INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A REVIEW ON IMPLEMENTATION FOR ENCRYPTED CLOUD DATA BY USING EFFICIENT METHOD OF AGGREGATE KEY.

MS. AKANKSHA D. KANSE[1], DR. A. S. ALVI[2]

1. ME (2nd year), Computer Science & Engineering, Prof. Ram Meghe Institute of Technology & Research, Badnera.
2. Professor, Computer Science & Engineering, Prof. Ram Meghe Institute of Technology & Research, Badnera.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: The prospective of selectively sharing encrypted data with various users with the help of public cloud storage may very much easiness security concerns over unintentional data leaks in the cloud. A key brave to designing such encryption schemes lies in the well-organized management of encryption keys. The preferred flexibility of sharing any group of selected documents with any group of users demands dissimilar encryption keys to be used for dissimilar documents. On the other hand, this also implies the necessity of robustly spreading to users a huge amount of keys for both encryption and search, and those users' needs to confidentially store the keys received by them, and then submit a uniformly huge amount of keyword trapdoors to the cloud in order to complete search on the shared data. The implied need for secure communication, storage, and complexity precisely converts the approach impractical. In this paper, we deal with this practical problem, which is largely neglected in the previous studies, by proposing the key aggregate searchable encryption (KASE) concept and to initialize the concept through a concrete KASE scheme, in which a data vendor only needs to distribute a single key to a user for sharing a large amount of documents, and the user needs to submit only one trapdoor on the cloud for asking the shared documents. The security analysis and performance evaluation both verify that our proposed schemes are provably and practically well-organized.

Keywords: Cloud Computing, Encryption, Key aggregation, Cloud Storage, Searchable Encryption.

Corresponding Author: MS. AKANKSHA D. KANSE

Access Online On:

www.ijpret.com

How to Cite This Article:

Akanksha D. Kanse, IJPRET, 2016; Volume 4 (9): 959-968

PAPER-QR CODE

INTRODUCTION

Cloud computing is popular and current technology that is being used in IT sector. As its flexibility of unlimited data storage and its access all over world. The cloud computing concepts based on "Pay As You Go" model and we need to pay storage cost to the company. So it's mainly importance to first reduce the cost of storage and remove the repetitive data. For the cost minimization, we need to take care about confidentiality of data and we cannot avoid the reality. A range of methods had been proposed in current time to provide confidentiality of cloud data.

Data sharing is a vital functionality in cloud storage. For example, bloggers allow their friends to see a division of their private data; an enterprise may allow his employees access to a portion of receptive data. The demanding problem is how to share encrypted data effectively. Users can download the encrypted data from the storage and then decrypt it and send them to other users for sharing, but it decreases the worth of cloud storage. Users should be capable to give the access privileges of the sharing data to others so that they can access these data from the server directly. Though, searching an efficient and reliable way to share partial data in cloud storage is not difficult.

I. Related work

The recent work done in the area is listed below which helps us to perform the research in the area. To report user's worries of potential data leaks in cloud storage, a common approach is for the data owner need to encrypt all the data earlier uploading that data on to the cloud, such that later the encrypted data may be retrieved and decrypted by the decryption key which is hold by end user . Such cloud storage is often called the cryptographic cloud storage [2].The two concepts presented in our approach is the key aggregation and searchable encryption. The first part that is key aggregation has been performed in the key aggregate cryptosystem paper till 2014 only, but this research does not address the concept of searchable encryption [1].

In [3], attribute based encryption (ABE) is applied to achieve fine-grained access control aware keyword search. As a result, in MUSE, the main problem is how to control which users can access which documents, whereas how to reduce the number of shared keys and trapdoors is not considered. Key aggregate searchable encryption can provide the solution for the latter, and it can make MUSE more efficient and practical.

In this paper [4], they propose a new method to enable effective fuzzy keyword search in a multi-user system over encrypted cloud data while maintaining keyword privacy. In this new system, differential searching privileges are supported, which is achieved with the technique of attribute-based encryption. Edit distance is utilized to quantify keywords similarity and develop fuzzy keyword search technique, which achieve optimized storage and representation overheads.

During this paper [5], we tend to gift an summary of body area network and their connected problems stress in security downside. We tend to conjointly offer the variations between Wireless Body Area Network and Wireless Sensor Network (WSN) that is inadequate to use in WBAN though some challenges visage by WBAN area unit in many ways just like WSN. Finally, we tend to highlight security challenges that also have to be compelled to be addressed to create WBAN actually present for a wide range of applications.

