Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

A Search Engine Tool for Query Processing On Encrypted Cloud

[1]R.Lalitha Padmini and [2]R.Bala Dinakar
[1]PG Student, [2]Assistant Professor,
[1,2]Department of computer Applications, Godavari Institute of Engineering and Technology, Rajahmundry, India

Abstract-- Searching of data from a cloud based server is most challenging task many research has been made in this area of retrieval of document using search keyword so one of the most important problem is storage and access of confidential documents form the centralized server most of the technique concentrate of keyword based search rather than improving the searching the technique so we in tis paper we implement a novel technique for searching the information of encrypted document using Bloom filter which give more efficiency in searching the Data and which also reduces the false alarm rating and also protects form attacks and also we analyses the false positive rate while framing of phrase key word

Keywords-- *Encryption, decryption, dual server encryption, cloud computing.*

I. INTRODUCTION

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 favourableposition of distributed storage is its pervasive clientability 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 defenceless 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 turned into a prominent application for undertakings and associations to lessen the weight of keeping up enormous information lately No withstanding, in all actuality, end clients may not by any means believe the cloud capacity servers and may want to scramble their information some time recently transferring them to the cloud server with a specific end goal to secure the information protection. This normally makes the information usage more troublesome than the conventional storage where information is kept in the nonappearance of encryption. One of the average arrangements is the searchable encryption which permits the client to recover the scrambled records that contain the client indicated catchphrases, where given the watchword trapdoor, the server can discover the information required by the client without any problem.

II. LITERATURE SURVEY

Cloud computing represents today's most exciting computing pattern shift in information technology. but, security and privacy are perceived as primary obstacles to its large adoption. Here, outline several critical security challenges and motivate further investigation of security solutions for a trustworthy public cloud environment. cloud computing is the latest concept for the long-dreamed vision of computing as a usefulness.It is necessary to store information on information storage servers such as mail servers and record servers in encoded frame to improve security and protection dangers. In any case, this typically suggests one needs to relinquish usefulness for security. For instance, if a customer wishes to recover just reports containing certain words, it was not beforehand known how to let the information stockpiling server play out the inquiry and answer the question without loss of information secrecy. the issue of seeking on information that is encoded utilizing a public open key framework. Consider client Bob who sends email to client Alice scrambled under Alice's open key. An email passage needs to test whether the email contains the watchword \urgent" with the goal that it could course the email as needs be. Alice, then again does not wish to give the door the capacity to unscramble every one of her messages. We done and develop an instrument that empowers Alice to give a key to the portal that empowers the door to test whether the word \urgent" is a watchword in the email without learning whatever else about the email. We allude to this system as Public Key Encryption with watchword Search. As another case, consider a mail server that stores different messages openly scrambled for Alice by others. Utilizing our instrument Alice can send the mail server a key that will empower the server to distinguish all messages containing some keyword which is we want to search.

The decent property in this plan permits the server to scan for a catchphrase, given the trapdoor. Thus, the verifier can just utilize an untrusted server, which makes this idea extremely down to earth. Taking after Byun et al. work, there have been ensuing works that have been proposed to upgrade this idea. Two vital ideas incorporate the supposed catchphrase speculating assault and secure channel free, proposed by Byun et al. what's more, Byun et al., separately. The previous understands the way that by and by, the space of the catchphrases utilized is extremely constrained, while the last considers the evacuation of secure channel between the beneficiary and the server to make PEKS down to earth. Lamentably, the current development of PEKS secure against catchphrase speculating assault is just secure under the irregular prophet display, which does not mirror its security in this present reality.

Moreover, there is no total definition that catches secure channel free PEKS plans that are secure against picked catchphrase assault, picked ciphertext assault, and against watchword speculating assaults, despite fact that these thoughts appear to be the most pragmatic use of PEKS primitives.

Another system, called secure server-assignment open key encryption with catchphrase seek (SPEKS), was acquainted with enhance the security of DPEKS (which experiences the on-line catchphrase speculating assault) by characterizing another security demonstrate 'unique ciphertext indistinguishability'.

