**An Efficient and Fine-grained Big Data Access Control Scheme with Privacy-preserving Policy**

How to control the access of the huge amount of big data becomes a very challenging issue, especially when big data are stored in the cloud. Ciphertext-Policy Attributebased Encryption (CP-ABE) is a promising encryption technique that enables end-users to encrypt their data under the access policies defined over some attributes of data consumers and only allows data consumers whose attributes satisfy the access policies to decrypt the data. In CP-ABE, the access policy is attached to the ciphertext in plaintext form, which may also leak some private information about end-users. Existing methods only partially hide the attribute values in the access policies, while the attribute names are still unprotected. In this paper, we propose an efficient and fine-grained big data access control scheme with privacy-preserving policy. Specifically, we hide the whole attribute (rather than only its values) in the access policies. To assist data decryption, we also design a novel Attribute Bloom Filter to evaluate whether an attribute is in the access policy and locate the exact position in the access policy if it is in the access policy. Security analysis and performance evaluation show that our scheme can preserve the privacy from any LSSS access policy

without employing much overhead.

**Index Terms—Big Data; Access Control; Privacy-preserving Policy; Attribute Bloom Filter; LSSS Access Structure**