

Survey on Multi-Keyword Ranked Search over Encrypted Cloud Data

Dr. R. Pragaladan¹ Ms. T. Lakshmi²

¹Assistant Professor & Head of Department ²M.Phil Part Time Research Scholar

^{1,2}Department of Computer Science & Engineering

^{1,2}Sri Vasavi College, Erode, India

Abstract— The arrival of cloud computing, data owners are enthused to outsource their unpredictable information management systems from nearby destinations to attractive open cloud for flexibleness and cost-effective savings. Considering secure information protection, sensitive information would be encoded in the past deploying that obsoletes usual information employ within original text keyword search. An encoded cloud information search service acts an essential importance. Other than thinking about the huge amount of information client and records in cloud, it is vital for the search service to permit multi-keyword query and present outcome match ranking to gather the important information retrieval prerequisite. The search encryption originates on particular keyword search or else Boolean keyword search, and infrequently separates the pursuit and end results. This paper portray and resolve the demanding issue of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), and found a collection of rigorous confidentiality prerequisite for suchlike a protected cloud information usage system to come a actuality. Among a range of multi-keyword semantics, the effective standard of “coordinate matching”, i.e., the same number of matches as feasible, to catching the similarity between search query and data documents is chosen, furthermore additionally utilizes “inner product similarity” to finitely formalize such like principle for similarity quantification.

Key words: Cloud Computing, Multi-Keyword Ranked Search over Encrypted Cloud Data (MRSE), Coordinate Matching, And Inner Product Similarity

I. INTRODUCTION

Cloud computing acts a one kind of distributed computing network and capability to run a program with many related PCs at the comparative time. It is also named as a productiveness of the computing since it utilizes pay per use worldview. In cloud computing, clients can rights to utilize a changeability of the resources like storage, programs, and application development platforms.

Cloud storage is computer data storage inside it more precious information of organizations, companies is stored to keep their data from virus and hacking. Therefore the advantage of cloud computing, more information proprietors bring together their sensitive data inside the cloud. With a set of data files saved in the cloud server, it is important to offer keyword based search service to the data client. To ensure the information protection, sensitive data is frequently encoded before deployed onto the cloud server and decrypted the files after downloaded, which makes the inquiry advances on plaintext broken.

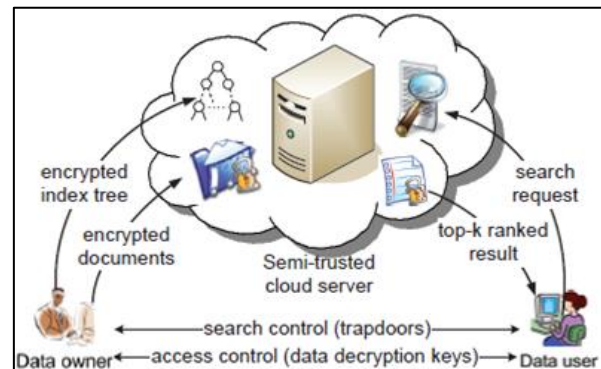


Fig. 1: Design of the Search upon Encoded Cloud Server

Inside cryptography, encryption stands the procedure for encoding a news or else data such that particular certified person can utilize it and those who are not endorsed can't use it. Encryption is the procedure of translating plain text information (plaintext) into something that lands to be arbitrary and futile (ciphertext). Decryption is the method toward altering above cipher text back in to the plaintext.

However, data encryption is a substantial overhead, and data recovery process brings about a muddled correspondence between the data client and cloud. Such data clients, approaches ranked search scheme to discover the majority proper data quickly, as opposed to arduously arranging completely through each match in the substance set.

Ranked search [10] enhances framework convenience by typical matching files in a ranked order with respect to certain significance criteria (for example keyword frequency). Ranked search expel the unnecessary network traffic by distribution reverse only the majority of the substantial information, which is extremely alluring in the "pay per use worldview" cloud perception. To get great pursuit outcome in addition to improve the client sharp expertise, such ranking system fundamentally hold up various keywords search, excessively abusive outcomes was created by single keyword search.

