(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101938497 B
(45)授权公告日 2013.01.30

(21)申请号 201010292110.1

(22)申请日 2010.09.26

(73)专利权人 深圳大学
地址 518060 广东省深圳市南山区南海大道3668号深圳大学计算机与软件学院

(72)发明人 陈剑勇 陈宝楷 纪震 储颖

(74)专利代理机构 深圳市顺天达专利商标代理有限公司 44217
代理人 易钊

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)
G06F 21/60(2013.01)

(56)对比文件
WO 2006/131906 A2,2006.12.14,
CN 101047978 A,2007.10.03,
CN 101605137 A,2009.12.16,
CN 101605137 A,2009.12.16,
CN 101442404 A,2009.05.27,
CN 1859086 A,2006.11.08,
CN 1859086 A,2006.11.08,

审查员 颜悦

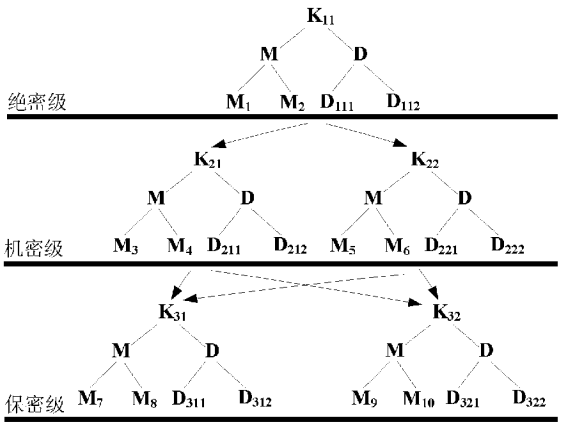
权利要求书 2 页 说明书 7 页 附图 3 页

(54)发明名称

多级保密文档组设置方法及其文件访问控制和密钥管理用户终端、服务终端、系统和方法

(57)摘要

本发明涉及多级保密文档组设置方法及文件访问控制和密钥管理用户终端、服务终端、系统和方法，该设置方法设置多个用于区分不同密级文档的保密等级，每个保密等级设置多个不相互重叠的文档组；每个文档组设置为包括根结点，及基于该根结点的左子节点和右子节点；左子节点设置为可以访问文档组的成员组，右子节点设置为文档组中的文档，根结点存储有供成员组访问文档的工作密钥；保密等级较高的文档组的右子节点设置为除了包含本身的文档外，还包含保密等级比其低一级的文档组。本发明对用户访问权限进行区分管理，配合用户访问权限的控制，实现了计算机文件的多级保护管理；同时增加密钥的软硬生命周期，使新旧密钥的有效更替，实现密钥使用安全。



CN 101938497 B

1. 一种多级保密文档组设置方法，其特征在于，包括以下步骤：

设置多个用于区分不同密级文档的保密等级，每个所述保密等级设置多个不相互重叠的文档组；

每个所述文档组设置为包括根结点，以及基于该根结点的左子节点和右子节点；

其中，所述左子节点设置为可以访问所述文档组的成员组，所述右子节点设置为所述文档组中的文档，所述根结点存储有供所述成员组访问所述文档的工作密钥；

保密等级较高的文档组的右子节点设置为除了包含本身的文档外，还包含保密等级比其低一级的文档组，保密等级较高的文档组中的成员默认拥有保密等级较低的文档组的工作密钥；

所述工作密钥设置为还包括文件访问控制权限标识与密钥版本号，所述文档组还用于密钥更新，根据旧的工作密钥的密钥版本号设定新的工作密钥的密钥版本号，将所述旧工作密钥的密钥版本号最后一位取反，得到所述新的工作密钥的密钥版本号，根据旧的工作密钥的文件访问控制权限标识与新的工作密钥的密钥版本号取得新密钥。

2. 根据权利要求 1 所述的多级保密文档组设置方法，其特征在于，所述文档组设置为采用编号 K_{im} 进行标识，其中 i 表示该文档组中的文档所属的保密等级，m 表示该文档组在所属的保密等级中所对应的文档组序号；每个所述文档组设置为采用自身编号作为根结点；其中，所述 i 和 m 为自然数。

