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 1, January -2017

# Review on Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data

Tarika P. Jawale. Prof. R.B. Mapari.

*G.S.Mandal's MIT Aurangabad.*

**Abstract** — *A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data Due to the expanding fame of cloud computing, more data owners are spurred to outsource their data to cloud servers for incredible accommodation and diminished expense in data management also can perform data dynamic operations on files. On the other hand, sensitive data ought to be encrypted before outsourcing for security prerequisites, which obsoletes data use like keyword-based document retrieval. A protected multi-keyword ranked search scheme over encrypted cloud data, which all the while underpins element update operations like deletion and insertion of documents. In particular, the vector space model and the generally utilized TF_IDF model are consolidated as a part of the index development and query generation.A unique tree-based index structure using a "Greedy Depth-first Search" algorithm to give proficient multi-keyword ranked search. The secure kNN algorithm is used to encrypt the index and query vectors, and then guarantee precise importance score figuring between encrypted index and query vectors. With a specific end goal to oppose measurable attacks, phantom terms are added to the index vector for blinding search results. Because of the utilization of our exceptional tree-based index structure.*

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

## I. INTRODUCTION

CLOUD computing has been considered as another model of enterprise IT infrastructure, which can compose gigantic resource of computing, storage and applications, and empower users to appreciate pervasive, helpful and on-demand network access to a mutual pool of configurable computing resources with incredible efficiency and insignificant economic overhead [1]. Pulled in by these engaging features, both individuals and enterprises are roused to outsource their data to the cloud, rather than buying software and hardware to deal with the data themselves.

In spite of the different points of interest of cloud services, outsourcing delicate information, (for example, e-mail, individual health records, organization account information, government archives, and so forth.) to remote servers brings privacy concerns. The cloud service providers (CSPs) that keep the data for users may access users' sensitive information without authorization. A general way to deal with secure the data privacy is to encrypt the data before outsourcing [2].

On the other hand, this will bring about a gigantic expense in terms of data ease of use. For example, the current techniques on keyword-based information retrieval, which are broadly utilized on the plaintext data, can't be straightforwardly connected on the encrypted data. Downloading all the data from the cloud and decrypt locally is clearly unrealistic.

With a particular final objective to address the above issue, analysts have illustrated some all-around helpful arrangements with totally homomorphic encryption [3] or missing RAMs [4]. In any case, these schedules are not down to earth in light of their high computational overhead for both the cloud server and user. In spite of what may be normal, more useful unique reason arrangements, for instance, searchable encryption (SE) plan have made specific responsibilities to the extent productivity, value and security. Searchable encryption scheme engage the user to store the encrypted data to the cloud and execute unequivocal word look for over cipher text domain. As being what is indicated, abundant works have been proposed under assorted risk models to finish distinctive interest value, for instance, single keyword search, closeness look, multi-keyword Boolean search, ranked search, multi-keyword ranked search, etc. Among them, multikeyword positioned quest finishes more thought for its pragmatic propriety. Starting late, some component arrangements have been reinforce embedding and erasing operations on archive gathering. These are colossal goes about as it is exceptionally possible that the data owner need to overhaul their data on the cloud server. Yet, few of the dynamic plan support successful multikeyword situated look. Inverse document recurrence (IDF)" model are joined in the list development and inquiry era to give multi keyword positioned seek. Keeping in mind the end goal to get high search Effectiveness, we develop a tree based list structure using a "Greedy Depth-first Search" calculation based on this list tree. Because of the uncommon structure of our tree-based list, the search scheme can flexibly accomplish sub-straight search time and manage the deletion and insertion of reports. The protected kNN algorithm is used to encrypt the index and query vectors, and in the interim guarantee relevance score calculation between encrypted index and query vectors. To oppose distinctive attacks in different threat models, we build two secure search schemes: the basic dynamic multi-keyword ranked search (BDMRS) scheme in the known ciphertext model, and the enhanced dynamic multi-

 

keyword ranked search (EDMRS) scheme in the known background model. Our commitments are condensed as takes after:

1) Design a searchable encryption scheme that underpins both the precise multi-keyword ranked search and flexible dynamic operation on document collection for multiple data owner environment.

2) Due to the uncommon structure of our tree-based index, the search complexity is in a general sense kept to logarithmic. What's more, practically speaking, the scheme can accomplish higher search proficiency by executing our "Greedy Depth-first Search" algorithm. Additionally, parallel search can be flexibly performed to further lessen the time cost of inquiry procedure.

