ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A New Framework to Address the Security Vulnerability of PEKS

K.Chandrakala[1], P.Gangadhara[2]

M.Tech, Dept of CSE, Shri Shirdi Sai Institute of Science and Engineering, Affiliated to JNTUA, Ananthapuramu, AP, India [1]

Assistant Professor, Dept of CSE, Shri Shirdi Sai Institute of Science and Engineering, Affiliated to JNTUA, Ananthapuramu, AP, India. [2]

ABSTRACT: Cloud computing is latest technology widely serving client oriented applications. It has the potential of sharing selective encrypted data via public cloud storage with multiple users which may alleviate security over accidental data leaks in the cloud. Efficient key management is important in encryption schemes. For sharing various documents with different groups in cloud, separate encryption keys are required. Security is required by owner to distribute large number of keys for encryption and searching, and by users to store received keys. Users have to submit equal number of trapdoors to the cloud for search operation. In such case features of security, storage and complexity are required at its best performance. In this paper we addressed the problem of secure data sharing system in cloud storage and studied different searchable encryption techniques with multi-user and multi-key schemes with aggregation of multiple attributes to reduce storage complexity and improve efficiency of search over shared data. A model for Key-Aggregate Searchable Encryption scheme is proposed, in which a data owner only necessitate to distribute a single key to a user for sharing a huge quantity of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents.

KEYWORDS: Searchable Encryption, Data Sharing, Cloud Storage, Data Privacy.

I. INTRODUCTION

Cloud computing is recent trend in IT infrastructure which enables organizations to consume resources of computing as a utility and organize data storage model which keeps data accessible and available for shared pool of configurable devices on-demand with coherence environment, low cost and least management efforts. However large data sharing leads to advertent data confidentiality problems. Many security schemes are generated against potential data leaks from which encryption is common approach. In cryptographic cloud storage, data owner before uploading files encrypts them such that only the person with decryption key can retrieve shared documents. This approach becomes impractical for key management and secure storage to implement with large scale cloud applications. Additionally looking and retrieving selective data from large number of encrypted documents is difficult for user. Searchable Encryption (SE) is resolution for this problem wherein owner encrypts keywords and uploads it together with encrypted data so that user can retrieve shared information with the aid of providing keyword trapdoor to cloud.

To shrink complexity of increase in number of trapdoors proportional to quantity of documents shared, Multi-key SE scheme is offered. So that single trapdoor is provided via consumer and server will get capacity to seek for that trapdoor's keyword in shared records even their encryption keys are extraordinary. Additional to lower quantity of encryption keys a concept of Key combination Encryption is introduced which flexibility to decrypt any number of ciphertext with consistent-size decryption key.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

II. REALATED WORK

A. D. Boneh, G. Di Crescenzo, R. Ostrovskyy and G.
Persianoz, "Public Key Encryption with keyword Search", 2004: In this paper the problem in public cloud system to search for encrypted data through encryption key is examined. Keyword as search query for email gateway is firstly introduced. Without learning contents of shared data gateway can search for specific keyword and verify qualified document to route document accordingly. This PEKS scheme may additionally enable server to determine all publicly encrypted records of owner by way of different users containing the same key phrase given by owner without decryption of information. Gateway analysis is performed to check encrypted keywords of sender and word of receivers choice, no extra information is discovered with the aid of the gateway. PEKS method implies Identity based Encryption (IDE) scheme the place owner encrypts data such that person having required attributes can most effective decrypt the shared report. This procedure regarded most effective single owner and user situation for performing key phrase search over a couple of shared files.

B. R. Curtmola, J. Garay, S. Kamara and R. Ostrovsky,
"Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions", 2006: The problem of SSC scheme used for single user i.e. ower is considered in this paper. In prior system only the owner of data could submit search queries and perform search over encrypted data outsourced to other party. The construction in this paper extended the work of searchable symmetric encryption to be used for multi-user environment, where searching can be performed by arbitrary group of parties instead of only owner. Opposite to the prior system which assured protection for purchasers performing all searches without delay, this scheme ensured safety constraints for any quantity of useful searches by specific users. Two SSE constructions are introduced as 1. Non-Adaptive Secure Construction (SSE-1) 2. An Adaptively Secure Construction (SSE-2). Multiple secure searching is achieved through SSC-2 where search queries are considered as function of previously obtained search results and trapdoors. In both constructions the work performed by server is constant with respect to size of data over each returned document.

