ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

An Efficient Privacy-Preserving Ranked Keyword Search Method over Encrypted Cloud Data.

Sai Pavan Kumar P, Yaswanth Sai P*, and Mercy Paul Selvan.

Dept of CSE, Faculty of Computing, Sathyabama University, Chennai, Tamil Nadu, India.

ABSTRACT

A protected and dynamic more-keyword related ranked search on encrypted data on cloud storage is increasing because of the cloud computing popularity; more users are provoked to store their data on cloud server for huge expedience and minimum cost in management of data. On the other hand, privacy data have to encrypted before outsource to cloud storage, that obsoletes data use like keyword related document recovery. In our proposed system, we suggest a protected multi-keyword related ranked search method on encrypted data on cloud storage, that concurrently helps dynamic operations such as interpolation and expunction of documents. Particularly, the model of vector space and more used TF-IDF method are joined in the construction of index and generation of query. We suggest a algorithm of "Greedy Depth-first search" and built a particular tree-related index scheme. The kNN technique is used to encrypt the query and index vectors, and same time assure correct significance score computation berween query vectors and index vectors. In the way to oppose the attacks related to statistical, terms of phantom are joined to the vector index for search results of blinding. Because of the use of particular tree-related structure of index, the suggested method can helps sub-linear time of search and contract with interpolation and expunction of documents lithely. Some wide-ranging testing is conducted to show the proposed system efficiency.

Keywords: GREEDY DEPTH FIRST SEARCH, KNN ALGORITHM, TRAP DOOR, SSL CERTIFICATION, ENTRYPTION, SEARCHING

Corresponding author

ISSN: 0975-8585

INTRODUCTION

Cloud is the extensive dreamed computing vision like as check, where users of cloud can faintly collect their records from the cloud storage by this way user can use the on-demand more quality services and application from shared configurable pool properties of computing [1]. The advantage given by this new model is limited to: reduce the trouble for storage space, universal access of information with independent environmental places and -minimize the hardware cost and software etc. The improving cloud computing popularity help to centralizes the more open information on the cloud storage like as e-mails, company finance information, government files and privacy health documents.

The issue between cloud server and data owner is, they are not using same domain for every time, this may gives some problems for unencrypted information [2] cloud may reveal some information to invalid users [3] or still be hacked [4]. It brings idea for that receptive information needs to be encrypted before to store for privacy of information and combating unwanted contact. Encrypting the information creates efficient information using a challenging job given that could be on more outsourced files. In addition, in cloud computing data or information owners can distribute their information with more no of users, who may would like to only get back particular information file they involved in by a given a gathering.

The best way is to achieve this task by using the keyword-related search. This type of keyword related method helps to user to exactly recover interest files and has been extensively applied in search states on plaintext. Unluckily, encrypted information, which restrict customer's ability to achieve the keyword related search and additionally stress the keyword protection privacy. It creates some issues for encrypted data. In first, ranked search that allow data user to discover the most related information fast is a more important problems. The no of information or data outsourced to cloud storage that the cloud storage should have the skill to execute search result placing to meet the command for effective data recovery [5]. Secondly, many-keyword related search is important for increase the accuracy of search result as one keyword related search frequently return a common results.

The final and important one in data managing system is update functionality that have to give as more as potential expediency to data owner. It is a normal procedure for all data owner needs update their document when they need to modify any document. So the system of data management that wants to support the deletion and insertion is more important one. In last year, more researchers have occupied in the area of searchable encryption on encrypted data and place forward some sequence of achievements. But still there are some challenging tasks wants to be achieved. To design a method that helping both multi-keyword related search and updating in dynamic are still demanding issues.

RELATED WORK

Searchable encryption in conventional way has been extensively studied as primitive of cryptographic, with center of attention on security definition efficiency and formalization improvements. The researchers Song et al, first presented searchable encryption technique. They suggested a method in the setting of symmetric key, where every word in the documents is encrypted separately by a particular two-layered encryption creation. Hence overhead in searching is linear for the whole length of file collection. Goh implemented a bloom filter-related file index, for minimizing workload for every search request relative to the no of documents in collection.

