Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 05, May -2018

# GROUP DATA SHARING FOR MULTI OWNER USING SINGLE KEY AGGREGATION

Kusalkar Jayashree[1],Midgule Swapnali[2], More Kajal[3], Nanekar Sonali[4], Prof.Ajay K. Gupta[5]

[1]*Department Of Computer Science and Engineering, SP`s Institute Of Knowledge College Of Engineering*
[2]*Department Of Computer Science and Engineering, SP`s Institute Of Knowledge College Of Engineering*
[3]*Department Of Computer Science and Engineering, SP`s Institute Of Knowledge College Of Engineering*
[4]*Department Of Computer Science and Engineering, SP`s Institute Of Knowledge College Of Engineering*

**Abstract**—*The largest issue for spread the data over a public cloud storage is Privacy. Data sharing is valuable functionality in cloud storage. The solution for secure data transfer is to encrypt the data before sharing and decrypting it after data retrieval by those who have the decryption keys. The practical issue of privacy protecting data sharing system based on public cloud storage which requires a data owner to spreading a large number of keys to users to enable them to access his/her files. By pointing this practical problem which is largely neglected in literature, we propose the concept of key aggregate Search Encryption (KASE) in which data owner only necessary to Spread a single trapdoor to group of users for sharing large number of documents and user only needs to submit a trapdoor to the cloud for querying and searching the shared a large number of documents.*

***Keywords***-*Searchable Encryption, Data Sharing, Cloud Storage, Data Privacy*

## I. INTRODUCTION

The ability of selectively distributing encrypted data with different users via public cloud storage may comfort security worry over unpredictable data leaks in the cloud. Designing the encryption schemes lies in the efficient management of encryption keys. The desired extensibility of sharing any group of selected files with any group of users demands different encryption keys to be used for different documents. The need of securely distributing to users a large number of key1s for Both encryption and search, and those users will have to securely store the Received keys, and submit an equally large number of keyword to the cloud in order to perform search over the shared data. The necessary for secure communication, storage, and complexity clearly renders the approach impractical. In KASE, Primary user only necessary to distribute a single Trapdoor, instead of number of Trapdoors for sharing files with Group of users, and users only needs to submit a trapdoor to the cloud server. The cloud server can use this aggregate trapdoor and some public information to perform search and return the result to Secondary User. Therefore, in KASE, the search right can be achieved by sharing the single Trapdoor. The responsibility of decryption rights can be achieved using the key-aggregate encryption approach. KASE scheme can be define as: To construction a key aggregate Search Encryption scheme under which any subset of the keyword cipher texts from any set of documents is searchable with a stable-size trapdoor generated by a balanced size combine key.

## II. EXISTING SYSTEM

Consider a example where two employees of a company would like to share some confidential business data using a public cloud storage service (e.g., dropbox or syncplicity). For instance, Primary User wants to upload a large collection of financial documents to the cloud storage, which are meant for the directors of different departments to review. Suppose those documents contain highly sensitive information that should only be accessed by authorized users, and Secondary User is one of the directors and is thus authorized to view documents related to his department. Due to concerns about potential Data leakage in the cloud, Primary User encrypts these documents with different keys, and produce keyword ciphertexts based on department names, before uploading to the cloud storage. Primary User then uploads and shares those documents with the directors using the sharing functionality of the cloud storage. In order for Secondary User to view the documents related to his department, Primary User must assign to Secondary User the rights both for keyword search over those documents, and for decryption of documents related to Bobs department. With a traditional approach, Primary User must securely send all the searchable encryption keys to Bob. After receiving these

keys, Secondary User must store them securely, and then he must generate all the keyword trapdoors using these keys in order to perform a keyword search. Primary User is assumed to have a private document set and for each document, a searchable encryption key is used. Without loss of any original concept, we suppose Primary User wants to share m documents with Bob. In this case, Primary User must send all the searchable encryption keys to Bob. Then, when Secondary User wants to retrieve documents containing a keyword w, he must generate keyword trapdoor Tri for each document with key and submit all the trapdoors to the cloud server. When m is sufficiently large, the key distribution and storage as well as the trapdoor generation may become too expensive for Bobs client-side device, which basically defies the purpose of using cloud storage.

## III. PROPOSED SYSTEM

In the existing system trapdoor is generated for number of files which we are sending to any user. Trapdoor contains the information of files and receiver of documents. But this trapdoor is unique for individual user. For another user we need to generate another instance of trapdoor which contains the information of receiver. In proposed method we are reducing the number of trapdoors to a single trapdoor of group of multiple users. And sending this aggregated trapdoor to each user of the group and allowing each user of group to access the contents of the file group. This data transfer will takes place when user confirms his identity in the group.This will reduce the generation of multiple trapdoors distributed over a cloud. Which results is faster data transfer and less use of memory for storing each trapdoor.(see Figure 1)

