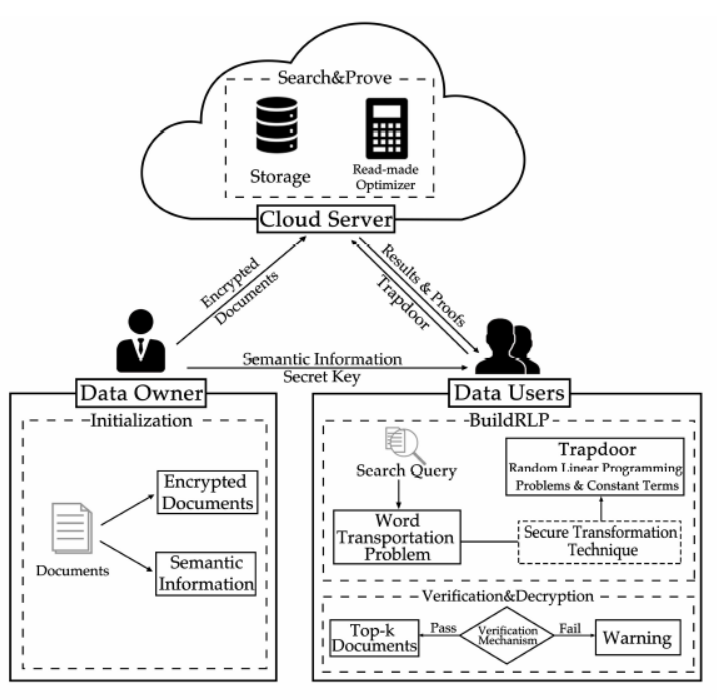
**A Data Sharing Using Searching Scheme by Matching Encrypted Data in Database**

**ABSTRACT**:

Semantic searching over encrypted data is a crucial task for secure information retrieval in public cloud. It aims to provide retrieval service to arbitrary words so that queries and search results are flexible. In existing semantic searching schemes, the verifiable searching does not be supported since it is dependent on the forecasted results from predefined keywords to verify the search results from cloud, and the queries are expanded on plaintext and the exact matching is performed by the extended semantically words with predefined keywords, which limits their accuracy. In this paper, we propose a secure verifiable semantic searching scheme. For semantic optimal matching on ciphertext, we formulate word transportation (WT) problem to calculate the minimum word transportation cost (MWTC) as the similarity between queries and documents, and propose a secure transformation to transform WT problems into random linear programming (LP) problems to obtain the encrypted MWTC. For verifiability, we explore the duality theorem of LP to design a verification mechanism using the intermediate data produced in matching process to verify the correctness of search results. Security analysis demonstrates that our scheme can guarantee verifiability and confidentiality. Experimental results on two datasets show our scheme has higher accuracy than other schemes.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * A verifiable semantic searching scheme that extends the query words to get the predefined keywords related to query words, then they used the extended keywords to search on a symbol-based trie index. * Their approach damages the semantic information due to straightly aggregating all the word vectors. We think that secure semantic searching schemes should further utilize a wealth of semantic information among words and perform optimal matching on the ciphertext for high search accuracy. | * In this paper, we propose a secure veriﬁable semantic. * Searching scheme that treats matching between queries and documents as an optimal matching task. We treat the document words as the query words as and the semantic information as and design the minimum word transportation cost (MWTC) as the similarity metric between queries and documents. |
| **EXISTING ALGORITHM**  kNN algorithm | **PROPOSED ALGORITHM:-**  semantic optimal matching onciphertext, we formulate word transportation (WT) |
| **EXISTINGALGORITHM**  introduced homomorphic encryption to encrypt relevance scores and realize a multikeyword  ranked search scheme under the vector space model.encryption techniques to propose a generic solution for supporting multi-keyword ranked searching schemes that can resist against several attacks brought by OPE-based schemes.  Secure Semantic Searching | **PROPOSED ALGORITHM:**  In this phase, data users perform VerDec () to verify the correctness of the search results and decrypt the top-k encrypted documents. To describe this algorithm in detail, we split it into Verify () and DecDoc (), as follows Verify is a deterministic verificationalgorithm, |
| **DRAWBACKS: -**   * It is worth spending more time to get higher search accuracy * The applications in practical scenarios | **ADVANTAGES: -**   * Therefore, it is challenging to design a secure semantic searching scheme to support verifiable searching. * The existing scheme is unable to support semantic searching and introduces multiple rounds of communication between data owners. |

**SYSTEM ARCHITECTURE**

**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