(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104318170 B
(45)授权公告日 2018.02.16

(21)申请号 201410522489.9

(22)申请日 2014.09.29

(65)同一申请的已公布的文献号
申请公布号 CN 104318170 A

(43)申请公布日 2015.01.28

(73)专利权人 广东欧珀移动通信有限公司
地址 523860 广东省东莞市长安镇乌沙海滨路18号

(72)发明人 俞义

(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 路凯 胡彬

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

(56)对比文件
US 2012/0246739 A1,2012.09.27,说明书第[0007]-[0066]段,附图2,权利要求6.
CN 103473514 A,2013.12.25,说明书第[0025]-[0043]段,附图1.
CN 101212239 A,2008.07.02,说明书第3页第1- 5段,附图1.
CN 102955917 A,2013.03.06,全文.
CN 103647587 A,2014.03.19,全文.
US 2007/0115113 A1,2007.05.24,全文.
CN 101063991 A,2007.10.31,全文.
Dirar Abu-Saymeh etc..An Application Security Framework for Near Field Communication.《2013 12th IEEE Conference on Trust, Security and Privacy in Computing and Communications》.2013,第396页右栏倒数第二段,398页右栏第一段,399页右栏倒数第二段,图5.

审查员 唐季超

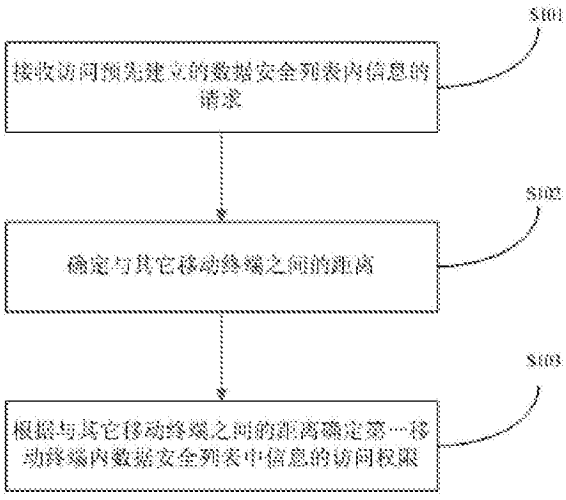
权利要求书3页 说明书11页 附图8页

(54)发明名称

一种基于多移动终端保护数据安全的方法及装置

(57)摘要

本发明公开了一种基于多移动终端保护数据安全的方法及装置,所述的基于多移动终端保护数据安全的方法包括:接收访问预先建立的数据安全列表内信息的请求;确定与其它移动终端之间的距离;根据与其它移动终端之间的距离确定数据安全列表中信息的访问权限。采用本实施例提供的技术方案,对于移动终端内的隐私数据和应用可以进行更好的保护,尤其在一个移动终端丢失的情况下,可以更好的保护用户的数据,同时,对于用户对于隐私数据和应用的访问也提供了更好的便利性。



CN 104318170 B

1.一种基于多移动终端保护数据安全的方法,包括:

接收访问预先建立的数据安全列表内信息的请求;

确定与绑定的其它移动终端之间的距离;

如果与所述的绑定的其它移动终端之间的距离不大于设定值,则按照原有数据安全保护方式对数据安全列表中的数据安全进行保护;如果与所述的绑定的其它移动终端之间的距离大于设定值,则将数据安全列表中的数据及应用进行加密,并关闭NFC功能;

其中,所述其他移动终端与当前移动终端为同一用户所携带,所述距离指示当前移动终端与所述其他移动终端是否都在用户的控制范围内,所述设定值的设置满足既能够考虑到所述距离的误差的影响,同时也不会对移动终端是否还处于用户的控制范围内的判断造成影响;

在确定与所述的绑定的其它移动终端之间的距离大于设定值之后,将数据安全列表中的数据及应用进行加密,并关闭NFC功能之前还包括:

检测与所述的绑定的其它移动终端的连接状态,如果与所述的绑定的其它移动终端未连接,则将数据安全列表中的数据及应用进行加密,并关闭NFC功能;

如果与所述的绑定的其它移动终端已连接,则检测是否能够得到所述的绑定的其它移动终端的对于数据安全列表中信息访问的许可,如果能够得到许可,则按照原有数据安全保护方式对数据安全列表中的数据安全进行保护;如果没有得到许可,则将数据安全列表中的数据及应用进行加密,并关闭NFC功能。

2.根据权利要求1所述的基于多移动终端保护数据安全的方法,其特征在于:所述的数据安全列表包括以下的一种或多种信息:隐私数据、重要应用、近距离无线通信技术NFC钱包。

3.根据权利要求1所述的基于多移动终端保护数据安全的方法,其特征在于:所述的确定与绑定的其它移动终端之间的距离具体包括:

测定当前移动终端的位置;

测定绑定的其它移动终端的位置;

计算与所述的绑定的其它移动终端之间的距离。

4.根据权利要求1所述的基于多移动终端保护数据安全的方法,其特征在于:所述的绑定的其它移动终端为可穿戴设备。

5.一种基于多移动终端保护数据安全的方法,包括:

接收访问预先建立的数据安全列表内信息的请求;

确定与绑定的其它移动终端的直接连接状态;

如果与绑定的其它移动终端能够直接连接,则按照原有数据安全保护方式对数据安全列表中的数据安全进行保护;如果与绑定的其它移动终端不能直接连接,则将数据安全列表中的数据及应用进行加密,并关闭NFC功能;