3. 根据权利要求 1 所述的多级保密文档组设置方法，其特征在于，所述右子节点中所包含的文档设置为包括文件内容及文件尾；其中，

所述文件尾包括：文件加密标识、文件访问权限标识、密钥版本号；

所述文件访问权限标识由文件保密级别和所属文档组信息构成。

4. 根据权利要求 1 所述的多级保密文档组设置方法，其特征在于，所述工作密钥设置为还包括：密钥控制符、密钥材料、随机数、密钥软生命周期和密钥硬生命周期；

其中，所述密钥硬生命周期为计算机系统所设定的密钥生命周期；所述密钥软生命周期为密钥硬生命周期结束前的其他原因导致的密钥失效时间。

5. 一种基于权利要求 1 所述的多级保密文档组设置方法的文件访问控制及密钥管理用户终端，其特征在于，包括：

用户登录服务器认证模块，用于获取用户 ID、用户密钥和用户登录时间，并发送给服务终端；

密钥生成与使用模块，用于生成工作密钥，并通过密钥软硬生命周期、密钥控制符实现新旧密钥之间的交替；

文件管理模块，用于存储文件，并将登录的用户 ID 所对应的文件保护范围信息发送给服务终端。

6. 一种基于权利要求 1 所述的多级保密文档组设置方法的文件访问控制及密钥管理服务终端，其特征在于，包括：

用户认证模块，用于根据服务端所保存的用户密钥对用户进行合法性认证，待合法用户通过后，根据用户密钥和登录时间生成一个和用户终端通讯共享的密钥，用于传递反馈信息；

权限配置模块，用于完成用户权限的更改、确定用户权限；

密钥管理模块，用于完成密钥的分配、更新和维护；

文件管理模块，用于对文件进行分级别、分组别，以及把文件的级别和组别信息发送给密钥管理模块；

密钥控制模块，用于通过用户权限配置、用户受限权限和用户端所保护的文件信息综合考虑，决定分配给用户的密钥材料。

7. 一种基于权利要求 1 所述的多级保密文档组设置方法的文件访问控制及密钥管理系统，其特征在于，包括如权利要求 5 所述的用户终端，以及与所述用户终端通信连接的如权利要求 6 所述的服务终端。

8. 一种基于权利要求 1 所述的多级保密文档组设置方法的文件访问控制及密钥管理方法，其特征在于，包括以下步骤：

获取用户 ID、用户密钥和用户登录时间；

根据服务端所保存的用户密钥对用户进行合法性认证，待合法用户通过后，根据用户密钥和登录时间生成一个和用户终端通讯共享的密钥，以传递服务终端的反馈信息；

根据登录的用户 ID 所对应的文件保护范围信息，对文件进行分级别、分组别，完成密钥的分配、更新和维护；

通过用户权限配置、用户受限权限和用户端所保护的文件信息综合考虑，决定分配给用户的密钥材料；

根据所分配的密钥材料，生成工作密钥。

9. 根据权利要求 8 所述的文件访问控制及密钥管理方法，其特征在于，所述通过用户权限配置、用户受限权限和用户端所保护的文件信息综合考虑，决定分配给用户的密钥材料步骤具体包括以下步骤：

取得用户默认权限；

过滤用户受限权限；

过滤用户不需要使用的密钥；

决定最终分配给用户的密钥材料。

10. 根据权利要求 8 所述的文件访问控制及密钥管理方法，其特征在于，所述完成密钥的更新过程包括以下步骤：

检查密钥的密钥硬生命周期是否到期；

如果密钥硬生命周期到期，设置该密钥较新版本密钥的密钥控制符，替代旧密钥，清除旧密钥；

如果密钥硬生命周期没到期，再判断密钥软生命周期是否到期；

如果密钥软生命周期到期，获取该密钥新版本密钥标识，设定新密钥，设置该密钥旧版本密钥的密钥控制符，更新树结构的密钥信息；

如果密钥软生命周期没到期，完成检查。

多级保密文档组设置方法及其文件访问控制和密钥管理用户终端、服务终端、系统和方法

技术领域

[0001] 本发明涉及计算机文件系统，更具体地说，涉及一种计算机文件系统的多级保密文档组设置方法及其文件访问控制和密钥管理用户终端、服务终端、系统和方法。

背景技术

[0002] 传统的计算机文件系统不支持用户访问权限控制，且不对文件进行加密存储，对重要的文件和普通文件没有被区分对待，因此文件可以随意被复制和传播，这不利于文件内容安全。

[0003] 有些计算机文件系统支持对文件进行加密，但是其无法保证加密密钥的安全。而文件加密的密钥安全对文件安全至关重要，一旦加密密钥被非法获取，那么将给文件保护带来危险。

[0004] 例如公开号为 CN 1567255A 的发明专利，公开了一种安全文件系统的存储及访问控制方法，其将数字签名技术和加密技术应用于文件系统中，通过对文件进行数字签名并实施原始性鉴别，防止文件被篡改；根据文件存储的不同密级要求，对存储文件采用不同的加密算法和加密强度进行加密，防止文件被窃取而导致信息泄露等内容。

[0005] 但是上述现有技术存在以下缺点：1、没有区分控制用户访问权限，不能实现灵活的文件分类管理；2、不能解决文件加密密钥更新的问题，不能很好地满足文件加密保护的安全性要求。

发明内容

[0006] 本发明要解决的技术问题在于，提供一种多级保密文档组设置方法及其文件访问控制和密钥管理用户终端、服务终端、系统和方法。

[0007] 本发明解决其技术问题所采用的技术方案是：

[0008] 构造一种多级保密文档组设置方法，其中，包括以下步骤：

[0009] 设置多个用于区分不同密级文档的保密等级，每个所述保密等级设置多个不相互重叠的文档组；

[0010] 每个所述文档组设置为包括根结点，以及基于该根结点的左子节点和右子节点；

[0011] 其中，所述左子节点设置为可以访问所述文档组的成员组，所述右子节点设置为所述文档组中的文档，所述根结点存储有供所述成员组访问所述文档的工作密钥；

[0012] 保密等级较高的文档组的右子节点设置为除了包含本身的文档外，还包含保密等级比其低一级的文档组，保密等级较高的文档组中的成员默认拥有保密等级较低的文档组的工作密钥。

