

# Multi-authority Attribute-Based Keyword Search over Encrypted Cloud Data

## ABSTRACT:

Searchable Encryption (SE) is an important technique to guarantee data security and usability in the cloud at the same time. Leveraging Cipher text-Policy Attribute-Based Encryption (CP-ABE), the Cipher text-Policy Attribute-Based Keyword Search (CP-ABKS) scheme can achieve keyword-based retrieval and fine-grained access control simultaneously. However, the single attribute authority in existing CP-ABKS schemes is tasked with costly user certificate verification and secret key distribution. In addition, this results in a single-point performance bottleneck in distributed cloud systems. Thus, in this paper, we present a secure Multi-authority CP-ABKS (MABKS) system to address such limitations and minimize the computation and storage burden on resource-limited devices in cloud systems. In addition, the MABKS system is extended to support malicious attribute authority tracing and attribute update. Our rigorous security analysis shows that the MABKS system is selectively secure in both selective-matrix and selective-attribute models. Our experimental results using real-world datasets demonstrate the efficiency and utility of the MABKS system in practical applications.

## **SYSTEM REQUIREMENTS:**

### **HARDWARE REQUIREMENTS:**

- System : Pentium i3 Processor.
- Hard Disk : 500 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 4 GB

### **SOFTWARE REQUIREMENTS:**

- Operating system : Windows 10.
- Coding Language : Java
- Web Framework : Flask

### **REFERENCE:**

Y. Miao, R. H. Deng, X. Liu, K. -K. R. Choo, H. Wu and H. Li, "Multi-Authority Attribute-Based Keyword Search over Encrypted Cloud Data," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 4, pp. 1667-1680, 1 July-Aug. 2021, doi: 10.1109/TDSC.2019.2935044.