International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# COPY RIGHT

ELSEVIER SSRN



IJIEMR Transactions, online available on 27th Sept 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 09

**DOI: 10.48047/IJIEMR/V11/ISSUE 09/27**

Title **EFFICIENT AND PRIVACY-PRESERVING MULTI-KEYWORD RANKED SEARCH WITH ACCESS CONTROL OVER ENCRYPTED CLOUD**

Volume 11, ISSUE 09, Pages: 231-239

Paper Authors

**Mrs. T. Lakshmi Prasanna, Mr.G.Srinivasa Veeranjaneyulu, Ms. Gautami Priya, Ms. V Suma Moulika, Ms. Sk Saleha**


USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# EFFICIENT AND PRIVACY-PRESERVING MULTI-KEYWORD RANKEDSEARCH WITH ACCESS CONTROL OVER ENCRYPTED CLOUD

**[1] Mrs. T. Lakshmi Prasanna, [2]Mr.G.Srinivasa Veeranjaneyulu, [3]Ms. Gautami Priya, [4]Ms. V Suma Moulika, [5]Ms. Sk Saleha**

[1]Associate Professor, Department of Master of Computer Applications, Narayana EngineeringCollege, Nellore, Andhra Pradesh, INDIA.

[2,3,4,5]PG Scholar, Department of Master of Computer Applications, Narayana EngineeringCollege, Nellore, Andhra Pradesh, INDIA.

**ABSTRACT—**With the explosive growth of records volume in the cloud computing environment, records proprietors are increasingly inclined to store their data on the cloud. Although data outsourcing reduces computation and storage expenses for them, it inevitably brings new protection and privateness concerns, as the information owners lose direct manage of touchy data. Meanwhile, most of the existing ranked keyword search schemes by and large focal point on enriching search effectivity or functionality, however lack of providing environment friendly get admission to manage and formal security evaluation simultaneously. To address these limitations, in this paper I suggest an environment friendly and privacy-preserving Multi-keyword Ranked Search scheme with Fine-grained get right of entry to manipulate (MRSF). MRSF can recognize quite accurate ciphertext retrieval by using combining coordinate matching with Term Frequency-Inverse Document Frequency (TF-IDF) and enhancing the invulnerable kNN method. Besides, it can correctly refine users' search privileges by means of making use of the polynomial-based get admission to strategy.

**Keywords:** Cloud computing, ranked keyword search, privacy-preserving, access control, secure kNN

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

## 1. INTRODUCTION

AS a new computing paradigm, cloud computing offers ubiquitous and on-demand get admission to to flexible computation and storage resources. Therefore, outsourcing local facts to cloud servers has grow to be a frequent exercise for agencies and individuals. While this measure notably reduces hardware and upkeep expenditure, statistics owners definitely lose direct control over their data. This actually has added some safety concerns, particularly to proprietors of particularly touchy statistics (i.e., digital medical records, monetary documents, etc.). With such suspicion, individuals and organisations may also be reluctant to outsource their touchy data to an untrusted third-party cloud service provider. Thus, protection concerns will emerge as one of the principal obstacles impeding the tremendous deployments of cloud computing. To prevent doable information leakage, statistics proprietors normally encrypt

their data earlier than outsourcing them to the commercial public cloud. However, conventional data encryption schemes disable the cloud from walking licensed calculations on its storage (e.g., retrieving the involved file for a sure customer), which disables the implementation of plaintext-based statistics retrieval applied sciences over outsourced data. Atrivial answer is to download all the records and decrypt them locally, but this may lead to a massive waste of bandwidth and computation resources. Thus, how to obtain efficient facts retrieval while ensuring information safety turns into a difficult issue. The Searchable Symmetric Encryption (SSE) is greatly regarded as a promising way to solve the dilemma between information utilization and confidentiality. Some inspiring SSE-based designs consist of Boolean key-word search schemes in these schemes enable conjunctive keyword search over encrypted data. However, none of these schemes are sufficient to grant a ranked search. The complex plan of SSE additionally prohibits its direct software in large-scale cloud data. To tackle the former issue, the first impervious ranked search scheme is proposed in, but it simply supports single key-word search.

