ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 12, December 2016**

# Privacy Preserving Ranked Fuzzy keyword searches for Multiple Data Owners in Cloud Computing

Vuppuluri Sai Lakshmi Usha[1], Dr.Sudhakar Putheti[2]

M.Tech, Dept. of CSE, Vasireddy Venkatadri Institute of Technology (VVIT), Namburu, Guntur, Andhra Pradesh, India[1]

Professor, Dept. of CSE, Vasireddy Venkatadri Institute of Technology (VVIT), Namburu, Guntur, Andhra Pradesh, India[2]

**ABSTRACT:** With the advent of cloud computing, it has become increasingly popular for data owners to outsource their data to public cloud servers while allowing data users to retrieve this data. For privacy concerns, secure searches over encrypted cloud data have motivated several research works under the single owner model. However, most cloud servers in practice do not just serve one owner; instead, they support multiple owners to share the benefits brought by cloud computing. In this paper, we propose schemes to deal with Privacy preserving Ranked Multi-keyword Search in a Multi-owner model along with it solves the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when an exact match fails. We systematically construct a novel secure search protocol which Generate fuzzy keyword set and also used Advanced Technique for Constructing Fuzzy Keyword Sets.

**KEYWORDS:** Searchable Encryption, Fuzzy keyword searches, Cloud Computing,

## I. INTRODUCTION

Cloud computing is an Internet computing in which data is stored and accessed via a remote third party server called thecloud, rather than being stored locally on the machine. The resources, software, and information needed are provided to users on demand. In cloud computing environment, data security is an on-going challenging task, hence the sensitive data has to be encrypted before outsourcing. The system retrieves the files from the cloud, by searching the keywords on the encrypted data. They are many searching techniques which were implemented in the cloud but the disadvantage with this technique is that they support only exact keyword search. The proposed work concentrates on solving the problems of the user who search the data with the help of fuzzy keyword on thecloud. And formalizes a solution to the problems of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Using fuzzy search the exact keywords are displayed along with similarity keywords, which solve the problems faced by the cloud users. It shows that the proposed solution is secure and privacy preserving, while correctly realizing the goal of fuzzy keyword search. The increasing popularity of cloud storage services has lead companies that handle critical data to think about using these services for their storage needs. Medical record databases, power system, historical information and financial data are some examples of critical data that could be moved to the cloud. However, the reliability and security of data stored in the cloud still remain major concerns. DEPSKY[1], a system that improves the availability, integrity, and confidentiality of information stored in the cloud through the encryption[2], encoding and replication of the data on diverse clouds that form a cloud-of-clouds. It deployed the system using four commercial clouds and used Planet lab to run clients accessing the service from different countries. The protocols improved the perceived availability and, in most cases, the access latency when compared with cloud providers individually. Moreover, the monetary costs of using DEPSKY on this scenario is twice the cost of using a single cloud, which is

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 12, December 2016**

optimal and seems to be a reasonable cost, given the benefits. Fuzzy keyword system is formalized to solve the problem of supporting efficient yet privacy preserving fuzzy search for achieving effective utilization of remotely stored encrypted data in multicolored Computing. Two advanced techniques (i.e., wildcard based and grambased techniques)[3][4][5][6] are designed to construct the storage efficient fuzzy keyword sets by exploiting two significant observations on the similarity metric of edit distance. Based on the constructed fuzzy keyword sets, a brand new symbol-based searching scheme is also proposed; where a multi-way tree structure is built up using symbols transformed from the resulted fuzzy keyword sets.

## II. SYSTEM STUDY

### *A. UNDERSTANDING SEARCHABLE ENCRYPTION:*

The searchable encryption was made by Song et al. In [3], they propose to encrypt each word in a file independently and allow the server to find whether a single queried keyword is contained in the file without knowing the exact word. Searchable encryption schemes provide an important mechanism to cryptographically protect data while keeping it available to be searched and accessed. In a common approach for their construction, the encrypting Entity chooses one or several keywords that describe the content of each encrypted record of data. To perform a search, a user obtains a trapdoor for a keyword of his/her interests and uses this trapdoor to find all the described by this keyword. We present a searchable encryption scheme that allows users to privately search by keywords on encrypted data in public key setting and decrypt the search result. To this end , we define and implements two primitives: public key encryption(PEOKS) and oblivious keyword search and committed blind anonymous identity-based encryption. PEOKS is an extension of public key encryption with akeyword search in which users can obtain trapdoor from the secret key holder without revealing the keywords. PEOKS scheme is used to build public key encrypted database that permits private searches i.e.; neither the keyword nor the search result is revealed.

