Trapdoor Reduction on Sharing Group Data in Cloud using Aggregation Key Scheme

Swapnil Bhoyar[1] Gaurav Kawade[2]
[1,2]Department of Computer Science & Engineering
[1,2]G.H Raisoni College of Engineering Nagpur, India

Abstract— In cloud environment, number of clouds storage are available and these functional part of data storing, data sharing on huge number of space available for data storing that's why number of organization are move towards the cloud system for the use of data store. In Aggregation Key Scheme, data owner is work for uploading & sharing data with multiple user at a time. Data leaks in cloud environment and that their common approach is occurring encrypt with all data before uploading to cloud and also the encrypted data will convert into decrypted by the used of aggregation keys. For designing and implementing general framework of Aggregation Key Method with seven different algorithms for providing security analysis parameter like setup phase, key generation phase, encryption phase, key extraction phase, trapdoor generation phase, trapdoor adjustment phase and trapdoor testing phase. The publicly cloud is always used to sharing some confidential industrial or business data. (Examples- Drop box, Open drive, Google Drive, etc.) The main goal of Aggregation Key scheme is to reduce trapdoor. If user occurring any type issue or query over shared data by multiple owners then he must generating multiple trapdoor to the cloud environment and these numbers of trapdoors under multi-owners setting destroy the way of Trapdoor by using RSA Trapdoor algorithm.

Key words: Cloud Environment, Sharing Group Data, Trapdoor, Searchable Encryption, Searchable Keyword, Aggregate Key

I. INTRODUCTION

Now a day, the huge amount of demand of cloud computing is occurred. There are many number of functionality of cloud storage like data sharing, data storing, data security etc. but every time many questions are arise in every one's mind is it to shared data to other with securely, efficiently, and flexible way used for developing or implementing that type of system and different types of techniques or algorithms are used for secure data in cloud storage system. In cloud data it's very flexible to access for rights user with the help of internet facilities. There are many types of cloud storage are available and some of the cloud storage is free up to some limitation of storage capacity.

These 3 parameters are very useful for this system:

- Sharing Group Data: - Many time the Sharing Group Data work on the number of clients/ users are registered in one or many group. This type of work is perform on many organization or industries but they all are work in a group creating.
- Cloud Environment: - Cloud environment is available in everywhere & day by day the used of cloud is in very large scale but how it is available then many cloud are available in free & many cloud are available in paid service. No one functionality are available in cloud they can convert data into encrypted format. Now the system developed to convert data into encrypted format by using different type of algorithm. Cloud always used for data sharing & data uploading. Cloud security is most important part because many data available in cloud then it need to be more secure.
- Trapdoor: In this trapdoor the concept is depend on mathematical function because trapdoor is accessing way or path of given

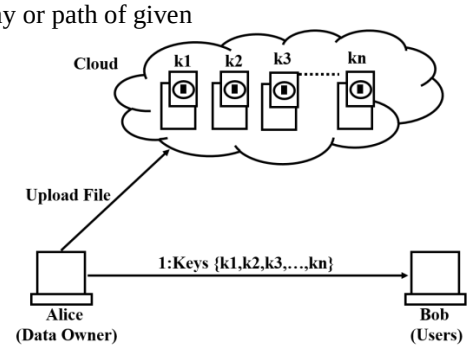

Fig. 1: Data uploading & generating shared key

As shown in figure 1, Data Owner (Alice) upload file to the cloud storage, So, Data uploadation the shared key generate using the AES algorithm and this data will be uploaded on encrypted format, So its provide more secure for storing[1].

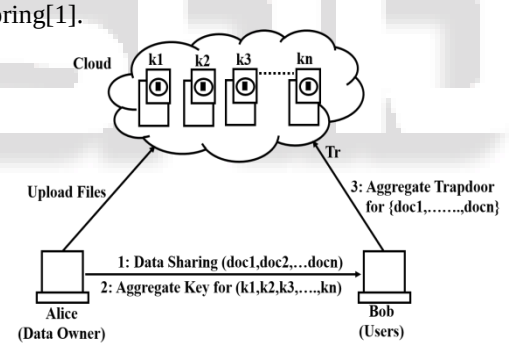

Fig. 2: Data Sharing & generating aggregate key and aggregate keyword send to user's mail

As shown in figure 2, Data Owner (Alice) share file to Users (Bob), at the time of Data sharing using the AES algorithm generating Keyword Trapdoor & Aggregate Key Trapdoor generated and send to their mail for using decryption purposed[1].

