计算机工程 2012, 38(3) 126-129 DOI: 10.3969/j.issn.1000-3428.2012.03.043 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

去中心化的安全分布式存储系统

贾亚茹[1]，刘向阳[2]，刘胜利[3]

(1. 河北无极中学，石家庄 052460；2. 河北省无极县教育局，石家庄 052460； 3. 上海交通大学计算机科学与工程系，上海 200240)

摘要： 提出一种去中心化的安全分布式存储系统。通过公钥加密和单钥加密相结合的方法，提高存储数据的保密性。对每个数据源使用不同的对称密钥进行分布式加密，采用分布式纠删码对加密后的数据进行编码。使用RS多项式编码和List Decoding译码方法存储加密的对称密钥，以保证系统的鲁棒性。分析结果表明，该方案的计算复杂度较低。

关键词： 分布式存储 分布式纠删码 去中心化存储 加密

Decentralized Secure Distributed Storage System

JIA Ya-ru [1], LIU Xiang-yang [2], LIU Sheng-li [3]

(1. Hebei Wuji High School, Shijiazhuang 052460, China; 2. Wuji Education Bureau of Hebei Province, Shijiazhuang 052460, China; 3. Dept. of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

Abstract: This paper proposes the decentralized secure distributed storage system. The privacy of data is fulfilled by the combination of public key system and symmetric key system. Symmetric key for data from different sources are different, hence encryptions can be implemented in a distributed way. The employment of decentralized erasure code, together with the distributed encryptions, makes possible the decentralization of the system. RS codes are used to store the encryption of symmetric keys, and the list decoding of RS codes ensures the robust. Analysis result shows that the computing efficiency of this system is higher.

Keywords: distributed storage distributed erasure code decentralized storage encryption

收稿日期 2011-05-25 **修回日期** **网络版发布日期** 2012-02-05

DOI: 10.3969/j.issn.1000-3428.2012.03.043

基金项目:

国家自然科学基金资助项目(60873229)；上海市青年科技启明星基金资助项目“模糊保密数据中的密钥提取和保护”(09QA 1403000)

通讯作者:

作者简介: 贾亚茹(1975－)，女，中学一级教师、学士，主研方向：安全存储；刘向阳，中学一级教师、学士；刘胜利，教授、博士

通讯作者E-mail: slliu@sjtu.edu.cn

扩展功能

本文信息

Supporting info

PDF(305KB)

[HTML] 下载

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

分布式存储

分布式纠删码

去中心化存储

加密

本文作者相关文章

贾亚茹

刘向阳

刘胜利

PubMed

Article by Gu, E. R.

Article by Liu, X. Y.

Article by Liu, Q. L.

参考文献：

[1] Dimakis A G, Prabhakaran V, Ramchandran K. Decentralized Erasure Codes for Distributed Networked Storage[J].IEEE Transactions on Information Theory.2006, 52(6):2809-2816

[2] Lin H Y, Tzeng W G. A Secure Decentralized Erasure Code for Distributed Networked

Storage[J].IEEE Transactions on Parallel and Distributed Systems.2010, 21(11):1586-1594

[3] Sudan M. Decoding of Reed-solomon Codes Beyond the Error Correction Bound[J].Journal of Complexity.1997, 13(1):180-

[4] McGowan J. Implementing Generalized Reed-solomon Codes and a Cyclic Code Decoder in GUAVA[EB/OL]. (2005-04-04). http://usna.edu/Users/math/wdj/mcgowan/mcgowan_mathhonors2004-

[5] 05.pdf.

[6] Berlekamp E R. Algebraic Coding Theory[M]. New York.[J].USA: McGraw-Hill.1968,:-

[7] Gemmell P, Sudan M. Highly Resilient Correctors for Polyno- mials[J].Information Processing Letters.1992, 43(4):169-174

本刊中的类似文章

1. 张元玲, 徐中伟, 万勇兵, 夏志翔.铁路信号安全通信协议中的MAC改进算法[J]. 计算机工程, 2012,38(3): 246-248
2. 王明辉, 王建东.基于口令的三方认证密钥交换协议[J]. 计算机工程, 2012,38(2): 146-147
3. 徐贤, 龙宇, 毛贤平.基于TPM的强身份认证协议研究[J]. 计算机工程, 2012,38(04): 23-27
4. 刘祝华, 曾高荣, 谢芳森.基于离散Hopfield网络的混沌图像加密算法[J]. 计算机工程, 2012,38(04): 112-115
5. 赵尔凡, 赵耿, 郑昊.基于多维混沌系统的图像加密算法[J]. 计算机工程, 2012,38(04): 119-121
6. 徐文华, 易法令, 熊伟.基于Chaff Matrix的可撤销声纹模板设计[J]. 计算机工程, 2012,38(04): 236-238
7. 麻浩, 王晓明.外包数据库的安全访问控制机制[J]. 计算机工程, 2011,37(9): 173-175
8. 胡若.异构分布式数据资源中的网格文件访问[J]. 计算机工程, 2011,37(8): 37-39
9. 魏靓, 张串绒, 郑连清.一种基于身份的广义签密方案[J]. 计算机工程, 2011,37(8): 4-6
10. 迟春见, 于万波, 魏小鹏.基于函数展开与超混沌系统的图像加密[J]. 计算机工程, 2011,37(8): 146-148

文章评论

反馈人		邮箱地址	
反馈标题		验证码	7592