### *B. PLAINTEXT FUZZY KEYWORD SEARCH.*

fuzzy search is a process that locates Web pages that are likely to be relevant to a search argument even when the argument does not exactly correspond to the desired information. A fuzzy search is done by means of a fuzzy matching program, which returns a list of results based on likely relevance even though search argument words and spellings may not exactly match. Exact and highly relevant matches appear near the top of the list. Subjective relevance ratings, usually as percentages, may be given.
Eg:Fuzzy Search: approximate string matching
Ex. Plagirisum will be corrected to Plagiarism

**Scenario:**

- User wants search keyword Plagiarism
- User misspelled it as Plagirisum and clicked on search button
- Data in the database is in encrypted form.
- Now we will try to search the encrypted data for inputted keyword Plagirisum. Which will convert to Plagiarism and display result?
- This is the technique which will help us to match the keyword Plagirisum with encrypted keywords in the database
- This is fuzzy keyword search over encrypted data in cloud computing

Fuzzy searching is much more powerful than exact searching when used for research and investigation. Fuzzy searching is especially useful when researching unfamiliar, foreign-language, or sophisticated terms, the proper spellings of which are not widely known. Fuzzy searching can also be used to locate individuals based on incomplete or partially inaccurate identifying information

### *C. FUZZY KEYWORD INVESTIGATION:*

The fuzzy keyword set can be defined by using edit distance as follows: Given a collection of n encrypted data files C = (F1, F2. . . FN) stored in the cloud server, a set of distinct keywords W = {w1, w2, …,wp} with predefined edit distance d, and a searching input (w, k) with edit distance k ($k \leq d$),the execution of fuzzy keyword search returns a set

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

of file IDs whose corresponding data files possibly contain the word w, denoted as FIDw: if w = wi belongs to W, then return FIDwi ; otherwise, if w does not belong to W,then return {FIDwi}, where ed(w,wi) ≤ k. Note that the above definition is based on the assumption that k ≤ d. Infect, d can be different for distinct keywords and the system will return {FIDwi} satisfying ed(w,wi) ≤ min{k, d} if theexact match fails. For example, the following is the listing variants after a substitution operation on the first character of keyword CASTLE: {AASTLE, BASTLE, DASTLE, · · · YASTLE, ZASTLE}.

## III. PRESENTED SYSTEM

For privacy concerns, secure searches over encrypted cloud data has motivated several research works under the single owner model. However, most cloud servers in practice do not just serve one owner. Secure search over encrypted data has recently attracted the interest of many researchers. Song et al. first define and solve the problem of secure search over encrypted data. They propose the conception of searchable encryption, which is a cryptographic primitive that enables users to perform a keyword-based search on an encrypted dataset, just as on a plaintext dataset. Searchable encryption is further developed.
Secure search over encrypted cloud data is first defined by Wang et al. and further developed. These researches not only reduce the computation and storage cost for secure keyword search over encrypted cloud data, but also enrich the category of search function, including secure ranked multi-keyword search, fuzzy keyword search, and similarity search.

**Disadvantages of Existing System:**

- Existing schemes are concerned mostly with single or boolean keyword search.
- All the existing schemes are limited to the single-owner model. As a matter of fact, most cloud servers in practice do not just serve one data owner; instead, they often support multiple data owners to share the benefits brought by cloud computing.