其中,在确定与绑定的其它移动终端不能直接连接之后,将数据安全列表中的数据及应用进行加密,并关闭NFC功能之前具体还包括:

检测与所述的绑定的其它移动终端的间接连接状态,如果与所述的绑定的其它移动终端未间接连接,则将数据安全列表中的数据及应用进行加密,并关闭NFC功能;

如果与所述的绑定的其它移动终端已间接连接,则检测是否能够得到所述的绑定的其

它移动终端的对于数据安全列表中信息访问的许可，如果能够得到许可，则按照原有数据安全保护方式对数据安全列表中的数据安全进行保护；如果没有得到许可，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能。

6.根据权利要求5所述的基于多移动终端保护数据安全的方法，其特征在于：所述的与其它移动终端直接连接包括以下任意一种连接方式：

WIFI直连、蓝牙配对连接、NFC连接。

7.根据权利要求6所述的基于多移动终端保护数据安全的方法，其特征在于：所述的绑定的其它移动终端为可穿戴设备。

8.一种基于多移动终端保护数据安全的装置，其特征在于，包括：

请求接收单元，用于接收访问预先建立的数据安全列表内信息的请求；

距离确定单元，用于确定与绑定的其它移动终端之间的距离；

访问权限确定单元，用于如果与所述的绑定的其它移动终端之间的距离不大于设定值，则按照原有数据安全保护方式对数据安全列表中的数据安全进行保护；如果与所述的绑定的其它移动终端之间的距离大于设定值，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能；

其中，所述其他移动终端与当前移动终端为同一用户所携带，所述距离指示当前移动终端与所述其他移动终端是否都在用户的控制范围内，所述设定值的设置满足既能够考虑到所述距离的误差的影响，同时也不会对移动终端是否还处于用户的控制范围内的判断造成影响；

所述的访问权限确定单元还具体用于：在确定与所述的绑定的其它移动终端之间的距离大于设定值之后，将数据安全列表中的数据及应用进行加密，并关闭NFC功能之前，检测与所述的绑定的其它移动终端的连接状态，如果与所述的绑定的其它移动终端未连接，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能；如果与所述的绑定的其它移动终端已连接，则检测是否能够得到所述的绑定的其它移动终端的对于数据安全列表中信息访问的许可，如果能够得到许可，则按照原有数据安全保护方式对数据安全列表中的数据安全进行保护；如果没有得到许可，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能。

9.一种基于多移动终端保护数据安全的装置，其特征在于，包括：

请求接收单元，接收访问预先建立的数据安全列表内信息的请求；

连接状态确定单元，用于确定与绑定的其它移动终端直接连接状态；

访问权限确定单元，用于如果与绑定的其它移动终端能够直接连接，则按照原有数据安全保护方式对数据安全列表中的数据安全进行保护；如果与绑定的其它移动终端不能直接连接，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能；

其中，所述访问权限确定单元还具体用于：在确定与绑定的其它移动终端不能直接连接之后，将数据安全列表中的数据及应用进行加密，并关闭NFC功能之前，检测与所述的绑定的其它移动终端的间接连接状态，如果与所述的绑定的其它移动终端未间接连接，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能；如果与所述的绑定的其它移动终端已间接连接，则检测是否能够得到所述的绑定的其它移动终端的对于数据安全列表中信息访问的许可，如果能够得到许可，则按照原有数据安全保护方式对数据安全列表中的数

据安全进行保护；如果没有得到许可，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能。

一种基于多移动终端保护数据安全的方法及装置

技术领域

[0001] 本发明涉及数据安全领域，尤其涉及一种基于多移动终端保护数据安全的方法及装置。

背景技术

[0002] 移动互联网的快速发展给人们带来便利，也给个人信息安全带来严峻挑战。手机用户的通话记录、通讯录、账号、个人私密文件都面临着被窥视与窃取的风险。

[0003] 手机上的个人信息包括位置信息、通讯信息、账号密码信息以及存储文件信息等四大类。其中，通讯信息包括通讯录、通话记录、短信等，手机内存储文件信息包括机主的照片、录音、视频等文件。此外，手机的一些硬件信息，比如IMEI号(手机串号)、无线网卡的Mac地址、硬件配置信息也都属于个人信息的范畴。此外，一些涉及银行和财产的应用，例如支付宝、手机银行、NFC钱包等也与用户的个人信息安全密切相关，一般都会通过账户和密码对这些信息和应用进行保护。

[0004] 如果通过一个加密软件来对这些数据进行统一的加密，用户在使用手机上这些功能时，每次都需要输入密码，会给操作带来一定的不便。

[0005] 随着移动智能终端的普及，用户往往携带多个移动终端，如何利用用户的多移动终端动态的保护移动终端上的信息及应用的安全成为一个日益重要的课题。

发明内容

[0006] 本发明的目的在于提出一种基于多移动终端保护数据安全的方法及系统，以动态的保护移动终端上的信息，能够根据不同的情况调整安全策略，使得用户使用更加方便。

