Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 10, October 2015, pg.35 – 39

RESEARCH ARTICLE

Highly Secure Data Sharing in Cloud Storage using Key-Pair Cryptosystem

[1]Abhilasha N.Madde, [2]Priyanka R. Powar, [3]Tanvi S. Bankar, [4]Harshada M.Somwanshi, [#]Prof.Amol Dhumane
Department Of Computer Engineering, NBN Sinhgad School of Engineering ,Ambegaon(BK), Pune
[1] abhilashamadde27@gmail.com, [2] priyanka.powar01@gmail.com, [3] tanvi.bankar@gmail.com, [4] harshu166149@gmail.com, [#] amol.dhumane@sinhgad.edu

Abstract— The importanat functionality of cloud is data storage. In this paper, we are going to discuss about how to flexibly, efficiently, and securely share the data with another client in cloud storage. New public-key cryptosystems is described here that produces constant-size cipher texts that has efficient delegation of decryption rights for any set of cipher-texts are possible. The new thing is that one can aggregate any set of secret keys and make them as concise as a single key, but including power of all keys being aggregated.. The secret key holder can free a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files which are outside the set remain secretly. This concise aggregate key can be secretly sent to others or be stored in a smart card with very limited secure storage. Security analysis is provided in oue standard model scheme. This schemes gives the first public-key patient-controlled encryption for flexible hierarchy.

Keywords— Agreegate Key, sharing data, Key agreegate encryption scheme, data storage on clouds, Key agreegate cryptosystem.

I. INTRODUCTION

Cloud storage is the most popular technology which is recently used in the market. The services based on the cloud include Software-as-a-Service (SaaS) and Platform as a Service (PaaS) and Infrastructure as a (IaaS). Cloud computing provides various facilities for storing data and sharing of data.

The data transfer using the cloud is in GB and TB. Thus cloud storage has advantageous like low cost and high availability of data. Major concern in the cloud computing environment is Cloud storage , as user can easily store any type of data on the cloud.

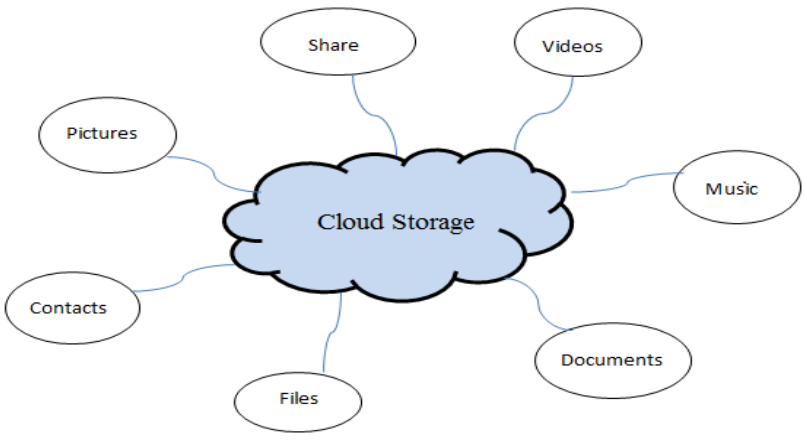

Fig A. Cloud storage

Cloud storage is a service where data is remotely maintain, managed and backup. Cloud storage is currently very popular now a days.There is big demand of outsourcing of data. It is used as basic technology for very online services for private applications.The public auditing system of data storage security in cloud computing provides a privacy-preserving auditing protocol [2]. It is necessary to make sure that the data integrity without compromising the anonymity of the data user. To ensure the integrity the user can verify metadata on their data, upload and verify metadata [3]. Encipher with public key Transmit Decipher with Hidden key Then there are 2 critical ways[refer Fig.C],

1. Alice encrypt whole picture with one encryption key and give secret key to bob.
2. Encrypt all picture with special key and send corresponding secret key to bob. Sharing information is main task of cloud. For example, bloggers can want their personal photo, Plain text to Chiper text.

CRYPTOSYSTEM

In cryptography, Cryptosysetm is set of cryptographic algorithm which is needed to implement a particular security service.

It cocsist three algorithm which are following:

1. Key Generation
2. Encryption
3. Decryption

Cipher is a pair of algorithm in that first pair is encryption and another one is decryption, that's why this system is called as cryposystem.
In this system key generation algorithm is very important.That's why cryptosystem term is used to refer a public key techniques.

