International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Secure Data Sharing In Distributed Cloud Storage Using a Novel Searchable Encryption

[1] T. Muneiah, [2] D. K. Shareef
[1]M.Tech Student, Department of Computer Science and Engineering, ALITS Engineering College, Affiliated to JNTUA, Andhra Pradesh, India
[2]Assistant Professor, Department of Computer Science and Engineering, ALITS Engineering College, Affiliated to JNTUA, Andhra Pradesh, India

ABSTRACT

Cloud computing is cutting-edge technology greatly serving consumer oriented applications. It has the abilities of sharing selective encrypted knowledge by way of public cloud storage with a couple of customers which may alleviate protection over unintended information leaks in the cloud. Efficient key management is fundamental in encryption schemes. For sharing various records with one-of-a-kind organizations in cloud, separate encryption keys are required. Protection is required by way of owner to distribute large number of keys for encryption and shopping, and with the aid of users to store received keys. Users ought to put up equal number of trapdoors to the cloud for search operation. In such case elements of security, storage and complexity are required at its best performance. In this paper we addressed the quandary of comfy information sharing method in cloud storage and studied special searchable encryption systems with multi-user and multi-key schemes with aggregation of a couple of attributes to minimize storage complexity and give a boost to effectivity of search over shared data. A mannequin for Key-aggregate Searchable Encryption(KASE) scheme is proposed, wherein an information owner handiest necessitate to distribute a single key to a person for sharing a significant number of records, and the person best desires to put up a single trapdoor to the cloud for querying the shared documents.

Keywords : Searchable Encryption, Information Sharing, Cloud Storage, Knowledge Privateness.

I. INTRODUCTION

Cloud computing is contemporary development in IT infrastructure which makes it possible for companies to devour assets of computing as a utility and arrange knowledge storage model which maintains data available and to be had for shared pool of configurable devices on-demand with coherence environment, low price and least administration efforts. Nonetheless gigantic data sharing results in advertent information confidentiality issues. Many safety schemes are generated in opposition to capabilities information leaks from which encryption is usual strategy. In cryptographic cloud storage, knowledge owner before uploading documents encrypts them such that best the character with decryption key can retrieve shared documents. This strategy becomes impractical for key administration and comfy storage to enforce with tremendous scale cloud applications. Moreover looking and retrieving selective data from huge number of encrypted records is intricate for user. Searchable Encryption (SE) is resolution for this obstacle in which owner encrypts key phrases and uploads it along side encrypted information in order that person can retrieve shared knowledge with the help of supplying key phrase trapdoor to cloud.

To scale back complexity of broaden in quantity of trapdoors proportional to number of records shared, Multi-key SE scheme is provided. So that single trapdoor is supplied via client and server will get potential to seek for that trapdoor's key phrase in shared files even their encryption keys are uncommon. Extra to scale down wide variety of encryption keys a idea of Key combination Encryption is presented which flexibility to decrypt any number of cipher text with constant-size decryption key.
In this paper, we tackle this mission through proposing the radical notion of key-aggregate searchable

encryption (KASE), and instantiating the idea via a concrete KASE scheme. The proposed KASE scheme applies to any cloud storage that helps the search-capable workforce information sharing functionality; this means that any person may selectively share a group of selected files with a group of chosen customers, even as allowing the latter to participate in keyword search over the former. To support searchable group knowledge sharing the primary necessities for effective key management are twofold.

II. Related Work

A. D. Boneh, G. Di Crescenzo, R. Ostrovskyy and G. Persianoz, "Public Key Encryption with key phrase Search", 2004: in this paper the trouble in public cloud process to seek for encrypted knowledge through encryption secrets examined. Key phrase as search query for e mail gateway is first of all introduced. Without learning contents of shared information gateway can seek for unique key phrase and verify qualified report to route record thus. This PEKS scheme may additionally enable server to determine all publicly encrypted documents of owner through one-of-a-kind customers containing the same key phrase given through owner without decryption of know-how. Gateway analysis is carried out to examine encrypted key words of sender and phrase of receiver's option, no extra expertise is learned with the support of the gateway. PEKS process implies identity founded Encryption (IDE) scheme the position owner encrypts data such that person having required attributes can most mighty decrypt the shared document. This method regarded most powerful single proprietor and consumer drawback for performing key phrase search over a few shared records.

B. R. Curtmola, J. Garay, S. Kamara and R. Ostrovsky,

"Searchable Symmetric Encryption: increased Definitions and efficient Constructions", 2006: The main issue of SSC scheme used for single consumer i.e. Proprietor is viewed on this paper. In prior process handiest the owner of data might post search queries and perform search over encrypted knowledge outsourced to other occasion. The construction on this paper accelerated the work of searchable symmetric encryption to be used for multi-consumer environment, where browsing can also be performed by means of arbitrary team of parties instead of most effective owner. Reverse to the prior method which certain defense for customers performing all searches without delay, this scheme ensured security constraints for any variety of useful searches through exact customers. Two SSE constructions are introduced as 1. Non-Adaptive cozy development (SSE-1) 2. An Adaptively cozy development (SSE-2). Multiple secure browsing is finished via SSC-2 where search queries are viewed as perform of earlier got search outcome and trapdoors. In each constructions the work performed by using server is constant with admire to dimension of information over each and every lower back report.

