International Journal For Technological Research In Engineering
Volume 4, Issue 4, December-2016 *ISSN (Online): 2347 - 4718*

ACHIEVE HIGHER SEARCH EFFICIENCY WITH FLEXIBLE ENCRYPTION SCHEME FOR MULTI-KEYWORD RANKED SEARCH ON CLOUD ENVIRONMENTS

Vijaya Sailaja.N[1], G. Subrahmanyam[2]
[1]M. Tech Student, [2]Assistant Professor
Department of CSE, Sri Vatsavai Krishnam Raju College of Engineering and Technology, Gollalakoderu Village, Bhimavaram Mandal, West Godavari District, Andhra Pradesh, India.

ABSTRACT: presently, the huge number of data owners is interested to outsource their data into the cloud. However, sensitive data should be encrypted before outsourcing for privacy needs that obsoletes data utilization like keyword-based document retrieval. In this work, we tend to gift a secure multi-keyword ranked search theme over encrypted cloud data, which at a similar time supports dynamic update operations like deletion and insertion of documents. Specifically, the vector house model and additionally the widely-used TF×IDF model are combined among the index construction and question generation. We tend to construct a special tree-based index structure and suggest a "Greedy Depth-first Search" algorithm to make accessible efficient multi-keyword ranked search. The secure KNN algorithm is used to encode the index and query vectors, and meanwhile ensure correct relevance score calculation between encoded index and query vectors. Thus on resist applied math attacks, phantom terms are added to the index vector for blinding search outcome. As a result of the use of our special tree-based index structure, the projected scheme can achieve sub linear search time and deal with the deletion and insertion of documents flexible. Through the experiments, we can prove that the proposed system is secure and flexible to multi-keyword search.

I. INTRODUCTION

Cloud Computing, a vital pattern for advanced information services, must outsource a necessary feasibility for data Users data. Controversy on privacy, however were presented as outsourcing of sensitive data, as well as e-mail, medical records and private photos endlessly expands explosively. Reports of data loss and data breaches in cloud computing systems from time to time appear. The most vital threat to privacy roots once users source their personal data to the cloud within the cloud itself. The figure one shows the cloud service suppliers capable of the data and thus the communication between the users and therefore the cloud will, lawful or unlawful to manage and monitor. To make sure privacy, cipher users usually the data before it brings to cloud out-sourcing, the main challenges for effective data use one in all the most common ways that to do this could be through keyword-based retrieval. Keyword-based retrieval is also a typical data service and wide utilized in the text scenarios applied, where the users supported keywords retrieve relevant files during a file record. However, it turns out to be a tough task in cipher text scenario, attributable to the restricted operations on encoded data .besides to enhance feasibility and save on costs at intervals the cloud paradigm, it is desirable to the question result to obtained with the foremost necessary files in place of all the files that got to purpose the interests of users that the files are elect thus as of relevance by users' corresponding interest and alone the files with the most effective relevancy are returned for users. To date, economical multi-keyword search on encoded data remains a tough drawback. It suggests that efforts embrace the search on encoded data not only data retrieval techniques like advanced data structures wont to represent the searchable index, and economical search algorithms, that lead through the corresponding system, but additionally the proper design of security protocols to create positive the security and privacy of the complete system. The blurring the keyword is detected by an innovative system and recursive vogue, without increasing the index so a high efficiency in terms the calculation and storage.

Figure 1: Architecture of Cloud Storage

A general approach to protect the confidentiality of data is to inscribe the data before outsourcing. However, this is often a massive value in terms of data, the user expertise lead. As an example, these techniques for keyword-based data retrieval that are sometimes used on the plaintext data cannot directly access the encoded applied data. Transfer all data among the cloud and regionally to decipher, is clearly impractical. to resolve the higher than drawbacks, researchers have some general purpose solutions with completely homomorphic cryptography or blind Rams created .These ways in which are impractical due to their high procedure issue for each the cloud Sever and users. Versatile search sub linearly accomplish by planned theme Search time and touch upon the deleting and inserting of documents. The secure KNN rule is employed to encipher the index and query vector, and within the meanwhile precise which means score calculation between encoded to create certain, index and query vectors.

