**Enabling Authorized Encrypted Search for Multi-Authority Medical Databases**

**Abstract:**

E-medical records are sensitive and should be stored in a medical database in encrypted form. However, simply encrypting these records will eliminate data utility and interoperability of the existing medical database system because encrypted records are no longer searchable. Moreover, multiple authorities could be involved in controlling and sharing the private medical records of clients. However, authorizing different clients to search and access records originating from multiple authorities in a secure and scalable manner is a nontrivial matter. To address the above issues, we propose an authorized searchable encryption scheme under a multi-authority setting. Speciﬁcally, our proposed scheme leverages the RSA function to enable each authority to limit the search capability of different clients based on clients’ privileges. To improve scalability, we utilize multi-authority attribute-based encryption to allow the authorization process to be performed only once even over policies from multiple authorities. We conduct rigorous security and cost analysis, and perform experimental evaluations to demonstrate that the proposed scheme introduces moderate overhead to existing searchable encryption scheme.

**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)