## II. LITRATURE SURVEY

**1] Fuzzy Keyword Search over Encrypted Data in Cloud Computing**
Authors: JaydipSen

In this paper, for the primary time a tendency to formalize and solve the matter of effective fuzzy keyword search over encrypted cloud information whereas maintaining keyword privacy. Fuzzy keyword search greatly enhances system usability by returning the matching files once users' looking out inputs specifically match the predefined keywords or the highest doable matching files supported keyword similarity linguistics, once precise match fails. In our answer, we have a tendency to exploit edit distance to quantify keywords similarity and develop a complicated technique on constructing fuzzy keyword sets, that greatly reduces the storage and illustration overheads. Through rigorous security analysis, we have a tendency to show that our projected answer is secure and privacy-preserving, whereas properly realizing the goal of fuzzy keyword search.

**2] Practical Techniques for Searches on Encrypted Data**
Authors: Seny Kamara

In this paper, a tendency to describe our science schemes for the matter of looking on encrypted knowledge and supply proofs of security for the ensuing crypto systems. Our techniques have variety of crucial blessings. they're incontrovertibly secure: they supply obvious secrecy for cryptography, within the sense that the untrusted server cannot learn something regarding the plaintext once solely given the ciphertext; they supply question isolation for searches, that means that the untrusted server cannot learn something a lot of regarding the plaintext than the search result; they supply controlled looking, so the untrusted server cannot look for AN discretional word while not the user's authorization; they additionally support hidden queries, so the user could raise the untrusted server to go looking for a secret word while not revealing the word to the server.

**3] A FULLY HOMOMORPHIC ENCRYPTION SCHEME**
Authors: Reza Curtmola, Juan Garay

In this Paper propose the first completely homomorphic encryption scheme, taking care of a focal open issue in cryptography. Such a plan permits one to figure subjective capacities over encypted data without the decoding key – i.e., given encryptions E(m1),...,E(mt) of m1,...,mt, one can efficiently process a smaller ciphertext that encrypts f(m1,...,mt) for any efficiently calculable capacity f. This issue was postured by Rivest et al. in 1978. Completely homomorphic encryption has various applications. For instance, it empowers private queries to a search engine– the user presents an encypted query and the search engine processes a brief encrypted answer while never taking a gander at the query in the clear. It likewise empowers looking on encrypted data – a user stores encypted files on a remote file server and can later have the server recover just files that (when decoded) fulfill some boolean limitation, despite the fact that the server can't unscramble the files all alone. All the more comprehensively, completely homomorphic encryption enhances the efficiency of secure m.

**4] Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions**
Authors: Dan Boneh

In this paper we have a tendency to show 2 solutions to SSE that at the same time relish the subsequent properties:

1. Each solutions ar a lot of economical than all previous constantround schemes. specially, the work performed by the server per came back document is constant as hostile linear within the size of the info.

2. Each solutions relish stronger security guarantees than previous constant-round schemes. In fact, we have a tendency to illustrate delicate however serious issues with previous notions of security for SSE, and show the way to style constructions that avoid these pitfalls. Further, our second answer additionally achieves what we have a tendency to decision reconciling SSE security, wherever queries to the server may be chosen adaptively (by the adversary) throughout the execution of the search; this notion is each necessary in observe and has not been antecedently thought of.

 

## III. ARCHITECTURE DESIGN:

A dynamic searchable encryption scheme whose updating operation can be completed by cloud server only, meanwhile reserving the ability to support multi-keyword ranked search. If it is needed to revoke a user in this scheme, we need to rebuild the index and distribute the new secure keys to all the authorized users.

.