II. RELATED WORK

Zhang et al. projected a scheme to handle secure multi-keyword stratified search during a multi-owner model. In this scheme, different data owners use different secret keys to encoded their documents and keywords whereas authorized data users will question while not knowing keys of these totally different data owners. However; these works don't support dynamic operations. Practically, the data owner may have to update the file collection once he transfers the gathering to the cloud server. Thus, the Secure Encryption schemes are expected to support the insertion and deletion of the file. There are also many dynamic searchable cryptography schemes. In the work of Song et al., the every file is considered as a sequence of fixed length words, and is separately indexed. This scheme supports simple update operations however with low efficiency. Goh planned a theme to get a sub-index (Bloom filter) for each file supported keywords. Then the dynamic operations will be simply completed throughout update of a Bloom filter along with the corresponding file. In 2012, Kamara et al. created an encrypted inverted index that can handle dynamic data with efficiency. But, this scheme is very complex to implement. After, as an improvement, Kamara et al. Planned a new search scheme supported tree-based index, which may handle dynamic update on document data keep in leaf nodes. However, their theme is designed only for single keyword Boolean search. In Cash et al. presented a data structure for keyword/identity tuple named "TSet". Then, a document will be depicted by a series of independent T-Sets. Supported this structure, Cash et al. planned a dynamic searchable cryptography theme. In their construction, new additional tuples are kept in another database within the cloud, and deleted tuples are recorded during a revocation list. The final search results achieved through excluding tuples within the revocation list from the ones retrieved from original and new added tuples. Yet, Cash et al.'s dynamic search scheme does not recognize the multi-keyword ranked search practicality.

III. FRAME WORK

This paper proposes a secure tree based search process over the encoded cloud data that supports multi keyword ranked search and dynamic procedure on the document collection. Specifically, the vector house model and therefore the widely-used "TF ×IDF" model area unit collective inside the index-construction and query-generation to produce multi keyword ranked search. Therefore on get high search efficiency, we have a tendency to create a tree based index approach and propose a Greedy Depth initial Search technique supported this index tree. The secure KNN rule is used to write in code the index and query vectors, and meantime guarantee correct relevancy score calculation between encoded index and query vectors. To resist completely different attacks in varied threat models, we create a two secure search schemes: the essential dynamic multi-keyword ranked search scheme among the best-known cipher-text model, and additionally the improved dynamic multi keyword ranked search scheme among the notable background model. By using this model the following benefits area unit thanks to the special construction of our tree based mostly index, the projected search scheme can flexibly reach sub linear search time and trot out the insertion and of deletion file. We design a searchable cryptography scheme that supports each the right multi keyword ranked search and flexible dynamic operation on file collection. Because of the special technique of our tree based index, the search complexity of the projected approach is basically reserved to logarithmic. And in practice, the projected scheme can achieve higher search efficiency by execution our Greedy Depth initial Search technique. Moreover, similar search can be flexibly performed to any reduce the time and price of search technique.

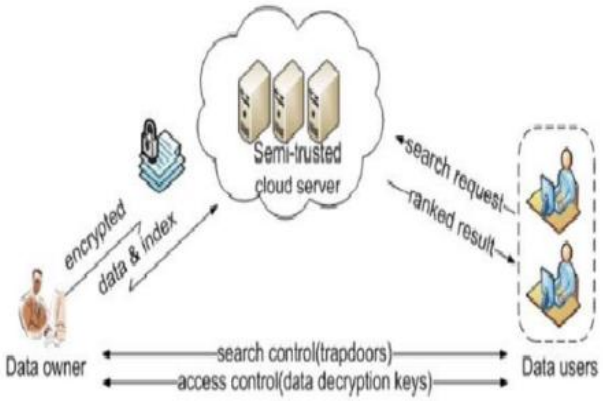


Figure 2: Architecture of Dynamic Multi Keyword Ranking Search

Data Owner contains a collection of documents that he desires to outsource to the cloud server in encrypted type whereas still keeping the flexibility to search on them for effective utilization. Afterwards, the data owner outsources the encrypted collection C and additionally the secure index I to the cloud server, and securely distributes the key data of trapdoor generation together with keyword inverse document frequency values and document cryptography to the approved data users. Moreover, the data owner is responsible for the update operation of his documents keep within the cloud server. Whereas updating, the data owner generate the update data locally and send it to the server. Data users are approved ones to access the file of data owner with t query-keywords the approved client will generate a trapdoor consistent with search control mechanisms to get k encoded document or file from cloud server. Then, the data user can decipher the documents with the shared cipher key. Cloud server stores the encoded document collection C and also the encoded searchable tree index I for data owner. Upon receiving the trapdoor from the data user, the cloud server executes search over the index tree I, and finally returns the corresponding collection of prime k ranked encoded documents. Besides, upon receiving the update data from the data owner, the server wishes to update the index I and document assortment C according to the received data. To modify secure, efficient, correct and dynamic multi data under the above models, our system has the following

Dynamic:

The projected scheme is designed to produce not only multi-keyword query and accurate result ranking, however additionally dynamic update on document collections.

