

共享文件加密存储分级访问控制方案的实现

李莉^{1,2}, 史国振¹, 王璇², 慈云飞¹

(1. 北京电子科技学院电子信息工程系, 北京 100070;

2. 西安电子科技大学通信工程学院, 陕西 西安 710071)

摘要: 为解决传统文件共享方式单一、安全性不足以及共享文件权限控制自主性过高的问题, 提出了一种文件加密存储分级访问控制方案, 通过在系统中增加分级管理单元, 实现对用户、文件的分级以及用户对文件访问权限的控制, 实现文件的访问范围可控; 通过文件的加密实现文件存储和传输的安全性; 分级密钥的使用, 简化了密钥的存储。服务器端文件的加解密操作通过专门的密码卡实现, 减轻了服务器端的工作量, 加速了文件的加解密处理。在基于 PC 和 Zynq 平台上进行了验证, 实现了预定功能。

关键词: 文件共享; 分级; 访问控制; 加密; 密码; 密钥

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00077

Implementation of shared file encrypted storage hierarchical access control scheme

LI Li^{1,2}, SHI Guo-zhen¹, WANG Xuan², CI Yun-fei¹

(1. School of Electronic and Information Engineering, Beijing Electronics Science and Technology Institute, Beijing 100070, China;

2. School of communication engineering, Xidian University, Xi'an 710071, China)

Abstract: The traditional file sharing way is single, lack of security, and the shared file's permission autonomous control is too high. To solve these problems, a file encrypted storage and hierarchical access control scheme was proposed. Through increasing classification management unit in the system, classification of users and documents, users of file access control were achieved, the scope of file access control was realized. Security of file storage and transmission was realized through encryption, the key storage was simplified using hierarchical key. Server file encryption and decryption operations were achieved through a special password card, which reduced the server workload and accelerated the file encryption and decryption processing. The scheme was verified on PC and Zynq platform, and the predetermined function was realized.

Key words: file sharing, classification, access control, encryption, password, key

1 引言

在信息化办公的现在, 企业在日常办公、产

品研发、开会讨论等活动中会产生大量文件, 这些文件往往需要共享。传统的共享方式是文件由产生者保存, 需要使用文件的员工使用移动硬盘、

收稿日期: 2016-03-02; 修回日期: 2016-05-17。通信作者: 李莉, lili103@besti.edu.cn

基金项目: 国家重点研发计划基金资助项目 (No.2016YFB0800304); 北京市自然科学基金资助项目 (No.4152048); 江苏省自然科学基金资助项目 (No.BK20150787)

Foundation Items: The National Key Research Program of China (No.2016YFB0800304), The Natural Science Foundation of Beijing (No.4152048), The Natural Science Foundation of Jiangsu Province (No.BK20150787)

U 盘等复制, 但这样存在很大的安全隐患。一方面, 大量的文件存储在客户端计算机中容易造成信息丢失; 另一方面, 使用移动存储设备可能会因为丢失、携带计算机病毒等因素造成信息泄露。FTP 服务器作为广泛使用的手段之一, 也因为存储空间有限、扩容麻烦、安全性低、账户间无关联、不支持在线编辑、分享、自动同步等功能而逐渐被云存储代替。企业网盘就是基于云计算理念推出的企业数据网络存储和管理解决方案, 利用互联网后台数据中心的海量计算和存储能力为企业提供数据汇总分发、存储备份和管理等服务。它是一个企事业单位私有的专用网盘系统, 具有强大和简单易用的文档在线编辑预览、协同办公、部门文件共享、自动定时备份、历史资料归档等丰富功能。也正是因为这诸多功能, 企业网盘受到了众多企业的青睐。

但是, 这些网盘在提供更多服务功能的同时, 对安全性却重视不足。主要体现在以下几方面。

1) 文件明文存储在服务器端, 可能会因服务器受到攻击、服务器管理者无意的失误或有意的窃密而造成信息泄露。2) 文件传输过程中没有加密或者仅使用 SSL 等网络协议加密技术。文件明态传输自然会面临很大的危险, 而仅使用网络协议加密技术也是不够可靠的, 因为这些加密技术是公开的, 时刻都有人在研究这些技术中的漏洞, 使用这些方法将面临一些已知或未知的威胁, 如目前已知的 OpenSSL 中的心脏滴血漏洞、SSL 3.0 中的 Poodle 漏洞等。3) 访问控制不够严格, 多数采用自主访问控制, 由资源所有者或管理员自主设定访问主体对资源的访问权限, 存在信息泄露的隐患, 没有体现人员权限的分级。