III. RELATED WORK

Many of the early works focused on single keyword searches. Recently researchers have proposed solutions on conjunctive keyword search, which involves multiple keywords other interesting problems, such as the ranking of search results and searching with keywords that might contain errors fuzzy keyword search, have search for phrases was also been considered the ability to recently investigated some examined the security of the examined the security of the found, solutions were proposed. Single keyword searches are only possible Data access and retrieve ability is not efficient.

IV. PROPOSED SYSTEM

According to our experiment, it also achieves a lower storage cost than all existing solutions the solution addresses the high computational cost noted in by reformulating phrase search as n-gram verification rather than a location search or a sequential chain verification. Our approach is also the first to effectively allow phrase search to run independently without first performing a conjunctive keyword search to identify candidate documents. The proposed solution can also be adjusted to achieve maximum speed or high speed with a reasonable storage cost depending on the application. Multiple keyword search can also perform has been increased with the reasonable cost.

V. IMPLEMENTATION

A. Data Owner Module

This module helps the owner to register those details also include login details. This module helps the owner to upload his file with encryption using RSA algorithm. This ensures the files to be protected from unauthorized user. Data owner has a collection of documents F ={f1; f2:::; fn} that he wants to outsource to the cloud server in encrypted form while still keeping the capability to search on them for effective utilization. In our scheme, the data owner firstly builds a secure searchable tree index I from document collection F, and then generates an encrypted document collection C for F. Afterwards, the data owner outsources the encrypted collection C and the secure index I to the cloud server, and securely distributes the key information of trapdoor generation and document decryption to the authorized data users. Besides, the data owner is responsible for the update operation of his documents stored in the cloud server. While updating, the data owner generates the update information locally and sends it to the server.

B. Data User Module

This module includes the user registration login details. This module is used to help the client to search the file using the multiple key words concept and get the accurate result list based on the user query. The user is going to select the required file and register the user details and get activation code in mail email before entered the activation code. After user can download the Zip file and extract that file. Data users are authorized ones to access the documents of data owner. With t query keywords, the authorized user can generate a trapdoor TD according to search control mechanisms to fetch k encrypted documents from cloud server. Then, the data user can decrypt the documents with the shared secret key.

C. Cloud Server and Encryption Module

This module is used to help the server to encrypt the document using RSA Algorithm and to convert the encrypted document to the Zip file with activation code and then activation code-send to the user for download. Cloud server stores the encrypted document collection C and the encrypted searchable tree index I for data owner. Upon receiving the trapdoor TD from the data user, the cloud server executes search over the index tree I, and finally returns the corresponding collection of top- k ranked encrypted documents. Besides, upon receiving the update information from the data owner, the server needs to update the index I and document collection C according to the received information. The cloud server in the proposed scheme is considered as “honest-but-curious”, which is employed by lots of works on secure cloud data search.

D. Rank Search Module

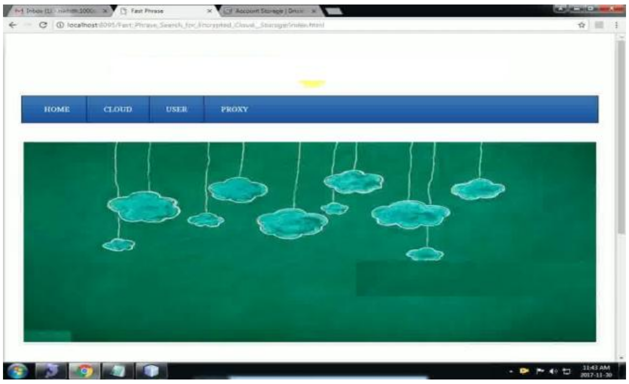
These modules ensure the user to search the files that are searched frequently using rank search. This module allows the user to download the file using his secret key to decrypt the downloaded data. This module allows the Owner to view the uploaded files and downloaded files. The proposed scheme is designed to provide not only multi-keyword query and accurate result ranking, but also dynamic update on document collections. The scheme is designed to prevent the cloud server from learning additional information about the document collection, the index tree, and the query.

