Key Accumulated Cryptosystem for Scalable Information Sharing in Cloud Storage

P. Supriya[#1] , C. Rajendra[*2] , Dr A. Srilakshmi[#3]

[1,2] *Dept of CSE, ASCET, GUDUR*

[3] *Govt. Degree College for women, Srikalahasti*

[1] supriyapenubolu@gmail.com
[2] srirajendra.c@gmail.com
[3] ayathusrilakshmi@gmail.com

***Abstract*--Cloud computing is employed to store and share expertise with the aid of anyone from any place inside the area. Cloud storage having main utility i.e., securely, effectively, flexibly share data with others. We provide an explanation for new public-key cryptosystems which produce steady cipher textual content. On this, we describe a cryptographic manner where secret keys are combined to make them compact as a single key. Here, the performance of all keys being aggregated. The owner of the secret key can presents the aggregate key to the second get together on demand, and then the receiver equipped to decrypt the records via making use of the aggregate key. This combination key is sent to others or saved in secure storage.**

Key words- Cloud storage, data sharing, key-aggregate encryption, patient-controlled encryption.

I. INTRODUCTION

Cloud storage is more popular in recent years. Nowadays, several organizations keep their huge amount of data in the cloud for saving the price in maintaining in house-storage. With cloud storage service, the member of an organization will share the data with alternative members simply by uploading their information to the cloud. Samples of organization which may get pleasure from this cloud storage and sharing service area unit, similar to international enterprises with many workers around the world, or establishments dealing with huge information, aid service suppliers, coordinating medical information from doctors, researchers, patients, etc. While the outsourcing information have provided any security to this information. So, that we provide cryptography system that is used to encrypt and decrypt the data. Since information operations in the cloud don’t seem to be clear to users and security breaches or improper practices area unit common and inevitable, users still have an enormous concern on protection of their information on the cloud. In Cloud computing, cloud refers to a distinct IT environment that is designed for the purpose of remotely provisioning scalable and measure IT resources. The term originated as a metaphor for the internet. This is, in essence, a network of networks providing remote access to a set of decentralized IT resources. Cloud computing as evolved through a number of phases which include grid and utility computing, Application Service Provision (ASP), and software as a service but the overarching the sixties. In cryptography, cryptosystem refers to suit of cryptographic algorithms needed to implement a particular security service, most commonly for concept of delivering computing resources through a global network is routed in achieving confidentiality. A cryptosystem consists of three algorithms:

1. Key generation,
2. Encryption,
3. Decryption.

Key generation is that the method of generating keys for cryptography. A secret is used to cipher and decipher no matter knowledge is being encrypted/decrypted., in scientific order systems hold symmetric-key algorithms and public-key algorithms. Symmetric-key algorithms use one shared key; keeping knowledge secret needs keeping this key secret. Public-key algorithms use a public key and a personal key. The general public secret is created out there to anyone. A sender encrypts knowledge with the general public key; solely the holder of the non-public key will decipher this knowledge.

Since public-key algorithms tend to be a lot of slower than symmetric-key algorithms, trendy systems resembling TLS and SSH use a mixture of the two: one party receives the other\'s public key, and encrypts a little piece of knowledge. The rest of the speech communication uses a (typically faster) symmetric-key algorithmic rule for encoding.

A. Authentication

Authentication is any system wherein a procedure verifies the identification of a person who wants to access it. On the grounds that access control is in most cases centered on the identity of the user who requests entry to a useful resource, Authentication is foremost to powerful security. Authentication may be applied using Credentials, every of which is composed of a consumer id and Password. Alternately, Authentication is also applied with clever playing cards, an Authentication Server or perhaps a Public Key Infrastructure. Users are frequently assigned Tickets, which are used to monitor their Authentication state. This helps more than a few techniques control entry control without usually asking for new Authentication understanding.

II. LITERATURE SURVEY

A. *Symmetric and Asymmetric key encryption*

The functionality of symmetric algorithm is converting the plaintext into cipher text. [5] In this encryption same key is used for both encryption and decryption. Asymmetric encryption is also known as public key encryption. In this technique we use two different keys, those are public key and private key, public key is used for encrypting the data and private key is a secret key, is used for decrypting the data. The public key can freely distribute over network.

