计算机应用 2013, 33(10) 2832-2834 DOI:
ISSN: 1001-9081 CN: 51-1307/TP

信息安全

云环境下的基于属性和重加密的密钥管理

罗文俊,徐敏

重庆邮电大学 计算机科学与技术学院，重庆 400065

摘要： 在云计算环境中如何安全地存储数据是云计算面临的挑战之一。加密是解决云计算中数据存储安全问题最主要的方法，而加密的一个保密性问题是密钥管理。提出了云环境下的基于属性和重加密的密钥管理方案。云服务提供商对不同用户进行重加密时，可以一次为一组用户重加密，从而减少了重加密的个数。数据拥有者可以对组用户生成和发送重加密密钥，而数据请求者可以使用属性集对应的一个密钥解密多个数据拥有者的数据，从而能减少两者的密钥发送量，降低密钥管理的难度，提高方案的效率。最后，对方案的安全性和性能进行了分析

关键词： 云计算 云安全 基于属性的加密 重加密 密钥管理

Attribute-based encryption and re-encryption key management in cloud computing

LUO Wenjun,XU Min

School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: The security problem of the data stored in the cloud is a challenge for cloud computing. Encryption is the main method to solve the problem of data storage security in cloud computing. The confidentiality issue of the encryption is the key management. The attribute-based encryption and re-encryption scheme in cloud computing was

扩展功能
本文信息
Supporting info
PDF(661KB)
[HTML全文]
参考文献[PDF]
参考文献
服务与反馈
把本文推荐给朋友
加入我的书架
加入引用管理器
引用本文
Email Alert
文章反馈
浏览反馈信息
本文关键词相关文章
云计算
云安全
基于属性的加密
重加密
密钥管理
本文作者相关文章
罗文俊
徐敏

proposed. It combined attribute-based encryption and re-encryption technology. The cloud server could re-encrypt for different users, and re-encrypt for a group of users at a time. Thereby the scheme reduced the number of re-encryption keys. The data owner could generate and send the keys of re-encryption for a group of users and the data requester could use the key corresponding to the attribute set to decrypt the data of several data owners, which reduced the amount of keys' transmission. The scheme reduced the difficulty of key management and improved the efficiency of the scheme. In the end, the security and efficiency of the scheme were discussed.

Keywords: cloud computing cloud security attribute-based encryption re-encryption key management

收稿日期 2013-04-15 修回日期 2013-06-08 网络版发布日期 2013-11-01

DOI:

基金项目:

重庆市自然科学基金资助项目

通讯作者: 徐敏

作者简介: 罗文俊（1966-）男，贵州绥阳人，教授，主要研究方向：信息安全、应用密码学；徐敏（1985-）女，湖北仙桃人，硕士研究生，主要研究方向：信息安全、应用密码学。