[0007] 为达此目的，本发明实施例采用以下技术方案：

[0008] 第一方面，提供一种基于多移动终端保护数据安全的方法，包括：

[0009] 接收访问预先建立的数据安全列表内信息的请求；

[0010] 确定与绑定的其它移动终端之间的距离；

[0011] 根据与绑定的其它移动终端之间的距离确定数据安全列表中信息的访问权限。

[0012] 第二方面，提供一种基于多移动终端保护数据安全的方法，包括：

[0013] 接收访问预先建立的数据安全列表内信息的请求；

[0014] 确定与绑定的其它移动终端的直接连接状态；

[0015] 根据与所述的绑定的其它移动终端的直接连接状态确定数据安全列表中信息的访问权限。

[0016] 第三方面，提供一种基于多移动终端保护数据安全的装置，包括：

[0017] 请求接收单元，用于接收访问预先建立的数据安全列表内信息的请求；

[0018] 距离确定单元，用于确定与绑定的其它移动终端之间的距离；

[0019] 访问权限确定单元，根据与所述的绑定的其它移动终端之间的距离确定数据安全列表中信息的访问权限。

[0020] 请求接收单元，用于接收访问预先建立的数据安全列表内信息的请求；

[0021] 距离确定单元，用于确定与绑定的其它移动终端之间的距离；

[0022] 访问权限确定单元，根据与所述的绑定的其它移动终端之间的距离确定数据安全列表中信息的访问权限。

[0023] 第四方面，提供一种基于多移动终端保护数据安全的装置，包括：

[0024] 请求接收单元，接收访问预先建立的数据安全列表内信息的请求；

[0025] 连接状态确定单元，用于确定与绑定的其它其它移动终端直接连接状态；

[0026] 访问权限确定单元，用于根据与所述的绑定的其它移动终端直接连接状态确定数据安全列表中信息的访问权限。

[0027] 采用本实施例提供的技术方案，对于移动终端内的隐私数据和应用可以进行更好的保护，尤其在一个移动终端丢失的情况下，可以更好的保护用户的数据，同时，对于用户对于隐私数据和应用的访问也提供了更好的便利性。

附图说明

[0028] 图1是本发明第一实施例提供的基于多移动终端保护数据安全的方法的流程示意图；

[0029] 图2是本发明第二实施例提供的基于多移动终端保护数据安全的方法的流程示意图；

[0030] 图3是本发明第三实施例提供的基于多移动终端保护数据安全的方法的流程示意图；

[0031] 图4是本发明第四实施例提供的基于多移动终端保护数据安全的装置的结构示意图；

[0032] 图5是本发明第五实施例提供的基于多移动终端保护数据安全的方法的流程示意图；

[0033] 图6是本发明第六实施例提供的基于多移动终端保护数据安全的方法的流程示意图；

[0034] 图7是本发明第七实施例提供的基于多移动终端保护数据安全的方法的流程示意图；

[0035] 图8是本发明第八实施例提供的基于多移动终端保护数据安全的装置的结构示意图。

具体实施方式

[0036] 为使本发明解决的技术问题、采用的技术方案和达到的技术效果更加清楚，下面将结合附图对本发明实施例的技术方案作进一步的详细描述，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。

[0037] 参考图1，图1是本发明第一实施例基于多移动终端保护数据安全的方法，其中，所述的移动终端指可以在移动中使用的计算机设备，广义的讲包括手机、笔记本、平板电脑、POS机甚至包括车载电脑。但是大部分情况下是指手机或者具有多种应用功能的智能手机

以及平板电脑。随着科技的发展，可穿戴设备也已成为智能终端的一种。由于可穿戴设备的便利性，易于被人所携带。更多时候作为所述的基于多移动终端保护数据安全的方法，包括：

[0038] 步骤S101，接收访问预先建立的数据安全列表内信息的请求；

[0039] 手机上的个人信息包括位置信息、通讯信息、账号密码信息以及存储文件信息等四大类。其中，通讯信息包括通讯录、通话记录、短信等，手机内存储文件信息包括机主的照片、录音、视频等文件。此外，手机的一些硬件信息，比如IMEI号(手机串号)、无线网卡的Mac地址、硬件配置信息也都属于个人信息的范畴。这些关系到用户个人安全的信息都需要进行相应的保护。可穿戴设备上检测人体健康的一些数据也需要得到保护。此外，一些涉及银行和财产的应用，例如支付宝、手机银行、NFC钱包等也需要进行加密保护。通过在移动终端内建立安全列表的方式，将以上的个人信息及涉及个人财产的相关应用加入到移动终端内的安全列表内，如果要访问安全列表中的相应信息和应用，必须通过验证及解密的方式。通过建立安全列表的方式，对用户的个人信息和重要应用进行保护。

[0040] 当用户通过操作要求对移动终端内的相应数据及要求进行访问时，移动终端会首先判定这些数据和应用是否属于前一步骤中安全列表中内的相应数据和应用，如果不属于安全列表中的数据和应用，则允许用户对其访问，如果属于安全列表中的数据和应用，则需要通过一些验证和解密的方式来确定用户是否可以访问这些数据和应用。

[0041] 步骤S102，确定与绑定的其它移动终端之间的距离。

[0042] 一般来说，用户可以采用携带多个移动终端，这些移动终端可以通过Mac地址或者其它方式绑定在一起。由于可穿戴设备可由用户穿戴在身上，便于携带，其中的用于绑定的配对的移动终端可以是可穿戴设备。如果用户所持有的多个移动终端距离都在一定的范围内，就说明这些移动终端还都在用户的控制范围内，并没有丢失，对用户的个人信息和重要应用的操作都是用户自己所进行的操作，对于这些操作可以视作是安全的操作。

[0043] 确定与其它移动终端的距离，可以首先确定两个智能终端的相应位置，确定智能终端的位置可以有多种方式，例如智能终端中大多内置有GPS模块，通过GPS模块可以快速准确的对移动终端进行定位，还可以采用移动运营网的基站定位方法对智能终端进行定位，基站定位则是利用基站对手机的距离的测算距离来确定手机位置的。此外还可以利用WIFI在小范围内定位来获取智能终端的位置。

