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 5, May 2017

A Secure And Dynamic Multi Keyword Ranked Fuzzy Search Scheme Over Encrypted Cloud Data.

Kapil Kasture, Rohan Tanpure, Piyush Dhale, Venkatesh Ghalge

B.E, Department of Computer Engineering, Dr.D.Y. Patil School of Engineering, Pune, India

ABSTRACT:With the increase in number of users in cloud where users can outsource their huge data on cloud and at the time of its need the information or the data can be retrieved from the cloud very easily. For the privacy purpose, secure search is provided, but it limits to single owner model and not for several one, so this paper proposes a system which will provide a secure search efficiently for several owners using Fuzzy logic to access several files or single files without causing no ambiguity and to get the exact output from the cloud server we will use string matching algorithm for mapping the distance between two strings and also ranking the strings for better efficiency. To detect the illegal user who is not authenticated we will provide authentication key to the users which will generate dynamic secret key which will overall secure the personal as well as enterprise information from the unknown identification.

KEYWORDS: several owners, Cloud computing, Ranked keyword search, Privacy preserving.

I. INTRODUCTION

Today in day to day life huge data cannot be stored on a device and at the time of retrieving the particular data from the massive one it can cause many difficulties, so with the increasing popularity of cloud and it's computing the huge data can be put forward on cloud servers where at the time of retrieval it can be easily retrieved from the cloud. There are many cloud server's providers, but we can't trust on anyone because none of the cloud don't give guarantee about your data weather it is safe or not or it can be misused, but today's cloud servers are encrypted, but there is no secure search performed on it.

Personal Information such as personal data, hospital record, management data, emails or passwords are very important to individual and all this information should be secured and can be securely retrieved when they need only by the authenticated user.

People are afraid to put their data on cloud due to this reasons, so In this paper our aim is to providea secure search on encrypted cloud using fuzzy logic which will support several owners as compared to single owners. With the secure search, we will give each and every user an authenticated key which will generate a dynamic secret key which will be useful to detect the illegal eavesdropping who tries to identify as authenticated user to steal the individual or enterprise information. The Data owners who put their data on cloud will be given a encrypted key as same for the user which will let know the authenticated user only wants the data and by using string matching algorithm the search result will be ranked and the distance will be mapped between two strings and the output will be efficiently carried out.

DOI: 10.15680/IJIRCCE.2017. 0505144

II. RELATED WORK

Privacy-preserving public auditing for secure cloud storage:

Users can remotely stored data on cloud without burden of its local storage & maintenance. For privacy purpose, individuals & enterprise users are reluctant to outsource their sensitive data(emails, personal health records, go confidential files).[3]

Practical techniques for searches on encrypted data:

Secure search service over encrypted cloud data is of a paramount importance. enables users to perform a keyword-based search on an encrypted dataset, just as on plaintext dataset these schemas were concerned mostly with single or Boolean keyword search.[5]

Privacy-aware Bed Tree Based Solution for Fuzzy Multi-keyword Search over Encrypted Data:

Traditional searchable encryption schemes typically only support exact keyword Matches. Using fuzzy logic for multi-keyword match in multi-owner model. Fuzzy keyword search solution consumes large storage size since it inserts every fuzzy keyword as a leaf node in the index tree.[1]

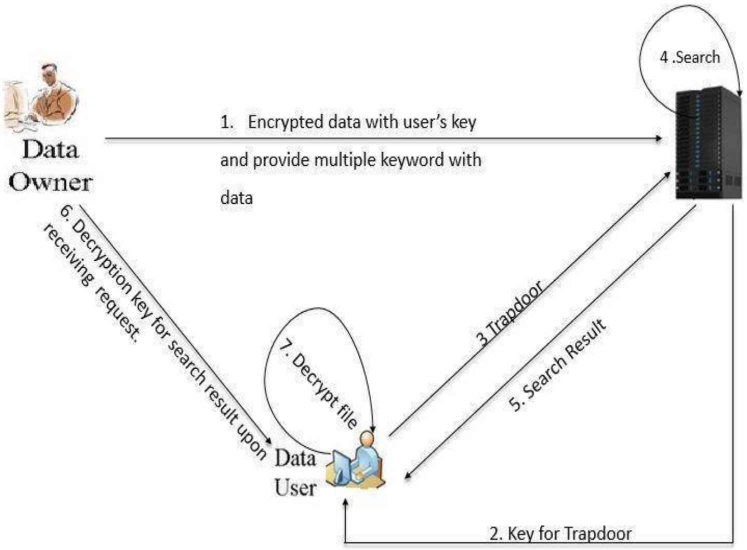
III.PROPOSED SYSTEM

Secure Searching and ranking: -

a. System will generate a search key for each user after approval from admin (one-time)
b. The User enters a keyword in order to retrieve the associated File.
c. Using that keyword along with the user's key and search key a trapdoor is calculated.
d. This trapdoor along with a search key used in this calculation is sent to the server.