[0013] 本发明所述的多级保密文档组设置方法，其中，所述文档组设置为采用编号 Kim 进行标识，其中 i 表示该文档组中的文档所属的保密等级，m 表示该文档组在所属的保密等级中所对应的文档组序号；每个所述文档组设置为采用自身编号作为根结点；其中，所述 i

和 m 为自然数。

[0014] 本发明所述的多级保密文档组设置方法，其中，所述右子节点中所包含的文档设置为包括文件内容及文件尾；其中，

[0015] 所述文件尾包括：文件加密标识、文件访问权限标识、密钥版本号；

[0016] 所述文件访问权限标识由文件保密级别和所属文档组信息构成。

[0017] 本发明所述的多级保密文档组设置方法，其中，所述工作密钥设置为包括：文件访问控制权限标识、密钥版本号、密钥控制符、密钥材料、随机数、密钥软生命周期和密钥硬生命周期；

[0018] 其中，所述密钥硬生命周期为计算机系统所设定的密钥生命周期；所述密钥软生命周期为密钥硬生命周期结束前的其他原因导致的密钥失效时间。

[0019] 本发明还提供了一种基于前面所述的多级保密文档组设置方法的文件访问控制及密钥管理用户终端，其中，包括：

[0020] 用户登录服务器认证模块，用于获取用户 ID、用户密钥和用户登录时间，并发送给服务终端；

[0021] 密钥生成与使用模块，用于生成工作密钥，并通过密钥软硬生命周期、密钥控制符实现新旧密钥之间的交替；

[0022] 文件管理模块，用于存储文件，并将登录的用户 ID 所对应的文件保护范围信息发送给服务终端。

[0023] 本发明还提供了一种基于前面所述的多级保密文档组设置方法的文件访问控制及密钥管理服务终端，其中，包括：

[0024] 用户认证模块，用于根据服务端所保存的用户密钥对用户进行合法性认证，待合法用户通过后，根据用户密钥和登录时间生成一个和用户终端通讯共享的密钥，用于传递反馈信息；

[0025] 权限配置模块，用于完成用户权限的更改、确定用户权限；

[0026] 密钥管理模块，用于完成密钥的分配、更新和维护；

[0027] 文件管理模块，用于对文件进行分级别、分组别，以及把文件的级别和组别信息发送给密钥管理模块；

[0028] 密钥控制模块，用于通过用户权限配置、用户受限权限和用户端所保护的文件信息综合考虑，决定分配给用户的密钥材料。

[0029] 本发明还提供了一种基于前面所述的多级保密文档组设置方法的文件访问控制及密钥管理系统，其中，包括前面所述的用户终端，以及与所述用户终端通信连接的服务终端。

[0030] 本发明还提供了一种基于前面所述的多级保密文档组设置方法的文件访问控制及密钥管理方法，其中，包括以下步骤：

[0031] 获取用户 ID、用户密钥和用户登录时间；

[0032] 根据服务端所保存的用户密钥对用户进行合法性认证，待合法用户通过后，根据用户密钥和登录时间生成一个和用户终端通讯共享的密钥，以传递服务终端的反馈信息；

[0033] 根据登录的用户 ID 所对应的文件保护范围信息，对文件进行分级别、分组别，完成密钥的分配、更新和维护；

[0034] 通过用户权限配置、用户受限权限和用户端所保护的文件信息综合考虑，决定分配给用户的密钥材料；

[0035] 根据所分配的密钥材料，生成工作密钥。

[0036] 本发明所述的文件访问控制及密钥管理方法，其中，所述通过用户权限配置、用户受限权限和用户端所保护的文件信息综合考虑，决定分配给用户的密钥材料步骤具体包括以下步骤：

[0037] 取得用户默认权限；

[0038] 过滤用户受限权限；

[0039] 过滤用户不需要使用的密钥；

[0040] 决定最终分配给用户的密钥材料。

[0041] 本发明所述的文件访问控制及密钥管理方法，其中，所述完成密钥的更新过程包括以下步骤：

[0042] 检查密钥的密钥硬生命周期是否到期；

[0043] 如果密钥硬生命周期到期，设置该密钥较新版本密钥的密钥控制符，替代旧密钥，清除旧密钥；

[0044] 如果密钥硬生命周期没到期，再判断密钥软生命周期是否到期；

[0045] 如果密钥软生命周期到期，获取该密钥新版本密钥标识，设定新密钥，设置该密钥旧版本密钥的密钥控制符，更新树结构的密钥信息；

[0046] 如果密钥软生命周期没到期，完成检查。

[0047] 本发明通过采用多级保密文档组设置方法，对文件进行分级别加密存储，只要用户有足够的权限都能正常读写文件，不影响合法用户的文件共享，同时也满足了文件的安全性要求。

[0048] 基于本发明的多级保密文档组设置方法，对用户访问权限进行区分管理，配合用户访问权限的控制，可以灵活的设置用户的访问权限，达到对文件分类的细化管理。对进入文件保护区的用户都要进行身份验证，合法的用户才能进入文件保护区，防止越权访问、禁止非法用户对保护文件的任何操作。实现了计算机文件的多级保护管理。

[0049] 同时，本发明还针对密钥泄露的安全隐患，定期或必要时对密钥进行更新，使得密钥使用安全，从而保证文件加密保护的安全。

附图说明

[0050] 下面将结合附图及实施例对本发明作进一步说明，附图中：

[0051] 图 1 是本发明较佳实施例的多级保密文档组结构图；

[0052] 图 2 是本发明较佳实施例的密钥管理图；

[0053] 图 3 是本发明较佳实施例的文档组密钥更新流程图；

[0054] 图 4 是本发明较佳实施例的密钥控制流程；

[0055] 图 5 是本发明较佳实施例的密钥分配及用户权限更改示意图；

[0056] 图 6 是本发明较佳实施例的文件访问控制及密钥管理系统功能模块结构图；

[0057] 图 7 是本发明较佳实施例的文件访问控制及密钥管理系统各功能模块间信息交互状态示意图。

具体实施方式

[0058] 本发明实施例的多级保密文档组设置方法设置的多级保密文档组结构如图 1 所示，该实施例包括以下步骤：设置多个用于区分不同密级文档的保密等级，每个保密等级设置多个不相互重叠的文档组；每个文档组设置为包括根结点，以及基于该根结点的左子节点和右子节点。其中，左子节点设置为为可以访问文档组的成员组，右子节点设置为为文档组中的文档，根结点存储有供成员组访问文档的工作密钥。保密等级较高的文档组的右子节点设置为除了包含本身的文档外，还包含保密等级比其低一级的文档组，保密等级较高的文档组中的成员默认拥有保密等级较低的文档组的工作密钥。

[0059] 本实施例中，优选地，文档组设置为采用编号 K_{im} 进行标识，其中 i 表示该文档组中的文档所属的保密等级，m 表示该文档组在所属的保密等级中所对应的文档组序号；每个文档组设置为采用自身编号作为根结点。其中，i 和 m 为自然数。

[0060] 本实施例中，优选地，右子节点中所包含的文档设置为包括文件内容及文件尾。其中，如下表 1 所示，文件尾包括：文件加密标识、文件访问权限标识、密钥版本号。文件访问权限标识由文件保密级别和所属文档组信息构成。

[0061] 表 1 文件结构

[0062]

文件内容（密文）	
文件尾	文件加密标识
	文件访问权限标识
	密钥版本号

[0063] 其中，如下表 2 所示，上述各实施例中的工作密钥设置为包括：文件访问控制权限标识、密钥版本号、密钥控制符、密钥材料、随机数、密钥软生命周期和密钥硬生命周期。其中，密钥硬生命周期为计算机系统所设定的密钥生命周期；密钥软生命周期为密钥硬生命周期结束前的其他原因导致的密钥失效时间。

[0064] 表 2 密钥结构

[0065]

文件访问权限标识+密钥版本号	密钥控制符	密钥材料	随机数	软/硬生命周期

[0066] 下面结合附图 1，以对上述实施例中的多级保密文档组结构的形成过程进行详细说明：

[0067] 首先根据保密级别将文档分为若干等级，这里假设分成三个等级 Pi（$1 \leqslant i \leqslant 3$），对应着三个保密级别，分别为保密级、机密级和绝密级。然后，在每个保密级别中，可以根据企业实际需要分为不相互重叠的文档组 Kim（其中 i 表明文档属于哪个保密级别，m 指明保密级中的哪个文档组）。

[0068] 每个文档组都有不同的工作密钥，它用于对文档组中的文件进行加解密。一个文档组可以生成一棵这样的树：文档组 ID 为根结点，左边孩子节点（左子节点）M 为可以访问该文档组的成员组，右边孩子节点（右子节点）D 为文档组中的文档，如图 1 所示。这样，通过文档组的根结点，成员组中的成员和该文档组的文件有了关联，这也说明，成员组中的成

员可以通过文档组的密钥对属于文档组的文件进行操作。

[0069] 保护级别较高的文档组右边孩子节点除了本身的文档外，文档组保护级别比其低一级的也都成为它的右孩子节点。由上至下，以此类推，这些以树的形式表示的文档组，组成由成员、密钥和文档对应起来的密钥管理图，如图 2 所示，假设每个文档组有两个成员和两个文件。