To further improve the efficiency of search mitzenmacher and chang also implemented a same per-file index method suggested a per-keyword related method, where a one encrypted index of hash table is creates for the whole file collection, with every entry containing of the keyword trapdoor in the setting of public key. Encryption in searchable has been measured in the setting of public-key. Aiming at patience of both format inconsistencies and minor types in the search input of user, fuzzy related keyword search on encrypted data has been suggested by Li et al. in [6]. Recently, a privacy-assured parallel mechanism on encrypted data has been suggested by researcher by want et al. in [7]. Reminder that all methods only Boolean related keyword search and other support the issue of ranked search which they are concentrating in this paper. In [8]

suggests a privacy preserving many keyword related ranked search method that extends their existing works in [8] with carry of many keyword query. They select the standard of "coordinate matching," i.e., as many matching as probable, to confine the match between data documents and many keyword search query and later formalize the standard by protected inner product computation method. The main drawback of the method is that cloud server has to traverse linearly to all the documents of whole index for every request of search. The researchers qin liu in [3] suggested that the gives data privacy, keyword privacy and semantic protection by public key encryption. CSP is concerned in limited decipherment by minimizing the computational and communication aerial in process of decryption for end users. The user gives the trapdoor of keyword encrypted by private key of users to CS by securely and recovery the encrypted related documents. The researcher Wenhae Sun in [6] suggested that search gives similarity related search ranking, privacy of keyword, Query and Index confidentiality and ability. The encrypted documents is creates by model of vector space sustaining distinctive and consolidate file search. Index of searchable is constructing by B tree of multidimensional. Owner builds query vector in encrypted format for keyword set. Search user receives the relevant encrypted query vector W form data owner which is used on CS side. Now CS finds index by Merkle-Damgard creations algorithm and compares file cosine measure and query vector then returns highest k-encrypted files list to user. Mercy Paul Selvan in [11] suggested an approach for multi keyword retrieval.

PROPOSED SYSTEM

Data owner:

In proposed system data owner responsible for upload data files. Here data owner contain documents collection D={d1,d2,….dn} that he/she would like to store the data on cloud server in encrypted format and at the same time, keeping the capacity to finds the documents for effective utilization. In our system, firstly data owner creates a protected searchable index of tree I form the collection of documents D, and then creates a document collection in encrypted format C for D. Then data owner outsource their data C with Index I to cloud server, and send the trapdoor information generation to valid data user by secure way. In addition data owner is also responsible for interpolation and expunction updating operations of her/his documents in cloud server. When updating time data owner update the information in local and forward it to cloud server.

Data users:

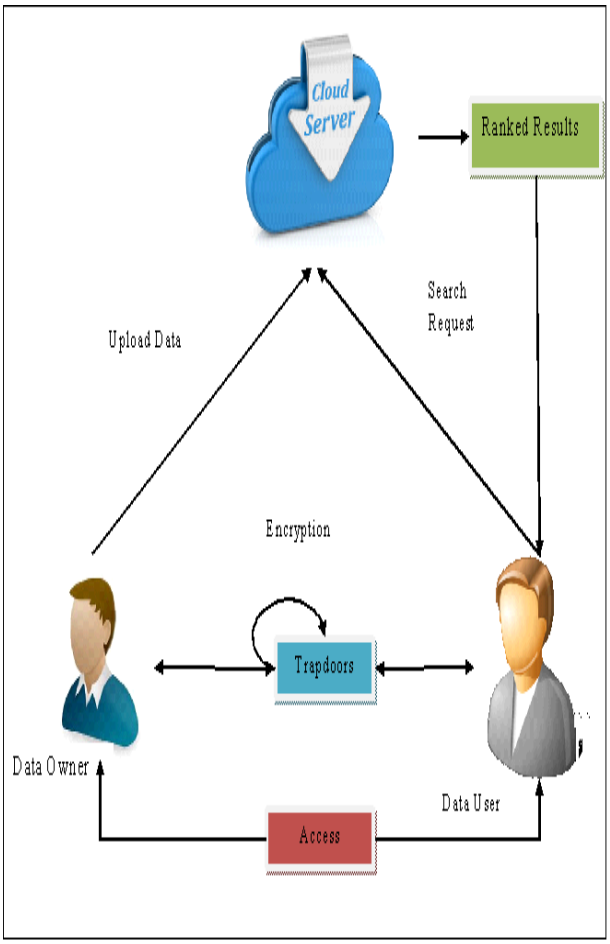
Data users are valid persons to access the data owner data or documents. With using the t query keywords, the valid user can creates a trapdoor TD relating to mechanisms of search control to obtain k encrypted data or documents from server. Then data user can easily decrypt the documents using the distributed secret key.

Cloud server

Cloud server is responsible for storing the encrypted documents C and tree Index of I by the data owner. By receiving the TD form the data user, cloud server searches the documents related to the index tree I, and lastly returns the relating collection of most k- ranked documents. In addition when ever data owner updates any information to any documents, the cloud server wants to update the index of I and collection of documents of C related to the receiving information.

Cipher-text process: In this process, cloud server only keeps the encrypted document collection C, index tree I, and TD give the user.That is why to say, the cloud server can behavior COA (cipher-text-only) in the model.