## 2. LITERATURE SURVEY

Searchable encryption is a promising method to replace the trivial approach that the user downloads encrypted outsourced facts then decrypts it to search. The current works more often than not make a contribution in two

ways: the encryption structure and the expansion of search functionalities. In this section, I review some recent achievements in this area in two aspects. Searchable Encryption. SE schemes can be divided into two categories, namely, Asymmetric Searchable Encryption (ASE) and Symmetric Searchable Encryption (SSE). The pioneering work proposed with the aid of Boneh et al. in is the first public-key encryption scheme that supports single keyword search. This work is extended in helping more operations over encrypted data such as conjunctive key-word search, range query, etc. However, the ASE schemes are less efficient than SSE schemes due to the complex encryption procedures. In, Yu et al.[1] proposed a two-round searchable encryption (TRSE) scheme that helps ranked multi-keyword search. In TRSE, homomorphic encryption is leveraged to encrypt index and question generated by means of a vector space model. Although TRSE guarantees excessive security, it takes two rounds of communications between the facts person and the cloud server to whole one search process. In the work of Cheng et al.[2] a public-key crypto gadget based kNN scheme is proposed. Different from the former invulnerable kNN methods based on symmetric encryption, the proposed scheme leverages the allotted two trapdoors public-key cryptosystem (DT-PKC), which allows secure k-NN query with more than one keys. The concept of SSE is first proposed through Song et al.[4] in, but this scheme lacks help for keywords relevance calculation and multi-keyword search. Another SSE based ranked search over encrypted data is proposed via Wang et al[5]. in, leveraging OPSE (order- preserving symmetric encryption). In order to habits kNN search over encrypted data set, Wong et al.[12] first proposed the asymmetric scalar product- preserving encryption (ASPE) in, which is viewed as the original impervious kNN scheme. Since then, ASPE has been entirely studied in many works, however, most ranked keyword search schemes based on ASPE are susceptible to level-3 attack, the place the adversary is capable to attain a certain quantity of undeniable textual content cipher text pairs. In a word, tightly closed kNN computation is an SE technique with excessive usability however pretty low security. Functionality extension. Proposed schemes in literature help at least one search functionality. As noted before, focal point on boolean keyword search, while, focus on multi-

keyword search. Schemes that center of attention on geometric search include. Relevance rankings in keyword/textual search are changed by using the distance between coordinate points, and the records structure is frequently designed mainly in those schemes. Other schemes aid blended search objects, for example, proposed a scheme that returns top-k region factors with keywords matching the queried keywords. In this paper, I mostly focal point on key-word search over encrypted data. There are variant performance extensions closer to keyword search schemes over encrypted data.

## 3. PROPOSED SYSTEM

To keep away from privateness leakage from indexes and queries submitted to the cloud, the basic invulnerable kNN method has been adapted to support MRSF. The modifications consist of the vector extensions, pseudorandom permutation function, and appended random varieties. I devise an efficient and privacy-preserving Multi-keyword Ranked Search scheme with Fine-grained get admission to manipulate over encrypted cloud statistics (MRSF). To supply a greater accurate and easy search service, we use the coordinate matching with TF-IDF as the similarity measure of MRSF.

MRSF utilizes a polynomial-based access method to warranty that statistics customers can solely get entry to data archives approved to them. I delicately diagram a polynomial feature with a distinctive property that, when a non-root thing (an unauthorized role) is input to this feature throughout the internal product calculation process, the end result will be a ways

larger than the most viable relevance score. To meet the needs of both sides, I also carefully assemble the position set from a super-incremental sequence. I build a polynomial basedtotally on the user roles and use it to generate a coefficient vector, which will be included in the sub indexes in the following index construction process. In the question token era process,the role of the facts person is padded into its query vector. At last, a filter in the looking out method will leave out the atypical relevance rankings to ensure that solely handy documentsare returned.

I consider a cloud storage system that helps ranked file retrieval in a privacy- keeping way. I reflect on consideration on three basic entities in our device model, particularly the data

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

owner, the cloud server, and the records user.

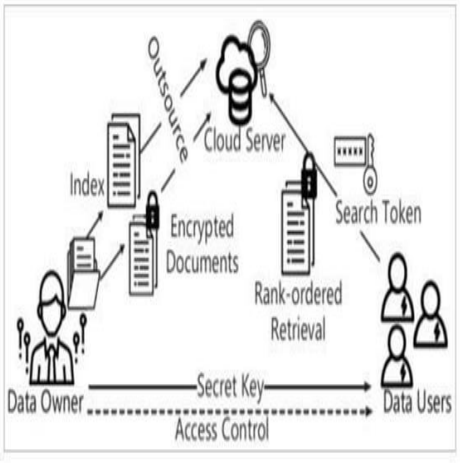


Fig.1 System Architecture

**Data Owner:**

The data owner ought to put up his/her encrypted facts files to the cloud server. Before data outsourcing, the statistics proprietor first builds encrypted searchable indexes for all data documents, then sends each indexes and encrypted files to the cloud. Besides, the information owner decides the get right of entry to roles for extraordinary statistics users.

