MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

SECURED FUZZY RANKED MULTIPLE-KEYWORD SEARCH FOR SEVERAL DATA-OWNER PARADIGM USING STRING MATCHING ALGORITHM IN CLOUD COMPUTING

Kapil Kasture, Rohan Tanpure, Piyush Dhale,
Venkatesh Ghalge, Prof.Jayashree Chaudhari

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.*

1. 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 provide a 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.

2. LITERATURE SURVEY

Privacy-preserving ranked multiple-keyword search for several data owners in cloud computing:

With the increase in the number of users in cloud computing the cloud is becoming day to day popular where we users can outsource their huge data on cloud server, but do we thing the information on cloud is secured? The sensitive data of an individual is not secured on cloud so this paper propose a privacy-preserving ranked multiple-keyword search for several data owners where the data of owners will be encrypted according to ranked wise results of multi-keyword. To perform a secure search on cloud severs this paper propose a secure search protocol without knowing the actual data of keywords and trapdoors. [1]

A view of cloud computing:

It is a subversive technology that is changing the way IT hardware & software is designed, purchased. used to outsource huge data on cloud which includes easy access of data, decreased in costs, quick deployment etc. [2]

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. [4]

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. [5]

3. PROPOSED SYSTEM

a) We define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality.
b) Among various multi-keyword semantics, we choose the efficient principle of “coordinate matching”.
c) To provide efficiency in accessing files in multiple-owner and single file or multiple-owner and multiple files paradigm.
d) In this application data owner is created a data or we can say file. Also data owner generate index for the file. After that owner encrypt the file and upload into the cloud. The application server also encrypts the file.
e) The data user when wants to access a specific file he/she send request to data owner. And it gets the decryption key. By using this key user decrypt the encrypted file. And get the plain text file.
f) In this phase, we make experiment on discovered problem. To overcome the issues we go through the various papers. While we going through the papers we found nice solutions to above problem:

3.1 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.

3.2 Multi-owner model and secure storage of owner's data: -

a. Here we propose Multi-Owner model over single Owner.

b. In multiple owner model has rights to upload the over server.

c. The user uploads the desired File to server which is securely stored using a User's key to access it.

d. Along with the secured storage of the file, the keywords or index related to that file is also stored in the Server.

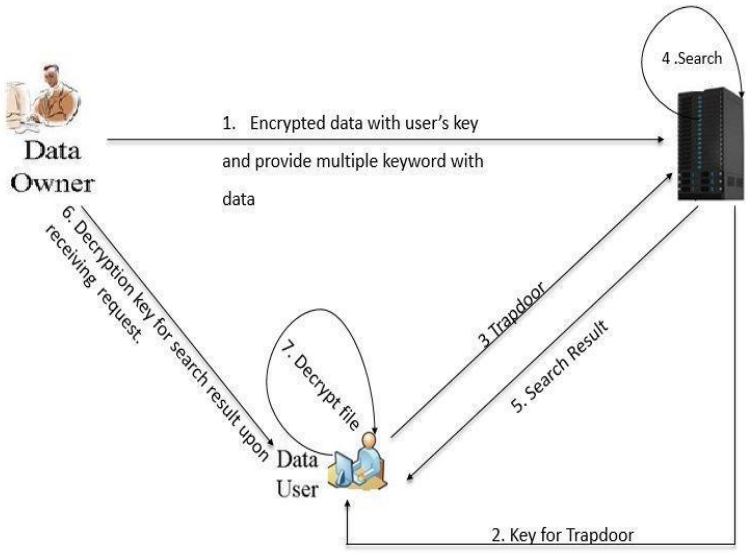

Fig 1: System Architecture

4. MATHEMATICAL MODEL

4.1 Input:

Inputs given to the system are: - {*F*: -plain text file, *IND*: -index file created from plain text file, *K*: -set of keywords/trapdoors used to find the files.}

4.2 Output:

Output will be: - {*RF*: -rank for the files, *F*: -searched files from the encrypted data}

4.3 Process:

Process will be performed: - *{O, F, C, W, T}*

O: -the data owner collection, denoted as a set of m data owners*, O: - {O1, O2,..Om}*

Fi: the plaintext files collection of *Oi,* denoted as a set of n data file

Fi=(Fi;1, Fi;2,. . . ,Fi;n).

Ci: the cipher text files collection of *Fi,* denoted as

Ci=(Ci;1, Ci;2,. . . ,Ci;n).

W: the keyword collection, denoted as a set of u keywords

The data owner *"O "*uploads the plaintext file *F* where data owner is

O = (O1,O2, . . . ,Om).

Files are : *Fi=(Fi;1, Fi;2,. . . ,Fi;n)* where this plain text files are encrypted and give the encrypted file as *Ci=(Ci;1, Ci;2,. . . ,Ci;n){cipher text files}.*

index file is created from these files and uploaded to the application server.

Ind = {indf | indf1, indf2 . . .indfn}

After the file has been uploaded, the data owner exchange the key with the data user, he wants to access these file.

4.4 Success Condition:

Output must be in ranked keyword search form if user is authenticated.

4.5 Failure Condition:

If user is not authenticated, access is not granted and may produce ambiguity. Huge database can lead to more time consumption to get the information.

5. ALGORITHMS

5.1 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:

b. (q, FR, a, b, G, n, h).

g) Select a random number *d*, *d∈[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 ≠ 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*

5.2 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.

5.3 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.

6. CONCLUSION & FUTURE SCOPE

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.

7. ACKNOWLEDGEMENT

It gives us great pleasure in presenting the preliminary project report on 'SECUREDFUZZY RANKED MULTI-KEYWORD SEARCH FOR SEVERAL DATAOWNER PARADIGM USING STRING MATCHING ALGORITHM IN CLOUDCOMPUTING'.

We would like to take this opportunity to thank our internal guide Prof. Jayashree Chaudhari. for giving us all the help and guidance We needed. We are really grateful to him for his kind support. His valuable suggestions were very helpful.

We are also grateful to Prof. S. S. Das, Head of Computer Engineering Department, DYPSOE, Lohegaon, Pune and to our Project Co-ordinator Prof. Amruta Chitari. for their indispensable support, suggestions and motivation during the entire course of the project.

In the end special thanks to our Director Dr. S. S. Sonawane who encouraged us and created a healthy environment for all of us to learn in best possible way.

We also thank all the staff members of our college and technicians for their help in making this project a successful one.

REFERENCES

[1]. Wei Zhang, Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member, IEEE, Jie Wu, Fellow, IEEE, and Siwang Zhou " Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing"

[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]. 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, Jan.2000, pp.44-55.

[5]. M.chuah and W.Hu, "Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data," in Proc.IEEE 31th International Conference on Distributed Computing Systems,Minneapolis, MN, Jun.2011, pp.383-392.