

Multi-Keyword Search over Encrypted Cloud Data

^{#1}Vaibhav Deshpande, ^{#2}Shrinivas Patil, ^{#3}Akshay Pawar, ^{#4}Asif Shaikh



¹deshpande.vaibhav31@gmail.com

²shripatil94@gmail.com

³akshaypawar87@gmail.com

⁴shaikhaasif3130@gmail.com

^{#1234}Department of Computer Engineering

KJCOEMR, SPPU Pune, India.

ABSTRACT

The innovation in cloud computing has encouraged the data owners to outsource their data managing system from local sites to profitable public cloud for excessive flexibility and profitable savings. But people can like full benefit of cloud computing, if we are able to report very real secrecy and security concerns that come with loading sensitive personal information. Allowing an encrypted cloud data search facility is of great significance. In view of the huge number of data users, documents in the cloud, it is important for the search facility to agree multi keywords query and arrange for result comparison ranking to meet the actual need of data recovery search and not regularly distinguish the search results. Related mechanisms on searchable encryption emphasis on single keyword search or Boolean keyword search, and often sort the search outcomes. In this system, we explain and solve the interesting problem of privacy preserving multi keywords ranked search over encrypted cloud data, and create a set of strict privacy necessities for such a safe cloud data application system to be effected in real. We first offer a basic idea for the multi keyword ranked search over encrypted cloud data (MRSE) based on effective comparison measure of coordinate matching, i.e. as many matches as possible, in order to capture the significance of data documents to the search query. Then we give two considerably developed multi keywords ranked search encryption schemes to reach many tough privacy requirements in two differ threat models

Keywords: Cloud computing, searchable encryption, privacy-preserving, keyword search, ranked search.

ARTICLE INFO

Article History

Received: 18th October 2017

Received in revised form :

18th October 2017

Accepted: 22nd October 2017

Published online :

9th November 2017

I. INTRODUCTION

Cloud computing has become new model which handles large resources of computing. Services provided by the cloud computing is storage and on demand services, both the individuals and organizations are motivated to the cloud. Instead of purchasing software and hardware devices.

Cloud provides secure online storage and there is no loss of data, the data is available at anytime and anywhere. Paper shows the general approach for data protection is to encrypt the data by using RSA-AES algorithm.

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.[3] 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. [1]

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[4] or missing RAMs.[5] 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 ciphertext 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 ranked search, etc. Among them, multi-keyword positioned quest finishes more thought for its pragmatic propriety. Starting late, some component arrangements have been proposed to 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 multi-keyword situated look.

II. PROBLEM STATEMENT

Actually large number of on-demand data users and huge amount of data documents in the cloud, this difficulty is challenging. It is essential for the search facility to permit multi keyword search query and make available result comparison ranking to see the effective data retrieval requirement. To develop the search result accuracy as well as to enrich the user searching experience, it is also essential for such ranking system to support multiple keywords search, as single keyword search regularly yields extreme coarse results. The searchable encryption method supports to give encrypted data as documents and agrees a user to firmly search over single keyword and retrieve documents of concern.

III. LITERATURE SURVEY

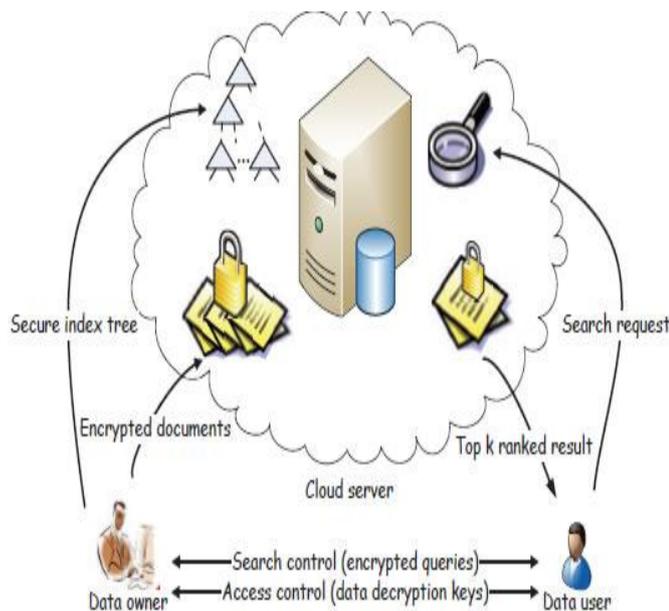
| Title | Author | Year | Review |
|---|---|------|---|
| Multi Keyword Ranked Search over Encrypted Cloud Data | Mr.G.S Suresh Associate professor Dept.of CSE | 2015 | Thus we proposed the problem of multiple-keyword ranked search over encrypted cloud data, and construct a variety of security requirements. From various multi-keyword concepts, we choose the efficient principle of coordinate matching. We first propose secure inner data |

