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 6, June 2015

An Efficient Cryptosystem for Secure Group based file Sharing in Cloud Storage Based on MES-2

Pramila Gharjale, Prakash Mohod

M. Tech Student, Computer Science and Engineering, G. H. Raisoni Institute of Technology and Engineering for Women, Nagpur, Maharashtra, India

Assistant Professor, Department of Computer Science and Engineering, G. H. Raisoni Institute of Technology and Engineering for Women, Nagpur, Maharashtra, India

ABSTRACT:- The Cloud storage means the storing the data online in the form of cloud. Data sharing is one of the important functionality in cloud. This approach describe one of the public-key cryptosystems as Key Aggregate Cryptosystem. This cryptosystem produce constant-size cipher texts, here decryption is more powerful since any set of cipher text can be decrypted at only one time by using aggregate key. which will show how one can communicate or share the data from cloud securely, efficiently and flexibly. The concept of this cryptosystem is that one can aggregate or gather any set of secret keys and from that gathering keys make single key which is compact. That means, the user who hold the secret key can send a constant-size aggregate key for set of cipher text in cloud , but the other encrypted files which is present outside the set will remain confidential. In this approach MES-2 that is Modern Encryption Standard-2 algorithm will be used for encryption.

KEYWORDS: Cloud storage, data sharing, key-aggregate encryption,Modern Encryption Standard-2

I. INTRODUCTION

The use of cloud storage is increases now a days. Every company or Every organization create a cloud or uses a cloud for his safety purpose. They store huge information in their cloud related to his company or organization so that if any employee want the information then they can directly access it from cloud. That means the employee or people related to that organization or company share the data from cloud. Sometimes company's useful information is also stored in the cloud but it is necessary that these information should not be leakage. Otherwise company or organization may face problem. for avoiding this problem user should share data securely so that useful or secret information related to that company or organization should not be leakage. There is many method for avoiding this problem like oruta, privacy preserving public key, Security mediator etc. They all uses third Party auditor (TPA) to handle the cloud data. Here TPA allowed to send the data or share the data to user. But in key aggregate cryptosystem user will get aggregate key and by using this key he can get set of ciphertext that he want. That means there is no need of TPA every time to Get the data from the cloud here user can access the data from the cloud direcly. Here user send the request to the server for getting some data, then user will form only one aggregate key for decrypting these set of the ciphertext and finally user will get set of the data that he want. There is only one key is require to share the set of data hence there is not require number of chhanel or communication requirement for sending the large number of key for large number of data. The key aggregate cryptosystem is public key cryptosystem because it uses number of key for encrypting the data and send another user only one key i.e. aggregate key for decrypting the set of ciphertext. In the key aggregate cryptosystem the master key, public key and ciphertext is of constant size. previous method is also used constant size key but they were need some hierarchical relationship. And in this type of cryptosystem no special relation between the classes is required [1].

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 6, June 2015

II. REVIEW OF LITERATURE

This section describes the various existing schemes which are compared in this paper [2-6].

2.1 KP-ABE, Proxy Re-Encryption & Lazy Encryption

This method is used in 2010 in the paper as "achieving secure, scalable and fine grain data access control in cloud computing " by cong wang, kui ren. The aim of this paper was getting secure, scalable and fine grained data access at cloud. Here assume that cloud server are more interested in file context and user access information than other secret information. Communication channel between user and proxy are assumes to be secure under existing security protocol such as ssl. The main goal of this paper is helping the data owner to get fine grain access control on file stored by cloud server. Generally data owner want to prevent cloud sever from being able to learn both content of the data file and privilege information which will be access by user. This paper was achieve goal by combining three techniques i.e. attribute Based Encryption, Proxy Re-encryption and lazy encryption. This scheme should be able to achieve security goal like user accountability. If all these goal achieved efficiently that means the system is scalable. The drawback of this paper is it uses KP-ABE and Proxy RE-encryption technique. The drawback of KP-ABE is the size of the key increases as number of attribute. PRE moves the secure key storage requirement from the delegate to the proxy. It is, thus, undesirable to let the proxy reside in the storage server That will also be inconvenient since every decryption requires separate interaction with the proxy.[6]

2.2 Dynamic Audit Services

This method is used in 2011 in the paper Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds by Yan Zhu, Gail Joon Ahn. This Paper propose a dynamic audit service for cheking the data integrity of an untrusted and outsourced storage. The above service is made based on the following technique. The disadvantages of this model is It require special type of storage for storing data like amazon simple storage, which is costly and require large bandwidth. This technique also require Fragment Structure and Index hash table which increases complexity [5].

