Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 6, June -2017

# Multiple-Keyword Ranking Search Over encrypted Data with Secure and Dynamic Operation.

[1]Mr. Santosh Yadavrao Divekar ,[2]Prof.Rajesh N. Phursule.

[1,2] *Dept.Of Computer Engineering,Imperial College of Engineering and Research Pune, India*

**Abstract** — *A Secure and Dynamic Multi-keyword Ranked explore Scheme over Encrypted Cloud Data Due to the increasing regard of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data operation like keyword-based essay retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic up-date operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TFIDF model are combined in the index construction and query generation. We construct a special tree-based index structure and propose a Greedy Depth-first Search algorithm to provide efficient multi-keyword ranked search. The locked KNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure perfect importance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are extra to the index vector for blind search results. Due to the use of our special tree-based index structure, the proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme.*

***Keywords***- *Searchable encryption, multi-keyword ranked search, dynamic data operation, cloud computing.*

## I. INTRODUCTION

Allotted computing has been considered as one more model of huge trade IT base, which can sort out monstrous asset of processing, stockpiling and functions, and empower clients to appreciate pervasive, high quality and on-curiosity approach entry to an original pool of configurable registering assets with uncommon efficiency and negligible economic overhead. Pulled in by means of these enticing add-ons, each humans and undertakings are spurred to outsource their expertise to the cloud, alternatively than acquire programming and apparatus to take care of the know-how themselves. Regardless of the exclusive facets of curiosity of cloud administrations, outsourcing sensitive knowledge, (for example, messages, character wellbeing documents, organization finance know-how, government documents, and so on.) to faraway servers brings protection considerations. The cloud govt supplier (CSPs) that keep the understanding for clients could get to purchasers' moody information without approval. A general option to take care of cozy the knowledge confidentiality is to encode the know-how earlier than outsourcing. Be that as it'll, this may occasionally convey about an colossal fee as regards understanding ease of use. For request, the present systems on magical word centered data.

Constitution of cloud computing are greatly used on the plaintext information, can't be frankly useful on the encrypted data. Downloading all the knowledge from the cloud and decrypt close by means of is certainly impractical. With the intention to tackle the above challenge, researchers have designed some basic-purpose options with utterly-homomorphic encryption or ignorant RAMs. Nonetheless, these methods are usually not sensible because of their excessive computational overhead for each the cloud sever and person. On the opposite, extra practical distinctive- rationale options, comparable to searchable encryption (SE) scheme have made specific contributions in phrases of efficiency, functionality and safety. Searchable encryption schemes enable the patron to retailer the encrypted information to the cloud and execute keyword search over ciphertext area. Up to now, profuse works have been proposed below exceptional risk items to reach quite a lot of search functionality, similar to single key phrase search, similarity search, multi-keyword boolean search, ranked search, multi-keyword ranked search, and so on. With them, multi- key phrase ranked search achieves increasingly interest for its practical applicability. Just lately, some dynamic schemes had been proposed to aid inserting and deleting operations on record collection. These are significant works as it is particularly feasible that the info owners have got to replace their knowledge on the cloud server. However few of the dynamic schemes support efficient multi- key phrase ranked search.

 

## II .LITRATURE SURVEY

**1] Practical Techniques for Searches on Encrypted Data**
Authors: Dawn Xiaodong Song
It's desirable to store knowledge on data storage servers such as mail servers and file servers in encrypted type to reduce security and privacy risks. However this often implies that one has to sacrifice functionality for safety. For instance, if a client desires to retrieve best documents containing certain words, it was not earlier recognized how one can let the data storage server participate in the hunt and answer the query without loss of knowledge confidentiality. On this paper, we describe our cryptographic schemes for the challenge of shopping on encrypted information and provide proofs of protection for the ensuing crypto programs. Our techniques have a number of vital benefits. They are provably at ease: they furnish provable secrecy for encryption, in the experience that the untrusted server cannot gain knowledge of something in regards to the plaintext when simplest given the ciphertext; they provide query isolation for searches, which means that the untrusted server cannot learn something extra about the plaintext than the search effect; they furnish managed looking, so that the untrusted server cannot seek for an arbitrary phrase without the consumer's authorization; they also support hidden queries, in order that the person could ask the untrusted server to seek for a secret phrase without revealing the word to the server. The algorithms we gift are easy, fast (for a document of size n, the encryption and search algorithms most effective need O(n) flow cipher and block cipher operations), and introduce nearly no house and communication overhead, and for that reason are realistic to use today.