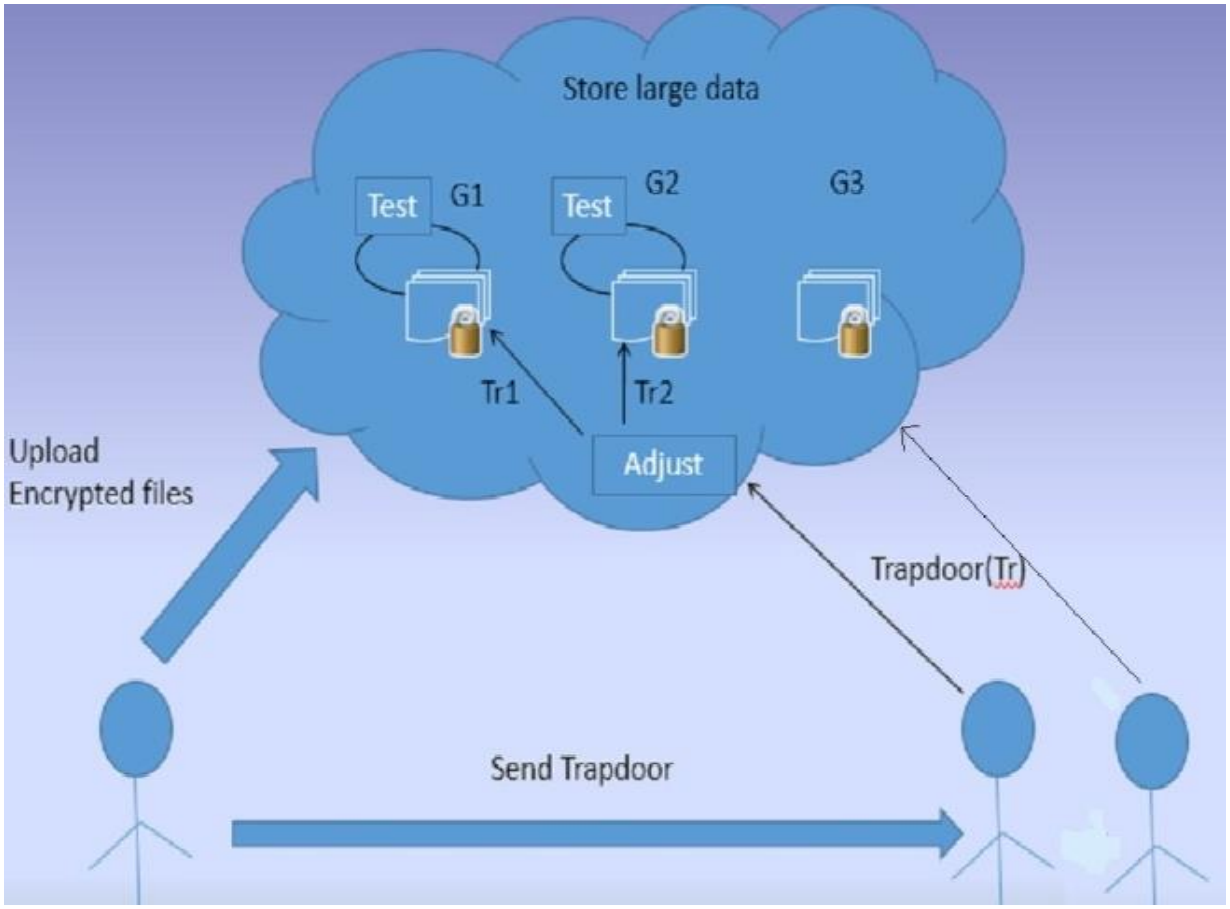
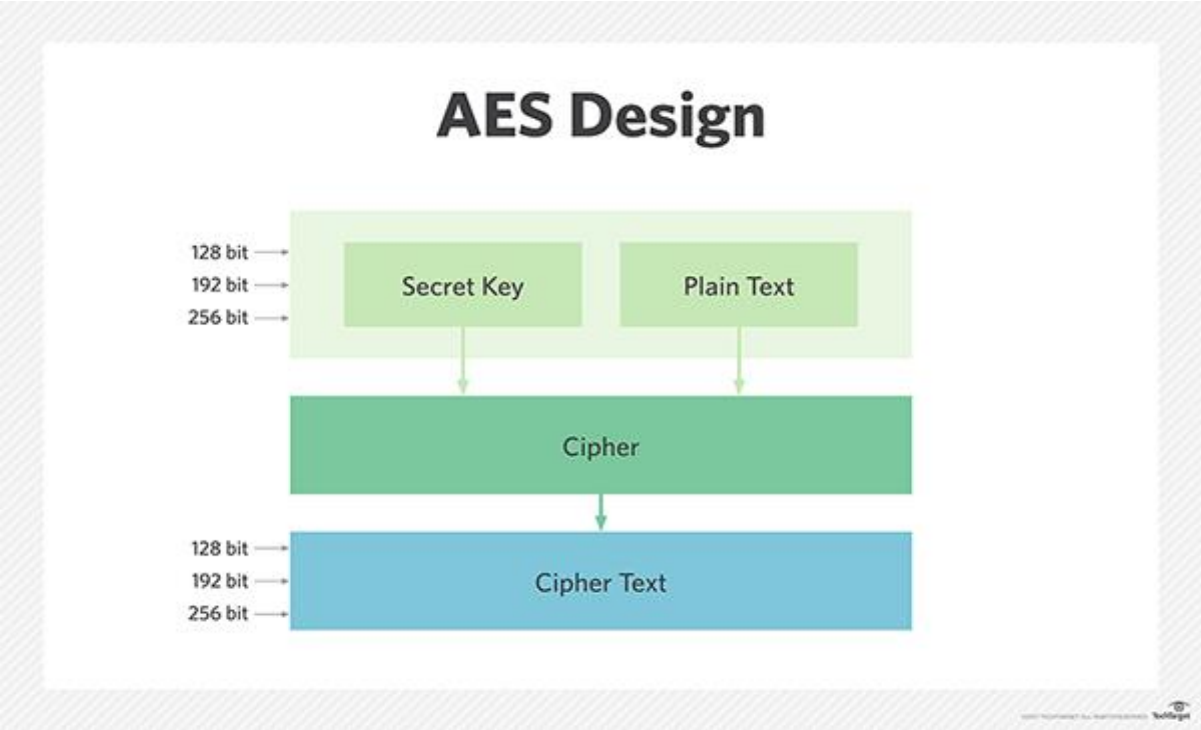