2.3 Oruta

This is one of the technique for preserving privacy on public auditing for shared data in the cloud used in 2012 by B. Wang, B. Li, Hui Li. Oruta is the first privacy preserving mechanism which allows public auditing on shared data which is stored in the cloud. This method explain ring signatures for computing the verification information which is needed to audit the integrity or collection of shared data. Here The identity of the signature on each block in shared data is kept separate from a third party auditor (TPA), but he is still able for verifying the integrity or collection of shared data without retrieving the whole file. It contain mainly three parties as shown in fig 2.The main objective of this method is Public auditability, Correctness, unforgeability, Identity Privacy. This method include mainly 3 algorithm as Keygen, RingSign, and RingVerify.The limitation of this method is One can not distinguish who is provide signe on each block which can achieve identity privacy [4].

2.4 Privacy preserving public auditing

This method is introduced in feb 2013 by C. Wang, S.S.M. Chow, Q. Wang, K. Ren. The privacy preserving public auditing support to make secure cloud storage with the help of third party auditor. The objective of this paper is Public auditability, Storage correctness, privacy preserving, Batch auditing and Lightweight. Here mainly 4 Parties are present as shown in fig. 3 as cloud server, Cloud user, Third Party auditor, Cloud service Provider.The public auditing scheme consist of 4 algorithm KeyGen, SigGen, VerifyProof, GenProof. Here use MAC technique to authenticate the data. The drawback of this paper is there may be possibility that data may leak to third party auditor [3].

2.5 Security mediator

This method is introduced in July 2013 by B. Wang , S. S. M. Chow , M. Li and H. Li. This method is able to generate verification metadata on outsourced data for data owners. The objectives of this paper is Public Verifiability, Verification Efficiency, Unforgeability, Anonymity , Data Privacy, Signing Efficiency. This paper consist of mainly 4 entities as shown in fig. 4 as Cloud server, Data Owner, Security mediator, Data user. It mainy contain & types of algorithm that are SetUp ,Blind, Sign, Unblind, Challenge, Response, and Verify. The Drawback of this approach is it uses only one security mediator which may fail or less reliable.If it uses multiple SEM then there will require again seven algorithm for each SEM which increases complexity [2].

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 6, June 2015

III. PROPOSED SCHEME

Above all method allow to TPA (Third Party Auditor) for checking the presence of file to data owner without exposing data. But sometimes user are not comfortable with TPA. For removing this drawback Key aggregate cryptosystem is introduced in Feb 2014 by Cheng Kang Chu, S. S. M. Chow and Robert H. Deng. In this method user encrypt their data by using their own key before uploading to the server. Key aggregate cryptosystem is one of the public key encryption scheme in which user encrypt a message under a public key as well as identifier of ciphertext called class. The key owner holds a one of the delegated key i.e. master-secret key, which is used to extract secret keys for set of different classes that he want .By gathering or collecting the extracted key make aggregate keys which is as compact as possible and by using that one aggregate key user can decrypt number of ciphertext classe that he require. The system architecture of this KAC is shown in fig 1.

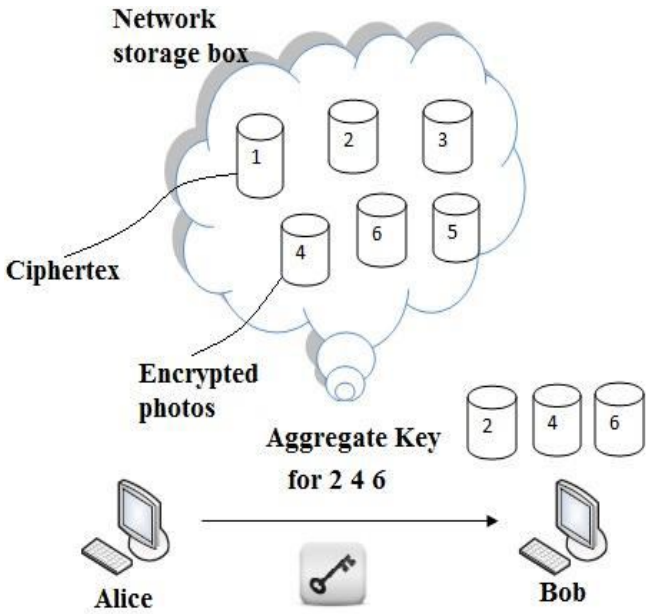

Fig. 1. Using KAC for data sharing in cloud storage

In KAC the size of the cipher text, Public key, Master key and aggregate key are of constant size. It consist mainly five algorithm Setup, KeyGen, Encrypt, Extract, Decrypt [1].