C. F. Zhao, T. Nishide, and ok. Sakurai, "Multi-consumer key phrase Search Scheme for secure data Sharing with fine-Grained entry manipulate", 2012: looking all keyword index in cloud storage to compare with given keyword and decrypt them just isn't nearly possible. Narrowing the scope of search results to patron's decrypt able file's staff using Attribute based Encryption (ABE) and CP-ABE to curb understanding leakage and lower looking complexity in multi-person cryptographic cloud storage environment is presented on this paper. This strategy is pleasant search for related files which person can decrypt and so is more efficient. The flexibleness of specifying the entry rights for individual shoppers in case of person revocation is furnished referred to as satisfactory grained access control. The Cipher text-coverage Attribute situated Encryption (CP-ABE) and Attribute established Signature (ABS) entry structure computation are used for offering differential entry rights.

D. Z. Liu, Z. Wang, X. Cheng, C. Jia and Ke Yuan, "Multi-consumer Searchable Encryption with Coarser-of keys to the consumer. The complexity and protection aspects Grained access manipulates in Hybrid Cloud", 2013:

The complexity of maintaining colossal authentication information for dynamic insertion and doing away with of purchasers in pleasant grained access manipulate scheme is resolved in this paper. Two schemes: 1. Identification centered Broadcast encryption (IBBE) for simplified entry manage by way of utilizing single random worth for addition or revocation of customers and management of keys and a pair of. SUSE scheme for comfy two part operation without private cloud or relied on centre via utilizing Pseudo Random Permutation (PRP) function, presents practical

implementation of MUSE system. Two section operations is implemented for encryption of keyword phrases and generating trapdoors. BE scheme immediately indicate security for re-encrypted trapdoor and symmetric key, and SUSE scheme ensures safety of keyword cipher text and encrypted files. This procedure is efficient in opposition to 1. Outside adversaries as relied on centre best respond to recognize customers by using Coarser-Grained access manipulate and a couple of. Inside adversaries as PRFs of SSC scheme is provably at ease

III. EXISTING SYSTEM

Believe that client 1 uploads all her private photographs and videos on Drop box, and she does not need to see her portraits by way of each person. Due to various information leakages in cloud there is also probability that patron 1 cannot consider satisfied with the aid of just counting on the privateness security offered via Drop box, so she encrypts all the photos utilising her possess keys before uploading. Someday, patron 1's friend, say customer 2, asks her to share her pics taken for the period of all these years which consumer 2 appeared in. Purchaser 1 then uses the percentage perform of Drop box, but the difficulty is methods to delegate the decryption rights for these pix to patron 2. A possible option client 1 can pick is to safely send patron 2 the secret keys included .Therefore there are two ways for her under the usual encryption paradigm:

1) Purchaser 1 encrypts all documents with a single encryption key and gives purchaser 2 the corresponding secret key straight. 2) Client 1encrypts files with special keys and sends patron 2 the corresponding secret keys undoubtedly, the primary method is inadequate because all data which is not but chosen could also be additionally leaked to client 2. For the second procedure, there are sensible issues on effectivity. The number of keys is similar to the quantity of the shared images, say, a thousand. Sending these secret keys requires a more secure channel, and storage of those keys requires pricey relaxed storage. The cost and complexities included traditionally rise with the quantity of the decryption keys to be shared. Briefly, it is a lot heavy and highly-priced to do.

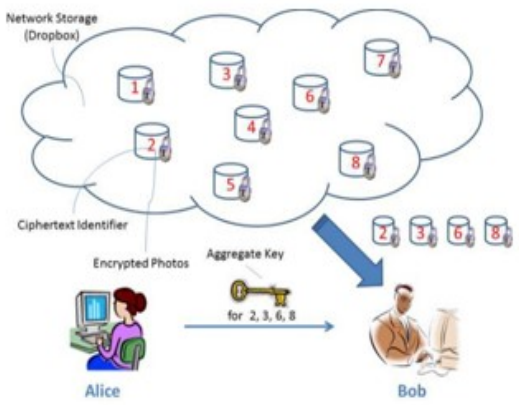

Figure 1: Network Storage (drop box)

IV. PROPOSED SYSTEM

On this paper, we deal with this task by the use of proposing the radical proposal of key-aggregate searchable encryption (KASE), and instantiating the advice by way of a concrete KASE scheme.
The proposed KASE scheme applies to any cloud storage that helps the searchable crew data sharing efficiency, which means that any client may just selectively share a bunch of chosen records with a gaggle of chosen customers, at the same time enabling the latter to participate in keyword search over the previous.

