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. 3, Issue 10, October 2015

Review of Scalable Data Sharing in Cloud Storage Using CP-ABE

Prajakta D.Patil[1], Chhaya Nayak[2]

[1] M.Tech Student, Dept. of CSE, B. M. Technology, RGPV University, Bhopal, MP, India

[2]Professor, Dept. of CSE, B. M. Technology, RGPV University, Bhopal, MP, India

ABSTRACT: Data sharing is an important functionality in cloud storage. We show how to securely, efficiently, and flexibly share data with CP-ABE method in secure cloud storage. We describe new public-key cryptosystems which produce constant-size ciphertexts such that efficient delegation of decryption rights for any set of ciphertexts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of ciphertext set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. To provide a secure data sharing we propose an attribute based encryption technique, there are two types namely KP-ABE (key policy attribute based encryption) and CP-ABE(Cipher text policy Attribute based Encryption). In this paper we propose CP-ABE scheme.

KEYWORDS: Cloud storage, data sharing, key-aggregate encryption, patient-controlled encryption, CP-ABE

I. INTRODUCTION

1.1 Basic Concept

Cloud storage is gaining quality recently. In enterprise settings, we have a tendency to see the increase in demand for information outsourcing that assists within the strategic management of company information. It’s conjointly used as a core technology behind several on-line services for private applications. Information sharing is a very important practicality in cloud storage. for instance, bloggers will let their friends read a set of their personal pictures; associate degree enterprise could grant her staff access to a little of sensitive information. The difficult drawback is the way to effectively share encrypted information. In fact users will transfer the encrypted information from the storage, decode them, then send them to others for sharing; however it loses the worth of cloud storage. Users ought to be able to delegate the access rights of the sharing information to others so they’ll access this information from the server directly. Secret writing keys conjointly associate with 2 flavors—symmetric key or uneven (public) key. Victimization symmetrical secret writing, once Alice desires the info to be originated from a 3rd party, she has got to offer the encrypted her secret key; clearly, this is often not perpetually fascinating. Against this, the secret writing key and decipherment key are completely different publicly key secret writing. The utilization of public-key secret writing offers additional flexibility for our applications. For instance, in enterprise settings, each worker will transfer encrypted information on the cloud storage server while not the data of the company’s master-secret key.

Suppose Alice place all information on Box.com and she or he doesn’t\'t need to show her information to everybody. As a result of information run prospects she doesn’t\'t trust on privacy mechanism provided by Box.com, therefore she encipher all information before uploading to the server. If Bob raise her to share some information then Alice use share performs of Box.com. However drawback now could be that the way to share encrypted information. There are 2 severe ways: one. Alice enciphers information with single secret key and shares that secret key directly with the Bob. 2. Alice will encipher information with distinct keys and send Bob corresponding keys to Bob via secure channel. In 1st approach, unwanted information conjointly get expose to the Bob that is insufficient. In second approach, no. of keys is as several as no. of shared files, which can be hundred or thousand moreover as transferring these keys need secure channel and cupboard space which might be high-ticket. So best resolution to on top of drawback is Alice encrypts information with distinct public keys, however send single decipherment key of constant size to Bob. Since the decipherment key ought to be sent via secure channel and unbroken secret little size is usually desirable. to style associate degree economical public-key secret writing theme that supports versatile delegation within the sense that any set of the cipher texts (produced by the secret writing scheme) is decode ready by a constant-size decipherment key (generated by the owner of the master-secret key).[2]