Search Efficiency:
The scheme aims to realize sub linear search efficiency by explore a special tree-based index and an economical search algorithm. Privacy-preserving: The scheme is designed to prevent the cloud server from learning further data about the document collection, the index tree, and also the query. The specific privacy necessities are summarized as follows, Index Confidentiality and query.
Confidentiality:
The underlying plaintext data, including keywords within the index and query, TF values of keywords hold on within the index, and IDF values of query keywords, ought to be protected from cloud server;
Trapdoor Unlink-ability:
The cloud server should not be ready to determine whether two encrypted queries (trapdoors) are generated from an equivalent search request;
Keyword Confidentiality: The cloud server could not establish the particular keyword in query, index or document collection by analyzing the statistical data like term frequency. Note that our projected scheme is not designed to shield access pattern, i.e. the sequence of returned documents.
Greedy DFS Algorithm
Below figure shows that the Greedy Depth First Search algorithm process i.e.,

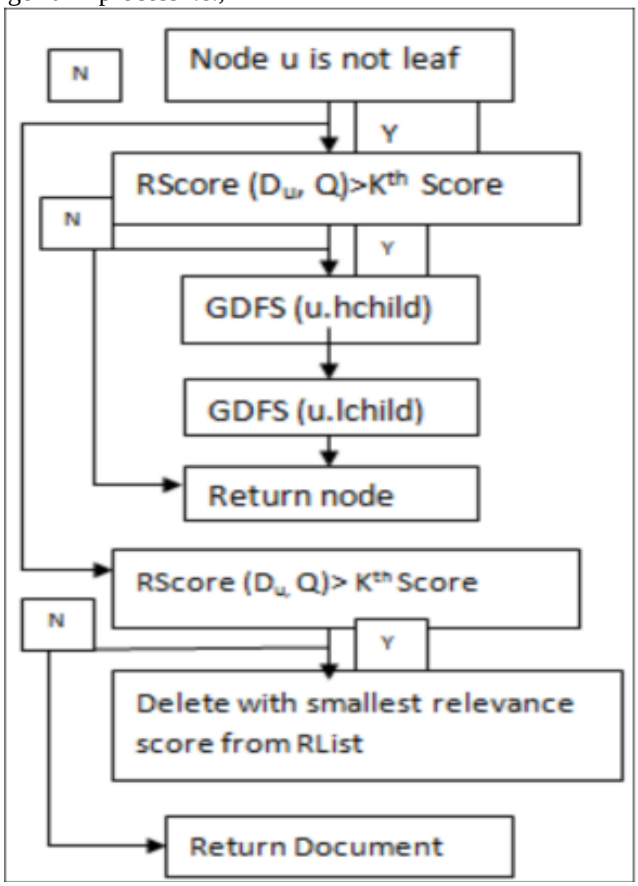
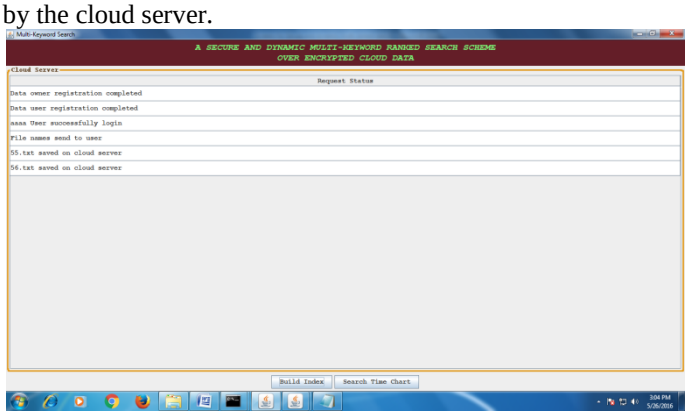


