Survey on Efficient Searching Over Encrypted Data in Cloud Computing

Priyanka Deshpande[1], Prof. D.V. Jadhav[2]
[1, 2] Department of Computer Engineering
[1, 2] Zeal College of Engineering & Research,Pune, India.

Abstract*-development in cloud computing have changed the view of IT, it encourages the data owner to store their information on the public cloud server such as Google Drive, Amazon, Microsoft Azure and so on. It has provided several advantages for the organizations as they can offer reliable information services to the clients and also they don't have to carry the burden of managing data. Cloud also provides Storage as a Service which is effective in terms of cost also user can get their data anytime and from anywhere. In common cloud service provider's deals with the data and privacy of it, however, there are some factors in view of which the privacy of data and identity of the user might be reviled such as an apostate employee, and so on. In this manner, owner of data must encode their individual information before outsourcing it to the public cloud server. As a data is encoded prior to storage it can spoil the performance of few vital data accessing operations such as searching of files. This survey present analysis on some of the systems developed for searching the encrypted data on the cloud.*

Keywords-Cloud Service Providers, Cloud Storage, Ranked-Search, Encrypted-Data Search, Secure cloud outsourcing.

I. INTRODUCTION

The rise in information and communication technologies (ICT) has modified the way associations and people used to day their every day work process and operations in business. As of late cloud computing has increased enormous consideration among analysts from both researchers and industry. It has developed as one of the promising advancements that is moving the processing worldview from conventional computing into the new time of cloud computing. The unavoidable access to dynamic unrestricted computing resources, system and communication framework with expanded versatility and adaptability has given figuring and correspondence to clients pervasively and at a moderate cost. Thus numerous establishments, associations and clients are relocating from customary processing situations to a cloud computing environment.

Although the advantages that gave by the cloud storage, notwithstanding, numerous security issues emerge in cloud storage that keep organizations from moving their information to cloud storage. Because of the certainties that cloud storage is normally facilitated by third party provider other than the information owner as well as cloud storage infrastructure is typically shared between various clients, information stored in cloud storage can be effortlessly focused by the masquerade attack as well as the insider information theft assault. These attacks undermine the security of information as well as the information protection of the stored information, as outcome, the information owner can't depend on cloud service providers to secure their important information. These attacks additionally incite the information owner to encode/encrypt all their important information, for example, the social security numbers (SSN), credit card information, and personal tax data before they can be spared in cloud storage. The encryption strategy may have reinforced the information security of cloud information; however it has additionally corrupted the efficiency of the information on the grounds that the encryption will minimize the search ability of the information. Particularly in the cloud computing environment, it is illogical for the client to download and unscramble the whole encoded information from the remote cloud server before a search takes place. In this way, an efficient scheme that backings search over encrypted information in cloud computing turns out to be extremely noteworthy before many organizations can exploit the cloud storage.

Many systems were developed in new researches that empower keyword search over encrypted data in cloud computing. The most well-known methods of these frameworks is indexing the keywords contain in every uploading information document to make a index file. The index document will be transferred alongside the encrypted information documents to the cloud storage for later hunt operation.

This survey presents the study of various systems implemented by various researchers for searching over encrypted data in cloud.

II. LITERATURE REVIEW

In paper [1] authors developed the MRSE-HCI system for adopting the needs of information explosion, retrieval of data as well as semantic search. Also a verifiable technique is developed to provide correctness as well as completeness of outcomes of results. At last they studied the efficiency of search as well as security.

In paper [2] authors have considered numerous famous authentication protocols for the context of next-generation mobile and CE network services. The basic weaknesses of current protocols can be solved using Zero Knowledge Proof (ZKP) technique to conform client passwords so an alternative ZKP protocol, SeDiCi 2.0, is depicted. This offers mutual as well as also two-factor authentication which can be seen as more secure against different phishing endeavors than existing trusted outsider protocols. The suitability of such a ZKP protocol for different CE-based cloud computing applications is illustrated. At last they developed an authentication protocol which is suitable for cloud-based services.

In paper [3] authors have developed a privacy-preserving, similarity-based text retrieval which not only restrict the server from accurately reconstructing the term composition of queries as well as files but also anonymizes the outcomes of search from unauthorized users. Also, the proposed system saves the relevance-ranking of the search server, as well as enables accounting of the number of files opened by every user.