### 3.1 System Model

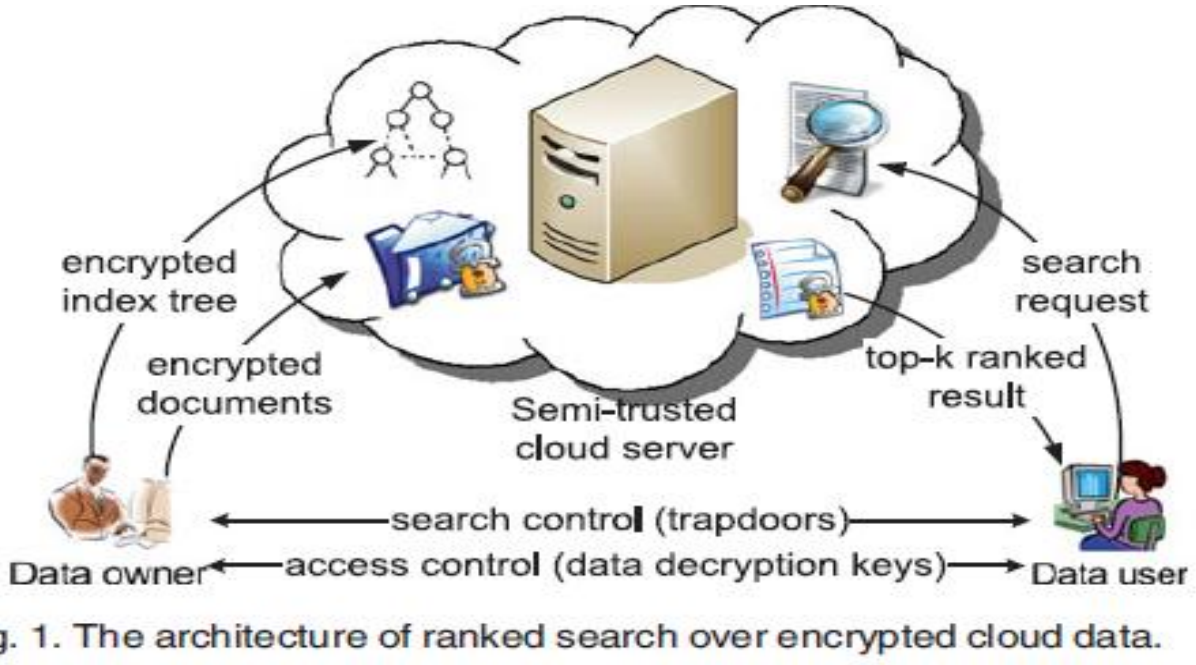


Fig. 1. The architecture of ranked search over encrypted cloud data.

***Fig 1 System Architecture***

The system model in this paper incorporates three unmistakable substances: data owners, data user and cloud server, as illustrated in Fig. 1.

There are multiple Data owner in system As Data owner has a gathering of records F = {f1; f2; :::; fn} that he needs to outsource to the cloud server in encoded structure while up 'til now keeping the ability to check on them for convincing utilization. data owner firstly manufactures a secure searchable tree index I from archive accumulation F, and a short time later makes a encrypted document gathering C for F. A brief span later, the data owner outsources the encoded accumulation C and the secure index I to the cloud server, and safely disseminates the key data of trapdoor era and document decryption to the approved data users. Additionally, the data owner is mindful of his documents stored in the cloud server. While updating, the data owner creates the upgrade data locally and sends it to the server also can perform data dynamic operations on files.

Data users are approved ones to get to the archives of data owner. With t query keywords, the approved user can create a trapdoor TD as indicated by search control mechanisms to get k encrypted documents from cloud server. By then, decrypt the documents with the shared secret key.

Cloud server stores the encrypted document accumulation C and the encrypted searchable tree index I for data owner. In the wake of tolerating the trapdoor TD from the data user, look over the index tree I, in conclusion gives back the relating gathering of top-k situated encoded reports. Also, in the wake of tolerating the update information from the data owner, the server needs to update the index I and document gathering C as per the received information.

After insertion or deletion of a record, we require updating synchronously the index. Since the index of DMRS scheme is planned as a balanced binary tree, the dynamic operation is done by redesigning hubs in the list tree. The report on record is just in view of archive recognizes, and no entrance to the substance of records is required

## IV. CONCLUSION

As from the survey of many schemes such as fuzzy keyword search, Holomorphic encryption scheme also an seething scheme on encrypted data also a symmetric searching scheme there are some drawbacks of all such system are User cannot search efficiently on encrypted files uploaded on cloud and also they didn't get the exact matching result for the file they search on cloud. So Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data improves the searching mechanism by uploading an encrypted index with that file and also users who search over encrypted file on cloud can get exact matching result of their search query for require file in cloud.

 

## V. ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

## VI. 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-preserving rank-ordered search," in *Proceedings of the 2007 ACM workshop on Storage security and survivability*. ACM, 2007, pp. 7–12.

 