Figure3. Greedy Depth First Search Algorithm

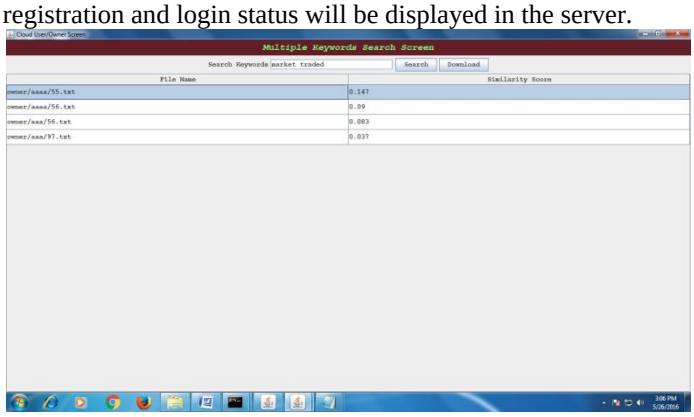
By using this Greedy DFS algorithm, we can get the better efficiency than traditional searching schemes.

IV. EXPERIMENTAL RESULTS

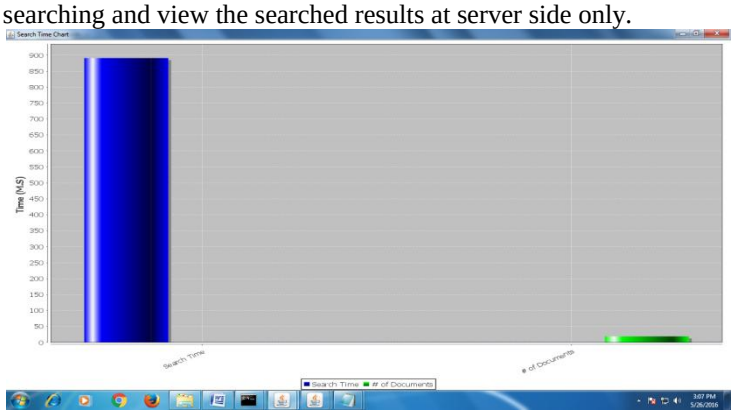
In experiments, data owner and data user must be registered in the cloud server. Their registered status will be maintained by the cloud server.



The above screen show that the data owner and data user registration and login status will be displayed in the server.



The above screen shows that the uploaded files are stored at server side only and in the form of encryption. And also user searching and view the searched results at server side only.



The above screen shows that the keyword searching time chart.

V. CONCLUSION

In this paper we describe and solve the drawback of multi key word ranked search over encrypted cloud data, and started a range of privacy requirements. Among various multi-keyword semantics, we choose the efficient similarity measure of "coordinate matching," i.e., as several equivalent as potential, to effectively capture the connation of outsourced documents to the question Keywords, and utilize "inner product similarity" to quantitatively calculate such comparison measure. So as to acquire the check of

supporting multi-keyword semantic while not privacy violation, we provide a basic plan of MRSE using secure inner product calculation. Then, we provide two improved MRSE schemes to realize numerous severe privacy desires in 2 different threat models. The any enhancements of our ranked search technique, also as supporting additional search semantics, i.e., TF x IDF, and dynamic data technique elaborate analyses in investigating privacy and efficiency assurance of projected schemes are mentioned, and testing on the real-world data set demonstrate our projected schemes that introduces low transparency on both calculation and communication.

REFERENCES

[1]. Secure Ranked Keyword Search over Encrypted Cloud Data, IEEE PAPER, 2010.
[2]. Zhihua Xia, "A Secure and Dynamic Multi keyword Ranked Search Scheme over Encrypted Cloud Data", and IEEE Transactions on Parallel and Distributed Systems, Vol: No: 99 Year 2015.
[3]. Cong Wang et al.,"Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data", IEEE Transactions on parallel and distributed systems, vol. 23, no. 8, August 2012.
[4]. 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.
[5]. S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security. Springer, 2010, pp. 136–149.
[6]. 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.
[7]. 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.
[8]. 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.
[9]. 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.
[10]. E.-J. Goh et al., "Secure indexes." IACR Cryptology e Print Archive, vol. 2003, p. 216, 2003.
[11]. 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.
[12]. 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.
[13]. 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.
[14]. Wenhai Sun et al., "Protecting Your Right: Attributebased Keyword Search with Finegrained Ownerenforced Search Authorization in the Cloud", IEEE INFOCOM 2014, Toronto, Canada, April 27 - May 2, 2014.
[15]. C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