**Cloud Server:**

The cloud server, which has notable computation power and huge storage capacities, presents records internet hosting and processing offerings for records proprietors and data users. Upon receiving the token from an approved records user, the cloud server first conducts search operations primarily based on encrypted indexes and token, then returns the applicable encrypted documents.

**DATA USER:**

The data user acquires the secret keys and the get entry to roles from the data owner via a tightly closed channel after issuing a search request. Next, the facts user generates his/her search token with the secret key, then sends it to the cloud server. The secret key is additionally used for decrypting the retrieved consequences off-line. Moreover, the polynomial- based access control mechanism is employed to manipulate the decryption competencies of data users

## 4. RESULTS

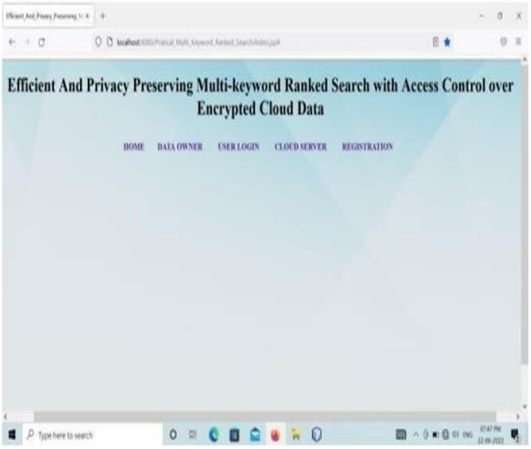


Fig.2 Home Page

In this screen, Cloud Server has to login with valid username and password. If the givencredentials are correct then the data owner main page will open.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org


Fig.3 Registration Page

In this screen, Data User and Data owner has to register by filling all required fields likename, password, email, role and then click submit.

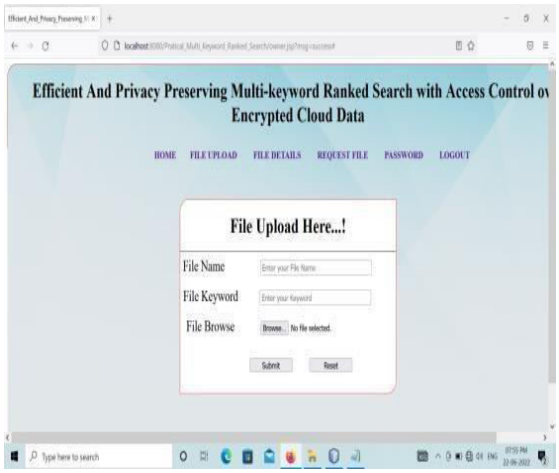


Fig.4 File Upload Page

In this screen, Data Owner will upload a file to cloud. Data owner will select the requiredfile to store in the cloud and given a name to the file and upload it.

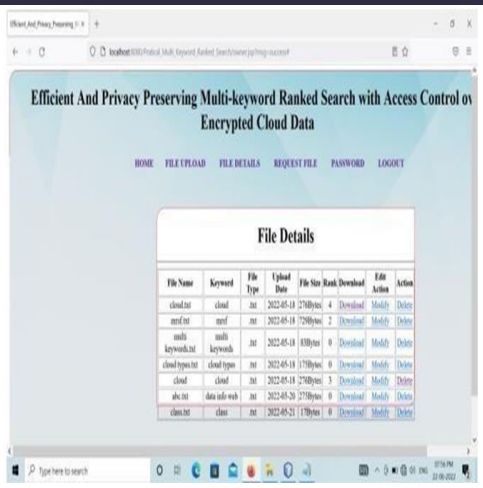


Fig.5 Uploaded File Details

In this screen, file details will be shown by Data owner and can make changes by him eitherhe can modify or delete the files