In this approach MES-2 that is Modern Encryption standard algorithm will be used for encryption. In the Modern Encryption Standard algorithm there is a use of Modified generalized Vernam cipher method with feedback with different block size from left to right. Here whole data is divided into different blocks and then applied vernam cipher to all blocks with different keys. The working of mes-2 algorithm is shown in fig. 2

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 6, June 2015

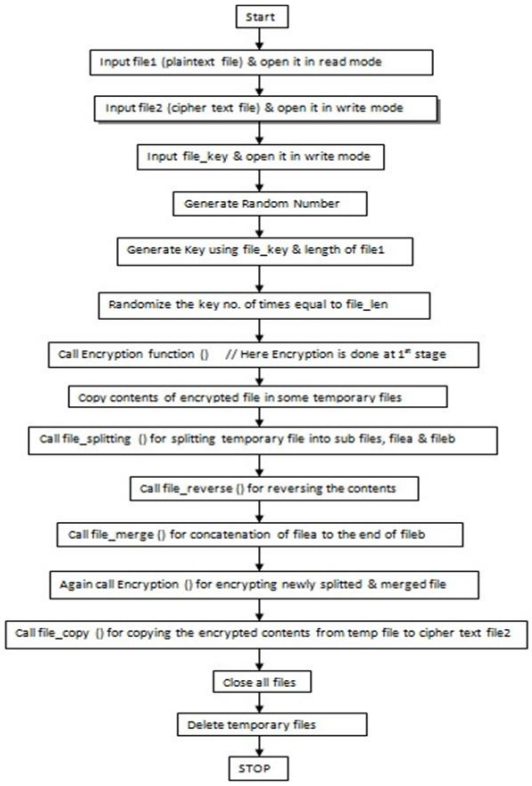

Fig. 2 flow chart for showing MES-2 working

IV. RESULTS

There are various results for sharing the data from the cloud. Fig. 3 Shows the Wampserver which is used for creating the cloud. Fig. $ shows the phpMyAdmin window which create the Database. Fig. 5 shows the wampserver homepage in which user can create his own account and after login he can upload the file, Share the file from data owner and with other user. Here use key aggregate cryptosystem for sharing the data securely, efficientlt & flexibly.