为此, 有必要研究文件共享中存在的安全问题, 针对这些问题提出一种行之有效的解决方案, 切实地保护共享文件的安全。本文设计了一种文件加密存储分级访问控制方案, 有效保护了文件共享时的机密性, 同时实现基于角色的分级访问控制, 有利于企业根据不同级别的人员分工进行不同权限级别文件的共享。

2 相关研究

目前, 国内外已有多家公司提供企业文件共

享的平台, 国内比较有名的有云盒子、亿方云、Dell 等, 国外的有 Share File、DropBox 等。它们的关注点在于提供尽可能多的服务功能, 如在线浏览分享的文件、提供群聊功能等。同时, 它们的权限设置方法与在 Windows 上分享文件的权限设置相似, 即由文件发布者指定某一个人对该文件具有哪些访问权限, 如读取、修改、写入等。这种权限设置自主性过高, 容易因设置者的失误造成文件的不当扩散。与当前在云存储中存在的问题类似, 平台提供者普遍忽略了对存储在云端的文件机密性保护, 增大了服务器端泄密的风险。

伴随着移动计算、云计算等新型计算模式的出现, 访问控制技术从最早的自主访问控制 (DAC)^[1]、强制访问控制 (MAC)^[2]到基于角色的访问控制模型 (RBAC)^[3], 逐渐向细粒度、分层次发展^[4,5]。目前, 云存储安全性的研究重点是如何将广泛应用于分布式系统的分级加密访问控制应用于云存储系统。分级加密访问控制的基本思想是将文件分类加密存储在云端, 同时将系统内的人员分为若干安全类, 通过一定方法, 高安全类的人员可以推导出本安全类的密钥和低安全类人员持有的密钥, 从而能够访问本级和低级别的文件。第一个分级加密访问控制方案是由 Akl 和 Taylor^[6]提出的, 其思想是由 CA 为每个安全类分配整数, 并且有偏序关系的 2 个安全类中, 低安全等级持有的整数被高安全等级持有的整数整除。这种方案容易被人理解, 但在应用中存在 2 个主要问题: 一是存储的整数量过大, 极大地消耗内存; 二是每次更新都必须更新整个系统, 计算资源消耗过大。此后, 一系列的改进方案被提出。Harn 等^[7]提出一种基于大数难分解的方案, 其方法与 Akl 方案相反, 减少了生成公开令牌所消耗的时间, 但需要的整数总量不变。Hwang 等^[8]结合 Akl 方案和 Harn 的数学思想于 2003 年提出一个减少整数选择过程的方案。Jung 等^[9]于 2011 年提出混合使用独立密钥和非独立密钥进行密钥分配的方案, 在一定程度上提高了系统的执行效率, 但也存在公共参数逐级递增变大的问题。程芳权等^[10]提出一种基于全局逻辑层次图 GLHG 的密钥推导机制的密钥管理方法, 提高密钥管理执行效率。这些研究都试图通过对数据密钥的安全共享和管

理实现对不同用户的选择性数据访问授权控制。

应用方案的实现多数是在基于角色的访问控制基础上进行的改进,通过给角色加入不同的属性和角色的分级处理,实现细粒度的访问控制^[13~15]。2007 年提出双层分级模型和数据重加密管理用户权限的云存储加密访问控制方案,但是计算消耗巨大。吕智泉等^[11]采用基于密文策略的属性加密实现了对密文的访问控制;熊厚仁等^[12]针对现有角色访问控制(RBAC)研究存在因角色设置单一带来适应性差、多域环境下角色或权限冗余、对资源管理关注不够等问题,提出支持资源管理的基于双层角色和组织的访问控制模型。池亚平等^[16]针对电子政务云跨域访问中用户资源共享访问控制细粒度不足的安全问题,提出一种基于用户等级的跨域访问控制方案,通过身份和访问控制管理(IAM),实现了基于用户等级的断言属性认证,消除了用户在资源共享中由于异构环境带来的阻碍。郝小龙^[17]通过在传统基于角色的访问控制 RBAC 中引入 GROUPS 属性,对其进行层次化,实现了电网视频监控系统中大规模授权的分级管理。本文提出的访问控制方案,针对企业共享文件的管理,根据人员实际职权范围的分级,引入分级密钥,通过分级密钥加密共享文件以及基于密码卡的加解密实现技术,实现文件的存储安全和分享安全。

