International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

REVIEW OF FUZZY KEYWORD SEARCH

Nivedita W. Wasankar[1], A.V. Deorankar[2]

[1]M. Tech. Scholar, Department of Computer Science and Engineering, Government College of Engineering, Amravati (MH) India

[2]Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering, Amravati (MH) India[2]

ABSTRACT:

Cloud computing maintains data and applications through the internet and central remote servers. Cloud computing allows customers and businesses to use applications without installation and they can access their personal files at any computer with internet access. This technology has most efficient computing by centralizing storage, memory, processing and bandwidth. Possibly the biggest concerns about cloud computing is security and privacy. If a client log in from any location to access data and applications, it's possible the client's privacy could be compromised and User want to retrieve only certain specific data files of their interest during the session.There are many searching technique that supports only exact keyword search. Using fuzzy keyword search, the exact keywords are displayed along with similarity keywords, which solve the problems encountered by the cloud users. This paper concentrates on fuzzy keyword search on cloud.This paper give literature survey on searchable encryption and single keyword search or Boolean keyword search and fuzzy keyword search.

Keywords:*Boolean keyword search,Cloud computing, fuzzy keyword search, searchable encryption, single keyword search.*

1. INTRODUCTION:

Cloud computing enables users to outsource their data to the cloud servers over internet. By storing their data into the cloud, the data owners can be freed from the burden of data storage and maintenance and enjoy the on-demand high quality data storage service. To protect data privacy and protect againstunauthorized accesses, important data has to be encrypted before outsourcing. It will provide end-to-end data confidentiality assurance in the cloud. In Cloud Computing, data owners may share their outsourced data with a large number of users. User want to retrieve only certain specific data files of their interest during the session. To overcome this problem, one of the best solution is to selectively retrieve the files through keyword based search instead of unnecessary information irrespective of user's interest. Keyword based search techniques gives only the data which the users wants. For example, google search. The actual traditional encryption method uses simple spell

check mechanism for keyword search. This mechanism does not support all types of keywords. It is not efficient because it needs more user interaction. The spell check algorithm gives unnecessarily burden to the user, so the user effort is more in this mechanism as compare to other. Another reason is that sometimes the user enters wrong keyword such as toy instead of boy. spell check algorithm does not work properly it will give result of toy.It only works for exact keyword match which restricts the users to perform keyword search which is not efficient in cloud computing Thus, the drawbacks of existing schemes show the need of new techniques which supports flexible search, by allowing both minor mistakes and format variations.

Fuzzy keyword search obviously 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 exact match fails. Edit distance is used to quantify keywords similarity using an advanced technique. It is wildcard-based technique to createfuzzy keyword sets. This technique eliminates the need for listing all the fuzzy keywords and the resulted size of the fuzzy keyword sets is reduced significantly. Fig. 1 [10] shows the system architecture. In whichto outsource a set of files to the cloud, the *data owner* constructs a secure searchable index for the file set and then uploads the encrypted files with the secure index on the *cloud server*. To search over the encrypted files, an authorized *user* first obtains the trapdoor from the data owner. The trapdoor is the "encrypted" version of search keyword(s). Then submits that trapdoor to the cloud server. Upon receiving the trapdoor, the cloud server executes the search algorithm on the secure indexes and gives the matched files to the user as the search results.

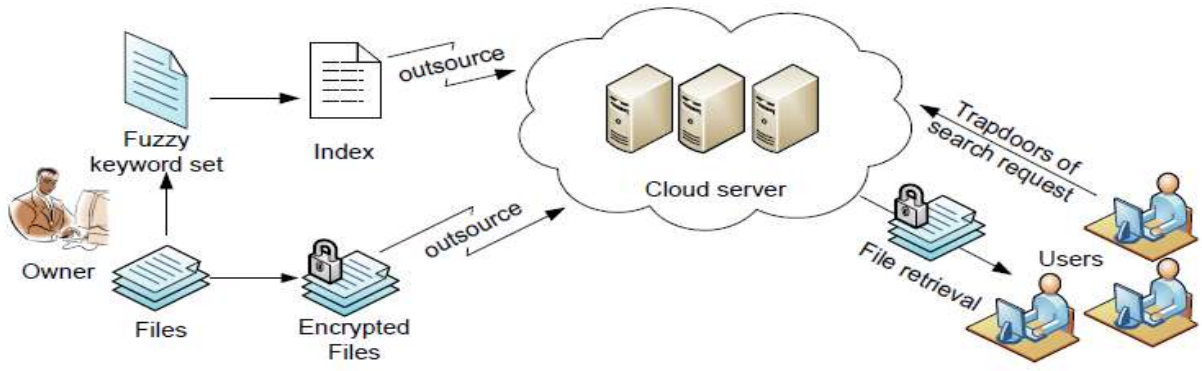

Fig. 1: Architecture of the fuzzy keyword search

2. RELATED WORK:

The concept of searches on encrypted data was first proposed by Song [1]. Song et al. [1] first introduced the concept of searchable encryption. They proposed a scheme in the symmetric key setting, in which each word in the file is encrypted individually under a special two-layered encryption construction. As a result, a searching

overhead is linear to the whole file collection length. Chang et al. [2] introduced a similar per-file index scheme. To further enhance search efficiency, Curtmola et al. [3] presenteda per-keyword based approach, in which a single encrypted hash table index is created for the entire file collection, with each entry consisting of the trapdoor of a keyword and an encrypted set of related file identifiers. Searchable encryption has also been measured in the public-key setting. Boneh et al. [4] proposedthe first public-key based searchable encryption scheme, similar to that of [1]. In their construction, anyone with the public key can write to the data stored on the server but only authorized users with the private key can search. Reminder that all these schemes support only boolean keyword search, and none of them support the ranked search problem.