## IV. PRAPOSED SYSTEM

In this paper, our proposed concept supporteffective fuzzy keyword search for Multiple Data Owners in Cloud Computing

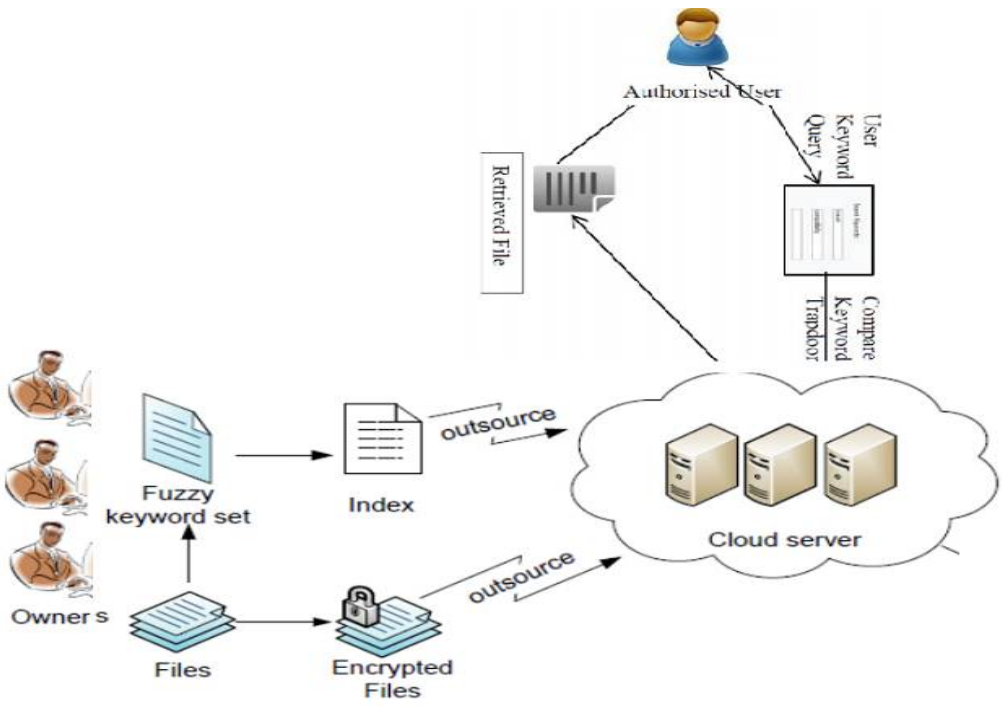


Fig 1.Architecture of fuzzy keyword search

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 12, December 2016**

***A. FUZZY KEYWORD SEARCH SCHEME*:** returns the search results according to the following rules: If the user's searching input exactly matches the pre-defined set of keywords, the server will return the files containing the keyword; If there exist some error in spelling or some format inconsistencies in the searching input, the server will return the closest possible results based on pre-specified similarity semantics. Architecture of fuzzy keyword search is shown in the Fig. 1. Let us consider a semi-trusted server. Even though data files are encrypted, the cloud server may try to derive other sensitive information from user's search requests while performing the keyword-based search over Cloud. Thus, the search should be done in a well secured way that permits data files to be securely retrieved during exhibiting as little information as possible to the cloud server. In this paper, when designing fuzzy keyword search scheme, we will follow the security definition deployed in the traditional searchable encryption .More specifically, it is required that nothing should be leaked from the remotely stored files and index beyond the outcome and the pattern of search queries

***B. CONSTRUCTION OF EFFECTIVE FUZZY KEYWORD SEARCH:*** The main idea behind performing the secure fuzzy keyword search consists of two concepts: 1) Generate fuzzy keyword set that include exact keyword along with keyword that that differ from exact keyword due to minor typos or due to inconsistency in formatting 2) To design mechanism to securely retrieve files based upon the keyword entered.

