Implementation of Searchable Encryption using Key Aggregation for Group Data Sharing in Cloud

Sanjana M. Kavatagi[1], Dr. Rashmi Rachh [2]
M.Tech Scholar[1], Associate Professor[2]
[1,2]*Dept of CSE, Visvesvaraya Technological University, Belagavi, Karnataka, India*

Abstract

Cloud computing is gaining popularity because of the services it provides but security is still an issue to be addressed. The data must be stored securely on cloud to avoid the security breaches such as data leaks. In order to store data securely, different encryption keys are used for sharing documents with different users. The users must generate large number of trapdoors for performing search over the files and decrypt them. This project aims to implement searchable encryption using key aggregation scheme, in which the data owner who uploads the file needs to distribute a single key to user for sharing number of files and the user needs to produce and send only one trapdoor to the cloud for querying over all the documents.

Keywords

Cloud storage, data privacy, searchable encryption, data sharing.

I. INTRODUCTION

Internet usage has been increased extensively in the past few years leading to the generation of large data both in case of personal data as well as business data. Storage of this data becomes a major concern. Cloud computing performs an important role in this concern. It is a method based on internet which allows computer to deal with the shared resources and other things for various devices as and when needed. It is a method for empowering ubiquitous, on-demand admittance to configurable computing assets. Basically, cloud computing permits the clients undertaking different capabilities to accumulate and further transform their information for possibly privately possessed cloud, or around a third-party server.Security of cloud refers to a wide set of policies, controls imparted to protect data, technologies, applications and related infrastructure of cloud. Cloud computing gives its users the capabilities to process and store their information in third party data centers. Security problems related to cloud is divided into two broad categories: security issues confronted toward cloud suppliers (organizations giving software-, platform-, alternately infrastructure-as-a-service by means of those cloud) and the security issues faced toward their clients (companies or associations who host provisions alternately store information on the cloud). Those obligations are shared. Those providers must guarantee that the framework is secure and their clients' information and their applications are preserved, along with the clients must detract measures to strengthen their provisions with the utilization of solid passwords and verification measures.

A) Ciphertext-policy ABE (CP-ABE)

In the CP-ABE, those encrypter controls entry strategy, Concerning illustration of those system that gets only some part of the complex computation, the configuration for framework gets a greater amount of complex, and the security of the framework may be more challenging.

B) Completely homomorphic encryption (FHE)

Completely homomorphic encryption permits clear computations with respect to encrypted information, likewise permits access to encrypted information without unscrambling.

C) Searchable encryption (SE)

Searchable encryption is an encoding technique which provides a secure method for search capability against encrypted information. To extend the efficiency of finding information, SE generates pivotal word indexes to safely perform client queries. SE schemes could be arranged under two categories: SE in view of secret-key cryptography and SE dependent upon public-key cryptography.

II. RELATED WORK

C Wang et al. [1] discussed a method for achieving scalability, information secrecy while accomplishing fine-grainedness towards characterizing and enforcing right approaches dependent upon information attributes, and permits those data owner to represent the calculation

assignments included in finegrained information gain on untrusted cloud servers without uncovering those underlying information substance. This objective will be attained towards exploiting and particularly joining together strategies from claiming attribute-based encryption (ABE), proxy re-encryption.

Y. Zhang et al. [2] recommended a secure multi-owner information imparting plan for progressive aggregations in the cloud. Utilizing progressive methods and group signature a few cloud clients might offer information anonymously with others. Encryption calculation expense and the overhead of the storage space of the plan is self governing the renounced clients.

C.K.Chu [3] suggested a plan that depicts new general population cryptosystems that process consistent cipher texts. One could combine any set of master keys and combine them to make one key, imparting the power of an aggregate key. This combined key might be saved on smart card or given to others successfully.

T. Nishide et al. [4] recommended a structure to secure method imparting from claiming particular well being records previously, utilizing the cloud storage. The method addresses the exceptional tests brought eventually using the various records or the users, in that maximally decrease the intricacy about maintenance of keys along with improvements of security ensures. It uses ABE to scramble the data, along these lines that it can have entry not best toward the particular clients as well as by clients starting with open domains with distinctive parts.

D. Wagner et al. [5] portrays a cryptographic method for the issues on seeking the encrypted information also giving acceptable evidences from claiming security for the newly accepted crypto frameworks. The procedure may be provably secure, that gives a standard method for encryption, with the assumption that the untrusted server cannot take anything around the plaintext when it is provided for those cipher text.

