计算机应用 2014, 34(1) 27-30 DOI: 10.11772/j.issn.1001-9081.2014.01.0027 ISSN: 1001-9081 CN: 51-1307/TP

先进计算

细粒度云存储数据完整性检测方法

余星,胡德敏,黄超

上海理工大学 光电信息与计算机工程学院,上海 200093

摘要： 在云存储服务中,为了使用户能够方便快捷知道其所存在云端服务器上数据的完整性,提出了一种细粒度云存储数据完整性检测方法。将文件分割成文件子块继而分割成基本块,通过引入双线性对和用户随机选择待检测数据块能无限次检测数据的完整性,此外通过可信第三方的引入解决云用户和云供应商纠纷,实现云存储数据的公开验证性。然后给出了所提出方法的正确性和安全性分析,通过实验证明了该方法能较好地检测云存储数据的完整性。

关键词： 云计算 云存储 数据完整性 数据动态更新 公开验证

Integrity check method for fine-grained cloud storage data

YU Xing,HU Demin,CHANG Huang

School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China

Abstract: In the cloud storage service, in order to know the integrity of the data stored by users on the cloud server, this paper proposed a check method for the integrity of data fine-grained cloud stored. In the proposed method, the file would be divided into sub-blocks and then basic blocks, and with bilinear pairings and data blocks to be detected selected by users randomly, data integrity could be infinitely detected. Furthermore, by introducing a trusted Third Party Auditor (TPA), the dispute between users and cloud storage provider could be well solved for public validation of cloud storage data. Afterwards, analysis of the correctness and security of the method were given in this paper. Finally, experiments verify that the method is able to detect the data integrity of cloud storage better.

Keywords: cloud computing cloud storage data integrity data dynamic updating public validation

收稿日期 2013-07-18 修回日期 2013-09-06 网络版发布日期 2014-02-14

DOI: 10.11772/j.issn.1001-9081.2014.01.0027

基金项目:

国家自然科学基金资助项目;上海市教委科研创新项目;上海市教委“晨光计划”项目

通讯作者: 余星

作者简介: 余星(1987-),男,湖北应城人,硕士研究生,主要研究方向:云计算、计算机网络;胡德敏(1963-),男,上海人,副教授,博士,主要研究方向:计算机网络、云计算、软件理论;黄超(1988-),男,浙江温州人,硕士研究生,主要研究方向:云计算、人工智能。
作者Email: yuxingqq@126.com

参考文献：

本刊中的类似文章

1. 贾磊 王灵矫 郭华 许亚伟 李娟.基于主机标识协议的增强型分布式移动管理[J]. 计算机应用, 2014,34(2): 341-345
2. 杨镜 吴磊 武德安 王晓敏 刘念伯.云平台下动态任务调度人工免疫算法[J]. 计算机应用, 2014,34(2): 351-

356
3．袁爱平 万灿军.云环境下基于改进遗传算法的虚拟机调度策略[J]. 计算机应用, 2014,34(2): 357-359
4．蔡嵩 张建明 陈继明 潘金贵.云计算环境中基于朴素贝叶斯算法的负载均衡技术[J]. 计算机应用, 2014,34(2): 360-364
5．莫志超 张未展 王军 郑炎.基于云计算的P2P流媒体服务器集群部署算法[J]. 计算机应用, 2014,34(2): 365-368
6．王冠 范红 杜大海.云存储访问控制方案的安全性分析与改进[J]. 计算机应用, 2014,34(2): 373-376
7．赵少卡 李立耀 凌晓 徐聪 杨家海.基于OpenStack的清华云平台构建与调度方案设计[J]. 计算机应用, 2013,33(12): 3335-3338
8．戴瑾 刘波 卞皓宇.基于云计算的电子邮件安全服务系统的设计与实现[J]. 计算机应用, 2013,33(12): 3350-3353
9．李春艳 张学杰.基于高性能计算的开源云平台性能评估[J]. 计算机应用, 2013,33(12): 3580-3585
10．李小六 张曦煌.虚拟化云计算数据中心能量感知资源分配机制[J]. 计算机应用, 2013,33(12): 3586-3590
11．洪晓静 王斌.可容忍信息泄露的指定验证者签名方案[J]. 计算机应用, 2013,33(12): 3514-3518
12．冯永 韩楠 贾东风.云计算环境下基于代表点增量层次密度聚类的微博事件检测及跟踪[J]. 计算机应用, 2013,33(12): 3559-3562
13．金伟健 王春枝.适于进化算法的迭代式MapReduce框架[J]. 计算机应用, 2013,33(12): 3591-3595
14．陈波 张曦煌.基于分层与容错机制的云计算负载均衡策略[J]. 计算机应用, 2013,33(11): 3155-3159
15．王芳 李美安 段卫军.基于动态自适应蚁群算法的云计算任务调度[J]. 计算机应用, 2013,33(11): 3160-3162
16．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
17．罗文俊 徐敏.云环境下的基于属性和重加密的密钥管理[J]. 计算机应用, 2013,33(10): 2832-2834
18．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
19．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
20．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
21．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
22．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
23．张雪枫 魏立线 王绪安.无证书的可公开验证聚合签密方案[J]. 计算机应用, 2013,33(07): 1858-1860
24．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
25．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
26．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
27．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
28．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
29．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
30．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
31．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
32．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
33．杜卫东 杨晓元 张祥火 王绪安.适应性选择密文安全的可公开验证加密方案[J]. 计算机应用, 2013,33(04): 1051-1054
34．杨健 王剑 汪海航 杨邓奇.移动云计算环境中基于代理的可验证数据存储方案[J]. 计算机应用, 2013,33(03): 743-747
35．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
36．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
37．陈冬晓 王鹏.基于校验编码备份的分布存储方案[J]. 计算机应用, 2013,33(01): 211-214
38．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
39．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
40．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
41．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