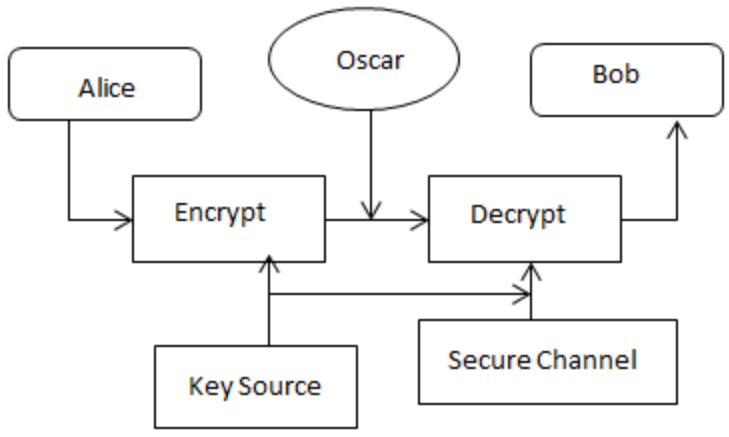

Fig.B Crptosystem Process

TYPES OF ENCRYPTION KEYS

There are two types of encryption keys:

1. *Symmetric Key Encryption:*

   In symmentic key encryption,encryption and decryption will done using single key or same key. but sometimes it will become very easy to hack this key for attacker.

2. *Asymmetric Key Encryption:*

   In asymmentic key encryption,encryption and decryption will done using different keys. It will become very difficult to attacker to hack different keys so it is moresecured than the sysmmetric key encryption.

   The performance of application using this become less than the symmetric key encryption.

CRYPTOGRAPHY SCHEMES FOR DATA STORAGE

cloud users will not have trust that the cloud server is doing a good job in terms of data privacy. For the security there is a cryptographic solution, with proven security replaced on number theoretic assumptions is more attractive.Whenever the users are not happy with trusting the security of their VM or the honesty of their technical staff. Those users are going to encrypt their data with their own keys before uploading the data on the cloud.

A. ORGANIZATION

This paper id organized as follows: Related work is explained in section II. The proposed system means the Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage is presented in section III .We conclude in section IV.

II. RELATED WORK

A. SYMMETRIC-KEY ENCRYPTION WITH COMPACT KEY

Benaloh et al. [4] presented an encryption scheme which is originally proposed for concisely transmitting large number of keys in broadcast scenario [5]. The construction is simple and we briefly review its key derivation process here for a concrete description of what are the desirable properties we want to achieve.
The derivation of the key for a set of classes (which is a subset of all possible ciphertext classes) is as follows.A composite modulus is chosen where p and q are two large random primes.
A master secret key is chosen at random. Each class is associated with a distinct prime. All these prime numbers can be put in the public system parameter. A constant-size key for set can be generated. For those who have been delegated the access rights for S' can be generated. However, it is designed for the symmetric-key setting instead.
The content provider needs to get the corresponding secret keys to encrypt data, which is not suitable for many applications. Because method is used to generate a secret value rather than a pair of public/secret keys, it is unclear how to apply this idea for public-key encryption scheme. Finally, we note that there are schemes which try to reduce the key size for achieving

B. ATTRIBUTE-BASED ENCRYPTION

Attribute-based encryption (ABE) [6], [7] allows each ciphertext to be associated with an attribute, and the master-secret key holder can extract a secret key for a policy of these attributes so that a ciphertext can be decrypted by this key if its associated attribute conforms to the policy.
For example, with the secret key for the policy $(1 \vee 3 \vee 6 \vee 8)$, one can decrypt ciphertext tagged with class 1, 3, 6 or 8. However, the major concern in ABE is collusion-resistance but not the compactness of secret keys. Indeed, the size of the key often increases linearly with the number of attributes it encompasses, or the ciphertext-size is not constant (e.g., [8]).

C. IBE WITH COMPACT KEY

Identity-based encryption (IBE) (e.g., [9], [10], [11]) is a public-key encryption in which the public-key of a user can be set as an identity-string of the user (e.g., an email address, mobile number). There is a private key generator (PKG) in IBE which holds a master-secret key and issues a secret key to each user with respect to the user identity.
The content provider can take the public parameter and a user identity to encrypt a message. The recipient can decrypt this ciphertext by his secret key. Guo et al. [12], [13] tried to build IBE with key aggregation.

In their schemes, key aggregation is constrained in the sense that all keys to be aggregated must come from different ―identity divisions‖. While there are an exponential number of identities and thus secret keys, only a polynomial number of them can be aggregated[1].

This significantly increases the costs of storing and transmitting ciphertexts, which is impractical in many situations such as shared cloud storage.

As Another way to do this is to apply hash function to the string denoting the class, and keep hashing repeatedly until a prime is obtained as the output of the hash function[1]. we mentioned, our schemes feature constant ciphertext size, and their security holds in the standard model.

In fuzzy IBE [10], one single compact secret key can decrypt ciphertexts encrypted under many identities which are close in a certain metric space, but not for an arbitrary set of identities and therefore it does not match with our idea of key aggregation.

D. PUBLIC KEY CRYPTOGRAPHY

Public-key cryptography [14], also known as asymmetric cryptography. It requires two distinct keys one of which is private and other one is public. Two parts of this key pair mathematically linked with each other

The public key is used for encryption and private key is used for decryption. Public Key encrypts the plain text to generate an encrypted data, while the private key is used to decrypt cipher text or to create original data. The term "asymmetric" arises from the use of different keys, each key is the inverse of the other.

Users can create their own public and private key-pair by doing mathematical computations and to use them for encryption as well as decryption. The strength of public-key cryptography is that it is "impracticable" to determine public key corresponding to a properly generated private key.

Thus the public key may be available without compromise in security, but the private key must not be disclosed to unauthorized person to read messages. Public-key algorithms are primary security methods in cryptographic applications and protocols.

They support various networking standards, such as (TLS) Transport la.yer Security, PGP. Some public key algorithms provide key distribution and secrecy (e.g., Diffie-Hellman key exchange), some provide digital signature (e.g., Digital signature), and some provide both (e.g., RSA).

E. CRYPTOGRAPHIC KEYS FOR A PREDEFINED HIERARCHY

Cryptographic key assignment schemes works on the basis of minimize the expense in storing and managing secret keys for general cryptographic use by using a tree structure [15]. By using ranked tree arrangement, a key for a given division can be used to originate the keys of its child nodes.

This can resolve the problem somewhat if one plans to share all files under a certain branch in the pyramid which otherwise means that the number of keys increases with the number of branches. So it is difficult to create a hierarchy that can save the number of total keys to be granted for all individuals concurrently.

III. PROPOSED SYSTEM

In this paper, we study how to make a decryption key more powerful in the sense that it allows decryption of multiple ciphertexts, without increasing its size. Specifically, our problem statement is “To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the ciphertexts (produced by the encryption scheme) is decryptable by a constant-size decryption key (generated by the owner of the master-secret key).”

We solve this problem by introducing a special type of public-key encryption which we call key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but also under an identifier of ciphertext called class.

That means the ciphertexts are further categorized into different classes. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes.

More importantly, the extracted 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.

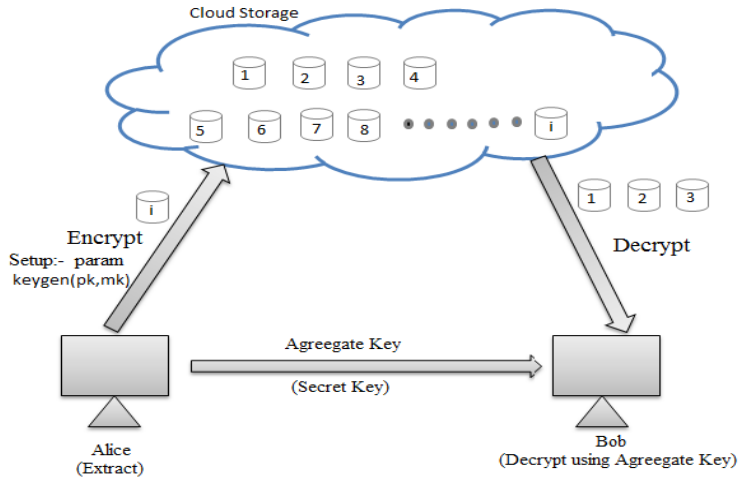

Fig C. Key Agreegate Cryptosystem(KAC)

A. KEY AGGREGATE CRYPTO- SYSTEM

The proposed system design an efficient public-key encryption scheme which supports flexible allocation. In this scheme any subset of the cipher texts (produced by the encryption scheme) is decrypt by a constant-size decryption key (generated by the proprietor of the master-secret key). We solve this problem by introducing a special type of public-key encryption called key-aggregate cryptosystem (KAC).

In KAC, users encrypt a message not only under a public-key, but also under an identifier of cipher text called **class**. Such that cipher texts are further categorized into different classes. The owner of the key holds a master-secret called Master secret key [1].