Z. L. Liu et al. [6] recommended a multi-user searchable encryption schemes that are built by providing the logic of searchable encryption for documents among the clients those can get it, also shows encryption may be used to attain coarse-grained control.

R. A. Popa et al. [7] introduces the idea about multi-key searchable encryption which permits a client to give an absolute pivotal word for documents encrypted with separate keys. The objective of the multi-key searchable encryption is to guarantee that the cloud server can perform pivotal word scan on documents with one trapdoor for separate documents.

III. PROPOSED SYSTEM

A. Problem Statement

The aim of this project is to design a searchable encryption scheme using key-aggregation. In this scheme, a set of encrypted files can be shared with a single aggregate key. Also, this scheme helps in searching the keywords from any set of documents with a single trapdoor for the entire set of files stored in the cloud. Searchable encryption using key aggregation helps in reducing the overhead of generating and sharing large number of keys one for each document.

B. System Architecture

The architecture diagram shown in fig. contains both the data owner and a data retriever who are participating in the system. Also it shows the data uploading on the cloud, key exchange between the users and the submission of the trapdoor.

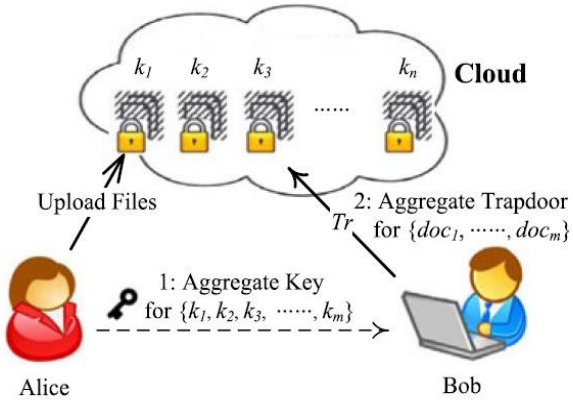

Fig System architecture

The one who is uploading the data is the data owner and the one who is retrieving the data is the user. One of the user stores the files into the cloud which are encoded by the asymmetric key encryption method to achieve security. The files are then uploaded in the cloud. The aggregate key for these sets of files that are uploaded is generated with the use of the private key and is delegated to the user by secure emails. Trapdoor is generated for these files with an aggregate key and the keyword that is used to carry out the search on entire set of files. At last, the file searched is decrypted with the secret key of the user. The searchable encryption with key aggregation framework consists of the following steps that constitute the model in detail are as follows:

•To start with, the cloud admin must activate the user to allow him to store the information on the cloud by updating his status as active. This

algorithm can be used commonly for all the users to update their status.

•Users who store the data on cloud, must generate a pair of public and secret keys with the Keygen algorithm.

•Encrypt algorithm is used to encrypt the keywords of each document by the key that is used as searchable encryption key.

• User who uploads the data can use the private key to produce an aggregate searchable encryption key for a set of selected files with the Extract algorithm.

•Aggregate key is shared with the users who have the rights to use those files. Later, as shown in the figure user can generate a keyword trapdoor with the Trapdoor algorithm which makes use of the aggregate key, and send it to the cloud.

•Once the trapdoor is received by the cloud, it performs a search for the keyword over a set of documents, then the adjust algorithm is run by the cloud server to produce the correct trapdoor for each document, later the test algorithm is executed to check whether the keyword is present in the document.

C. Basic Searchable Encryption Technique

Searchable encryption mainly has two different techniques, symmetric searchable encryption, and the one which allows searching keyword along with public key encryption. Both of these techniques can be explained in similar way with a set of algorithms as in the basic technique.

•Setup: It is the initial step in the scheme through which the users are assigned some features that allows them to store their files on the cloud.

•Encrypt: Once the user is allowed to store their files on the cloud, he makes use of this algorithm to scramble the information and produce its pivotal word cipher texts. It takes the number of documents and some of the essential keys to produce the information cipher text also pivotal word cipher texts.

•Trpdr: This calculation will be run by the client who produces a trapdoor for a file making use of some keys.

•Test: To carry out a search for file with the keyword, test is performed by the server on the entire set of documents. With the trapdoor and the pivotal word cipher texts, outputs if it holds those specified pivotal word.

