International Innovative Research Journal of Engineering and Technology

ISSN NO: 2456-1983

International Conference on Emerging Innovation in Engineering and Technology

ICEIET-2017

An Efficient Privacy-Preserving Search System Over Encrypted Cloud Data

R.KANDHAN[1], R.ANANTHAN[2], P.TAMILSELVAN[3], MR.D.SATHYAMURTHY[4]

[1,2,3]UG Scholar, B.E. Computer Science and Engineering.
[4] Assistant Professor, Dept. of CSE.
MRK Institute of Technology, Kattumannarkoil.
[1]kandhanramalingam0@gmail.com,[2]ananthanr01@gmail.com,[3]tamilselvan.ts3@gmail.com

ABSTRACT:

As cloud computing becomes prevalent, more and more sensitive information are being centralized into the cloud. For the protection of data privacy, sensitive data usually have to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Existing techniques are focusing on multi-keyword exact match or single keyword fuzzy search. Wang's scheme was only effective for a one letter mistake in keyword but was not effective for other common spelling mistake. We propose an efficient multi-keyword ranked search scheme based on wang et al's scheme. We develop a new method of keyword transformation based on the uni-gram, which will simultaneously improve the accuracy rate and ability to handle spelling mistakes.

Index Terms: Multi-keyword, Fuzzy search, Encryption

I. INTRODUCTION

Due to the various benefits of cloud computing, various individuals and enterprises are interested in storing more sensitive data such as customers information, personal health records, emails, secret files of government to the cloud. By storing their data into the cloud, the data owners can be relieved from the burden of data storage and maintenance so as to enjoy the on-demand high quality data storage services. However, the fact that data owners and cloud server are not in the same trusted domain may put the outsourced data at risk, as the cloud server may longer be fully trusted in such a cloud environment due to some reasons, so the cloud environment may leak an information to unauthorized entities or be hacked. For retrieving the data in a most secure and privacy preserving method the keyword search techniques is used and to search the data in more efficient manner. The fuzzy keyword search is introduced. So efficiency of fuzzy keyword search is the main aspect in the security of data retrieval.

II. LITERATURE REVIEW

Under this topic we are using different kind of papers for improving our project result. The newly added traits on here is, to implement more then one misspelled word in the given keywords by using uni-gram method. To improve accuracy of search result and to enhance user searching experience it is crucial for ranking system to support multiple keyword search, as a single keyword search of an yields far too coarse results [2]. Recently, the importance of fuzzy search has receive attention in the context of plaintext searching in information retrieval community [4],[5],[6]. For privacy, several Search request Access control **ADMIN USER Cloud server**researches which works under single owner model are motivated by secure searches over encrypted cloud data but in practical cloud server not just support single owner model but also support

multi owner scheme to deal with Privacy Preserving Ranked Multi model(PRMSM) [1],[3].

III. EXISTING SYSTEM

In this section, we first describe the main steps of our scheme and subsequently discuss the differences between our scheme and the original scheme. This method is effective for a one letter mistake in keyword. Finally, we will present additional details of our scheme. In previous work they are proposed a technique called, multi-keyword exact match or single keyword fuzzy search. It is purely based on Locality-Sensitive Hashing (LSH) it relays on [18], Bloom Filtering, Bi-gram.

3.1 Disadvantages:

- It may occur more spelling mistakes in a keyword, it is not effective.
- Compulsorily need to use predefined dictionary.
- Output is not more accurate.

IV. PROPOSED SYSTEM

Here we are implementing the new techniques to improvise the features of an existing system. The newly proposed features are added in this system is, To allow multi-keyword fuzzy search scheme. We develop a new method of keyword transformation is based on Uni-gram. Then indexed the database, for provide more security with the help of Triple DES. It may provide more accuracy, neglecting the use of predefined dictionary and reduced the searching time.

4.1 Advantages:

- Fuzzy ranked search supports dynamic update.
- It provide multi data owner scheme and privacy guarantee.
- It resolve the problem of multiple mistakes in given keyword.
- User can easily update the new keywords.

V. MODULES DESCRIPTION

In this project, we are having three modules. Namely,

1. System Formation.
2. Cloud Server.
3. Data Requesting.

Now, we are going to explain the each module in briefly and the system architecture is depicted in following figure 1

Figure 1

5.1 System Formation:

System Formation is entirely related to admin processes. So it is also called as admin module.

To give an authority for user, to registration, file access permission and updating of database. The few other process of the system is given,

- By the way of Triple DES, the Encryption and Decryption are done.
- Indexing for give more effective and accurate file searching.

5.2 Cloud Server:

The system process are held at in this phase is, given as the list of below.

- It may provide search results in short time duration.
- The main storage spaces are allotted by cloud server.
- The processed data are reserved at the above mentioned storage.

5.3 Data Requesting:

This module is described on user related process as specified in system architecture. The user operations of this module is follows,

- The request from user to admin and cloud server.
- Both of the request from the user to admin and cloud storage is, for get authority and data access respectively.
- To retrieve the search results from remote server system with the help of admin to user.

CONCLUSION

As the results of this project is gives, for the first time to formalize and solve the problem of supporting efficient yet privacy-preserving fuzzy search for achieving effective utilization of remotely stored encrypted data in cloud. And also multi keyword fuzzy search system differential with new privileges is addressed.

6.1 Future Work:

For furthermore works are implement by using this paper is suggested as follows, the way input given is in the form of voice recoganization method and give a way to add other few security related properties, are implemented in this project.

6.2 Result:

The appropriate result for a cloud related search are implemented by this method. It provide effective and accurate result for encrypted cloud data searching.

REFERENCES:

[1] B. Wang. S. Yu, w. Lou, and Y. T. Hou, “Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud,” in Proc. IEEE INFOCOM. Apr/May 2014, pp. 2112-2120.

[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc. IEEE INFOCOM, Apr. 2011, pp. 829-837.
[3] W. Sun et al., "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. 8th ASIACCS, 2013, pp.71-82.
[4] Z. Xu, W. Kang, R. Li, K.C. Yow, and C.-Z. Xu, "Efficient multi-keyword ranked query on encrypted data in the cloud," in Proc. 18th IEEE Int. Conf. Parallel Distrib. Syst., Dec. 2012. Pp. 244-251.
[5] Z. Xia, X. Wang, X. Sun, and Q. Wang ,
" A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, "IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340-352, Feb. 2016, doi: 10.1109/TPDS.2015.2401003.
[6] Z. Fu, J. Shu, X. Sun, and D. Zhang, "Semantic keyword search based on trie over encrypted cloud data," in Proc. 2nd Int. Workshop Security Cloud Comput., Kyoto, Japan, Jun. 2014, pp. 59-62.
[7] Z. Fu, J. Shu, X. Sun, and N. Linge, "Smart cloud search services: verifiable keyword-based semantic search over encrypted cloud data," IEEE trans. Consum. Electron., vol. 60, no. 4, pp. 762-770, Nov. 2014.
[8] 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), Jun. 2011, pp. 273-281.
[9] C. Liu, L. Zhu, l. Li, and Y. Tan, "Fuzzy keyword search on encrypted cloud storage data with small index," in Proc. ICCCIS, Sep. 2011, pp. 269-273Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. CCS, 2006, pp. 79-88.
[11] 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, Apr. 2012, pp. 1156-1167.
[12] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1-5.
[13] J. Wang, X. Yu, and M. Zhao, "Privacy-preserving ranked multi-keyword fuzzy search on cloud encrypted data supporting range query," Arabian J. Sci. Eng., vol. 40, no. 8, pp. 2375-2388, 2015.
[14] E.-J. Goh, "Secure indexes," in Proc. Cryptol. ePrint Arch. Oct. 2003, pp. 1-19.
[15] P. Indyk and R. Motwani, "Approximate nearest neighbors: Towards removing the curse of dimensionally," in Proc. 30th ACM Symp. Theory Comput., 1998, pp. 604-613.
[16] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Commun. ACM, vol. 13, no. 7, pp. 422-426, 1970.
[17] X. Xiao, F. Li, and B. Yao, "Secure nearest neighbor revisited," in Proc. Int. Conf. Data Eng., 2013, pp. 733-744.
[18] M. Datar, N. Immorlica, P. Indyk, and V.S. Mirrokni, "Locality-sensitive hashing scheme based on p-stable distributions," in Proc. SCG, 2004, pp. 253-262.
[19] RFC. Request For Comments, accessed on Jul. 1 2016. [Online]. Available: http://www.ietf.org/rfc.html
[20] M.F. Porter, "An algorithm for suffix stripping," Program, vol. 14, no. 3, pp. 130-137, 1980.
[21] J.B. Lovins, "Development of a stemming algorithm," Mech. Transl. Comput. Linguistics, vol. 11, pp. 22-31, Mar/Jun. 1968.
[22] I.H. Witten, A, Moffat, and T.C. Bell, "Managing gigabytes: Compressing and indexing documents and images," IEEE Trans. Inf. Theory, vol. 41, no. 6, pp. 2101-2102, Nov. 1995.
[23] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. 4th Theory Cryptogr. Conf., Amsterdam, Netherlands, Feb. 2007, pp. 535-554.
[24] P. Golle, J. Staddon, and B. Waters. "Secure conjunctive keyword search over encrypted data," in Proc. 2nd Int. Conf. ACNS, Yellow Mountain, China Jun. 2004, pp. 31-45.
[25] D.X. Song, D. Wagner, and A. Perring, "Practical techniques for searches on encrypted data," in Proc. SP, 2000, pp. 44-55.
[26] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. 30th IEEE Int. Conf. Distrib. Comput. Syst., Genoa, Italy, Jun. 2010, pp. 253-262.
[27] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword search on remote encrypted data," in Proc. ACNS, 2005, pp. 442-455.
[28] J. Wang, X. Chen, X. Huang, I. You, and Y. Xiang, " Verifiable auditing for outsourced database in cloud computing," IEEE Trans. Comput., vol. 63, no. 11, pp. 3293-3303, Nov. 2015.
[29]W. Zhang, Y. Lin, and Q. Gu, " Catch you if you misbehave: Ranked keyword search results verification in cloud computing," IEEE Trans. Cloud Comput., to be published, doi: 1109/TCC.2015.2481389.
[30] 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..