(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 103152425 A
(43)申请公布日 2013.06.12

(21)申请号 201310084757.9

(22)申请日 2013.03.15

(71)申请人 苏州九光信息科技有限公司
地址 215000 江苏省苏州市苏州工业园区星湖街 328 号创意产业园 15-203 单元

(72)发明人 耿振民 杨磊

(74)专利代理机构 上海光华专利事务所 31219
代理人 高磊

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)

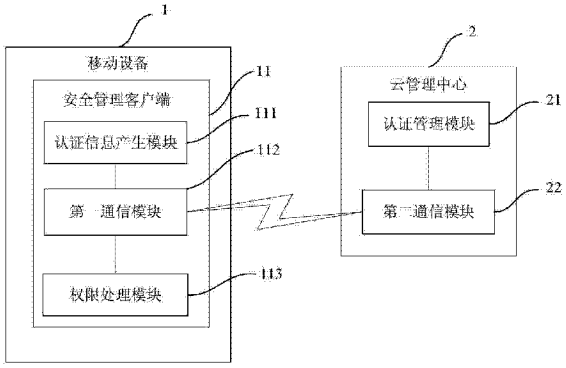
权利要求书1页 说明书5页 附图1页

(54)发明名称

基于云技术的移动设备的安全管理系统

(57)摘要

本发明提供一种基于云技术的移动设备的安全管理系统。所述系统通过位于移动设备的认证信息产生模块在所述移动设备开机时获取用于表示所述移动设备的至少一个标识信息，并基于所获取的标识信息生成认证信息；再由第一通信模块，将所述认证信息发送给与所述安全管理客户端通信的云管理中心；所述云管理中心中的认证管理模块将所获取的认证信息进行合法认证，并在确定所获取的认证信息合法时，确定所获取的认证信息所对应的使用所述移动设备的权限信息；并由第二通信模块将所确定的权限信息返回至所述第一通信模块，以供所述安全管理客户端中的权限处理模块按照所述第一通信模块所获取的权限信息对所述移动设备的操作进行权限管理。



CN 103152425 A

1. 一种基于云技术的移动设备的安全管理系统，其特征在于，至少包括：

位于移动设备的安全管理客户端，包括：

认证信息产生模块，用于在所述移动设备开机时获取用于表示所述移动设备的至少一个标识信息，并基于所获取的标识信息生成认证信息；

第一通信模块，用于将所述认证信息发送给与所述安全管理客户端通信的云管理中心；

其中，所述云管理中心包括：

认证管理模块，用于将所获取的认证信息进行合法认证，并在确定所获取的认证信息合法时，确定所获取的认证信息所对应的使用所述移动设备的权限信息；

第二通信模块，用于将所确定的权限信息返回至所述第一通信模块，以供所述安全管理客户端中的权限处理模块按照所述第一通信模块所获取的权限信息对所述移动设备的操作进行权限管理。

2. 根据权利要求 1 所述的基于云技术的移动设备的安全管理系统，其特征在于，所述认证管理模块还用于从所获取的认证信息中提取所述标识信息，并将所述标识信息与预存储的相应的多个标识信息进行匹配，在匹配成功时，认定所获取的认证信息合法。

3. 根据权利要求 1 或 2 所述的基于云技术的移动设备的安全管理系统，其特征在于，在所述认证管理模块认证所获取的认证信息不合法时，所述认证管理模块还用于指示所述安全管理客户端重新提供所述认证信息，并限定一天之内重复获取所述认证信息的次数。

4. 根据权利要求 1 所述的基于云技术的移动设备的安全管理系统，其特征在于，所述第一通信模块还用于从当前所通信的基站处获取所述移动设备所在位置，并将所述位置通发送至所述云管理中心。

5. 根据权利要求 4 所述的基于云技术的移动设备的安全管理系统，其特征在于，所述认证管理模块在确定所获取的认证信息合法时，还根据所述移动设备历史的位置确定当前所获取的移动设备的位置是否位于常用位置，若不是，则认定所述移动设备安全异常，若是，则确定将相应的权限信息发送至所述安全管理客户端。