[0044] 通过上一步骤获取的两个智能终端的位置，可以计算出与其它移动智能终端之间的距离。

[0045] 步骤S103，根据与所述的绑定的其它移动终端之间的距离确定数据安全列表中信息的访问权限。

[0046] 通过上一步骤获取的与其它移动终端之间的距离，可以判断出移动终端是否都在用户的控制范围内，如果在用户控制范围内，可以认定为是用户要求访问于安全列表中的数据和应用，可以相应采用较简单的安全验证策略进行验证，如果判断移动终端其中一个或多个不在用户控制范围内，应该采用相应的高级别的安全列表中的数据和应用的安全保护。

[0047] 本实施例通过接收访问预先建立的数据安全列表内信息的请求；确定与绑定的其它移动终端之间的距离；根据与所述的绑定的其它终端之间的距离确定数据安全列表中信

息的访问权限，能够根据获取到的移动终端的位置来获取移动终端之间的距离，通过移动终端之间的距离进而判断移动终端是否还在用户所控制的范围，并根据是否在用户控制的范围来确定对移动终端内安全列表内的信息及应用的访问采用不同的安全策略，能够对于移动终端内的数据和应用进行更好的保护，同时，在确认移动终端都在用户的控制范围下，也可方便用户访问数据及应用，可有选择性的要求用户输入密码来对数据和应用进行访问。

[0048] 图2示出了本发明第二实施例。

[0049] 图2是本发明第一实施例基于多移动终端保护数据安全的方法的流程示意图，所述的基于多移动终端保护数据安全的方法以本发明第一实施例为基础，进一步的，将所述的根据移动终端之间的距离确定数据安全列表中信息的访问权限进一步优化为：如果移动终端之间的距离不大于设定值，则按照原有数据安全保护方式对数据安全进行保护；如果移动终端之间的距离大于设定值，则将第数据安全列表中的数据及应用进行加密，并关闭NFC功能。

[0050] 所述的基于多移动终端保护数据安全的方法包括：

[0051] 步骤S201，接收访问预先建立的数据安全列表内信息的请求。

[0052] 将需要保密的数据信息及应用放入数据安全列表中，通过建立安全列表的方式，对用户的个人信息和重要应用进行保护。智能终端获取用户通过操作要求对移动终端内的相应数据及要求进行访问的请求。

[0053] 步骤S202，确定与绑定的其它移动终端之间的距离。

[0054] 通过获取移动终端的相应位置，进而获取到与其它移动终端之间的距离。

[0055] 步骤S203，判断与所述的绑定的其它移动终端之间的距离是否大于预设值，如果大于预设值，则转入步骤S204，如果不大于预设值则转到步骤S205。

[0056] 对于上一步骤所获取的与所述的绑定的移动终端之间的距离与预设值进行比较。预设值的设定综合考虑到对于移动终端的定位误差，预设值应该既能满足由于定位误差所导致的计算出的移动终端之间的距离错误，同时也能够准确的判断出移动终端是否还在用户的控制范围内。在本实例中，可以将预设值设定为200m，这样既能够考虑到误差的影响，同时也不会对移动终端是否还处于用户的控制范围内的判断造成影响。

[0057] 步骤S204，将数据安全列表中的数据及应用进行加密，并关闭NFC功能。

[0058] 如果与绑定的移动终端之间的距离大于预设值，则可以判断出移动终端中至少有一个已经不在用户所控制的范围内，可能意味着对数据和应用的访问请求并不是用户所作出的，这时候需要对数据和应用进行高级别的保护。对于数据安全列表中的数据及应用应进行加密，对于类似NFC钱包支付这种无需输入支付密码的应用，应该将其关闭。

[0059] 步骤S205，按照原有数据安全保护方式对数据安全进行保护。

[0060] 如果移动终端之间的距离不大于预设值，则可以判断出移动终端都在用户所控制的范围内，对于数据和应用的访问操作时用户自己本身所作出的，对于数据和应用的访问是安全的。这时，对于数据及应用的访问安全策略的设定可以沿用移动终端原有的数据及应用的安全保护方式对数据及应用安全进行保护，例如，原有对移动终端内的数据及应用保护都需要输入相应的密码才可访问，则在访问保护的数据和应用时，仍需输入相应的密码才可访问，如果原有的原有对移动终端内的数据及应用保护为可以直接访问，则在访问

保护的数据和应用时，也可直接访问。

[0061] 本实施例通过对将所述的根据移动终端之间的距离确定数据安全列表中信息的访问权限进一步优化为：如果与绑定的移动终端之间的距离不大于设定值，则按照原有数据安全保护方式对数据安全进行保护；如果移动终端之间的距离大于设定值，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能。在一个移动终端丢失的情况下，对于移动终端内的数据和应用安全能够进行更好的保护。如果没有丢失，可以简化用户操作的相应步骤，提高了用户体验。

[0062] 图3示出了本发明第三实施例。

[0063] 图3是本发明第三实施例基于多移动终端保护数据安全的方法的流程示意图，所述的基于多移动终端保护数据安全的方法以本发明第二实施例为基础，进一步的，在确定与绑定的移动终端之间的距离大于设定值之后，将数据安全列表中的数据及应用进行加密，并关闭NFC功能之前还包括：

[0064] 检测与所述的绑定的其它移动终端的连接状态，如果与所述的绑定的其它移动终端未连接，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能；

