(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 102622311 A
(43)申请公布日 2012.08.01

(21)申请号 201110451568.1

(22)申请日 2011.12.29

(71)申请人 北京神州绿盟信息安全科技股份有限公司
地址 100089 北京市海淀区北洼路 4 号益泰大厦 3 层

(72)发明人 刘洋 于洋

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 刘芳

(51)Int.Cl.
G06F 12/14(2006.01)

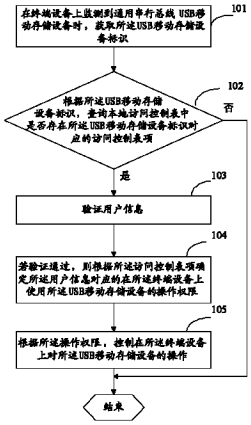
权利要求书 3 页 说明书 7 页 附图 3 页

(54)发明名称

USB移动存储设备访问控制方法、装置及系统

(57)摘要

本发明实施例公开了一种USB移动存储设备访问控制方法、装置及系统，其中，该方法包括：在终端设备上监测到USB移动存储设备时，获取所述USB移动存储设备标识；根据所述USB移动存储设备标识，查询本地访问控制表中是否存在所述USB移动存储设备标识对应的访问控制表项，若存在，则对用户信息进行验证；若验证通过，则根据所述访问控制表项确定所述用户信息对应的在所述终端设备上使用所述USB移动存储设备的操作权限；根据所述操作权限，控制在所述终端设备上对所述USB移动存储设备的操作。因此，本发明实施例能解决现有技术中对移动储存设备的监控存在通用性较差的问题。



CN 102622311 A

1. 一种 USB 移动存储设备访问控制方法，其特征在于，包括：

在终端设备上监测到通用串行总线 USB 移动存储设备时，获取所述 USB 移动存储设备标识；

根据所述 USB 移动存储设备标识，查询本地访问控制表中是否存在所述 USB 移动存储设备标识对应的访问控制表项，若存在，则对用户信息进行验证；

若验证通过，则根据所述访问控制表项确定所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限；

根据所述操作权限，控制在所述终端设备上对所述 USB 移动存储设备的操作。

2. 根据权利要求 1 所述的方法，其特征在于，所述查询本地访问控制表中是否存在所述 USB 移动存储设备标识对应的访问控制表项之后还包括：

若本地访问控制表中不存在所述 USB 移动存储设备标识对应的访问控制表项，则根据用户指令向注册服务器发送注册信息，所述注册信息包括所述用户信息、所述 USB 移动存储设备标识和所述终端设备标识；

接收所述注册服务器发送的加密后的所述 USB 移动存储设备标识对应的访问控制表项，所述 USB 移动存储设备标识对应的访问控制表项包括所述用户信息、所述 USB 移动存储设备标识、所述终端设备标识和所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限；

将加密后的所述 USB 移动存储设备标识对应的访问控制表项存储到本地访问控制表中。

3. 根据权利要求 2 所述的方法，其特征在于，所述查询本地访问控制表中是否存在所述 USB 移动存储设备标识对应的访问控制表项之前还包括：

对本地访问控制表中的访问控制表项进行解密。

4. 根据权利要求 1-3 中任一项所述的方法，其特征在于，所述操作权限包括：读写操作、只读操作、禁止操作；

根据所述操作权限，控制在所述终端设备上对所述 USB 移动存储设备的操作具体包括：

若所述操作权限为读写操作，则允许在所述终端设备上对所述 USB 移动存储设备进行读操作和写操作；

若所述操作权限为只读操作，则允许在所述终端设备上对所述 USB 移动存储设备进行读操作；

若所述操作权限为禁止操作，则不允许在所述终端设备上对所述 USB 移动存储设备进行任何操作。

5. 根据权利要求 4 所述的方法，其特征在于，若所述操作权限为读写操作，还包括：

当监测到在所述终端设备上对所述 USB 移动存储设备进行写操作时，将所述终端设备上的文件加密后写入所述 USB 移动存储设备中；

当监测到在所述终端设备上对所述 USB 移动存储设备进行读操作时，将所述 USB 移动存储设备中的文件解密后读取到所述终端设备中。

6. 根据权利要求 2 或 3 所述的方法，其特征在于，所述根据用户指令向注册服务器发送注册信息之后还包括：

所述注册服务器接收所述注册信息；

根据所述用户信息、所述 USB 移动存储设备标识和所述终端设备标识，分配所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限；

生成所述 USB 移动存储设备标识对应访问控制表项，并进行加密后返回。

7. 一种 USB 移动存储设备访问控制装置，其特征在于，包括：

监测模块，用于在终端设备上监测到通用串行总线 USB 移动存储设备时，获取所述 USB 移动存储设备标识；

查询模块，用于根据所述 USB 移动存储设备标识，查询本地访问控制表中是否存在所述 USB 移动存储设备标识对应的访问控制表项；

验证模块，用于若本地访问控制表中存在所述 USB 移动存储设备标识对应的访问控制表项，则对用户信息进行验证；

确定模块，用于若验证通过，则根据所述访问控制表项确定所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限；

控制模块，用于根据所述操作权限，控制在所述终端设备上对所述 USB 移动存储设备的操作。

8. 根据权利要求 7 所述的装置，其特征在于，所述装置还包括：

发送模块，用于若本地访问控制表中不存在所述 USB 移动存储设备标识对应的访问控制表项，则根据用户指令向注册服务器发送注册信息，所述注册信息包括所述用户信息、所述 USB 移动存储设备标识和所述终端设备标识；

接收模块，用于接收所述注册服务器发送的加密后的所述 USB 移动存储设备标识对应的访问控制表项，所述 USB 移动存储设备标识对应的访问控制表项包括所述用户信息、所述 USB 移动存储设备标识、所述终端设备标识和所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限；

储存模块，用于将加密后的所述 USB 移动存储设备标识对应的访问控制表项存储到本地访问控制表中。

9. 根据权利要求 8 所述的装置，其特征在于，所述查询模块还用于，在查询本地访问控制表中是否存在所述 USB 移动存储设备标识对应的访问控制表项之前，对本地访问控制表中的访问控制表项进行解密。

10. 根据权利要求 7-9 中任一项所述的装置，其特征在于，所述操作权限包括：读写操作、只读操作、禁止操作；

所述控制模块包括：

第一控制单元，用于若所述操作权限为读写操作，则允许在所述终端设备上对所述 USB 移动存储设备进行读操作和写操作；

第二控制单元，用于若所述操作权限为只读操作，则允许在所述终端设备上对所述 USB 移动存储设备进行读操作；

第三控制单元，用于若所述操作权限为禁止操作，则不允许在所述终端设备上对所述 USB 移动存储设备进行任何操作。

11. 根据权利要求 10 所述的装置，其特征在于，所述第一控制单元包括：

第一控制子单元，用于当监测到在所述终端设备上对所述 USB 移动存储设备进行写操

作时，将所述终端设备上的文件加密后写入所述 USB 移动存储设备中；

第二控制子单元，用于当监测到在所述终端设备上对所述 USB 移动存储设备进行读操作时，将所述 USB 移动存储设备中的文件解密后读取到所述终端设备中。

12. 一种终端设备，其特征在于，包括如权利要求 7-11 中任一项所述的 USB 移动存储设备访问控制装置。

13. 一种 USB 移动存储设备访问控制系统，其特征在于，包括：如权利要求 12 所述的终端设备和注册服务器；

所述注册服务器，用于接收所述终端设备中 USB 移动存储设备访问控制装置发送的注册信息，所述注册信息包括用户信息、USB 移动存储设备标识和终端设备标识；根据所述用户信息、所述 USB 移动存储设备标识和所述终端设备标识，分配所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限；生成所述 USB 移动存储设备标识对应的访问控制表项，并进行加密后返回给所述 USB 移动存储设备访问控制装置。

USB 移动存储设备访问控制方法、装置及系统

技术领域

[0001] 本发明涉及领域信息安全领域，尤其涉及一种 USB 移动存储设备访问控制方法、装置及系统。

背景技术

[0002] 通用串行总线 (Universal Serial Bus，简称USB) 移动存储设备的广泛使用，使信息传递更加方便，若不能有效控制其使用，会使内网信息安全存在严重的问题。

[0003] 为防止内网终端上的涉密文件、内部文档或私人隐私被人使用 USB 移动存储设备带走，以及防止外部带有病毒的 USB 移动存储设备插入内网终端使用而导致内网计算机中毒，现有的一种 USB 移动存储设备管理方案是禁止 USB 移动存储设备在终端上使用。但是，这种方案不能对 USB 移动存储设备的访问进行灵活控制，例如，某些确实需要使用 USB 移动存储设备携带计算机文件的场景无法得到满足。

[0004] 现有的另一种方案使用 Windows 操作系统对 USB 移动存储设备的进行写保护机制或者对 Windows 应用层的 API 进行挂接，从而达到实现对 USBUSB 移动存储设备的读写操作进行监控，并且能够阻断相关的读写操作。但是，这种方案的通用性较差，不同平台不同软件可能使用不同的读写方式对 USB 移动存储设备进行修改，应用层的保护机制很难对所有的读写方式进行监控，通用性较差。

发明内容

[0005] 本发明实施例提供了一种 USB 移动存储设备访问控制方法、装置及系统，用以解决现有技术中对移动储存设备的监控存在通用性较差的问题。

[0006] 本发明实施例提供一种 USB 移动存储设备访问控制方法，包括 ：

[0007] 在终端设备上监测到通用串行总线 USB 移动存储设备时，获取所述 USB 移动存储设备标识 ；

[0008] 根据所述 USB 移动存储设备标识，查询本地访问控制表中是否存在所述 USB 移动存储设备标识对应的访问控制表项，若存在，则对用户信息进行验证 ；

[0009] 若验证通过，则根据所述访问控制表项确定所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限 ；

[0010] 根据所述操作权限，控制在所述终端设备上对所述 USB 移动存储设备的操作。

[0011] 本发明实施例还提供了一种 USB 移动存储设备访问控制装置，包括 ：

[0012] 监测模块，用于在终端设备上监测到通用串行总线 USB 移动存储设备时，获取所述 USB 移动存储设备标识 ；

[0013] 查询模块，用于根据所述 USB 移动存储设备标识，查询本地访问控制表中是否存在所述 USB 移动存储设备标识对应的访问控制表项 ；

[0014] 验证模块，用于若本地访问控制表中存在所述 USB 移动存储设备标识对应的访问控制表项，则对用户信息进行验证 ；

[0015] 确定模块，用于若验证通过，则根据所述访问控制表项确定所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限；

[0016] 控制模块，用于根据所述操作权限，控制在所述终端设备上对所述 USB 移动存储设备的操作。

[0017] 本发明实施例还提供了一种终端设备，包括上述 USB 移动存储设备访问控制装置。

[0018] 本发明实施例还提供了一种 USB 移动存储设备访问控制系统，包括：上述终端设备和注册服务器；

[0019] 所述注册服务器，用于接收所述终端设备中 USB 移动存储设备访问控制装置发送的注册信息，所述注册信息包括用户信息、USB 移动存储设备标识和终端设备标识；根据所述用户信息、所述 USB 移动存储设备标识和所述终端设备标识，分配所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限；生成所述 USB 移动存储设备标识对应的访问控制表项，并进行加密后返回给所述 USB 移动存储设备访问控制装置。

[0020] 本发明实施例通过在终端设备上监测到 USB 移动存储设备时，获取所述 USB 移动存储设备标识和用户信息，查询本地访问控制表确定所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限，根据所述操作权限控制在所述终端设备上对所述 USB 移动存储设备的操作，可以基于用户信息、终端设备、USB 移动存储设备设置不同的操作权限，控制用户在终端设备上对 USB 移动存储设备的操作，解决现有技术中对移动储存设备的监控存通用性较差的问题，能够实时灵活的控制 USB 移动存储设备的操作权限，有效保证内网终端设备上文件的安全性。

附图说明

[0021] 图 1 为本发明实施例一提供的 USB 移动存储设备访问控制方法的流程示意图；

[0022] 图 2 为本发明实施例二提供的 USB 移动存储设备访问控制方法的流程示意图；

[0023] 图 3 为本发明实施例三提供的 USB 移动存储设备访问控制装置的结构示意图；

[0024] 图 4 为本发明实施例四提供的 USB 移动存储设备访问控制装置的结构示意图；

[0025] 图 5 为本发明实施例六提供的 USB 移动存储设备访问控制系统的结构示意图。

具体实施方式

[0026] 实施例一

[0027] 图 1 为本发明实施例一提供的 USB 移动存储设备访问控制方法的流程示意图；包括：

[0028] 步骤 101、在终端设备上监测到通用串行总线 USB 移动存储设备时，获取所述 USB 移动存储设备标识。

[0029] 举例来说，USB 移动存储设备访问控制装置在终端设备上监测到 USB 移动存储设备。具体地，USB 移动存储设备访问控制装置可以通过安装在终端设备中的监控程序来实现，该监控程序中的磁盘过滤驱动会在终端设备启动时就加载到内核中，并监控该终端设备所有的即插即用 (Plug-and-Play，简称 PNP) 动作，任何 USB 移动存储设备的插入都会被磁盘过滤驱动识别，USB 移动存储设备标识可以自动从所述 USB 移动存储设备中读出。终

端设备具体可以是计算机、PDA、手机等设备。

[0030] 步骤 102、根据所述 USB 移动存储设备标识，查询本地访问控制表中是否存在所述 USB 移动存储设备标识对应的访问控制表项，若是则执行步骤 103，否则结束。

[0031] 举例来说，终端设备的本地访问控制表可以是预先设置的，也可以是从服务器中同步获取的。

[0032] 步骤 103、验证用户信息。

[0033] 具体地，用户信息可以包括用户名和 / 或密码和 / 或用户角色。本实施例的验证用户信息可以进一步保证对 USB 移动存储设备的操作权限的控制。

[0034] 举例来说，用户信息可以通过在终端设备上弹出提示输入用户信息的对话框，以使用户输入该用户信息。

[0035] 步骤 104、若验证通过，则根据所述访问控制表项确定所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限。

[0036] 举例来说，两个用户信息中的用户名和密码不同，该两个用户信息对应的同一 USB 移动存储设备的访问权限可以不同，或者两个用户信息中的用户名和密码相同，但用户角色不同，该两个用户信息对应的同一 USB 移动存储设备的访问权限也可以不同，如用户名都为 user，密码都是 123，若用户角色为研发部，则该用户信息对应的该 USB 移动存储设备的访问权限可以是读写操作，若用户角色为市场部，则该用户信息对应的该 USB 移动存储设备的访问权限只有读操作。

[0037] 步骤 105、根据所述操作权限，控制在所述终端设备上对所述 USB 移动存储设备的操作。

[0038] 本发明实施例通过在终端设备上监测到 USB 移动存储设备时，获取所述 USB 移动存储设备标识和用户信息，查询本地访问控制表确定所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限，根据所述操作权限控制在所述终端设备上对所述 USB 移动存储设备的操作，可以基于用户信息、终端设备、USB 移动存储设备设置不同的操作权限，控制用户在终端设备上对 USB 移动存储设备的操作，解决现有技术中对移动储存设备的监控存通用性较差的问题，能够实时灵活的控制 USB 移动存储设备的操作权限，有效保证内网终端设备上文件的安全性。

[0039] 实施例二

[0040] 图 2 为本发明实施例二提供的 USB 移动存储设备访问控制方法的流程示意图；在图 1 所示方法实施例一基础上的进一步扩展，包括：

[0041] 步骤 201、在终端设备上监测到 USB 移动存储设备时，获取所述 USB 移动存储设备标识。

[0042] 举例来说，USB 移动存储设备访问控制装置在终端设备上监测到 USB 移动存储设备。具体地，USB 移动存储设备访问控制装置可以通过安装在终端设备中的监控程序来实现，该监控程序中的磁盘过滤驱动会在终端设备启动时就加载到内核中，并监控该终端设备所有的即插即用 (Plug-and-Play，简称 PNP) 动作，任何 USB 移动存储设备的插入都会被磁盘过滤驱动识别。终端设备具体可以是计算机、手机等设备。而终端设备上新的分区加载动作会被监控程序中的文件系统过滤驱动获取到，对于任何新加载的分区，文件系统过滤驱动会在内核中生成对应的过滤驱动设备，并附加到新分区的内核设备对象的设备栈中。

[0043] 如磁盘过滤驱动获取到新插入的 USB 移动存储设备后会通知应用层，应用层通过 Windows 消息的截取获取所有新增的盘符，再通知给内核中的文件系统过滤驱动需要监控哪些分区。这样所有 USB 移动存储设备的分区上的文件读写操作都会经过文件系统过滤驱动的监控，未被阻断的读写操作还会经过磁盘过滤驱动的过滤。

[0044] 步骤 202、根据所述 USB 移动存储设备标识，查询本地访问控制表中是否存在所述 USB 移动存储设备标识对应的访问控制表项；若是，则执行步骤 205，否则执行步骤 203。

[0045] 步骤 203、根据用户指令向注册服务器发送注册信息，所述注册信息包括用户信息、所述 USB 移动存储设备标识和所述终端设备标识。

[0046] 举例来说，若本地访问控制表中不存在所述 USB 移动存储设备标识对应的访问控制表项，终端设备向用户返回注册提示，如请求用户输入用户信息，然后将用户返回的用户指令中包含的用户信息、获取到 USB 移动存储设备标识和自身的终端设备标识发送给注册服务器，注册服务器根据所述用户信息、所述 USB 移动存储设备标识和所述终端设备标识，分配所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限，生成所述 USB 移动存储设备标识对应的访问控制表项，所述 USB 移动存储设备标识对应的访问控制表项包括所述用户信息、所述 USB 移动存储设备标识、所述终端设备标识和所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限。

[0047] 本实施例的注册服务器还可以将 USB 移动存储设备标识对应的访问控制表项加密存储在即可扩展标记语言 (Extensible Markup Language，简称 XML) 文件中，并将加密存储的访问控制表项发送给终端设备。

[0048] 进一步地，所有希望在终端设备上正常使用的 USB 移动存储设备第一次插入终端设备时都要进行注册。注册成功后，USB 移动存储设备的相关信息会存储到注册服务器的数据库中，由注册服务器统一保存所有终端设备的可用的 USB 移动存储设备的信息，大大降低了由终端设备篡改 USB 移动存储设备操作权限的可能。所有注册成功的 USB 移动存储设备可以由注册服务器统一分配每个 USB 移动存储设备的操作权限，这些操作权限可以具体到单独的终端设备和用户，即可以规定哪些用户在哪些终端设备可以使用哪些 USB 移动存储设备。这些信息总汇成一个访问控制表存储在注册服务器的 XML 文件中，每个终端设备可以得到一份该访问控制表的副本，作为本地访问控制表，任何访问控制表的更新都可以由注册服务器下发更新指令要求每个终端设备对其进行更新。

[0049] 步骤 204、接收所述注册服务器发送的加密后的所述 USB 移动存储设备标识对应的访问控制表项并储存在本地访问控制表中。

[0050] 本实施例中为了保证存储在终端设备上的访问控制表项的安全性和保密性，注册服务器对访问控制表项进行加密后再发送给终端设备，具体的加密方法可以是和终端设备预先协商好的或预先对应设置的，终端设备在需要查看访问控制表项时，可以用相应的解密方法对其进行解密。对应地，本实施例的步骤 202 之前，先对本地访问控制表中的访问控制表项进行解密。

[0051] 步骤 205、验证用户信息。

[0052] 举例来说，本步骤中的用户信息可以通过在终端设备上弹出提示输入用户信息的对话框，以使用户输入该用户信息。

[0053] 步骤 206、若验证通过，则根据所述访问控制表项确定所述用户信息对应的在所述

终端设备上使用所述 USB 移动存储设备的操作权限。

[0054] 步骤 207、根据所述操作权限，控制在所述终端设备上对所述 USB 移动存储设备的操作。

[0055] 举例来说，操作权限包括：读写操作、只读操作、禁止操作；根据所述操作权限，控制在所述终端设备上对所述 USB 移动存储设备的操作具体包括：

[0056] 若所述操作权限为读写操作，则允许在所述终端设备上对所述 USB 移动存储设备进行读操作和写操作；

[0057] 若所述操作权限为只读操作，则允许在所述终端设备上对所述 USB 移动存储设备进行读操作；

[0058] 若所述操作权限为禁止操作，则不允许在所述终端设备上对所述 USB 移动存储设备进行任何操作。

[0059] 进一步地，为了提高操作的安全性，若所述操作权限为读写操作，当监测到在所述终端设备上对所述 USB 移动存储设备进行写操作时，将所述终端设备上的文件加密后写入所述 USB 移动存储设备中；当监测到在所述终端设备上对所述 USB 移动存储设备进行读操作时，将所述 USB 移动存储设备中的文件解密后读取到所述终端设备中。这样，对于必须从某个终端设备拷贝文件到指定的终端设备上，而又不希望该文件流通到其他位置的，本实施例通过加密存储的方式，使得只有特定的终端设备可以使用 USB 移动存储设备，而在这些 USB 移动存储设备上的文件写入时均进行了加密处理，只有特定的终端设备才能解密该 USB 移动存储设备的内容，读取到正常的文件。

[0060] 本实施例通过注册服务器对 USB 移动存储设备的操作权限进行统一注册，可以基于用户信息、终端设备、USB 移动存储设备设置不同的操作权限，控制用户在终端设备上对 USB 移动存储设备的操作，解决现有技术中对移动储存设备的监控存通用性较差的问题，能够实时灵活的控制 USB 移动存储设备的操作权限，有效保证内网终端设备上文件的安全性。进一步地，采用磁盘过滤驱动和文件系统过滤驱动结合的方式，解决现有方案因为 Windows 操作系统其监控的层次较高，很容易被更加底层的读写技术绕过，使监控失效的问题。

[0061] 图 3 为本发明实施例三提供的 USB 移动存储设备访问控制装置的结构示意图；包括：

[0062] 监测模块 31，用于在终端设备上监测到通用串行总线 USB 移动存储设备时，获取所述 USB 移动存储设备标识；

[0063] 查询模块 32，用于根据所述 USB 移动存储设备标识，查询本地访问控制表中是否存在所述 USB 移动存储设备标识对应的访问控制表项；

[0064] 验证模块 33，用于若本地访问控制表中存在所述 USB 移动存储设备标识对应的访问控制表项，则对用户信息进行验证；

[0065] 确定模块 34，用于若验证通过，则根据所述访问控制表项确定所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限；

[0066] 控制模块 35，用于根据所述操作权限，控制在所述终端设备上对所述 USB 移动存储设备的操作。

[0067] 本实施例所示装置可以执行图 1 所示方法实施例所述方法，其实现原理和技术效

果不再赘述。

[0068] 图 4 为本发明实施例四提供的 USB 移动存储设备访问控制装置的结构示意图；在图 3 所示实施例的装置的基础上的扩展。

[0069] 所述装置还包括：

[0070] 发送模块 36，用于若本地访问控制表中不存在所述 USB 移动存储设备标识对应的访问控制表项，则根据用户指令向注册服务器发送注册信息，所述注册信息包括所述用户信息、所述 USB 移动存储设备标识和所述终端设备标识；

[0071] 接收模块 37，用于接收所述注册服务器发送的加密后的所述 USB 移动存储设备标识对应的访问控制表项，所述 USB 移动存储设备标识对应的访问控制表项包括所述用户信息、所述 USB 移动存储设备标识、所述终端设备标识和所述用户信息对应的在所述终端设备上使用所述 USB 移动存储设备的操作权限；

[0072] 储存模块 38，用于将加密后的所述 USB 移动存储设备标识对应的访问控制表项存储到本地访问控制表中。

[0073] 对应地，查询模块 32，还用于在查询本地访问控制表中是否存在所述 USB 移动存储设备标识对应的访问控制表项之前，对本地访问控制表中的访问控制表项进行解密。

[0074] 举例来说，本实施例的操作权限包括：读写操作、只读操作、禁止操作；

[0075] 对应地，控制模块 35 包括：

[0076] 第一控制单元 351，用于若所述操作权限为读写操作，则允许在所述终端设备上对所述 USB 移动存储设备进行读操作和写操作；

[0077] 第二控制单元 352，用于若所述操作权限为只读操作，则允许在所述终端设备上对所述 USB 移动存储设备进行读操作；

[0078] 第三控制单元 353，用于若所述操作权限为禁止操作，则不允许在所述终端设备上对所述 USB 移动存储设备进行任何操作。

[0079] 举例来说，本实施例的读写操作还包括加密读写操作，对应地，第一控制单元 351 包括：

[0080] 第一控制子单元，用于当监测到在所述终端设备上对所述 USB 移动存储设备进行写操作时，将所述终端设备上的文件加密后写入所述 USB 移动存储设备中；

[0081] 第二控制子单元，用于当监测到在所述终端设备上对所述 USB 移动存储设备进行读操作时，将所述 USB 移动存储设备中的文件解密后读取到所述终端设备中。

[0082] 本实施例所示装置可以执行图 2 所示方法实施例所述方法，其实现原理和技术效果不再赘述。

[0083] 本发明实施例五提供一种终端设备，包括：上述实施例三或实施例四所述的 USB 移动存储设备访问控制装置，可以执行图 1 或图 2 所示方法实施例的方法，其实现原理和技术效果类似，此处不再赘述。

[0084] 图 5 为本发明实施例六提供的 USB 移动存储设备访问控制系统的结构示意图，包括：实施例五所述的终端设备 51 和注册服务器 52；

[0085] 注册服务器 52，用于接收所述终端设备中 USB 移动存储设备访问控制装置发送的注册信息，所述注册信息包括用户信息、USB 移动存储设备标识和终端设备标识；根据所述用户信息、所述 USB 移动存储设备标识和所述终端设备标识，分配所述用户信息对应的在

所述终端设备上使用所述 USB 移动存储设备的操作权限；生成所述 USB 移动存储设备标识对应的访问控制表项，并进行加密后返回给所述 USB 移动存储设备访问控制装置。

[0086] 本实施例所示的系统可以具体用于执行图 1 或图 2 所示方法实施例的方法，其实现原理和技术效果类似，此处不再赘述。

[0087] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

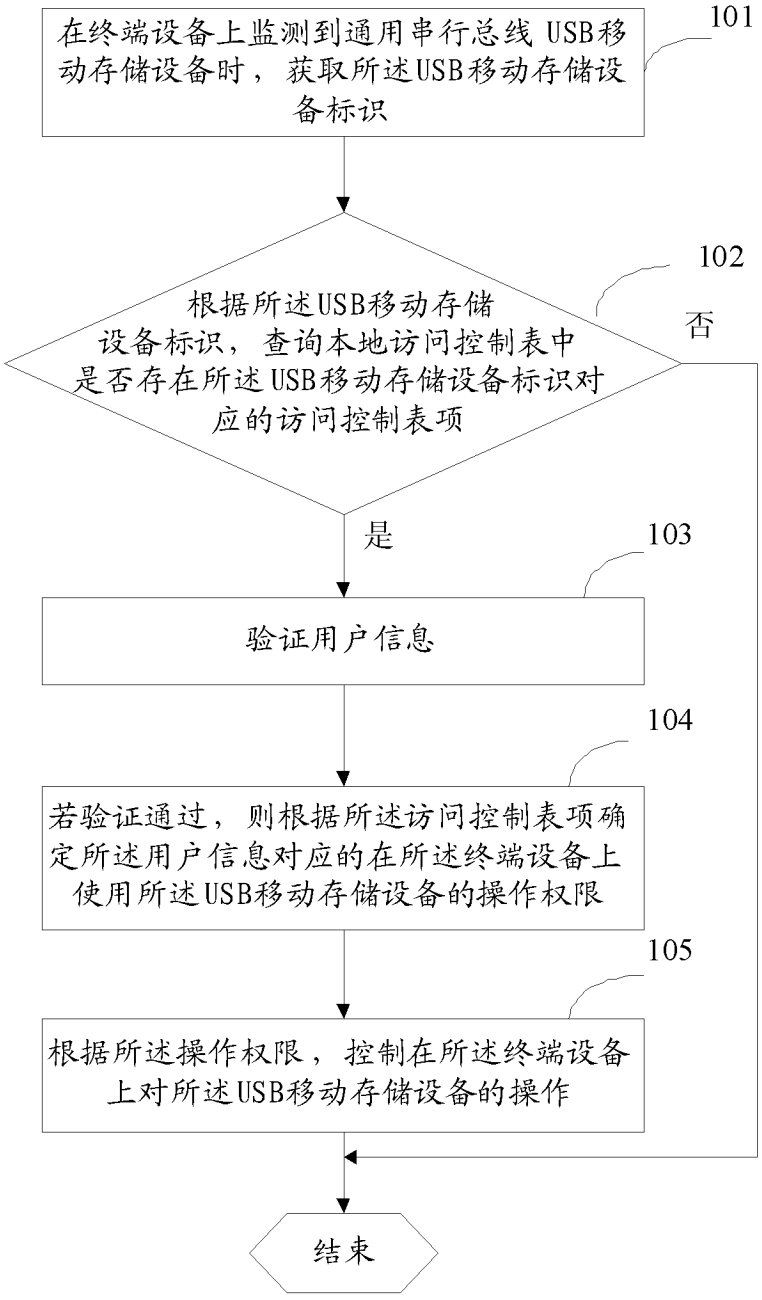

在终端设备上监测到通用串行总线 USB移动存储设备时，获取所述USB移动存储设备标识
101
根据所述USB移动存储设备标识，查询本地访问控制表中是否存在所述 USB移动存储设备标识对应的访问控制表项
102
否
是
103
验证用户信息
104
若验证通过，则根据所述访问控制表项确定所述用户信息对应的在所述终端设备上使用所述USB移动存储设备的操作权限
105
根据所述操作权限，控制在所述终端设备上对所述USB移动存储设备的操作
结束

图 1

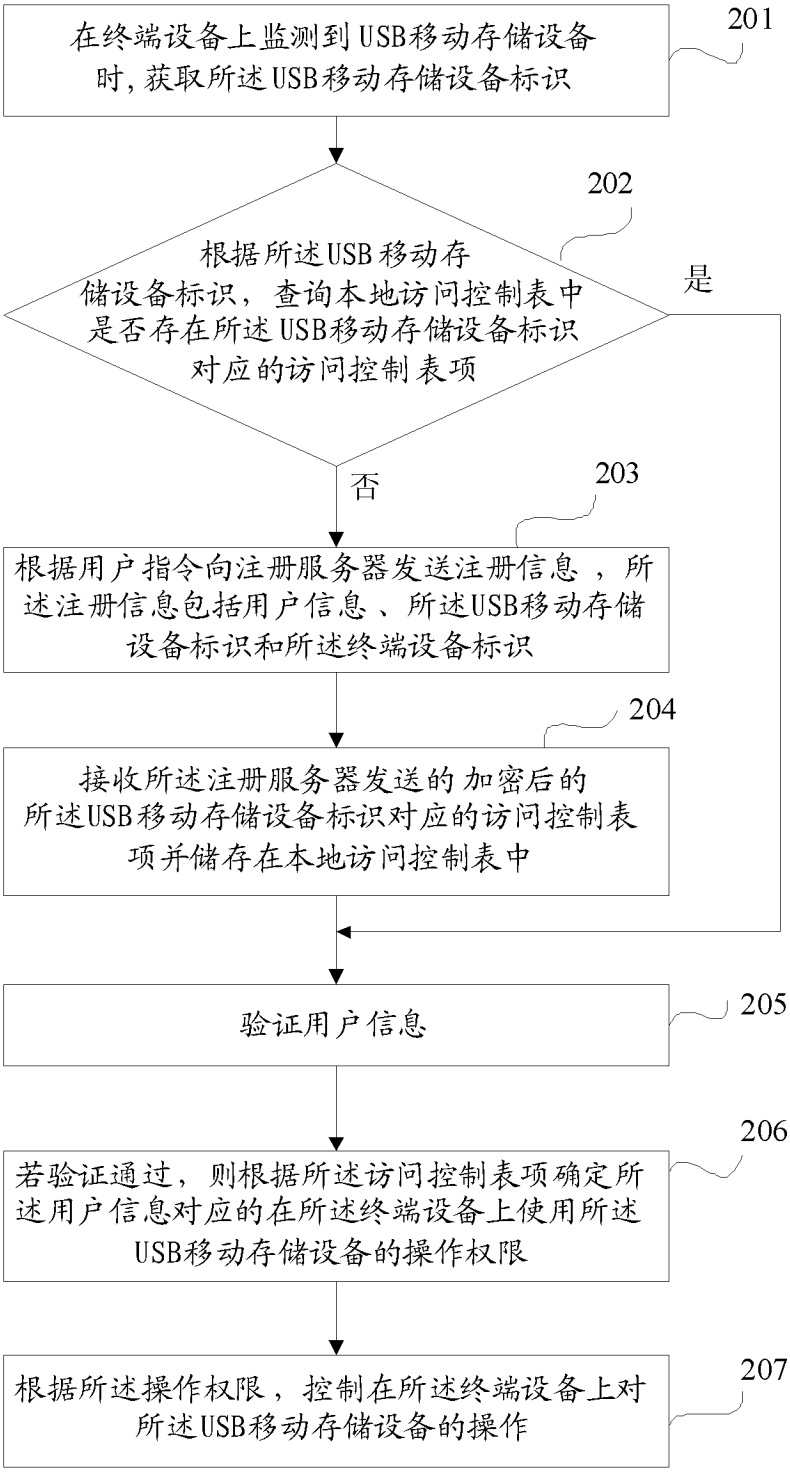

在终端设备上监测到USB移动存储设备时，获取所述USB移动存储设备标识
201
根据所述USB移动存储设备标识，查询本地访问控制表中是否存在所述USB移动存储设备标识对应的访问控制表项
202
是
否
根据用户指令向注册服务器发送注册信息，所述注册信息包括用户信息、所述USB移动存储设备标识和所述终端设备标识
203
接收所述注册服务器发送的加密后的所述USB移动存储设备标识对应的访问控制表项并储存在本地访问控制表中
204
验证用户信息
205
若验证通过，则根据所述访问控制表项确定所述用户信息对应的在所述终端设备上使用所述USB移动存储设备的操作权限
206
根据所述操作权限，控制在所述终端设备上对所述USB移动存储设备的操作
207

图 2

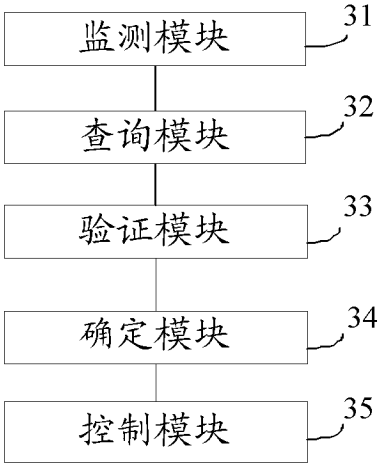

监测模块
31
查询模块
32
验证模块
33
确定模块
34
控制模块
35

图 3

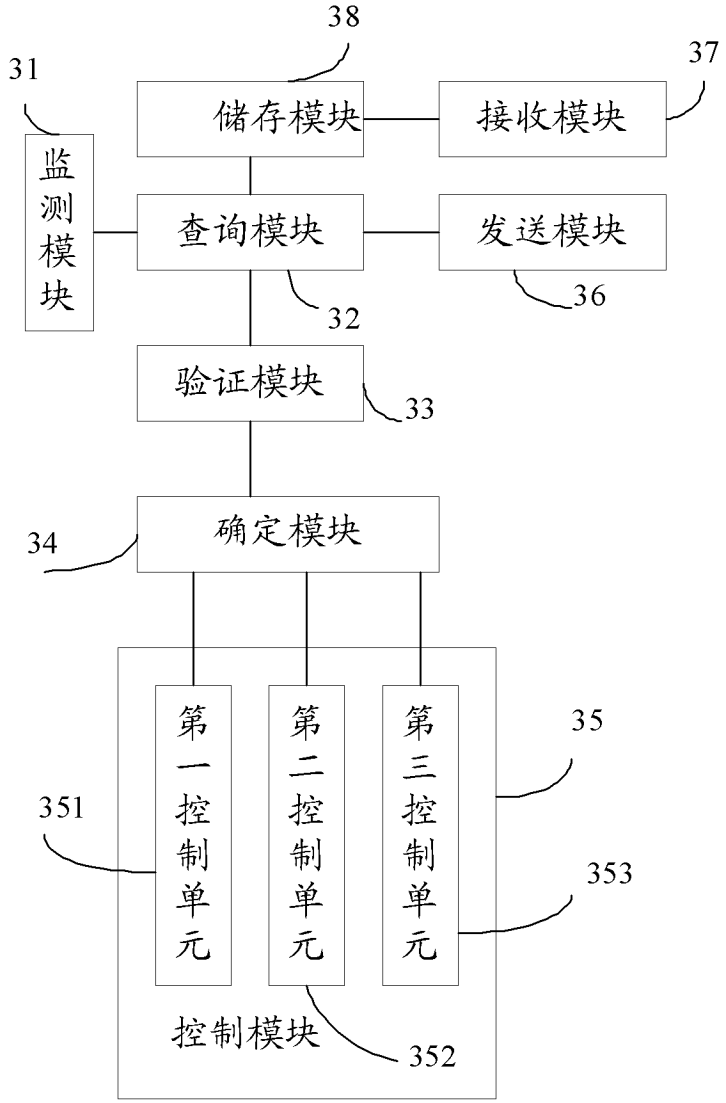

38
31
储存模块
37
接收模块
监测模块
查询模块
发送模块
32
36
验证模块
33
确定模块
34
第一控制单元
第二控制单元
第三控制单元
35
351
353
控制模块
352

图 4

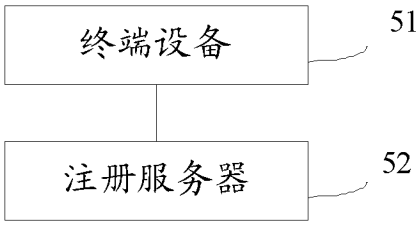

终端设备
51
注册服务器
52

图 5