| | | | |
|---|--|------|--|
| | VTU,CIT, Gubbi,T umkur | | computation. Also we achieve effective ranking result using k-nearest neighbor technique. This system is currently work on single cloud Provide better security in multi-user systems. |
| Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data | Ning Cao, Wenjing Lou, Department of ECE, Illinois Institute of Technology, | 2016 | In this paper, for the first time we define and solve the problem of multi-keyword ranked search over encrypted cloud data, and establish a variety of privacy requirements. Among various multi-keyword semantics, we choose the efficient similarity measure of "coordinate matching". For meeting the challenge of supporting multi-keyword semantic without privacy breaches, we propose a basic idea of MRSE using secure inner product computation. |
| A SECURE AND DYNAMIC MULTI-KEYWORD RANKED SEARCH SCHEME OVER ENCRYPTED CLOUD DATA | LeMenz Infotech | 2015 | In this paper, we propose a light-weight search approach that supports efficient multi-keyword ranked search in cloud computing system. Our basic scheme employs the polynomial function to hide the encrypted keyword and search patterns for efficient multi-keyword ranked search. We then improve the basic scheme and propose a privacy-preserving scheme which utilizes the secure inner product method for protecting the privacy of the searched multi-keywords. The experiment results demonstrate that our scheme can enable the encrypted multi-keyword ranked search service with high efficiency in cloud computing |
| A Review Paper on Multi keyword Ranked Search on Encrypted Cloud Data | <i>IOSR Journal of Computer Engineering</i> | 2015 | In this paper, a safe, effective and dynamic search scheme is proposed, which underpins the exact multi-keyword ranked search as well as the dynamic deletion and insertion of documents. We assemble a special |

| | | |
|--|--|---|
| | | <p>keyword balanced binary tree as the index, and intend a “Greedy Depth-first Search” algorithm to acquire preferable effectiveness over linear search. Likewise, the parallel search procedure can be completed to further lessen the time cost. The plan's security is ensured against two risk models by utilizing the safe kNN algorithm. Trial results display the efficiency of our proposed scheme. In the proposed scheme, the information proprietor is in charge of producing overhauling data and sending them to the cloud server.</p> |
|--|--|---|

IV. PROPOSED SYSTEM

Architecture explanation



This paper proposes a secure tree-based search scheme over the encrypted cloud data, which supports multi-keyword ranked search and dynamic operation on the document collection. Specifically, the vector space model and the widely-used “term frequency (TF) × inverse document frequency (IDF)” model are combined in the index construction and query generation to provide multi-keyword ranked search. In order to obtain high search efficiency, we construct a tree-based index structure and propose a “Greedy Depth-first Search” algorithm based on this index tree.

The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and

query vectors. To resist different attacks in different threat models, we construct 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.

Data User Module: This module includes the user registration login details.

Data Owner Module: This module helps the owner to register them details and also include login details.

File Upload Module: This module help the owner to upload his file with encryption using RSA algorithm. This ensures the files to be protected from unauthorized user.

File Download Module: This module allows the user to download the file using his secret key to decrypt the downloaded data.

Rank Search Module: This module ensures the user to search the file that are searched frequently using rank search.

View Uploaded and Downloaded File: This module allows the Owner to view the uploaded files and downloaded files.

V. CONCLUSION

A safe, effective and dynamic search scheme is proposed, which underpins the exact multi-keyword ranked search as well as the dynamic deletion and insertion of documents.

In the proposed scheme, the information proprietor is in charge of producing overhauling data and sending them to the cloud server. It offers fitting semantic separation between terms to achieve the question keyword expansion. Such an active data owner may not be astoundingly suitable for the appropriated distributed computing model

REFERENCES

[1] G. Keerthana, S. Prabu, P. Swarnalatha, “An Efficient Data Security in Cloud Computing using Cryptography”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 6, Issue 5, 2016, pp: 654-660

[2] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Financial Cryptography and Data Security Springer, 2010, pp. 136–149.

[3] C. Chen, X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, A. Y. Zomaya, “An Efficient Privacy-Preserving Ranked Keyword Search Method”, IEEE Transactions On Parallel And Distributed Systems, Vol. 27, No. 4, 2016.”

[4] 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. on Communications (ICC12), pp. 917-922, 2012.

[5] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious RAMs," *Journal of the ACM (JACM)* vol. 43, no. 3, pp. 431–473

[6] Chia-Mu Yu, Chi-Yuan Chen, and Han-Chieh Chao, Privacy-Preserving Multikeyword Similarity Search Over Outsourced Cloud Data, 1932-8184 2015 *IEEE Systems Journal*.

[7] Wenhai Sun, Bing Wang, Ning Cao, Ming Li, Wenjing Lou, Y. Thomas Hou, Hui Li, Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking, *IEEE Transactions On Parallel And Distributed Systems*, Vol. 25, No. 11, November 2014.

[8] Zhangjie Fu, Xingming Sun, Nigel Linge, Lu Zhou, Achieving Effective Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Synonym Query, *IEEE Transactions on Consumer Electronics*, Vol. 60, No. 1, February 2014.

[9] Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou, Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data, *IEEE Transactions On Parallel And Distributed Systems*, Vol. 25, No. 1, January 2014.

[10] Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue, Minglu Li, Toward Secure Multi-keyword Top-k Retrieval over Encrypted Cloud Data, *IEEE Transactions On Dependable And Secure Computing*, Vol. 10, No. 4, July/August 2013 239.