作者Email: xuminmail@163.com

参考文献：

本刊中的类似文章

1．朱东方 苏群星 刘鹏远.装备分布式虚拟维修训练云仿真关键技术[J]. 计算机应用, 2013,33(10): 2778-2782

2．任敏.云计算环境下密钥协商协议的应用与改进[J]. 计算机应用, 2013,33(10): 2835-2837

3．罗浩宇 陈旺虎.基于社会网络特征的云服务副本放置策略[J]. 计算机应用, 2013,33(08): 2143-2146

4．武小年 邓梦琴 张明玲 曾兵.云计算中基于优先级和

费用约束的任务调度算法[J]. 计算机应用, 2013,33(08): 2147-2150
5．刘卫宁 靳洪兵 刘波.基于改进量子遗传算法的云计算资源调度[J]. 计算机应用, 2013,33(08): 2151-2153
6．郭凤羽 禹龙 田生伟 于炯 孙华.云计算环境下对资源聚类的工作流任务调度算法[J]. 计算机应用, 2013,33(08): 2154-2157
7．吴胜艳 许力 林昌露.基于门限属性加密的安全分布式云存储模型[J]. 计算机应用, 2013,33(07): 1880-1884
8．熊辉 王川.云应用分类与基于预测的细粒度云资源提供[J]. 计算机应用, 2013,33(06): 1534-1539
9．朱贺新 王正鹏 刘业辉 方水平.基于统一可扩展固件接口的可信密码模块驱动研究与设计[J]. 计算机应用, 2013,33(06): 1646-1649
10．熊金波 姚志强 金彪.云计算环境中结构化文档形式化建模[J]. 计算机应用, 2013,33(05): 1267-1270
11．王光波 马自堂 孙磊 吴乐.基于架构负载感知的虚拟机聚簇部署算法[J]. 计算机应用, 2013,33(05): 1271-1288
12．王素贞 杜治娟.基于移动Agent的移动云计算系统构建方法[J]. 计算机应用, 2013,33(05): 1276-1280
13．闫歌 于炯 杨兴耀.云计算环境下科学工作流两阶段任务调度策略[J]. 计算机应用, 2013,33(04): 1006-1009
14．张雪萍 龚康莉 赵广才.基于MapReduce的K-Medoids并行算法[J]. 计算机应用, 2013,33(04): 1023-1025
15．李海峰 蓝才会.可公开验证的代理重加密签密方案[J]. 计算机应用, 2013,33(04): 1055-1060
16．杜垚 郭涛 陈俊杰.云环境下机群弹性负载均衡机制[J]. 计算机应用, 2013,33(03): 830-833
17．秦志光 柯涛 刘梦娟 王聪.面向云平台的资源分配策略研究[J]. 计算机应用, 2013,33(02): 299-307
18．徐翔 邹复民 廖律超 朱铨.基于GemFire的海量数据计算性能实验分析[J]. 计算机应用, 2013,33(01): 226-229
19．王留洋 俞扬信 周淮.云计算中虚拟资源的智能多代理设计[J]. 计算机应用, 2012,32(12): 3291-3294
20．梁秋实 吴一雷 封磊.基于MapReduce的微博用户搜索排名算法[J]. 计算机应用, 2012,32(11): 2989-2993
21．陈廷伟 周山杰 秦明达.面向云计算的任务分类方法[J]. 计算机应用, 2012,32(10): 2719-2723
22．姚婧 何聚厚.基于自适应蜂群算法的云计算负载平衡机制[J]. 计算机应用, 2012,32(09): 2448-2450

23. 王鹏.云计算系统相空间广义热力学参数定义及分析[J]. 计算机应用, 2012,32(08): 2172-2175
24. 段翰聪 李俊杰 陈宬 李林.异构环境下降低慢任务抖动的调度算法——DPST[J]. 计算机应用, 2012,32(07): 1910-1912
25. 徐骁勇 潘郁 凌晨.云计算环境下资源的节能调度[J]. 计算机应用, 2012,32(07): 1913-1915
26. 左利云 左利锋.云资源中多目标集成蚁群优化调度算法[J]. 计算机应用, 2012,32(07): 1916-1919
27. 陈庆奎 周利珍.基于HBase的大规模无线传感网络数据存储系统[J]. 计算机应用, 2012,32(07): 1920-1923
28. 张敏情 付文华 吴旭光.基于组合设计和身份加密的分簇无线传感器网络密钥管理方案[J]. 计算机应用, 2012,32(05): 1392-1396
29. 陈琳 齐文新 齐宇.基于云计算的自动气象监测网络系统研究与实现[J]. 计算机应用, 2012,32(05): 1415-1417
30. 张春艳 刘清林 孟珂.基于蚁群优化算法的云计算任务分配[J]. 计算机应用, 2012,32(05): 1418-1420
31. 胡军国 祁亨年.基于云计算平台的CO2空间数据融合算法[J]. 计算机应用, 2012,32(04): 1003-1008
32. 汪竹 梅林 李磊 赵太银 胡光岷.适应大规模数据处理的动态服务私有云系统[J]. 计算机应用, 2012,32(04): 1009-1012
33. 吴丘林 李乔良.基于对称平衡不完全区组设计的持续安全管理密钥预分配方案[J]. 计算机应用, 2012,32(04): 960-963
34. 江志雄 金海 黄晓庆.基于并行机制的商务智能系统BI-PaaS[J]. 计算机应用, 2012,32(03): 595-598
35. 周相兵 杨兴江 马洪江.基于划分算法的SaaS寻址中断软件生成策略[J]. 计算机应用, 2012,32(02): 561-565
36. 孙磊 戴紫珊.安全服务云框架研究[J]. 计算机应用, 2012,32(01): 13-15
37. 杨星 马自堂 孙磊.云环境下基于性能向量的虚拟机部署算法[J]. 计算机应用, 2012,32(01): 16-19
38. 孙梅 赵兵.基于身份的Ad Hoc网密钥管理方案[J]. 计算机应用, 2012,32(01): 104-106