**MD KAMAL ur RAHMAN IRSHAD, et al, International Journal of Computers, Electrical and Advanced Communication Engineering [IJCEACE]™. Thomson Reuters (WOS) Research ID: D-1150-2018, Volume 10, Issue 19, PP: 13 - 18, JAN - JUL' 2021.**

# VARIED WORDS ARRANGED SEARCH REPLICA ON CLOUD DATA SUPPORT ACTIVE OPERATIONS

**MD Kamal ur Rahman Irshad 1*, Mohammed Muzafferuddin Arshad 2**

*1. M.Tech Student. 2. Assistant Professor*
*Dept of CSE, Vif College of Engineering and Technology, Hyderabad, T.S, India*

**ABSTRACT:**

Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers to provide great convenience and lower costs in data management. However, sensitive data must be encrypted before outsourcing based on privacy requirements, eliminating data usage such as keyword-based document retrieval. In this document, we present a secure multi-keyword search scheme organized on encrypted data in the cloud, simultaneously supporting dynamic update processes such as document insertion and deletion. Specifically, the vector space model and the TF × IDF model widely used in index generation and query construction are combined. We are building a proprietary tree-based index structure and proposing a "Greedy-Depth First" algorithm to provide efficient multi-keyword ranked search. The kNN security algorithm is used to encode the index and the query vectors, while ensuring the accuracy of the calculation of the connection points between the encrypted index and the query vectors. To resist statistical attacks, dummy terms are added to the index vector to anonymize search results. Due to the use of our tree-based index structure, the proposed scheduler can achieve near-linear search time and handle document removal and insertion flexibly. Extensive tests are underway to demonstrate the efficiency of the proposed system.

***Keywords: — Searchable encryption, multi-keyword ranked search, dynamic update, cloud computing***

## 1. INTRODUCTION:

Cloud computing has been considered a new model for enterprise IT infrastructure, which can organize huge resources for computing, storage, and applications, allowing users to enjoy ubiquitous, convenient and low-cost network access. it demands a common pool of efficiently configurable computing resources. and minimum economic expenses [1]. By attracting these compelling features, both individuals and organizations are motivated to outsource their data to the cloud, rather than buying software and hardware to manage the data themselves. Despite the many advantages of cloud services, outsourcing confidential information (such as emails, personal medical records, company funding data, government documents, etc.) to remote servers raises privacy concerns. Cloud Service Providers (CSPs) that maintain user data can access confidential user information without permission. The general approach to protecting the confidentiality of data is to encrypt the data before outsourcing it [2]. However, this will result in a high cost in terms of data usability. For example, current keyword-based information retrieval technologies that are widely used in plain text data cannot be applied directly to encrypted data. Downloading all the data from the cloud and decrypting it locally is clearly impractical. To address the aforementioned problem, researchers have designed some general-purpose solutions with fully symmetric encryption [3] or discrete RAM [4]. However, these methods are not practical due to the high computational load of both the cloud server and the user. In contrast, practical special-purpose solutions, such as Search Encoder (SE) schemes, have made definite contributions in terms of efficiency, functionality, and security. Search ciphers allow the customer to store encrypted data in the cloud and perform keyword searches across the ciphertext domain. So far, abundant works under different threat models have been proposed to achieve various search functions, such as single keyword search, similarity search, logical multi-keyword search, ranked search, multi-keyword categorized search, etc. . It attracts more and more attention to its practical application. Recently, some dynamic layouts have been suggested to support inserts and deletions in a set of documents. This is an important business because data owners will most

likely need to update their data on the cloud server. But few dynamic layouts support efficient multi-word categorized search. This document proposes a secure tree-based search scheme on encrypted data in the cloud, which supports multi-word categorized search and dynamic operation across the document set. Specifically, the vector space model and the "term frequency (TF) × inverted document frequency (IDF)" model widely used in index generation and query generation combine to provide a multi-word categorized search. To obtain high search efficiency, we build a tree-based index structure and propose a "greedy search depth first" algorithm based on this index tree. Due to the special structure of our tree-based index, the proposed research plan can achieve near-linear search time with flexibility and handle the removal and insertion of documents. The kNN security algorithm is used to encode the index and the query vectors, while ensuring the accuracy of the calculation of the connection points between the encrypted index and the query vectors. To combat the different attacks on the different threat models, we created two Safe Search schemes: the Basic Dynamic Multiple Keyword Search Scheme (BDMRS) in the well-known Cryptographic Text Model, and the Enhanced Dynamic Multiple Word Search System. Key (EDMRS). in the well-known background model. Our contributions are summarized as follows: 1) We designed a cryptographic search system that supports both precise ordered multi-keyword searching and dynamic and flexible document collection. 2) Due to the special structure of our tree-based indicator, the search complexity of the proposed scheme remains mainly logarithmic. In practical terms, the proposed scheme can achieve greater search efficiency by implementing

## 2. TERMINOLOGY AND PROBLEM STATEMENT

The general way to protect the confidentiality of data is to encrypt it before outsourcing it. Search ciphers allow the customer to store encrypted data in the cloud and perform keyword searches across the ciphertext domain. Till now, abundant works under different threat models have been proposed to fulfill various search functions, such as single keyword search, similarity search, multi-keyword logical search, classified search, multi-keyword classified search, etc. Classified research is paying increasing attention to its practical application. Recently, some dynamic layouts have been

suggested to support inserts and deletions in a set of documents. This is an important business because data owners will most likely need to update their data on the cloud server. Huge cost in terms of ease of use of the data. For example, current keyword-based information retrieval technologies that are widely used in plain text data cannot be applied directly to encrypted data. Downloading all the data from the cloud and decrypting it locally is clearly impractical. Current system methods are impractical due to the high computational load of both the cloud server and the user.

