**Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting**

**ABSTRACT:**

Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) facilitates search queries and supports ﬁne-grained access control over encrypted data in the cloud. However, prior CP-ABKS schemes were designed to support unshared multi-owner setting, and cannot be directly applied in the shared multi-owner setting (where each record is accredited by a ﬁxed number of data owners), without incurring high computational and storage costs. In addition, due to privacy concerns on access policies, most existing schemes are vulnerable to off-line keyword-guessing attacks if the keyword space is of polynomial size. Furthermore, it is difﬁcult to identify malicious users who leak the secret keys when more than one data user has the same subset of attributes. In this paper, we present a privacy-preserving CP-ABKS system with hidden access policy in Shared Multi-owner setting (basic ABKS-SM system), and demonstrate how it is improved to support malicious user tracing (modiﬁed ABKS-SM system). We then prove that the proposed ABKS-SM systems achieve selective security and resist off-line keyword-guessing attack in the generic bilinear group model. We also evaluate their performance using real-world datasets.

**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)