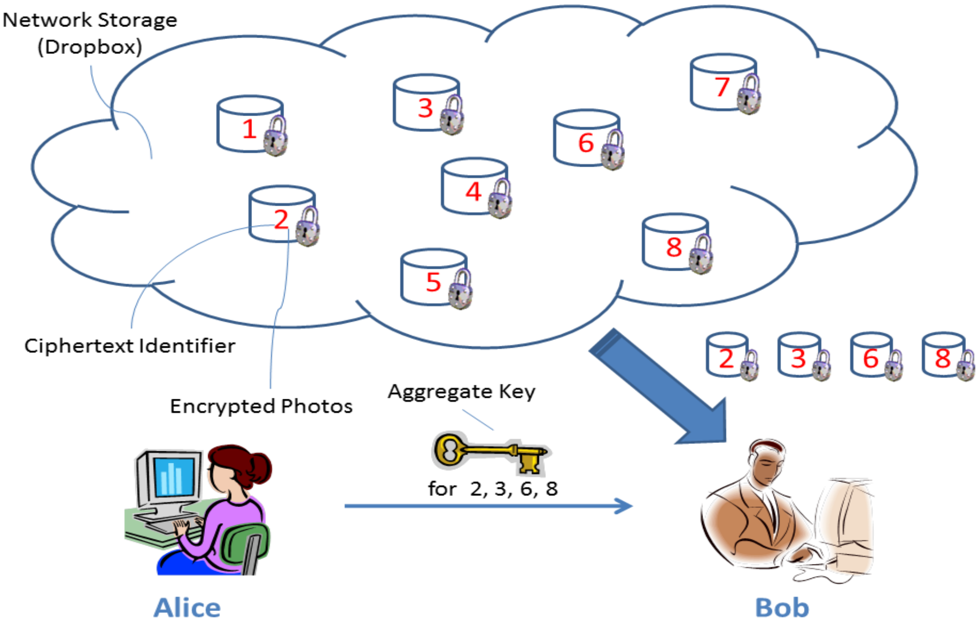

Fig. 1. Alice shares files with identifiers 2, 3, 6 and 8 with Bob by sending him a single aggregate key.

1.2 Problem Definition:

An elementary drawback we regularly study is concerning investment the secrecy of little piece of data into the power to perform science functions (e.g., encryption, authentication) multiple times. to style Associate in Nursing economical public-key encoding theme that supports versatile delegation within the sense that any set of the cipher texts (produced by the encoding scheme) is rewrite ready by a constant-size decipherment key (generated by the owner of the master-secret key).

1.3Objective:

To minimize the expense in storing and managing secret keys for general crypto logic use. Utilizing a tree structure, a key for a given branch is wont to derive the keys of its descendant nodes (but not the opposite method round). Simply granting the parent key implicitly grants all the keys of its descendant nodes. A planned a way to come up with a tree hierarchy of symmetric-keys by exploitation recurrent evaluations of pseudorandom function/block cipher on a hard and fast secret. The thought is generalized from a tree to a graph.

1.4 Motivation:

The motivates to reduce the secure storage and this is a trade-off between two kinds of storage. The parameter can be

placed in no confidential local storage or I n a cache provided by the service company. hey can also be fetched on demand, as not all of them are required in all occasions.

II. LITERATURE SURVEY

Several researchers have done the qualitative and quantitative analysis of Cloud storage data sharing : Below in literature discussing some of them.

In the paper “SPICE – Simple Privacy-Preserving Identity-Management for Cloud Environment,” have shown how to securely, efficiently, and flexibly share data with others in cloud storage by S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-

M.Yiu [2]. B. Wang, S.S.M. Chow, M. Li, and H. Li, “Storing Shared Data on the Cloud via Security-Mediator”, presented A novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated [3]. S.S.M. Chow, C.-K. Chu, X. Huang has proposed The new public-key cryptosystems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts in the “Dynamic Secure Cloud Storage with Provenance” ,paper [4]. The author D. Boneh, C. Gentry, B. Lynn, and H. Shacham of the paper “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps”, proposed how to eliminates the power consuming decryption operations at the aggregator node for the data aggregation and further encryption for the secure transmission of aggregated data [5]. In, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records”, how A novel patient centric framework and a mechanism for data access control to PHRs stored in semi structured servers is presented by J. Benaloh, M. Chase, E. Horvitz, and K. Lauter [6]. In “Privacy-Preserving Public Auditing for Secure Cloud Storage,” the authors C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, proposed a privacy-preserving public auditing system for data storage security in Cloud Computing. They utilize the homomorphic linear authenticator and random masking to guarantee that the TPA (Third Party auditor) would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users’ fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, They further extended their privacy- preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency [7]. In this paper they implemented a prototype application that demonstrates proof of concept of a security mechanism presented by Stolfo et al [9]. Yong Cheng, Jiangchun Ren, Zhiying Wang, Songzhu Mei, Jie Zhou[10],In this paper presents a novel technique, attributes union, for promoting the CP-ABE algorithm’s applications in cryptographic access control systems. Attributes unionizing means that I can reduce the number of components in ciphertext and private secret keys. And I can reduce the storage and computational overhead to a constraint by unionizing attributes. The attributes union can be also used for modifying other existing CP-ABE algorithms. We benefit a lot from attributes union, since the number of attributes only has a mini effect on it. Fengli Zhang, Qinyi Li1, Hu Xiong [11] , Here, they give the efficiency analysis and comparing of some existence revocable ABE schemes . |PK|, |CT| and |SK| present the size of public parameters, the overhead of the ciphertext and the size of user’s private key, respectively. Security model is denoted by “Sec-Model” which demonstrates the scheme can be proved either in full security model and selective security model.

Key Aggregate Cryptosystem proposed in,” Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage “by Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng , it can aggregates any set of secret key and make them as compact as single key and can be conveniently sent to other or be stored in a smart card with very limited secure storage[1]. In this paper we are going to use Cipher text-Policy Attribute-based Encryption (CP-ABE) as detailed below.

III. PROPOSED WORK

Cipher text-Policy Attribute-based Encryption (CP-ABE) is considered one amongst the foremost appropriate technologies for information access management in cloud storage, as a result of it provides data house owners a lot of direct management on access policies. Efficient method of iris image classification by using cryptography algorithm with aim of achieving the required level of security. For encryption we are using bio-chaotic stream cipher that encrypts the iris images via the electronic media as well as it is used to encrypt the images in order to store into the databases for making them more secure with the help of biometric key and a bio-chaotic function.

DOI: 10.15680/IJIRCCE.2015. 0310007

IV. ARCHITCTURE & METHODOLOGY

4.1 Architecture

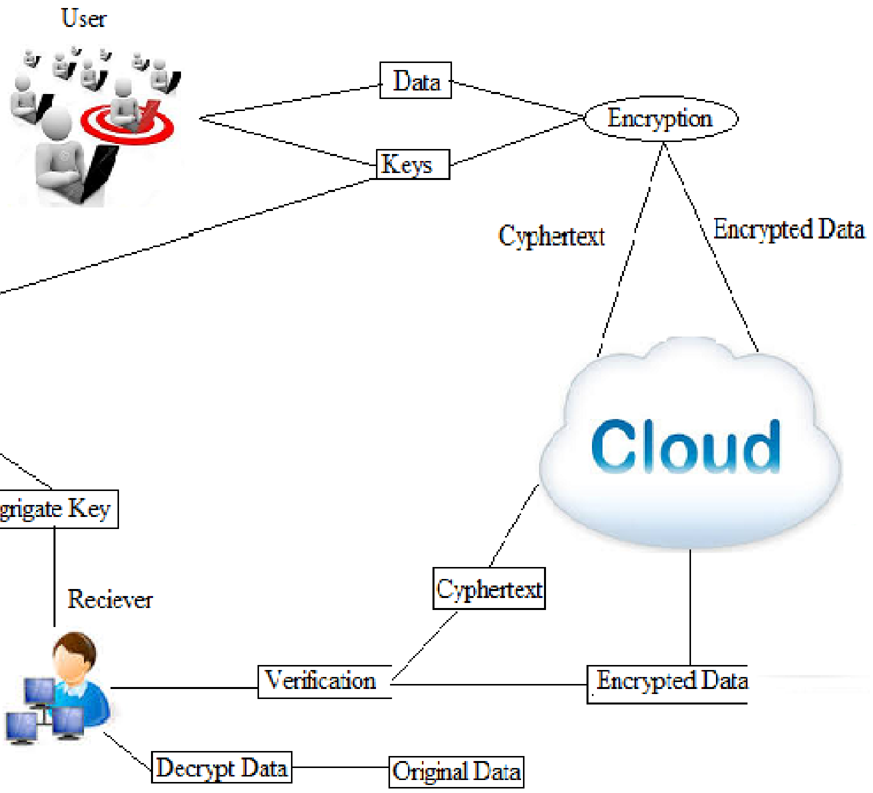

Fig 2: Architecture Diagram

As shown in fig 2, The data owner establishes the general public system parameter via Setup and generates a public/master-secret3 key try via Key info. Messages is encrypted via write by anyone World Health Organization additionally decides what cipher text category is related to the plaintext message to be encrypted. the info owner will use the master-secret to get AN combination cryptography key for a group of cipher text categories via Extract. The generated keys is passed to delegates firmly (via secure e-mails or secure devices) Finally, AN user with an combination key will decipher any cipher text only if the cipher text's category is contained within the combination key via decipher.

Key Generation: dead by the info owner to indiscriminately generate a public/master-secret key try.

Encrypt: dead by anyone World Health Organization desires to write information. On input a public-key pk, AN index I denoting the cipher text category, and a message m, it outputs a cipher text C.

Extracts: dead by the info owner for authorization the decrypting power for a particular set of cipher text categories to a delegate. On input the master-secret key msk and a group S of indice corresponding to completely different categories, it outputs the combination key for set S denoted by Kansas.

Decrypt: dead by a delegate World Health Organization received AN combination key Kansas generated by Extract. On input Kansas, the set S, AN index i denoting the cipher text category the cipher text C belongs to, and C, it outputs the decrypted result m if i two S.

4.2 Methodology:

Mathematical Module

Let S ={SP, KG, En, Ex, Dn}

Where,

SP	setup an account on an untrusted server
KG	Key generation i.e Public /Master Key
En	Encrypt Data
Ex	Extract Aggregate key
Dn	Decrypt Data

Process:

1. **Setup ($1^{\lambda}, n$) :** Executed by the data owner to setup an account on an un trusted server

   Let g $\mathcal{E}$ G and $\alpha \in_R \mathbb{Z}_p$

   Where G bilinear group and p is prime order

   Where $2^{\lambda} \leq p \leq 2^{\lambda+1}$

   Compute $g_i = g^{\alpha^i} \in$ G

   Where i=1… n, n+2

   System parameter =(g, g1, ……., gn, gn+2)

2. **Key Gen()** : Executed by the data owner to randomly generate a public/master-secret key pair

   Select $\gamma \in_R \mathbb{Z}_p$

   Where $\mathbb{Z}_p$ is prime number

   Out put the public and private key

3. **Encrypt(pk, i, m) :**Executed by anyone who wants to encrypt data.

   Let m be the message and be the index i

   Where m $\in G_T$ and i $\in$ {1,2,….n}

   Let randomly select $t \in_R \mathbb{Z}_p$

   Where $\mathbb{Z}_p$ is prime number

   And compute the cipher text c as (g^t,$(vg_i)^t$, m,$e(g1, gn)^t$)

4. **Extract(msk = γ, s):** Executed by the data owner for delegating the decrypting power For the set s of indices j's aggregate key is

   Ks = $\pi_{j \in S} g^{\gamma}_{n+1-j'}$

   Where S does not include 9,g_{n+1-j} =$g^{\alpha^{n_1-j}}$ always retrieve from param

5. **Decrypt: (Ks, S, I, C) :**Executed by a delegate who received an aggregate key KS generated by Extract

   Check if $i \notin S$ the out put $\perp$.

   Otherwise,

Return message m= c3.e(Ks.$\pi_{j\epsilon S, j\neq i} g^{,c1}_{n+1-j+i}$,c1) /e($\pi_{j\epsilon S} g_{n+1-j}, c2$))

Let γ *be the knowlede of data owner*, the term $e(g1, gn)^t$ can be recoverd by e.$(c1, gn)^\gamma$ =e$(g^t, gn)^\gamma$= e(g1, $gn)^t$

1. leakage-resilient cryptosystem:

Public key Encryption scheme:
Let AE = (K, E, D) of PPT algorithm
Where k is input security parameter1^λ ,
It outputs the public private key pair (pk, sk).
Where E gets as its input pk and message m ε M (M ,for some message space)
Its output is a cipher text c.
For decryption D on input the secrete key sk and α ciphertext c, the output a message m or $\perp$
Where the probability is taken over randomness of K, E, and D

V. CONCLUSION

In cloud storage users data privacy is a cardinal question . We consider how to compress secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text classes in cloud storage. No matter which one among the power set of classes, the delegate can always get an aggregate key of constant size. In cloud storage, the number of cipher texts usually grows rapidly without any restrictions. So we have to reserve enough cipher text classes for the future extension. Otherwise, we need to expand the public-key. Although the parameter can be downloaded with cipher texts, it would be better if its size is independent of the maximum number of cipher text classes.

The aggregate key encryption combined with ciphertext, which obviate attacks with high security. Key distribution can be managed easily with perfect security. The access policy and cryptographic schemes are getting more versatile and often involve multiple keys for a single application. Approach is more flexible than other key assignment which can only save a data.

REFERENCES

1 Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, Senior Member," Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014.

2 S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-M.Yiu, "SPICE – Simple Privacy-Preserving Identity-Management for Cloud Environment, "Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS), vol. 7341, pp. 526-543, 2012.

3 B. Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," Proc. IEEE 33rd Int'l Conf. Distributed Computing Systems (ICDCS), 2013.

4 S.S.M. Chow, C.-K.Chu, X. Huang, J. Zhou, and R.H. Deng, "Dynamic Secure Cloud Storage with Provenance," Cryptography and Security, pp. 442-464, Springer, 2012.

5 D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22ndInt'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '03), pp. 416-432, 2003.

6 J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.

7 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, Feb. 2013.

8 L. Hardesty, Secure Computers Aren't so Secure. MIT press, http://www.physorg.com/news176107396.html, 2009.

9 G.Jai Arul Jose, C.Sajeev, "Implementation of Data Security in Cloud Computing",International Journals of P2P Network Trends and Technology, Vol. 1, Issue 1, 2011

10 Yong Cheng, Jiangchun Ren, Zhiying Wang, "Attributes Union in CP-ABE Algorithm for Large Universe Cryptographic Access Control," Second International Conference on Cloud and Green Computing,pp.180-186, Nov 2012.

11 Fengli Zhang, Qinyi Li, Hu Xiong, "Efficient Revocable Key-Policy Attribute Based Encryption with Full Security," Eighth International Conference on Computational Intelligence and Security,pp. 477-481,Nov 2012.