The multi- keyword search method [9] ensures that the questioned keywords be present in a document or not. If the user searches for a single or more keywords, there will possibly be many correct matches where some of them may well not be useful to user at all. Thusly, it is hard to choose about which documents are most matched. Attach ranking capability with the method by adding extra index information for frequently occurring keywords in a file. With ranking, the user is able to recover only the top k matches where k is selected by the client. In order to level the documents, a ranking function is required, which assigns relevant scores to every file matching to a given search query. Among the largest utilized estimations in information recovery stands the term frequency. Term frequency is characterized as the quantity of occasion a keyword shows up in a document.

A semantic multi-keyword ranked ontology keyword mapping and search system over the encoded cloud information, which meanwhile meets a type of strict confirmation necessities. This arrangement first use the "Latent Semantic Analysis" to reveal connection amongst conditions and documents. The vector comprising of TF values as indexes to documents. These vectors constitute a grid, from which dissect the latent semantic association among conditions and documents by LSA. Second, use guaranteed "k-nearest neighbour (k-NN)" to attain protected pursuit performance. This course of action could restore the right coordinating records, as and the documents including the terms latent semantically identified with the enquiry keyword. This scheme accepts Gauss-Jordan to process the inverse matrix. The period of generating key is determined by the size of the matrix.

II. LITERATURE REVIEW

A. Efficient & Secure Ranked Multi-Keyword Search on Encrypted Cloud Data

On one offer, clients who don't basically have earlier learning of the encrypted cloud information, need to post process each retrieved file taking the final objective to discover ones most coordinating their enthusiasm; On the other offer, perpetually retrieving all files containing the queried keyword additionally brings about superfluous network traffic, which is completely unfortunate in the present pay-as-you-use cloud worldview. The proposed ranking method of Cengiz Orencik et al. [1] shows to be productive to return exceedingly significant files detailing to submitted search terms. Security is a principle issue for cloud computing, both as far as lawful consistence and client trust and desires to be examined at each period of outline. From this work, fundamental theme taken is of preserving privacy of data. This work just portrays protection of information however doesn't permit indexed search in addition to doesn't hide user's identity.

B. Secure Ranked Keyword Search over Encrypted Cloud Data

Cong Wang et al. [2] proposed a technique that rouse and tackle the issue of supporting proficient efficient ranked keyword search for accomplishing viable usage of remotely stored encoded information in cloud. This strategy first give an essential plan ranked keyword search underneath the state-of-the-art searchable symmetric encryption (SSE) and demonstrate that along subsequent the similar existing accessible encryption structure, it is extremely useless to accomplish ranked search. At that instant properly debilitate the security ensure, turn to the recently created crypto primitive OPSE, and determine a proficient one-to-many order-preserving mapping function, that permits the successful ranked searchable symmetric encryption (RSSE) to be summarized. Through careful security investigation, the proposed preparation is secure and privacy-preserving, while successfully understanding the aim of ranked keyword search.

C. Authorized Private Keyword Search over Encrypted Data in Cloud Computing

Ming Li et al. [3] addressed the issue of Authorized Private Keyword Search (APKS) over encrypted data in cloud computing, where numerous information owners encode their records adjacent to with a keyword index to permit searches by multiple clients. The arrangements permit proficient multi-dimensional keyword searches with range query; allow appointment and repudiation of search capacities. In addition, improvement about the enquiry confidentiality hides users' query keyword against the server. To restrict the presentation of delicate data because of unlimited query abilities, this one recommends a scalable, fine-grained approval structure where clients pick up their search capacities from local trusted authorities (LTAs) as indicated by their traits. The primary favourable position of plans in this classification is they hinder the overhead for users to attain search abilities.

D. Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking

Wenhai Sun et al. [4] considered a privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking problem. To help multi-keyword search with search result ranking, to formulate the search index supported on term frequency $TF \times IDF$ and the vector range reveal with cosine comparability measure to accomplish higher search result exactness. Towards improve the search efficiency, a tree-based index structure and dissimilar alteration plans designed for multi-dimensional (MD) algorithm with the goal that the useful search effectiveness is greatly improved than that of linear search. To additionally upgrade the search protection, two safe index systems to congregate the strict protection prerequisites under solid risk models, i.e., told ciphertext representation and told background model. The MD-algorithm is primarily proposed for plaintext database search. On account of privacy-preserving similarity-based multi-keyword ranked text search, it can't be connected in a clear way.