Popa [6] firstly introduces the concept of multi-key searchable encryption (MKSE) scheme and puts ahead the first feasible scheme in 2013. MKSE allows a user to provide a single keyword trapdoor to the server, but it permits the server to find for that trapdoor's keyword in documents encrypted with different keys. The goal of KASE scheme, it sound very similar to but actually these two behaves totally different.

Searchable symmetric encryption (SSE) permits a client side to encrypt its data or information in such a way that this data can still be searched. The most instant application of SSE is to cloud storage, wherever it enables a client to strongly outsource its data to an untrusted cloud provider without reducing the ability to search over it. S. Kamara [7] recommended a new technique known as "Dynamic searchable symmetric encryption" that means SSE has been the center of dynamic study and a gathering of schemes that achieve a variety of levels of confidentiality and effectiveness have been proposed. To report this, we firstly advise the SSE scheme to satisfy all the properties like sub linear search time, security against adaptive chosen keyword attacks, the ability to add and delete records and compact indexes. In addition, we implement our scheme and conduct performance estimation, showing that our approach is efficient and complete for deployment.

To allow a number of documents encrypted by different keys to be decrypted with only one aggregate key, user will able t encrypt a message with the help of public-key, and under the identifier of each document. The construction is inspired by the broadcast encryption scheme [8].

Jin Li [9] propose a new concept called hidden attribute-based signature, it is motivated by the current developments in attribute-based cryptosystem of multi key searchable encryption. With this technique, users are capable to sign messages with any division of their elements issued from an element center. In this notion, a signature verifies not to the identity of the individual who authorized a message, but instead to a claim regarding the attributes the fundamental signer possesses. Users cannot copy signature with attributes which they have not been issued.

II. proposed work

A. Motivation

As we are aware cloud computing is the recent workflow model in IT industry and it gives flexibility in data operation, it also gives the reason of data security. To manage the security of data deployed over the cloud we propose the technique of encryption of data, but it gives the overhead of managing keys for multiple keys. Also the searching in the encrypted content is quite critical. We are proposing a method of searchable encryption and key aggregation system.

B. Problem statement

Cloud computing has given the users the accessibility to deploy number of files to the centralized cloud and share those with number of users. The flexibility of cloud computing always comes with the hurdles of security concerns. The data owner always needs to encrypt the files before uploading and it must decrypt before end users. This system needs secure storage of keys, but as files gets increased in number keys management becomes complex. We have proposed the system called as (KASE). The system proposes aggregate key for file sharing in groups and searchable encryption. We have observed that to create trapdoors manually for specific files it becomes very tedious and hence we have applied the TF-IDF technique to avoid manual job.

C. System Architecture

Solving Approach:

In this paper, proposing a KASE scheme to solve the above mentioned problem in problem definition. We need to concentrate on two techniques

1. Key Aggregation

2. Searchable Encryption

Key aggregation:

The key aggregation scheme I am proposing is based on the hierarchical modeling of your document segments over cloud. In this scheme I divide the documents in tree and tree is based on parent child relation. I need to create aggregate key for each parent node and I need to share these keys through secure channel to the end user. If the user will provide key of any parent node the documents under the child of that parent node will be available for download. I can add any node in the tree dynamically.

Searchable Encryption:

To perform search operation on encrypted text over cloud we need to extract some important keywords from the documents in upload them over cloud with files. These are called as trapdoors and used by end users to search content over cloud. But to extract trapdoors from the documents manually is somehow a tedious job so I am applying a technique to extract trapdoors from the documents.

Modules Information:-

Modules 1:-UI creation and application setup:

In this module I will create basic framework for application and I will create login for multiple entities and I will define their roles.

Module 2:- Dynamic Aggregate key generation and trapdoor generation

In this module I will implement the aggregate key generation for documents uploaded. The uploaded documents will be scanned for trapdoors and will be deployed over cloud with encrypted document.

Module 3:- Document retrieval

In this module end user will try to search the document he is trying to look for. The user will submit the trapdoors to the cloud and based on the trapdoors cloud will display the documents mostly related to.

Module 4:- Analysis and testing and deployment

This phase is final and I will perform testing and I will perform the analysis phase to compare with the existing method. The last step will be to deploy the application with the real time cloud environment.