Multi-owner model and secure storage of owner’s data: -

a. Here we propose Multi-Owner model over single Owner.
b. The user uploads the desired File to server which is securely stored using a User's key to access it.
c. In multiple owner model has rights to upload the over server.
d. Along with the secured storage of the file, the keywords or index related to that file is also stored in the Server.


Data Owner
1. Encrypted data with user's key and provide multiple keyword with data
4 .Search
6. Decryption key for search result upon receiving request.
7. Decrypt file
3 Trapdoor
5. Search Result
Data User
2. Key for Trapdoor

Fig(a). Proposed System

IV. PROPOSED ALGORITHM

1. *Elliptic Curve Cryptography Algorithm:*

a) Select the file type then select plain text from the file

b) After selecting file select the output file

c) After selecting output file check if file compress or not

d) If the file compress then check the plain text is converted to cipher text or not (encrypted file)

e) If text in file are hidden or converted to cipher text, then encryption is successful.

f) For retrieving encrypted, hidden, compressed message select the output file for retrieving output file enter key or password.

a. Key generation: *(q, FR, a, b, G, n, h).*

g) Select a random number *d*, $d \in [1, n–1]$

h) parameters Compare $Q = dG$.

i) public key is *Q* and private key is *d.*

j) A public key $Q = (xq, yq)$ associated with the domain parameters *(q, FR, a, b, G, n, h)* is validated

using the following procedure

1. Check that $Q \neq O$
2. Check that *xq* and *yq* are properly represented elements of *Fq*
3. Check if *Q* lies on the elliptic curve defined by *a* and *b*.
4. Check that $nQ = O$

2. Levenstein Algorithm

S=string. D=distance value.

T=threshold distance

S= (s1,s2,s3 ….)

Set of strings.

Input = (s1,s2,.. Sn)

For all strings calculate *D*.

All *Ds* of *S* which are less than *T*. Return to user.

3. N-Gram Algorithm

S=string. D=distance value.

N=max number of combination.
S= (s1,s2,s3….)

Set of strings.

Input = (s1,s2,.. Sn) For 1 to n

Generate number of combinations.

Search the indexed file with max number of combination matched. Return to user.

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

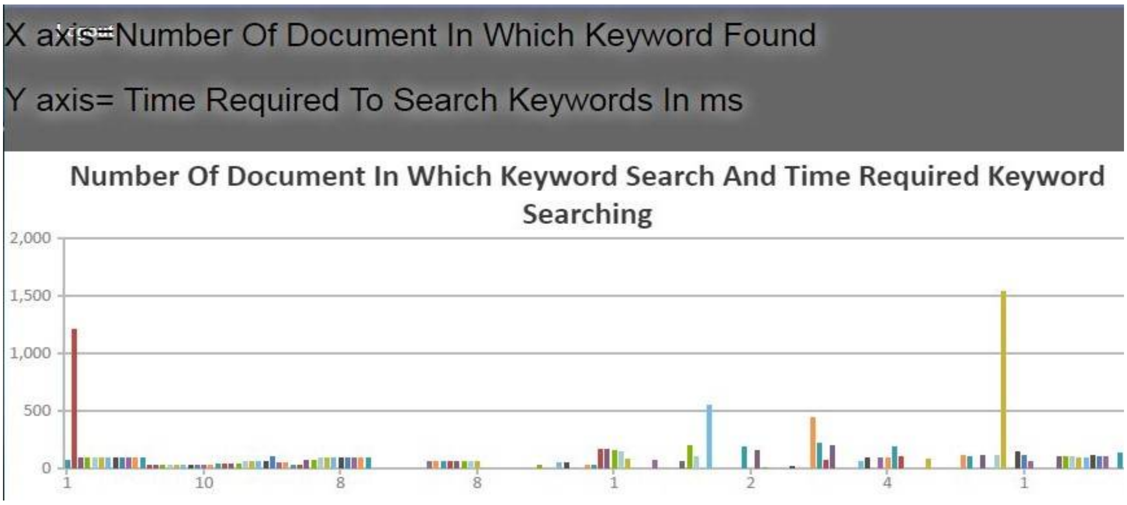
Vol. 5, Issue 5, May 2017

V. SIMULATION RESULTS

A) Index Construction

Fig.shows that, given the same keyword dictionary (u=4000), time of index construction for these schemes increases linearly with an increasing number of files, while SRMSM and PRMSM spend much less time on index construction. Fig. 6(b) demonstrates that, given the same number of files (n=1000), SRMSM and PRMSM consume much less time than MRSEon constructing indexes. Additionally, SRMSM andPRMSM are insensitive to the size of the keyword dictionary for index construction, while MRSE suffers a quadratic growth with the size of keyword dictionary increases. Fig. 6(c) shows the encoding efficiency of our proposed AOPPF. The time spent on encoding increases from 0.1s to 1s when the numberof keywords increases from 1000 to 10000. This timecost can be acceptable.

