REVIEW ON DYNAMIC MULTI-KEYWORD RANKED SEARCH OVER ENCRYPTED MOBILE CLOUD DATA

[1]Manshi Ratanghayra, [2]Prof. Dhaval Nimavat
[1]Student, [2]Head of Department
[1]Atmiya Institute of Science and Technology,
[2]Atmiya Institute of Science and Technology, Rajkot, India

Abstract*—The popularity of using cloud service is increasing on a rapid scale. Here, the core idea is to out-source the mobile data into the external cloud server. But the big point of concern is, whether our sensitive data is stored securely or not and whether the securely stored data can be accessed with ease and only to the one who are intended to access it. The question of whether the data antiquates data utilization like keyword based document retrieval. Thus, allowing keyword-based search on encrypted cloud data is of vital prominence. In this paper, an attempt is made to survey various searching techniques towards effective search over encrypted cloud data.

***Index Terms*—Cloud computing, Multi-keyword Ranked search, Searchable encryption, Sparse matrix, Dynamic operation.**

I. INTRODUCTION

Nowadays, cloud computing is considered as the highly developed and innovative technology. Due to its offerings like flexibility and low management costs and also now more and more companies and users are planning to out-source their local data to the public clouds. Even though cloud has many benefits, the most important area of concern in cloud computing is privacy and security. Thus, the solution is to encrypt the sensitive data before out-sourcing to the public cloud server. However, it makes the traditional plain-text keyword search method antiquate and thus results in huge overhead on the encrypted data availability. Apparently, it is quite unrealistic to download and decrypt all data on the client side. Thus, in today's infrastructure, it is necessary to build a secure search service on encrypted data. This paper presents a survey of a secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. The below **Fig.1** shows the concept of cloud computing.

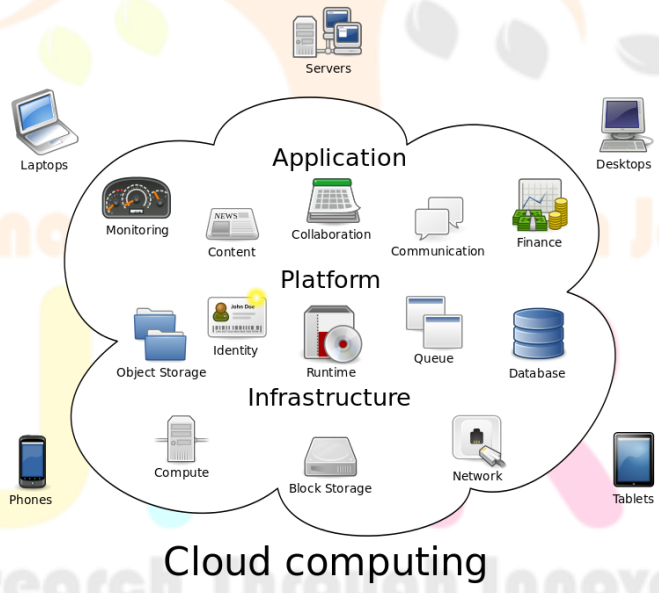

Figure 1. Cloud Computing concept [1]

This paper is organized as follows: In Section 2, the literature survey of the papers related to the searchable encryption techniques. It shows the comparative study in Section 3. Then the paper is concluded in Section 4.

II. LITERATURE SURVEY

This section of paper server the literature survey of various papers related to Multi-keyword ranked search over encrypted cloud data in cloud. It describes the research work already done by the authors corresponding to searchable encryption in cloud computing.

[Lanxiang Chen, Et. al][2] This paper proposed a novel and efficient scheme which is improved from traditional secure kNN computation. It supports dynamic operation on document collection, allowing insertion and deletion operations in document. The future work consist of fine-grained access authorization and the revocation of the user are big challenges.

[Tao Peng, Et. al][3] This paper proposes Multi-Level Access Control Scheme. It protects user data by providing different security levels, while offering multilevel access control and valid identity authentication. This scheme is effective in multilevel data security, flexible in authorized resource sharing, and secure against various malicious attacks. For future work**,** they will improve this scheme by deploying

multiple Authentication servers to avoid the potential bottleneck between users and the transparent servers, and ensure high availability of the system.

[ChengGuo, Et. al][4] This paper uses Identity-based encryption which is a suitable scheme for dynamic cloud storage. It solves the secret-key leakage problem by setting up an effective identity authentication. This scheme supports secure, efficient, and flexible data sharing via cloud storage. Its future work includes flexible and leakage-resilient delegation scheme with compact keys.