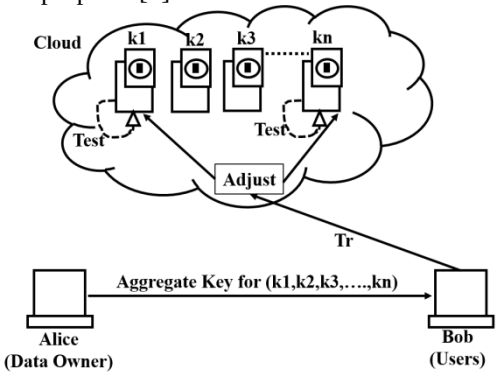

Fig. 3: Search data as per given Trapdoor

As shown in figure 3, Users (Bob) access the file using that trapdoor, both trapdoor are adjust to that file then it will decrypt otherwise decryption fail[1].

II. RELATED WORK

Individualize researches have been carried out on the securely group data sharing on cloud system using the different methodologies.

In this paper [1], the researched on sharing group data on cloud system which is done with the help of Broadcast encryption & searchable encryption method. In this research work Key Aggregate Searchable Encryption framework is used for sharing group data. The drawback is that, the implemented system is only work from Data Owner side not from User side.

In this paper [2], the researched on Attribute Based Encryption techniques use for Fine Grain Access of Shared data is in encrypted & its limitation is occurring of attribute base for more time to spend for check one by one attribute in encrypted data.

In this paper [3], the researched on hierarchical scalable access control technique used for secure multiple communication with the centralized key. In hierarchical technique to access more time.

In this paper [4], the researched on Identity based encryption technique is depend on pairing the private key generator with IBE.

While performing the literature survey it is observed that, these systems are not suitable for secure data sharing and could not solve the problem of data leak on cloud system. Hence, to overcome the problem of data leak on the cloud system is proposed.

Sr. no	IEEE Paper Titles	Methods/ Algorithm	Limitations
1	Key Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage	KESA Method with public key encryption	Trapdoor reduction work not completed
2	Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data	ABE Method	Number of attribute check then its gives more time spend
3	Scalable Hierarchical Access Control in Secure Group Communications	Centralized Key Management with Hierarchical Access Control	More time access for separating Hierarchical Control
4	Identity-Based Encryption from the Weil Pairing,	IBE Method	Pairing depends on Private Key Generator with IBE

Fig. 1: Research Papers

III. PROPOSED PLAN

As per the analysis above the algorithm being used among all the work done the Aggregation Key method with the efficient cost and time. It gives a great idea to analyse the method above and to improve the work further. For the method used the security of cloud in secure storage and access of data in cloud computing which is AES seems more suitable and efficient algorithm for the further work to be preceded.

In Data Owner process for upload the files with the Master-Secret Key to the Cloud. Encrypted Aggregate Key and Encrypted Searchable Keyword will be generated by using the input parameters given while uploading the files. He/she can view the list of active users available for accessing the files from cloud. In this paper, used for trapdoor as a aggregate key & aggregate keyword. He/she can view the files available in the cloud to share with a respective single user or a group of users registered with the groups.

In User process the trapdoor generate with the help of Key aggregate searchable encryption method. Initially users should produce the Encrypted Aggregate Key and Encrypted searchable keyword. By using this encrypted Aggregate key and the searchable encrypted keyword the Trapdoor Generation Process will be carried on for accessing the Cloud.