Outcome:

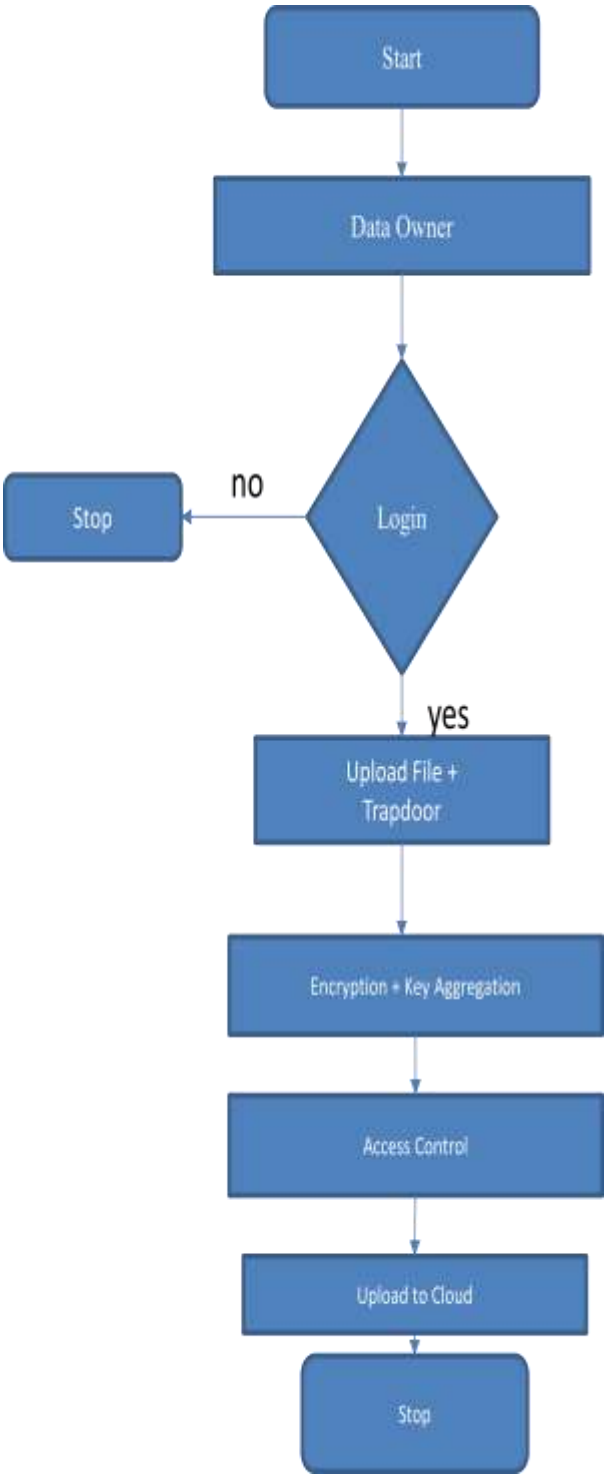
The application can be easily use in real time cloud computing platform and for the organization which manages their data over cloud keeping minimum computational cost.

