iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Privacy public cloud auditing by using KAC for scalable data sharing

M.Pavithra[1], S.Thivaharan[2],
[1] Pg scholar, Department of Computer Science, Kalaignar Karunanidhi Institute of Technology, Coimbatore
[2] Assistant Professor, Department of Information Technology, Kalaignar Karunanidhi Institute of Technology, Coimbatore

***Abstract*— Data sharing is an important role in cloud computing. Cloud computing technology is commonly used so that the data or information can be outsourced on cloud which is easily accessed. The objective is we show how to share the data in securely, efficiently, flexibly, and with other users in cloud computing. The various cryptographic techniques are used to share the data secure. So data owner encrypts the data and uploads on server. In this system, we launch a new public-key cryptosystem which create a ciphertext which is of stable size. That is, the secret keys are combined to form them compact as distinct key. Here, power of all keys being aggregated. This aggregate key can be shared to others or stored in a smart card with very limited storage. We also create a signature with encryption which is used to protect the user's data.**

Keywords: Cloud storage, data sharing, Cloud Auditor, Key-Aggregate Encryption.

I. INTRODUCTION

Cloud storage is growing popularity recently. In enterprise, the rise in need for data outsourcing demands the intentional management of shared data. Data can be stored on cloud remotely and can have access to large applications with quality services which are shared among customers [1].

Cloud service provider need to make sure whether audits are held for who have physical access to the server. As Cloud Service Provider stores the data of different users on same server it is possible that is leaked to others. The public auditing system of data storage security in cloud computing provides a privacy-preserving auditing protocol [2].

To make sure that the data integrity without compromising the anonymity of the data user is required. To ensure the integrity of user can check metadata on their data, upload and verify metadata [3].

The main worry is how to share the data securely the reply is cryptography. There are many cryptographic schemes in which third party will verify the files availability on behalf of data owner without leaking anything about data. Cloud users do not belief strongly on these third parties in terms of confidentiality. To overcome such situations research is going on. One of the study motivated users to encrypt their data themselves. Data owner uses their own keys and encrypt the data. Then uploads them to the server, also a public auditing system is provided to prevent the third party interruption.

Sharing and securing data, files photos is an essential role of cloud storage. Below figure shows the situation. Assumes that Alice uploads all her private files on dropbox and she does not want to release her files to others. Alice does not trust the privacy protection options provided by dropbox. For better privacy she decides her own encryption key to encrypt and decrypt the files. Suppose some day she wants to share few data with her friend Bob, either she can encrypt all files with single key and send him or she can encrypt with different keys and send it. The un-chosen data may be leaked to bob if the single key produced for encryption so create distinct keys of data and send single key for sharing.

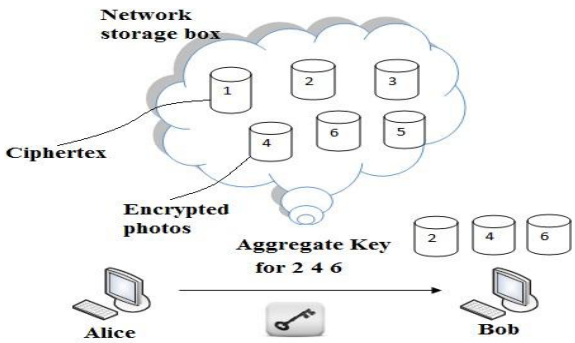


Fig 1: File sharing between Alice and Bob [].

A new technique of public-key encryption is used which is called as key-aggregate cryptosystem (KAC) [4]. The encryption is done through an identifier of ciphertext known as class, with public key. The key owner has the master secret key which is

helpful for extracting secret key. So the above scenario now the Alice can send an aggregate key to bob through a E-mail and the encrypted data is downloaded from dropbox using this aggregate key. This is shown in figure 1.

II. RELATED WORK

Authentication is used to provide privacy and security to the sensible information. Generally authentication is the way by which the computer system validates a user's gain access to information. But nowadays there are various cryptographic techniques for authentication such as Attribute Based Encryption, Identity Based Encryption, and Key aggregate cryptosystem.

A. Attribute Based Encryption

Goyal and Waters, "Attribute Based Encryption for Fine Grained Access Control of Encrypted Data" [2], presented a technique Key-Policy Attribute Based Encryption (KP-ABE). In this cryptosystem, ciphertexts are labeled with set of attributes and secret keys are associated with access structures that control with ciphertexts a user is able to decrypt. While this primitive was shown to be useful for fault-tolerant encryption with biometrics, the need of expressibility seems to limit its applicability to larger system. The KP-ABE constructions do not hide the set of attributes under which information is encrypted. This is the drawback of KP-ABE cryptosystem. In 2007 Bethencourt et al. proposed a ciphertext policy attribute based encryption (CP-ABE) [3]. Data owner only believes the key provider as CP-ABE technique addresses the difficulty of KP-ABE.