The master-secret is used to extract secret keys for different files. Most importantly, the extracted key is an aggregate key which is same as a secret key for a single file, but aggregates the power of all such keys, such that the decryption power for any subset of cipher text classes. Using this solution, Alice can send a single aggregate key to Bob via a secure channel like email.

The encrypted photos can be downloaded by Bob from Alice's Drop box space and then use this aggregate key for decrypting these encrypted photographs.

These technique consist of five polynomial-time algorithm.

Setup: executed by data holder to setup an account on untrusted server. The output is public system paprmeter param, which is remove from others algoritm input.

KeyGen: To randomly create public/master-secret key pair it is executed by the data owner.

Encrypt: executed by any one who want encrypt data.

Extract: Data owner execute it and gets the aggregate key for set of the indices.

Decrypt: executed by delegate who receive or gat the aggregate key.

B. RSA

In our scheme.we used RSA algorithm it is based on asymmetric key. RSA stands for Ron **R**ivest,Adi **S**hamir and Leonard **A**dlemen.

RSA is one of the first public key crptosystem.It is widely used for a secure data transmission.In cryptosystem public is known as encryption key.The decryption key is a different from encryption key that is kept as secret key.

This algorithm publicly described in 1997.

The RSA algorithm based on public key.A user of RSA creates the public key that key based on large prime numbers.The prime numbers kept as secret.Anyone can use the public key to encrpt a message but that person determines the cipher text.

When the user wants that encrypted message then we use the pair of public key and private key for decrypt that message then the user access or read that message.

In decryption,we converts the cipher text into plain text by using pair of public key and private key.

C. IMPORTANCE OF KAC

1. Size of decryption key is constatnt.
2. Size of cipher text is constatnt.
3. Type of encryption is public-key.

D. ADVANTAGES OF KAC

1. A decryption key has functionality to allow decryption of multiple cipher texts, without raising its size because of this it become more powerful..
2. The size of master-secret key, cipher text, public-key, and
3. aggregate key in our KAC schemes are all are kept constant size.
4. There is, no special relation is required between the classes that's why KAC is flexible.
5. The main application of KAC is efficient data sharing scheme.
6. When the delegation key to be efficient and flexible then the key aggregation property is especially useful.
7. This scheme allow sender to share their data in a confidential and selective way, with a fixed and small cipher text expansion, by distributing to each authorized user a single, compact, small aggregate key.
8. The delegation of decryption is implemented using the aggregate key.
9. There are multiple cipher text classes which are in large size.
10. Key management becomes easy.
11. Perticular authorized member can view their data.

IV. CONCLUSION

In our scheme, we study how to squeeze together secret keys in public-key cryptosystems. For different cipher text classes in cloud storage, this compressed key support delegation of secret keys are used. Our new approach is more flexible than hierarchical key assignment whichis used in existing system. The compressed key can only save spaces if all key-holders share a similar set of rights.In our scheme key management become easy. It has functionality like allowing decryption of multiple cipher texts without raising the size that functionality make this more powerful.

REFERENCES

[1] 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 Transaction on Parellel and Distributed System, vol. 25, no. 2, February 2014

[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] 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.

[5] J. Benaloh, ―Key Compression and Its Application to Digital Fingerprinting,‖ Microsoft Research, Tech. Rep., 2009.

[6] 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.

[7] M. Chase and S. S. M. Chow, ―Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,‖ in ACM Conference on Computer and Communications Security, 2009, pp. 121–130.

[8] 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.

[9] 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.

[10] A. Sahai and B. Waters, ―Fuzzy Identity-Based Encryption,‖ in Proceedings of Advances in Cryptology - EUROCRYPT ’05, ser. LNCS, vol. 3494. Springer, 2005, pp. 457–473.

[11] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, ―Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions,‖ in ACM Conference on Computer and Communications Security, 2010, pp. 152–161.

[12] F. Guo, Y. Mu, and Z. Chen, ―Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key,‖ in Proceedings of Pairing-Based Cryptography (Pairing ’07), ser. LNCS, vol. 4575. Springer, 2007, pp. 392–406.

[13] 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.

[14]. Christof Paar, Jan Pelzl, “Introduction to Public-key Cryptography”, Understanding Cryptography, Springer, 2009.

[15] S.G. Akl and P.D. Taylor, “Cryptographic Solution to a Problem of Access Control in a Hierarchy,” ACM Trans. Computer Systems,vol. 1, no. 3, pp. 239-248, 1983