[0070] 在密钥管理图中，如图 2 所示，就单个文档组的树结构来讨论，通过层与层之间的关系，处于高一级保护级别的成员默认情况下可以拥有本组文档和较低保护级别的文档组的工作密钥。例如，Kim 下的成员可以拥有保密第 1 级中第 m 组文档的工作密钥，同时拥有比保密级别 1 低的所有工作密钥。且每个文档组是不相互重叠的，每个文档组可访问成员也是不相互重叠的，因此，成员工作密钥的分配、文档组密钥的更新、成员组中成员的进入 / 退出所引起的密钥更新都可以依照如图 2 所示的密钥管理图进行管理。

[0071] 本发明还提供了一种基于前面的多级保密文档组设置方法的文件访问控制及密钥管理方法，其中，包括以下步骤 ：

[0072] 获取用户 ID、用户密钥和用户登录时间 ；

[0073] 根据服务端所保存的用户密钥对用户进行合法性认证，待合法用户通过后，根据用户密钥和登录时间生成一个和用户终端通讯共享的密钥，以传递服务终端的反馈信息 ；

[0074] 根据登录的用户 ID 所对应的文件保护范围信息，对文件进行分级别、分组别，完成密钥的分配、更新和维护 ；

[0075] 通过用户权限配置、用户受限权限和用户端所保护的文件信息综合考虑，决定分配给用户的密钥材料 ；

[0076] 根据所分配的密钥材料，生成工作密钥。

[0077] 上述实施例中，通过用户权限配置、用户受限权限和用户端所保护的文件信息综合考虑，决定分配给用户的密钥材料步骤，即密钥控制，流程图如图 4 所示，具体包括以下步骤 ：取得用户默认权限 ；过滤用户受限权限 ；过滤用户不需要使用的密钥 ；决定最终分配给用户的密钥材料。

[0078] 上述实施例中，完成文档组密钥的更新过程流程图如图 3 所示，包括以下步骤 ：检查密钥的密钥硬生命周期是否到期 ；如果密钥硬生命周期到期，设置该密钥较新版本的密钥控制符，替代旧密钥，清除旧密钥，更新树结构的密钥信息，完成更新 ；如果密钥硬生命周期没到期，再判断密钥软生命周期是否到期 ；如果密钥软生命周期到期，获取该密钥新版本的密钥标识，设定新密钥，设定该密钥旧版本密钥的密钥控制符，更新树结构的密钥信息，完成更新 ；如果密钥软生命周期没到期，完成检查。

[0079] 其中，文档组密钥更新，根据旧密钥的密钥版本号设定新的密钥版本号，具体是旧密钥的密钥版本号最后一位取反，得到新密钥的密钥版本号，目的是既能与旧密钥区分，又可以根据旧密钥的文件访问控制权限标识 + 密钥版本号轻松取得新密钥。接着设定更新密钥的材料和生命周期，并设置新密钥的新老密钥控制符为 11，区别于旧的密钥，而旧密钥的新老密钥控制符则设置为 10，表示新老密钥同时存在。在密钥管理图结构中，存储在该文档组的结点信息中。服务器分配密钥给用户时，只需读取相关文档组结点上的密钥信息，新旧密钥同时存在时，新旧版本都要发送给用户。服务器发现旧密钥硬生命周期已经越期时，将用新密钥取代旧密钥，即把旧密钥的信息从文档组结点中清除，并将新密钥的新老密钥控

制符设置为 00。

[0080] 当读文件需要使用密钥时，首先匹配用户的访问权限，如果合法，再到用户的工作密钥列表中搜索与文件头中（文件访问权限标识 + 密钥版本号）一致的标识，然后取出工作密钥的内容，对文件内容进行解密。写文件操作完成后，文件保存到磁盘时，需要对文件内容进行加密。首先，通过文件新老密钥控制符判断文件的加密密钥是否应该更新，若控制符为 10，则说明该文件的加密密钥处在新老交替阶段。先把文件头中的密钥版本号最后一位取反，再到用户的工作密钥中列表中搜索和（文件访问权限标识 + 密钥版本号）一致的标识，取出该密钥对文件进行加密保存。

[0081] 需要理解的是，本发明的密钥管理图（附图 2）所提到的用户、密钥和文件之间的对应关系是一种逻辑关系，通过图的形式可以更直观地理解和实现用户权限和密钥的管理，但是可以表示这种逻辑关系的方法还有很多，因此并不限于附图中所表示的内容。

[0082] 本发明还提供了一种基于前面的多级保密文档组设置方法的文件访问控制及密钥管理用户终端，与一服务终端通信连接，包括用户登录服务器认证模块、密钥生成与使用模块和文件管理模块。其中，用户登录服务器认证模块，用于获取用户 ID、用户密钥和用户登录时间，并发送给服务终端；密钥生成与使用模块，用于生成工作密钥，并通过密钥软硬生命周期、密钥控制符实现新旧密钥之间的交替；文件管理模块，用于存储文件，并将登录的用户 ID 所对应的文件保护范围信息发送给服务终端。

[0083] 本发明还提供了一种基于前面的多级保密文档组设置方法的文件访问控制及密钥管理服务终端，包括用户认证模块、权限配置模块、密钥管理模块、文件管理模块和密钥控制模块。其中，用户认证模块，用于根据服务端所保存的用户密钥对用户进行合法性认证，待合法用户通过后，根据用户密钥和登录时间生成一个和用户终端通讯共享的密钥，用于传递服务终端的反馈信息；权限配置模块，用于完成用户权限的更改、确定用户权限；密钥管理模块，用于完成密钥的分配、更新和维护；文件管理模块，用于对文件进行分级别、分组别，以及把文件的级别和组别信息发送给密钥管理模块；密钥控制模块，用于通过用户权限配置、用户受限权限和用户端所保护的文件信息综合考虑，决定分配给用户的密钥材料。

[0084] 本发明还提供了一种基于前面实施例中所述的多级保密文档组设置方法的文件访问控制及密钥管理系统，如图 6 所示，包括前面实施例中的用户终端和服务终端，该用户终端和服务终端之间的信息交互如图 7 所示。用户终端的用户登陆服务器认证模块，它需要向服务器端提供用户 ID、用户密钥和登陆时间等信息并等待服务器的反馈；密钥生成与使用模块主要负责文件工作密钥的生成和新旧密钥之间的协调：只有进入文件保护区时，才生成文件工作密钥，用户退出文件保护区时，该模块销毁所有工作密钥，以达到密钥使用的安全；通过密钥软硬生命周期、密钥控制符等实现新旧密钥的无缝交替，无须用户参与。文件管理模块负责用户终端所保护的文件范围，服务器端需要根据该模块提供用户端文件存在信息控制分配的密钥材料。

[0085] 服务终端的用户认证模块负责用户的登陆认证，利用服务器端保存的用户密钥对用户进行合法性认证，合法用户通过认证后，该模块使用用户密钥和登陆时间生成一个和用户终端通讯共享的密钥，用于传递服务器端的反馈信息。权限配置模块负责用户权限的更改、确定用户权限。密钥管理模块是最为重要的，通过它以实现密钥的使用安全，它负责密钥的分配、更新、维护等工作。文件管理模块主要负责文件的分级别、分组别，然后把这些

信息传递给密钥管理模块。密钥控制模块的功能是控制服务器分配给用户哪些需要的密钥材料，它是通过用户权限配置、用户受限权限和用户端所保护的文件信息综合考虑，决定分配给用户的密钥材料。

[0086] 在本实施例的系统中，如图 5 所示，当密钥分配和更改用户权限时，在用户终端和服务器端，它们之间的通讯和各自内部的处理需要完成的任务分别有 ：

[0087] 在用户终端 ：用户登录认证，并把登录时间作为随机数一并发送给服务器，同时在用户端保存这一登录时间 T。用户使用自己的登录密钥和登录时间产生用户密钥，解密由服务器密钥管理 / 密钥控制模块返回的密钥材料并生成文件的工作密钥。

[0088] 在服务器端 ：服务器根据用户在密钥管理图中的 ID 确定该用户所属权限，再配合密钥控制模块，决定用户应该分配哪些密钥。服务器利用用户登录密钥生成用户密钥，加密应该分配的密钥材料并发送给用户。当企业员工退出企业时，员工工作时所使用的密钥必须更新。根据员工的 ID 和权限策略管理确定哪些文档组的密钥需要更新，更新操作和文档组密钥更新类似。有新的员工加入企业时，只需要将员工添加到他所属的文档组。企业员工在企业部门间调动时，权限发生改变时，可以根据员工在密钥管理图中的 ID 和权限策略管理确定哪些文档组的密钥需要更新。

[0089] 本发明通过采用多级保密文档组设置方法，对文件进行分级别加密存储，只要用户有足够的权限都能正常读写文件，不影响合法用户的文件共享，同时也满足了文件的安全性要求。

[0090] 基于本发明的多级保密文档组设置方法，对用户访问权限进行区分管理，配合用户访问权限的控制，可以灵活的设置用户的访问权限，达到对文件分类的细化管理。对进入文件保护区的用户都要进行身份验证，合法的用户才能进入文件保护区，防止越权访问、禁止非法用户对保护文件的任何操作。实现了计算机文件的多级保护管理。