B. Identity Based Encryption

Sahai and Waters, "Fuzzy Identity-Based Encryption" presented a new type of identity-based encryption that called fuzzy IBE. In fuzzy IBE, it observes an identity as set of descriptive attributes. In this technique allows for a secret key for an identity, p, to decrypt a ciphertext encrypted with an identity, q, if and only if the identities p and q are close to each other. Therefore, this scheme allows a certain amount of fault-tolerance in the identities. Fuzzy-IBE produces to the two new applications. The first is an IBE system that uses biometric identities. That is it can show a user's identity such as iris scan, finger print. Since biometric measurements are noisy, we cannot use already present IBE systems. However, the fault-tolerant property of fuzzy-IBE allows for a secret key to decrypt a ciphertext encrypted with a slightly different measurement of the same biometric. Another application in fuzzy-IBE is Attribute Based Encryption. This technique is already explained in previous paragraph. The main drawback of this technique is to create a fuzzy-IBE where the attributes come from multiple authorities.

C. Key Aggregate Cryptosystem

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. Andrew Chi-Chih Yao and Yunlei Zhao," Privacy-Preserving Authenticated Key-Exchange Over Internet" presents a Diffie–Hellman key exchange (DHKE), a core cryptographic mechanism for ensuring network security. For key-exchange over the Internet both security and privacy are desired. Develop a family of privacy-preserving authenticated DHKE protocols named deniable Internet key-exchange (DIKE) both in the traditional PKI setting and in the identity-based setting.

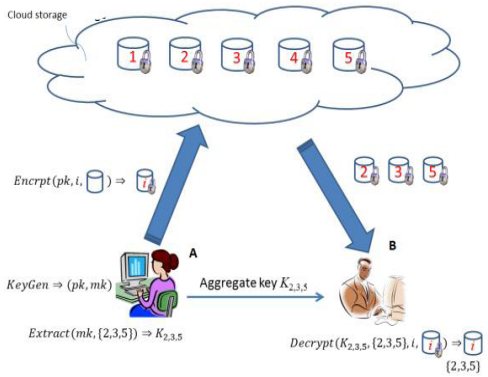


Fig. 2: Using KAC for data sharing in cloud storage

Compared with existing system we describe following features:

A. We can upload and share a secure data in cloud.

B. We use public key encryption, and create aggregate key for the data storing in cloud.
C. The owner will perform the basic encryption algorithm.
D. We propose a key Aggregate technique.

III.PROBLEM STATEMENT

In this article, it is studied how to use modern cryptographic techniques along with public auditing system so that the data sharing in clouds become secure. Generally we study about how to use small piece of knowledge into cryptographic functions. However, in this paper we study how to make decryption key more powerful. Decryption key should be powerful in the sense that it should allow decryption of multiple ciphertext without increasing its size.

Key Aggregate Cryptosystem is a special type of public-key encryption known as KAC. In KAC users encrypts a message not under a public-key. These encrypted messages are classified under ciphertext classes. The key owner possesses a master-secret key, which is used to extract secret keys for different ciphertext classes. The extracted key is an aggregate key which is as compact as secret key for a single class.

To solve the above problem we propose key aggregate encryption for prevent keys.

The KAC scheme has five polynomial-time algorithms and it is as follows:

Setup(1l, n): This is executed by the data owner to create an account on any untrusted server. The security level parameter and the number of ciphertext classes n is taken as input. The public system parameter param is given as output.

KeyGen: The data owner executes this algorithm for randomly generating a public/master-secret key pair (pk, msk).

Encrypt (pk, i , m): It is executed by the one who wants to encrypt the data. Public-key pk, an index i, corresponding to ciphertext class and a message m is taken as input. The ciphertext C is given as output.

Extract (msk, S): This is executed by the data owner for giving the decrypting power for certain set of ciphertext classes to the user. The master-secret key msk, and a set S of indices belonging to different classes is given as input.

The aggregate key for the set S is given as output i.e. KS.

Decrypt (KS, S, i, C): It is executed by the delegatee who got the an aggregate key KS, the set S, an index I associating the ciphertext class to which ciphertext C belongs to. The output obtained will be the message m if I belong to S.