**2] Public Key Encryption That Allows PIR Queries**
Authors: Dan Boneh
Consider the subsequent main issue: Alice needs to carry here mail utilizing a storage-supplier Bob (such as a Yahoo! Or hot mail electronic message account). This storage-supplier ought to furnish for Alice the potential to gather, retrieve, search and delete emails however, even as, ought to learn neither the content material of messages dispatched from the senders to Alice (with Bob as Associate in Nursing middleman), nor the search standards utilized by Alice. A trivial resolution is that messages can doubtless be dispatched to Bob in encrypted kind and Alice, whenever she needs to hunt for a few message, can raise Bob to ship her replica of the whole info of encrypted emails. This withal is hugely inefficient. We are going to be fascinated with choices that are account economical and, while, respect the privacy of Alice. During this paper, we have a tendency to show the way to produce a public-key secret writing theme for Alice that allows PIR browsing over encrypted files. Our answer is that the initial to disclose no partial experience regarding the consumer's search (including the entry sample) within the public-key surroundings and with non-trivially tiny communication complexness. This provides a theoretical choice to a state of affairs posed by method of Boneh, DiCrescenzo, Ostrovsky and Persiano on "Public-key secret writing with keyword Search." The principal technique of our answer in addition makes it doable Single-Database PIR writing with sub-linear account complexness, that we have a tendency to bear in mind of freelance interest.

**3] Public Key Encryption with keyword Search**
Authors: Dan Boneh
We study the matter of looking out on knowledge that's encrypted employing a public key system. Take into account user Bob WHO sends email to user Alice encrypted below Alice's public key. Associate in Nursing email entryway desires to check whether or not the e-mail contains the keyword \urgent" so it might route the e-mail consequently. Alice, on the opposite hand doesn't would like to present the entryway the flexibility to decipher all her messages. We have a tendency to outline and construct a mechanism that allows Alice to produce a key to the entryway that allows the entryway to check whether or not the word \urgent" could be a keyword within the email while not learning the rest concerning the e-mail. we have a tendency to visit this mechanism as PublicKey coding with keyword Search. As another example, take into account a mail server that stores varied messages publically encrypted for Alice by others. Mistreatment our mechanism Alice will send the mail server a key that may modify the server to spot all messages containing some special keyword, however learn nothing else. We have a tendency to outline the idea of public key coding with keyword search and provide many constructions.

**4] A Fully Homomorphic Encryption Scheme**
**Author:** Craig Gentry
We propose the first absolutely homomorphic coding theme, resolution a central open downside in cryptography. Such a theme permits one to figure whimsical functions over encrypted knowledge while not the secret writing key – i.e., given encryptions E(m1),...,E(mt) of M1,...,mt, one will efficiently figure a compact ciphertext that encrypts f(m1,...,mt) for any efficiently calculable operate f. This downside was exhibit by Rivest et al. in 1978. Absolutely homomorphic coding has various applications. as an example, it allows non-public queries to a look engine – the user submits associate degree encrypted question and therefore the program computes a compendious encrypted answer while not ever staring at the question within the clear. It conjointly allows looking on encrypted knowledge – a user stores encrypted files on a distant file server and may later have the server retrieve solely files that (when decrypted) satisfy some Boolean constraint, even if the server cannot decode the files on its own. A lot of broadly speaking, absolutely homomorphic coding improves the efficiency of secure multiparty computation.

 

## III. PRAPOSED SYSTEM:

A dynamic searchable coding theme whose change operation will be completed by cloud server solely, in the meantime reserving the power to support multi-keyword hierarchal search. If it's required to revoke a user during this theme, we want to reconstruct the index and distribute the new secure keys to all or any the licensed users.

