**ACCESS CONTROL FOR ENCRYPTED CLOUD DATA WITH PRACTICAL MULTI-KEYWORD RANKED SEARCH**

**ABSTRACT**:

With the explosive growth of data volume in the cloud computing environment, data owners are increasingly inclined to store their data on the cloud. Although data outsourcing reduces computation and storage costs for them, it inevitably brings new security and privacy concerns, as the data owners lose direct control of sensitive data. Meanwhile, most of the existing ranked keyword search schemes mainly focus on enriching search efficiency or functionality, but lack of providing efficient access control and formal security analysis simultaneously. To address these limitations, in this paper we propose an efficient and privacy-preserving Multi-keyword Ranked Search scheme with Fine-grained access control (MRSF). MRSF can realize highly accurate ciphertext retrieval by combining coordinate matching with Term Frequency-Inverse Document Frequency (TF-IDF) and improving the secure kNN method. Besides, it can effectively refine users’ search privileges by utilizing the polynomial-based access strategy. Formal security analysis shows that MRSF is secure in terms of confidentiality of outsourced data and the privacy of index and tokens. Extensive experiments further show that, compared with existing schemes, MRSF achieves higher search accuracy and more functionalities efficiently.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * Many previous works have been aware of the privacy preserving problem in searchable encryption area. * Prove that their secure kNN scheme based on Asymmetric Scalar-Product-preserving Encryption (ASPE) can resist the known-sample attack, where an attacker holds the plaintext of outsourced indexes but is unaware of the encrypted values. * To address this problem, an advanced APSE scheme is later proposed in [24]. It combines a random asymmetric splitting process and artificial random dimensions with the former APSE. | * To address the former issue, the first secure ranked search scheme is proposed in but it just supports single keyword search. * A later proposed multi-keyword ranked search scheme can quickly locate relevant results with minor additional computation overheads. * However, the keyword dictionary in [3] has to be rebuilt completely once new keywords are added. |
| **EXISTING ALGORITHM**  Cipher-Policy Attribute-Based Encryption (CP-ABE) and the Cipher Policy Attribute-Based Keyword Search (CP-ABKS) | **PROPOSED ALGORITHM:-**  **M**ulti-keyword **R**anked **S**earch scheme with **F**ine-grained access control (MRSF) |
| **ALGORITHM DEFINITION:-**  CP-ABE schemes incur heavy computational costs, which often grow with the complexityof the access structure. The computational and storage costs of existing CP-ABKS schemes are approximately proportional to the complexity of access policy as well [57]. As it is concluded in [58], approaches that adopt asymmetric encryption methods to protect data from unauthorized access usually have huge key numbers, which incurs a high key management burden. Thus, inventing a light-weight access  control mechanism over keyword search schemes is still in  demand. | **ALGORITHM DEFINITION:-**  In MRSF, the data owner needs to generate the secret key and assignments of the access role before transmitting them to the data user through a secure channel. In the next step,  the data owner generates a subindex for each document in the document set and encrypts every subindex by adding a random vector and permutating. All subindexes will be split according to certain rules before being submitted to the cloud server. If a data user wants to query over the outsourced documents, he/she needs to generate his search token. First, the keywords in the search query will be  marked out in a binary vector, then the vector is extended by the dummy keywords and the access role. After this, the vector will be encrypted and split similarly to the subindex.  After receiving the search token from the data user, the cloud server will calculate the relevance score between each subindex and the token. Although every document has a relevance score, only a part of them can pass the filter, which aims to prevent unauthorized accesses from the data user. After the filtering process, the cloud server will rank the highest k legal relevance scores and save their corresponding document names in a list. At last, the cloud returns the top-k encrypted documents. The following sections describe our scheme in detail. |
| **DRAWBACKS:-**   * Less accuracy * It will have a less security issues. * Low Privacy-Preserving. | **ADVANTAGES:-**   * Higher search accuracy * Lightweight Fine-grained access control. * Higher privacy-preserving level and formal security proof |

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS**:

System : Pentium i3 Processor

Hard Disk : 500 GB.

Monitor : 15’’ LED

Input Devices : Keyboard, Mouse

RAM : 2 GB

**SOFTWARE REQUIREMENTS:**

Operating system : Windows 10.

Coding Language : Java.

Tool : Netbeans 8.2

Database : MYSQL

**REFERENCE**:

Jiayi Li, Jianfeng Ma, Yinbin Miao, Ruikang Yang, Ximeng Liu, and Kim-Kwang Raymond Choo, Senior Member, IEEE, “Practical Multi-keyword Ranked Search with Access Control over Encrypted Cloud Data”, IEEE TRANSACTIONS ON CLOUD COMPUTING, 2021.