云计算中数据存储安全的变色龙 Hash 认证树优化审计

李斌 1，李启明 2
(1 福建师范大学 协和学院， 福建 福州 350117; 2 南京大学 计算机软件新技术国家重点实验室，江苏 南京 210023)

摘要： 为提高云计算中数据存储安全性，提出一种云计算中数据存储安全的变色龙 Hash 认证树优化审计方法.首先，提出了一种优化的公共审计协议.通过为 TPA 站点上的用户数据进行同态线性验证器存储，实现对云存储服务器（CSS）响应大小的优化.同时还利用准随机函数优化了对 CSS 的质询请求；其次，使用变色龙散列和一个改进的变色龙认证树，在客户端数据（云计算）上执行高效的动态数据更新，支持块级更新和细粒度更新；最后，通过彻底的安全性和性能分析，证明了所提方法是安全和高效的.
关键词： 云计算；数据存储；变色龙认证树；第三方审计；准随机函数

Chameleon Hash Authentication Tree Optimization Audit for Data Storage Security in Cloud Computing

LI Bin1, Li Qi-ming2
(1 Concord University College Fujian Normal University, Fuzhou 350117, China;
2 Information Engineering College, Shanghai Maritime University, Shanghai 201306, China)

Abstract： In order to improve the security of data storage in cloud computing, a chameleon Hash authentication tree optimized audit method for data storage security in cloud computing is proposed. Firstly, an optimized public audit protocol is proposed. The validator homomorphic linear stored as user data on the TPA site, the cloud storage server (CSS) the size of the optimal response. At the same time, the query request of CSS is optimized by using quasi random function; Secondly, using chameleon hashing and an improved chameleon authentication tree, efficient dynamic data updates are performed on the client data (cloud), supporting block level updates and fine grained updates; Finally, through thorough security and performance analysis, it is proved that the proposed method is secure and efficient.
Key words： cloud computing; data storage; chameleon authentication tree; third party audit; quasi random function

作者简介：
李斌男，(1982-)，硕士，讲师.研究方向为软件架构与设计、机器学习.E-mail:ljjtianjin1980@sina.com.
李启明男，(1982-)，博士，副教授.研究方向为大数据分析、高性能计算.