[0065] 如果与所述的绑定的其它移动终端已连接，则检测是否能够得到所述的绑定的其它移动终端的对于数据安全列表中信息访问的许可，如果能够得到许可，则按照原有数据安全保护方式对数据安全列表中的数据安全进行保护；如果没有得到许可，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能。所述的基于多移动终端保护数据安全的方法，包括：

[0066] 步骤S301，接收访问预先建立的数据安全列表内信息的请求。

[0067] 将需要保密的数据信息及应用放入数据安全列表中，通过建立安全列表的方式，对用户的个人信息和重要应用进行保护。智能移动终端获取用户通过操作要求对移动终端内的相应数据及要求进行访问的请求。

[0068] 步骤S302，确定与绑定的其它移动终端之间的距离。

[0069] 通过获取移动终端的相应位置，进而获取到与绑定的其它移动终端之间的距离。

[0070] 步骤S303，判断与所述的绑定的移动终端之间的距离是否大于预设值，如果大于预设值，则转入步骤S304，如果不大于预设值则转到步骤S305。

[0071] 将移动终端之间的距离与预设值进行比较，根据不同的比较结果转入不同的处理步骤。

[0072] 步骤S304，按照原有数据安全保护方式对数据安全进行保护。

[0073] 步骤S305，检测与所述的绑定的其它移动终端连接状态，如果与所述的绑定的其它移动终端未连接，则转入步骤S308，如果与所述的绑定的其它移动终端已连接，则转入步骤S306。

[0074] 对于已经与所述的绑定的其它移动终端之间的距离大于预设值的，可以分为两种情况，第一，某一移动终端可能被盗或者丢失，已经不在用户的控制范围内；第二，由于用户的疏忽，导致并未同时携带多个移动终端，但都在其控制下，使得移动终端之间的距离大于预设值，在这种情况下，如果用户仍然需要访问受保护的个人信息或者应用时，可以通过互联网或者其它的连接方式来对受保护的个人信息数据及应用进行访问。

[0075] 步骤S306，检测是否能够得到所述的绑定的其它移动终端的对于数据安全列表中

信息访问的许可，如果能够得到许可，转到步骤S304，如果不能得到许可，则转到步骤S307。

[0076] 当移动终端通过互联网或者其它方式连接后，用户需要访问受保护的个人信息数据及应用时，需要得到绑定的其它移动终端的相应确认，这样可以确保由于移动终端之间的距离大于设定值，用户对于受保护的个人信息数据及应用的访问要求是由用户自己所提出时，可以完成对受保护的个人信息数据及应用的访问。

[0077] 如果能够接收到所述的绑定的其它移动终端所发出的对于受保护的个人信息数据和应用访问请求的许可，则说明此两件移动终端还仍在用户的控制下，对受保护的个人信息数据和应用访问请求是由用户自己所做出的，可以认为这时对受保护的个人信息数据和应用访问请求是安全的，可以按照原有数据安全保护方式对数据安全进行保护。

[0078] 步骤S307，将数据安全列表中的数据及应用进行加密，并关闭NFC功能。

[0079] 如果不能够接收到所述的绑定的移动终端所发出的对于受保护的个人信息数据和应用访问请求的许可，则说明至少有一个移动终端已经不在用户的控制下，这时对受保护的个人信息数据和应用访问请求是危险的，应该将移动终端内数据安全列表中的数据及应用进行加密，并关闭NFC功能。

[0080] 本实施例通过在确定移动终端之间的距离大于设定值之后，将数据安全列表中的数据及应用进行加密，并关闭NFC功能之前还包括：检测是否能够得到所述的绑定的其它移动终端的对于数据安全列表中信息访问的许可，如果能够得到许可，则按照原有数据安全保护方式对数据安全列表中的数据安全进行保护；如果没有得到许可，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能。在移动终端与绑定的其它移动终端之间的距离大于设定值的情况下，通过连接确认的方式方便用户对受保护的个人信息数据及应用的访问。方便用户对受保护的个人信息数据及应用的访问。

[0081] 图4示出了本发明第四实施例。

[0082] 图4是本发明第四实施例基于多移动终端保护数据安全的装置的结构图。

[0083] 由图4可以看出，所述的基于多移动终端保护数据安全的装置包括：数据请求接收单元401、距离确定单元402、访问权限确定单元403。其中

[0084] 所述的请求接收单元，用于接收访问预先建立的数据安全列表内信息的请求；

[0085] 所述的距离确定单元，用于确定与绑定的移动终端之间的距离；

[0086] 所述的访问权限确定单元，用于根据与所述的绑定的移动终端之间的距离确定数据安全列表中信息的访问权限。

[0087] 进一步的，所述的访问权限确定单元具体用于：如果与所述的绑定的其它移动终端之间的距离小于设定值，则按照原有数据安全保护方式对数据安全进行保护；如果与所述的绑定的其它移动终端之间的距离大于设定值，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能。

[0088] 更进一步的，所述的访问权限确定单元还具体用于：所所述的在确定与所述的绑定的其它移动终端之间的距离大于设定值之后，将数据安全列表中的数据及应用进行加密，并关闭NFC功能之前还包括：

[0089] 检测与所述的绑定的其它移动终端的连接状态，如果与所述的绑定的其它移动终端未连接，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能；

[0090] 如果与所述的绑定的其它移动终端已连接，则检测是否能够得到所述的绑定的其

它移动终端的对于数据安全列表中信息访问的许可，如果能够得到许可，则按照原有数据安全保护方式对数据安全列表中的数据安全进行保护；如果没有得到许可，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能。

[0091] 上述基于多移动终端保护数据安全的装置可执行本发明实施例所提供的基于多移动终端保护数据安全的的方法，具备执行方法相应的功能模块和有益效果。

[0092] 图5示出了本发明第五实施例。

[0093] 图5是本发明第五实施例基于多移动终端保护数据安全的方法的流程示意图。

[0094] 所述的基于多移动终端保护数据安全的方法，包括：

[0095] 步骤S501，接收访问预先建立的数据安全列表内信息的请求；

[0096] 将需要保密的数据信息及应用放入数据安全列表中，通过建立安全列表的方式，对用户的个人信息和重要应用进行保护。

[0097] 智能移动终端获取用户通过操作对移动终端内的相应数据及要求进行访问的请求。

[0098] 步骤S502，确定与绑定的其它移动终端直接连接状态。

[0099] 移动终端可以通过直接连接进行连接，一般可以采用WIFI直连、蓝牙配对以及NFC连接等方式直接连接。以上三种连接方式都要求两个移动终端要保持在一定的范围之内才可以连接成功，当两个移动终端设备距离较远时，两个移动终端设备是无法直接连接成功的。当两个移动终端设备能够连接成功时，说明此两个移动终端在同一范围内，对于数据和应用的访问操作时用户自己本身所作出的，对于受保护的个人信息数据和应用的访问是安全的。

[0100] 步骤S503，根据与所述的绑定的其它移动终端直接连接状态确定数据安全列表中信息的访问权限。

[0101] 通过上一步骤获取的与绑定的其它移动终端的直接连接状态，可以判断出此两个移动终端是否都在用户的控制范围内，如果移动终端都在用户控制范围内，可以认定为是用户要求访问于安全列表中的数据和应用，可以相应采用较简单的安全验证策略进行验证，如果判断出移动终端中一个或多个不在用户控制范围内，应该采用相应的高级别的安全列表中的数据和应用的安全保护。

[0102] 本实施例通过建立数据安全列表；接收访问数据安全列表内信息请求；确定与其它移动终端的直接连接状态；根据与绑定的其它移动终端的直接连接状态确定数据安全列表中信息的访问权限，通过对与所述的绑定的其它移动终端的直接连接状态来判断移动终端是否都在用户控制的范围来确定安全列表内的信息及应用的访问采用不同的安全策略，能够对于移动终端内的数据和应用进行更好的保护，与第一实施例相比，简化了移动终端是否在用户的控制范围内的判断，对于移动终端内的数据和应用进行更好的保护。

[0103] 图6示出了本发明第六实施例。

[0104] 图6是本发明第六实施例基于多移动终端保护数据安全的方法的流程示意图。所述的基于多移动终端保护数据安全的方法以本发明第五实施例为基础，进一步的，将所述的根据与绑定的其它移动终端的直接连接状态确定数据安全列表中信息的访问权限进一步优化为：如果与绑定的其它终端能够直接连接，则按照移动终端原有数据安全保护方式对数据安全进行保护；如果与绑定的其它终端不能直接连接，则将移动终端内数据安全列

表中的数据及应用进行加密，并关闭NFC功能。

[0105] 所述的基于多移动终端保护数据安全的方法，包括：

[0106] 步骤S601，接收访问预先建立的数据安全列表内信息的请求；

[0107] 将需要保密的数据信息及应用放入数据安全列表中，通过建立安全列表的方式，对用户的个人信息和重要应用进行保护。

[0108] 智能移动终端获取用户通过操作对移动终端内的相应数据及要求进行访问的请求。

[0109] 步骤S602，确定与绑定的其它移动终端直接连接状态，如果不能够直接连接，则转入步骤S603，如果能够直接连接则转到步骤S604。

[0110] 确定与绑定的其它移动终端通过WIFI直连、蓝牙配对以及NFC连接等方式能否直接连接，并根据能否直接连接，选择不同的安全策略。

[0111] 步骤S603，将数据安全列表中的数据及应用进行加密，并关闭NFC功能。

[0112] 如果与所述的绑定的其它移动终端无法直接连接，则可以判断出至少有一个移动终端已经不在用户所控制的范围内，可能意味着对数据和应用的访问请求并不是用户所作出的，这时候需要对数据和应用进行高级别的保护。对于数据安全列表中的数据及应用应进行加密，对于类似NFC钱包支付这种无需输入支付密码的应用，应该将其关闭。

[0113] 步骤S604，按照原有数据安全保护方式对数据安全进行保护。

[0114] 如果与所述的绑定的其它移动终端能够直接连接，则可以判断出移动终端都在用户所控制的范围内，对于数据和应用的访问操作时用户自己本身所作出的，对于数据和应用的访问是安全的。这时，对于数据及应用的访问安全策略的设定可以沿用原有的数据及应用的安全保护方式对数据及应用安全进行保护，例如，原有对移动终端内的数据及应用保护都需要输入相应的密码才可访问，则在访问保护的数据和应用时，仍需输入相应的密码才可访问，如果原有的原有对移动终端内的数据及应用保护为可以直接访问，则在访问保护的数据和应用时，也可直接访问。

[0115] 本实施例通过对绑定的多个移动终端能否直接连接来确定相应的数据和应用保护策略。能够在一个移动终端丢失的情况下，对于移动终端内的数据和应用安全能够进行更好的保护。如果没有丢失，可以简化用户操作的相应步骤，提高了用户体验。