3 分级访问控制策略

在本文所提方案中,人员、文件、密钥均需要分级管理,且文件、人员、密钥的级别一一对应。访问主体为用户和授权管理单位,客体为服务器端加密存储的文件。人员、文件、密钥的分级管理阐述如下。

1) 人员的分级管理。人员级别由应用场景决定,根据人员在单位中的实际职权范围由授权管理单位确定人员级别,假设人员划分为 A、B、C、D 4 个等级,其反映了被定级人员的权限,也决定了其能够访问的文件范围。A 级为最高等级,可以访问 A、B、C、D 等级的文件;B 级次之,可以访问 B、C、D 等级的文件;C 级更次之,可以访问 C、D 等级的文件;D 级仅可以访问 D 级别的文件。

2) 文件的分级管理。文件的级别反映出文件的共享范围,根据文件的内容由授权管理单位确定文件级别,文件等级与人员等级一致,划分为 A、B、C、D 4 个等级。

3) 密钥的分级管理。不同等级的文件在存储时采用不同的等级密钥加密,等级密钥由授权管理单位决定。密钥等级划分与文件等级一致,其中,A 等级密钥用于 A 级别文件的加解密,B 等级密钥用于 B 级别文件的加解密,C 等级密钥用于 C 级别文件的加解密,D 等级密钥用于 D 级别文件的加解密。

每个等级拥有相应的权限,某一人员所拥有的权限由他被赋予的级别决定。本文用五元组 (U, R_U, O, R_O, P, S) 来描述访问控制策略中的各个元素,其中, $U = \{U_i\}$ 表示人员, $R_U = \{R_{U_i}\}$ 表示人员等级, $O = \{O_i\}$ 表示文件资源, $R_O = \{R_{O_i}\}$ 表示文件等级, $P = \{P_r, P_w, P_c, P_d\}$ 表示权限, $S = \{r, w, c, d\}$ 表示会话。其中, r 表示读取操作, w 表示写/修改操作, c 表示生成/提交操作, d 表示删除操作, P_r, P_w, P_c, P_d 分别为相应操作的权限。

1) $UR \subseteq U \times R_U$, 表示人员与人员等级之间多对一的关系。

2) $OR \subseteq O \times R_O$, 表示文件与文件等级之间多对一的关系。

3) $RUO \subseteq R_U \times R_O$, 表示人员等级与文件等级之间一对多的关系。

人员等级和文件等级间具有偏序关系,即 $R_{U_i} \in R_U$, 若 $R_{U_2} \prec R_{U_1}$, 则

$$P_r(R_{U_2}) \subseteq P_r(R_{U_1}) \quad (1)$$

$$P_w(R_{U_2}) \subseteq P_w(R_{U_1}) \quad (2)$$

$$P_c(R_{U_2}) \subseteq P_c(R_{U_1}) \quad (3)$$

$R_{O_i} \in R_O$, 若 $R_{O_2} \prec R_{O_1}$, 则

$$P_r(R_{U_i}) = \{(U_i, O_j) | j \geq i\} \quad (4)$$

$$P_w(R_{U_i}) = \{(U_i, O_j) | j \geq i\} \quad (5)$$

$$P_c(R_{U_i}) = \{(U_i, O_j) | j \leq i\} \quad (6)$$

即高等级的人员可以访问自身等级以下的文件,但是只能生成自身等级以上的文件。每一级别角色的权限定义如表 1 所示,其中,文件等级为 own 时,表示此文件为非共享文件,此时只有

表 1 文件访问控制矩阵

用户等级	文件等级 A			文件等级 B			文件等级 C			文件等级 D			文件等级 own			
	<i>r</i>	<i>w</i>	<i>c</i>	<i>r</i>	<i>w</i>	<i>c</i>	<i>r</i>	<i>w</i>	<i>c</i>	<i>r</i>	<i>w</i>	<i>c</i>	<i>r</i>	<i>w</i>	<i>c</i>	<i>d</i>
A	√	√	√	√	√	×	√	√	×	√	√	×	√*	√*	√*	√*
B	×	×	√	√	√	√	√	√	×	√	√	×	√*	√*	√*	√*
C	×	×	√	×	×	√	√	√	√	√	√	×	√*	√*	√*	√*
D	×	×	√	×	×	√	×	×	√	√	√	√	√*	√*	√*	√*

