(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 103530581 A
(43)申请公布日 2014.01.22

(21)申请号 201310468447.7

(22)申请日 2013.10.09

(71)申请人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街 21 号

(72)发明人 田新雪 袁晓静

(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 21/80(2013.01)
G06F 21/62(2013.01)

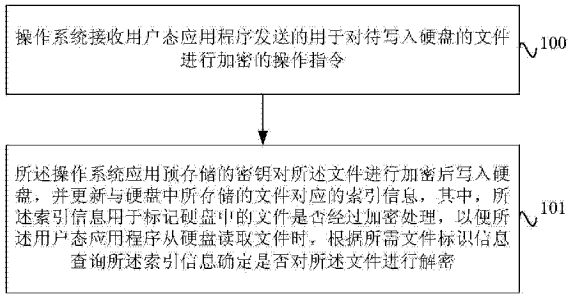
权利要求书2页 说明书4页 附图2页

(54)发明名称

硬盘加密方法和操作系统

(57)摘要

本发明提供一种硬盘加密方法和操作系统，其中，该方法包括：操作系统接收用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令，应用预存储的密钥对文件进行加密后写入硬盘，并更新与硬盘中所存储的文件对应的索引信息，其中，索引信息用于标记硬盘中的文件是否经过加密处理，以便用户态应用程序从硬盘读取文件时，根据所需文件标识信息查询所述索引信息确定是否对文件进行解密。通过本发明实施例提供的硬盘加密方法和操作系统，提高了硬盘所存储数据信息的安全性，有利于保护用户数据隐私。



CN 103530581 A

1. 一种硬盘加密方法，其特征在于，包括：

操作系统接收用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令；

所述操作系统应用预存储的密钥对所述文件进行加密后写入硬盘，并更新与所述硬盘中所存储的文件对应的索引信息，其中，所述索引信息用于标记硬盘中的文件是否经过加密处理，以便所述用户态应用程序从硬盘读取文件时，根据所需文件标识信息查询所述索引信息确定是否对所述文件进行解密。

2. 根据权利要求 1 所述的硬盘加密方法，其特征在于，在所述接收用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令之前，所述方法还包括：

所述操作系统向密钥管理服务器发送包括用户标识信息的密钥获取请求消息；

所述操作系统接收所述密钥管理服务器返回的、根据存储的用户信息获取的与所述用户标识信息对应的密钥并保存。

3. 根据权利要求 1 所述的硬盘加密方法，其特征在于，所述操作系统应用预存储的密钥对所述文件进行加密后写入硬盘具体包括：

所述操作系统调用核心态中的相应的系统代码运行预设的密钥获取子程序获取预存储的密钥；

所述操作系统应用所述密钥对所述文件进行加密，并将加密后的文件传递到核心态，通过核心态对硬盘进行写操作保存加密后的文件。

4. 根据权利要求 1 所述的硬盘加密方法，其特征在于，所述用户态应用程序从硬盘读取文件时，根据所需文件标识信息查询所述索引信息确定是否对所述文件进行解密具体包括：

所述操作系统接收所述用户态应用程序发送的包括文件标识信息的查询请求消息；

所述操作系统根据所述文件标识信息查询所述索引信息，判断与所述文件标识信息对应的文件是否经过加密处理，若是，则从所述硬盘读取所述文件并应用所述密钥进行解密处理后发送给所述用户态应用程序，否则，从所述硬盘读取所述文件直接发送给所述用户态应用程序。

5. 根据权利要求 1-4 任一所述的硬盘加密方法，其特征在于，

若所述操作系统出现故障且根据用户信息通过第三方管理平台的合法性验证后，则根据所述操作系统的标识信息从所述第三方管理平台获取与所述操作系统对应的密钥，并通过其他操作系统启动计算机，应用所述密钥对存储在所述硬盘中经过加密的文件进行解密处理。

