SHIV SHAKTI
International Journal in Multidisciplinary and Academic Research (SSIJMAR)
Vol. 7, No. 2, April 2018 (ISSN 2278 – 5973)

# Privacy Preserving Multi Keyword Search For Multiple Data Owners

Manikantha Desu and M.Mounica, P.Manisha, V.Lahari sowmya,
Department of Computer Science and Engineering,
Hyderabad Institute of Technology and Management,
JNTUH, Hyderabad, Telangana, India.

"Corresponding Author: sneham.cse@hitam.org"

**Abstract :** With the advent of cloud computing, it has become increasingly popular for data owners to outsource their data to public cloud servers while allowing data users to retrieve this data. For privacy concerns, secure searches over encrypted cloud data has motivated several research works under the single owner model. However, most cloud servers in practice do not just serve one owner; instead, they support multiple owners to share the benefits brought by cloud computing. In this paper, we propose schemes to deal with privacy preserving ranked multi-keyword search in a multi-owner model (PRMSM). To enable cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel additive order and privacy preserving function family. To prevent the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, we propose a dynamic secret key generation protocol and a new data user authentication protocol. Furthermore, PRMSM supports efficient data user revocation. Extensive experiments on real-world datasets confirm the efficacy and efficiency of PRMSM.

## 1. INTRODUCTION

CLOUD computing is a subversive technology that is changing the way hardware and software are designed and purchased [1]. As a new model of computing, cloud computing provides abundant benefits including easy access, decreased costs, quick deployment and flexible resource management, etc. Enterprises of all sizes can leverage the cloud to increase innovation and collaboration. Despite the abundant benefits of cloud computing, for privacy concerns, individuals and enterprise users are reluctant to outsource their sensitive data, including emails, personal health records and government confidential files, to the cloud. This is because once sensitive data are outsourced to a remote cloud, thecorresponding data owners lose direct control of these data [2]. Cloud service providers (CSPs) would promise to ensure owners' data security using mechanisms like virtualization and firewalls.

However, these mechanisms do not protect owners' data privacy from the CSP itself, since the CSP possesses full control of cloud hardware, software, and owners' data. Encryption on sensitive data before outsourcing can preserve data privacy against CSP. However, data encryption makes the traditional data utilization service based on plain text keyword search a very challenging problem. A trivial solution to this problem is to download all the encrypted data and decrypt them locally. However, this method is obviously impractical because it will cause a huge amount of communication overhead.Therefore, developing a secure search service over encrypted cloud data is of paramount importance.

## 2. LITERATURE SURVEY

Because of the expanding fame of distributed computing, an ever increasing number of information proprietors are roused to outsource their information to cloud servers for incredible accommodation and decreased cost in information administration. Nevertheless, fragile data should be encoded before outsourcing for security requirements, which obsoletes data utilize like catchphrase based record recuperation. In this paper, we show an ensured multi-catchphrase situated look for scheme over mixed cloud data, which in the meantime supports dynamic revive operations like eradication and expansion of chronicles. Specifically, the vector space exhibit and the comprehensively used TF x IDF show are combined in the record advancement and request age. We manufacture a one of a kind tree-based rundown structure and propose an "Insatiable Depth-first Search" count to give capable multi-catchphrase situated look. The safe kNN computation is utilized to encode the document and request vectors, and after that certification correct significance score figuring between mixed record and question vectors. With a particular true objective to restrict verifiable attacks, phantom terms are added to the rundown vector for blinding rundown things. In light of the use of our phenomenal tree-based rundown structure, the proposed plan can finish sub-straight request time and deal with the cancelation and expansion of chronicles adaptably. Wide examinations are coordinated to demonstrate the adequacy of the proposed plot.

## 3. METHOD AND ANALYSIS

**System Overview:**

Define a multi-owner model for privacy preserving with the encrypted key which is shared between and user and owner Generating the Keys also uses a encryption algorithm, so key is also secured.
Constructing a secure search protocol, which not only enables the cloud server to perform secure ranked keyword search without knowing the actual data of both keywords and trapdoors.
The searching mechanism is even implemented with the help of k-means or even with better algorithm. This phenomena helps us build a better model in maintaining the search parameters for indexing them to the data and keyword.

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.
There is no security key for accessing the data from the resources files.
No algorithm used for the security features.

