International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

ENHANCED SEARCH SCHEME BASED ON EFFICIENT MULTI-KEYWORD RANKED SEARCH IN CLOUD

M. Lawanya Shri[1], Vinoth Kumar.S[2], Priya G[3]

[123]*VIT University, Vellore*

ABSTRACT

As the popularity of cloud increases, a large number of data owners were motivated for outsourcing the information to the cloud servers which will be convenient for users and also reduction in cost for managing the data. But confidential information has to be encrypted in prior to outsource the data to provide privacy and security that can be used for data retrieval through keyword based scheme. The paper provides a multiple keyword rank search technique on data encrypted that can be used to support dynamic operations such as insertion and deletion of data in document. Widely used models are vector space and TF-IDF were commonly used in combination with the query generation and construction of index. An index structure is constructed on the basis of tree and an algorithm is proposed which is depth-first search tree, a greedy algorithm that helps to provide efficiency in multiple keyword rank search. A secure algorithm called KNN is used for encrypting the query vectors and also the index. The usage of KNN algorithm also provides accurate score computation among the query vectors and indexes which are encrypted. To protect from statistical attacks, apparition words were included in the index to bind with the search result. As a special tree-based indexing structure was implemented, the proposed method will achieve more efficiency in time for search and also provides flexibility for performing insertion and deletion operations in a document. Substantial procedures were used for the demonstration of the proposed scheme for achieving greater efficiency.

I. INTRODUCTION

Distributed computing is a regular expression used to express an assorted qualities of disconnected sorts of registering thoughts that abandon awesome numeral of PCs that are associated through a constant correspondence organize that is the Internet. In science, distributed computing is the ability to run a program on many connected PCs in the meantime. The term encompass can be unsurprising to its utilization in showcasing to offer facilitated military use. Distributed computing depends on sharing of assets to achieve consistency and money related framework alike to a utility (like the power matrix) over a system. The fixates expand viability common additionally -assigned perform transmission belonging various. For instance, a distributed computing check which serves American clients amid American business timings with a particular application (e.g. email) while similar assets are getting reallocated and serve Indian clients all through Indian business timings with an extra application (e.g. web server). This component must take full favourable position of the utilization of

registering forces, therefore, diminishing environmental harm too, since less power, air softening up et cetera, is mandatory for a similar capacity. The appearance "influencing to cloud" additionally discloses to an association moving far from a customary CAPEX demonstrate that is purchasing the gave equipment and lessen in esteem it over a timeframe to the OPEX display that is utilize shared cloud transportation and pay as you utilize it. Defenders keep up that distributed computing permit Corporation to evade coordinate framework expenses and meeting point on activities that separate their organizations as and substitute of transportation. Advocates likewise keeps up that distributed computing grant plans to get their applications ought to run faster, with better reasonability and less conservation, and empower IT to all the more rapidly change belonging to meet irregular and flighty industry require.

II. PROPOSED MODEL

This paper presents some structure like tree inquiry plot that denotes the cloud structure implementation underpins many catchphrase places pursuit through performance of a report performance involving. In particular, the display generally utilized "term frequency (TF) × Inverse document frequency (IDF)" module or consolidated function record development inquiry era the give many watchword positioned seek. With a specific end goal to acquire high hunt proficiency, we develop a tree-based file structure and invension a "Greedy Depth-first Search". The secure kNN calculation denote to encode all the status question vector from the mean time warrant precise importance main figuring middle scrambled list inquiry vector. To oppose diverse assaults in various risk models, we develop two secure pursuit plots: the essential element multi-catchphrase positioned seek (BDMRS) conspire in the known cipher text display, and the improved element multi-watchword positioned look (EDMRS) conspire in the known foundation demonstrate.

- It guarantees the client to look the records that are sought much of the time utilizing rank hunt.
- It permits the client to download the record utilizing his mystery key to decode the downloaded information.
- It permits the Owner to see the transferred records and downloaded documents.
- The proposed work is intended to give not just multi-catch phrase question and exact outcome positioning, additionally dynamic refresh on archive accumulations. The plan is intended to keep the cloud server from taking in extra data about the report gathering, the list tree, and the inquiry.

Information or records can order of F= f1; f2..., fn; in the above figure they are represented three moddules they are data owner, data user, and cloud. Data owner is reponsible for the encrypte the document and it can send to the cloud. Then the cloud can storing the data. It is form in the index tree based structure in the cloud. Cloud server can be used in the semi trusted.

A user can search the data in the cloud with the help of multi keyword rank search. A user can enter the query in the search index and it retrieves the tree based structure. Search control denotes the data user involving the search and it can identified the function through decryption method. Encryption and decryption is in the cryptography objectives. Encryption means at can convert into the plaintext into the cipher text. Encryption is fully depend on the plaintext and decryption is fully based on cipher text.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

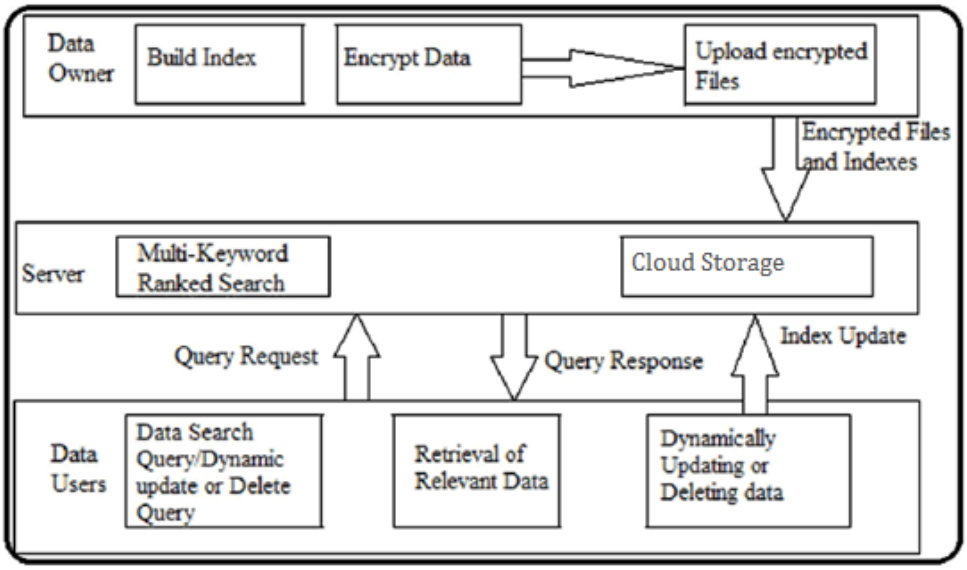

Fig 1. Proposed Architecture

- Data owner contains build index, encrypt data and finally upload the encrypted file in the cloud server.
- In server can implement like multi keyword ranked search and stored in the storage device.
- In data, user can search the data using data search query and dynamic update and delete the data in the data user module.
- User can dynamically update and delete the data in the cloud

III. DATA HOLDER MODULE

This module is used to login the user for security reason the user gives the correct user name and password. This module cans encrypt the data using RSA algorithm. The file can be arranged in the order of F=f1; f2;::::;fn and store in the cloud . All the file or document can encrypted by owner and upload in the cloud. File F can be decrypted only the user and modified can done by the owner. The automatic key generation can generate in the mail that is called secret key. When you get the secret key you can access the data in the cloud. While updating the document the owner can generate the information in the cloud user. All the data can be arranged in the index tree format. Collection of C can be arranged in the file F. Data owner can register our name, password, mail_id, role, location. User name contain the name of the user, password contain is unique identification, mail_id denote the user can receive the secret key by the mail. Role means it is the user or owner it depend on selection. Location option is used for registered location.

IV. DATA BUYER MODULE

This module is implement to using the user can search the document in the cloud. User also registers the registration form for using the identification. When the user can register they automatically generate the secret key. User can search the data and download the data but they cannot modify the data. All the download data can be representing in the form of Zip document it can be extract in the future uses. User can need the information

the owner can approve the client request. User can down the registration form and they get secret key from the mail. And the user can enter the login page they must enter the mail id, password and secret key in the mail what you get. Secret key can be change each and every time when the user can enter the user login page. If user needs any file they can send the request to the owner.

V. CLOUD HOST AND ENCODING MODULE

This module is used to help the cloud can encrypt the data by using RSA algorithm and it convert into the encrypted Zip file and the secret key can send to the mail in the user and the user can download the file. It can allow the cloud login and password to enter the cloud page. The owner can give the permission to access the data in the cloud server. All the data can be stored in the cloud. It is a top-k- ranked search data in the cloud. If the owner can update any information it can changed in the cloud itself. Encryption and decryption can handle with RSA algorithm. All the file can done and store in the cloud environment.