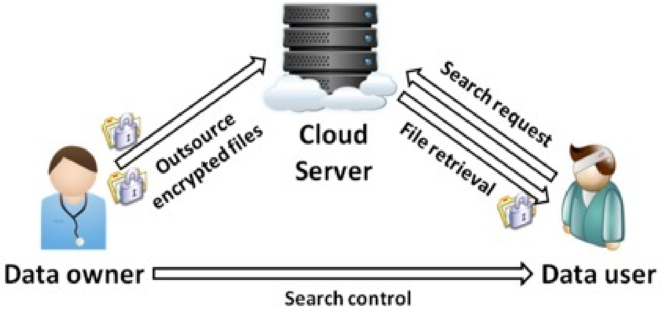
In paper [4] authors have developed a verifiable privacy-preserving multi-keyword text search (MTS) system having similarity-based ranking. For backing multi-keyword search as well as search result ranking, authors developed the search index based on term frequency as well as the vector space model with cosine similarity measure for getting high search accuracy results. For maximizing efficiency of search, they developed a tree-based index structure as well as different adaptive techniques for multi-dimensional (MD) algorithm hence the practical search efficiency is higher as compared with linear search.

In paper [5] authors have developed multi-keyword search system which enables file keyword search and also supports linear, gram based as well as semantic searches. Authors also implemented a special tree-based index structure as well as developed a fuzzy Search Server which generates wild card based fuzzy keyword Set that can handle KGA (Keyword Guessing Attack) as well as gives efficient multi-keyword ranked search.

In paper [6] authors tackled issue of data privacy as well as analyzed existing systems. After that developed an Efficient Privacy-Preserving Multi-keyword Ranked Search on Encrypted Data in Cloud Computing, proposed system makes use of LSI as well as hierarchical clustering for accessing as possible as files also maximized the efficiency of the search on encrypted data in the cloud environment. They utilized the semantic relationship in files as well as the query for achieving the efficient search that is well ranked depending on the query keywords with preserving data privacy.

In paper [7] authors have developed a secure, efficient as well as dynamic search system that supports accurate multi-keyword ranked search as well as the dynamic deletion and insertion of file. Also generated a special keyword balanced binary tree similar to index as well as implemented “Greedy Depth-first Search” algorithm for getting higher efficiency compared to linear search.

The basic architecture diagram of cloud given as follows:



Basic architecture of cloud

Table 1: Survey Table

Sr. No.	**Title**	**Paper Details**	**Method Used**	**Advantages**	**Limitations**
1.	An efficient privacy-preserving ranked keyword search method	Developed the MRSE-HCI architecture	Verifiable Search Based on Authenticated Index	Solves the multi-keyword ranked search problem	Multiple Data Owners not allowed.

2.	Security analysis of authentication protocols for next-generation mobile and CE cloud services	Developed an authentication protocol	Zero Knowledge Proof (ZKP) techniques	Provides a suitable solution for CE-based cloud authentication services	Efficiency can be increased
3.	Privacy-preserving similarity based text retrieval	Developeda privacy-preserving, similarity-based text retrieval model	Vectorspace model	Privacy protection is achieved	retrieval effectiveness can be increased
4.	Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking	Verifiable privacy-preserving multi-keyword text search (MTS)	Term frequency and the vector space model	Effective and efficient	efficient secure search functions over encrypted data
5.	Encrypted multi-keyword ranked search supporting gram based search technique	Developed multi-keyword search system	kNN algorithm	Reduces the need of enumerating all the keywords	Access control is not provided

III. CONCLUSION

This survey provides the details study of the various systems designed by different researchers for searching the encrypted data on cloud environment also listed their advantages and disadvantages. To overcome the disadvantages in the present system authors proposed a new system for searching the encrypted data in cloud environment.

REFERENCES

[1] C. Chen "An efficient privacy-preserving ranked keyword search method." IEEE Transactions on Parallel and Distributed Systems 27.4 (2016): 951-963.

[2] S. Grzonkowski, P. M. Corcoran, and T. Coughlin, "Security analysis of authentication protocols for next-generation mobile and CE cloud services", in Proc. IEEE Int. Conf. Consumer Electron., 2011, Berlin, Germany, 2011, pp. 8387.

[3] H. Pang, J. Shen, and R. Krishnan, "Privacy-preserving similarity based text retrieval", ACM Trans. Internet Technology, vol. 10, no. 1, pp. 39, Feb. 2010.

[4] W. Sun et al., "Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 11, pp. 3025-3035, Nov. 2014.

[5] D. Kamini, M. Suresh and S. Neduncheliyan, "Encrypted multi-keyword ranked search supporting gram based search technique," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-6.

[6] S. Ahmad and P. S. Kumar, "An efficient privacy-preserving multi-keyword ranked search over encrypted data in cloud computing," 2016 IEEE Annual India Conference (INDICON), Bangalore, India, 2016, pp. 1-6.

[7] Z. Xia, X. Wang, X. Sun and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," in IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340-352, Feb. 1 2015.