混合云下面向隐私保护的访问控制方法

屠袁飞 1,2,3，夏　峰 1,杨　庚 2,3

（1 南京工业大学 计算机科学与技术学院, 江苏 南京 211816; 2 南京邮电大学 计算机学院,
江苏 南京 210003; 3 江苏省无线传感网高技术研究重点实验室，江苏 南京 210003）

摘　要： 基于属性的加密(Attribute-based encryption, ABE)已被广泛研究，其支持细粒度的访问控制可用来共享数据，然而存储容量大以及计算开销大使其难以得到广泛运用.将现有的支持属性匿名的 ABE 算法的密文数据进行分割并分别存储在不同的云环境中，用于匹配且计算量与存储量小的部分存储在私有云中，利用先匹配后解密的思路提高系统的整体运行效率.从正确性、安全性以及复杂性等方面做出证明，通过与以往的部分 ABE 算法进行对比以及给出的具体实验说明方案的可行性.

关键词： 云计算；基于属性的访问控制；混合云；隐私保护

Privacy-preserving Ciphertext-Policy Attribute-Based Encryption in Hybrid Cloud

TU Yuan-fei1,2,3, XIA Feng1, YANG Geng2,3

(1 School of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, China;
2 College of Computer Science & Technology, Nanjing University of Post &
Telecommunication, Nanjing 210003, China; 3 Jiangsu High Technology Research Key
Laboratory for Wireless Sensor Networks, Nanjing 210003, China)

Abstract： Attribute-based encryption(ABE) has been widely studied recently to support fine-grained access control of shared data, but the file size and cost of computing make it hard to be widely used.This paper aims to solve the problem using hybrid cloud. This paper modify the existing privacy-preserving method to store some message with small size and low computing cost in the private cloud for matching, users could decrypt the file in the public cloud only after the matching phase under the “match-then-decrypt” method. The proposed construction is proven to be secure and the experiment result shows the solution is efficient and practical.

Key words： cloud computing; attribute-based access control; hybrid cloud; privacy-preserving

作者简介：
屠袁飞　男，(1984-)，博士研究生，助理工程师.研究方向为数据隐私保护与访问控制.
E-mail：935127868@qq.com.
杨　庚　男，(1961-)，博士，教授，博士生导师.研究方向为网络安全、分布与并行计算、大规模科学工程计算.