**Fast Boolean Queries With Minimized Leakage for Encrypted Databases in Cloud Computing**

**Abstract:**

This research revisits the fundamental problem of processing privacy-preserving Boolean queries over outsourced databases on untrusted public clouds. Much current searchable encryption (SE) schemes try to seek an appropriate trade-off between security and efﬁciency, yet most of them suffer from an unacceptable query leakage due to their conjunctive/disjunctive terms that are processed individually. We show, however, this trade-off still can be deeply optimized for more security. We consider a Boolean formula as a set of deterministic ﬁnite automatons (DFAs) and propose a novel approach to running an encryptedDFA,whichcanbeeffectivelyandefﬁcientlyprocessedbythecloud.Wegivethreeconstructions for conjunctive, disjunctive, and Boolean queries, respectively. Their notable advantages are single-round, highly-efﬁcient,adaptively-secure,andleakage-minimized.Alotofexperimentsaremadetoevaluateoverall efﬁciency. Testing results show that the schemes achieve enhanced security almost without sacriﬁcing anything of search efﬁciency.

**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)