[Jian Shen, Et. al][5] This paper uses One-way hash functions, String concatenation operations and XOR operations. It is a novel lightweight authentication-based access control scheme, which is designed by exclusive-or operations, string concatenation and hash functions resulting in lower computation cost. Also, the main computing work is transferred to the authorized agency, hence, the computation of the user side and the server side is lower than the related authentication scheme for cloud.

[Zhirong Shen, Et. al][6] This paper proposes a novel scheme called Keyword Search with Access Control (KSAC) which It shows an efficient multi-keyword search scheme that can return the ranked search results based on the accuracy. The performance evaluation has shown that it can achieve improve efficiency in terms of search time and search functionality. Its future direction include possibility to use authentication and access control techniques in searchable encryption technique.

III. COMPARITIVE STUDY

Table I Comparative analysis of related papers.

Sr. No.	Title	Author	Proposed Method	Advantages	Research Gap /Limitation
1.	DMRS: an efficient dynamic multi-keyword ranked search over encrypted cloud data	Lanxiang Chen Et Al. 2017	Improved KNN Scheme	Allows Dynamic updation of uploaded Documents.	Access Control and Authentication yet to be covered.
2.	A Multilevel Access Control Scheme for Data Security in Transparent Computing	Tao Peng Et Al 2017	Multi-Level Access Control Scheme	Offers multilevel access control and valid identity authentication	Low system availability problem.
3.	Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage	ChengGuo Et Al. 2017	Identity-based encryption	Secure, efficient, and flexible data sharing	Can use more Compact keys than the one used.
4.	An Authorized Identity Authentication-based Data Access Control Scheme in Cloud	Jian Shen Et Al. 2016	-One-way hash functions -String concatenation operations -XOR operations	Lower computation cost	Main computing work is transferred to the authorized agency.
5.	Keyword Search With Access Control Over Encrypted Cloud Data	Zhirong Shen Et Al. 2016	Hierarchical Predicate Encryption	Perform multi-field query search	Cost for injecting noise
6.	The Method of Ensuring Confidentiality and Integrity Data in Cloud Computing	Andrey N. Rukavitsyn 2017	EaaS-service for encryption	Based on OpenStack platform	Searchable encryption issue not addressed.
7.	Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage	Hongwei Li 2015	Searchable encryption, Blind storage	Returns Ranked Search results	Authentication and access control

IV. CONCLUSION

After the comparative study of various literatures, it is concluded that each approach has its own pros and cons. Neither paper covers authentication and access control on encrypted cloud data which allows multi keyword ranked search on encrypted cloud data. Individual approaches including searchable encryption with multi keyword ranked search exists. Also papers consisting authentication and access control on cloud storage exists. So a new hybrid approach, where searchable encryption and access control with authentication can be combined, can be devised.

V. ACKNOWLEDGMENT

I heartily acknowledge Prof. Dhaval Nimavat, Atmiya Institute of Technology, Rajkot, my family and well-wishers.

REFERENCES

[1] https://en.wikipedia.org/wiki/Cloud_computing

[2] Chen, Lanxiang, et al. "DMRS: an efficient dynamic multi-keyword ranked search over encrypted cloud data." *Soft Computing* 21.16 (2017): 4829-4841.

[3] Peng, Tao, Qin Liu, and Guojun Wang. "a multilevel access Control scheme for Data security in Transparent Computing." *Computing in Science & Engineering* (2016).

[4] Guo, Cheng, et al. "Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage." *Future Generation Computer Systems* (2017).

[5] Shen, Jian, et al. "An authorized identity authentication-based data access control scheme in cloud." *Advanced Communication Technology (ICACT), 2016 18th International Conference on*. IEEE, 2016.

[6] Shen, Zhirong, Jiwu Shu, and Wei Xue. "Keyword Search With Access Control Over Encrypted Cloud Data." *IEEE Sensors Journal* 17.3 (2017): 858-868.

[7] Rukavitsyn, Andrey N., et al. "The method of ensuring confidentiality and integrity data in cloud computing." *Soft Computing and Measurements (SCM), 2017 XX IEEE International Conference on*. IEEE, 2017.

[8] Li, Hongwei, et al. "Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage." *IEEE Transactions on Emerging Topics in Computing* 3.1 (2015): 127-138.