### 3.1 System Model

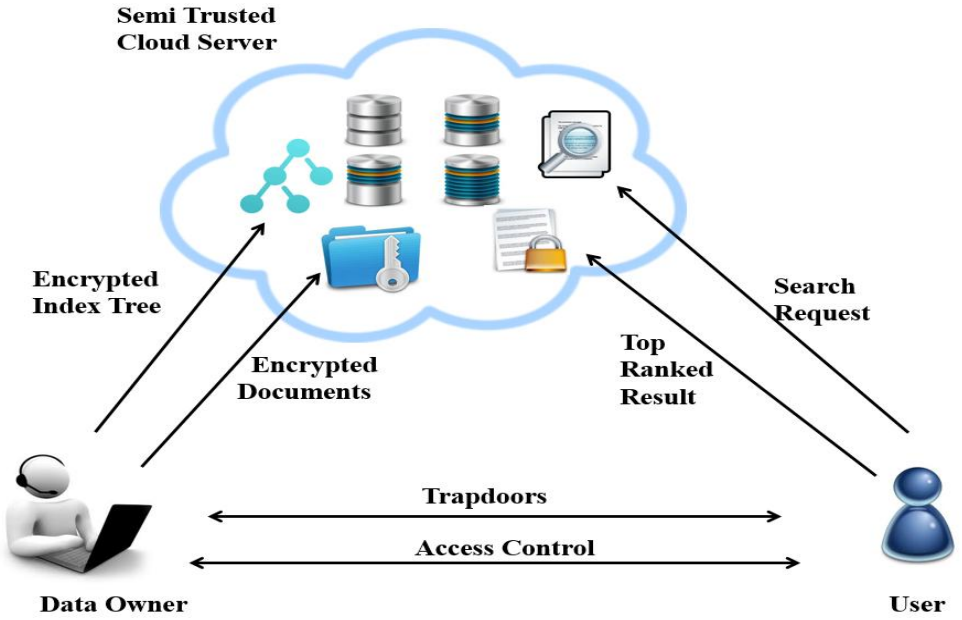


***Figure 1 System Architecture***

The system model during this paper incorporates 3 clear substances: information homeowners, information user and cloud server, as illustrated in Figure one.

There are a unit multiple information owner in system As information owner incorporates a gathering of records F = that he has to source to the cloud server in encoded structure whereas up 'til currently keeping the flexibility to ascertain on them for convincing utilization. information owner first manufactures a secure searchable tree index I from archive accumulation F, and a brief time later makes an encrypted document gathering C for F. a short span later, the info owner outsources the encoded accumulation C and therefore the secure index I to the cloud server, and safely disseminates the key information of trapdoor era and document decoding to the approved information users. In addition, the info owner is aware of his documents hold on within the cloud server. Whereas change, the information owner creates the upgrade information domestically and sends it to the server can also perform data dynamic operations on files.

Data user's area unit approved ones to induce to the archives of knowledge owner. With t question keywords, the approved user will produce a trapdoor TD as indicated by search management mechanisms to induce k encrypted documents from cloud server. By then, decode the documents with the shared secret key.

Cloud server stores the encrypted document accumulation C and therefore the encrypted searchable tree index I for information owner. Within the wake of tolerating the trapdoor TD from the info user, look over the index tree I, finally offers back the relating gathering of top-k settled encoded reports. Also, within the wake of tolerating the update data from the info owner, the server has to update the index I and document gathering C as per the received data.

After insertion or deletion of a record, we have a tendency to need change synchronously the index. Since the index of DMRS theme is planned as a balanced binary tree, the dynamic operation is finished by redesigning hubs within the list tree. The report on record is simply visible of archive acknowledges, and no entrance to the substance of records is needed

## IV. CALCULATION

**Step1: Initialization**

-The data owner randomly generates the secret key $K = (S;M1;M2)$

Where, $S$ is a $(m+1)$-dimensional binary vector.

-$M1$ and $M2$ are two $(m + 1) \times (m + 1)$ invertible matrices.