D. Proposed system Design

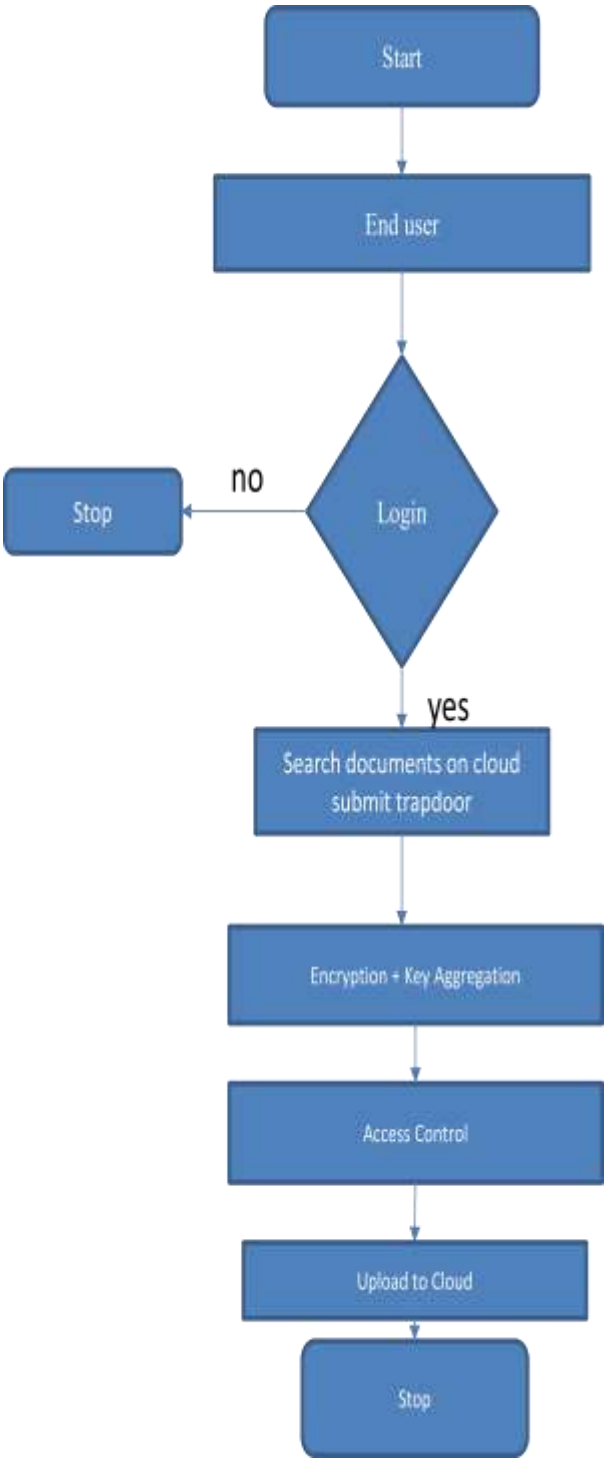
Data Flow Diagrams

A data flow diagram (DFD) is a flowchart of the "flow" of data throughout an information system, modeling its process aspects. Often they are a primary step used to create an overview of the system which can be in future it will expand. A DFD show the kinds of information that will be input to system and output from the system, where the data will come from which location and go to which location, and where the data we needs to stored. It does not show information about the timing of processes, or information about whether processes will operate in series or in parallel.

Step1: Upload



Step 2: Download



Description of proposed Architecture:

To design such system which takes the concept of key aggregate searchable encryption (KASE) and initializing the concept through a concrete KASE scheme, in which a data owner only have to allocate a single key to a user for sharing a huge amount of documents, and the user only needs to submit only one trapdoor to the cloud for asking the shared documents. The security analysis and performance estimation shows that our proposed schemes are secure and efficient.

Search query as input and by analyzing the search results it returns the clusterd results. The purpose of paper is that to produce clustered results and gathering user goal which is keyword or name for cluster. And this clustered result will minimize the time span to check relevant result. And such clustering also gives more relevant result.

To permit secure and confidential data sharing and collaboration in the Cloud, there needs to first be proper key management in the Cloud. First, data owners have to allocate an only one aggregate key (instead of a group of keys) to end user for sharing huge amount of files. Second, the user only needs to submit an only one aggregate trapdoor using TF-IDF to the cloud for performing keyword search over any number of shared files.

III. CONCLUSION

In this paper, we are Considering the practical problem of privacy maintaining data sharing system based on public cloud storage which requires a data owner to assign a huge amount of keys to the users side to permit them to access his/her documents, we are proposing first time the model of key-aggregate searchable encryption (KASE) scheme and concept a concrete KASE scheme. Both analysis and estimate results prove that our work can provide an effective solution to constructing data sharing system based on public cloud storage. In this paper, a KASE scheme, when allocating number of documents with the user, the owner only needs to distribute a single key to a user and then user needs to submit a only one trapdoor when he requests over all documents shared by the same owner. However, if a user wants to query over documents shared by different types of vendor, he must generate multiple trapdoors to the cloud. Nowadays Federated clouds, attracted a lot of attention, but our KASE cannot be applied in this case directly.

REFERENCES

1. C. Chu, S. Chow,W. Tzeng, et al. "Key-Aggregate Crypto system for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.
2. R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In: Proceedings of the 13th AC conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.
3. C. Dong, G. Russello, N. Dulay. "Shared and searchable encrypted data for un trusted servers", Journal of Computer Security, pp. 367-397, 2011.
4. J. W. Li, J. Li, X. F. Chen, et al. "Efficient Keyword Search over Encrypted Data with Fine-Grained Access Control in Hybrid Cloud", In: Network and System Security 2012, LNCS, pp. 490-502, 2012.
5. M. Li, W. Lou, K. Ren. "Data security and privacy in wireless body area networks", Wireless Communications, IEEE, 17(1): 51-58, 2010.
6. R. A. Popa, N. Zeldovich. "Multi-key searchable encryption". Cryptology ePrint Archive, Report 2s013/508, 2013.
7. S. Kamara, C. Papamanthou, T. Roeder. "Dynamic searchable symmetric encryption", Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965- 976, 2012.
8. D. Boneh, C. Gentry and B. Waters. "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys", CRYPTO'05, pp. 258C275, 2005.
9. J. Li, K. Kim. "Hidden attribute-based signatures without anonymity revocation", Information Sciences, 180(9): 1681-1689, Elsevier, 2010.