To preserve searchable cluster data sharing the primary requisites for effective key administration are twofold. First, an information proprietor effectively requires distributing a single combination key (as an alternative of a group of keys) to a person for sharing any wide variety of documents. 2d, the consumer best wishes to post a single aggregate trapdoor (as a substitute of a group of trapdoors) to the cloud for performing keyword search over any number of shared files. We first classify a long-established framework of key mixture searchable encryption (KASE) composed of seven polynomial algorithms for defense parameter setup, key generation, encryption, key extraction, and trap door new unlock, trapdoor adjustment, and trapdoor checking out. We then illustrate each and every priceless and security requirements for designing a authentic KASE scheme.

We then instantiate the KASE framework by means of designing a concrete KASE scheme. After supplying exact constructions for the seven algorithms, we analyse the efficiency of the scheme, and set up its defense through certain analysis.

SYSTEM ARCHITECTURE

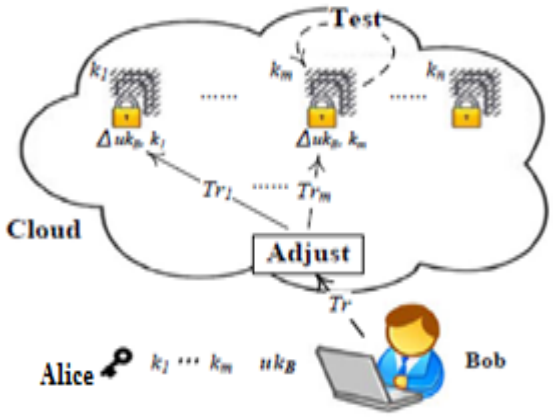

Figure 2 : Framework of key-aggregate searchable encryption

V. IMPLEMENTATION

Data Owner:

In this module we did through the information owner to setup an account on an untrusted server. On input a safeguard stage parameter 1λ and the number of cipher text courses n (i.e., class index will have to be an integer bounded through 1 and n), it outputs most people process parameter param, which is neglected from the center of the reverse algorithms for brevity.

Network Storage (Drop box):

With our decision, Alice can comfortably ship Bob a single combination key via a comfy email. Bob can down load the encrypted photographs from Alice's Drop box field and then use this combination key to decrypt these encrypted photos. On this neighborhood Storage is untrusted 1/3 social gathering server or drop box.

Encrypted Aggregate Key and Searchable Encrypted key Transfer:

The information proprietor establishes the public system parameter by means of Setup and generates a public/grasp-secret key pair via KeyGen. Messages may even be encrypted by way of Encrypt with the help of anyone who additionally decides what cipher text category is related to the simple textual content message to be encrypted. The knowledge proprietor can use the master-secret to generate an combo decryption key for a collection of cipher text guides through Extract. The generated keys may also be exceeded to delegates securely (via secure e-mails or cozy instruments) eventually; any purchaser with an combination key can decrypt any cipher text furnished that the cipher texts class is contained inside the combo key via Decrypt.

Trapdoor generation:

Trapdoor iteration algorithm is run through the character that has the combination key to perform a search. It takes as enter the combination searchable encryption key keg and a key phrase w, then outputs just one trapdoor Tr.

File User:

The generated keys can also be passed to delegates securely (through comfortable e-mails or at ease devices) ultimately; any consumer with the Trapdoor keyword generation procedure can decrypt any cipher text supplied that the cipher texts class is contained within the Encrypted mixture key and Searchable Encrypted key by way of Decrypt.

VI. CONCLUSION

A suggestion of key-combination searchable encryption (KASE) and assemble a concrete KASE scheme is proposed , each evaluation and evaluation results verify that our work can furnish an potent procedure to constructing useful knowledge sharing method based on public cloud storage. In a KASE scheme, the proprietor only desires to allocate a single key to a character when sharing plenty of records with the consumer and the customer needs to put up a single trapdoor when he queries over all documents shared via the equal proprietor. However, if a character wants to query over files shared through a couple of householders, he need to generate a couple of trapdoors to the cloud. How to cut back the wide variety of trapdoors under multi-condominium house owners surroundings, Multi-proprietor report sharing by the use of single trapdoor may also be future work.

VII. REFERENCES

[1]. M. Bellare, S. Keelveedhi, and T. Ristenpart. Dupless: Serveraided encryption for deduplicated storage. In USENIX Security Symposium, 2013.

[2]. M. Bellare, S. Keelveedhi, and T. Ristenpart. Message-locked encryption and secure deduplication. In EUROCRYPT, pages 296-312, 2013.

[3]. M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. J. Cryptology,22(1):1-61, 2009.

[4]. M. Bellare and A. Palacio. Gq and schnorr identification schemes:Proofs of security against impersonation under active and concurrent attacks. In CRYPTO, pages 162-177, 2002.

[5]. S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider. Twin clouds: An architecture for secure cloud computing. In Workshop on Cryptography and Security in Clouds (WCSC 2011), 2011.

[6]. J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer. Reclaiming space from duplicate files in a serverless distributed file system. In ICDCS, pages 617-624, 2002.

[7]. D. Ferraiolo and R. Kuhn. Role-based access controls. In 15th NIST-NCSC National Computer Security Conf., 1992.

[8]. J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou. Secure deduplication with efficient and reliable convergent key management. In IEEE Transactions on Parallel and Distributed Systems, 2013.