-Data owner sends $(K; sk)$ to search users through a secure channel, *sk-SECRET KEY.*

 

**Step 2: Index Building**

- The data owner firstly utilizes symmetric encryption algorithm (e.g., AES) to encrypt the document collection ($F1; F2; \cdots ; FN$) with the symmetric key $sk$.
-Ecrypted Document is $Cj(j = 1; 2; \cdots ;N)$.
- Data owner generates an $m$-dimensional binary vector $P$ according to
$Cj(j = 1; 2; \cdots ;N)$, where each bit $P[i]$ indicates whether the encrypted document contains the keyword $wi$, i.e., $P[i] = 1$ indicates yes and $P[i] = 0$ indicates no. Then she extends $P$ to a $(m + 1)$-dimensional vector $P'$, where $P'[m + 1] = 1$.
- If $S[i] = 0(i = 1; 2; \cdots ;m + 1)$, $pa[i]$ and $pb[i]$ are both set as $P'[i]$;
If $S[i] = 1(i = 1; 2; \cdots ;m + 1)$, the value of $P'[i]$ will be randomly split into $pa[i]$ and $pb[i]$ ($P'[i] = pa[i]+pb[i]$).
- Then, the index of encrypted document $Cj$ can be calculated as
$Ij = (paM1; pbM2)$.
-Data owner send $Cj \,||FIDj\,||Ij$ $(j = 1; 2; \cdots ;N)$ to cloud.

**Step 3: Trapdoor Generation**

- The search user firstly generates the keyword set f$W$ for searching. Then, she creates a $m$-dimensional binary vector $Q$ according to f$W$, i.e., $Q[i] = 1$ indicates yes and Q[$i$] = 0 indicates no
- The search user extends $Q$ to a $(m + 1)$-dimensional vector $Q'$, where
$Q'[m + 1] = -s$
- The search user chooses a random number r > 0 to generate $Q'' = r \cdot Q'$. Then she splits $Q''$ into two $(m + 1)$ vectors $(qa; qb)$: if $S[i] = 0(i = 1; 2; \cdots ;m + 1)$, the value of $Q''[i]$ will be randomly split into $qa[i]$ and $qb[i]$.

- $S[i] = 1(i = 1; 2; \cdots ;m + 1)$, $qa[i]$ and $qb[i]$ are both set as $Q''[i]$.

**Step4: Query**

- With the index $Ij(j = 1; 2; \cdots ;N)$ an, the cloud server calculates the query result as:

$$\begin{aligned} R_j = I_j \cdot T_{\widetilde{W}} &= (p_a M_1, p_b M_2) \cdot (M_1^{-1} q_a, M_2^{-1} q_b) \\ &= p_a \cdot q_a + p_b \cdot q_b = P' \cdot Q'' \\ &= rP' \cdot Q' = r \cdot (P \cdot Q - s) \end{aligned}$$

## V. ACKNOWLEDGMENT

We might need to convey the analysts and additionally distributers for creating their assets accessible. We tend to in addition appreciative to commentator for his or her vital recommendations what is more conveying the college powers for giving the duty-bound base and backing.

## VI CONCLUSION

In this paper, a safe, effective and dynamic search theme is planned, that underpins the precise multi-keyword hierarchic search furthermore because the dynamic deletion and insertion of documents. We tend to assemble a special keyword balanced binary tree because the index, and propose a "Greedy Depth-first Search" formula to amass preferred effectiveness over linear search. Likewise, the parallel search procedure may be completed to any reduce the time value. The plan's security is ensured against 2 risk models by utilizing the safe kNN formula. Trial results show the potency of our planned theme. Within the planned theme, the knowledge man of affairs is accountable of manufacturing overhauling data and causation them to the cloud server. Consequently, the info owner has to store the un-encrypted index tree and data that are necessary to cipher the force values.
Such a vigorous information owner might not be astoundingly appropriate for the condemned distributed computing model. It may be a vital nonetheless hard future work to style a dynamic searchable secret writing theme whose change operation may be completed by cloud server solely. What is more, because the giant portion of works concerning searchable secret writing, our theme in the main considers the take a look at from the cloud server.

## VII REFRENCES

[1] 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.
[2] 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.
[3] 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.

 

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

 