(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105550598 A
(43)申请公布日 2016.05.04

(21)申请号 201510997538.9

(22)申请日 2015.12.25

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 北京奇安信科技有限公司

(72)发明人 胡启宇 潘山 江爱军

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 苏培华

(51)Int.Cl.
G06F 21/62(2013.01)

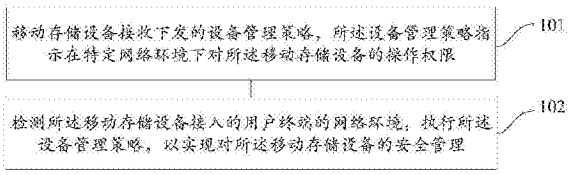
权利要求书1页 说明书11页 附图1页

(54)发明名称

一种移动存储设备的安全管理方法和装置

(57)摘要

本发明提供了一种移动存储设备的安全管理方法和装置，所述方法包括：移动存储设备接收下发的设备管理策略，所述设备管理策略指示在特定网络环境下对所述移动存储设备的操作权限，检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理，避免了病毒侵入和信息泄密等问题，保证了移动存储设备的安全。并且，通过在不同网络环境下配置对应策略，根据移动存储设备接入的用户终端连接的网络环境，对移动存储设备的访问操作进行控制，从而保证了移动存储设备的安全。



CN 105550598 A

1.一种移动存储设备的安全管理方法，其中，包括：

移动存储设备接收下发的设备管理策略，所述设备管理策略指示在特定网络环境下对所述移动存储设备的操作权限；

检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理。

2.根据权利要求1所述的方法，其中，所述移动存储设备接收下发的设备管理策略包括：

接收所述服务端针对所述用户终端的内网连接历史下发的设备管理策略。

3.根据权利要求1所述的方法，其中，所述内网连接历史为曾连接内网，则所述设备管理策略指示在内网环境下对所述移动存储设备仅可执行读操作和写操作，以及在外网环境下对所述移动存储设备仅可执行读操作。

4.根据权利要求1所述的方法，其中，所述执行所述设备管理策略，以实现对所述移动存储设备的安全管理包括：

接收对所述移动存储设备的访问操作，若所述访问操作不符合所述设备管理策略指示的在当前网络环境下设定的操作权限，则对所述访问操作进行拦截。

5.根据权利要求2所述的方法，其中，在所述移动存储设备接收下发的设备管理策略之前，所述方法还包括：

检测所述用户终端的内网连接历史，上传至对应的服务端。

6.根据权利要求5所述的方法，其中，所述检测所述用户终端的内网连接历史包括：

通过访问所述用户终端的连网历史，和/或，检测所述用户终端是否存在内网中的特定文件，来判断所述用户终端是否曾连接内网。

7.根据权利要求4所述的方法，其中，所述接收对所述移动存储设备的访问操作包括：

生成所述移动存储设备对应的文件夹，接收用户针对所述文件夹发起的访问操作；

或，接收某个程序根据所述设备标识发起的访问操作。

8.根据权利要求4所述的方法，其中，在所述接收对所述移动存储设备的访问操作之后，所述方法还包括：

调用预置在所述移动存储设备的第一安全驱动对所述访问操作进行安全验证，并确定验证成功。

9.一种移动存储设备的安全管理装置，其中，包括：

设备管理策略接收模块，用于移动存储设备接收下发的设备管理策略，所述设备管理策略指示在特定网络环境下对所述移动存储设备的操作权限；

设备管理策略执行模块，用于检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理。

10.根据权利要求9所述的装置，其中：

所述设备管理策略接收模块，具体用于接收所述服务端针对所述用户终端的内网连接历史下发的设备管理策略。

一种移动存储设备的安全管理方法和装置

技术领域

[0001] 本发明涉及软件技术领域，特别是涉及一种移动存储设备的安全管理方法，以及一种移动存储设备的安全管理装置。

背景技术

[0002] U盘全称USB闪存盘，是一种使用USB接口与终端设备连接的移动存储设备，具有存储容量大、数据存储速度快、体积小和使用方便等优点，正被越来越多的用户使用。

[0003] 访问U盘时，可以将U盘插入终端设备，通过打开页面显示的U盘盘符访问U盘，将所需数据存储于U盘内或从U盘中下载所需数据。

[0004] 但是，普通U盘对数据的访问操作没有任何访问控制，带来了病毒侵入和信息泄密等问题。

发明内容

[0005] 鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的移动存储设备的安全管理方法和移动存储设备的安全管理装置。

[0006] 依据本发明的一个方面，提供了一种移动存储设备的安全管理方法，包括：

[0007] 移动存储设备接收下发的设备管理策略，所述设备管理策略指示在特定网络环境下对所述移动存储设备的操作权限；

[0008] 检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理。

[0009] 可选地，所述移动存储设备接收下发的设备管理策略包括：

[0010] 接收所述服务端针对所述用户终端的内网连接历史下发的设备管理策略。

[0011] 可选地，所述内网连接历史为曾连接内网，则所述设备管理策略指示在内网环境下对所述移动存储设备仅可执行读操作和写操作，以及在外网环境下对所述移动存储设备仅可执行读操作。

[0012] 可选地，所述执行所述设备管理策略，以实现对所述移动存储设备的安全管理包括：

[0013] 接收对所述移动存储设备的访问操作，若所述访问操作不符合所述设备管理策略指示的在当前网络环境下设定的操作权限，则对所述访问操作进行拦截。

[0014] 可选地，在所述移动存储设备接收下发的设备管理策略之前，所述方法还包括：

[0015] 检测所述用户终端的内网连接历史，上传至对应的服务端。

[0016] 可选地，所述检测所述用户终端的内网连接历史包括：

[0017] 通过访问所述用户终端的连网历史，和/或，检测所述用户终端是否存在内网中的特定文件，来判断所述用户终端是否曾连接内网。

[0018] 可选地，所述接收对所述移动存储设备的访问操作包括：

[0019] 生成所述移动存储设备对应的文件夹，接收用户针对所述文件夹发起的访问操

作；

[0020] 或，接收某个程序根据所述设备标识发起的访问操作。

[0021] 可选地，在所述接收对所述移动存储设备的访问操作之后，所述方法还包括：

[0022] 调用预置在所述移动存储设备的第一安全驱动对所述访问操作进行安全验证，并确定验证成功。

[0023] 本发明还提供了一种移动存储设备的安全管理装置，包括：

[0024] 设备管理策略接收模块，用于移动存储设备接收下发的设备管理策略，所述设备管理策略指示在特定网络环境下对所述移动存储设备的操作权限；

[0025] 设备管理策略执行模块，用于检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理。

[0026] 可选地，所述设备管理策略接收模块，具体用于接收所述服务端针对所述用户终端的内网连接历史下发的设备管理策略。

[0027] 可选地，所述内网连接历史为曾连接内网，则所述设备管理策略指示在内网环境下对所述移动存储设备仅可执行读操作和写操作，以及在外网环境下对所述移动存储设备仅可执行读操作。

[0028] 可选地，所述设备管理策略执行模块，具体用于接收对所述移动存储设备的访问操作，若所述访问操作不符合所述设备管理策略指示的在当前网络环境下设定的操作权限，则对所述访问操作进行拦截。

[0029] 可选地，所述装置还包括：

[0030] 内网连接历史检测模块，用于在所述移动存储设备接收下发的设备管理策略之前，检测所述用户终端的内网连接历史，上传至对应的服务端。

[0031] 可选地，所述内网连接历史检测模块，具体用于通过访问所述用户终端的连网历史，和/或，检测所述用户终端是否存在内网中的特定文件，来判断所述用户终端是否曾连接内网。

[0032] 可选地，所述设备管理策略执行模块包括：

[0033] 第一访问操作接收子模块，用于生成所述移动存储设备对应的文件夹，接收用户针对所述文件夹发起的访问操作；

[0034] 或，第二访问操作接收子模块，用于接收某个程序根据所述设备标识发起的访问操作。

[0035] 可选地，所述装置还包括：

[0036] 安全验证进行模块，用于在所述接收对所述移动存储设备的访问操作之后，调用预置在所述移动存储设备的第一安全驱动对所述访问操作进行安全验证，并确定验证成功。

[0037] 通过本发明实施例，对移动存储设备配置设备管理策略并下发至移动存储设备，指示在特定网络环境下对所述移动存储设备的操作权限，进一步检测所述移动存储设备接入的用户终端的网络环境，并执行所述设备管理策略，根据移动存储设备接入的用户终端连接的网络环境，对移动存储设备的访问操作进行控制，以实现对所述移动存储设备的安全管理，避免了病毒侵入和信息泄密等问题，保证了移动存储设备的安全。

[0038] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，

而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0039] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0040] 图1示出了根据本发明实施例1的移动存储设备的安全管理方法的流程图；

[0041] 图2示出了根据本发明实施例2的移动存储设备的安全管理方法的流程图；

[0042] 图3示出了根据本发明实施例1的移动存储设备的安全管理装置的结构框图；

[0043] 图4示出了根据本发明实施例2的移动存储设备的安全管理装置的结构框图。

具体实施方式

[0044] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0045] 参照图1，示出了根据本发明实施例1的一种移动存储设备的安全管理方法的步骤流程图，具体可以包括如下步骤：