VI. RANK HUNT MODULE

This module is used to user can search the file in the cloud by using ranked search frequently using. In this module is mainly using downloading the file can using the secret key formation. This module is used to owner can view the uploading file and downloading files. In proposed system is designed is provide to not only the multi keyword query and also the perfect result and update the document collection. It is mainly designed for learning, extra information about the document collection.

VII. CONCLUSION AND FUTUREWORK

In this paper, a secure, efficient and dynamic search scheme is proposed, which supports not only the accurate multi-keyword ranked search but also the dynamic deletion and insertion of documents. We construct a special keyword balanced binary tree as the index, and propose a "Greedy Depth-first Search" algorithm to obtain better efficiency than linear search. In addition, the parallel search process can be carried out to further reduce the time cost. The security of the scheme is protected against two threat models by using the secure kNN algorithm. Experimental results demonstrate the efficiency of our proposed scheme.

There are still many challenge problems in symmetric SE schemes. In the proposed scheme, the data owner is responsible for generating updating information and sending them to the cloud server. Thus, the data owner needs to store the unencrypted index tree and the information that are necessary to recalculate the IDF values. Such an active data owner may not be very suitable for the cloud computing model.

REFERENCES

[1] K. Ren, C.Wang, Q.Wang*et al.*, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography and Data Security*. Springer, 2010, pp. 136–149.

[3] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[4] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," *Journal of the ACM (JACM)*, vol. 43, no. 3, pp. 431–473, 1996.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology-Eurocrypt 2004*. Springer, 2004, pp. 506–522.

[6] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, "Public key encryption that allows pir queries," in *Advances in Cryptology-CRYPTO 2007*. Springer, 2007, pp. 50–67.

[7] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Security and Privacy, 2000. S&P 2000.Proceedings.2000 IEEE Symposium on*. IEEE, 2000, pp. 44–55.

[8] E.-J. Goh *et al.*, "Secure indexes." *IACR Cryptology ePrint Archive*, vol. 2003, p. 216, 2003.

[9] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in *Proceedings of the Third international conference on Applied Cryptography and Network Security*. Springer-Verlag, 2005, pp. 442–455.

[10] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 79–88.

[11] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–5.

[12] M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in *Data Engineering (ICDE), 2012 IEEE 28th International Conference on*. IEEE, 2012, pp. 1156–1167.

[13] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in *INFOCOM, 2012 Proceedings IEEE*. IEEE, 2012, pp. 451–459.

[14] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in *IEEE INFOCOM*, 2014.

[15] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in *Applied Cryptography and Network Security*. Springer, 2004, pp. 31–45.

[16] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in *Proceedings of the First international conference on Pairing-Based Cryptography*. Springer-Verlag, 2007, pp. 2–22.

[17] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in *Proceedings of the 7th international conference on Information and Communications Security*. Springer-Verlag, 2005, pp. 414–426.

[18] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proceedings of the 4th conference on Theory of cryptography*. Springer-Verlag, 2007, pp. 535–554.

[19] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 262–267, 2011.

[20] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in *Advances in Cryptology–EUROCRYPT 2008*. Springer, 2008, pp. 146–162.

[21] E. Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in *Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography*. Springer-Verlag, 2009, pp. 457–473.

[22] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in *Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques*. Springer-Verlag, 2010, pp. 62–91.

[23] A. Swaminathan, Y. Mao, G.-M. Su, H. Gou, A. L. Varna, S. He, M.Wu, and D.W. Oard, "Confidentiality-preserving rank-ordered search," in *Proceedings of the 2007 ACM workshop on Storage security and survivability*. ACM, 2007, pp. 7–12.

[24] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+ r: Topk retrieval from a confidential index," in *Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology*. ACM, 2009, pp. 439–449.

[25] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 8, pp. 1467–1479, 2012.

[26] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in *IEEE INFOCOM*, April 2011, pp. 829–837.

[27] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*. ACM, 2013, pp. 71–82.

[28] C. Orencik, M. Kantarcioglu, and E. Savas, "A practical and secure multi-keyword search method over encrypted cloud data," in *Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on*. IEEE, 2013, pp. 390–397.