注：“*”操作仅限于文件的所有者。

文件的所有者才能够对文件进行读取、下载、生成提交保存以及删除操作。例如，A 级别人员的权限包括可以读取并修改 A、B、C、D 4 个等级的所有文件，只可以生成 A 等级的文件；B 级别人员的权限则为可以读取并修改 B、C、D 等级的所有文件，只可以生成 A、B 等级的文件；以此类推，D 级别人员可以读取并修改 D 等级的所有文件，可以生成所有等级的文件。

这样的权限管理方式，一方面方便对用户权限的管理，授权管理单位只需要对不同的角色等级进行权限的约束设置，另一方面也使文件的管理更加方便、合理，通过文件的等级即可限制文件共享的范围。

4 系统模型方案总体架构

本文方案中包含认证中心 CA、分级管理单元、服务器、密码卡、客户端 5 个主体部分。CA 负责服务器和用户的公私钥对的生成、维护、更新和销毁；分级管理单元负责确定用户、文件的等级；服务器用于存放共享文件，负责实现对客户端的身份认证、会话密钥的生成及文件传输等，共享文件在服务器

端均以密态形式存储；密码卡负责对共享文件的加解密操作以及各等级密钥的生成、维护、更新和销毁，保证等级密钥不出卡；客户端负责从服务器下载文件，向服务器上传文件，会话密钥的生成及文件的加解密等。系统模型方案总体架构如图 1 所示。

在此架构中，共享文件始终以密态形式存储在服务器端，且是以对应的等级密钥 k_{scale} 加密存储的，即服务器中存储的文件 C 为

$$C = Enc(k_{scale}, P) \quad (7)$$

按照访问控制策略，只要具有相应的用户等级就可以获取文件。由此可知等级密钥非常关键，一旦等级密钥失密，所有对应等级文件的安全性就会受到影响。据此等级密钥由密码卡生成并存储在密码卡中，由密码卡根据文件等级完成文件的加解密操作。密码卡负责维护密钥信息列表、用户和客户端无法获知等级密钥，从而保证等级密钥的安全性。

为了实现文件的密文存储、密文传输，系统采用三级密钥管理机制。除了等级密钥 k_{scale} 外，还采用了传输密钥 k_{trans} 和会话密钥 $k_{session}$ 。其中，

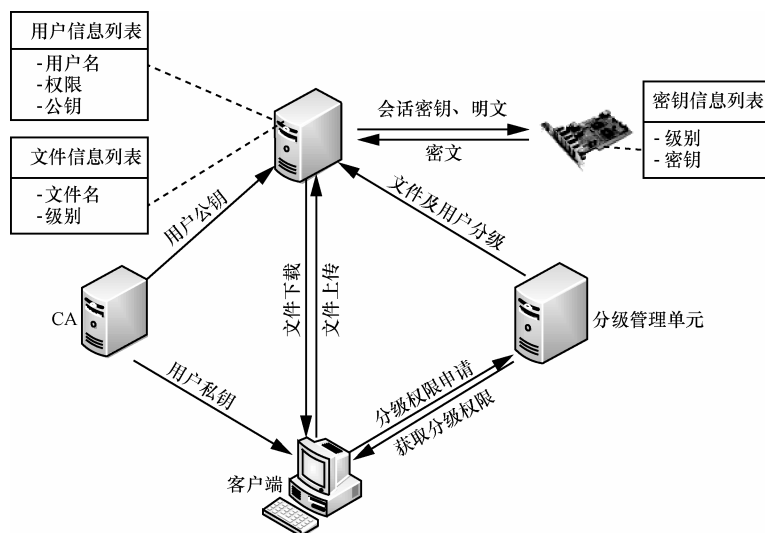


图 1 方案总体架构

会话密钥 k_{session} 用于对传输过程中的明文进行加密, 保证文件的密态传输。 k_{session} 由文件的发送方随机生成, 从而保证文件在传输过程中一次一密, 保证了文件的安全性。