Our contributions are:

1. We propose public auditing for additional security purpose. The owner will generate the key for encryption.
2. The decryption of multiple cipher text the size is constant in our scheme
3. We add a signature to perform authentication in cloud. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message and that the message was not altered in transit.

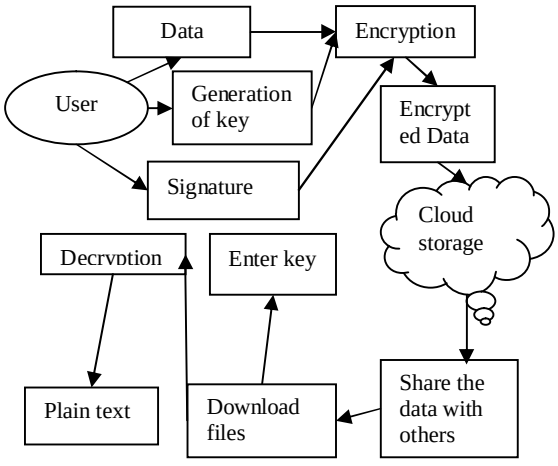


Fig 3: Using KAC with signature for data sharing in cloud

Algorithms for Secret key encryption

1. Start
2. Select file which we want to send.
3. Suppose files are i1, i2, i3, generate random key of respective file. Suppose that are sk1, sk2, sk3 Let, sk1=123, sk2=456, sk3=789

4. Combine the keys and add separator (ie.0) between them

5.Take one Quadratic equation, F(x)=a1x+a2x2+c Let,a1=19,a2=6,x=3(as sending files are 3) 6.F(x)=(19*3)+6*(32)+s F(x)=57+54+c F(x)=111+s 7.f(x)=111+12304560789 =1.230456e10 8.1.230456e10 this is aggregate key send via email.

IV. IMPLEMENTATION AND RESULTS

To authorize the effectiveness of our technique, we have produced a cloud audit system based on key aggregate cryptosystem. This system has been implemented in public cloud environment, which is used to storing and retrieving the data in cloud. We used a public cloud such as Aspose public cloud which is distributed cloud storage and constructed within the framework of Iaas. In this article, we consider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different ciphertext classes in cloud storage. No issue which one among the power set of classes, the delegatee can always get an aggregate key of stable size. The data's are stored in cloud (other party's control), also he can't able to access the data. All data's are gets encrypted. The third party can't able to release keys to illegal users secretly without the authorization of owner. By our evaluation, this method gives high percent of secure than the existing system.

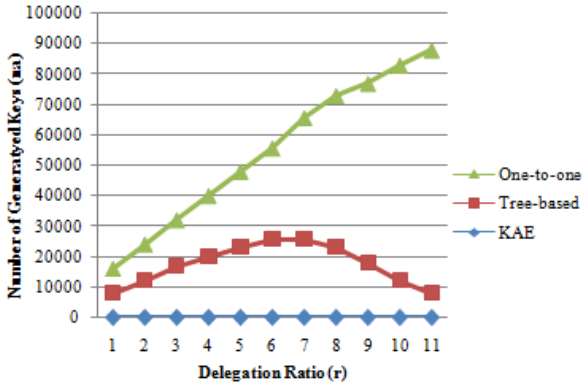


Fig.4: Computation time of tag generation for 1MB of data

V. CONCLUSIONS

Protect users' data privacy is a central concern of cloud storage. Cryptographic schemes are getting more and more flexible with the help of mathematical tools. Single application involves multiple keys. In this article, we consider how to "compress" or "aggregate" secret keys in public-key cryptosystems. This supports assignment of secret keys to different cipher text classes in cloud storage. It does not matter which class is among the power set of classes. The delegate to whom aggregate key is handed over always gets an aggregate key of constant size. The confidentiality of the encrypted files is preserved outside the set. There is no burden on the network overload, as there is utilization of compact aggregate keys. It also saves the expensive secure storage required to store these secret keys. There is no fuss of dealing with a hierarchy of delegation classes, more flexible than hierarchical approach. Regardless of the type among power set of classes, an aggregate key of constant size can be obtained. This will in turn reduce the secure storage and the overhead on the network.

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 Transactions On Parallel And Distributed System, Vol 25, No. 2 February 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," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.