D. Algorithms Involved in Searchable Encryption with Key Aggregation

Searchable encryption using key-aggregate concept contains seven polynomial algorithms which are explained as follows:

• Setup: This algorithm may be executed by the cloud administration supplier to start up the plan. With respect to entry of a security parameter and the greater amount of files n from claiming documents which belongs to an information owner, it outputs general framework parameter.

• Keygen: A key pair with arbitrary combination is generated for each of them who is using the services by this algorithm.

• Encrypt: Before storing the files on the cloud, they must be made secure by scrambling the information and also the words must encoded. This is done by the user using encryption algorithm. With the information about the user keys, it produces the cipher text for files.

• Extract: This algorithm may be run by the information manager to produce an aggregate searchable encryption key to hand over the pivotal word scan for a specific set of documents. Private key and list of documents is given to this algorithm which produces an aggregate key for those files.

• Trapdoor: To carry out the search on all files an aggregate key is required. This is executed by the client who needs the aggregate key to perform a scan. The key generated in the previous step and the words extracted from the files are given as input to produce the trapdoor.

• Adjust: The trapdoor generated in the previous step is for the entire set of documents. This must be set for individual files, which can be done based on the general parameters and the index given for files.

• Test: In order to carry out the pivotal word search over the complete set of documents by the server, some information like trapdoor and record list must be given. After the search is performed, the outcome will be given to indicate whether the word is found in the files.

E. Modules Description

•Data owner: Data owner is the one who stores files on to the cloud. He is allowed to store his files once he is registered with the system and with the generation of public parameters.

•Cloud storage: The cloud will generate some public parameters that can be used by the users and store files on the cloud. Other operations like generating the right trapdoor are done in the cloud environment.

•Aggregate key transfer: An aggregate key is generated by selecting the files that are uploaded. This key is shared with the data retriever through secure email.

•Trapdoor generation: A trapdoor is generated by consuming the aggregate key and the keyword. With the adjust algorithm right trapdoor is generated for each file.

•File user: Once the trapdoor is delivered to the cloud, search over the documents is performed and the file containing the keyword is retrieved, it is then decrypted with the private key of the user and can be downloaded.

IV. CONCLUSIONS

The implementation of searchable encryption with key-aggregation is been achieved by designing an efficient scheme. The sharing of group of files to different users though public cloud that needs generation of huge number of keys is managed and shared securely through emails. In this scheme, data owner needs to produce a single aggregate key for sharing a group of documents and the user needs to deliver a single trapdoor to the cloud to search over the entire set of documents and for downloading the documents. This work can be extended to reduce the number of trapdoors under the multi-owner participation as a future work.

REFERENCES

[1] S.Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc.IEEE Conf. Comput. Commun., 2010.
[2] X.Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure multi-owner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst.
[3] C.K. Chu, S. Chow, W. G. Tzeng, J. Y. Zhou, and R. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," IEEE Trans. Parallel Distribution Systems.
[4] F.Zhao, T. Nishide, and K. Sakurai, "Multi-user keyword search scheme for secure data sharing with fine-grained access control," in Proc. Int. Conf. Inf. Security Cryptol., 2012, pp. 406–418.
[5] X.Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Privacy, 2000, pp. 44–55.
[6] Z.L. Liu, Z. Wang, X. C. Cheng, and , C. F. Jia, K. Yuan, "Multiuser searchable encryption with coarser-grained access control in hybrid cloud," in Proc. 4th Int. Conf. Emerging Intell. Data Web Technol., 2013, pp. 249–255.
[7] R.A. Popa and N. Zeldovich, "Multi-key searchable encryption," Cryptol. ePrint Archive, Rep. 2013/508, 2013.
[8] R.Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security,2010, pp. 282–292.
[9] R.Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 79–88.
[10] P.Van, S. Sedghi, and J. M. Doumen, "Computationally efficient searchable symmetric encryption," in Proc. 7th VLDB Conf. Secure Data Manage., 2010, pp. 87–100.
[11] S.Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in Proc. ACM Conf. Comput. Commun. Security, 2012, pp. 965–976.
[12] D.Boneh, C. G, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn., 2004, pp. 506–522.
[13] Y.Hwang and P. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Proc. Int. Conf. Pairing-Based Cryptograph. C Pairing, 2007, pp. 2–22.