[0091] 同时，本发明还针对密钥泄露的安全隐患，定期或必要时对密钥进行更新，使得密钥使用安全，从而保证文件加密保护的安全。

[0092] 应当理解的是，对本领域普通技术人员来说，可以根据上述说明加以改进或变换，而所有这些改进和变换都应属于本发明所附权利要求的保护范围。

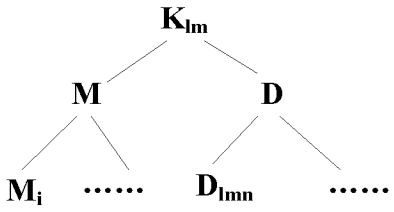

K_{lm}
M
D
M_i
……
D_{lmn}
……

图 1

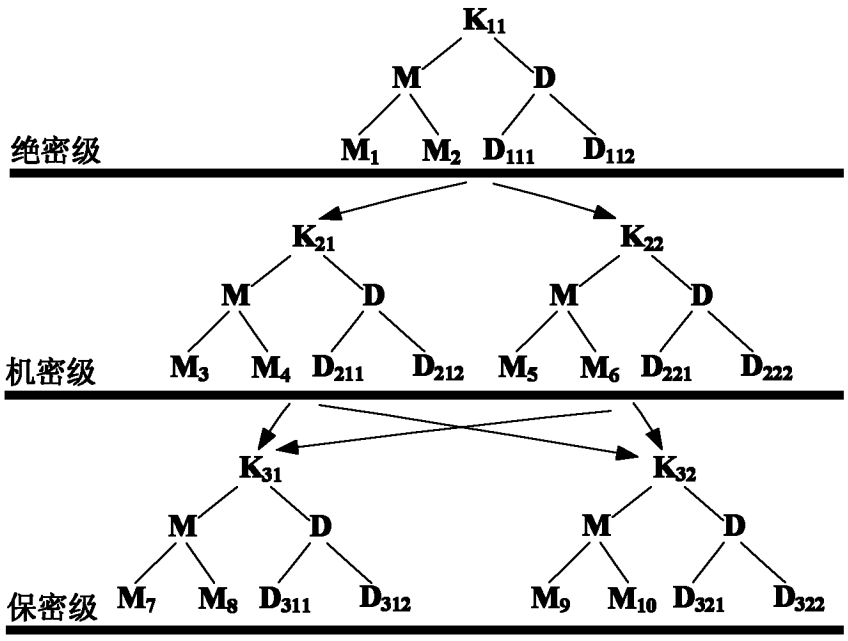

K_{11}
M
D
绝密级
M_1
M_2
D_{111}
D_{112}
K_{21}
K_{22}
M
D
M
D
机密级
M_3
M_4
D_{211}
D_{212}
M_5
M_6
D_{221}
D_{222}
K_{31}
K_{32}
M
D
M
D
保密级
M_7
M_8
D_{311}
D_{312}
M_9
M_{10}
D_{321}
D_{322}

图 2

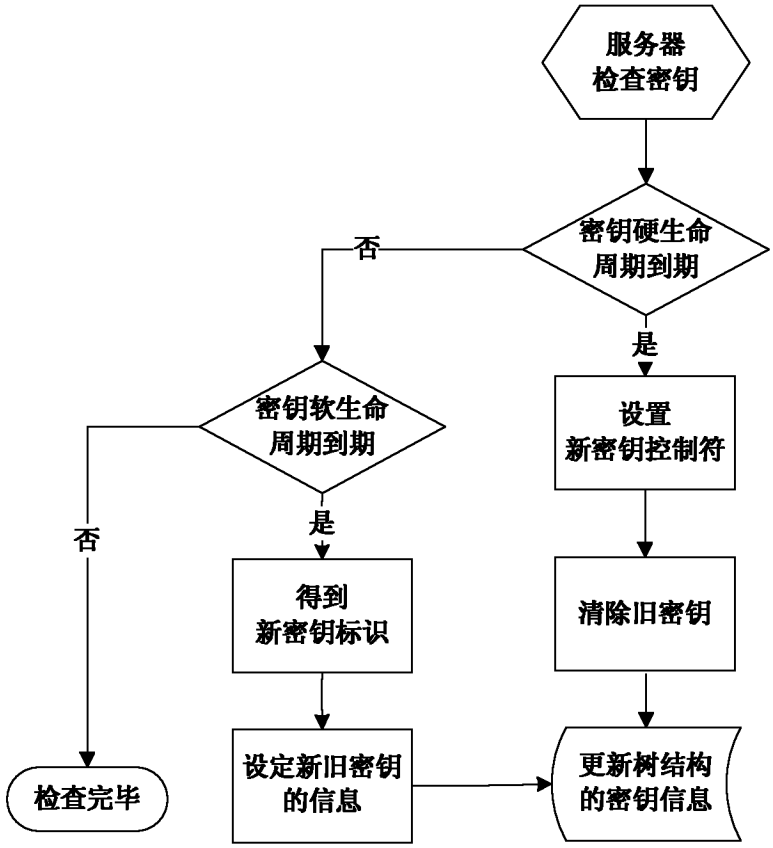

服务器
检查密钥
密钥硬生命
周期到期
否
是
密钥软生命
周期到期
设置
新密钥控制符
否
是
得到
新密钥标识
清除旧密钥
检查完毕
设定新旧密钥
的信息
更新树结构
的密钥信息