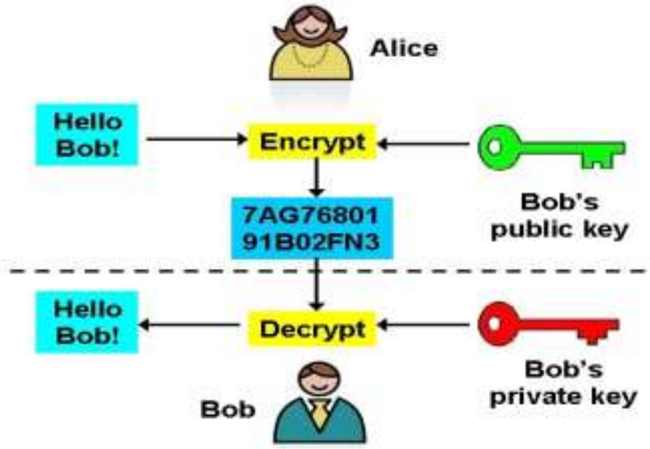

Fig 1: Asymmetric key encryption

B. *Compact key in identity-Based Encryption (IBE*)

Identity Based secret writing could be a style of public key secret writing. [7], [9], [13] during this technique the public key of a user can set identity string of the user. Private keys are generated by a third party private key generator. Private Key generator publishes a public master key and retains the private master key. With the correct ID, user can contact the public key generator to obtain the private key [6] .This way, message may be encrypted without a prior distribution of keys between individual reduces the complexity of encryption process. In this, we have one problem i.e., sending this secret key requires a secure channel.

C. *Attribute-Based Encryption*

It is a type of public key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g.: the country he lives or the kind of subscription he has) [3], [4]. In such a system, the decryption of a cipher text is possible only with the set of attributes of the user key matches the attribute of the cipher text. A crucial security aspect of attribute-Based encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

D. *Encryption key strategy*:

The secret writing plan which is introduced for sending large number of keys in telecast manner. Benaloh et al. [1] and [2] propose this work. The development is basic and that we quickly survey its key abstract thought handle here for a cement depiction of what are the attractive properties we need to achieve. The deduction of the key for an assignment of categories is as taken when. A composite module is picked wherever P and Q are two irregular primes. An expert mystery key is picked at arbitrary. Each category is connected with a specific prime. All these prime numbers is placed within the general population framework parameter. A consistent size key for a set is made. For the people who are assigned the entrance rights for set can be created. In any case it is planned for the symmetric key setting. The content provider must get the relating mystery keys to write code. This is not appropriate for few applications. Since strategy is used to supply mystery esteem as opposition one or two open mystery keys, it is doubtful way to apply this thought for open key secret writing arrange. At long last, we tend to note of that there are plans that arrange to reduce the key size for accomplishing confirmation in symmetric key secret writing, on the opposite hand, giving of decipherment force is not a worry in these plans.

Cloud computing is looking as architecture for succeeding generation. It has many advantages though have risks of attacker who can access the data or release the user's identity. While setting a cloud user and service providers authentication is necessary. The issue arises whether cloud service provider or user is not compromised. The data will leak if any one of them in compromised. The cloud should be simple, preserving the privacy and also maintaining user's identity [10]. Privacy preserving public auditing for storage is the one, that information for the verification method in cloud information centers exploit third party auditor with privacy for information integrity mechanism. The information ought to be defending associate random masking and homomorphism linear critic. This analysis having several advantages that area unit supports the batch auditing for multiuser impression and also the limitations, that area unit ends up in a knowledge dynamism that is not tuned for batch auditing scheme.

III. KEY-AGGREGATE CRYPTOSYSTEM

Consider information privacy, through the server we can access our data after authentication only, which implies any sudden privilege can expose information. In cloud computing environment, things become worse. Assume that Alice keeps all her photos on Drop box, and he or she doesn't need to disclose to everybody, as a result of some unwanted reasons. Alice doesn't happy with the privacy protection provided by the Drop box. So, she encodes all files before uploading. Later Alice friend Bob asks her to share the photos in which Bob appeared.

Then Alice utilizes the share function of Drop box and shares the photos. However here downside is the way to provide the coding rights to Bob.

