Efficient Revocable Multi-Authority Attribute-Based Encryption for Cloud Storage

ABSTRACT:

As is known, attribute-based encryption (ABE) is usually adopted for cloud storage, bothfor its achievement of fine-grained access control over data, and for its guarantee of data confidentiality.Nevertheless, single-authority attribute-based encryption (SA-ABE) has its obvious drawback in that onlyone attribute authority can assign the users' attributes, enabling the data to be shared only within themanagement domain of the attribute authority, while rendering multiple attribute authorities unable toshare the data. On the other hand, multi-authority attribute-based encryption (MA-ABE) has its advantagesover SA-ABE. It can not only satisfy the need for the fine-grained access control and confidentialityof data, but also make the data shared among different multiple attribute authorities. However, existingMA-ABE schemes are unsuitable for the devices with resources-constraint, because these schemes areall based on expensive bilinear pairing. Moreover, the major challenge of MA-ABE scheme is attributerevocation. So far, many solutions in this respect are not efficient enough. In this paper, on the basis of theelliptic curves cryptography, we propose an efficient revocable multi-authority attribute-based encryption(RMA-ABE) scheme for cloud storage. The security analysis indicates that the proposed scheme satisfiesindistinguishable under adaptive chosen plaintext attack assuming hardness of the decisional Diffie-Hellman problem. Compared with the other schemes, the proposed scheme gets its advantages in that it is moreeconomical in computation and storage.

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. Ling, H. Gu, H. Wang and L. Zhang, "An Efficient Ciphertext Index Retrieval Scheme Based on Edge Computing Framework," in IEEE Access, vol. 9, pp. 37975-37988, 2021, doi: 10.1109/ACCESS.2021.3061676.