ISSN: 0975-8585



. **Figure 1:Cloud Server**

SECURE AND EFFICIENT MULTI-KEYWORD SEARCH OVER ENCRYPTED CLOUD DATA:

In cloud storage users who do not have previous information of encrypted data, have to process every recovery file in place to search most suitable their interest; On the further move, recovering all files related to the keyword of query create unnecessary traffic in network, which is more undesirable in today pay service of cloud archetype. In our proposed system specific and solved the issue of powerful yet secure and sound rank related keyword search on encrypted data. The ranked search greatly improves usability of systems by return the similar files in ranking order related to the particular significance keyword thus helping for reasonable consumption of data hosting of privacy preserving on cloud computing . In our proposed system it solves some challenging issues of multi-keyword related privacy-preserving ranked search on encrypted data (MRSE) [2], and creates a set of severe privacy requirements for cloud data utilization system. The suggested ranking process proves to be effective for searching the related documents in cloud storage.

ALGORITHM

RSA is algorithm used for decryption and encryption of data. Basically it is a public key technique; in this encrypted data could be sending without the secret key exchange. It is also used for message sign. In early requirements the TPA and user creates their own public key and private key with reverence by the RSA algorithm. Public keys want to be distributed between them by SLA or some ways for encrypting message. The private key is used for decrypting message.

With the respect of the RSA algorithm, the user needs to select two relevant prime numbers v1 and u1 with these, following standards are calculated. n1= v1 * u1 fn1 = (v1-1) * (u1-1) Then, α1 is chosen as public

ISSN: 0975-8585

key. So, TPA private key is: β1 = (1/α1) % fn1 likewise, the user chooses his/her own relevant prime numbers v2 and u2 with these public and private key of user is calculated as: n2 = v2 * u2 fn2 = (v2-1) * (u2-1) The α2 is stated as user public key. So the user private key is: β2 = (1/α2) % fn2 Now, TPA key set is: { α1, n1}, {β1, n1} user key set is: {α2, n2}, {β2, n2} with the created sets of public key is exchanged among TPA and the user.

RESULT AND DISCUSSION

COMPUTATION TIME

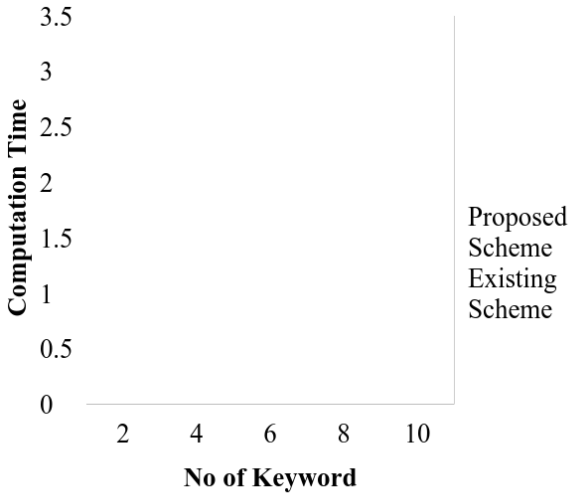


Figure 2:Computation Time

Fig.2 shows computation time. Based on number of keywords the computation time will change. When compare to existing scheme the proposed scheme has better computation time.

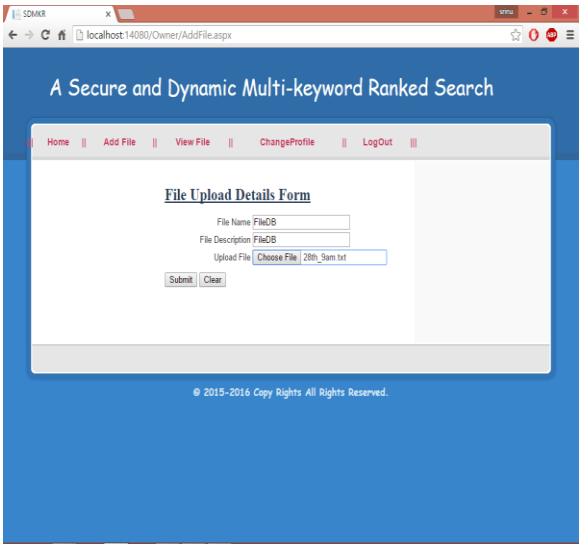


Figure 3: File Upload

Fig. 3 shows file upload. The data owner has to choose file to upload into the cloud server before that the data owner have to register with cloud server.