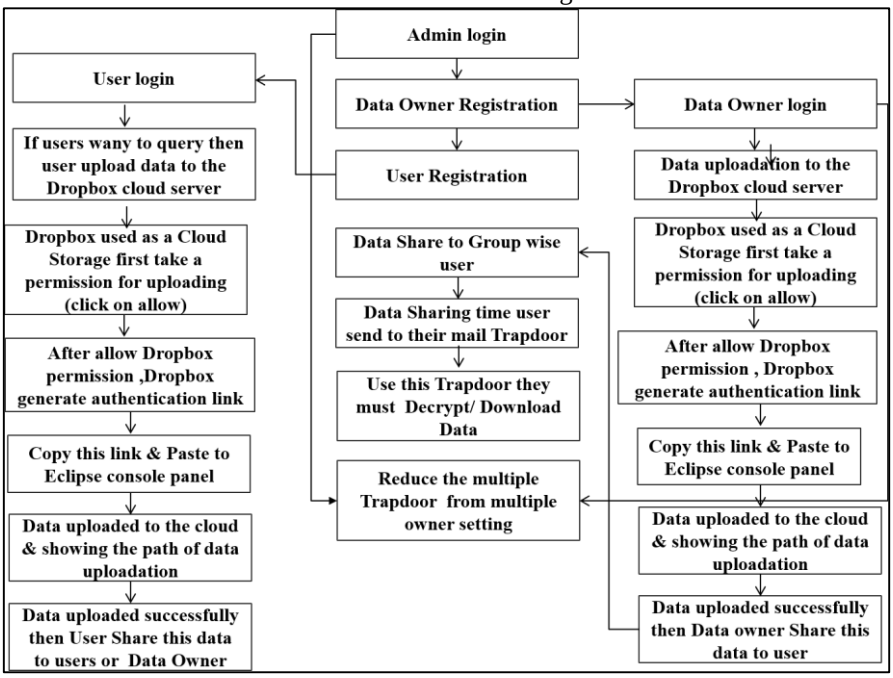

Fig. 4: Flowchart of Aggregation Key scheme

In a KASE method, This trapdoor reduction it's used for the load balancing concept and after completing work for sharing data from owner destroy the way for going to these file.

A. Steps:

- At first, registration is required for accessing share data, both data owner & user's registration is required. In users registration they will be categories into groups.
- After both registration completed, they can use the system as per given login id & password.
- The whole work start for the data owner side first like data upload to the cloud with encrypted format & generate aggregate key, data share to user with aggregate key & aggregate keyword, maintain user details record, maintain records of sharing data & generating keys etc.
- After sharing data from data owner side, user can access data with the given keys & decrypt or view these data in original format.
- If user occurred problem of shared data then user can also upload data to cloud & these data access directly gives to data owner.
- After all work completed then data owner reduce the trapdoor from user side because user work on this data after that they doesn't want it then data owner reduce it. They user panel always work in fast due to less data available on their panel.

IV. IMPLEMENTATION DETAILS

As per the analysis above the algorithm being used among all the work done the Aggregation Key method with the efficient cost and time. It gives a great idea to analyse the method above and to improve the work further. For the method used the security of cloud in secure storage and access of data in cloud computing which is AES seems more suitable and efficient algorithm for the further work to be preceded

A. Requirement for Designing Aggregation Key Method:

The Aggregation Key Framework design some functional requirement analysis like Compactness, Searchability, Delegation, Controlled Searching & Query Privacy etc. These functional requirement are explain in details as shown in below.

- Compactness: The KASE method requirement demands for ensuring the aggregate key size to be independent of data to be shared.
- Searchability: The KASE method requirement analysis to generate trapdoor for the given keyword for any type of searching encrypted data. Also number of key reducing search capability occurred.
- Delegation: The KASE method requirement analysis for right user only access to search keyword with aggregation method.
- Controlled Searching: The KASE method requirement analysis unauthorized user or attackers cannot search any data without permission of Data owner because they doesn't know the aggregate trapdoor then it's very difficult to search or attack on system.
- Query Privacy: The KASE method requirement analysis for untrusted or unauthorized cloud server to search any type of data.

B. Implementation of KASE Framework:

The implementation of Aggregation Key Framework is depend on seven polynomial phase like Setup phase , Keygen phase, Encrypt phase, Exact phase, Trapdoor phase, Adjust phase and Test phase etc. These all phase are explain in details as shown in below.