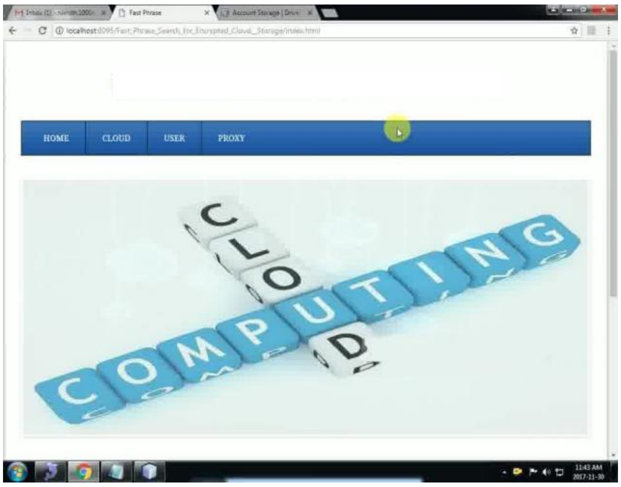
VI. ALGORITHM STEPS

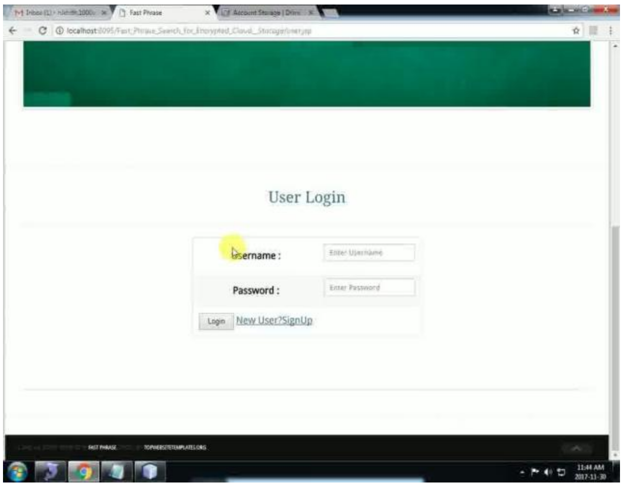
A. DS-PEKS scheme is defined by the following algorithms

1. Takes as input the security parameter _, generates the system parameters P;
2. Key-Gen(P): Takes as input the systems parameters P,
3. outputs the public/secret key pairs (pkFS; skFS), and (pkBS; skBS) for the front server, and the back server respectively;
4. DS-PEKS(P; pkFS; pkBS; kw1): Takes as input P, the front server’s public key pkFS, the back server’s public key pkBS and the keyword kw1, outputs the PEKS ciphertext CTkw1 of kw1;
5. DS-Trapdoor(P; pkFS; pkBS; kw2): Takes as input P, the front server’s public key pkFS, the back server’s public key pkBS and the keyword kw2, outputs the trapdoor Tkw2;
6. FrontTest(P; skFS;CTkw1 ; Tkw2): Takes as input P, the front server’s secret key skFS, the PEKS ciphertext CTkw1 and the trapdoor Tkw2, outputs the internal testing-state CITS;
7. BackTest(P; skBS;CITS): Takes as input P, the back server’s secret key skBS and the internal testing-state CITS, outputs the testing result 0 or 1;

VII. RESULT


Inbox (1)
Fast Phrase
Account Storage | Drive
localhost:8095/Fast_Phrase_Search_for_Encrypted_Cloud_Storage/index.html
HOME
CLOUD
USER
PROXY



