**Enabling Veriﬁable and Dynamic Ranked Search Over Outsourced Data**

**Abstract:**

Cloud computing as a promising computing paradigm is increasingly utilized as potential hosts for users’ massive dataset. Since the cloud service provider (CSP) is outside the users’ trusted domain, existing research suggests encrypting sensitive data before outsourcing and adopting Searchable Symmetric Encryption (SSE) to facilitate keyword-based searches over the ciphertexts. However, it remains a challenging task to design an effective SSE scheme that simultaneously supports sublinear search time, efﬁcient update and veriﬁcation, and on-demand information retrieval. To address this, we propose a Veriﬁable Dynamic Encryption with Ranked Search (VDERS) scheme that allows a user to perform top-K searches on a dynamic document collection and verify the correctness of the search results in a secure and efﬁcient way. Speciﬁcally, we ﬁrst provide a basic construction, VDERS0, where a ranked inverted index and a veriﬁable matrix are constructed to enable veriﬁable document insertion in top-K searches. Then, an advanced construction, VDERS⋆, is devised to further support document deletion with a reduced communication cost. Extensive experiments on real datasets demonstrate the efﬁciency and effectiveness of our VDERS 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)