**Verifiable and Multi-keyword Searchable Attribute-based Encryption Scheme for Cloud Storage**

**ABSTRACT:**

In an attribute-based searchable encryption (ABSE) scheme, data owners can encrypt their data with access policy for security consideration, and encrypt keywords to obtain keyword index for privacy keyword search, and data users can search interesting keyword on keyword indexes by keyword search trapdoor. However many existing searchable encryption schemes only support single keyword search and most of existing attribute-based encryption (ABE) schemes have high computational costs at user client. These problems significantly limit the application of attribute-based searchable encryption schemes in practice. In this paper, we propose a verifiable and multi-keyword searchable attribute-based encryption (VMKS-ABE) scheme for cloud storage, in our new scheme multi-keyword can be searched and the search privacy is protected. That is, the cloud sever can search the multi-keyword with keyword search trapdoor but it does not know any information of the keywords searched. In the proposed scheme, many computing tasks are outsourced to the cloud proxy server, which greatly reduces the computing burden at user client. Besides, the scheme also supports the verification of the correctness of outsourced private key. The proposed scheme is proved secure that the keyword index is indistinguishable under the adaptive keyword attacks in the general group model, and the ciphertext is selective secure under selective plaintext attacks in the random oracle model. The security and experimental results show that our scheme is suitable for practicability.

**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)