**A PRACTICAL ATTRIBUTE-BASED DOCUMENT COLLECTION HIERARCHICAL ENCRYPTION SCHEME IN CLOUD COMPUTING**

**ABSTRACT:**

Ciphertext-policy attribute-based encryption can provide fine-grained access control and secure data sharing to the data users in cloud computing. However, the encryption/decryption efficiency of existing schemes can be further improved when encrypting a large document collection. In this paper, we propose a practical Ciphertext-Policy Attribute-Based Hierarchical document collection Encryption scheme named CP-ABHE. By practical, we mean that CP-ABHE is more efficient in both computation and storage space without sacrificing data security. In CP-ABHE, we first construct a set of integrated access trees based on the documents’ attribute sets. We employ the greedy strategy to build the trees incrementally and grow the trees by dynamically combining the small ones. Then all the documents on an integrated access tree are encrypted together. Different to existing schemes, the leaves in different access trees with the same attribute share a same secret number which is employed to encrypt the documents. This greatly improves the performance of CP-ABHE. The security of our scheme is theoretically proved based on the Decisional Bilinear Diffie-Hellman assumption. Simulation results illustrate that CP-ABHE performs very well in terms of security, efficiency and the storage size of the ciphertext..

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1 GB

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/UBUNTU.
* Implementation : NS2
* NS2 Version : 2.28
* Front End : OTCL (Object Oriented Tool Command  Language)
* Tool : Cygwin (To simulate in Windows OS)