B) Compared with index construction, trapdoor generationconsumes relatively less time. Fig. demonstrates that, given the same number of queried keywords (q=100), SRMSM and PRMSM are insensitive to the size of keyword dictionary on trapdoor generation and consumes 0.026s and 0.031s, respectively. Meanwhile, MRSE increases from 0.04s to 6.2s. Fig. shows that, given the same number of dictionary size (u=4000), when the number of queried keywords increases from 100 to 1000, the trapdoor generation time for MRSE is 0.31s, and remains unchanged. While SRMSM increases from 0.024s to 0.25s, PRMSM increases from 0.031s to 0.31s. We observe that PRMSM spends a little more time than SRMSM on trapdoor generation; the reason is that PRMSM introduces an additional variable to ensure the randomness of trapdoors.



X axis=Number Of Document In Which Keyword Found

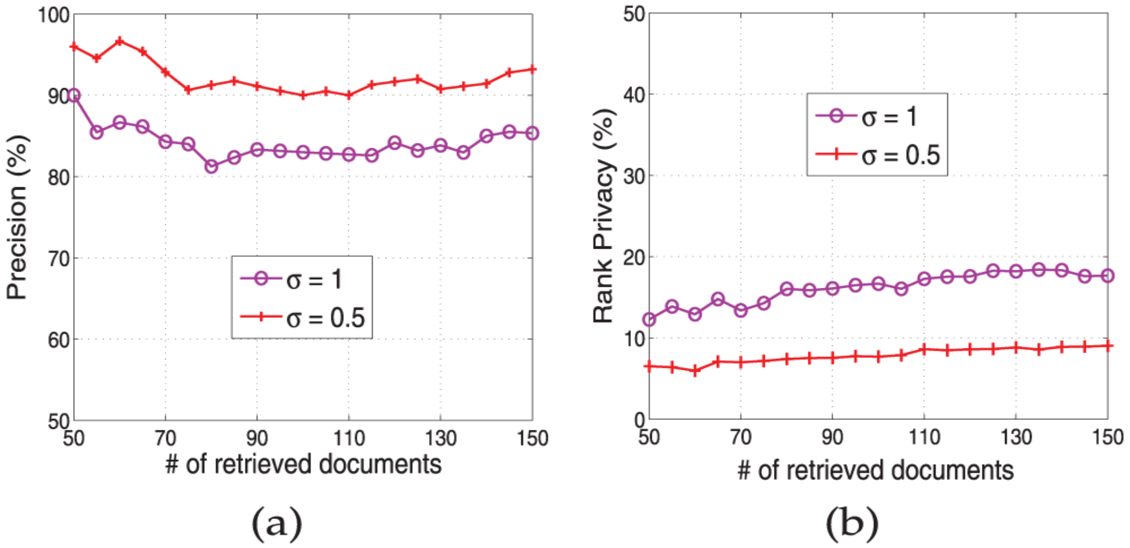
Y axis= Time Required To Search Keywords In ms

Number Of Document In Which Keyword Search And Time Required Keyword Searching
2,000
1,500
1,000
500
0
1
10
8
8
1
2
4
1

Fig(b). Simulation result 1

From above figure we found number of documents in which keyword is searched using fuzzy logic. The graph shows the statistics of different n-documents with related keyword.

DOI: 10.15680/IJIRCCE.2017. 0505144



Fig(c). Graph representation

In the above graph (a) shows percentage of precision from retrieved documents and graph (b) shows percentage of ranking privacy from retrieved documents.

VI.CONCLUSION AND FUTURE WORK

In this paper, we define the problem of secure multiple-keyword search for several data owners and several data users in the cloud computing environment. different from prior works, our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data using fuzzy logic for secure searching over encrypted cloud.

REFRENCES

[1]. D.B.et al., "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," *EUROCRYPT*, vol. 43, pp. 506-522,2004.

[2]. M.Armbrust, A. Fox, R.Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A.Rabkin, I. Stoica, and M.Zaharia, "A view of cloud computing," Communication of the ACM, vol. 53,no.4,pp.50-58,2010.

[3]. C.Wang, S.S.Chow, Q.Wang, K.Ren, and W.Lou, "Privacy-preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol.62, no.2, pp.362-375, 2013.

[4]. B.Chor ,, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *Journal of the ACM*, vol. 45, no. 6, pp. 965–981, 1998

[5]. D.Song, D.Wagner, and A.Perrig,"Practical techniques for searches on encrypted data," in Proc.IEEE International Symposium on Security and Privacy, Nagoya, Japan, , pp.44-55,Jan.2000