***C. ADVANCED TECHNIQUE FOR CONSTRUCTING FUZZY KEYWORD SETS:***
effective fuzzy keyword search constructions with regard to both storage and search efficiency, we now propose two advanced techniques to improve the straightforward approach for constructing the fuzzy keyword set

**i. Wildcard-based Fuzzy Set Construction**
all the variants of keywords to be listed when an operation is performed at the same position. Based on the above approach, we use a wild card to denote the edit operations performed at the same position. This technique edits distance to solve the problems. It includes the following steps:
i)It builds an index with each keyword k. To build index data owner computes f(sk , k).
ii)Construct the secret key sk. This sk is shared among the data owner and user if he is an authorized user.
iii)Searching can be done with secret key sk , keyword k.
iv)Compare the secret key sent by the user and existed key at the data owner. If both are same, returns the requested file.
For example, for the keyword FEVER with the pre-set edit distance 1, its wildcard based fuzzy keyword set can be constructed as FEVER,1 = {FEVER, *FEVER, *EVER, FE*VER, F*VER, FEV*ER, FEV*R, FEVE*R, FEVE*, FEVER*}

**ii.Gram-based Fuzzy Set Construction**
Another efficient technique for constructing fuzzy set is based on grams. The gram of a string is a substring that can be used as a signature for efficient approximate search [11]. While gram has been widely used for constructing inverted listfor matching purpose. Here, edit operations will affect only one character in the given keyword and all remaining are same. For example, the gram based fuzzy set EFEVER, 1 for the keyword FEVER can be constructed a {FEVER, EVER,FVER, FEER, FEVR, FEVE}

## V. SYTSEM IMPLEMENTATION

System Implementation consist of various parts described as follows:

1. Data Owner
2. Authorized user
3. Cloud server

***A. DATA OWNER* :** Data owner have the set of files ,they create the index file from fuzykeyword set and send that file to the cloudserver . Finally Data owner encrypt that file where DES algorithm is used for encryption which makes data

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 12, December 2016**

secure and protect it from unauthorized access and send encrypted file to the cloud server as well as send the encryption key to the authorized user .

***B. AUTHORIZED DATA USER*:**In order to access file user must have authorization. Authorization of user provided to the user by unique key which he gets when he perform login for the first time. All the fuzzy search words in trie can be found by depth first search approach. User can get search result by entering keywords along with conjunction of single words i.e. AND,OR,BOTH. For example, if file has attribute, Illeness: cold, Fever, hospital: A, B, C, D. then user can access that file with dummy attribute (AND,OR,BOTH) as illness: fever AND hospital :A etc

***C. CLOUD SERVER:*** Cloud server Upon receiving the trapdoor, the cloud server searches the encrypted index of each data owner and returns the corresponding set of encrypted files.

## VI. CONCLUSION

In this paper, we explore the problem of secure multi-keyword search for multiple data owners and multiple 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.

## REFERENCES

[1] AlyssonBessani, Miguel Correia, Paulo Sousa, and Bruno Quaresma, DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds, University of Lisbon, Faculty of Sciences, Portugal.
[2] Dan Boneh, Giovanni Di Crescenzo, and RafailOstrovsky, Public Key Encryption with keyword Search, in Stanford University.
[3] INF 3800, Edit Distance, 2011.02.21.
[4] M. Hellmann, Fuzzy Logic Introduction, LaboratoireAntennes Radar Telecom, F.R.E CNRS 2272.
[5] William B. Cavnar and John M. Trenkle, N-Gram-Based Text Categorization, in Environmental Research Institute of Michigan.
[6] V. Levenshtein, Binary codes capable of correcting spurious insertions and deletions of ones, in Vol. 163,No.4, pp.845-848, 1965 August.
[7] FengBao, Robert H. Deng, Private query on encrypted data in multi user settings, in School of Information Systems, Singapore Management University.
[8] Jan Kremer, cloud computing and virtualization,"in Jan Kremer Consulting Services.
[9] Mohammed A. AlZain, Eric Pardede, cloud computing security: From single to multi user settings, RMIT University, Melbourne 3001, Australia.
[10] Ranjeethkumar. M, "A noval implementation of fuzzy keyword search over encrypted data in cloud computing ", in International Journal of Computer Trends and Technology- July to Aug Issue 2011
[11]. S. Ji, G. Li, C. Li, and J. Feng, "Efficient interactive fuzzy keyword search," in Proc. of WWW'09, 2009.