Cao et al. [5] presented a privacy-preserving multi-keyword ranked search scheme in which coordinate matching is use to realize ranked search. Xu et al. [6] gives the keyword access frequencies into account during the system generation of the ranked list in the returning results and added the issue of the index update.Li et al. [12] proposed a fine-grained multi-keyword search schemes over encrypted cloud data. Their scheme allows the precise keyword search and personalized user experience which hires a classified sub-dictionaries technique to achieve better efficiency on index building, trapdoor generating and query. Wang et al. [13] presented a practical inverted index based public key searchable encryption scheme. Their scheme gives stronger security guarantee of the index and trapdoor privacy and is more efficient as compared to the existing public-key searchable encryption schemes. Fu et al. [14] constructed a user interest model for individual user by examine the users search history to allow use to retrieve relevant documents from the cloud based on his own interest.

In recent times, aiming at acceptance of both minor mistakes and format inconsistencies in the user search input, fuzzy keyword search over encrypted cloud data has been proposed by Li. et al in [10].They solved the fuzzy keyword search by utilizing edit distance to extend keyword set. Then Liu et al. [8] upgraded the scheme by reducing the index size. Chuah and Hu [7] proposed a privacy-aware bedtree based approach to support fuzzy multi-keyword search, which considered the pre-defined phrases as the single keyword. Kuzu et al. [9] presented a similarity search scheme in which minhash based on Jaccard distance used to support fault tolerant keyword search. Wang et al. [11] engaged a score table to make the scheme that support to range query.

3. CONCLUSION:

As we know, cloud computing is the latest advanced technology, a user can store his personal and private encrypted files in a cloud and can retrieve them whenever he wants. In this paper, we present the literature review on fuzzy keyword search. 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 exact match fails.

REFERANCES:

[1] D. Song, D. Wagner, and A. Perrig, Practical techniques for searches on encrypted data, in *Proc. of IEEE Symposium on Security andPrivacy'00*, 2000.

[2] Y.-C. Chang and M. Mitzenmacher, Privacy preserving keyword searches on remote encrypted data, in *Proc. of ACNS'05*, 2005.

[3] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, Searchable symmetric encryption: improved definitions and efficient constructions, in *Proc. of ACM CCS'06*, 2006.

[4] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, Public key encryption with keyword search, in *Proc. of EUROCRYP'04, volume 3027 of LNCS*. Springer, 2004.

[5] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, Privacy-preserving multi keyword ranked search over encrypted cloud data, in *Proc. IEEEINFOCOM*, pp. 829–837,Apr. 2011.

[6] Z. Xu, W. Kang, R. Li, K. C. Yow, and C.-Z. Xu, Efficient multikeyword ranked query on encrypted data in the cloud, in *Proc. 18th IEEE Int. Conf. Parallel Distrib. Syst.*, pp. 244–251Dec. 2012.

[7] M. Chuah and W. Hu, Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data, in *Proc. 31st Int. Conf.Distrib. Comput. Syst. Workshops (ICDCSW)*, pp. 273–281,Jun. 2011.

[8] C. Liu, L. Zhu, L. Li, and Y. Tan, Fuzzy keyword search on encrypted cloud storage data with small index, in *Proc. ICCCIS*, pp. 269–273,Sep. 2011.

[9] M. Kuzu, M. S. Islam, and M. Kantarcioglu, Efficient similarity search over encrypted data, in *Proc. 28th IEEE Int. Conf. Data Eng.*, Washington, DC, USA, pp. 1156–1167,Apr. 2012.

[10] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, Fuzzy keyword search over encrypted data in cloud computing, in *Proc. IEEEINFOCOM*, pp. 1–5,Mar. 2010.

[11] J.Wang, X. Yu, and M. Zhao, Privacy-preserving ranked multi-keyword fuzzy search on cloud encrypted data supporting range query,*ArabianJ. Sci. Eng.*, vol. 40, no. 8, pp. 2375–2388, 2015.

[12] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. S. Shen, Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data,*IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 3, pp. 312–325, May/Jun. 2016.

[13] B. Wang, W. Song, W. Lou, and Y. T. Hou, Inverted index based multi-keyword public-key searchable encryption with strong privacy guarantee, in *Proc. IEEE INFOCOM*, pp. 2092–2100Apr./May 2015.

[14] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, Enabling personalized search over encrypted outsourced data with efficiency improvement,*IEEE Trans. Parallel Distrib. Syst.*, to be published, doi: 10.1109/TPDS.2015.2506573.