IMPROVING SECURITY FOR PROTECTING DATA PRIVACY IN SECURE SEARCHABLE CLOUD STORAGE

[1]B. SWAPNA, [2]SUJANA DAYAM

[1]M. Tech,Computer Science & Engineering, Bhaskar Engineering College,Hyderabad.

[2]Assistant Professor,Computer Science & Engineering,Bhaskar Engineering College,Hyderabad.

ABSTRACT— ***Now a day's there will be growing reputation of cloud computing, huge range of customers and statistics owners are influenced to outsource their facts to cloud servers for massive convenience and decreased cost required for information management. However, important facts ought to be encrypted earlier than outsourcing for privacy requirements, which uses records usage technique like keyword-primarily based record retrieval. Searchable encryption is of increasing enthusiasm for making sure the data protection in at ease searchable distributed garage. In this paper, we studies the safety of an outstanding cryptographic primitive, particularly, Public Key Encryption with Keyword Search (PEKS) that's quite valuable in several utilizations of cloud storage. The traditional PEKS structure reports an inalienable instability known as interior Brute Force keyword guessing attack propelled through the pernicious server. To address this security vulnerability, we recommend any other PEKS system named Dual Server PEKS (DS-PEKS). Through this propose system, we can improve the security for cloud storage systems.***

Keywords: Public Key Encryption, Cryptography, Keyword Guessing Attacks

1. INTRODUCTION

Cryptography is the practice of transforming data to make it indecipherable by a third party, unless a particular piece of secret information is made available to them. Many different forms of cryptographic algorithms exist, each designed for a different purpose. An alternative is public-key cryptography, which is typically used to send messages to other people.

Today's mail servers such as IMAP servers, file servers and other data storage servers typically must be fully trusted—they have access to the data, and hence must be trusted not to reveal it without authorization—which introduces undesirable security and privacy risks in applications. Previous work shows how to build encrypted file systems and secure mail servers, but typically one must sacrifice functionality to ensure security. The basic crisis is that moving the computation to the data storage looks too difficult when the data is encrypted, as well as many computation problems over encrypted data previously had no practical solutions.

With the fast improvement of distributed computing and portable systems administration innovations, clients tend to get to their put away information from the remote distributed storage with cell phones. The fundamental favorable position of distributed storage is its pervasive client availability furthermore it's for all intents and purposes boundless information stockpiling capacities. Notwithstanding such advantages gave by the cloud, the real test that remaining parts is the worry over the secrecy and protection of information while embracing the distributed storage administrations. For example, decoded client information put away at the remote cloud server can be defenseless against outer assaults started by unapproved outcasts and inside assaults started by the dishonest cloud service provider (CSPs) organizations. There are a few reports that affirm information breaks identified with cloud servers, because of malignant assault, burglary or inward mistakes. This raises sympathy information may contain extremely delicate individual association/data. Distributed cloud storage outsourcing has become outstanding software for undertakings and institutions to reduce the burden of keeping up big information recently. No withstanding, in all reality, cease clients won't with the aid of any approach consider the cloud ability servers and can want to scramble their information some time lately moving them to the cloud server with a particular cease aim to comfortable the statistics safety. This normally makes the statistics utilization tougher than the traditional storage where statistics is kept within the nonappearance of encryption. One of the average arrangements is the searchable encryption which lets in the patron to recover the scrambled records that comprise the purchaser indicated catchphrases, wherein given the watchword trapdoor, the server can discover the information required by the client with none problem.

2. RELATED WORK

R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky revisited the problem of searchable symmetric encryption, which allows a customer to store its statistics on a faraway server in one of this way that it may seek over it in a private manner. We make numerous contributions which include new safety definitions and new structures. Motivated by using subtle problems in all previous security definitions for SSE, we advocate new definitions and point out that the existing notions have sizable sensible drawbacks: contrary to the natural use of searchable encryption, they best guarantee security for customers that carry out all their searches right away. We address this problem through introducing stronger definitions that guarantee protection even if users carry out extra practical searches. We also advise two new SSE structures. Surprisingly, regardless of being provably secure below this stronger safety definitions, these are the most efficient schemes up to now and are (asymptotically) foremost (i.e., the design carried out by using the server in step with again report is steady within the size of the facts).

