**USING THE BLOOM FILTER, A DYNAMIC MULTI-KEYWORD RANKED SEARCH ACROSS ENCRYPTED CLOUD DATA**

**ABSTRACT:-**

Cloud computing has become a popular approach to manage personal data for the economic savings and management flexibility in recent year. However, the sensitive data must be encrypted before outsourcing to cloud servers for the consideration of privacy, which makes some traditional data utilization functions, such as the plaintext keyword search, impossible. To solve this problem, we present a multi-keyword ranked search scheme over encrypted cloud data supporting dynamic operations efficiently. Our scheme utilizes the vector space model combined with TF X IDF rule and cosine similarity measure to achieve a multi-keyword ranked search. However, traditional solutions have to suffer high computational costs. In order to achieve the sub-linear search time, our scheme introduces Bloom filter to build a search index tree. What is more, our scheme can support dynamic operation properly and effectively on the account of the property of the Bloom filter, which means that the updating cost of our scheme is lower than other schemes. We present our basic scheme first, which is secure under the known ciphertext model. Then, the enhanced scheme is presented later to guarantee security even under the known background model. The experiments on the real-world data set show that the performances of our proposed schemes are satisfactory.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * Searchable encryption can provide some useful techniques for cloud services on the basic of keyword search. Searchable encryption allows users to get access to relevant data by searching their encrypted data. * Their scheme utilizes two-layered encryption, which can guarantee the correctness of the trapdoor. Although this scheme is proven to be secure, it is based on a weak security model. | * In this paper we propose our multi-keyword search schemes which can support dynamic operations properly and the efficiency of dynamic operations in our schemes is satisfactory. * Our schemes can achieve the sub-linear search time. And, both the search efficiency and the index tree construction efficiency in our scheme are better than other related schemes. |
| **EXISTING ALGORITHM**  Searchable Encryption (SE) | **PROPOSED ALGORITHM:-**  Multi-Keyword Ranked Search Scheme (MKRSS) |
| **DRAWBACKS:-**   * Suffer high computational costs * Can only support exact single keyword search | **ADVANTAGES:-**   * Can achieve the sub-linear search time. * Can support dynamic operations. |

**MINIMUMSYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**

* PROCESSOR : DUAL CORE 2 DUO.
* RAM : 2GB DD RAM
* HARD DISK : 250 GB

**SOFTWARE REQUIREMENTS**

* FRONT END : J2EE (JSP, SERVLET)
* BACK END : MY SQL 5.5
* OPERATING SYSTEM : WINDOWS 7
* IDE : ECLIPSE