为便于文件的共享, 所有上传的密态共享文件, 必须经过解密后, 由对应的等级密钥加密后才能存储至数据服务器。即文件上传时客户端执行 $C' = \text{Enc}(k_{\text{session}}, P)$, 服务器端执行 $P = \text{Dec}(k_{\text{session}}, C')$ 、 $C = \text{Enc}(k_{\text{scale}}, P)$, 存储密文 C 。这样, 不同的用户只要具有相应的权限, 都可以实现对文件的解密操作。文件下载时服务器端执行 $P = \text{Dec}(k_{\text{scale}}, C)$ 、 $C' = \text{Enc}(k_{\text{session}}, P)$, 客户端执行 $P = \text{Dec}(k_{\text{session}}, C')$ 获取明文 P 。

传输密钥 k_{trans} 用于加密会话密钥, 保证会话密钥的安全性, 保证文件的接收方 (服务器或客户端) 能够对传输的密文进行正确的解密。传输密钥采用 CA 生成的公私钥对实现, 客户端采用私钥进行加密/解密, 服务器端采用公钥进行解密/加密, 从而实现对会话密钥的加密和获取会话密钥。

这种工作方式在对不同级别的文件进行加解密操作时, 只需要查找等级密钥信息表即可, 不需要进行复杂的密钥推导运算, 简化了整个系统运算的复杂度; 同时由于等级密钥的数量有限, 可以达到在增加数据密态存储安全性的同时, 也不会占用太多的密钥存储资源。用户需要下载共享文件时, 必须用等级密钥解密后, 再用随机生成的会话密钥加密才能传输。服务器端文件的加解密操作完全由密码卡完成, 通过密码算法的硬件实现加速文件的明密文转换。

5 访问控制流程

5.1 身份认证流程

本文方案采用公钥密码与时间戳相结合的方法进行身份认证。

1) 客户端向服务器发出带有用户自身 ID 的身份认证请求。

2) 服务器根据请求中的 ID 查询用户的公钥, 生成时间戳及有效期并用公钥加密发送给客户端。

3) 客户端用私钥解密获取时间戳及有效期并判断, 若在有效期内, 则客户端用自己的私钥加密时间戳返回给服务器, 否则重新向服务器请求身份认证。

4) 服务器使用用户公钥解密时间戳, 判断

是否在有效期内, 并比对自己之前发送的时间戳, 若二者一致, 则说明客户端身份合法, 通过身份认证, 否则反馈信息“身份认证失败”。

5.2 文件上传流程

用户通过服务器的身份认证后, 才可以上传权限范围内的等级文件。文件在上传过程中和上传到服务器上后均处于密态, 文件上传流程如图2所示。

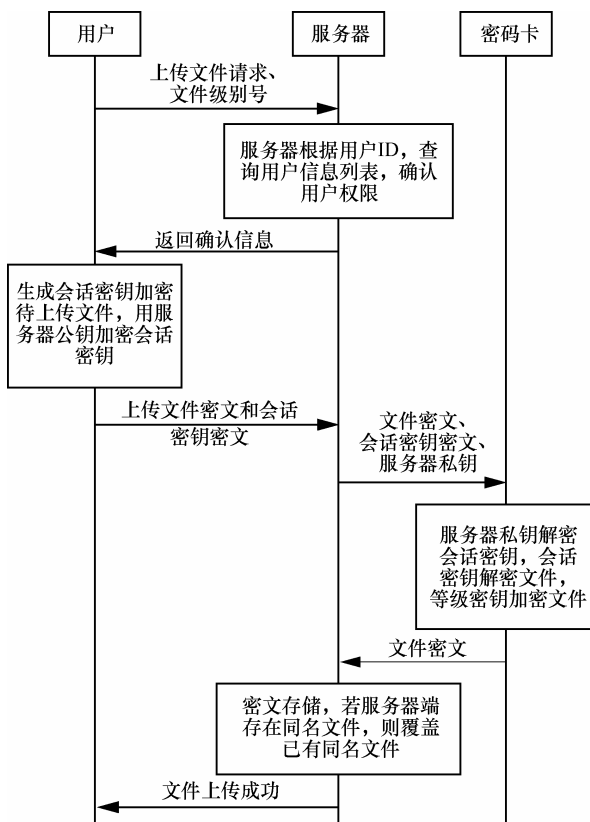


图2 文件上传流程

1) 身份认证通过后, 用户发出申请上传某一等级文件的请求。

2) 服务器根据用户 ID 查询用户权限列表, 确定用户权限。

3) 用户生成一个会话密钥, 加密待上传文件, 再用服务器公钥加密会话密钥, 将密文和被加密的会话密钥上传给服务器。

4) 服务器将私钥及会话密钥密文和文件密文传给密码卡。

5) 密码卡使用服务器私钥解密会话密钥, 用会话密钥解密文件, 并根据文件的密级使用对应的密钥加密文件, 并存储在服务器端; 若服务器端存在相同文件名的文件, 则覆盖已有同名文件。