The foremost purpose of Dalia Khader studies become to have a PEKS this is at ease beneath a preferred version in place of the random oracle model best. To accomplish that, step one turned into finding an IBE scheme that has key privacy notions. Use of IBE with Weil pairing to build a PEKS become demonstrated and the scheme become comfy under a delegated keyword assault but beneath the random oracle most effective. The IBE cautioned by Boneh and Boyenin additionally turned into no longer useful in building a PEKS as proven. It was tempting to try to show the K-resilient IBE to have a belief of key privacy because it turned into shown that the Cramer-Shoup encryption is comfortable. The KRIBE followed a variety of strategies from this encryption scheme and KRIBE changed into

proved to be at ease. The new PEKS scheme changed into then used to assemble a public key encryption with conjunctive key-word search and a public key encryption that does not need a secure channel. However, the brand new PEKS scheme still has some drawbacks because of the constraints of the KRIBE scheme itself, in which the variety of malicious customers is limited to a few cost K. That is the range of trapdoors generated inside the PEKS is restrained to at most K. Nevertheless, that is not a severe trouble where we should use a reasonably big K for email looking programs.

J. Baek, R. Safavi-Naini, and W. Susilo mentioned three troubles associated with PEKS and proposed provably secure PEKS schemes that eliminate comfy channel and encrypt a couple of keywords efficiently. A thrilling open problem is to design a PEKS scheme based on a primitive aside from the BDH trouble.

3. FRAMEWORK

A. System Overview

Public Key Encryption with Keyword Search (PEKS) that enables a user to search encrypted data in the asymmetric encryption setting. In a PEKS system, using the receiver's public key, the sender attaches some encrypted keywords (referred to as PEKS cipher texts) with the encrypted data. The receiver then sends the trapdoor of a to-be-searched keyword to the server for data searching. Given the trapdoor and the PEKS cipher text, the server can test whether the keyword underlying the PEKS cipher text is equal to the one selected by the receiver. If so, the server sends the matching encrypted data to the receiver.

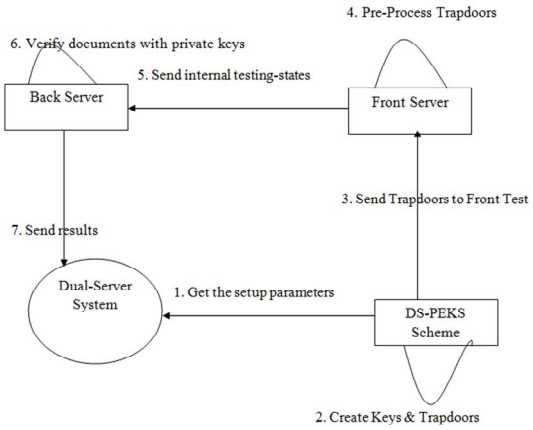

Fig1. DS-PEKS System work flow

DS-PEKS scheme mainly consists of (KeyGen, DS − PEKS, DS − Trapdoor, FrontTest, BackTest). To be more precise, the KeyGen algorithm generates the public/private key pairs of the front and back servers instead of that of the receiver. Moreover, the trapdoor generation algorithm DS − the algorithm Trapdoor takes as input the receiver's private key. Such a difference is due to the different structures used by the two systems. In the conventional PEKS, because there is best one server, if the trapdoor generation algorithm is public, then the server can release a guessing

attack against a keyword ciphertext to get better the encrypted key-word. However, beneath the DS-PEKS framework, we can nonetheless achieve semantic safety whilst the trapdoor generation algorithm is public. Another distinction among the traditional PEKS and our proposed DS-PEKS is that the take a look at set of rules is divided into two algorithms, FrontTest algorithm and BackTest algorithm run by independent servers. This is important for achieving safety in opposition to the internal keyword guessing attack.

