**Secure Phrase Search for Intelligent Processing of Encrypted Data in Cloud-Based IoT**

**Abstract:**

Phrase search allows retrieval of documents containing an exact phrase, which plays an important role in many machine learning applications for cloud-based IoT, such as intelligent medical data analytics. In order to protect sensitive information from being leaked by service providers, documents (e.g., clinic records) are usually encrypted by data owners before being outsourced to the cloud. This, however, makes the search operation an extremely challenging task. Existing searchable encryption schemes for multi-keyword search operations fail to perform phrase search, as they are unable to determine the location relationship of multiple keywords in a queried phrase over encrypted data on the cloud server side. In this paper, we propose P3, an efﬁcient privacy-preserving phrase search scheme for intelligent encrypted data processing in cloud-based IoT. Our scheme exploits the homomorphic encryption and bilinear map to determine the location relationship of multiple queried keywords over encrypted data. It also utilizes a probabilistic trapdoor generation algorithm to protect users’ search patterns. Thorough security analysis demonstrates the security guarantees achieved by P3. We implement a prototype and conduct extensive experiments on real-world datasets. The evaluation results show that compared with existing multikeyword search schemes, P3 can greatly improve the search accuracy with moderate overheads..

**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)