**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**
**IMPACT FACTOR: 5.258**

*IJCSMC, Vol. 5, Issue. 4, April 2016, pg.210 – 216*

# Seclusion Preserving Ranked Multi-Keyword Investigate for Manifold Records in Cloud Computing

**P.Padmapriya [1], T.Sravani [1], P.Umasri [1], N.Aravind [1], N. Lakshmi Narayana [2]**

[1]UG Scholar, Department of Computer Science & Engineering, St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh, India

[2]Asst.Professor, Department of Computer Science & Engineering, St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh, India

[1] padmapriyapeteti@gmail.com, [2] thisisnarayan@gmail.com

***Abstract:*** *Observing the view of cloud computing, it has become augmenting popular for data owners to outside supplier their information to public cloud servers while allowing data users to regain this data. To relate to seclusion, safe searches over encrypted cloud data have provoke more research works under the sole owner model. However, most cloud servers in practice do not just Serve unique owner; instead, they support multiple owners to share the benefits brought by cloud computing. In this paper, we suggest -To keep safe the secrecy and several owner model search several keywords and Ranked. To make possible cloud servers to execute safe to look omission knowing the real information of both keywords and trapdoors, To keep alive the privacy of related scores between keywords and files and rank the search result, we suggest a novel Additive Order and Privacy Preserving Function family and dynamic hidden key creation rule and a new data user to establish as genuine rule.*

***Keywords:*** *Cloud computing, ranked keyword search, several owners, privacy preserving*

## I. INTRODUCTION

Cloud storage system, is set of storage servers, and provides long-term storage services over the Internet. Storing data in a third party's cloud system causes grave to connect to over data secret. Normal hidden schemes defend data secret but have some limitation to functionality of the storage system because a few operations are supported over hidden information. Building a grave storage system that compatible several functions is endurance when system is distributed. Service providers of cloud would pledge to owners data security using phenomenon like virtualization and firewalls. These phenomenons do not protect owners data privacy from the CSP itself, since the CSP control whole of cloud hardware, software, and owners' data. Hiding the sensitive data before send outside can stored data confidentiality against CSP. Data hidden makes the conventional data utilization service based on plaintext keyword search a very challenging problem. A solution to this problem is to download all the hidden data and create the original data using the hidden key, but this is not practical cause it create extra overhead In this paper, we suggest when search multiple owner multiple keywords that time provide the privacy and show the result in ranking form to make easy cloud servers to perform safe search excluding knowing the real value of both keywords and trapdoors, we properly build a novel safe search rule. So that various data owners use distinct keys to hide their files and keywords. Genuine data users can get a query excluding knowing confidential keys of these various data owners. To rank the search results and preserve the privacy of relevance scores between keywords and files, we suggest a family which preserves privacy, which helps the cloud server return the most relevant search results to data users without revealing any sensitive information. To protect from disclosing the result we propose a novel dynamic secret key generation protocol and a new data user authentication rule[1].

The main contributions of this paper are listed as follows:

- We define search data on cloud that data is hidden format and also providing the privacy when search the multiple keywords.
- We suggest an capable data user authentication rule, which stop attackers to disclose hidden key and only genuine data user can do search.
- We suggest a approach that performs multiple key word search and rank them properly.

## II. LITERATURE SURVEY

***Secured Multi-keyword Ranked Search over Encrypted Cloud Data***: In cloud computing data possessor are goaded to farm out their complex data management systems from local sites to the commercial public cloud for greater flexibility and economic savings. To ensure safety of stored data, it is must to encrypt the data before storing. It is necessary to invoke search with the encrypted data also. The specialty of cloud data storage should allow copious keywords in a solitary query and result the data documents in the relevance order. In [1], main aim is to find the solution of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving strict system-wise privacy in the cloud computing paradigm. A variety of multi- keyword semantics are available, an efficient similarity measure of "coordinate matching" (as many matches as possible), to capture the data documents' relevancy to the search query is used. Specifically "inner product similarity", i.e., the number of query keywords appearing in a document, to quantitatively evaluate such similarity measure of that document to the search query is used in MRSE algorithm.

The main limitation of this paper was, the user's identity(ID) is not kept hidden. Due to this, whoever puts the data on Cloud Service Provider was known. This may be risky in some situations where confidentiality of data need to be maintained. Hence, this drawback is overcome in the proposed system.

***Privacy Preserving Keyword Searches on Remote Encrypted Data***: Consider the problem: a user *U* wants to store his files in an encrypted form on a remote file server *S*. Later the user *U* wants to efficiently retrieve some of the encrypted files containing specific keywords, keeping the keywords themselves secret and not to endanger the security of the remotely stored files. For example, a user may want to store old e-mail messages encrypted on a server managed by Yahoo or another large vendor, and later retrieve certain messages while travelling with a mobile device. In [2], solutions for this problem under well-defined security requirements are offered.