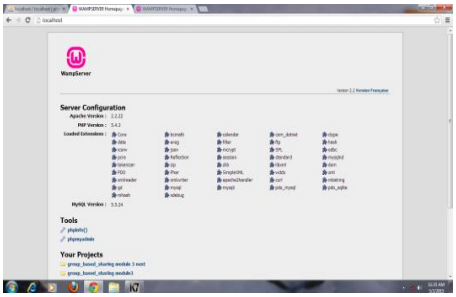

Fig. 3 cloud server creation

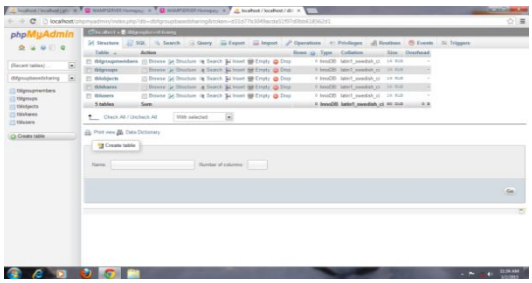

Fig. 4 database creaion

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 6, June 2015

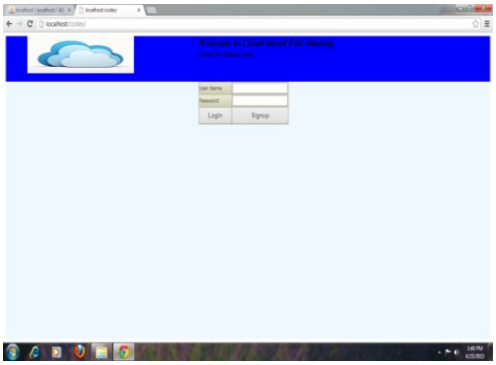

Fig.5 Homepage

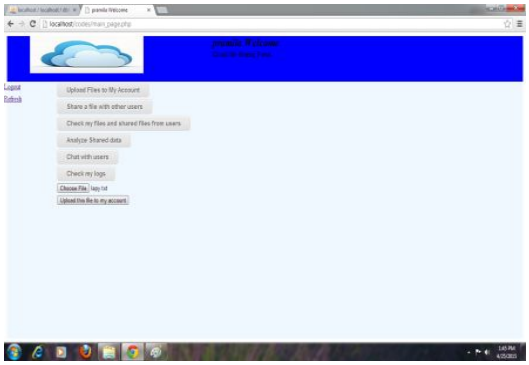

Fig.6 various option showing on homepage

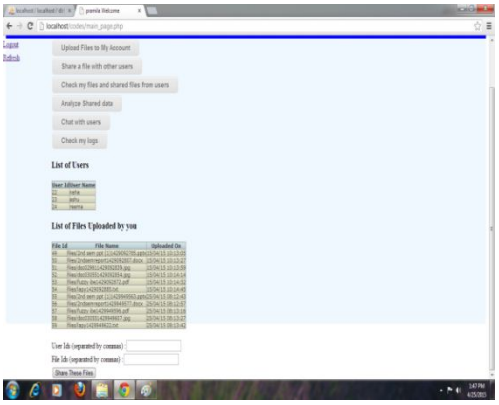

Fig.7 file uploading & sharing with aggregate keys

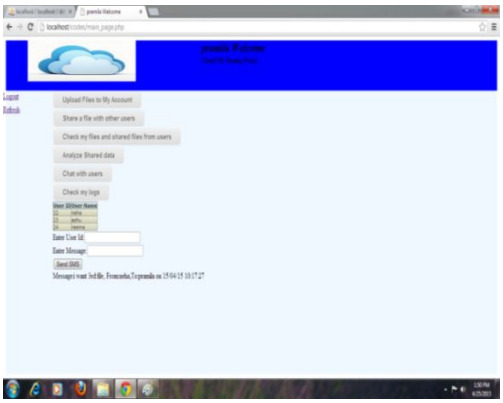

Fig.8 sending message to other user

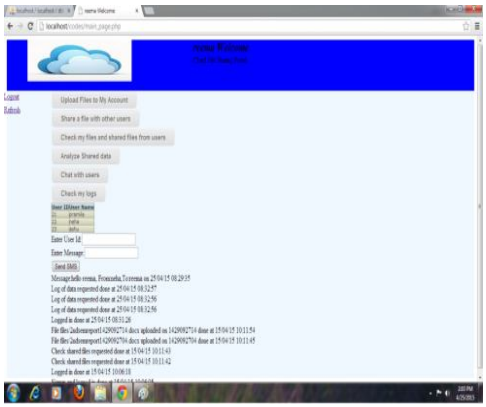

Fig.9 check log of user

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 6, June 2015

V. CONCLUSION

How to protect user's data privacy is a main important question of cloud storage. With the help of mathematical tools, different cryptographic schemes are more versatile than proposed sheme and always involve multiple keys for single application. Here we study and compare different techniques for sharing data securely with other in cloud storage and found that Key aggregate cryptosystem is more efficient and secure than other. In this survey we found that how key aggregate cryptosystem is more secure and provide more flexibility during sharing of data with other in cloud storage. Here Modern Encryption Standard-2 algorithm will be used for encryption which provide more security

REFERENCES

[1] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng,Senior Member, IEEE, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" IEEE Transaction computer,2014

[2] S. J. Manowar, A.M. shahu, "Introduction to Modern Encryption Standard (MES)-II: An independent and efficient Cryptographic approach for Data Security" IJCSIT2014

[3] J. suba, Seenivasan , "Multi Owner Data Sharing with Privacy Preserving in Cloud Security Mediator" IJSR 2014

[4] 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.

[5] 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.

[6] T. Paigude, T.A, chavan," A survey on Privacy Preserving Public Auditing for Data Storage Security" IJCSTT 2013

[7] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," in *IEEE Cloud*, June 2012, pp. 295–302

[8] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S.Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in *Proc. ACM Symposium on Applied Computing (SAC)*,2011, pp. 1550–1557.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained access control in cloud computing,"in *Proc. of IEEE INFOCOM'10*, San Diego, CA, USA, March 2010.

[10] R. Canetti and S. Hohenberger, "Chosen-Ciphertext Secure Proxy Re-Encryption," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 185-194, 2007.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06),pp. 89-98, 2006