

梁鹏,沈昌祥,宁振虎.云计算下可信虚拟群体内访问控制研究[J].通信学报,2013,(Z1):207~215

云计算下可信虚拟群体内访问控制研究

On access to trusted virtual group under cloud computing

投稿时间: 2013-07-05

DOI: 10.3969/j.issn.1000-436x.2013.Z1.027

中文关键词: [云计算](#) [密码学访问控制](#) [密钥管理](#) [生产型信息系统](#)

英文关键词: [cloud computing](#) [cryptographic access control](#) [key management](#) [production information system](#)

基金项目: 国家科技重大专项“新一代宽带无线移动通信网”基金资助项目(2012ZX03002003); 国家高技术研究发展计划(“863”计划)基金资助项目(2009AA01Z437); 国家核高基金资助项目(2010ZX01037-001-001)

作者

单位

[梁鹏, 沈昌祥, 宁振虎](#)

[北京工业大学 计算机学院 北京市可信计算北京市重点实验室 北京 100124](#)

摘要点击次数: 122

全文下载次数: 52

中文摘要:

针对缺乏适合基于云计算的生产型重要信息系统内部隔离机制的问题,对云计算模式下现有的访问控制技术进行了比较,提出了基于两级密钥管理的访问控制方案。第一级构造了一个基于单项散列函数的访问控制多项式实现了子群体间信息流的隔离,即实现了生产型重要信息系统内部部门间的信息隔离;在第一级密钥管理的基础上,提出了子群体间层次密钥管理,实现不同部门间信息流的访问控制。然后对该方案的安全性和复杂度进行了分析。最后,通过实例和仿真实验对基于两级密钥管理的访问控制方案进行了验证。

英文摘要:

There is no appropriate internal isolation mechanism for important production information system based on cloud computing. Here the main access control technologies were compared thoroughly and then two-layer key management scheme was put forward. In terms of the first layer, access control polynomial based on one-way hash function was constructed to achieve the separation of information flow between subgroups, that is, the information isolation within any department of a company was accomplished. Based on the first layer, a hierarchical key management was presented for different subgroups so as to realize the access control between different departments of a company. Then the security and complexity were analyzed. Finally, through the example and simulation experiment, the access control model based on two-layer key management scheme was verified.

[查看全文](#) [查看/发表评论](#) [下载PDF阅读器](#)

关闭

版权所有:《通信学报》

地址:北京市丰台区成寿寺路11号邮电出版大厦8层 电话:010-81055478, 81055479
81055480, 81055482 电子邮件: xuebao@ptpress.com.cn

技术支持:北京勤云科技发展有限公司