For traditional encryption, there are two ways to giving the decryption rights to receiver.

1. Alice encrypts all files with single cryptography key and offers Bob the corresponding secret key directly.

2. Alice encrypts files with distinct keys and sends Bob the corresponding secret key.

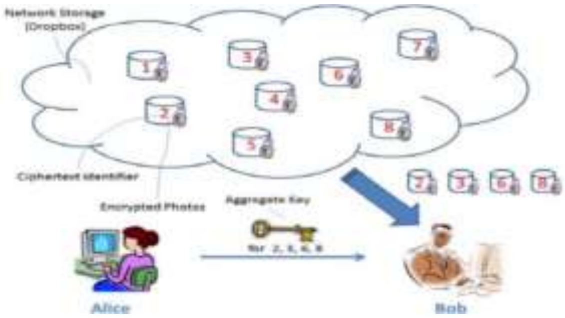

Fig: Fig 2: Alice shares files with identifiers 2, 3, 6 and 8 with Bob by sending him a single aggregate key

Clearly, the first method is insufficient because all personal data may be leaked to Bob. Obviously, the first technique is insufficient since all unchosen information is leaked to Bob. For the second technique, there are sensible issues on efficiency of such keys are as several because the number of the shared photos, say, a hundred. Transferring these secret keys inherently needs a secure channel, and storing these keys needs rather dearly-won secure storage. The prices and complexities concerned typically increase with the quantity of the coding keys to be shared. Here, we plan the systematic public key encryption technique which must do the perfect delegation of cipher text is decipher by constant size decryption key. We rectify this problem by introducing a special variety of public-key encoding that we have a tendency to call key-aggregate cryptosystem (KAC).

In this key aggregate Cryptosystem, users encode the data by using their public key and identifier. The ciphertext area unit more classified into totally different categories. The owner of the key contains the master secret key. Extracted key have often combination key that is as compact as a secret key for one category, however aggregates the ability of the many such keys, i.e., the secret writing power for any set of cipher texts categories. With our solution Alice can merely send Bob one combination key via a secure email. Bob will transfer the encrypted photos from Alice's Drop box area so use this combination key to decipher these encrypted photos.

A. Description of the algorithm

This mainly consists of five polynomial time algorithm:

1. Setup: The data owner executes the setup phase for an account on server which is not trusted. The input for this is a security parameter.

2. KeyGen: This is also executed by the data owner to generate public key and master secret key pair (pk, msk)

3. Encrypt: This is executed by data owner to encrypt the data. For this input is public key, index, message then it produces the ciphertext.

4. Extract: This extract function is executed by the data owner for giving the decryption powers to the receiver. For this input is master secret key, the set S then it outputs the combination key i.e., aggregate key

5. Decrypt: This is executed by the receiver who has the decryption authorities. For this input is Ks, the set S, an index i, and C then it outputs the decrypted result.

IV. CONCLUSION

In cloud computing, we mainly concentrate on how to protect the user's data. For a single application also we use multiple keys. In this paper, we study "how to compress" secret keys in public key cryptosystems which support delegation of secret keys for different ciphertext classes in cloud storage. A drawback in our work is that predefined certain number of most ciphertext categories. In cloud storage, the amount of ciphertexts sometimes grows quickly. We have got to order the enough ciphertext categories for future extension. Carrying these delegated keys in mobile device doesn't have a trusted hardware is caused to leak the keys. For this we design a leakage resilient cryptosystem for flexible and efficient key delegation.

REFERENCES

[1] 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.

[2] J. Benaloh, “Key Compression and Its Application to Digital Fingerprinting,” Microsoft Research, Tech. Rep., 2009.

[3] 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.

[4] 406.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.

[5] ChristofPaar, Jan Pelzl, “Introduction to Public-key Cryptography”, Understanding Cryptography, Springer, 2009.

[6] 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.

[7] D. Boneh, X. Boyen, and E.-J. Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext,” in Proceedings of Advances in Cryptology - EUROCRYPT ’05, ser. LNCS, vol. 3494. Springer, 2005, pp. 440–456.

[8] 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.

[9] 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.

[10] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, “SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment,” in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.

Selected Paper from International Conference on Computing (NECICC-2k15)