- Setup phase: The implementation of Aggregation Key method will use the Cloud server i.e. Drop Box Cloud. These system will be initialize by using APP_KEY & APP_SECRET because without authentication of this server no one user can access data from cloud. If the both keys are match with authorized Cloud server then got permission to access data otherwise permission reject from server side.
- Key generation phase: The implementation of KASE method will use for key generating. These key generation phase has been used for generating key with two algorithm like AES & RSA. By using AES algorithm has been used for Aggregate Keyword generating & RSA algorithm has been used for Aggregate Key generating. These two key are very useful for data security.
- Encrypt phase: The implementation of Aggregation Key method for uploading data with encrypted format with the help of AES algorithm & generate the aggregate keyword by using AES algorithm. Upload data to cloud is input phase and the aggregate keyword is generating as output phase. These algorithm will be initialize by given string phase & it will be generated by using random initial vector.
- Exact phase: The implementation of Aggregation Key method of exact phase can be used for data sharing time because Aggregate trapdoor is used for decrypt data or view data. These aggregate trapdoor will be match on shared file then it will exact file from encrypted format to original format otherwise not.
- Trapdoor phase: The implementation of Aggregation Key method of Trapdoor phase is both aggregate key & aggregate trapdoor. In trapdoor phase is used for reducing the trapdoor of shared data then it has been used for RSA Trapdoor algorithm. These trapdoor are depend on aggregate keyword if their keyword will be match then it will reduce otherwise error occurred for wrong trapdoor used.
- Adjust phase: The implementation of Aggregation Key method of adjust phase is used for the to check the APP_KEY & APP_SECRET of Drop Box cloud If these phase match then it has access otherwise not. Same concept used for aggregate trapdoor if it is match then it access. Every key will be adjust with the given phase.
- Test phase: The implementation of Aggregation Key method of test phase is check the shared key with users data if shared key match with data then it decrypt and if shared key is not match with data then it occurs error. Also these phase is always work with rights user because they got permission to granted for decrypting data with given keys.

V. EXPERIMENTAL RESULT

In this experimental result, the main objective of this system is to reduce the trapdoor with the help of Aggregation Key method.

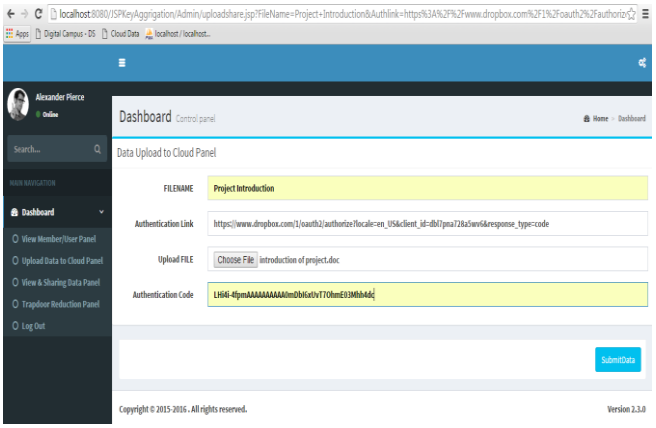

Fig. 5: Dropbox Cloud Authentication code for Data Uploading

In Fig. 5, it shows Data upload to cloud for Authentication link provide authentication code from cloud panel, with the help of cloud panel data can easily upload to the cloud in encrypted format.

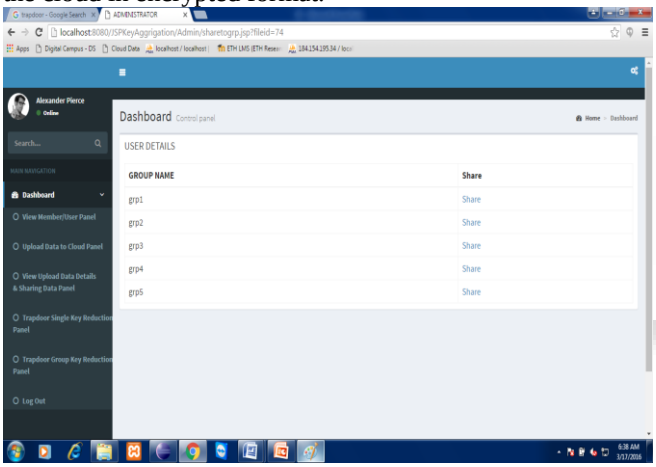

Fig. 6: Sharing group data panel

In Fig. 6, it shows many groups for sharing purpose but in this case it work on dynamic way for sharing group data.

