ABDKS: attribute-based encryption with dynamic keyword search in fog computing

Fei MENG, Leixiao CHENG, Mingqiang WANG

Frontiers of Computer Science, DOI: 10.1007/s11704-020-9472-7

Problems & Ideas

The ciphertext search phase can also be divided into two parts. First, the user's access permissions are detected, and then the matching degree between the target keywords and the ciphertext keywords is checked, instead of performing a permission check for each target keyword. , This also greatly reduces the computing pressure of the cloud server.

Problems & Ideas

- Problems in previous ABKS schemes
  - The search algorithm requires that each keyword to be identical between the target keyword set and the ciphertext keyword set, otherwise the algorithm doesn't output any search result, which is not conducive to use.
  - These schemes are vulnerable to what we call a peer-decryption attack, that is, the ciphertext may be eavesdropped and decrypted by an adversary who has sufficient authorities but no information about the ciphertext keywords.
- Ideas: The search algorithm should be divided into two parts.
  - User’s access authority is verified at first.
  - Then, check the correlation between the target keywords and the ciphertext keywords is checked.

Main Contributions

- **In ABDKS, the search algorithm requires only one keyword to be identical between the two keyword sets and outputs the corresponding correlation which reflects the number of the same keywords in those two sets.**
- **The ABDKS is resistant to peer-decryption attack, since the decryption requires not only sufficient authority but also at least one keyword of the ciphertext.**
- **The ABDKS shifts most computational overheads from resource constrained users to fog nodes.**

Table 2 Functional comparison among various ABKS schemes.

Schemes	Fine-grained access control	Keyword search	Attribute update	Dynamic keyword search	Peer-decryption resis-tance
[23]	√		√		
[9]	√	√			
[10]	√	√	√		
ABDKS	√	√	√	√	√