6) 文件上传完成。

5.3 文件访问流程

当用户通过服务器的身份认证后,才可以申请访问文件,服务器根据访问控制策略判断用户是否有权限访问相应文件。在此流程中,文件在服务器下发给用户的过程中处于密态,文件访问流程如图3所示。

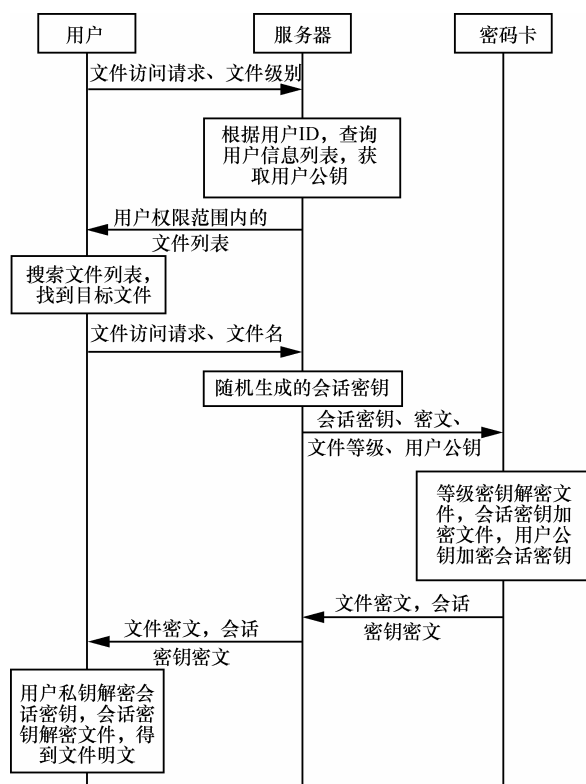


图3 文件访问流程

1) 身份认证通过后,用户向服务器发送某一等级文件访问请求。

2) 服务器根据用户ID查询用户信息列表,获取用户公钥,向用户提供权限范围内的文件列表。

3) 用户搜索文件列表,找到目标文件,并向服务器发出访问该文件请求。

4) 服务器将此密态存储的文件、文件等级、用户公钥以及随机生成的会话密钥发送至密码卡。

5) 密码卡根据文件等级获取密钥,解密文件后,再用会话密钥加密获得文件密文,用用户公钥加密会话密钥获得会话密钥密文,将文件密文和会话密钥密文回传至服务器。

6) 服务器将密文和被加密的会话密钥一同发送给用户。

7) 用户用自己的私钥解密得到会话密钥,再

用会话密钥解密文件,得到文件明文。

8) 文件访问完成。

6 结束语

本文方案通过给用户、文件一定的等级分类,采用一定的分级访问控制策略,实现了对共享文件的分级访问控制,在一定程度上解决了共享文件权限控制自主性过高的问题;通过文件按文件等级的加密存储,保证了文件在服务器端的安全性;通过基于公私钥对的会话密钥加密,保证了文件在传输过程中的安全性。密码卡的使用使文件的加解密操作得以快速执行,减轻了服务器端的压力,也在一定程度上提高了用户的使用体验。方案实现中,本文采用PC机模拟服务器和客户端,采用ARM+FPGA体系架构的芯片ZYNQ-7000实现密码卡的功能,其中,FPGA逻辑部分实现密码算法IP核,ARM部分实现与PC机的通信,验证了此方案的可行性。后期将进一步研究分级访问控制策略的细化以及如何提高多用户交叉访问场景下的快速访问控制方案。

参考文献:

- [1] BUGLIESI M, COLAZZO D, CRAFA S, et al. A type system for discretionary access control[J]. Periodical, 2009, 19(4): 839-875.
- [2] XU L, ZHANG H Q, DU X H, et al. Research on mandatory access control model for application system[C]//The International Conference on Networks Security, Wireless Communications and Trusted Computing. c2009: 159-163.
- [3] SANDHU R, COYNE E, FEINSTEIN H, et al. Role-based access control models[J]. IEEE Computer, 1996, 29(2):38-47.
- [4] WANG G J, LIU Q, WU J. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services[C]//The 17th ACM Conference on Computer and Communications Security. c2010:735-737.
- [5] 李风华, 苏锐, 史国振, 等. 访问控制模型研究进展及发展趋势[J]. 电子学报, 2012, 40(4): 806-813.
- [6] LI F H, SU M, SHI G Z, et al. Research status and development trends of access control model[J]. Acta Electronica Sinica, 2012, 40(4): 806-813.
- [7] AKL S G. Cryptographic solution to a problem of access control in a hierarchy[J]. ACM Transactions on Computer Systems, 1983.
- [8] HARN L, LIN H Y. A cryptographic key generation scheme for multilevel data security[J]. Computers and Security, 1990.
- [9] HWANG M S, YANG W P. Controlling access in large partially ordered hierarchies using cryptographic keys[J]. The Journal of Systems and Software, 2003.
- [10] LO J W, HWANG M S, LIU C H. An efficient key assignment scheme for access control in a large leaf class hierarchy[J]. Information Sciences, 2010 (4).

- [10] 程芳权, 彭智勇, 宋伟, 等. 可信云存储环境下支持访问控制的密钥管理[J]. 计算机研究与发展, 2013, 8:1613-1627.
CHENG F Q, PENG Z Y, SONG W, et al. Key management for access control in trusted cloud storages[J]. Journal of Computer Research and Development, 2013, 8:1613-1627.
- [11] 吕智泉, 张敏, 冯登国. 云存储密文访问控制方案[J]. 计算机科学与探索, 2011, 5(9): 836-844.
LV Z Q, ZHANG M, FENG D G. Cryptographic access control scheme for cloud storage [J]. Journal of Frontiers of Computer Science & Technology, 2011, 5(9): 836-844.
- [12] 熊厚仁, 陈性元, 张斌, 等. 基于双层角色和组织的可扩展访问控制模型[J]. 电子与信息学报, 2015, 7: 1612-1619.
XIONG H R, CHEN X Y, ZHANG B, et al. Scalable access control model based on double-tier role and organization[J]. Journal of Electronics & Information Technology, 2015, 7: 1612-1619.
- [13] 李怀明, 王慧佳, 符林. 基于组织的 Web 服务访问控制模型[J]. 计算机工程, 2014, 11: 65-70.
LI H M, WANG H J, FU L. Organization-based access control model for Web service[J]. Computer Engineering, 2014, 11: 65-70.
- [14] 熊智, 王平, 徐江燕, 等. 一种基于属性的企业云存储访问控制方案[J]. 计算机应用研究, 2013, 2: 513-517.
XIONG Z, WANG P, XU J Y, et al. Attribute based access control strategy for enterprise cloud storage [J]. Application Research of Computers, 2013, 2: 513-517.
- [15] 王小威, 赵一鸣. 一种基于任务角色的云计算访问控制模型[J]. 计算机工程, 2012, 24:9-13.
WANG X W, ZHAO Y M. A task-role-based access control model for cloud computing [J]. Computer Engineering, 2012, 24:9-13.
- [16] 池亚平, 王艳, 王慧丽, 等. 基于等级的电子政务云跨域访问控制技术[J]. 计算机应用, 2016, 2:402-407.
CHI Y P, WANG Y, WANG H L, et al. Cross-domain access control for e-government cloud based on classification [J]. Journal of Computer Applications, 2016, 2:402-407.
- [17] 郝小龙. 改进的 RBAC 模型在电网视频监控平台中的应用[J]. 计算机技术与发展, 2014, 12: 212-215.
HAO X L. Application of improved RBAC model in grid video monitoring platform[J]. Computer Technology and Development, 2014, 12: 212-215.

作者简介:



李莉(1974-), 女, 山东青岛人, 西安电子科技大学博士生, 北京电子科技学院副教授、硕士生导师, 主要研究方向为网络与系统安全、嵌入式系统安全应用。



史国振(1974-), 男, 河南济源人, 博士, 北京电子科技学院副教授、硕士生导师, 主要研究方向为网络与系统安全、嵌入式安全。



王璇(1991-), 女, 山东菏泽人, 西安电子科技大学硕士生, 主要研究方向为多核调度。



慈云飞(1989-), 男, 安徽池州人, 北京电子科技学院硕士生, 主要研究方向为访问控制和信息安全。