ISSN: 0975-8585

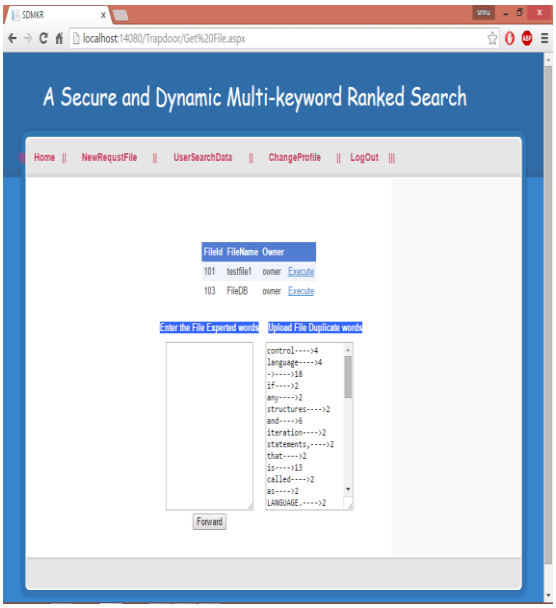


Figure 4: Trapdoor

Fig.4 shows Trapdoor. The trapdoor encrypts the data before uploading in to the cloud server. It converts the original data into duplicate words.

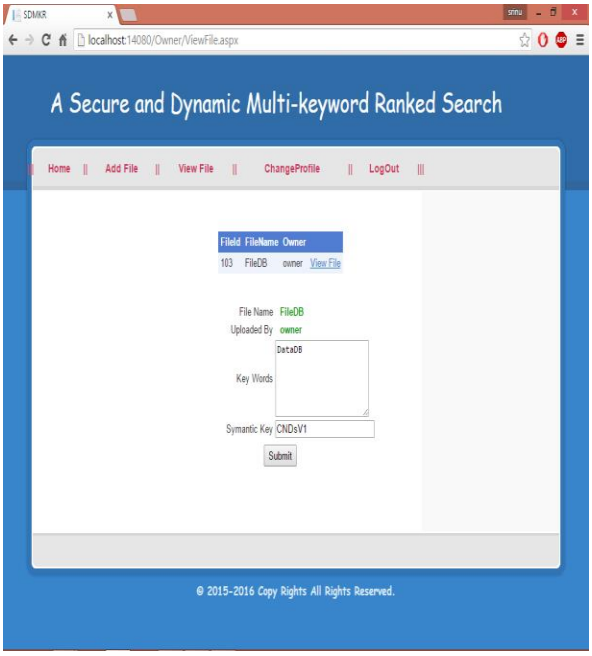


Figure 5:Data User

Fig. 5 shows Data user. By using Symantec key the data owner search the file to download from the cloud server. The data user get the Symantec key from the trapdoor.

CONCLUSION

ISSN: 0975-8585

Our proposed system supports the secure and dynamic search method; it not only supports the multi-keyword ranking search also the updating operation like interpolation and expunction of documents. We builds a particular keyword related binary tree as index, and suggests a "Greedy Depth-first search" technique to get better competence than linear search. In extra, the process of parallel search can be accepted out to minimize the cost of time. The scheme security is confined against besides two threat methods by the secure kNN technique. Our experimental results show the effectiveness of our suggested system.

REFERENCES

[1] N. Cao, Lou, J. Li and C. Wang, "Secure ranked keyword search over encrypted cloud data," Proc. IEEE 30th Int'l Conf.. Distributed computing systems, 2010.

[2] Cloud security alliance "Security guidance for critical areas of focus in cloud computing," http://www.cloudsecurityalliance.org, 2009. 10. Z. Slocum, "Your google docs: soon in search results?" http://news.cnet.com/8301-17939_109-10357137-2.html, 2009.

[3] B.Kerbs, "Payment processor breach may be largest ever,'' http://voices.washingonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html, Jan. 2009.

[4] K. Ren, C. Wang, W. Lou and N. Cao "Enabling Secure And Efficient Ranked Keyword Search Over Outsourced Cloud Data", IEEE Transactions on parallel and distributed systems, volume. 23, issue 8, **(2012)** August, pp. 1467–1479.

[5] W. Lou, J. Li, Q. Wang and J. Li "Fuzzy keyword search over encrypted data in cloud computing," Proc. IEEE Infocom '10, 2010

[6] S. Yu, C. Wang, K. Mahendra and R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," Proc. Ieee Infocom, 2012.

[7] N. Cao and W. Lou "Privacy-preserving multi-keyword ranked search over encrypted cloud data", Proc. Ieee Infocom '11, 2011.

[8] Bargav Jayaraman , "Privacy preserving string pattern matching on outsourced data".

[9] Q. Wang, J. Li, W. Lou and K. Ren "Fuzzy keyword search over encrypted data in cloud computing," Proc. Ieee Infocom '10, 2010.

[10] Wenhai Sun et al, "Privacy-Preserving multikeyword text search in the cloud supporting similarity-based ranking", the 8th ACM Symposium on information, Computer and communications security, Hangzhou, China, May 2013.

[11] Mercy Paul Selvan, A. Chandra Sekar and K. kousalya, "An Approach Towards Secure Multi Keyword Retrieval", Journal of Theoretical & Applied Information Technology 85(1), 2016.