

**CHENNAI – PONDICHERRY**

**EFFICIENT RETRIEVAL OVER DOCUMENTS ENCRYPTED BY ATTRIBUTES IN CLOUD COMPUTING**

**ABSTRACT:**

Secure document storage and retrieval is one of the hottest research directions in cloud computing. Though many searchable encryption schemes have been proposed, few of them support efficient retrieval over the documents which are encrypted based on their attributes. In this paper, a hierarchical attribute-based encryption scheme is first designed for a document collection. A set of documents can be encrypted together if they share an integrated access structure. Compared with the ciphertext-policy attribute-based encryption schemes, both the ciphertext storage space and time costs of encryption/decryption are saved. Then, an index structure named attribute-based retrieval features (ARF) tree is constructed for the document collection based on the TF-IDF model and the documents' attributes. A depth-first search algorithm for the ARF tree is designed to improve the search efficiency which can be further improved by parallel computing. Except for the document collections, our scheme can be also applied to other datasets by modifying the ARF tree slightly. A thorough analysis and a series of experiments are performed to illustrate the security and efficiency of the proposed scheme.