**CHAPTER-2**

**INTRODUCTION**

The data security issues have attracted increasingly higher attention from researchers in cloud environment. In order to protect the privacy of personal data, the data owners encrypt the documents before outsourcing them to the cloud. However, the encrypted data may make the traditional search mechanism based on plaintext keyword search obsolete. How to efficiently retrieve the encrypted data from the cloud has become a serious challenge. Cipher text retrieval has become one of the most important issues studied in the field of information security. In order to address the above issue, some researchers have proposed some fully-holomorphic encryption methods. However, these methods are not practical for users and cloud servers due to high computational costs. On the other hand, some more practical solutions have been designed. For example, many searchable encryption (SE) schemes have been proposed to enable search over the encrypted data, including single keyword search, similarity search, multi-keyword Boolean search, ranked search, multi-keyword ranked search, etc. Among them, the multi-keyword ranked search has attracted more and more attention for its practical applicability. Cao et al. proposed the MRSE scheme, and it can achieve the multi-keyword ranked search over the encrypted data. To obtain the most relevant documents, the documents are ranked according to the number of matched query keywords, but this scheme is not accurate enough. In order to improve the search accuracy, some multi-keyword search schemes [2], [3] have been proposed, and the vector space model and the “term frequency (TF) \* inverse document frequency (IDF)” model are combined to get the ranking search results. However, the ranking search results are only based on the number of keyword matches, or the “TF \* IDF” model cannot return more accurate top-k documents that satisfy the user interest. Moreover, the above solutions suffer from loss of accuracy because the dummy keywords are added to the query vector and document vector.

**LITERATURE SURVEY**

### Title: [Privacy-preserving multi-keyword ranked search over encrypted cloud data](https://ieeexplore.ieee.org/abstract/document/6674958/)

# Author: N.Cao

# Abstract: With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data have to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance.

### Title: [Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking](https://dl.acm.org/doi/abs/10.1145/2484313.2484322)

# Author: W Sun

# Abstract: With the increasing popularity of cloud computing, huge amount of documents are outsourced to the cloud for reduced management cost and ease of access. Although encryption helps protecting user data confidentiality, it leaves the well-functioning yet practically-efficient secure search functions over encrypted data a challenging problem. In this paper, we present a privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking to address this problem.

### Title: [A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data](https://ieeexplore.ieee.org/abstract/document/7039216/)

# Author:Z xia

# Abstract: Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations.

# Title: An Efficient Ranked Multi-Keyword Search for Multiple Data Owners Over Encrypted Cloud Data

# Author: Adi Shamir

# Abstract: With the development of cloud storage, more data owners are inclined to outsource their data to cloud services. For privacy concerns, sensitive data should be encrypted before outsourcing. There are various searchable encryption schemes to ensure data availability. However, the existing search schemes pay little attention to the efficiency of data users' queries, especially for the multi-owner scenario. In this paper, we proposed a tree-based ranked multi-keyword search scheme for multiple data owners. Specifically, by considering a large amount of data in the cloud, we utilize the TF × IDF model to develop a multikeyword search and return the top-k ranked search results

### Title: [Practical techniques for searches on encrypted data](https://ieeexplore.ieee.org/abstract/document/848445/)

**Author**: DX Song

# Abstract: It is desirable to store data on data storage servers such as mail servers and file server sin encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide