**SYSTEM ANALYSIS:**

**EXISTING SYSTEM:**

First, most existing schemes focus on encrypting a single access tree. However, it is impossible that all the documents in share a single access tree and how to construct a set of optimized access trees for the document collection is a huge challenge. Second ,in most existing schemes, when the documents are mapped to a set of shared access trees, the data users need to store a large number of secret keys which will be analyzed in Hierarchical Document Encryption. Apparently, this is a heavy burden for the data users especially for an extremely large document collection and how to decrease the amount of secret keys for the data users is another challenge. Except for access control, document search efficiency is also a challenge for a large document collection. To our knowledge, most existing schemes cannot support time efficient retrieval over the documents which are organized under attribute-based access control mechanism. access trees incrementally and each access tree grows by continuously splitting the nodes in the tree. Then we design a ciphertext-policy attribute-based hierarchical document collection encryption scheme called CP-ABHE.

**DISADVANTAGES OF EXISTING SYSTEM:**

* However, all these schemes cannot support effective, flexible and efficient document search because of their simple functionalities.
* The sensitive information, such as personal information, company financial data and government documents, to the public is a big threat to the data owners. In addition, to make full use of the data on the cloud, the data users need to access them flexibly and efficiently is not possible.

**PROPOSED SYSTEM:**

To support the previously discussed service, we first design an algorithm to generate hierarchical access trees for the document collection. The proposed algorithm employs the greedy strategy to build the access trees incrementally and each access tree grows by continuously splitting the nodes In the tree. Then we design a ciphertext-policy attribute-based hierarchical document collection encryption scheme called CP-ABHE. In the proposed scheme, a set of documents can share a same integrated access tree and be encrypted together rather than being encrypted individually. In this way, both the ciphertext storage space and time costs of the encryption/decryption are saved. To support accurate and efficient document search over the encrypted documents, a complicated index structure is then constructed for the document collection. We first map the documents to document vectors based on the TF-IDF model and, in addition, the attributes of the documents are also taken into consideration. The similarity function between the document vectors is carefully designed and the vectors are organized based on their relative similarities in the attribute-based retrieval features (ARF) tree. Specifically, the similar vectors compose micro clusters which are then aggregated with each other to generate macro clusters until all the vectors belong to one cluster.

**ADVANTAGES OF PROPOSED SYSTEM:**

* An advantage of the scheme is that the data users can decrypt all the authorized documents by computing the secret key once.
* To make the data users able to access part of on demands, a possible approach is encrypting the documents through attribute-based encryption(ABE) schemes ,before outsourcing them to the cloud.
* In these scheme can upload the multiples file by encrypting and we can download the multiple files at a time