Crypt Cloud: Secure and Expressive Data Access Control for Cloud Storage

ABSTRACT:

Secure cloud storage, which is an emerging cloud service, is designed to protect the confidentiality of outsourced data butalso to provide flexible data access for cloud users whose data is out of physical control. Ciphertext-Policy Attribute-Based Encryption(CP-ABE) is regarded as one of the most promising techniques that may be leveraged to secure the guarantee of the service. However,the use of CP-ABE may yield an inevitable security breach which is known as the misuse of access credential (i.e. decryption rights),due to the intrinsic "all-or-nothing" decryption feature of CP-ABE. In this paper, we investigate the two main cases of access credentialmisuse: one is on the semi-trusted authority side, and the other is on the side of cloud user. To mitigate the misuse, we propose thefirst accountable authority and revocable CP-ABE based cloud storage system with white-box traceability and auditing, referred to asCryptCloud+. We also present the security analysis and further demonstrate the utility of our system via experiments.

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. Ning, Z. Cao, X. Dong, K. Liang, L. Wei and K. -K. R. Choo, "CryptCloud$^+$+: Secure and Expressive Data Access Control for Cloud Storage," in IEEE Transactions on Services Computing, vol. 14, no. 1, pp. 111-124, 1 Jan.-Feb. 2021, doi: 10.1109/TSC.2018.2791538.