(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 103427990 A
(43)申请公布日 2013.12.04

(21)申请号 201210155173.1

(22)申请日 2012.05.18

(71)申请人 华为终端有限公司
地址 518129 广东省深圳市龙岗区坂田华为基地 B 区 2 号楼

(72)发明人 辜志力

(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
代理人 申健

(51)Int.Cl.
*H04L 9/32*(2006.01)
*H04L 29/06*(2006.01)

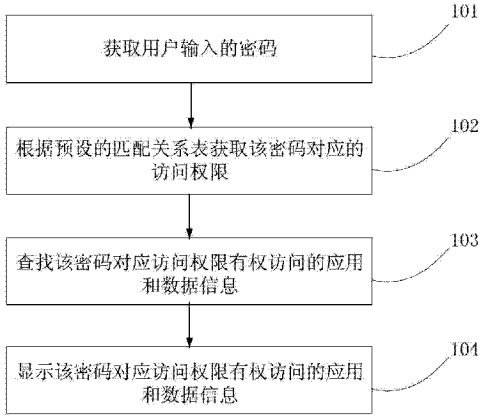
权利要求书2页 说明书6页 附图4页

(54)发明名称

权限认证的方法及终端设备

(57)摘要

本发明公开了一种权限认证的方法及终端设备，涉及终端设备应用技术领域，为在用户登录账户时完成权限认证并显示权限对应的应用和数据而发明。所述方法包括：获取用户输入的密码，所述密码用于登录账户或解锁屏幕；根据预设的匹配关系表，获取所述密码对应的访问权限；查找所述密码对应的访问权限有权访问的应用和数据信息；显示所述密码对应访问权限有权访问的应用和数据信息。本发明主要应用于多用户登录同一系统时的信息保护。




CN 103427990 A

1. 一种权限认证的方法，其特征在于，包括：

获取用户输入的密码，所述密码用于登录账户或解锁屏幕；

根据预设的匹配关系表，获取所述密码对应的访问权限；

查找所述密码对应的访问权限有权访问的应用和数据信息；

显示所述密码对应访问权限有权访问的应用和数据信息。

2. 根据权利要求 1 所述的方法，其特征在于，在所述获取用户输入的密码前，所述方法进一步包括：

接收并保存所述用户设置的至少一个访问权限；

接收并保存所述用户设置的每个访问权限有权访问的应用和数据信息。

3. 根据权利要求 2 所述的方法，其特征在于，所述接收并保存所述用户设置的至少一个访问权限，包括：

接收并保存所述用户设置的网络管理员权限，所述网络管理员权限有权访问所有应用和数据信息，并且有权设置访问权限、每个访问权限有权访问的应用和数据信息以及密码与访问权限的映射关系。

4. 根据权利要求 3 所述的方法，其特征在于，在所述接收并保存所述用户设置的每个访问权限有权访问的应用和数据信息之后，所述方法进一步包括：

接收所述用户设置的所述密码与所述访问权限之间的映射关系，并将接收到的所述用户设置的所述密码与所述访问权限之间的映射关系保存到所述匹配关系表中，所述密码与所述访问权限之间的映射关系包括一个密码与一个访问权限之间一一映射的关系，或者一个密码集合与一个访问权限之间的映射关系。

5. 根据权利要求 4 所述的方法，其特征在于，当增加新用户时，所述方法进一步包括：

接收所述用户设置的所述新用户的密码与所述访问权限之间的映射关系，并将接收到的所述用户设置的所述新用户的密码与所述访问权限之间的映射关系保存到所述映射关系表中。

6. 根据权利要求 1 至 5 中任意一项所述的方法，其特征在于，所述密码为字符序列、图像、声音或指纹中的一种。

7. 一种终端设备，其特征在于，包括：

获取单元，用于获取用户输入的密码，所述密码用于登录账户或解锁屏幕；

匹配单元，用于根据预设的匹配关系表，获取所述获取单元获取的所述密码对应的访问权限；

查找单元，用于查找所述匹配单元获取的所述密码对应的访问权限有权访问的应用和数据信息；

显示单元，用于显示所述查找单元查找的所述密码对应访问权限有权访问的应用和数据信息。

8. 根据权利要求 7 所述的终端设备，其特征在于，所述终端设备还包括接收单元，用于接收所述用户设置的至少一个访问权限；

存储单元，用于保存所述接收单元接收的所述用户设置的至少一个访问权限。

9. 根据权利要求 8 所述的终端设备，其特征在于，所述接收单元进一步用于接收所述用户设置的每个访问权限有权访问的应用和数据信息；

所述存储单元进一步用于保存所述接收单元接收的所述用户设置的每个访问权限有权访问的应用和数据信息。

10. 根据权利要求 8 所述的终端设备，其特征在于，所述接收单元进一步用于接收所述用户设置的网络管理员权限，所述存储单元进一步用于保存所述接收单元接收的所述用户设置的网络管理员权限，所述网络管理员权限有权访问所有应用和数据信息，并且有权设置访问权限、每个访问权限有权访问的应用和数据信息以及设置密码与访问权限的映射关系。

11. 根据权利要求 10 所述的终端设备，其特征在于，所述接收单元进一步用于接收所述用户设置的所述密码与所述访问权限之间的映射关系；

所述存储单元进一步用于将所述接收单元接收的所述用户设置的所述密码与所述访问权限之间的映射关系保存在所述匹配关系表中；

其中，所述密码与所述访问权限之间的映射关系包括一个密码与一个访问权限之间一一映射的关系，或者一个密码集合与一个访问权限之间的映射关系。

12. 根据权利要求 11 所述的终端设备，其特征在于，当增加新用户时，所述接收单元进一步用于所述用户设置的所述新用户的密码与所述访问权限之间的映射关系；

所述存储单元进一步用于将所述接收单元接收到的所述用户设置的所述新用户的密码与所述访问权限之间的映射关系保存到所述映射关系表中。

# 权限认证的方法及终端设备

## 技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种权限认证的方法及终端设备。

## 背景技术

[0002] 目前电脑、手机等终端设备普遍采用账户（屏幕）锁定技术，用户在登录账户或屏幕解锁时需要输入预设密码，由此实现用户信息的安全保护。对于多操作系统终端设备，用户在登录不同操作系统时，需要输入不同的用户名及密码，由此实现操作系统的权限保护。

[0003] 上述锁定技术虽然可以实现对账户内容的保护，但都属于单权限锁定技术，即只区分用户是否有权登录账户，而对账户内的用户信息不作权限划分。在实际应用中，对于多用户使用同一台终端设备的场景，允许某些用户点击部分应用或数据，而对于某些敏感信息则不允许该部分用户查看。例如，不允许儿童使用网络浏览器，企业用户数据的隔离保护等。

[0004] 对于多权限的操作，现有技术中普遍采用为不同权限使用者设置禁止使用的应用和禁止访问的数据信息的方法，用户在登录账户或系统后，当点击应用或数据时，具有权限的用户可以直接打开访问，不具有权限的用户则被提示无法访问，从而实现多权限操作。

[0005] 在实现上述多权限操作的过程中，发明人发现现有技术中至少存在如下问题：用户在登录账户后无法直观获知哪些应用或数据无法访问，只有在点击应用或数据被提示无法访问时才可获知无权访问该应用或数据，频繁的尝试性点击以及禁止访问提示会降低用户的使用体验。

## 发明内容

[0006] 本发明的实施例提供一种权限认证的方法及终端设备，在用户登录账户后只显示该用户有权访问的应用和数据信息，能够提高用户的使用体验。

[0007] 一方面，本发明实施例提供了一种权限认证的方法，包括：

[0008] 获取用户输入的密码，所述密码用于登录账户或解锁屏幕；

[0009] 根据预设的匹配关系表，获取所述密码对应的访问权限；

[0010] 查找所述密码对应的访问权限有权访问的应用和数据信息；

[0011] 显示所述密码对应访问权限有权访问的应用和数据信息。

[0012] 另一方面，本发明实施例还提供了一种终端设备，包括：

[0013] 获取单元，用于获取用户输入的密码，所述密码用于登录账户或解锁屏幕；

[0014] 匹配单元，用于根据预设的匹配关系表，获取所述获取单元获取的所述密码对应的访问权限；

[0015] 查找单元，用于查找所述匹配单元获取的所述密码对应的访问权限有权访问的应用和数据信息；

[0016] 显示单元，用于显示所述查找单元查找的所述密码对应访问权限有权访问的应用和数据信息。

[0017] 本发明实施例提供的权限认证的方法及终端设备，能够根据密码获取用户的访问权限，在用户登录账户时只显示用户有权访问的应用和数据信息，从而不需要用户亲自点击才能区分有权和无权访问的应用及数据信息，并且减少了用户频繁的点击和减少了禁止访问的提示，从而可以提高用户的使用体验。

## 附图说明

[0018] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0019] 图 1 为本发明实施例中权限认证的方法流程图；

[0020] 图 2 为本发明另一个实施例中权限认证的方法流程图；

[0021] 图 3 为本发明实施例中终端设备的结构示意图；

[0022] 图 4 为本发明实施例中另一个终端设备的结构示意图。

## 具体实施方式

[0023] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0024] 本发明实施例提供了一种权限认证的方法，如图 1 所示，所述方法包括如下步骤：

[0025] 101、获取用户输入的密码。

[0026] 所述密码用于登录账户或解锁屏幕。

[0027] 102、根据预设的匹配关系表获取该密码对应的访问权限。

[0028] 所述匹配关系表用于表征用户输入的密码和访问权限之间的对应关系。

[0029] 103、查找该密码对应访问权限有权访问的应用和数据信息。

[0030] 104、显示该密码对应访问权限有权访问的应用和数据信息。

[0031] 当成功登录账户或解锁屏幕时，显示该密码对应访问权限有权访问的应用和数据信息，而对该密码对应访问权限无权访问的应用和数据信息则不予显示。由于不同的访问权限对应不同种类及数量的应用和数据信息，所以不同访问权限的用户登录账户后，账户中应用和数据信息的种类及数量就不相同，相当于，为用户建立个人账户环境。

[0032] 本发明实施例提供的权限认证的方法，能够根据密码获取用户的访问权限，在用户登录账户时只显示用户有权访问的应用和数据信息，而对于用户无权访问的应用和数据信息则不予显示，从而不需要用户亲自点击才能区分有权和无权访问的应用及数据信息，并且减少了用户频繁的点击和减少了禁止访问的提示，从而可以提高用户的使用体验。

[0033] 进一步的，作为对图 1 所示方法的进一步扩展，本发明实施例还提供了一种权限认证的方法。如图 2 所示，所述方法包括如下步骤：

[0034] 201、接收并保存用户设置的至少一个访问权限信息和用户设置的每个访问权限有权访问的应用和数据信息。

[0035] 在本实施例中，先由用户或管理员在终端设备上进行设置，可以设置至少一个访问权限，以及每个访问权限访问的应用和数据信息。终端设备再对用户或管理员的设置信息进行保存。

[0036] 例如，用户设置三个访问权限，访问权限 A 可以访问办公应用和全部文档数据，访问权限 B 可以访问办公应用、游戏应用以及网络应用，访问权限 C 可以访问网络应用和全部文档数据。

[0037] 此外，用户还可以为所有应用和文档数据设置访问级别，然后设置每个访问权限可以访问的访问级别。访问权限可以访问自身访问级别以下访问级别的所有应用和文档数据。例如，将网络应用的访问级别设置为 3 级，将游戏应用的访问级别设置为 2 级，将办公应用的访问级别设置为 1 级。设置访问权限 A 的访问级别为 3 级，即访问权限 A 可以访问网络应用、游戏应用及办公应用；设置访问权限 B 的访问级别为 2 级，即访问权限 B 可以访问游戏应用和办公应用；设置访问权限 C 的访问级别为 1 级，即访问权限 C 只可以访问办公应用。同理，当用户设置完后，终端设备需要保存用户的设置的所有应用和文档数据设置访问级别，以及设置的每个访问权限可以访问的访问级别。

[0038] 进一步的，用户还可以设置网络管理员权限，所述网络管理员权限为最高权限，可以访问所有的应用和文档数据，并且有权设置每个访问权限可以访问的应用和文档数据。当用户设置完后，终端设备需要保存用户设置的网络管理员权限。

[0039] 设置访问权限的用户为对终端设备具有最高访问权限的用户，所述网络管理员权限即为该用户的访问权限。例如对于公司中的电脑，领导或网管人员具有网络管理员权限，对于家庭用电脑，父母具有网络管理员权限。

[0040] 202、接收用户设置的密码与访问权限之间的映射关系信息，并将该用户设置的密码与访问权限之间的映射关系信息保存在匹配关系表中。

[0041] 具有网络管理员权限的用户可以设置匹配关系表，即设置密码与访问权限之间的映射关系。终端设备将用户设置的密码与访问权限之间的映射关系保存在匹配关系表中。

[0042] 此外，用户可以为每一个用户设置一个访问权限，再为该访问权限设置相应的密码，即用户需要设置一个密码与一个访问权限之间一一映射的关系，也可以为多个用户设置同一个访问权限，再为该访问权限设置多个密码，即一个密码集合与一个访问权限之间的对应关系。例如，为五个密码设置五个访问权限，每个密码对应一个访问权限。或者，为五个密码设置 3 个访问权限，三个密码对应一个访问权限，剩下两个密码分别对应一个访问权限。

[0043] 203、获取用户输入的密码。

[0044] 在用户登录账户或解锁屏幕时，获取用户的密码。

[0045] 204、根据预设的匹配关系表获取该密码对应的访问权限。

[0046] 根据步骤 202 中的匹配关系表以及步骤 203 中获取的密码，查找该密码对应的访问权限。

[0047] 205、查找所述访问权限有权访问的应用和数据信息。

[0048] 根据所述访问权限在已保存的每个访问权限有权访问的应用和数据信息中查找所述访问权限有权访问的应用和数据信息。

[0049] 206、显示所述访问权限有权访问的应用和数据信息。

[0050] 当用户成功登录账户或解锁屏幕时，显示该密码对应访问权限有权访问的应用和数据信息，而对该密码对应访问权限无权访问的应用和数据信息则不予显示。例如，密码 1 的访问权限为访问权限 B，则在登录账户或屏幕解锁后，显示办公应用、游戏应用以及网络应用，而文档数据则不予显示。

[0051] 进一步的，当有新用户增加时，还可以设置新用户密码与访问权限之间的映射关系，终端设备接收用户设备的新用户密码与访问权限之间的映射关系，并将接收的新用户密码与访问权限之间的映射关系保存到映射关系表中。具体的，用户可以为该新用户新设置一个访问权限，终端设备在匹配关系表中建立该新用户密码与新设置的访问权限之间映射关系。或者，用户在匹配关系表中为新用户密码选择一个已设置的访问权限，终端设备保存用户设置的新用户密码与已设置访问权限之间的映射关系。

[0052] 本发明实施例所述密码包括但不仅限于字符序列、图像、声音或指纹，本发明实施例对此不做限制。

[0053] 在本发明实施例的一个应用场景中，公司电脑中存储财务数据、人事数据以及销售数据，总经理、人事经理和销售经理通过各自密码登陆电脑操作系统查看相应数据。其中总经理密码的访问权限为网络管理员权限，可以查看财务数据、人事数据以及销售数据，人事经理密码的访问权限只可以查看人事数据，销售经理密码的访问权限只可以查看销售数据。当总经理登陆电脑操作系统时，电脑显示财务数据、人事数据以及销售数据，当人事经理登陆电脑操作系统时，电脑只显示人事数据，当销售经理登陆电脑操作系统时，电脑只显示销售数据。

[0054] 本发明实施例中有权设置访问权限、访问权限有权访问的内容以及用户密码与访问权限之间映射关系的用户，为对所述终端设备具有最高管理权的用户，例如该用户可以是具有网络管理员权限的用户。

[0055] 本发明实施例提供的权限认证的方法，能够根据密码获取用户的访问权限，在用户登录账户时只显示用户有权访问的应用和数据信息，而对于用户无权访问的应用和数据信息则不予显示，从而不需要用户亲自点击才能区分有权和无权访问的应用及数据信息，并且减少了用户频繁的点击和减少了禁止访问的提示，从而可以提高用户的使用体验。

[0056] 此外，本发明实施例提供的权限认证的方法，还允许用户设置根据用户的不同身份设置不同级别的访问权限。

[0057] 参考图 2 所示方法实施例，本发明实施例提供了一种终端设备，用以实现图 2 所示的方法实施例。所述终端设备包括但不仅限于台式电脑、笔记本电脑、手机、平板电脑，以及其他具有密码解锁或密码登录的数码设备。如图 3 所示，所述终端设备包括 ：获取单元 31、匹配单元 32、查找单元 33 以及显示单元 34，其中，

[0058] 所示获取单元 31，用于获取用户输入的密码，所述密码用于登录账户或解锁屏幕。对于触摸屏式终端设备，所述获取单元 31 可以为触摸屏幕 ；对于非触摸屏式终端设备，所述获取单元 31 可以为键盘。此外，当密码形式为图像或声音时，所述获取单元 31 还可以为摄像头或麦克风。

[0059] 所述匹配单元 32，用于根据预设的匹配关系表，获取所述获取单元 31 获取的密码对应的访问权限。所述匹配单元 32 可以为所述终端设备主板中具有匹配功能的芯片，或者集合匹配功能的处理器。

[0060] 所述查找单元 33，用于根据所述匹配单元 32 获取的该密码对应的所述访问权限，查找所述访问权限有权访问的应用和数据信息。所述查找单元 33 可以为所述终端设备主板中具有查找功能的芯片，或者集合查找功能的处理器。

[0061] 所述显示单元 34，用于显示所述查找单元 33 查找的所述访问权限有权访问的应用和数据信息，而对所述查找单元 33 查找的所述访问权限无权访问的应用和数据信息则不予显示。所述显示单元 34 可以为所述终端设备的屏幕。

[0062] 当用户成功登录账户或解锁屏幕时，所述显示单元 34 显示该密码对应访问权限有权访问的应用和数据信息，而对该密码对应访问权限无权访问的应用和数据信息则不予显示。例如，密码 1 的访问权限为访问权限 B，则在登录账户或屏幕解锁后，显示办公应用、游戏应用以及网络应用，而文档数据则不予显示。

[0063] 进一步的，如图 4 所示，所述终端设备还包括 ：

[0064] 接收单元 41，用于接收用户设置的至少一个访问权限，接收用户设置的每个访问权限有权访问的应用和数据信息。

[0065] 存储单元 42，用于保存所述接收单元 41 接收的用户设置的至少一个访问权限，以及用户设置的每个访问权限有权访问的应用和数据信息。

[0066] 例如，用户可以设置三个访问权限，访问权限 A 可以访问办公应用和全部文档数据，访问权限 B 可以访问办公应用、游戏应用以及网络应用，访问权限 C 可以访问网络应用和全部文档数据。所述存储单元 42 将用户设置的三个访问权限以及三个访问权限有权访问的应用户或文档数据进行保存。

[0067] 此外，所述接收单元 41 和所述存储单元 42 还可以分别接收和保存用户对所有应用和文档数据设置的访问级别，以及每个访问权限可以访问的访问级别。访问权限可以访问自身访问级别以下访问级别的所有应用和文档数据。例如，用户将网络应用的访问级别设置为 3 级，将游戏应用的访问级别设置为 2 级，将办公应用的访问级别设置为 1 级。设置访问权限 A 的访问级别为 3 级，即访问权限 A 可以访问网络应用、游戏应用及办公应用 ；设置访问权限 B 的访问级别为 2 级，即访问权限 B 可以访问游戏应用和办公应用 ；设置访问权限 C 的访问级别为 1 级，即访问权限 C 只可以访问办公应用。

[0068] 所述接收单元 41 还用于接收用户设置的网络管理员权限，所述存储单元 42 还用于存储所述接收单元 41 接收的用户设置的网络管理员权限，所述网络管理员权限有权访问所有应用和数据信息，并且有权设置访问权限、每个访问权限有权访问的应用和数据信息密码与访问权限的映射关系。

[0069] 所述接收单元 41 还用于接收用户设置的密码与访问权限之间的映射关系，所述存储单元 42 还用于将所述接收单元 41 接收的用户设置的密码与访问权限之间的映射关系保存到匹配关系表中，所述密码与访问权限之间的映射关系包括一个密码与一个访问权限之间一一映射的关系，或者一个密码集合与一个访问权限之间的映射关系。

[0070] 用户可以为每一个用户设置的一个访问权限，即一个密码与一个访问权限之间一一映射的关系，也可以为多个用户设置的同一个访问权限，即一个密码集合与一个访问权限之间的对应关系。例如，用户为五个密码设置五个访问权限，每个密码对应一个访问权限。或者，用户为五个密码设置 3 个访问权限，三个密码对应一个访问权限，剩下两个密码分别对应一个访问权限。所述存储单元 42 将用户的上述设置进行保存。

[0071] 进一步的，当增加新用户时，所述接收单元 41 还用于接收用户设置的新用户密码与访问权限之间的映射关系，所述存储单元 42 还用于保存所述接收单元 41 接收的用户设置的新用户密码与访问权限之间的映射关系。

[0072] 当有新用户增加时，用户可以为该新用户新设置一个访问权限，所述存储单元 42 在匹配关系表中保存该新用户密码与新设置的访问权限之间映射关系。或者，用户在匹配关系表中为新用户密码选择一个已设置的访问权限，所述存储单元 42 保存用户设置的新用户密码与已设置访问权限之间的映射关系。

[0073] 本发明实施例中有权设置访问权限、访问权限有权访问的内容以及用户密码与访问权限之间映射关系的用户，为对所述终端设备具有最高管理权的用户，例如该用户可以是具有网络管理员权限的用户。

[0074] 本发明实施例所述密码包括但不仅限于字符序列、图像、声音或指纹，本发明实施例对此不做限制。

[0075] 本发明实施例提供的终端设备，能够根据密码获取用户的访问权限，在用户登录账户时只显示用户有权访问的应用和数据信息，而对于用户无权访问的应用和数据信息则不予显示，从而不需要用户亲自点击才能区分有权和无权访问的应用及数据信息，并且减少了用户频繁的点击和减少了禁止访问的提示，从而可以提高用户的使用体验。

[0076] 此外，本发明实施例提供的终端设备，还允许用户设置根据用户的不同身份设置不同级别的访问权限。

[0077] 通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在可读取的存储介质中，如计算机的软盘，硬盘或光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述的方法。

[0078] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

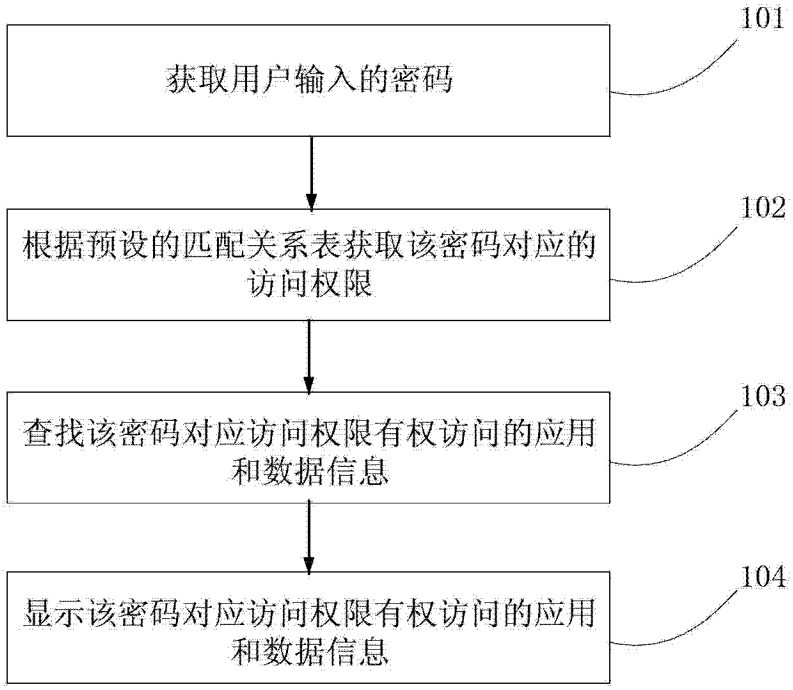

101
获取用户输入的密码
102
根据预设的匹配关系表获取该密码对应的访问权限
103
查找该密码对应访问权限有权访问的应用和数据信息
104
显示该密码对应访问权限有权访问的应用和数据信息

图 1

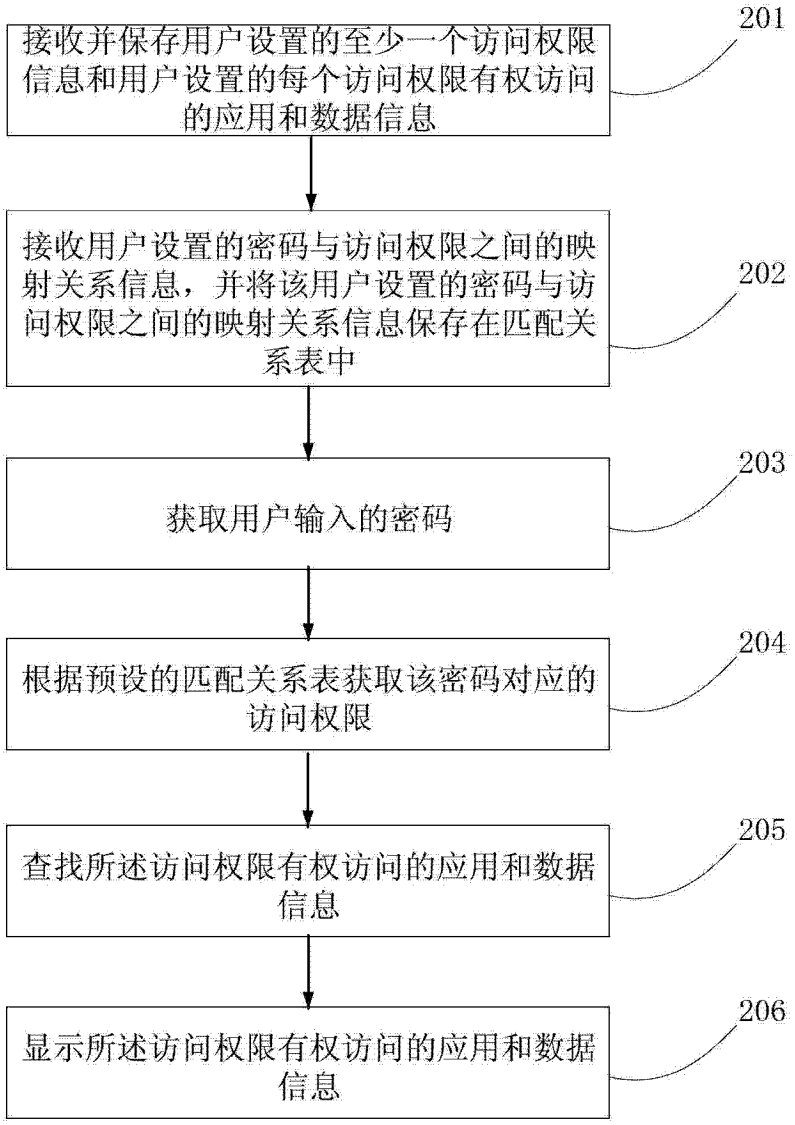

接收并保存用户设置的至少一个访问权限信息和用户设置的每个访问权限有权访问的应用和数据信息
201
接收用户设置的密码与访问权限之间的映射关系信息，并将该用户设置的密码与访问权限之间的映射关系信息保存在匹配关系表中
202
获取用户输入的密码
203
根据预设的匹配关系表获取该密码对应的访问权限
204
查找所述访问权限有权访问的应用和数据信息
205
显示所述访问权限有权访问的应用和数据信息
206