6. 根据权利要求 1 所述的基于云技术的移动设备的安全管理系统，其特征在于，所述标识信息包括：所述移动设备的硬件信息、预存储在所述移动设备中的个人信息、及所述移动设备中插入的 sim 卡中的标识信息中的一种或多种。

7. 根据权利要求 1 所述的基于云技术的移动设备的安全管理系统，其特征在于，所述权限信息包括：所述移动设备中的文件夹或软件的操作权限、所述移动设备上传 / 下载文件的权限中的一种或多种。

基于云技术的移动设备的安全管理系统

技术领域

[0001] 本发明涉及一种认证管理方案，特别是涉及一种基于云技术的移动设备的安全管理系统。

背景技术

[0002] 随着各企事业单位的规模不断扩大，跨地域的各企事业单位越来越多。为了员工出差方便，公司为员工配备了便于携带的移动设备，如平板电脑、手机等。然而，员工在使用这些移动设备时，通常不注意公司内部资料的安全，当移动设备被盗或利用移动设备传输文件时，经常会将公司内部资料泄露出去。可见，公司配备的移动设备难于管理。

[0003] 因此，需要对现有的设备认证管理系统进行改进，使之能够管理移动设备。

发明内容

[0004] 鉴于以上所述现有技术的缺点，本发明的目的在于提供一种基于云技术的移动设备的安全管理系统，用于解决现有技术中移动设备中的公司资料难于权限管理的问题。

[0005] 为实现上述目的及其他相关目的，本发明提供一种基于云技术的移动设备的安全管理系统，其至少包括：位于移动设备的安全管理客户端，包括：认证信息产生模块，用于在所述移动设备开机时获取用于表示所述移动设备的至少一个标识信息，并基于所获取的标识信息生成认证信息；第一通信模块，用于将所述认证信息发送给与所述安全管理客户端通信的云管理中心；

[0006] 其中，所述云管理中心包括：认证管理模块，用于将所获取的认证信息进行合法认证，并在确定所获取的认证信息合法时，确定所获取的认证信息所对应的使用所述移动设备的权限信息；第二通信模块，用于将所确定的权限信息返回至所述第一通信模块，以供所述安全管理客户端中的权限处理模块按照所述第一通信模块所获取的权限信息对所述移动设备的操作进行权限管理。

[0007] 优选地，所述认证管理模块还用于从所获取的认证信息中提取所述标识信息，并将所述标识信息与预存储的相应的多个标识信息进行匹配，在匹配成功时，认定所获取的认证信息合法。

[0008] 优选地，在所述认证管理模块认证所获取的认证信息不合法时，所述认证管理模块还用于指示所述安全管理客户端重新提供所述认证信息，并限定一天之内重复获取所述认证信息的次数。

[0009] 优选地，所述第一通信模块还用于从当前所通信的基站处获取所述移动设备所在位置，并将所述位置通发送至所述云管理中心。

[0010] 优选地，所述认证管理模块在确定所获取的认证信息合法时，还根据所述移动设备历史的位置确定当前所获取的移动设备的位置是否位于常用位置，若不是，则认定所述移动设备安全异常，若是，则确定将相应的权限信息发送至所述安全管理客户端。

[0011] 优选地，所述标识信息包括：所述移动设备的硬件信息、预存储在所述移动设备中

的个人信息、及所述移动设备中插入的 sim 卡中的标识信息中的一种或多种。

[0012] 优选地，所述权限信息包括：所述移动设备中的文件夹或软件的操作权限、所述移动设备上传 / 下载文件的权限中的一种或多种。

[0013] 如上所述，本发明的基于云技术的移动设备的安全管理系统，具有以下有益效果：通过安装在移动设备中的安全管理客户端收集能够表征用户及移动设备的标识信息，并生成唯一的认证信息，由云管理中心来认证所生成的认证信息，如此能方便集中管理和分配位于各地的移动设备的权限；另外，收集各移动设备所在位置，能够掌控使用移动设备是否被盗，防止移动设备中的文件或应用被泄露；再者，所述云管理中心对认证失败的移动设备给予重复提交认证信息的机会，能够防止由于丢包而导致的认证信息获取不全，同时也防止移动设备丢失、或客户端被破解后对权限信息的滥用。