The schemes are efficient as no public-key cryptosystem is involved. Indeed, the approach is independent of the encryption method chosen for the remote files. They are incremental too. In that, user *U* can submit new files which are secure against previous queries but still searchable against future queries. From this, the main theme taken is of storing data remotely on other server and retrieving that data from anywhere via mobile, laptop etc.

***Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data:*** On one hand, users who do not necessarily have prior knowledge of the encrypted clouddata, have to post process every retrieved file in order to find ones most matching their interest; On the other hand, invariably retrieving all files containing the queried keyword further incurs unnecessary network traffic, which is absolutely undesirable in today's pay-as-you-use cloud paradigm. This paper has defined and solved the problem of effective yet secure ranked keyword search over encrypted cloud data [4]. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency) thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. For the first time, the paper has defined and solved the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. The proposed ranking method proves to be efficient to return highly relevant documents corresponding to submitted search terms. The idea of proposed ranking method is used in our proposed system in order to enhance the security of data on Cloud Service Provider.

***Providing Privacy Preserving in Cloud Computing:***

Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust and needs to be considered at every phase of design. The [5] paper tells the importance of protecting individual's privacy in cloud computing and provides some privacy preserving technologies used in cloud computing services. Paper tells that it is very important to take privacy into account while designing cloud services, if these involve the collection, processing or sharing of personal data. From this paper, main theme taken is of preserving privacy of data. This paper only describes privacy of data but doesn't allow indexed search as well as doesn't hide user's identity. Thus, these two drawbacks are overcome in our proposed system.

## III. PROBLEM FORMULATION

### A. System Model

The system model can be considered as three entities, as depicted in Figure1:the data owner, the data user and the cloud server.

**Data owner** has a collection of data documents D □ $\{d1 , d 2 , ..., d m \}$ .A set of distinct keywords W =□ $\{w1 , w2 , ..., wn \}$ is extracted from the data collection *D* . The data owner will firstly construct an encrypted searchable index *I* from the data collection *D* . All files in *D* are encrypted and form a new file collection, *C* .Then, the data owner upload both the encrypted index *I* and the encrypted data collection *C* to the cloud server.

**Data user** provides *t* keywords for the cloud server. A corresponding trapdoor *w T* through search control mechanisms is generated. In this paper, we assume that the authorization between the data owner and the data user is approximately done.

**Cloud server** received *w T* from the authorized user. Then, the cloud server calculates and returns to the corresponding set of encrypted documents. Moreover, to reduce the communication cost, the data user may send an optional number *l* along with the trapdoor *T* so that the cloud server only sends back top- *l* files that are most relevant to the search query.

### B. THREAT MODELS AND DESIGN GOALS

The cloud server is considered as "honest-but-curious" in our model. Particularly, the cloud server both follows the designated protocol specification but at the same time analyzes data in its storage and message flows received during the protocol so as to learn additional information[12].

In this paper, we purpose to achieve security and ranked search under the above model. The designed goals of our system are following:

**Multi-keyword Ranked Search:** It supports both multi-keyword query and support result ranking.

**Privacy-Preserving:** Our scheme is designed to meet the privacy requirement and prevent the cloud server from learning additional information from index and trapdoor.

*1) Index Confidentiality*. The *TF* values of keywords are stored in the index. Thus, the index stored in the cloud server needs to be encrypted;

*2) Trapdoor Unlinkability*. The cloud server could do some statistical analysis over the search result. Meanwhile, the same query should generate different trapdoors when searched twice. The cloud server should not be able to deduce relationship between trapdoors.

*3) Keyword Privacy*. The cloud server could not discern the keyword in query, index by analyzing the statistical information like term frequency.

## IV. EXISITING SYSTEM & DISADVANTAGES

The large number of data users and documents in cloud, it is crucial for the search service to allow multi-keyword query and provide result similarity ranking to meet the effective data retrieval need. The searchable encryption focuses on single keyword search or Boolean keyword search, and rarely differentiates the search results. Existing searchable encryption schemes allow a user to securely search over encrypted data through keywords without first decrypting it. These techniques support only conventional Boolean keyword search, without capturing any relevance of the files in the search result. In this there is a single data owner to upload files in the cloud.