[0116] 图7示出了本发明第七实施例。

[0117] 图7是本发明第七实施例基于多移动终端保护数据安全的方法的流程示意图，所述的基于多移动终端保护数据安全的方法以本发明第六实施例为基础，进一步的，在确定与其它移动终端不能直接连接之后，将数据安全列表中的数据及应用进行加密，并关闭NFC功能之前还包括：

[0118] 检测与其它移动终端连接状态，如果与其它移动终端未连接，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能；

[0119] 如果与其它移动终端已连接，则则检测是否能够得到所述的绑定的其它移动终端的对于数据安全列表中信息访问的许可，如果能够得到许可，则原有数据安全保护方式对数据安全进行保护；如果没有得到许可，则将数据安全列表中的数据及应用进行加密。

[0120] 所述的基于多移动终端保护数据安全的方法，包括：

[0121] 步骤S701，接收访问预先建立的数据安全列表内信息的请求；

[0122] 在本实施例中，所述的多移动终端为手机和可穿戴设备，手机和可穿戴设备分别将需要保密的数据信息及应用放入数据安全列表中，通过建立安全列表的方式，对用户的个人信息和重要应用进行保护。手机和可穿戴设备可以分别获取用户通过操作要求对手机和可穿戴设备内的相应数据及应用进行访问的请求。

[0123] 步骤S702，确定与绑定的其它移动终端直接连接状态，如果不能够直接连接，则转入步骤704，如果能够直接连接则转到步骤703。

[0124] 手机和可穿戴设备进行绑定，并确定手机与可穿戴设备的能否通过WIFI直连、蓝牙配对以及NFC连接等方式直接连接。并根据能否直接连接确定后续的处理步骤。

[0125] 步骤S703，按原有数据安全保护方式对数据安全进行保护。

[0126] 手机和可穿戴设备距离较近，连接正常时，按原有数据安全保护方式对数据安全进行保护在这里分为两种情况：如果可穿戴设备没有对手机以及手机对穿戴设备都没有设置数据保护，则手机在使用中访问保护的数据，或者打开保护的应用程序时，不需要输入密码，直接可以进行访问；如果可穿戴设备对手机以及手机对穿戴设备都设置了数据保护，则手机在使用中访问保护的数据，或者打开保护的应用程序时，需要输入密码，可穿戴设备在访问保护的数据或者应用程序时，也需要输入密码。

[0127] 步骤S704，检测与绑定的其它移动终端间接连接状态，如果与其它移动终端未能间接连接，则转入步骤S706，如果与其它移动终端能够间接连接，则转入步骤S705。

[0128] 对于已经确定手机与可穿戴设备无法直接连接的，可以分为两种情况，第一，手机与可穿戴设备中某一移动终端可能被盗或者丢失，已经不在用户的控制范围内；第二，由于用户的疏忽，导致并未同时携带手机与可穿戴设备，但都在其控制下，由于距离的原因使得手机和可穿戴设备无法直接连接，在这种情况下，如果用户仍然需要访问手机和可穿戴设备中的受保护的个人信息或者应用时，可以通过间接连接方式来对受保护的个人信息数据及应用进行访问。这里所说的间接连接，是指手机和可穿戴设备通过互联网或者移动网络或其它方式与所述的绑定的其它移动终端建立的相应连接。

[0129] 步骤S705，检测是否能够得到所述的绑定的其它移动终端的对于数据安全列表中信息访问的许可，如果得到许可，转到步骤S703，如果没有得到许可，则转到步骤S706。

[0130] 当手机与可穿戴设备通过互联网或者其它方式连接后，用户需要访问手机或者可穿戴设备中受保护的个人信息数据及应用时，需要得到相应的所绑定的其它移动终端的相应确认，例如需要访问手机中受保护的个人信息数据及应用必须得到可穿戴设备所发出的许可，或者访问可穿戴设备中受保护的个人信息数据及应用要得到手机的许可。这样可以确保由于绑定的手机与可穿戴设备之间的距离过大，无法直接连接，对于用户对于受保护的个人信息数据及应用的访问要求是由用户自己所提出的情况，能够保证用户能够访问安全信息列表中的个人信息和应用。

[0131] 手机如果能够接收到绑定的可穿戴设备所发出的对于受保护的个人信息数据和应用访问请求的许可，则说明可穿戴设备还仍在用户的控制下，对受保护的个人信息数据和应用访问请求是由用户自己所做出的，可以认为这时对受保护的个人信息数据和应用访问请求是安全的，可以按照原有数据安全保护方式对数据安全进行保护。

[0132] 步骤S706，提示与绑定的移动终端无法间接连接，并将数据安全列表中的数据及应用进行加密，并关闭NFC功能。

[0133] 可穿戴设备和手机距离超出连接范围时，并且没有通过互联网或者其他方式相连接，手机和可穿戴设备会有相应提示用户，使用户能够了解当前可穿戴设备与手机的状态。可穿戴设备和手机距离超出连接范围时，并且没有通过互联网或者其他方式相连接则说明可穿戴设备和手机至少有一个移动终端已经不在用户的控制下，这时对受保护的个人信息数据和应用访问请求是危险的，应该将数据安全列表中的数据及应用进行加密，并关闭NFC功能。