42. 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
43. 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
44. 谢华成 陈向东.面向云存储的非结构化数据存取[J]. 计算机应用, 2012,32(07): 1924-1928
45. 段翰聪 李俊杰 陈成 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
46. 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
47. 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
48. 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
49. 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
50. 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
51. 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
52. 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
53. 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
54. 董继光 陈卫卫 田浪军 吴海佳.大规模云存储系统副本布局研究[J]. 计算机应用, 2012,32(03): 620-624
55. 周敬利 周正达.改进的云存储系统数据分布策略[J]. 计算机应用, 2012,32(02): 309-312
56. 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
57. 曹夕 许力 陈兰香.云存储系统中数据完整性验证协议[J]. 计算机应用, 2012,32(01): 8-12
58. 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
59. 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
60. 李志敏 徐馨 李存华.基于身份的公开验证签密方案[J]. 计算机应用, 2012,32(01): 99-103
61. 姚婧 何聚厚.基于模糊聚类分析的云计算负载平衡策略[J]. 计算机应用, 2012,32(01): 213-217
62. 屈振新 余传明.以云计算为支撑的海量本体推理研究[J]. 计算机应用, 2011,31(12): 3324-3326
63. 葛君伟 李志强 方义秋.云存储环境下基于分散式服务器的Erasure Code算法[J]. 计算机应用, 2011,31(11): 2940-2942
64. 廖彬 于炯 张陶 杨兴耀.基于P2P的分布式文件系统下载效率优化[J]. 计算机应用, 2011,31(09): 2317-2320
65. 江小平 李成华 向文 张新访.云计算环境下朴素贝叶斯文本分类算法的实现[J]. 计算机应用, 2011,31(09): 2551-2554
66. 陈俊 陈孝威.移动IPv4/IPv6的虚拟机迁移过渡框架[J]. 计算机应用, 2011,31(05): 1180-1183
67. 刘进军 赵生慧.面向云计算的多虚拟机管理模型的设计[J]. 计算机应用, 2011,31(05): 1417-1419
68. 徐光侠 陈蜀宇.面向移动云计算弹性应用的安全模型[J]. 计算机应用, 2011,31(04): 952-955
69. 李建锋 彭舰.云计算环境下基于改进遗传算法的任务调度算法[J]. 计算机应用, 2011,31(01): 184-186
70. 曹宁 吴中海 刘宏志 张齐勋.HDFS下载效率的优化[J]. 计算机应用, 2010,30(8): 2260-2065
71. 陈全 邓倩妮.云计算及其关键技术[J]. 计算机应用, 2009,29(09): 2562-2567
72. 王会歌 王彩芬 李泳斌 杨小东.没有pairing的无证书公钥签名方案[J]. 计算机应用, 2008,28(6): 1395-1397
73. 王书海 冯志勇 綦朝晖.权限可控的公开验证代理签密方案[J]. 计算机应用, 2008,28(12): 3163-3164
74. 徐吉斌 叶震.一种可公开验证的基于身份的签密方案[J]. 计算机应用, 2007,27(6): 1553-1555
75. 陈宏兵 刘志军 李千目 许满武 .可更新数据的数据完整性保护方法[J]. 计算机应用, 2006,26(9): 2105-2108