Disadvantage:

- » Single-keyword search without ranking
- » Boolean- keyword search without ranking
- » Single-keyword search with ranking

## V. PROPOSED SYSTEM & ADVANTAGES

Consider the Cloud data hosting service contains four different entities, as listed in fig. 1: the data owner, the data user, the trusted third party, and the cloud server. Consider data owner will registers on cloud for cloud computing service. Anonymous algorithm is used to process the registration information of user and then saves anonymous data to registration database. The data owner has a collection of data documents D to be outsourced to the cloud server in the encrypted form E. Before outsourcing, the data owner will first build an encrypted searchable index I from D to enable searching capability over E for effective data utilization. The data owner will outsource the encrypted document collection D to the cloud server and encrypted index to the trusted third party. The trusted third party will check the integrity of outsourced data without violating user privacy policies. Anonymous identifiers are assigned to user using efficient algorithms. The data user send the encrypted search query to the cloud server along with his session ID. This encrypted search query is transferred to the trusted third party for processing by cloud server. The trusted third party will search index using "string matching" and sends the search results to the cloud server which returns the corresponding set of encrypted documents to the data user.

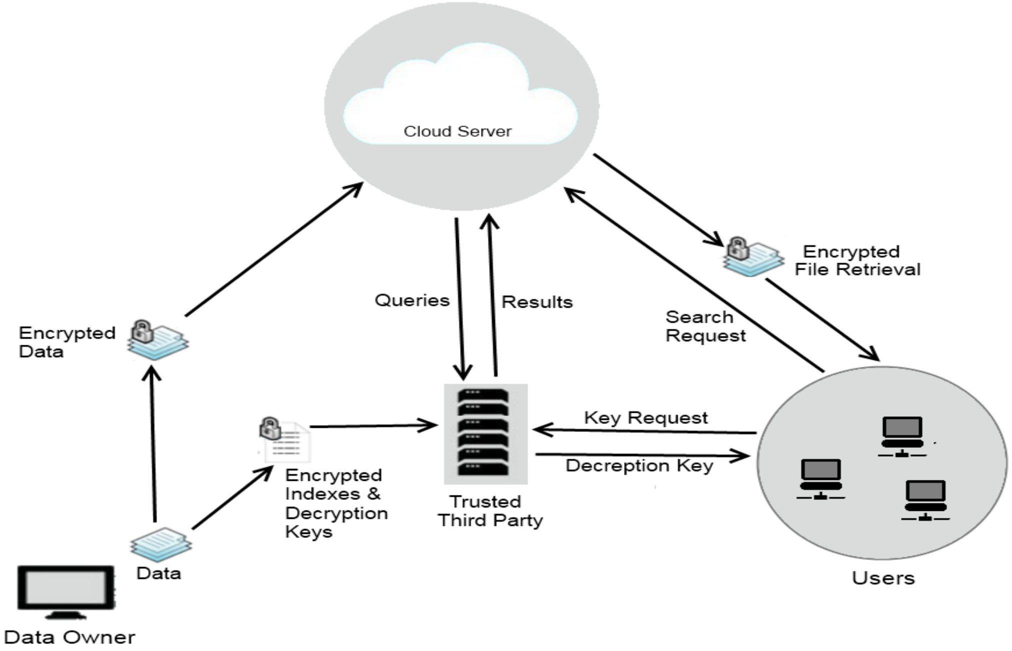


Fig.1 Architecture of search over encrypted data cloud

To enable ranked search for effective utilization of outsourced cloud data under the aforementioned model, our system design should simultaneously achieve security and performance guarantees as follows. Multi-keyword ranked search. To design search schemes which allow multi-keyword query and provide result similarity ranking for effective data retrieval, instead of returning undifferentiated results. Privacy-preserving. To prevent the cloud server from learning additional information from the data set and the index, and to meet privacy requirements. Efficiency. Above goals on functionality and privacy should be achieved with low communication and computation overhead.

## Advantages:

- Multi-keyword ranked search over encrypted cloud data (MRSE).
- “Coordinate matching” by inner product similarity.
- We propose an Additive order and Privacy Preserving Function Family (AOPPF).
- It is a secured process.

### VI. Privacy-Preserving Public Auditing for Secure Cloud Storage

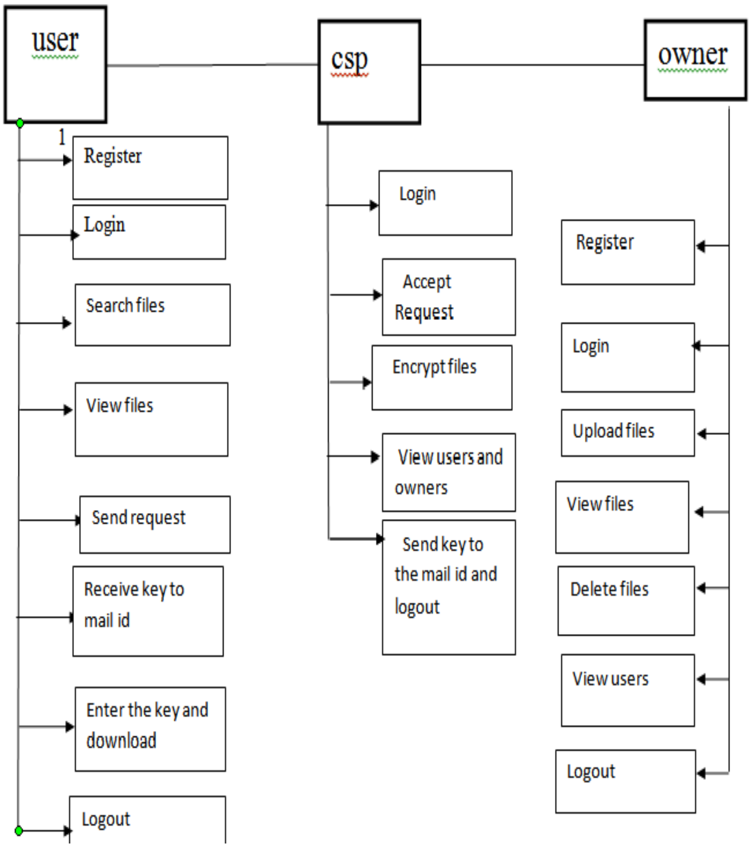
Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