E. Cryptographic Cloud Storage

At the point when the advantages of utilizing an open cloud infrastructure are reasonable, it presents critical safety and protection risks. Truth be told, it creates the impression that the greatest trouble to the selection of cloud storage is unease over the mystery and dependability of data. In [11], S. Kamara et al. proposed an outline of the advantages of a cryptographic storage service, for instance, diminishing the lawful presentation of both clients and cloud suppliers, and accomplishing administrative consistence is given. Other than this, cloud services that could be based over a cryptographic storage service, for instance, secure reinforcements, documented, wellbeing record systems, and protected data replace and e-disclosure is expressed briefly.

F. Privacy-Preserving Ranked Multi-Keyword Search Leveraging Polynomial Function in Cloud Computing

Yanzhi Ren et al. [5] anticipated a light-weight search approach that backings efficient multi-keyword ranked ontology keyword mapping and explore in cloud computing scheme. This fundamental plan utilizes the polynomial function to conceal the encrypted keyword and search

patterns for efficient Multi keyword ranked ontology keyword mapping and search. To upgrade the search protection, this plan uses the safe inner product technique in support of defending the confidentiality of the explored multi-keywords. This plan dispenses with the predefined binary index vector utilized in the current multiple-keyword search scheme and permits effective index update, making it flexible to a significant number of searching keywords.

G. Privacy Preserving Multi-Keyword Ranked Search with Anonymous Id Assignment over Encrypted Cloud Data

Shiba Sampat Kale et al. [6] tended to and attempted the testing issue of privacy-preserving Multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (MROS), and sets up an understanding of strict security requirements for suchlike a secure cloud information use framework to be executed in genuine.

Stringent protection is given by relegating the cloud client a unique ID. This client ID is kept evaded the cloud provision supplier and additionally the foreigner user to shield the client's information on cloud from the CSP and the outsider client. In that, by concealing the client's identity, the secrecy of client's information is kept up. Task of anonymous ID to the client to give greater security to the information on cloud server is finished.

In this work, an algorithm for anonymous sharing of private data among N parties is produced. This system is used constantly to assign these nodes ID numbers running from 1 to N. This task is anonymous in that the identities got are obscure to alternate individuals from the gathering.

Achieving Secure, Scalable and Fine-Grained Data Access Control in Cloud Computing

A privacy-preserving public auditing system for information storage protection in Cloud Computing design was depicted by Shucheng Yu et al. [7]. It uses the homomorphism sequential authenticator and arbitrary masking to make sure that the TPA would typically not locate a few data regarding the information content set left in the cloud server among the effective reviewing process, which eradicate the load of cloud client from the endless and conceivably costly evaluating assignment, it additionally eases the client's dread of his/her outsourced information spillage.

H. Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

Ning Cao et al. [8] proposed a technique that characterize and take care of the difficult issue of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing. Among dissimilar multi-keyword semantics, Ning Cao et al., choose the expert resemblance quantify of "coordinate matching", i.e., what amount equals as could reasonably be expected, to catch the applicability of information files to the search enquiry. Additionally utilize "inner product similarity" to measurably consider such nearness quantify. This arrangement in perspective secure inner product calculation, and after that give two basically enhanced this plan to achieve altered strict protection requirements in two diverse risk models.