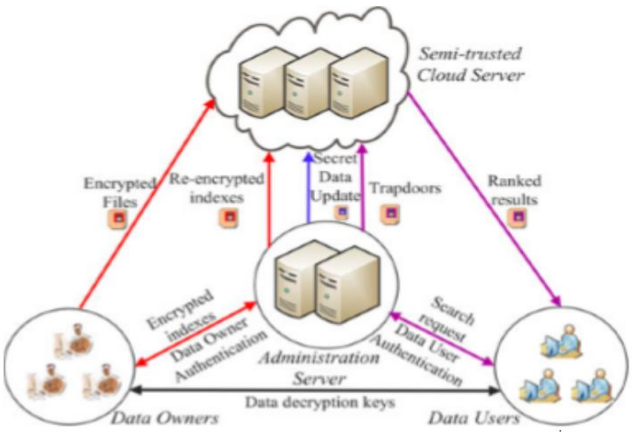



*Fig 3.0: BLOCK DIAGRAM*

## 4. REQUIREMENT SPECIFICATION

The reason for this SRS record is to distinguish the necessities andfunctionalities for Intelligent Network Backup Tool. The SRS will characterize how our group and the customer consider the last item and the attributes or usefulness it must have. This record additionally makes a note of the discretionary prerequisites which we intend to execute yet are not required for the working of the venture. This stage assesses the required necessities for the Images Processing for an orderly method for assessing the prerequisites a few procedures are included. The initial step associated with dissecting the prerequisites of the framework is perceiving the idea of framework for a solid examination and all the case are defined to better comprehend the investigation of the dataset.

## 5. SYSTEM WORKING

MODULES:

Cloud Accounts:

The cloud accounts will be created for the user and the accessor

Encryption Key:

The keys will be created for accessing the data between user and the accessor

Information Sharing:

The data is shared once the keys are actived and authentication is done

Keyword Search:

The keywords are searched based on the KNN algorithm and are indexed to each article

Top Articles:

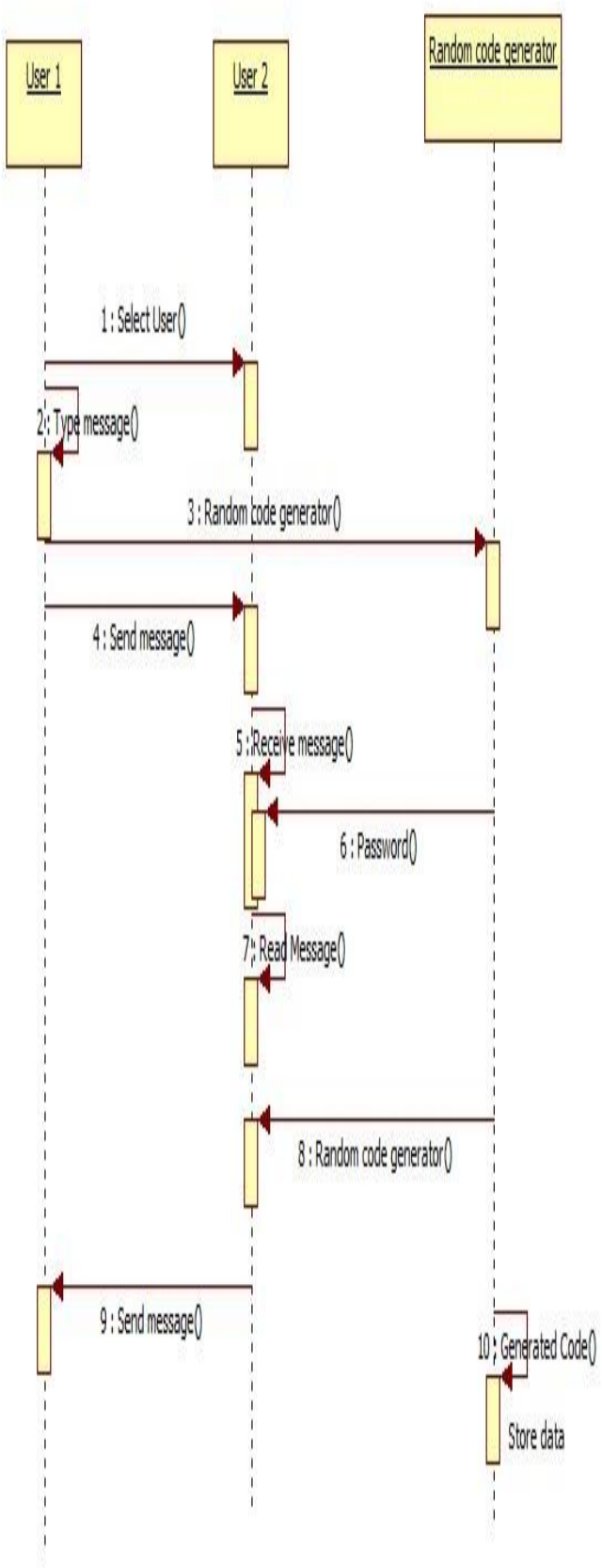
The searching techniques are implemented and then top articles are shared between the users.

The System Design Document describes the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human-machine interfaces, detailed design, processing logic, and external interfaces.

This section describes the system in narrative form using non-technical terms. It should provide a high-level system architecture diagram showing a subsystem breakout of the system, if applicable. The high-level system architecture or subsystem diagrams should, if applicable, show interfaces to external systems. Supply a high-level context diagram for the system and subsystems, if applicable. Refer to the requirements trace ability matrix (RTM) in the Functional Requirements Document (FRD), to identify the allocation of the functional requirements into this design document.

This section describes any constraints in the system design (reference any trade-off analyses conducted such, as resource use versus productivity, or conflicts with other systems) and includes any assumptions made by the project team in developing the system design.

The organization code and title of the key points of contact (and alternates if appropriate) for the information system development effort. These points of contact should include the Project Manager, System Proponent, User Organization, Quality Assurance (QA) Manager, Security Manager, and Configuration Manager, as appropriate.



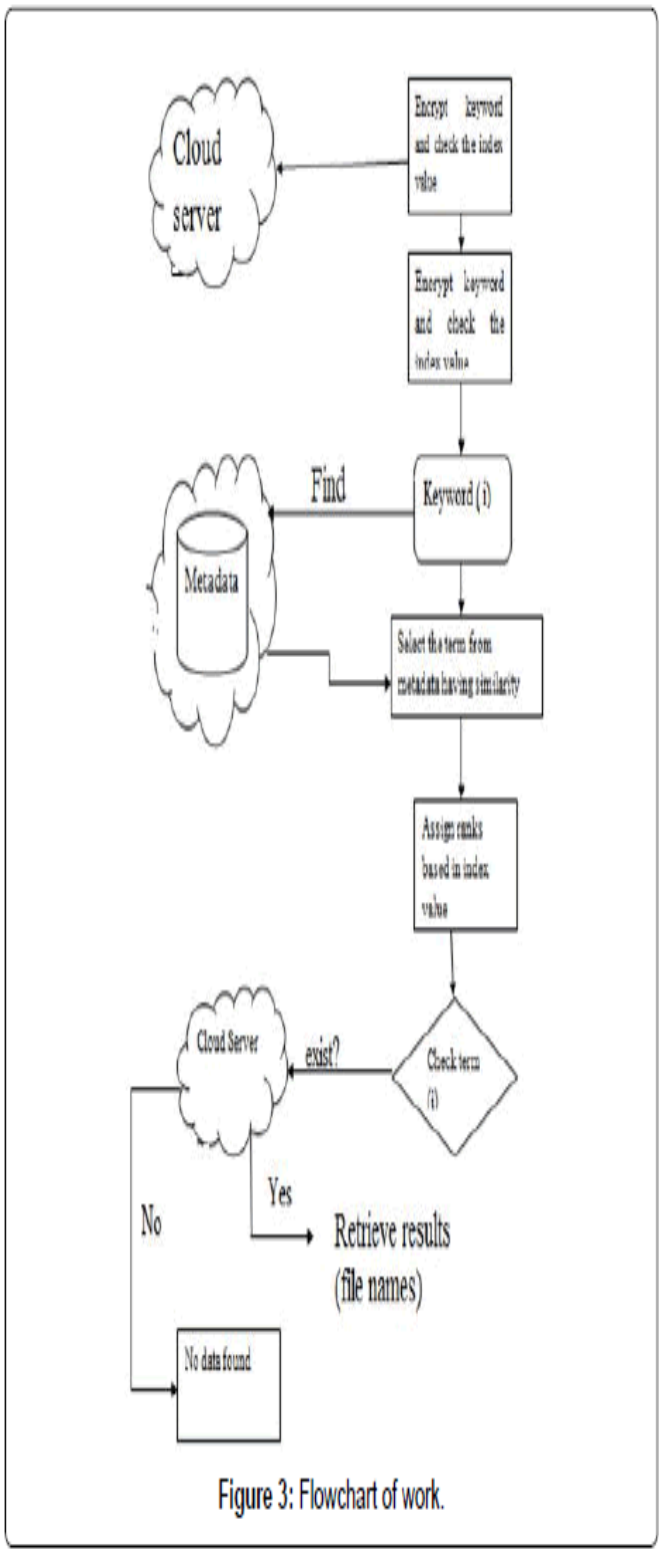


Figure 3: Flowchart of work.

## 6.Conclusion:

In this paper, we explore the problem of secure multi-keyword search for multiple data owners and multiple data users in the cloud computing environment. Different from prior works, our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data. To efficiently authenticate data users and detect attackers who steal the secret key and perform illegal searches, we propose a dynamic secret key generation and a new data user authentication protocols. In order to enable the cloud server to perform secure search among multiple owners' data encrypted with different secret keys, we systematically construct a novel secure search protocol. To preserve the privacy of relevance scores between keywords & files and rank the search results , we propose a additive order and privacy preserving function family. Further, we show that our approach is computationally efficient, even for large data and keyword sets. As our future work, on one hand, we will consider the problem of secure fuzzy keyword search in a multi-owner paradigm. On the other hand, we plan to implement our scheme on the commercial clouds.

## 7. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[3] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc.

IEEE Int. Symp. Security Privacy, Nagoya, Japan, Jan. 2000, pp. 44–55.

[4] E. Goh. (2003). Secure indexes [Online]. Available: http://eprint.iacr.org/

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Security, Oct. 2006, pp. 79–88

| | |
|---|---|
|  | *Manikantha Desu*<br>*Assistant professor*<br>HITAM |
|  | *M. Mounica*<br>CSE<br>HITAM |
|  | *P. Manisha*<br>CSE<br>HITAM |
|  | *V. Lahari sowmya*<br>CSE<br>HITAM |
| | |