附图说明

[0014] 图 1 显示为本发明的基于云技术的移动设备的安全管理系统的结构示意图。

[0015] 元件标号说明

[0016]	1	移动设备
[0017]	11	安全管理客户端
[0018]	111	认证信息产生模块
[0019]	112	第一通信模块
[0020]	113	权限处理模块
[0021]	2	云管理中心
[0022]	21	认证管理模块
[0023]	22	第二通信模块

具体实施方式

[0024] 以下通过特定的具体实例说明本发明的实施方式，本领域技术人员可由本说明书所揭露的内容轻易地了解本发明的其他优点与功效。本发明还可以通过另外不同的具体实施方式加以实施或应用，本说明书中的各项细节也可以基于不同观点与应用，在没有背离本发明的精神下进行各种修饰或改变。

[0025] 如图 1 所示，本发明提供一种基于云技术的移动设备的安全管理系统，所述安全管理系统用于保护移动设备内的文件或应用、存放公司服务器上的文件的使用安全。所述安全管理系统包括移动设备、云管理中心，其中，所述移动设备指带有 sim 卡槽和 SD 卡槽、且能通过移动网络与云管理中心、公司服务器进行通信的设备，其包括但不限于：手机、平板电脑等。所述云管理中心为一种能够按照预设的程序进行大量数据、逻辑运算的设备，其包括但不限于：嵌入式设备、服务器。所述公司服务器是在所述云管理中心的管理下，为所述移动设备提供文件或获取来自所述移动设备的文件的服务器。

[0026] 所述移动设备 1 中安装有安全管理客户端 11，所述安全管理客户端 11 包括：认证信息产生模块 111、第一通信模块 112。

[0027] 所述认证信息产生模块 111 用于在所述移动设备 1 开机时获取用于表示所述移动设备 1 的至少一个标识信息，并基于所获取的标识信息生成认证信息。其中，所述标识信息

包括任何能够唯一标识所述移动设备 1 或持有所述移动设备 1 的用户的信息，其包括但不限于：所述移动设备 1 的硬件信息、预存储在所述移动设备 1 中的个人信息、或所述移动设备 1 中插入的 sim 卡中的标识信息，也可以是上述信息中的组合。

[0028] 具体地，所述认证信息产生模块 111 在所述移动设备 1 开机后自动运行，利用所述移动设备 1 的操作系统或虚拟机提供的接口来获取硬件信息，从所述移动设备 1 的 SD 卡中读取预存储的用户信息，以及从 sim 卡中读取 sim 卡中的标识信息，并根据预设的算法将所获取的三个信息转换成一个唯一的、用于表示所述移动设备 1 的认证信息。其中，所述算法可以是：哈希算法、SM1 算法等。

[0029] 所述第一通信模块 112 用于将所述认证信息发送给与所述安全管理客户端 11 通信的云管理中心 2。其中，所述第一通信模块 112 包括：插在所述移动设备 1 中 sim 卡。

[0030] 接着，所述云管理中心 2 包括：认证管理模块 21、第二通信模块 22。

[0031] 所述第二通信模块 22 用于通过移动网络与所述第一通信模块 112 通信。

[0032] 所述认证管理模块 21 用于将所获取的认证信息进行合法认证，并在确定所获取的认证信息合法时，确定所获取的认证信息所对应的使用所述移动设备 1 的权限信息。其中，所述权限信息包括任何用于限制移动设备 1 上的应用或操作公司文件的信息，其包括但不限于：所述移动设备 1 中的文件夹或软件的操作权限、所述移动设备 1 上传 / 下载文件的权限中的一种或多种。