B. Smooth Projective Hash Functions

Smooth Projective Hash Functions (SPHF) has been introduced by Cramer and Shoup under the name hash proof systems. An SPHF for a language *L* allows hashing a word *X*, in two different ways:

1. With some secret key (the hashing key, usually denoted *hk*)
2. With the associated public key (the projection key, usually denoted *hp*).

It must satisfy two properties:

- If the word is in the language, both ways of hashing will return the same hash value
- If the word is outside the language, the hash obtained with the secret key is statistically indistinguishable from random, even given the public key.

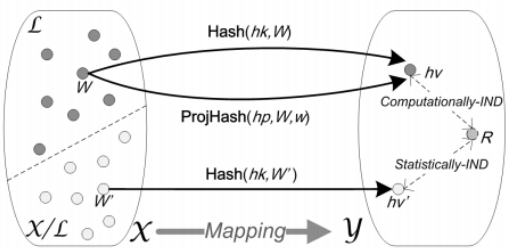

Fig2. Smooth Projective Hash Function

Intuitively, this will be used as a sort of specified-verifier zero-information evidence (although it does no longer fulfill the classical 0-knowledge property): to prove the word belongs to language (*X€L*), the prover receives the projection key *hp* from the verifier, and hashes the word with admire to language, using *hp*, and sends again the end result. The verifier contrasts it to the hash attained with the secret key as well as accepts the proof if both hashes are the identical.

C. Functions of Dual Server

In this proposed DS-PEKS scheme, we have two servers such as;

1. Front Server
2. Back Server

Front Server:

In the DS-PEKS scheme, after receiving the query from the receiver, the front server pre-processes the trapdoor and all the PEKS ciphertexts using its private key, and then sends some internal testing-states to the back server with the corresponding trapdoor and PEKS ciphertexts are hidden.

Back Server:

The back server can then decide which documents are queried by the receiver using its private key and the received internal testing-states from the front server.

4. CONCLUSION

In this paper we proposed a Dual-Server Public Key Encryption with Keyword Search (DS-PEKS) to prevent the inside keyword guessing attacks in cloud storage systems. The proposed framework improved the security vulnerabilities of the existing PEKS framework. And also we introduced Smooth Projective Hash Function to improve the DS-PEKS system efficiency.

REFERENCES

[1] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, “A new general framework for secure public key encryption with keyword search,” in Proc. 20th Australasian Conf. Inf. Secur. Privacy (ACISP), 2015,pp. 59–76.

[2] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEE Symp. Secur. Privacy, May 2000,pp. 44–55.

[3] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” in Proc. ACM SIGMOD Int. Conf. Manage.Data, 2004, pp. 563–574.

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” in Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS), 2006,pp. 79–88.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Publickey encryption with keyword search,” in Proc. Int. Conf. EUROCRYPT,2004, pp. 506–522.

[6] R. Gennaro and Y. Lindell, “A framework for password-based authenticated key exchange,” in Proc. Int. Conf. EUROCRYPT, 2003,pp. 524–543.

[7] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, “Building an encrypted and searchable audit log,” in Proc. NDSS, 2004, pp. 1–11.

[8] M. Abdalla et al., “Searchable encryption revisited: Consistencyproperties, relation to anonymous IBE, and extensions,” in Proc. 25thAnnu. Int. Conf. CRYPTO, 2005, pp. 205–222.

[9] D. Khader, “Public key encryption with keyword search based onK-resilient IBE,” in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA), 2006,pp. 298–308.

[10] P. Xu, H. Jin, Q. Wu, and W. Wang, “Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack,” IEEE Trans. Comput., vol. 62, no. 11, pp. 2266–2277,Nov. 2013.