图 2

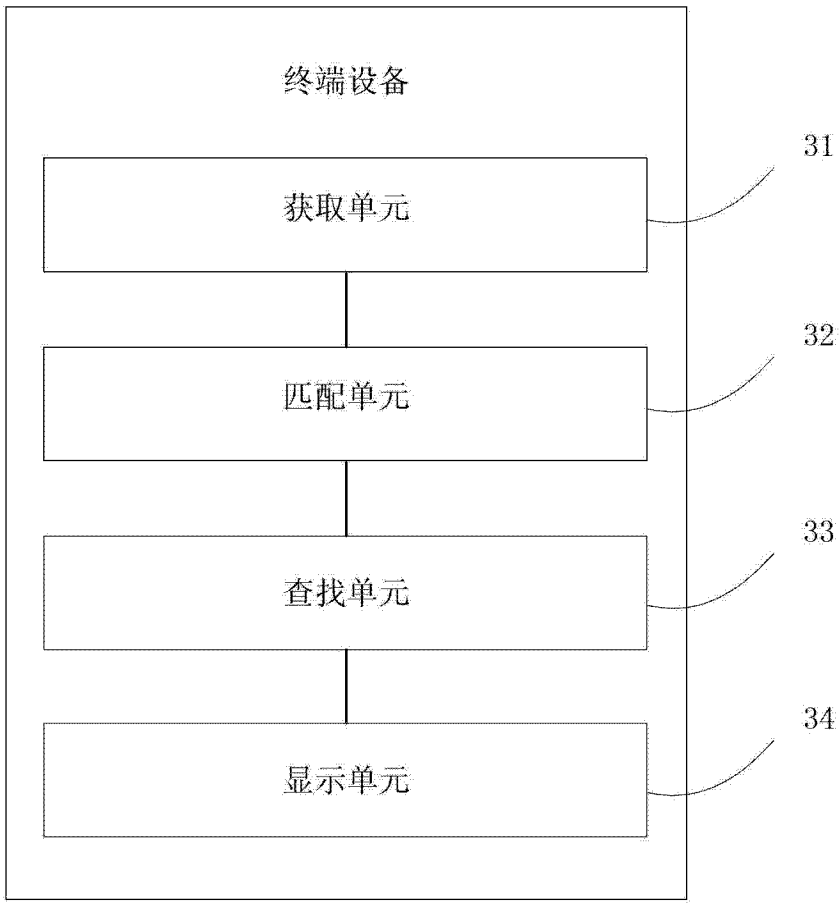



图 3

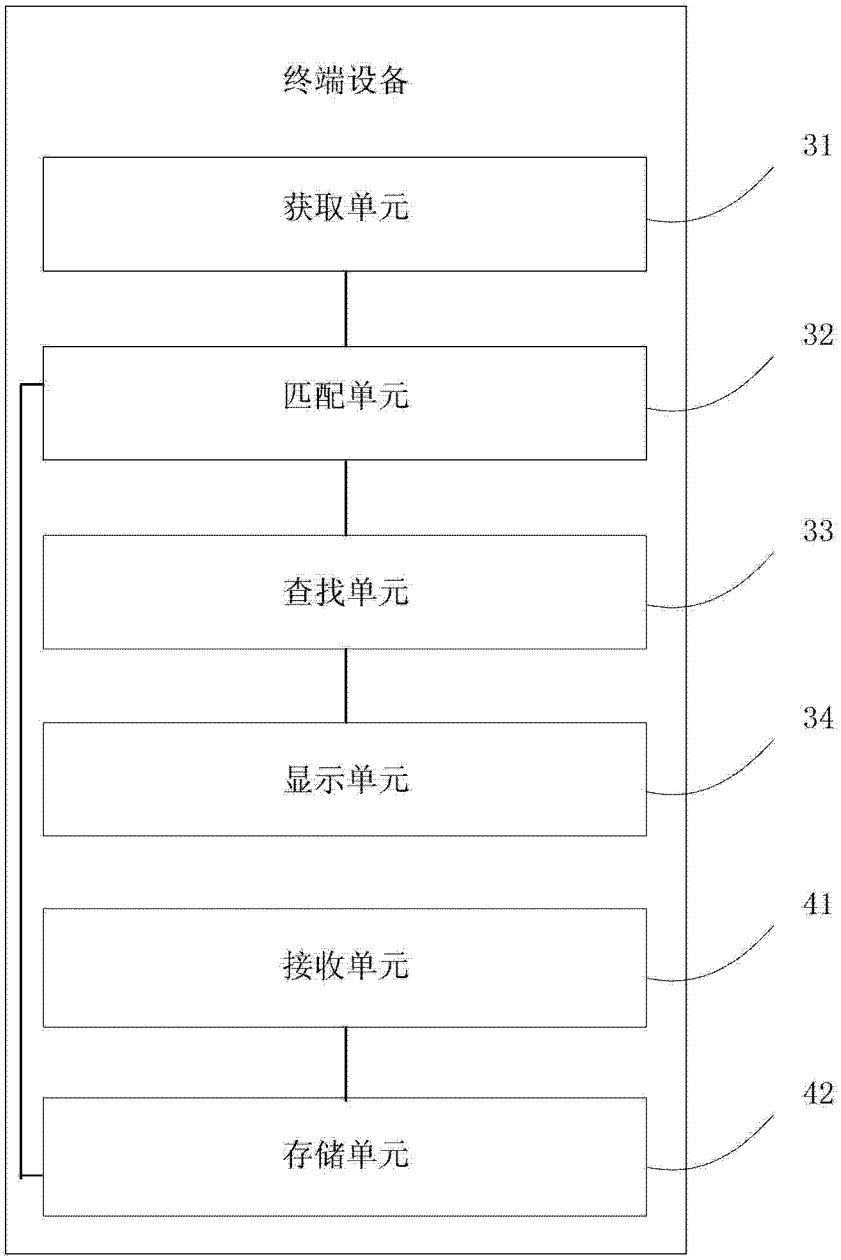



图 4