Sr. No	Paper Title	Objective
1	Efficient and Secure Ranked Multi-Keyword Search on Encrypted Cloud Data	This paper has characterized and solved the crisis of viable yet secure ranked keyword search over encrypted cloud data.
2	Secure Ranked Keyword Search over Encrypted Cloud Data	Main focus is around the arrangement of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving strict system-wise security in the cloud computing paradigm.
3	Authorized Private Keyword Search over Encrypted Data in Cloud Computing	The results permit productive multi-dimensional keyword searches with range query; allow appointment and repudiation of search capabilities.
4	Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking	Principle thought is to formalize and tackle the issue of successful fuzzy keyword search over encoded cloud data though keeping up keyword security.
5	Cryptographic Cloud Storage	This scheme diminishing the lawful introduction of the both customers and cloud providers, and accomplishing executive consistence is given.
6	Privacy-Preserving Ranked Multi-Keyword Search Leveraging Polynomial Function in Cloud Computing	This plan utilizes the polynomial function to hide the encrypted keyword and search patterns for productive Multi-keyword ranked keyword search.
7	Privacy Preserving Multi-Keyword Ranked Search with Anonymous Id Assignment over Encrypted Cloud Data	Principle objective is to get the entrance to users information which is put away remotely from anyplace as per users accommodation.
8	Achieving Secure, Scalable and Fine-Grained Data Access Control in Cloud Computing	This plan takes out the heap of cloud client from the dull and conceivably costly inspecting task.
9	Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data	The main aim of this scheme is to accomplishing viable usage of remotely put away encrypted data in cloud computing.

Table 1: Review Summary

III. CONCLUSION

Thusly we looked into the issue of multi-keyword ranked search over encrypted cloud data, and develop an assortment of security prerequisites. Among altered multi-keyword semantics, we decide on the expert law of “coordinate matching”, i.e., whatever amount equivalents as might reasonably be expected, to viably catch closeness between queried keywords and outsourced documents, and employs “inner product similarity” to measurably formalize such a standard for similarity estimation.

For addressing the multifaceted nature of supporting multi-keyword semantic without protection breaks, we suggests a fundamental MRSE scheme by secure inner product calculation, and altogether enhance it to accomplish protection prerequisites in two levels of risk models. Serious examination exploring protection and effectiveness assurances of proposed procedure is given, and researches on this present reality dataset show our proposed procedure present low overhead on both calculation and communication. As our upcoming job, we will consider supporting other multi-keyword semantics (e.g., weighted query) over encrypted information, respectability check of rank order in search result and protection ensures in more grounded risk show.

REFERENCES

- [1] Cengiz Orencik and Erkey Savas, “Efficient and Secure Ranked Multi-Keyword Search on Encrypted Cloud Data”, Proceedings of the EDBT/ICDT Workshop, 186-195, 2012.
- [2] Cong Wang, Ning Cao, Jin Li, Kui Ren and Wenjing Lou, “Secure Ranked Keyword Search over Encrypted Cloud Data”, IEEE 30th ICDCS, 253-262, 2010.
- [3] Ming Li, Shucheng Yu, Ning Cao and Wenjing Lou, “Authorized Private Keyword Search over Encrypted Data in Cloud Computing”, IEEE 31th ICDCS, 383-392, 2011.
- [4] Wenhai Sun, Bing Wang, Ning Cao, Ming Li, Wenjing Lou, Y. Thomas Hou and Hui Li, “Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking”, Proceeding of the 8th ACM SIGSAC, 71-82, 2013.
- [5] Yanzhi Ren, Yingying Chen, Jie Yang and Bin Xie, “Privacy-Preserving Ranked Multi-Keyword Search Leveraging Polynomial Function in Cloud Computing”, IEEE Global Communication Conference, 2014.
- [6] Shiba Sampat Kale and Prof. Shivaji R Lahane, “Privacy Preserving Multi-Keyword Ranked Search with Anonymous ID Assignment over Encrypted Cloud Data”, IJCSIT, Vol. 5 (6), 7093-7096, 2014.
- [7] Shucheng Yu, Cong Wang, Kui Ren and Wenjing Lou, “Achieving Secure, Scalable and Fine-Grained Data Access Control in Cloud Computing”, Proceeding IEEE INFOCOM, 2010.
- [8] [Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou, “Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data”, IEEE Transactions on Parallel and Distributed Computing, Vol. 25, 2014.
- [9] R. Vanishree and G. S. Suresh, “Multi-Keyword Ranked Search over Encrypted Cloud Data”, IJARCET, Vol. 4(5), 2015.
- [10] Marru Sushma and B. Nehru, “MRSE in Cloud Data using Coordinate Matching & Inner Product Similarity”, IJATIR, Vol. 7(12), 2292-2295, 2015.
- [11] S. Kamara and K. Lauter, “Cryptographic Cloud Storage”, Proceedings 14th International Conference on Financial Cryptography and Data Security, 2010.