[0033] 具体地，所述认证管理模块 21 中预存储各移动设备 1 的认证信息，并将所获取的认证信息与所存储的认证信息进行匹配，如匹配成功，则认定所获取的认证信息合法，再将所存储的对应所述认证信息的权限信息通过所述第二通信模块 22 返回给所述安全管理客户端 11，所述安全管理客户端 11 中的权限处理模块 113 按照所述第一通信模块 112 所获取的权限信息对所述移动设备的操作进行权限管理。

[0034] 例如，所获取的认证信息包括：硬件信息，则所述认证管理模块 21 利用算法提取所述硬件信息，并将所获取的硬件信息与预存储的硬件信息进行匹配，匹配到后，将所述硬件信息所对应的权限信息发送给所述第一通信模块 112，其中，所述权限信息包括：允许查看文件夹 A 中的所有文件的权限，所述第一通信模块 112 将所述权限信息提供给所述权限处理模块 113，所述权限处理模块 113 根据所述权限信息监控用户的操作，当用户打开文件夹 A 时，允许其查看文件夹 A 中的所有文件，但禁止修改文件、或删除文件等操作。

[0035] 优选地，所述认证管理模块 21 还用于从所获取的认证信息中提取所述标识信息，并将所述标识信息与预存储的相应的多个标识信息进行匹配，在匹配成功时，认定所获取的认证信息合法。

[0036] 具体地，所述认证管理模块 21 利用认证信息产生模块 111 中的生成算法的反运算从所获取的认证信息中提取所包含的所有标识信息，并将各标识信息一一进行匹配，若所有标识信息匹配成功，则认定所获取的认证信息合法，反之，若有至少一个标识信息匹配不成功，则认定所获取的人性信息不合法，并生成认证失败的信息，由所述第二通信模块 22 返回给所述安全管理客户端 11，则所述安全管理客户端 11 根据所述认证失败的信息禁止用户对指定文件夹或应用软件的操作。

[0037] 更为优选地，在所述认证管理模块 21 认证所获取的认证信息不合法时，所述认证管理模块 21 还用于指示所述安全管理客户端 11 重新提供所述认证信息，并限定一天之内

重复获取所述认证信息的次数。

[0038] 具体地，当所述认证管理模块 21 无法解析所获取的认证信息、或认证所述认证信息不合法时，所述认证管理模块 21 根据封装所述认证信息的数据包中包含的移动设备 1 的地址信息，向所述地址信息返回重新发送认证信息的指令，以供所述安全管理客户端 11 中的认证信息产生模块 111 基于所述重发指令重新执行；与此同时，所述认证管理模块 21 对所述地址信息进行倒计数，每当来自所述地址信息的认证信息如若认证不合法，则倒计数值减一，如此，直至倒计数值减为零，则当天所述移动设备 1 无法再进行认证。未经认证的安全管理客户端 11 将禁止用户操作所述安全管理客户端 11 所指定的文件夹或应用软件。

[0039] 作为一种优选方案，所述第一通信模块 112 还用于从当前所通信的基站处获取所述移动设备 1 所在位置，并将所述位置通发送至所述云管理中心 2。

[0040] 具体地，所述第一通信模块 112 利用 sim 卡与基站的通信，确定自身在所述基站所覆盖的区域的位置信息，并将所述位置信息及所述认证信息一并发送至所述云管理中心 2。

[0041] 所述云管理中心 2 的认证管理模块 21 在确定所获取的认证信息合法后，还根据所述移动设备 1 历史的位置确定当前所获取的位置信息是否位于常用位置，若不是，则认定所述移动设备 1 安全异常，若是，则确定将相应的权限信息发送至所述安全管理客户端 11。