6. 一种操作系统，其特征在于，包括：

接收模块，用于接收用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令；

处理模块，用于应用预存储的密钥对所述文件进行加密后写入硬盘，并更新与所述硬盘中所存储的文件对应的索引信息，其中，所述索引信息用于标记硬盘中的文件是否经过加密处理，以便所述用户态应用程序从硬盘读取文件时，根据所需文件标识信息查询所述索引信息确定是否对所述文件进行解密。

7. 根据权利要求 6 所述的操作系统，其特征在于，在所述接收用户态应用程序发送的

用于对待写入硬盘的文件进行加密的操作指令之前，

所述处理模块，还用于向密钥管理服务器发送包括用户标识信息的密钥获取请求消息；

所述接收模块，还用于接收所述密钥管理服务器返回的、根据存储的用户信息获取的与所述用户标识信息对应的密钥并保存。

8. 根据权利要求 6 所述的操作系统，其特征在于，所述处理模块具体用于：

调用核心态中的相应的系统代码运行预设的密钥获取子程序获取预存储的密钥；

应用所述密钥对所述文件进行加密，并将加密后的文件传递到核心态，通过核心态对硬盘进行写操作保存加密后的文件。

9. 根据权利要求 6 所述的操作系统，其特征在于，

所述接收模块，还用于接收所述用户态应用程序发送的包括文件标识信息的查询请求消息；

所述处理模块，还用于根据所述文件标识信息查询所述索引，判断与所述文件标识信息对应的文件是否经过加密处理，若是，则从所述硬盘读取所述文件并应用所述密钥进行解密处理后发送给所述用户态应用程序，否则，从所述硬盘读取所述文件直接发送给所述用户态应用程序。

硬盘加密方法和操作系统

技术领域

[0001] 本发明实施例涉及通信技术领域，尤其涉及一种硬盘加密方法和操作系统。

背景技术

[0002] 目前针对企业员工计算机信息泄露所进行的安全措施很多，比如限制 U 口的写访问，限制网络上传等信息安全手段，特别是一些企业单位，采用了员工计算机信息审计的方法，通过安装信息审计软件，实时的记录和向企业内网上传计算机文档操作的过程，一定程度上对员工故意泄密形成了很大的威慑。

[0003] 但是，当员工把硬盘拿下来连接到别的电脑上，便可以对任何数据进行拷贝，或者员工从 U 盘或者光盘启动另外一个操作系统，从而对本计算机上的硬盘进行监控拷贝，因此，亟需一种针对硬盘泄密的安全保护方法。

发明内容

[0004] 针对现有技术的上述缺陷，本发明实施例提供一种硬盘加密方法和操作系统。

[0005] 本发明一方面提供一种硬盘加密方法，包括：

[0006] 操作系统接收用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令；

[0007] 所述操作系统应用预存储的密钥对所述文件进行加密后写入硬盘，并更新与所述硬盘中所存储的文件对应的索引信息，其中，所述索引信息用于标记硬盘中的文件是否经过加密处理，以便所述用户态应用程序从硬盘读取文件时，根据所需文件标识信息查询所述索引信息确定是否对所述文件进行解密。

[0008] 本发明另一方面提供一种操作系统，包括：

[0009] 接收模块，用于接收用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令；

[0010] 处理模块，用于应用预存储的密钥对所述文件进行加密后写入硬盘，并更新与所述硬盘中所存储的文件对应的索引信息，其中，所述索引信息用于标记硬盘中的文件是否经过加密处理，以便所述用户态应用程序从硬盘读取文件时，根据所需文件标识信息查询所述索引信息确定是否对所述文件进行解密。

[0011] 本发明实施例提供的硬盘加密方法和操作系统，通过操作系统应用预存储的密钥对待写入硬盘的文件进行加密后写入硬盘，并更新用于标记硬盘中的文件是否经过加密处理的索引信息，从而当用户态应用程序从硬盘读取文件时，操作系统根据所需文件标识信息查询索引信息确定是否对文件进行解密。从而提高了硬盘所存储数据信息的安全性，有利于保护用户数据隐私。

附图说明

[0012] 图 1 为本发明实施例提供的一个硬盘加密方法的流程图；

[0013] 图 2 为本发明实施例提供的另一个硬盘加密方法的流程图；

[0014] 图 3 为本发明实施例提供的一个操作系统的结构示意图。

具体实施方式

[0015] 图 1 为本发明实施例提供的一个硬盘加密方法的流程图，如图 1 所示，该方法包括：

[0016] 步骤 100，操作系统接收用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令；

[0017] 当用户态应用程序需要对待存储到硬盘的文件进行加密时，向操作系统发送用于对待写入硬盘的文件进行加密的操作指令。

[0018] 步骤 101，所述操作系统应用预存储的密钥对所述文件进行加密后写入硬盘，并更新与所述硬盘中所存储的文件对应的索引信息，其中，所述索引信息用于标记硬盘中的文件是否经过加密处理，以便所述用户态应用程序从硬盘读取文件时，根据所需文件标识信息查询所述索引信息确定是否对所述文件进行解密。

[0019] 当操作系统接收到用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令，应用预存储的密钥对待存储的文件进行加密后写入硬盘，并更新用于标记硬盘中的文件是否经过加密处理的索引信息，其中，索引信息记录硬盘中存储的所有文件，记录与每个文件的标识信息对应的加密情况，进一步地，为了节约资源索引信息可以仅记录硬盘中经过加密处理的文件的标识信息，或者仅记录硬盘中没有经过加密处理的文件的标识信息。需要说明的是，本实施例中操作系统中预先存储的密钥可以是用户预先设置的，也可以是通过向其他服务器发送鉴权消息，当服务器根据鉴权消息对用户身份验证通过后，向用户返回与其对应的密钥。经过上述操作系统根据用户指示对用户态应用程序欲存储到硬盘中的文件经过加密处理后，从而当用户态应用程序需要从硬盘读取文件时，该操作系统可以根据所需文件标识信息查询之前建立的索引信息确定该文件是否经过加密处理，以便确定在将文件发送给用户态应用程序之前是否对文件进行解密处理。由此可见，本实施例提供的硬盘加密方法通过操作系统应用预存储的密钥对待写入硬盘的文件进行加密后写入硬盘，并更新用于标记硬盘中的文件是否经过加密处理的索引信息，从而当恶意用户启动其它操作系统运行用户态应用程序从该硬盘读取文件时，由于其它操作系统中并没有预先存储密钥，因此不能解密待获取的加密文件，从而提高了硬盘所存储数据信息的安全性。

[0020] 本实施例提供的硬盘加密方法和操作系统，通过操作系统应用预存储的密钥对待写入硬盘的文件进行加密后写入硬盘，并更新用于标记硬盘中的文件是否经过加密处理的索引信息，从而当用户态应用程序从硬盘读取文件时，操作系统根据所需文件标识信息查询索引信息确定是否对文件进行解密。从而提高了硬盘所存储数据信息的安全性，有利于保护用户数据隐私。

[0021] 图 2 为本发明实施例提供的另一个硬盘加密方法的流程图，如图 2 所示，该方法包括：

[0022] 步骤 200，操作系统向密钥管理服务器发送包括用户标识信息的密钥获取请求消息，并接收所述密钥管理服务器返回的、根据存储的用户信息获取的与所述用户标识信息对应的密钥并保存；

[0023] 对文件信息的安全性要求较高的企业通常设置有密钥管理服务器，该密钥管理服务器中存储有与每个用户的用户标识信息对应的密钥，用户在启动操作系统之后与密钥管理服务器建立连接，操作系统向密钥管理服务器发送包括用户标识信息的密钥获取请求消息，密钥管理服务器根据存储的用户信息获取的与用户标识信息对应的密钥并返回给操作系统，操作系统接收该密钥并进行保存。

[0024] 步骤 201，操作系统接收用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令；

[0025] 当用户态应用程序需要对待存储到硬盘的文件进行加密时，向操作系统发送用于对待写入硬盘的文件进行加密的操作指令。

[0026] 步骤 202，所述操作系统应用预存储的密钥对所述文件进行加密后写入硬盘，并更新与所述硬盘中所存储的文件对应的索引信息，其中，所述索引信息用于标记硬盘中的文件是否经过加密处理；

[0027] 所述操作系统调用核心态中的相应的系统代码运行预设的密钥获取子程序获取预存储的密钥，该密钥是上述从密钥管理服务器获取的，然后应用该密钥对待存储的文件进行加密，并将加密后的文件传递到核心态，通过核心态对硬盘进行写操作保存加密后的文件，并更新用于标记硬盘中的文件是否经过加密处理的索引信息，其中，索引信息记录硬盘中存储的所有文件，记录与每个文件的标识信息对应的加密情况，进一步地，为了节约资源索引信息可以仅记录硬盘中经过加密处理的文件的标识信息，或者仅记录硬盘中没有经过加密处理的文件的标识信息。

[0028] 步骤 203，所述操作系统接收所述用户态应用程序发送的包括文件标识信息的查询请求消息；

[0029] 当用户态应用程序需要从硬盘读取文件时，向操作系统发送包括文件标识信息的查询请求消息。

[0030] 步骤 204，所述操作系统根据所述文件标识信息查询所述索引信息，判断与所述文件标识信息对应的文件是否经过加密处理，若是，则从所述硬盘读取所述文件并应用所述密钥进行解密处理后发送给所述用户态应用程序，否则，从所述硬盘读取所述文件直接发送给所述用户态应用程序。

[0031] 操作系统接收用户态应用程序发送的查询请求消息之后，根据所需文件标识信息查询之前建立的索引信息确定该文件是否经过加密处理，若查询获知该文件经过加密处理，则从硬盘读取该文件并应用上述从密钥管理服务器获取的密钥进行解密处理后发送给用户态应用程序，若查询获知该文件没有经过加密处理，则从硬盘读取该文件直接发送给用户态应用程序。

[0032] 本实施例提供的硬盘加密方法和操作系统，通过操作系统应用从密钥管理服务器获取的密钥对待写入硬盘的文件进行加密后写入硬盘，并更新用于标记硬盘中的文件是否经过加密处理的索引信息，从而当用户态应用程序从硬盘读取文件时，操作系统根据所需文件标识信息查询索引信息确定是否对文件进行解密。从而提高了硬盘所存储数据信息的安全性，有利于保护用户数据隐私。

[0033] 基于上述实施例，进一步地，若上述操作系统出现故障，则用户将硬盘挂载到其他计算机上启动新的操作系统，然后通过新的操作系统与第三方管理平台建立连接，向第三

方管理平台发送出现故障的操作系统的标识信息和用户信息，第三方管理平台首先根据用户信息对该用户的合法性进行鉴权，若验证用户合法，则查询本地存储的密钥信息获取与出现故障的操作系统的标识信息对应的密钥并发送给新的操作系统，当新的操作系统接收到用户态应用程序发送的查询请求消息之后，从硬盘读取该文件，若判断该文件经过加密处理，则应用上述从第三方管理平台获取的密钥进行解密处理后发送给用户态应用程序。

[0034] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0035] 图 3 为本发明实施例提供的一个操作系统的结构示意图，如图 3 所示，该操作系统包括：接收模块 11 和处理模块 12，其中，接收模块 11 用于接收用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令；处理模块 12 用于应用预存储的密钥对所述文件进行加密后写入硬盘，并更新与所述硬盘中所存储的文件对应的索引信息，其中，所述索引信息用于标记硬盘中的文件是否经过加密处理，以便所述用户态应用程序从硬盘读取文件时，根据所需文件标识信息查询所述索引信息确定是否对所述文件进行解密。

[0036] 本实施例提供的操作系统中各模块的功能和处理流程，可以参见上述图 1 所示的方法实施例，其实现原理和技术效果类似，此处不再赘述。

[0037] 进一步地，在所述接收用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令之前，处理模块 12 还用于向密钥管理服务器发送包括用户标识信息的密钥获取请求消息；接收模块 11 还用于接收所述密钥管理服务器返回的、根据存储的用户信息获取的与所述用户标识信息对应的密钥并保存。

[0038] 具体地，处理模块 12 具体用于：调用核心态中的相应的系统代码运行预设的密钥获取子程序获取预存储的密钥；应用所述密钥对所述文件进行加密，并将加密后的文件传递到核心态，通过核心态对硬盘进行写操作保存加密后的文件。

[0039] 进一步地，接收模块 11 还用于接收所述用户态应用程序发送的包括文件标识信息的查询请求消息；处理模块 12 还用于根据所述文件标识信息查询所述索引，判断与所述文件标识信息对应的文件是否经过加密处理，若是，则从所述硬盘读取所述文件并应用所述密钥进行解密处理后发送给所述用户态应用程序，否则，从所述硬盘读取所述文件直接发送给所述用户态应用程序。

[0040] 本实施例提供的操作系统中各模块的功能和处理流程，可以参见上述图 2 所示的方法实施例，其实现原理和技术效果类似，此处不再赘述。

[0041] 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精神和范围。

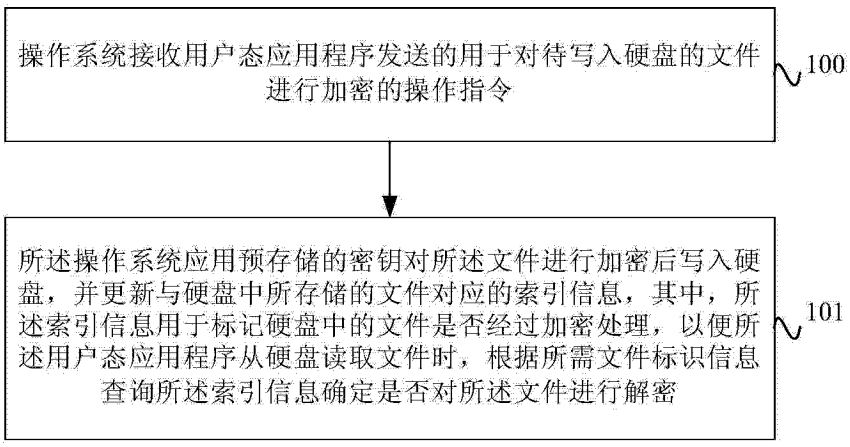

操作系统接收用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令
100
所述操作系统应用预存储的密钥对所述文件进行加密后写入硬盘，并更新与硬盘中所存储的文件对应的索引信息，其中，所述索引信息用于标记硬盘中的文件是否经过加密处理，以便所述用户态应用程序从硬盘读取文件时，根据所需文件标识信息查询所述索引信息确定是否对所述文件进行解密
101

图 1

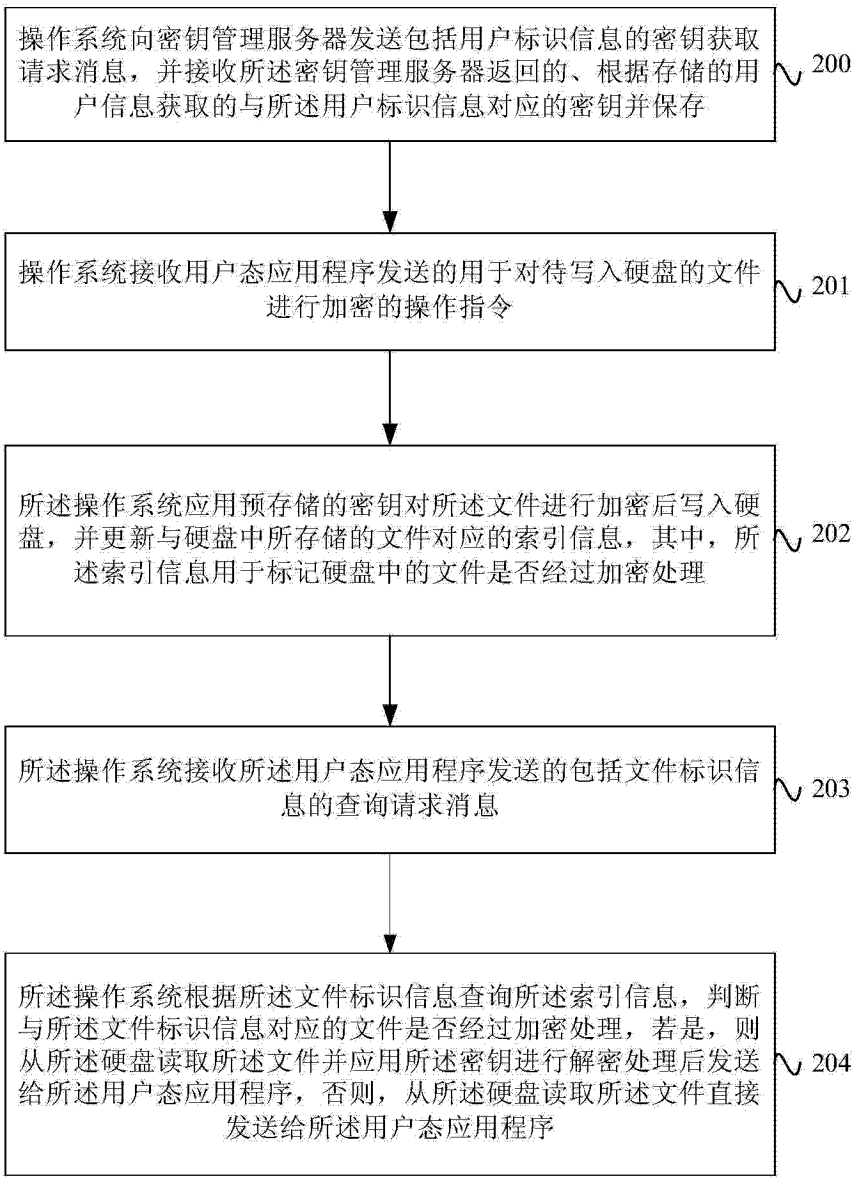

操作系统向密钥管理服务器发送包括用户标识信息的密钥获取请求消息，并接收所述密钥管理服务器返回的、根据存储的用户信息获取的与所述用户标识信息对应的密钥并保存
200
操作系统接收用户态应用程序发送的用于对待写入硬盘的文件进行加密的操作指令
201
所述操作系统应用预存储的密钥对所述文件进行加密后写入硬盘，并更新与硬盘中所存储的文件对应的索引信息，其中，所述索引信息用于标记硬盘中的文件是否经过加密处理
202
所述操作系统接收所述用户态应用程序发送的包括文件标识信息的查询请求消息
203
所述操作系统根据所述文件标识信息查询所述索引信息，判断与所述文件标识信息对应的文件是否经过加密处理，若是，则从所述硬盘读取所述文件并应用所述密钥进行解密处理后发送给所述用户态应用程序，否则，从所述硬盘读取所述文件直接发送给所述用户态应用程序
204

图 2

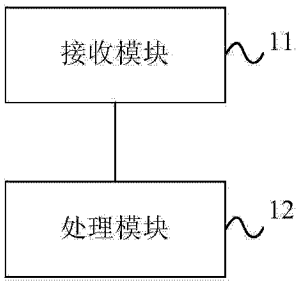

接收模块
11
处理模块
12

图 3