International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 5, Issue 5 (May 2016), PP.76-80

Fuzzy Keyword Searches for Multiple PHR Owners in Cloud Computing

Birru Devender[1], Md. Khalid Imam Rahmani[2]

[1]Associate Professor, Holy Mary Institute of Technology and Science, Affiliated to JNTU, Hyderabad, T.S, India.
[2]Professor, Holy Mary Institute of Technology and Science, Affiliated to JNTU, Hyderabad, T.S, India.

Abstract: With the beginning of cloud computing, it has become increasingly popular for PHR owners to outsource their documents to public cloud servers while allowing users to retrieve this data. For privacy concerns, secure searches over encrypted cloud data have motivated several research works under the single PHR owner model. However, most cloud servers in practice do not just serve one PHR owner; instead, they support multiple PHR owners to share the benefits brought by cloud computing. In this paper, we propose schemes to deal with Preserving Fuzzy 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 similar documents when users' searching inputs exactly match the predefined keywords or the closest possible similar Health records 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 a remote computing within which documents are stored and accessed from third party server referred to as the cloud, instead of being keeps maintains on the machine. The resources, software, and data required provided to users on demand. In cloud computing, information security is AN ongoing difficult task; hence the sensitive information must be encrypted before outsourcing. The system retrieves the files from the cloud, by looking out the keywords on the encrypted information. They are several looking out techniques that were enforced within the cloud however the disadvantage with this system is that they support single keyword search. The projected work concentrates on determination the issues of the user World Health Organization search the information with the assistance of fuzzy keyword on the cloud. And formalizes an answer to the issues of effective fuzzy keyword search over encrypted cloud information whereas maintaining keyword privacy. Exploitation fuzzy search the precise keywords square measure displayed at the side of similarity keywords that solve the issues featured by the cloud users. It shows that the projected resolution is secure and privacy conserving, whereas properly realizing the goal of fuzzy keyword search. The increasing quality of cloud storage services has lead corporations that handle vital information to admit exploitation these services for his or her storage desires. case history databases, power grid, historical data and monetary information square measure some samples of vital information that would be affected to the cloud. However, the irresponsibleness and security of knowledge keep within the cloud still stay major issues. DEPSKY [1], a system that improves the provision, integrity, and confidentiality of knowledge keep within the cloud through the encryption [2], cryptography and replication of the information on various clouds that kind a cloud-of-clouds. It deployed the system exploitation four industrial clouds and used Planet work to run purchasers accessing the service from completely different countries.

The protocols improved the perceived convenience and, in most cases, the access latency compared with cloud suppliers on an individual basis. Moreover, the financial prices of exploitation DEPSKY on this situation is doubly the price of employing a single cloud, that is perfect and looks to be an affordable price, given the advantages. Fuzzy keyword system is formalized to unravel the matter of supporting economical however privacy conserving fuzzy seek for achieving effective utilization of remotely keep encrypted information in painted Computing. 2 advanced techniques (i.e., wildcard based mostly and gram based techniques) [3] [4] [5] [6] square measure designed to construct the storage economical fuzzy keyword sets by exploiting 2 vital observations on the similarity metric of edit distance. Supported the made fuzzy keyword sets, a fresh symbol based looking out theme is additionally proposed; wherever a multi-way tree structure is made up exploitation symbols reworked from the resulted fuzzy keyword sets.

II. SYSTEM STUDY

2.1Understanding 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 a keyword 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.

2.2 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.
E.g. Fuzzy Search: approximate string matching
Ex. Plagiarism will be corrected to Plagiarism

Scenario:

- User wants search keyword Plagiarism
- User misspelled it as Plagiarism 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 Plagiarism. Which will convert to Plagiarism and display result?
- This is the technique which will help us to match the keyword Plagiarism 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.

1.1. 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 ≤ d),the execution of fuzzy keyword search returns a set 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 the exact 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 have 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 support effective fuzzy keyword search for Multiple Data Owners in Cloud Computing.

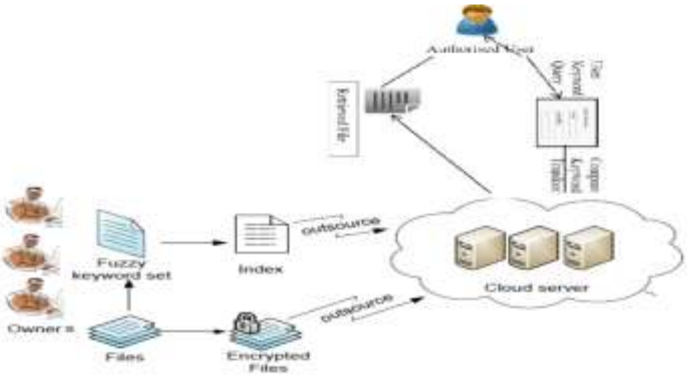

Fig 1. Architecture of fuzzy keyword search

4.1. 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

4.2. 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.

4.3. 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

4.3.1. 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*}

4.3.2. 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. PHR Owner
2. User
3. Admin

1. PHR Owner

PHR owner have the set of files, they create the index file from fuzzy keyword set and send that file to the cloud server. Finally PHR owner encrypt that file where AES algorithm is used for encryption which makes data 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.

2. User:

In order to access document the user should have authorization. Authorization of user provided to the user by distinctive key that he gets once he perform login for the primary time. All the fuzzy search words in index may be found by DFS approach. User will get search result by getting into keywords in conjunction with conjunction of single words i.e. AND, OR, BOTH. For example, if file has attribute, Illness: 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.

3. Admin

Admin upon receiving the request, the admin searches the encrypted index of each PHR owner document and returns the corresponding set of encrypted Documents.

VI. CONCLUSION

In this paper, we survey the problem of Fuzzy-keyword search for multiple PHR owners and multiple data users in the cloud computing environment. Different from Literature works; our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data.

REFRENCES

[1] Alysson Bessani, 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] Feng Bao, 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] Ranjeeth kumar. 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.

[12] Md. Khalid Imam Rahmani, Neeta Wadhwa and Vaibhav Malhotra, “Alpha-Qwerty Cipher: An Extended Vigenere Cipher”, Advanced Computing: An International Journal (ACIJ) 3 (3) 2012, pp. 107-118.

[13] Md. Khalid Imam Rahmani, M A Ansari, A K Goel, “An Efficient Indexing Algorithm for CBIR” Computational Intelligence & Communication Technology (CICT), 2015, IEEE, DOI: 10.1109/CICT.2015.165.

[14] Md. Khalid Imam Rahmani and M A Ansari, “Fuzzy Image Retrieval: Recent Trends”, Indian Journal of Industrial and Applied Mathematics, 2013, Volume 4, Issue 2, pp. 131-137, DOI: 10.5958/j.1945-919X.4.2.014.