[0042] 本实施例的安全管理系统的工作过程如下：

[0043] 在所述移动设备 1 启动时，所述认证信息产生模块 111 获取所述硬件设备的硬件信息、SD 卡中存储的用户信息及 sim 卡中的标识信息，并根据预设的算法将所获取的各信息进行运算，以生成唯一的认证信息，并提供给所述第一通信模块 112，与此同时，所述第一通信模块 112 通过与基站的通信，从所述基站处获取所述移动设备 1 当前所在位置信息，并将所述认证信息及所述位置信息一并发送给所述云管理中心 2 的第二通信模块 22，所述认证管理模块 21 将来自所述第二通信模块 22 的认证信息进行解析，以得到所述认证信息中所包含的所有标识信息，再将各标识信息一一进行匹配，若匹配通过，则读取所述认证信息所对应的权限信息，接着，所述认证管理模块 21 再将所获取的位置信息与所存储的所述移动设备 1 历史中的位置信息进行比较，若无历史记录，则认定所述移动设备 1 所在位置异常，则向管理员报警，并不允许所述第二通信模块 22 发送所述权限信息，如果有历史记录，则认定所述移动设备 1 所在位置正常，允许所述第二通信模块 22 将所述权限信息发送给所述安全管理客户端 11，接着，由所述权限处理模块 113 监控用户对所述移动设备的操作，并按照所述权限信息的指示限制所述用户的非法操作。

[0044] 综上所述，本发明的基于云技术的移动设备的安全管理系统，通过安装在移动设备中的安全管理客户端收集能够表征用户及移动设备的标识信息，并生成唯一的认证信息，由云管理中心来认证所生成的认证信息，如此能方便集中管理和分配位于各地的移动设备的权限；另外，收集各移动设备所在位置，能够掌控使用移动设备是否被盗，防止移动设备中的文件或应用被泄露；再者，所述云管理中心对认证失败的移动设备给予重复提交认证信息的机会，能够防止由于丢包而导致的认证信息获取不全，同时也防止移动设备丢失、或客户端被破解后对权限信息的滥用。所以，本发明有效克服了现有技术中的种种缺点而具高度产业利用价值。

[0045] 上述实施例仅例示性说明本发明的原理及其功效，而非用于限制本发明。任何熟悉此技术的人士皆可在不违背本发明的精神及范畴下，对上述实施例进行修饰或改变。因

此，举凡所属技术领域中具有通常知识者在未脱离本发明所揭示的精神与技术思想下所完成的一切等效修饰或改变，仍应由本发明的权利要求所涵盖。

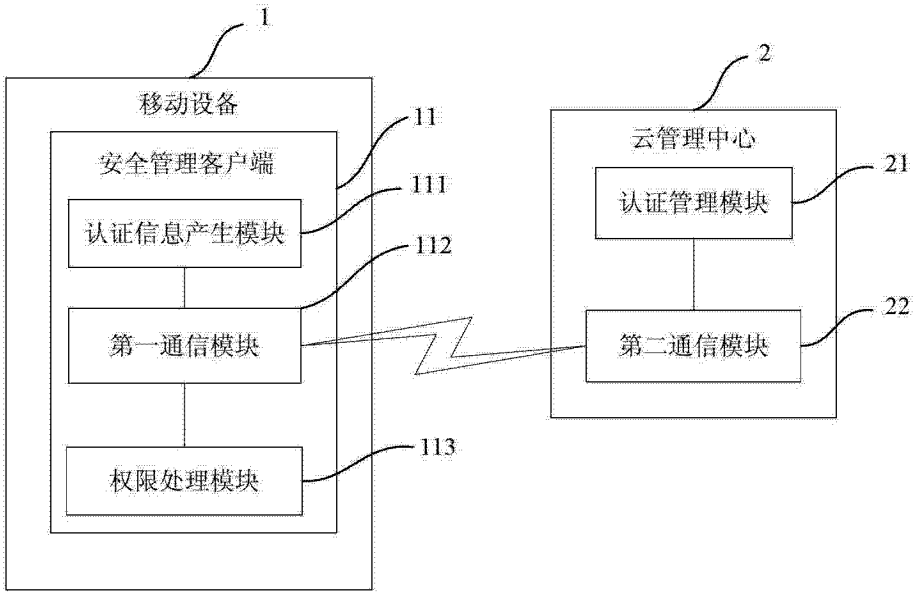

1
移动设备
11
安全管理客户端
111
认证信息产生模块
112
第一通信模块
113
权限处理模块
2
云管理中心
21
认证管理模块
22
第二通信模块

图 1