C. F. Zhao, T. Nishide, and K. Sakurai, "Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control", 2012: Searching all keyword index in cloud storage to match with given keyword and decrypt them is not practically feasible. Narrowing the scope of search results to consumer's decryptable file's workforce using Attribute based Encryption (ABE) and CP-ABE to minimize understanding leakage and shrink browsing complexity in multi-user cryptographic cloud storage environment is presented in this paper. This approach is best search for related files which user can decrypt and so is more efficient. The pliability of specifying the entry rights for man or woman customers in case of user revocation is provided known as fine grained access control. The Ciphertext-policy Attribute based Encryption (CP-ABE) and Attribute based Signature (ABS) access constitution computation are used for providing differential access rights.

D. Z. Liu, Z. Wang, X. Cheng, C. Jia and Ke Yuan, "Multi-user Searchable Encryption with Coarser- of keys to the user. The complexity and security aspectsGrained Access Control in Hybrid Cloud", 2013:

The complexity of maintaining enormous authentication information for dynamic insertion and removing of customers in fine grained access control scheme is resolved in this paper. Two schemes: 1. Identification based Broadcast encryption (IBBE) for simplified access manage by way of using single random worth for addition or revocation of customers and management of keys and 2. SUSE scheme for secure two section operation without private cloud or trusted centre by making use of Pseudo Random Permutation (PRP) operate, offers functional implementation of MUSE procedure. Two segment operation is carried out for encryption of key words and generating trapdoors. BE scheme directly imply security for re-encrypted trapdoor and symmetric key, and SUSE scheme ensures security of keyword ciphertext and encrypted files. This system is efficient against 1. External adversaries as trusted centre only respond to identified users by Coarser-Grained Access Control and 2. Internal adversaries as PRFs of SSC scheme is provably secure.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

III. EXISTING SYSTEM

Suppose that Client 1 uploads all her private pictures and videos on Dropbox, and she does not want to see her photos by everyone. Due to various data leakages in cloud there may be possibility that client 1 cannot feel satisfied by just relying on the privacy protection provided by Dropbox, so she encrypts all the pictures using her own keys before uploading. One day, Client 1's friend,say client 2, asks her to share her pictures taken during all these years which client 2 appeared in. client 1 then uses the share function of Dropbox, but the problem is how to delegate the decryption rights for these pictures to client 2. A possible option client 1 can choose is to securely send client 2 the secret keys included .Therefore there are two ways for her under the traditional encryption paradigm:

1)client 1 encrypts all files with a single encryption key and gives client 2 the corresponding secret key directly. 2)client 1encrypts files with distinct keys and sends client 2 the corresponding secret keys surely, the first technique is inadequate since all data which is not yet choosen may be also leaked to client 2. For the second method, there are practical concerns on efficiency. The number of keys is equivalent to the number of the shared photos, say, a thousand. Sending these secret keys requires a more secure channel, and storage of these keys requires expensive secure storage. The cost and complexities included generally rise with the number of the decryption keys to be shared. In short, it is much heavy and costly to do.

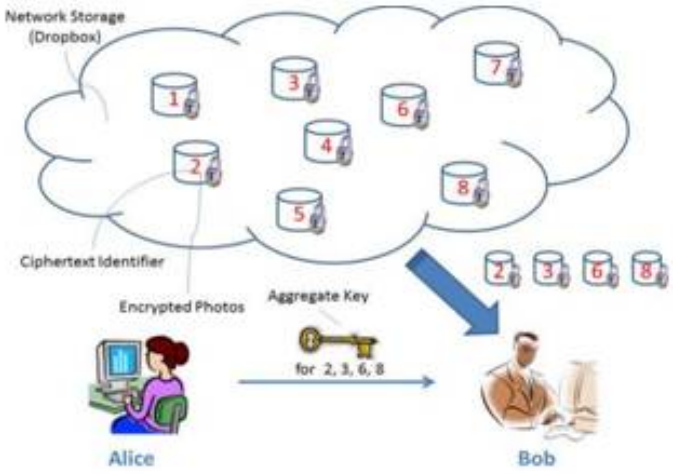

Fig 1: Network Storage (drop box)