[0046] 步骤101，移动存储设备接收下发的设备管理策略，所述设备管理策略指示在特定网络环境下对所述移动存储设备的操作权限。

[0047] 移动存储设备可以为具有接口(例如USB接口等)的U盘、硬盘或是其他可移动使用并可作为存储介质的设备(例如移动终端等)。用户终端可以为台式电脑、笔记本电脑、手机、PAD等终端设备，所述终端设备安装有供接口(例如USB等)插入的卡槽(例如USB卡槽等)。可以通过将移动存储设备的接口插入用户终端的卡槽，连接移动终端设备和用户终端。

[0048] 网络环境是指将分布在不同地点的多个用户终端物理上互联，依据某种协议互相通信，实现软、硬件及其网络文化共享的系统。由于网络种类不同，网络环境可以分为内网环境或外网环境等，特定网络环境可以为多种网络环境中的一种或多种。

[0049] 设备管理策略可以为对移动存储设备进行安全管理的策略，设备管理策略可以指示在特定网络环境下对所述移动存储设备的操作权限，可以为读操作、写操作、格式化操作和其他访问操作中至少一种。不同的网络环境可以对应不同的设备管理策略，例如当公司内网中的计算机包含大量的机密文件时，为防止局域网内计算机因受外网病毒威胁，设备管理策略可以指示对连接内网计算机的移动存储设备仅可执行读操作，不可执行写操作。

[0050] 具体操作中，设备管理策略可以预先存储至对应的服务器、移动存储设备所连的用户终端或其他适合位置，本发明在此不做限制。服务器或用户终端可以在接收下载设备管理策略的指示后，将存储的设备管理策略下发至移动存储设备。

[0051] 实际操作中，在移动存储设备接入用户终端前，可以根据预设操作打开用户终端安装的访问管理客户端，生成移动存储设备的管理界面。

[0052] 管理界面为信息配置界面，在管理界面中可以展示移动存储设备的设备标识和对应的登录框，登录框内可以展示有多个属性信息以及关联的输入栏，例如设备厂商信息、设备序列单号、单位信息、部门信息、使用人信息、备注信息等属性信息；还可以展示初始口令、口令尝试次数和口令复杂度要求等属性信息，以及针对各个属性信息配置的输入栏。

[0053] 对于首次接入的移动存储设备，可以接收在所述管理界面中对所述移动存储设备的属性设置操作，通过在管理界面中配置属性信息完成对移动存储设备的注册，可以将移动存储设备的注册信息存储于用户终端的登录服务器内以供查看，同时移动存储设备的注册行为可以以日志的形式记录在登录服务器内。

[0054] 对于非首次接入的移动存储设备，可以在生成的管理界面中输入属性信息，生成对所述移动存储设备的登录信息，并判断登录信息和注册信息是否一致，若一致，则判定验证成功，可以进一步接收用户对移动存储设备的访问操作；若不一致，则判定验证失败，禁止接收用户对移动存储设备的访问操作，实现对移动存储设备的安全的初步保护。

[0055] 步骤102，检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理。

[0056] 移动存储设备接收下发的设备管理策略后，开始检测移动存储设备接入的用户终端的网络环境，依据设备管理策略指示的特定网络环境下对所述移动存储设备的操作权限，对所述移动存储设备的访问操作进行监控，以实现对所述移动存储设备的安全管理。

[0057] 依据本发明实施例，对移动存储设备配置设备管理策略并下发至移动存储设备，指示在特定网络环境下对所述移动存储设备的操作权限，进一步检测所述移动存储设备接入的用户终端的网络环境，并执行所述设备管理策略，根据移动存储设备接入的用户终端连接的网络环境，对移动存储设备的访问操作进行控制，以实现对所述移动存储设备的安全管理，避免了病毒侵入和信息泄密等问题，保证了移动存储设备的安全。

[0058] 参照图2，示出了根据本发明实施例2的移动存储设备的安全管理方法的流程图，具体可以包括如下步骤：

[0059] 步骤201，检测所述用户终端的内网连接历史，上传至对应的服务端。

[0060] 内网连接历史指示用户终端对内网的历史连接行为，例如曾连接内网或未曾连接内网。可以通过检测用户终端是否发生内网连接行为，待检测结束后，将检测结果上传至对应的服务端，以供服务器根据接收的检测结果配置相应的设备管理策略。

[0061] 内网用户终端可以通过连接内网下载内网中的文件，因此可以遍历用户终端的各个文件，通过检测用户终端是否存在内网中的特定文件，来判断用户终端是否曾连接内网。具体地，若检测到用户终端存在内网中的特定文件，则判定用户终端曾连接内网。具体可以通过遍历用户终端的各个文件，并逐个检测文件，或是在内网相关文件的关联保存位置获取并检测文件。具体判断文件是否是内网关联的特定文件时，可以根据内网关键词、内网标识、文件类型、文件下载路径等各种信息进行识别，还可以是其他任意识别方式或是预置的识别规则，本发明对此并不做限制。

[0062] 用户终端历史访问过多个网络，因此还可以通过查找网络访问历史判断用户终端是否曾连接内网。例如通过查找操作系统相关位置记录的网络连接历史，或是通过第三方程序记录的网络连接历史，或是其他任意可获取网络连接历史的位置进行获取。其中，判断是否曾连接内网，具体可以通过内网的内网标识或是内网的其他相关信息进行识别。

[0063] 检测用户终端的内网连接历史的方法可以为上述任意一种方法或多种方法的组合，本发明在此不做限制。

[0064] 步骤202，接收服务端针对所述用户终端的内网连接历史下发的设备管理策略。

[0065] 服务端可以是用户终端或移动存储设备对应的网络端。服务端接收到对用户终端的内网连接历史的检测结果后，可以对不同的检测结果配置不同的设备管理策略。待设备管理策略配置完成后，服务端可以将配置的策略下发至用户终端，作为对移动存储设备进行安全管理的依据。

[0066] 具体操作中，当内网连接历史为曾连接内网时，说明用户终端曾连接过内网，为了保证移动存储设备的安全，避免移动存储设备受到外网病毒的威胁，设备管理策略可以指示在内网环境下对移动存储设备仅可执行读操作和写操作，以及在外网环境下对移动存储设备仅可执行读操作，即不允许从外网中下载数据。

[0067] 实际操作中，移动存储设备可以采用NTFS新技术文件系统，相比于常用的FAT32文件系统，NTFS新技术文件系统内存更大、可以在多个硬盘上存储文件，同时NTFS能够提供各种FAT版本所不具备的性能、安全性、可靠性与先进特性的高级文件系统。例如，NTFS通过标准事务日志功能与恢复技术确保卷的一致性。如果系统出现故障，NTFS能够使用日志文件与检查点信息来恢复文件系统的一致性。在Windows 2000和Windows XP中，NTFS还能提供诸如文件与文件夹权限、加密、磁盘配额以及压缩之类的高级特性。

[0068] 步骤203，检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理。

[0069] 具体操作中，可以接收对所述移动存储设备的访问操作，并判断所述访问操作是否符合所述设备管理策略指示的在当前网络环境下设定的操作权限，若是，则允许所述访问操作访问移动存储设备；若否，则对所述访问操作进行拦截，避免移动存储设备受到威胁，实现对所述移动存储设备的安全管理。

[0070] 优选地，可以在检测所述移动存储设备接入的用户终端的网络环境后，生成所述移动存储设备对应的文件夹，接收用户针对所述文件夹发起的访问操作。实际操作中，可以在弹出的页面中展示生成的文件夹，用户可以针对展示的文件夹发起访问操作；也可以在弹出的页面中展示文件夹所在路径以供用户查找，如路径“我的电脑/可移动存储设备I”，用户依据所述路径查找文件夹并对找到的文件夹发起访问操作。

[0071] 还可以在检测所述移动存储设备接入的用户终端的网络环境后，接收某个程序根据设备标识发起的访问操作，例如由其他驱动程序或非驱动程序通过逆向操作发现隐藏的设备标识，并对所述设备标识发起访问操作。其中，备标识为对接入用户终端的移动存储设备配置的设备盘符，可以是文字、数字、字符和其他标识中至少一种，例如“可移动存储设备I”。访问操作可以为读操作、写操作或格式化操作等。

[0072] 具体操作中，为了防止通过识别设备标识及相关操作直接访问移动存储设备，保护移动存储设备的安全，可以取消所述设备标识在所接入的用户终端的操作系统关联位置的展示，例如取消设备标识在“我的电脑”中的展示。由于设备标识不展示，无法通过识别设备标识及相关操作直接访问移动存储设备，而是需要通过完成后续其他操作才能访问移动存储设备，从而实现了对移动存储设备的访问的控制，保证了移动存储设备的安全。

[0073] 具体地，可以通过修改所述用户终端的操作系统的注册表的关联设置项为不展示

接入的移动存储设备，不展示设备标识，例如可以在注册表中查找路径HKEY_CURRENT_USER→Software→Microsoft→Windows→CurrentVersion→Ploicies→Explorer，找到“NoDrives”的选项后将其删除，从而隐藏设备标识。

[0074] 需要说明的是，虽然移动存储设备的设备标识不展示，但是其他程序还是可以通过例如逆向操作等操作方式发现隐藏的设备标识。

[0075] 优选地，在接收对所述移动存储设备的访问操作之后，可以调用预置在所述移动存储设备的第一安全驱动对所述访问操作进行安全验证，判断访问操作是否会对用户终端产生威胁，只有在验证访问操作为安全操作后，才执行设备管理策略。

[0076] 移动存储设备内预置有第一安全驱动的安装文件，安装后的第一安全驱动用于对访问操作进行安全验证。具体地，在移动存储设备接入用户终端后，用户终端的操作系统检测用户终端内是否需要安装第一安全驱动，在检测到所述用户终端内需要安装第一安全驱动时，指示用户终端运行移动存储设备内存储的第一安全驱动的安装文件，以实现第一安全驱动可用。

[0077] 第一驱动程序用于验证发起访问操作的程序是否安全，进而验证访问操作是否为安全操作。

[0078] 在移动存储设备的终端服务器中预先设置有第一安全程序名单，用于对发起操作访问的程序进行验证。具体地，第一程序名单可以是白名单，默认白名单中的程序为安全程序，若发起访问操作的程序命中白名单，则说明所述程序为安全程序；也可以是黑名单，默认黑名单中的程序为危险程序，若发起访问操作的程序命中黑名单，则说明所述程序为危险程序。还可以是其他验证方法，本发明在此不做限制。

[0079] 验证访问操作时，若所述访问操作由用户通过文件夹触发，则验证所述访问操作为安全操作，无需调用第一安全驱动对其进行安全验证；若所述访问操作由某个程序根据所述设备标识发起，则验证所述访问操作是否为安全操作，具体地，可以调用第一安全驱动验证发起访问操作的应用程序或驱动是否属于第一安全程序名单，此时第一安全程序名单为白名单，若属于，则判定所述访问操作为安全操作，可以进一步根据所述访问操作访问所述移动存储设备；如果不属于，则判定所述访问操作为危险操作，阻止对移动存储设备进行访问操作。

[0080] 移动存储设备内置有主控芯片，主控芯片设置有一个或多个访问控制接口，可以通过访问所述设备标识对应的移动存储设备的访问控制接口，与其他设备进行数据传输，将所述访问操作发送至所述移动存储设备；进一步主控芯片可以依据访问操作对数据进行处理，通过访问控制接口将处理后的数据反馈至与其连接的用户终端。

[0081] 在实际操作中，可以将所述移动存储设备的设备标识与所述第一安全驱动进行关联，可以在第一安全驱动对访问操作验证成功后，对关联的设备标识对应的移动存储设备进行访问操作。

[0082] 进一步，在调用预置在所述移动存储设备的第一安全驱动对所述访问操作进行安全验证之前，还可以调用预置在所述移动存储设备的第二驱动程序验证所述访问操作是否为安全操作。

[0083] 第二驱动程序用于验证发起访问操作的程序是否安全，进而验证访问操作是否为安全操作。

[0084] 在移动存储设备的终端服务器中预先设置有第二安全程序名单，用于对发起操作访问的程序进行验证。具体地，第二程序名单可以是白名单，默认白名单中的程序为安全程序，若发起访问操作的程序命中白名单，则说明所述程序为安全程序；也可以是黑名单，默认黑名单中的程序为危险程序，若发起访问操作的程序命中黑名单，则说明所述程序为危险程序。还可以是其他验证方法，本发明在此不做限制。

[0085] 当访问操作由用户终端内的某个程序触发时，可以在接收对所述移动存储设备的访问操作后，从终端服务器中获取第二安全程序名单，并且判断发起所述访问操作的程序是否属于第二安全程序名单，此时第二访问名单为白名单，若属于，则判定发起所述访问操作的程序为安全程序，所述访问操作为安全操作。其中，第一安全驱动的第一安全程序名单不同于第二安全驱动的第二安全程序名单，例如程序名称不同、程序分类不同、程序来源不同(例如外网下载、用户终端原始程序等)、程序大小不同和其他不同，本发明在此不做限制。使用两个安全驱动分别对访问操作进行验证，进一步保证了移动存储设备的安全。

[0086] 在具体操作中，触发访问请求的方式可以为用户针对文件夹发起的、某个程序根据设备标识发起的或其他适用方式。若所述访问操作由用户通过文件夹触发，则验证所述访问操作为安全操作，即不调用第二安全驱动对所述访问操作进行安全验证；若所述访问操作由某个程序根据所述设备标识发起，则验证所述访问操作是否为安全操作，例如判断发起所述访问操作的程序是否在第二安全程序名单中，若在，则验证成功，之后再调用第一安全驱动验证所述访问操作是否安全。

[0087] 依据本发明实施例，对移动存储设备配置设备管理策略并下发至移动存储设备，指示在特定网络环境下对所述移动存储设备的操作权限，进一步检测所述移动存储设备接入的用户终端的网络环境，并执行所述设备管理策略，根据移动存储设备接入的用户终端连接的网络环境，对移动存储设备的访问操作进行控制，以实现对所述移动存储设备的安全管理，避免了病毒侵入和信息泄密等问题，保证了移动存储设备的安全。

[0088] 参照图3，示出了根据本发明实施例1的移动存储设备的安全管理装置的结构框图，具体可以包括如下模块：

[0089] 设备管理策略接收模块301，用于移动存储设备接收下发的设备管理策略，所述设备管理策略指示在特定网络环境下对所述移动存储设备的操作权限。

[0090] 设备管理策略执行模块302，用于检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理。

[0091] 依据本发明实施例，对移动存储设备配置设备管理策略并下发至移动存储设备，指示在特定网络环境下对所述移动存储设备的操作权限，进一步检测所述移动存储设备接入的用户终端的网络环境，并执行所述设备管理策略，根据移动存储设备接入的用户终端连接的网络环境，对移动存储设备的访问操作进行控制，以实现对所述移动存储设备的安全管理，避免了病毒侵入和信息泄密等问题，保证了移动存储设备的安全。

[0092] 参照图4，示出了根据本发明实施例2的移动存储设备的安全管理装置的结构框图，具体可以包括如下模块：

[0093] 内网连接历史检测模块401，用于在所述移动存储设备接收下发的设备管理策略之前，检测所述用户终端的内网连接历史，上传至对应的服务端。

[0094] 设备管理策略接收模块402，用于移动存储设备接收下发的设备管理策略，所述设

备管理策略指示在特定网络环境下对所述移动存储设备的操作权限。

[0095] 设备管理策略执行模块403，用于检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理。

[0096] 本发明实施例中，优选地，所述设备管理策略接收模块，具体用于接收所述服务端针对所述用户终端的内网连接历史下发的设备管理策略。

[0097] 本发明实施例中，优选地，所述内网连接历史为曾连接内网，则所述设备管理策略指示在内网环境下对所述移动存储设备仅可执行读操作和写操作，以及在外网环境下对所述移动存储设备仅可执行读操作。

[0098] 本发明实施例中，优选地，所述设备管理策略执行模块，具体用于接收对所述移动存储设备的访问操作，若所述访问操作不符合所述设备管理策略指示的在当前网络环境下设定的操作权限，则对所述访问操作进行拦截。

[0099] 本发明实施例中，优选地，所述装置还包括：

[0100] 内网连接历史检测模块，用于在所述移动存储设备接收下发的设备管理策略之前，检测所述用户终端的内网连接历史，上传至对应的服务端。

[0101] 本发明实施例中，优选地，所述内网连接历史检测模块，具体用于通过访问所述用户终端的连网历史，和/或，检测所述用户终端是否存在内网中的特定文件，来判断所述用户终端是否曾连接内网。

[0102] 本发明实施例中，优选地，所述设备管理策略执行模块包括：

[0103] 第一访问操作接收子模块，用于生成所述移动存储设备对应的文件夹，接收用户针对所述文件夹发起的访问操作；

[0104] 或，第二访问操作接收子模块，用于接收某个程序根据所述设备标识发起的访问操作。

[0105] 本发明实施例中，优选地，所述装置还包括：

[0106] 安全验证进行模块，用于在所述接收对所述移动存储设备的访问操作之后，调用预置在所述移动存储设备的第一安全驱动对所述访问操作进行安全验证，并确定验证成功。

[0107] 依据本发明实施例，对移动存储设备配置设备管理策略并下发至移动存储设备，指示在特定网络环境下对所述移动存储设备的操作权限，进一步检测所述移动存储设备接入的用户终端的网络环境，并执行所述设备管理策略，根据移动存储设备接入的用户终端连接的网络环境，对移动存储设备的访问操作进行控制，以实现对所述移动存储设备的安全管理，避免了病毒侵入和信息泄密等问题，保证了移动存储设备的安全。

[0108] 对于上述基于地理位置的来电管理装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0109] 本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

[0110] 本领域技术人员易于想到的是：上述各个实施例的任意组合应用都是可行的，故上述各个实施例之间的任意组合都是本发明的实施方案，但是由于篇幅限制，本说明书在此就不一一详述了。

[0111] 在此提供的基于地理位置的来电管理方案不与任何特定计算机、虚拟系统或者其

它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造具有本发明方案的系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0112] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0113] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0114] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0115] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0116] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例的移动存储设备的安全管理方案中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如，计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0117] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实

现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0118] 本发明公开了A1、一种移动存储设备的安全管理方法，其中，包括：

[0119] 移动存储设备接收下发的设备管理策略，所述设备管理策略指示在特定网络环境下对所述移动存储设备的操作权限；

[0120] 检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理。

[0121] A2、根据A1所述的方法，其中，所述移动存储设备接收下发的设备管理策略包括：

[0122] 接收所述服务端针对所述用户终端的内网连接历史下发的设备管理策略。

[0123] A3、根据A1所述的方法，其中，所述内网连接历史为曾连接内网，则所述设备管理策略指示在内网环境下对所述移动存储设备仅可执行读操作和写操作，以及在外网环境下对所述移动存储设备仅可执行读操作。

[0124] A4、根据A1所述的方法，其中，所述执行所述设备管理策略，以实现对所述移动存储设备的安全管理包括：

[0125] 接收对所述移动存储设备的访问操作，若所述访问操作不符合所述设备管理策略指示的在当前网络环境下设定的操作权限，则对所述访问操作进行拦截。

[0126] A5、根据A2所述的方法，其中，在所述移动存储设备接收下发的设备管理策略之前，所述方法还包括：

[0127] 检测所述用户终端的内网连接历史，上传至对应的服务端。

[0128] A6、根据A5所述的方法，其中，所述检测所述用户终端的内网连接历史包括：

[0129] 通过访问所述用户终端的连网历史，和/或，检测所述用户终端是否存在内网中的特定文件，来判断所述用户终端是否曾连接内网。

[0130] A7、根据A4所述的方法，其中，所述接收对所述移动存储设备的访问操作包括：

[0131] 生成所述移动存储设备对应的文件夹，接收用户针对所述文件夹发起的访问操作；

[0132] 或，接收某个程序根据所述设备标识发起的访问操作。

[0133] A8、根据A4所述的方法，其中，在所述接收对所述移动存储设备的访问操作之后，所述方法还包括：

[0134] 调用预置在所述移动存储设备的第一安全驱动对所述访问操作进行安全验证，并确定验证成功。

[0135] 本发明还公开了B9、一种移动存储设备的安全管理装置，其中，包括：

[0136] 设备管理策略接收模块，用于移动存储设备接收下发的设备管理策略，所述设备管理策略指示在特定网络环境下对所述移动存储设备的操作权限；

[0137] 设备管理策略执行模块，用于检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理。

[0138] B10、根据B9所述的装置，其中：

[0139] 所述设备管理策略接收模块，具体用于接收所述服务端针对所述用户终端的内网连接历史下发的设备管理策略。

[0140] B11、根据B9所述的装置，其中，所述内网连接历史为曾连接内网，则所述设备管理策略指示在内网环境下对所述移动存储设备仅可执行读操作和写操作，以及在外网环境下对所述移动存储设备仅可执行读操作。

[0141] B12、根据B9所述的装置，其中：

[0142] 所述设备管理策略执行模块，具体用于接收对所述移动存储设备的访问操作，若所述访问操作不符合所述设备管理策略指示的在当前网络环境下设定的操作权限，则对所述访问操作进行拦截。

[0143] B13、根据B10所述的装置，其中，所述装置还包括：

[0144] 内网连接历史检测模块，用于在所述移动存储设备接收下发的设备管理策略之前，检测所述用户终端的内网连接历史，上传至对应的服务端。

[0145] B14、根据B13所述的装置，其中：

[0146] 所述内网连接历史检测模块，具体用于通过访问所述用户终端的连网历史，和/或，检测所述用户终端是否存在内网中的特定文件，来判断所述用户终端是否曾连接内网。

[0147] B15、根据B12所述的装置，其中，所述设备管理策略执行模块包括：

[0148] 第一访问操作接收子模块，用于生成所述移动存储设备对应的文件夹，接收用户针对所述文件夹发起的访问操作；

[0149] 或，第二访问操作接收子模块，用于接收某个程序根据所述设备标识发起的访问操作。

[0150] B16、根据B12所述的装置，其中，所述装置还包括：

[0151] 安全验证进行模块，用于在所述接收对所述移动存储设备的访问操作之后，调用预置在所述移动存储设备的第一安全驱动对所述访问操作进行安全验证，并确定验证成功。

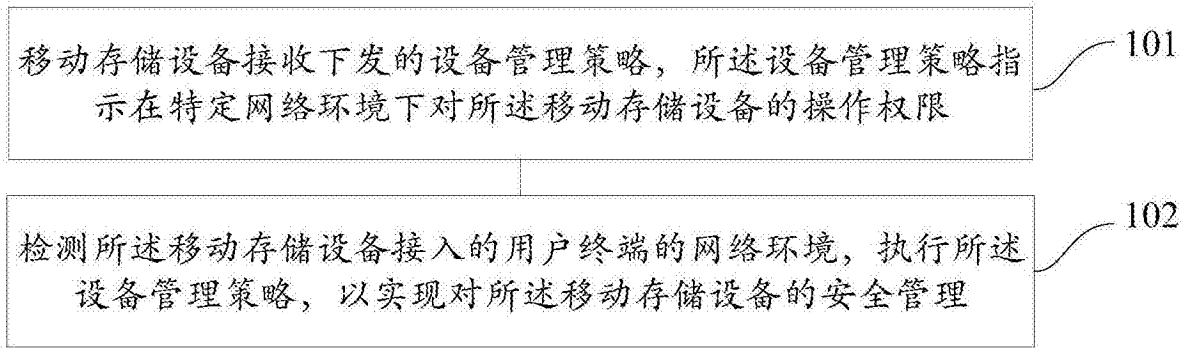

移动存储设备接收下发的设备管理策略，所述设备管理策略指示在特定网络环境下对所述移动存储设备的操作权限
101
检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理
102

图1

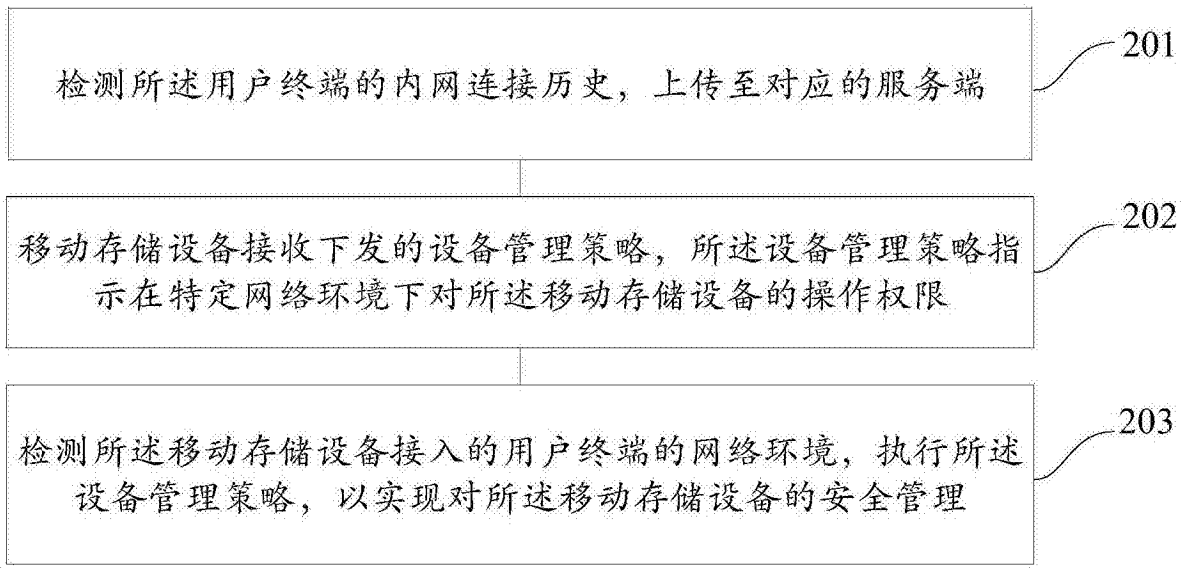

检测所述用户终端的内网连接历史，上传至对应的服务端
201
移动存储设备接收下发的设备管理策略，所述设备管理策略指示在特定网络环境下对所述移动存储设备的操作权限
202
检测所述移动存储设备接入的用户终端的网络环境，执行所述设备管理策略，以实现对所述移动存储设备的安全管理
203

图2

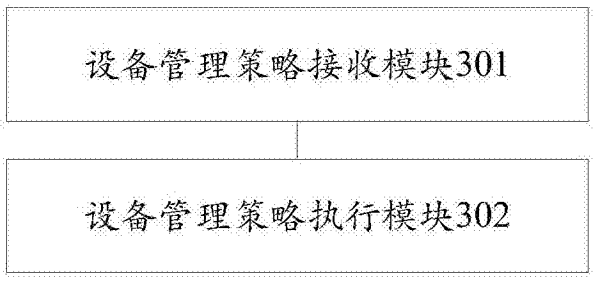

设备管理策略接收模块301
设备管理策略执行模块302

图3


内网连接历史检测模块401
设备管理策略接收模块402
设备管理策略执行模块403

图4