A Verifiable Semantic Searching Scheme byOptimal Matching over Encrypted Datain Public Cloud

ABSTRACT:

Semantic searching over encrypted data is a crucialtask for secure information retrieval in public cloud. It aimsto provide retrieval service to arbitrary words so that queriesand search results are flexible. In existing semantic searchingschemes, the verifiable searching does not be supported since itis dependent on the forecasted results from predefined keywordsto verify the search results from cloud, and the queries areexpanded on plaintext and the exact matching is performed by theextended semantically words with predefined keywords, whichlimits their accuracy. In this paper, we propose a secure verifiablesemantic searching scheme. For semantic optimal matching onciphertext, we formulate word transportation (WT) problem tocalculate the minimum word transportation cost (MWTC) asthe similarity between queries and documents, and propose asecure transformation to transform WT problems into randomlinear programming (LP) problems to obtain the encryptedMWTC. For verifiability, we explore the duality theorem of LPto design a verification mechanism using the intermediate dataproduced in matching process to verify the correctness of searchresults. Security analysis demonstrates that our scheme canguarantee verifiability and confidentiality. Experimental resultson two datasets show our scheme has higher accuracy than otherschemes.

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:

W. Yang and Y. Zhu, "A Verifiable Semantic Searching Scheme by Optimal Matching Over Encrypted Data in Public Cloud," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 100-115, 2021, doi: 10.1109/TIFS.2020.3001728.