## 3. IMPLEMENTING DYNAMIC FACETED SEARCH

This document proposes a secure tree-based search scheme on encrypted data in the cloud, which supports categorized search with multiple keywords and dynamic processing across the document set. Specifically, the vector space model and the widely used "term frequency (TF) × inverse document frequency (IDF)" model are combined in index generation and query generation to provide a classified search of multiple keywords. . To obtain high search efficiency, we build a tree-based index structure and propose a "greedy search depth first" algorithm based on this index tree. The kNN security algorithm is used to encode the index and the query vectors, while ensuring the accuracy of the calculation of the connection points between the encrypted index and the query vectors. To combat the different attacks on the different threat models, we created two Safe Search schemes: the Basic Dynamic Multiple Keyword Search Scheme (BDMRS) in the well-known Cryptographic Text Model, and the Enhanced Dynamic Multiple Word Search System. Key (EDMRS). in the well-known background model. Due to the special structure of our tree-based index, the proposed research plan can achieve near-linear search time with flexibility and handle the removal and insertion of documents.

We designed a searchable encryption system that supports both an accurate ordered search of multiple keywords and a dynamic and flexible document collection.

Due to the special structure of our tree-based indicator, the complexity of the search on the proposed chart remains mainly logarithmic. In practical terms, the proposed scheme can achieve higher search efficiency by implementing the "Greedy in depth first" algorithm. Additionally, parallel search can

be performed flexibly to further reduce the time cost of the search process.

## 4. THE SYSTEM AND THREAT MODELS

The system model in this document includes three different types Entities: data owner, data user, and cloud server, such as It is shown in Figure 1.

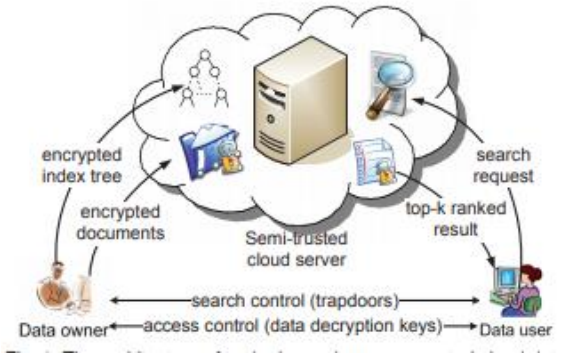


**Figure 1: System Architecture**

**Data owner**: You have a document set F = {f1, f2... fn} that you want to outsource the cloud server in encrypted form while retaining the ability to search it for efficient use. In our schema, the data owner first creates a secure index for search tree I from document set F, then creates encrypted document set C for FA then the data owner outsources both the cipher set C as the secure Index I to the cloud server, and securely distribute key private information. He creates a door scan (including keyword IDF values) and decrypts documents for authorized data users. Furthermore, the data owner is responsible for updating his documents stored on the cloud server. During an update, the data owner creates the update information locally and sends it to the server.

**Data users** you are authorized to access the documents of the owner of the data. With the query keywords, the authorized user can create a TD hatch according to the search control mechanisms to retrieve encrypted documents from the cloud server. After that, the data user can decrypt the documents with the shared secret key

## 4. CONCLUSION:

There are still a lot of challenge issues on symmetric SE graphics. In the proposed scheme, the data owner is responsible for creating the update information and sending it to the cloud server. Therefore, the data owner must store the unencrypted index tree and the information required to recalculate the IDF values. This active data owner may not be very suitable for a cloud computing model. It may be useful and challenging future work to design a searchable dynamic cryptographic system whose upgrade process can be completed with the cloud server only,

while retaining the ability to support multi-keyword classified searches. Also, since most of the crypto work is searchable, our plan primarily takes into account the cloud server challenge. In fact, there are many safe challenges in a multi-user system. First, all users usually keep the same secure key to create a swing door in a symmetrical SE scheme. In this case, revoking the user is quite a challenge. If it is necessary to delete a user in this scheme, we must rebuild the index and distribute the new security keys to all authorized users. Second, symmetric SE charts generally assume that all data users are trustworthy. It is not practical and the dishonest data user will lead to many security problems. For example, a rogue data user can search for documents and distribute decrypted documents to unauthorized documents. Furthermore, the rogue data user can distribute their secure keys to unauthorized keys. In future work, we will try to improve the SE chart to address these challenges.

**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 CryptologyEurocrypt 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.