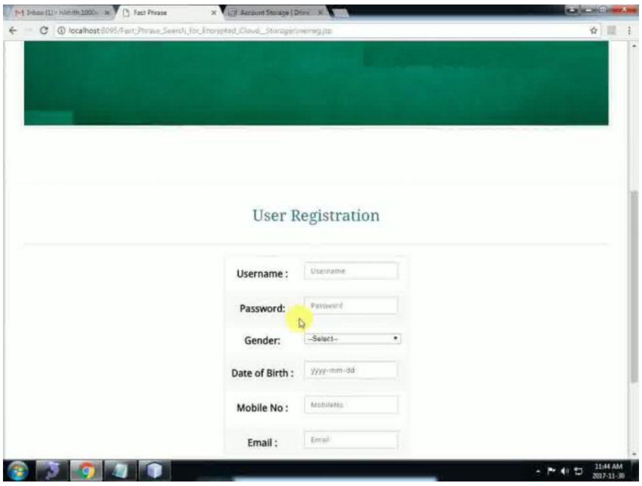


User Login

Username :

Password :

Login New User?SignUp



User Registration

Username :

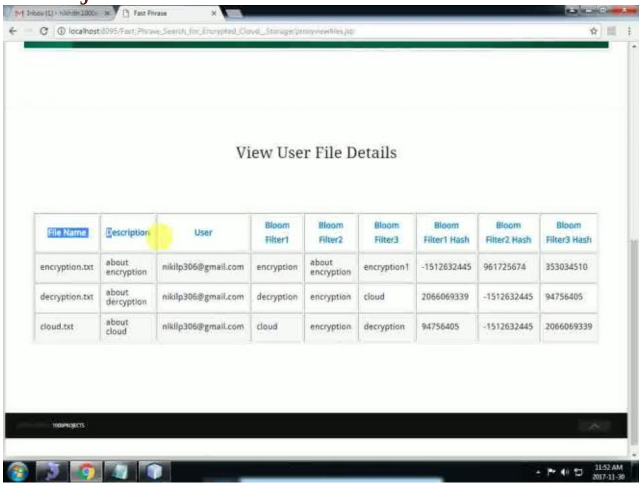
Password:

Gender: --Select--

Date of Birth :

Mobile No :

Email :



View User File Details

File Name	Description	User	Bloom Filter1	Bloom Filter2	Bloom Filter3	Bloom Filter1 Hash	Bloom Filter2 Hash	Bloom Filter3 Hash
encryption.txt	about encryption	nikilp306@gmail.com	encryption	about encryption	encryption1	-1512632445	961725674	353034510
decryption.txt	about dercyption	nikilp306@gmail.com	decryption	encryption	cloud	2066069339	-1512632445	94756405
cloud.txt	about cloud	nikilp306@gmail.com	cloud	encryption	decryption	94756405	-1512632445	2066069339

CONCLUSION

The Existing techniques on keyword-based encryption, which are widely used on the plaintext data, cannot be directly applied on the encrypted data. Downloading all the data from the cloud and decrypt locally is obviously impractical. In this paper, we proposed another structure, named Dual- Server Public Key Encryption with Keyword Search (DSPEKS), that can keep within brute-force keyword attack which is an innate weakness of the PEKS system. In future, according to technical view our proposed system is efficient and cost effective.

References

[1] Hacigümüş H, Iyer B, Li C, Mehrotra S (2002) Executing sql over encrypted data in the database-serviceprovider model. In: Proceedings of SIGMOD, ACM, pp 216–227.

[2] Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34:1–11.

[3] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in IEEE Symposium on Security and Privacy, 2000, pp. 44–55.

[4] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in EUROCRYPT, 2004, pp. 506–522.

[5] L. Fang,W. Susilo, C. Ge, and J.Wang, “Public key encryption with keyword search secure against keyword guessing attacks without random oracle,” Inf. Sci., vol. 238, pp. 221–241, 2013.

[6] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, “A new general framework for secure public key encryption with keyword search,” in Information Security and Privacy - 20th Australasian Conference, ACISP, 2015, pp. 59– 76.

[7] Zhihua Xia, Member, IEEE, Xinhui Wang, Xingming Sun, Senior Member, IEEE, and Qian Wang, Member, IEEE, “A Secure and Dynami Multi-key-word Ranked Search Scheme over Encrypted Cloud Data”.