**A Fast and Accurate Privacy-Preserving Multi-keyword Top-k Retrieval Scheme Encrypted Cloud Data**

**ABSTRACT**

As cloud computing technology develops, more and more documents are encrypted before being transferred to the cloud for convenience and cost-saving reasons. Therefore, it is crucial to figure out how to create a multi-keyword ranked search scheme that is quick and accurate over encrypted cloud data. In this study, we offer a fast and accurate top-k multi-keyword retrieval-supporting searchable encryption (FASE) technique. The index and query vectors are encrypted using a holomorphic order-preserving technique. The encryption technique performs the secure calculation of relevance score between encrypted index and query vectors and supports homomorphic addition, homomorphic multiplication, and order comparison over encrypted data. The encryption method can guarantee that the relevance score computation (SIi T) is not exposed to the cloud server and can also secure the ranking operator's privacy. In contrast to the conventional approach, the query vector and document vector are not given dummy keywords, and the top-k search precision of the FASE scheme is 100%. By effectively matching the document mark vector and query mark vector, a large number of irrelevant documents are efficiently filtered out to increase search efficiency, and the time required to determine the relevance score and ranking is significantly decreased. Furthermore, not only are more accurate search results returned, but the search efficiency is also increased according to the two-round ranking of the keyword matching degree and the relevance score. Theoretical study and experimental findings support the FASE scheme's ability to perform quick and precise multi-keyword ranking searches. It may successfully increase search performance, decrease the time required to create an index, and offer ranking results that more closely meet user needs in addition to maintaining data privacy and security.