmai...

(no subject) Inbox

Your Crypthography Key <roginiram2@ 3:29 PM (0 minutes ago)

to me

Key/ Password: Pv2K6aJK

Click here to Reply or Forward

swetha Ram

roginiram2@gmail.com

0 GB (0%) of 15 GB used

©2013 Google - Terms & Privacy

Last account activity: Sep 15

Inbox - dotn
Inbox (2)
(no subject)
cloud storag
Cloud Storag
What is clou
Cloud Storag
Google
Gmail
COMPOSE
Inbox (3)
Starred
Important
Sent Mail
Drafts
More
Dotnet
New Hangout
Find friends to chat with
More
1 of 6
Show details
iversity.org - Education. Online. Free. - Take Great University Courses (MOOCs) from the USA and Europe – On
Why this ad?
IVERSITY.ORG
Education. Online. Free.
Take Great University Courses (MOOCs) from the USA and Europe – Online & Free!
Facebook® Account Sign Up
World's Largest Online Community. Join for Free & Enjoy the Benefits!
Facebook.com
Manage
Details
Desktop
15:30
05-10-2013

Conclusion

User's information privacy is a pivotal question of cloud storage. With extra numerical tools, cryptographic schemes we consider how to develop an efficient and flexible encryption scheme which decrypts any number of subset of cipher text by a single secret key. Here a delegate will always get a constant size aggregate key. So decryption of any number of cipher texts is possible by an aggregate key. This approach is more flexible than hierarchical key assignment which simply saves spaces if owner distribute a similar set of privileges.

References

[1] "Key-Aggregate Cryptosystem for Resizable Data Sharing in Cloud Storage" Cheng-Kang chu, Sherman S. M chow, Wen-Guey T, Senior Member IEEE, Vol.25,No.2, FEB 2014.

[2] Archana Sharma C.N, Dr. K Thipswamy "Literature Survey on Key Aggregate Cryptosystem for Multi File Data Sharing in Cloud International", Journal of Advanced Research in CS and Software Engineering Volume 5, Issue 4,2015.

[3] Goldie Lee Joe and Dr. N. K. Sakthi "Development of Enhanced Key-Aggregate for Secure Cloud Storage"

International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181.

[4] G. Suganyadevi, S. PunithaDevi “Effective Data Sharing in Cloud Using Aggregate Key” Journal of Engineering and Technology, Vol. 4, Special Issue 6, May 2015.

[5] C. Wang, K. Ren, W. Lou, and J. Li, “Towards Publicly Auditable Cloud Data Storage Services,” vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[6] Xiao Zhifeng and Xiao Yang, “Security and privacy in cloud computing Approach.” IEEE Communications Surveys & Tutorials 15, 2 (2013), 843–859.

[7] G. Ateniese, B. Masucci, “Provably-Secure Time-Bound Hierarchical Schemes,” J. Cryptology, vol. 25, no. 2, pp. 243–270, 2012.

[8] D. Boneh, R. Canetti, S. Halevi,“Chosen-Ciphertext Security from IBE,” SIAMCOMP, vol. 36, no. 5, pp. 1301–1328, 2007.

[9] D. Boneh, C. Gentry, “Collusion Resistant Encryption with Ciphertexts and Private Keys,” in Proceedings of CRYPTO ’05, ser. LNCS, vol. 3621. Springer, 2005, pp. 258–275.

[10] F. Guo, Y. Mu, “IBE: How to Decrypt Ciphertexts Using a Single Decryption Key.

[11] Identity Based Encryption : IBE - Wikipedia, the free encyclopedia