IV. PROPOSED SYSTEM

In this paper, we address this undertaking by means of proposing the novel proposal of key-aggregate searchable encryption, and instantiating the suggestion by way of a concrete scheme.
The proposed scheme applies to any cloud storage that helps the searchable crew data sharing performance, which means any consumer may just selectively share a bunch of chosen documents with a group of chosen users, whilst allowing the latter to participate in keyword search over the former.
To sustain searchable cluster data sharing the foremost necessities for efficient key management are twofold.. First, a data owner simply requires to distribute a single aggregate key (instead of a group of keys) to a user for sharing any quantity of files. Second, the user only needs to submit a single aggregate trapdoor (instead of a group of trapdoors) to the cloud for performing keyword search over any number of shared files. We first classify a common framework of key aggregate searchable encryption composed of seven polynomial algorithms for safety parameter setup, key generation, encryption, key extraction, trapdoor new release, trapdoor adjustment, and trapdoor checking out. We then illustrate each useful and protection requirements for designing a legitimate scheme.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

We then instantiate the framework through designing a concrete scheme. After offering targeted constructions for the seven algorithms, we analyse the efficiency of the scheme, and establish its protection through designated analysis.

SYSTEM ARCHITECTURE

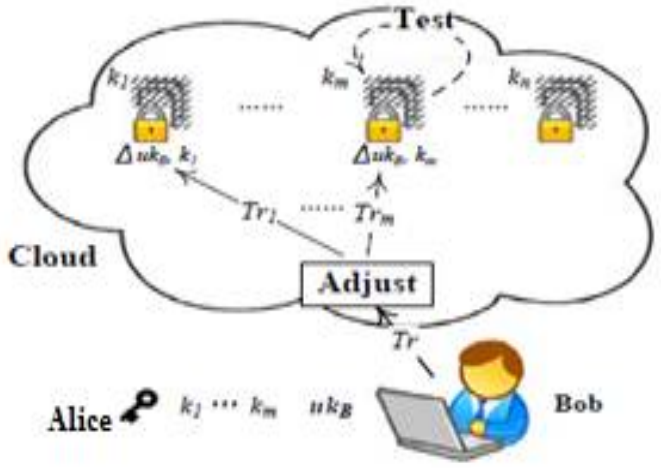

Fig1:Framework of key-aggregate searchable encryption.

V. IMPLEMENTATION

Data Owner:

In this module we executed through the data owner to setup an account on an untrusted server. On input a safety stage parameter 1λ and the number of ciphertext classes n (i.e., category index will have to be an integer bounded via 1 and n), it outputs the general public procedure parameter param, which is omitted from the enter of the opposite algorithms for brevity.

Network Storage (Drop box):

With our resolution, Alice can simply ship Bob a single combination key through a relaxed e-mail. Bob can down load the encrypted images from Alice's Dropbox area and then use this mixture key to decrypt these encrypted snap shots. On this community Storage is untrusted third celebration server or dropbox.

Encrypted Aggregate Key and Searchable Encrypted key Transfer:

The Data owner establishes the public procedure parameter through Setup and generates a public/master-secret key pair via KeyGen. Messages will also be encrypted through Encrypt with the aid of anyone who additionally decides what ciphertext class is associated with the plain text message to be encrypted. The information owner can use the master-secret to generate an combination decryption key for a collection of ciphertext courses by way of Extract. The generated keys can also be handed to delegates securely (through comfy e-mails or comfy instruments) sooner or later; any consumer with an mixture key can decrypt any ciphertext provided that the ciphertexts class is contained within the mixture key via Decrypt.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Trapdoor generation:

Trapdoor generation algorithm is run via the person who has the mixture key to perform a search. It takes as input the aggregate searchable encryption key kagg and a key phrase w, then outputs only 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 ciphertext supplied that the ciphertexts class is contained within the Encrypted mixture key and Searchable Encrypted key by way of Decrypt.

VI. CONCLUSION

A concept of key-aggregate searchable encryption scheme is proposed , both analysis and analysis results verify that our work can provide an robust method to building practical information sharing method based on public cloud storage. In this scheme, the owner only needs to allocate a single key to a person when sharing lots of files with the user, and the consumer wishes to submit a single trapdoor when he queries over all records shared by way of the identical owner. Nevertheless, if a person needs to query over records shared by way of a couple of homeowners, he ought to generate multiple trapdoors to the cloud. The way to shrink the quantity of trapdoors below multi-house owners surroundings, Multi-proprietor report sharing by means of single trapdoor can be future work.

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.