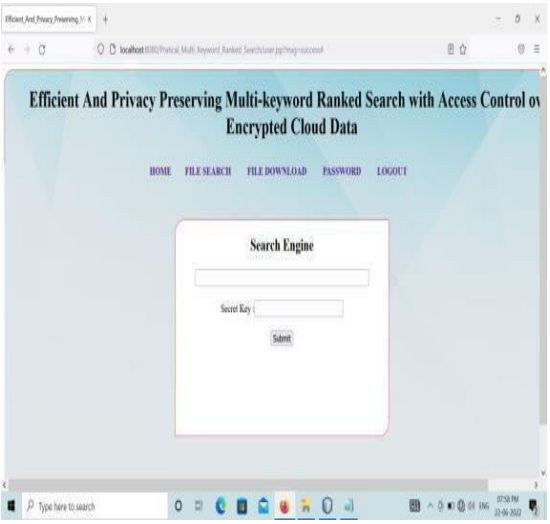


Fig.6 Search Engine

In this screen, User will search the file by entering secret key and will submit by him. Aftersubmitting the request will send to the Data owner and will give permission.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

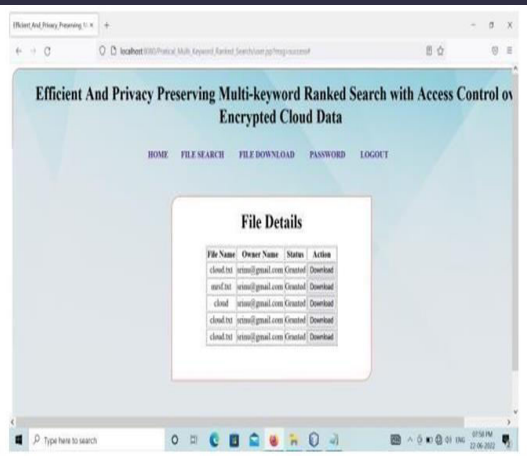


Fig.7 File Download Details

In this screen, User will download the file once the Data Owner granted the permission to theresponse send by him.

## 5. CONCLUSION AND FUTURE ENHANCEMENTS

In this paper, I suggest a privacy-preserving multikeyword search scheme with light-weight fine-grained get entry to control (MRSF). Compared with preceding schemes, besides realizing get right of entry to control, MRSF achieves a higher search performance and greater security level. In order to improve the practicability and safety of MRSF, I combine the TF-IDF rule with the conventional coordinate matching method and integrate the access control method with the accelerated tightly closed kNN scheme. Formal security definitions and corresponding evaluation show that MRSF is IND-CLS-CPA secure, I additionally show that MRSF is resistant to the consultant KPAs. Finally, good sized opinions exhibit the influential elements for search accuracy and efficiency of MRSF. As a future work, I layout to discover and advance a protocol that lets in a couple of users to share facts throughout distinct cloud servers, with the motivation of enhancing the effectivity of information sharing among multiple users.

## 6. BIBLIOGRAPHY

[1] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Toward secure multi-keyword top-k retrieval over encrypted cloud data," IEEE Transactionson Dependable and Secure Computing, vol. 10, no. 4, pp. 239–250, July2013.

[2] K. Cheng, L. Wang, Y. Shen, H. Wang, Y. Wang, X. Jiang, andH. Zhong, "Secure k-nn query on encrypted cloud data withmultiple keys," IEEE Transactions on Big Data, pp. 1–1, 2017.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp.222–233, Jan 2014.

[4] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proceeding 2000 IEEE Symposiumon Security and Privacy. S P 2000, May 2000,pp. 44–55.

[5] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure andefficient ranked keyword search over outsourced cloud data,"IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8,pp. 1467–1479, Aug 2012.

[6] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," Journal of Computer Security, vol. 19, no. 5, pp. 895–934,2011.

[7] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited:consistency properties, relation to anonymousibe, and extensions," in Advances in Cryptology – CRYPTO 2005.Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 205–222.

[8] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology -EUROCRYPT 2004, C. Cachin and J. L. Camenisch, Eds. Springer Berlin Heidelberg, 2004, pp. 506–522.

[9] Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, "Efficient multi-keyword ranked query on encrypted data in the cloud," in 2012 IEEE18th International Conference on Parallel and Distributed Systems, Dec2012, pp. 244–251.

[10] 104th United States Congress, "Health insurance portability and accountability act of 1996 (hippa)," 1996.

[11] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data accesscontrol based on trust and reputation in cloud computing," IEEETransactions on Cloud Computing, vol. 5, no. 3, pp. 485–498, July2017.

[12] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure knn computation on encrypted databases," in Proceedings of the2009 ACM SIGMOD International Conference on Management of Data,ser. SIGMOD '09. New York, NY, USA: ACM, 2009, pp. 139– 152.[Online]. Available: http://doi.acm.org/10.1145/1559845.1559862