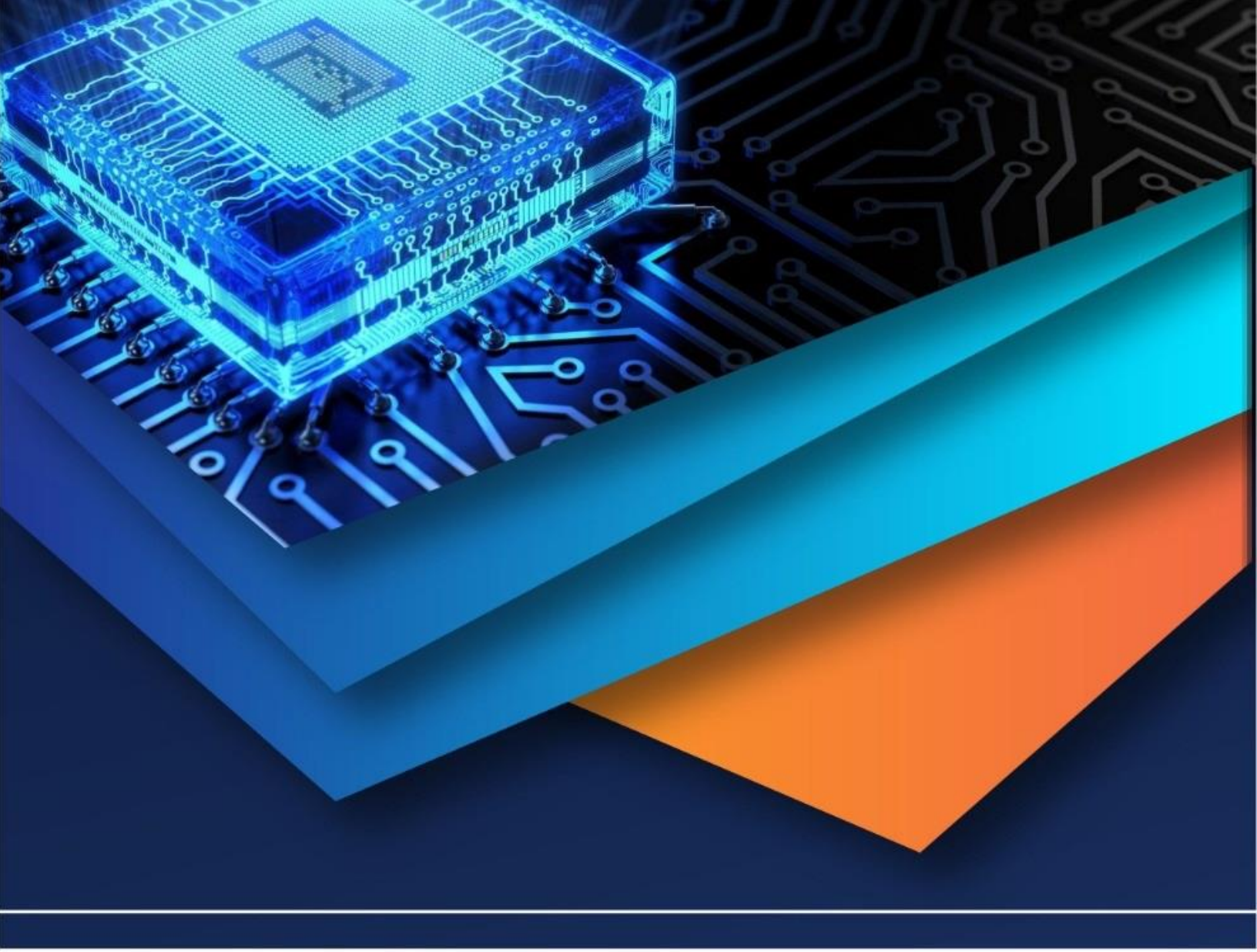
[3] Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans.Computers, vol. 62, no. 2, pp. 362–375, 2013.

[4] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems -ICDCS 2013. IEEE, 2013..

[5] Ramakrishna Jadhav, Snehal Nargundi," A Reviewon Key Aggregate Cryptosystem for scalable data sharing in cloud storage" in IJRET: International Journal of Research in Engineering and Technology, Vol 03, Issue: 11 Nov-2014.

[6] Garima Kumari, Lakshmi madhuri, "Key Aggregate Cryptosystem & intrusion detection for data sharing in cloud" in Multidisciplinary Journal of Research in Engineering and Technology, Volume 1, Issue 3.

[7] Shweta. P. Tenginkai, Vani K. S, "Cryptographic Algorithms for Efficient and Secure Data Sharing in Cloud Storage " in International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2015



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY