**Hidden Ciphertext Policy Attribute-Based Encryption with Fast Decryption for Personal Health Record System**

**ABSTRACT:**

Since cloud computing has been playing an increasingly important role in real life, the privacy protection in many ﬁelds has been paid more and more attention, especially, in the ﬁeld of Personal Health Record (PHR). The traditional ciphertext-policy attribute based encryption(CP-ABE) provides the ﬁne-grained access control policy for encrypted PHR data, but the access policy is also sent along with ciphertext explicitly. However, the access policy will reveal the users’ privacy because it contains too much sensitive information of the legitimate data users. Hence it is important to protect users’ privacy by hiding accesspolicies.Inmostofthepreviousschemes,althoughtheaccesspolicyishidden,theyfacetwopractical problems: (1) these schemes do not support large attribute universe, so their practicality in PHR is greatly limited, and (2) the cost of decryption is especially high since the access policy is embedded in ciphertext. To address these problems, we construct a CP-ABE scheme with efﬁcient decryption, where both the size of public parameters and the cost of decryption are constant. Moreover, we also show the proposed scheme achieves full security in the standard model under static assumptions by using the dual system encryption method.

**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)