图 3

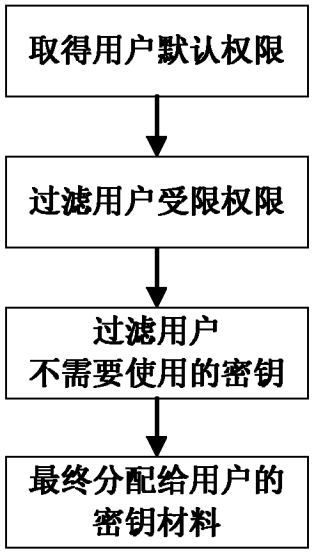

取得用户默认权限
过滤用户受限权限
过滤用户
不需要使用的密钥
最终分配给用户的
密钥材料

图 4

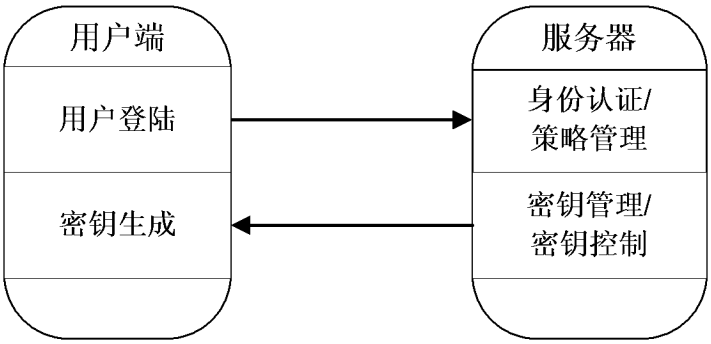

用户端
用户登陆
密钥生成
服务器
身份认证/
策略管理
密钥管理/
密钥控制

图 5

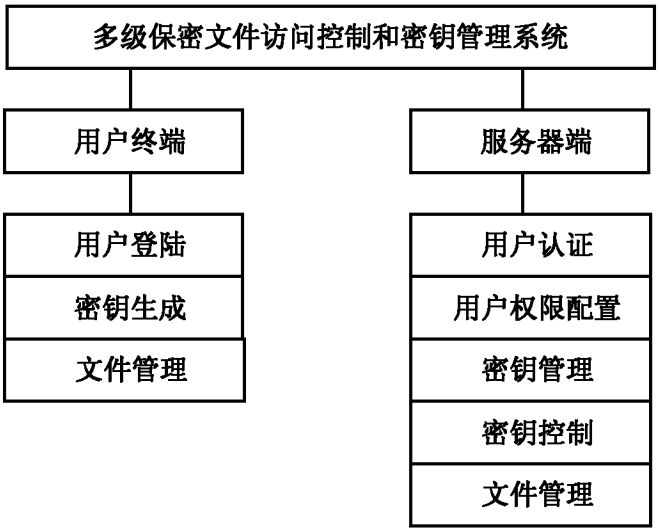

多级保密文件访问控制和密钥管理系统
用户终端
服务器端
用户登陆
密钥生成
文件管理
用户认证
用户权限配置
密钥管理
密钥控制
文件管理

图 6

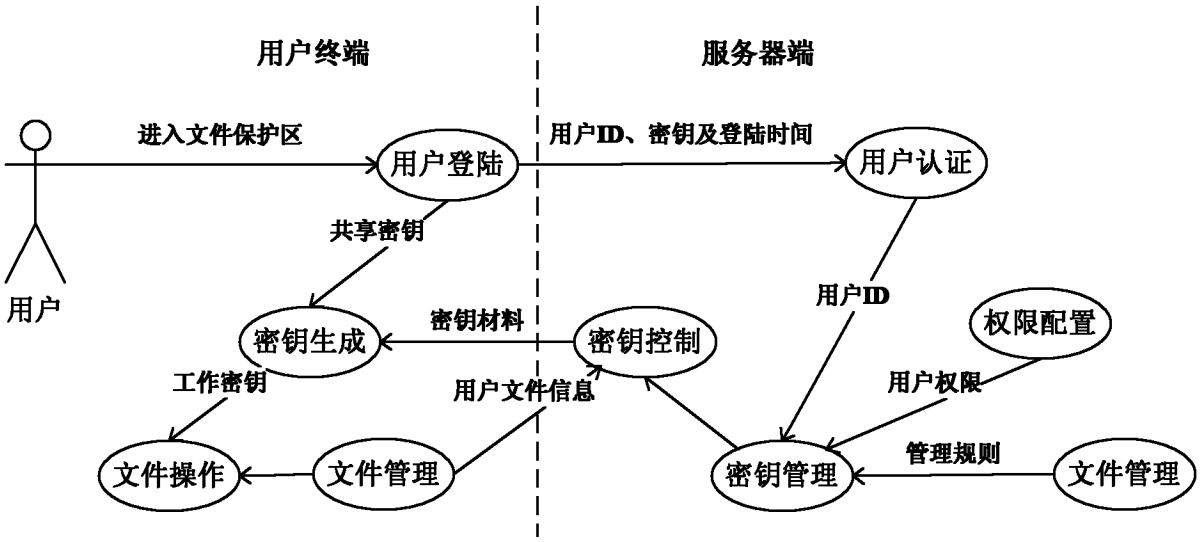

用户终端
服务器端
进入文件保护区
用户登陆
用户ID、密钥及登陆时间
用户认证
用户
共享密钥
用户ID
密钥生成
密钥材料
密钥控制
权限配置
工作密钥
用户文件信息
用户权限
文件操作
文件管理
密钥管理
管理规则
文件管理

图 7