Figure 1: Architecture diagram of group data sharing

## IV. ALGORITHM

**1)AES:**AES or Advanced Encryption Standards (also known as Rijndael) is one of the most widely used methods for encrypting and decrypting sensitive information .This encryption method uses what is known as a block cipher algorithm to ensure that data can be stored securely.

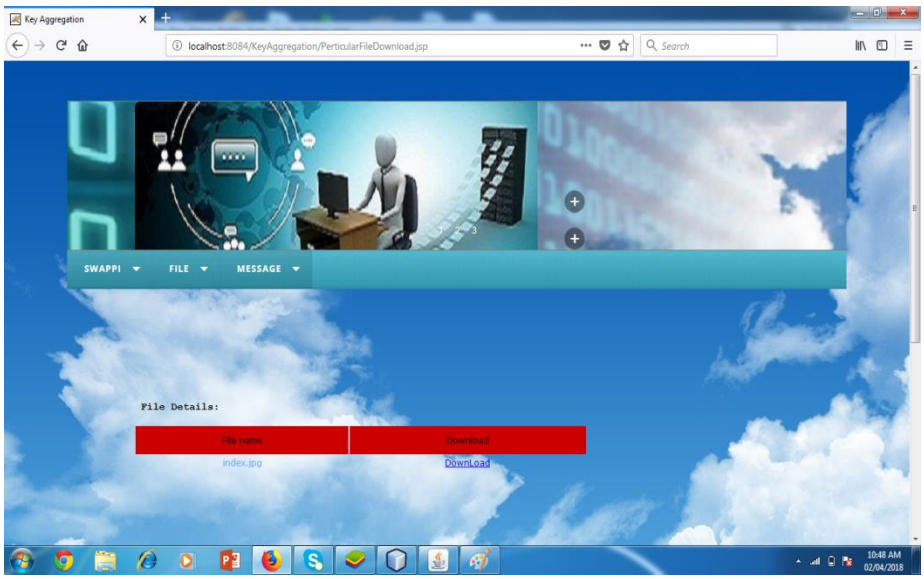



**2)RSA:**

a) Choose two distinct prime numbers p and q.
b) Find n such that n = pq. , n will be used as the modulus for both the public and private keys.
c) Find the totient of n, m. m=(p-1)(q-1).
d) Find e,such that gcd(e,m)=1
e) Now find d, ed mod m=1
f) Find private key =(e.n)
g) Find public key =(d.n)
h) Now calculate ciphertext $c=p^e \bmod n$
i) Now calculate plaintext $p=c^d \bmod n$.

**3)SHA:**The Secure Hash Algorithms are a family of cryptographic hash function published by the National Institute of Standards and Technology (NIST) . It is used for matching user and file identity.

## V. RESULTSET



## VI.CONCLUSION

In multi user system multiple trapdoors are generated. We are reducing these trapdoors to single trapdoor for multiple users. This will reduce the storage overhead of Number of keys and increase data transfer speed.

## VII.REFERENCE PAPERS

[1] Baojiang Cui, Zheli Liu_ and Lingyu Wang," Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage", IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015.

[2] X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multiownerdata sharing for dynamic groups in the cloud", IEEETransactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191.

[3] Z. Liu, Z. Wang, X. Cheng, et al. "Multi-user SearchableEncryption with Coarser-Grained Access Control in HybridCloud", Fourth International Conference on Emerging IntelligentData and Web Technologies (EIDWT), IEEE, pp. 249-255, 2013.

[4] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In: Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.

[5] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.

[6]S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing", Proc. IEEE INFOCOM, pp. 534-542, 2010.