**Memory Leakage-Resilient Dynamic and Verifiable Multi-keyword Ranked Search on Encrypted Smart Body Sensor Network Data**

**Abstract:**

 Outsourcing of encrypted smart body sensor network data to the edge or the cloud is now an entrenched practice within organizations, for example to reduce cost and enhance productivity (to some extent), while ensuring data is not accessible to misbehaving cloud service providers. Although there are a large number of searchable symmetric encryption schemes designed to support searching operations on encrypted data, a fully functional and memory leakage-resilient scheme for smart body sensor network data is lacking. This security property is highly desirable as the resource-sharing environment may be prone to various kinds of memory leakage. In this paper, a memory leakage-resilient dynamic and verifiable multikeyword ranked search scheme (MLR-DVMRS) on encrypted smart body sensor network data is proposed. As each sensor device has inherent characteristics to identify itself, this property can be used to authenticate the device. The proposed scheme utilizes physically unclonable functions (PUFs) and fuzzy extractors to achieve memory leakage-resilience. Meanwhile the vector space model, TF-IDF measure method, and order-preserving encryption (OPE), are used to achieve dynamic and multikeyword ranked search functionalities. A formal security analysis is given to prove the security of MLR-DVMRS. Besides the comprehensive functionalities of MLR-DVMRS, experimental results demonstrate that the efficiency of MLR-DVMRS is superior to MRSE (a multi-keyword ranked search over encrypted cloud data scheme) for large data collection.

**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)