Towards Achieving Keyword Search overDynamic Encrypted Cloud Data with Symmetric-Key based Verification

ABSTRACT:

Verifiable Searchable Symmetric Encryption, as an important cloud security technique, allows users to retrieve theencrypted data from the cloud through keywords and verify the validity of the returned results. Dynamic update for cloud data isone of the most common and fundamental requirements for data owners in such schemes. To the best of our knowledge, theexisting verifiable SSE schemes supporting data dynamic update are all based on asymmetric-key cryptography verification, whichinvolves time-consuming operations. The overhead of verification may become a significant burden due to the sheer amount ofcloud data. Therefore, how to achieve keyword search over dynamic encrypted cloud data with efficient verification is a criticalunsolved problem. To address this problem, we explore achieving keyword search over dynamic encrypted cloud data withsymmetric-key based verification and propose a practical scheme in this paper. In order to support the efficient verification ofdynamic data, we design a novel Accumulative Authentication Tag (AAT) based on the symmetric-key cryptography to generatean authentication tag for each keyword. Benefiting from the accumulation property of our designed AAT, the authentication tagcan be conveniently updated when dynamic operations on cloud data occur. In order to achieve efficient data update, we design anew secure index composed by a search table ST based on the orthogonal list and a verification list VL containing AATs. Owing tothe connectivity and the flexibility of ST, the update efficiency can be significantly improved. The security analysis and theperformance evaluation results show that the proposed scheme is secure and efficient.

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:

X. Ge et al., "Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key Based Verification," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 1, pp. 490-504, 1 Jan.-Feb. 2021, doi: 10.1109/TDSC.2019.2896258.