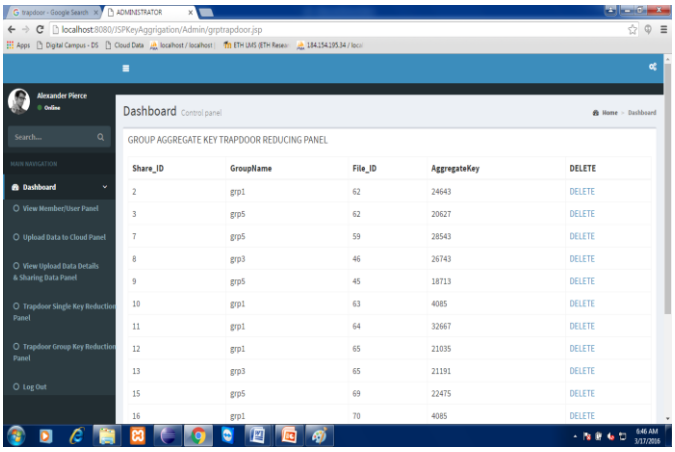

Fig. 7: Trapdoor Reduction Panel

In Fig. 7, Trapdoor reduction panel showing all details of group with their key & file id. By the used of data reduction using Trapdoor RSA algorithm.

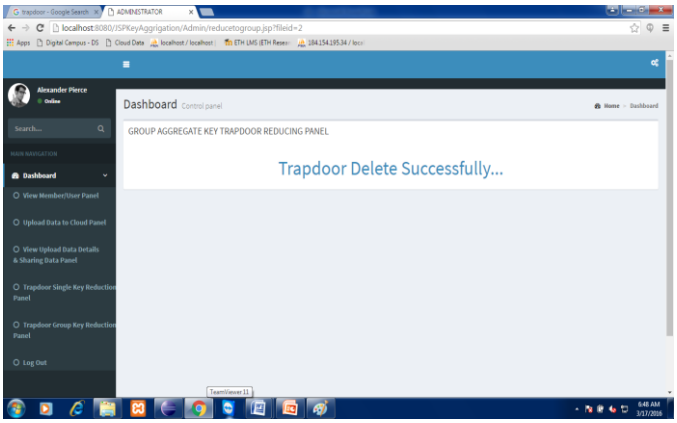

Fig. 8: Trapdoor Reduction completed

In Fig. 8, its shows trapdoor completely reduce by using given method.

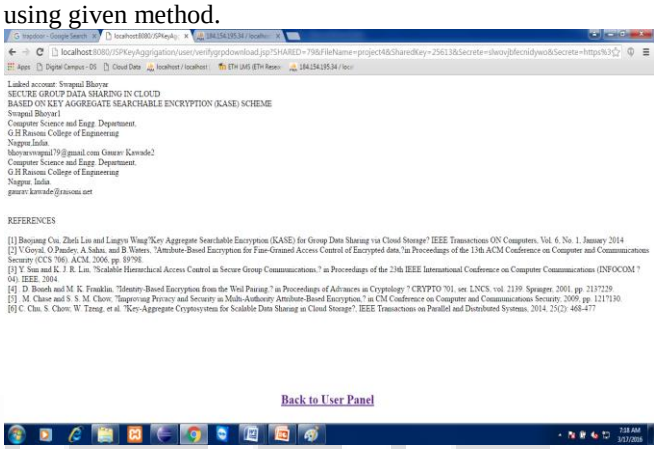

Fig. 9: Data show in Decrypted format

In Fig. 9, its shows Data in original or decrypted format using given aggregation key & keyword if it's both match with given data.

VI. CONCLUSIONS

I proposed the AES Algorithm, to secure data in cloud with the help of Aggregation Key scheme and reduce the way for going to file after completing task using multiple owner setting. This concept is basically work on designed high security system which is use from small to large organisation to store important data or document.

REFERENCES

[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. 6, No. 1, January 2014

[2] 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.

[3] Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," in Proceedings of the 23th IEEE International Conference on Computer Communications (INFOCOM '04). IEEE, 2004.

[4] 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.

[5] M. Chase and S. S. M. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” in CM Conference on Computer and Communications Security, 2009, pp. 121–130.

[6] C. Chu, S. Chow, W. Tzeng, et al. “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage”, IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477

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

[8] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Com-puting”,Proc. IEEE INFOCOM, pp. 534-542, 2010.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance:The Essential of Bread and Butter of Data Forensics in Cloud Computing”,Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.

[10] X. Liu, Y. Zhang, B. Wang, and J. Yan. “Mona: secure multi-owner data sharing for dynamic groups in the cloud”, IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191.

