Practical Multi-keyword Ranked Search with Access Control over Encrypted Cloud Data

ABSTRACT:

With the explosive growth of data volume in the cloud computing environment, data owners are increasingly inclined to store their data on the cloud. Although data outsourcing reduces computation and storage costs for them, it inevitably brings new security and privacy concerns, as the data owners lose direct control of sensitive data. Meanwhile, most of the existing ranked keyword search schemes mainly focus on enriching search efficiency or functionality, but lack of providing efficient access control and formal security analysis simultaneously. To address these limitations, in this paper we propose an efficient and privacy-preserving Multi-keyword Ranked Search scheme with Fine-grained access control (MRSF). MRSF can realize highly accurate ciphertext retrieval by combining coordinate matching with Term Frequency-Inverse Document Frequency (TF-IDF) and improving the secure kNN method. Besides, it can effectively refine users' search privileges by utilizing the polynomial-based access strategy. Formal security analysis shows that MRSF is secure in terms of confidentiality of outsourced data and the privacy of index and tokens. Extensive experiments further show that, compared with existing schemes, MRSF achieves higher search accuracy and more functionalities efficiently.

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:

J. Li, J. Ma, Y. Miao, Y. Ruikang, X. Liu and K. -K. R. Choo, "Practical Multi-keyword Ranked Search with Access Control over Encrypted Cloud Data," in *IEEE Transactions on Cloud Computing*, doi: 10.1109/TCC.2020.3024226.