As the data produced by enterprises and individuals that need to be stored and utilized is rapidly increasing, data owners are motivated to outsource their local complex data management systems into the cloud for its great flexibility and economic savings. To protect data privacy and combat unsolicited accesses in cloud and beyond, sensitive data has to be encrypted before outsourcing .To explore such a privacy-assured and effective cloud data utilization service with high service-level performance and usability, by investigating the two challenging research tasks: fuzzy keyword search and ranked keyword search over encrypted cloud data.

**Fuzzy keyword search**, opposing to exact keyword match, tolerates minor typos and format inconsistencies in user search request, and greatly enhances system usability and user searching experience. Its challenge lies in the fact that two words similar to each other would no longer be so after one-way cryptographic transformation (for encrypted keyword search).

**Ranked keyword search** further ensures the file retrieval accuracy and allows the user to find the most/least relevant information efficiently. We explore the statistical measure approach (i.e. relevance score) from information retrieval (IR), and properly hide the scores in an order-preserved manner. The resulting design is expected to facilitate efficient server-side ranking without losing keyword privacy.

## VII. SYSTEM ARCHITECTURE



## VIII. CONCLUSION & FUTURE SCOPE

The previous work mainly focused on providing privacy to the data on cloud in which using multi-keyword ranked search was provided over encrypted cloud data using efficient similarity measure of co-ordinate matching. The previous work [4] also proposed a basic idea of MRSE using secure inner product computation. There was a need to provide more real privacy which this paper presents. In this system, stringent privacy is provided by assigning the cloud user a unique ID. This user ID is kept hidden from the cloud service provider as well as the third party user in order to protect the user's data on cloud from the CSP and the third party user. Thus, by hiding the user's identity, the confidentiality of user's data is maintained. In this paper, the asserting problem of searching encrypted cloud data using ranked multi-keyword (MRSE) is defined and solved. Out of distinct multi-keyword semantics, the adequate similarity measuring of "coordinates matching" and "inner product similarity, i.e., possibilities of many matches for capture the documents from query search perceptible evaluations for similarity measures. Adopting the basic idea for the MRSE based on secure inner product computation and archive privacy requirements in two distant thread models. Experiments based on the real-world data further showing an indeed advent of low overhead on computation and communication. In future, the cloud server is treated as entrusted state, the integrity checking of the rank order in search results analyse.

## REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 1, pp. 50–55, 2009.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *RLCPS,January 2010, LNCS. Springer, Heidelberg*.

[3] A. Singhal, "Modern information retrieval: A brief overview," *IEEE Data Engineering Bulletin*, vol. 24, no. 4, pp. 35–43, 2001.

[4] I.H.Witten, A.Moffat and T.C.Bell "Managing Gigabytes: Compressing and indexing documents and images", Morgan Kaughmann Publishing, San Fransisco, 1999.

[5] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. of S&P*, 2000.

[6] E.-J. Goh, "Secure indexes," Cryptology ePrint Archive, 2003, http:// eprint.iacr.org/2003/216.

[7] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in *Proc. of ACNS*, 2005.

[8] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proc. of ACM CCS*, 2006.

[9] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. of EUROCRYPT*, 2004.

[10] M. Bellare, A. Boldyreva, and A. ONeill, "Deterministic and efficiently searchable encryption," in *Proc. of CRYPTO*, 2007.

[11] 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 anonymous ib e, andextensions," *J. Cryptol.*, vol. 21, no. 3, pp. 350–391, 2008.

[12] [12] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proc. of IEEE INFOCOM'10 Mini-Conference*, San Diego, CA, USA, March 2010.

[13] [13] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. S. III, "Public key encryption that allows pir queries," in *Proc. of CRYPTO*, 2007.

[14] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in *Proc. of ACNS*, 2004, pp.