[0134] 本实施例通过对在所述的基于多移动终端保护数据安全的方法在确定与绑定的其它移动终端不能直接连接之后，将数据安全列表中的数据及应用进行加密，并关闭NFC功能之前具体还包括：检测与所述的绑定的其它移动终端的间接连接状态，如果与所述的绑定的其它移动终端未间接连接，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能；如果与所述的绑定的其它移动终端已间接连接，则检测是否能够得到所述的绑定的其它移动终端的对于数据安全列表中信息访问的许可，如果能够得到许可，则按照原有数据安全保护方式对数据安全列表中的数据安全进行保护；如果没有得到许可，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能。增加的相应步骤能够在用户忘记同时携带多个移动终端，使移动终端之间无法直接连接的情况下，通过连接确认的方式方便用户对受保护的个人信息数据及应用的访问。方便用户对受保护的个人信息数据及应用的访问。

[0135] 图8示出了本发明第八实施例。

[0136] 图8是本发明第八实施例基于多移动终端保护数据安全的装置的结构图。

[0137] 由图8可以看出，所述的基于多移动终端保护数据安全的装置包括：请求接收单元801、连接状态确定单元802、访问权限确定单元803。其中

[0138] 所述的请求接收单元，用于接收访问预先建立的数据安全列表内信息的请求；

[0139] 所述的连接状态确定单元，用于确定与其它终端直接连接状态；；

[0140] 所述的访问权限确定单元，用于根据与其它终端直接连接状态确定数据安全列表中信息的访问权限。

[0141] 进一步的，所述的访问权限确定单元具体用于：所述的根据与其它移动终端直接连接状态确定数据安全列表中信息的访问权限具体包括：

[0142] 如果与其它移动终端能够直接连接，则按照原有数据安全保护方式对数据安全进行保护；如果与其它移动终端不能直接连接，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能。

[0143] 更进一步的，所述的访问权限确定单元还具体用于：在确定与绑定的其它移动终端不能直接连接之后，将数据安全列表中的数据及应用进行加密，并关闭NFC功能之前具体还包括：

[0144] 检测与所述的绑定的其它移动终端的间接连接状态，如果与所述的绑定的其它移动终端未间接连接，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能；

[0145] 如果与所述的绑定的其它移动终端已间接连接，则检测是否能够得到所述的绑定的其它移动终端的对于数据安全列表中信息访问的许可，如果能够得到许可，则按照原有数据安全保护方式对数据安全列表中的数据安全进行保护；如果没有得到许可，则将数据安全列表中的数据及应用进行加密，并关闭NFC功能。上述基于多移动终端保护数据安全的装置可执行本发明实施例所提供的基于多移动终端保护数据安全的的方法，具备执行方法

相应的功能模块和有益效果。

[0146] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0147] 本领域普通技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个计算装置上，或者分布在多个计算装置所组成的网络上，可选地，他们可以用计算机装置可执行的程序代码来实现，从而可以将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件的结合。

[0148] 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，各个实施例之间的相同或相似的部分互相参见即可。

[0149] 以上所述仅为本发明的优选实施例，并不用于限制本发明，对于本领域技术人员而言，本发明可以有各种改动和变化。凡在本发明的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

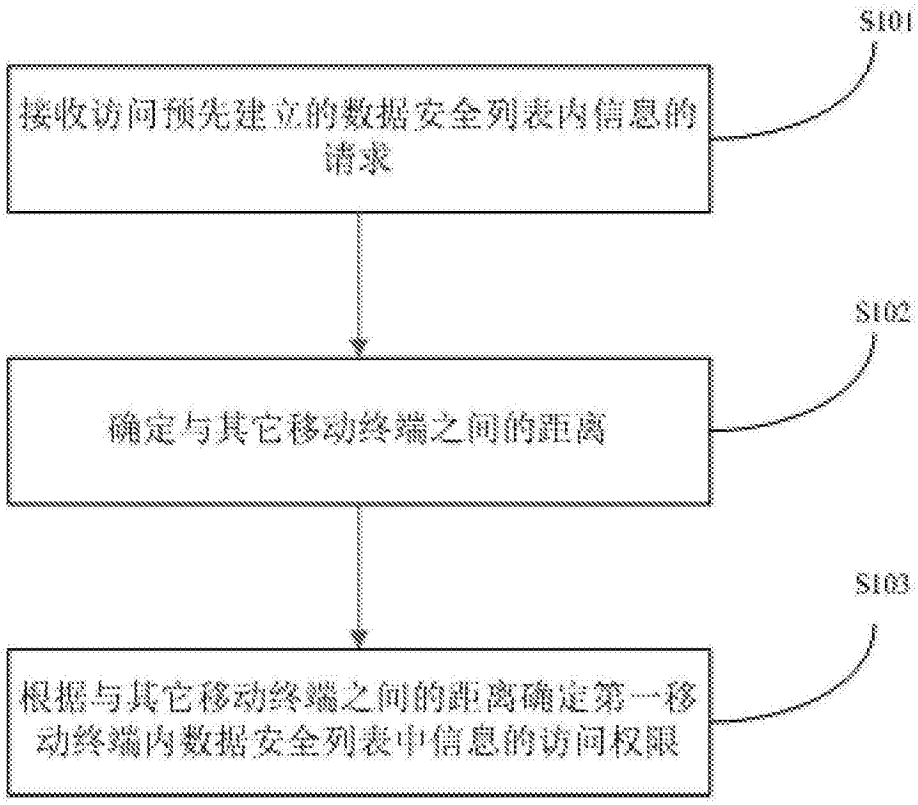

S101
接收访问预先建立的数据安全列表内信息的请求
S102
确定与其它移动终端之间的距离
S103
根据与其它移动终端之间的距离确定第一移动终端内数据安全列表中信息的访问权限

图1

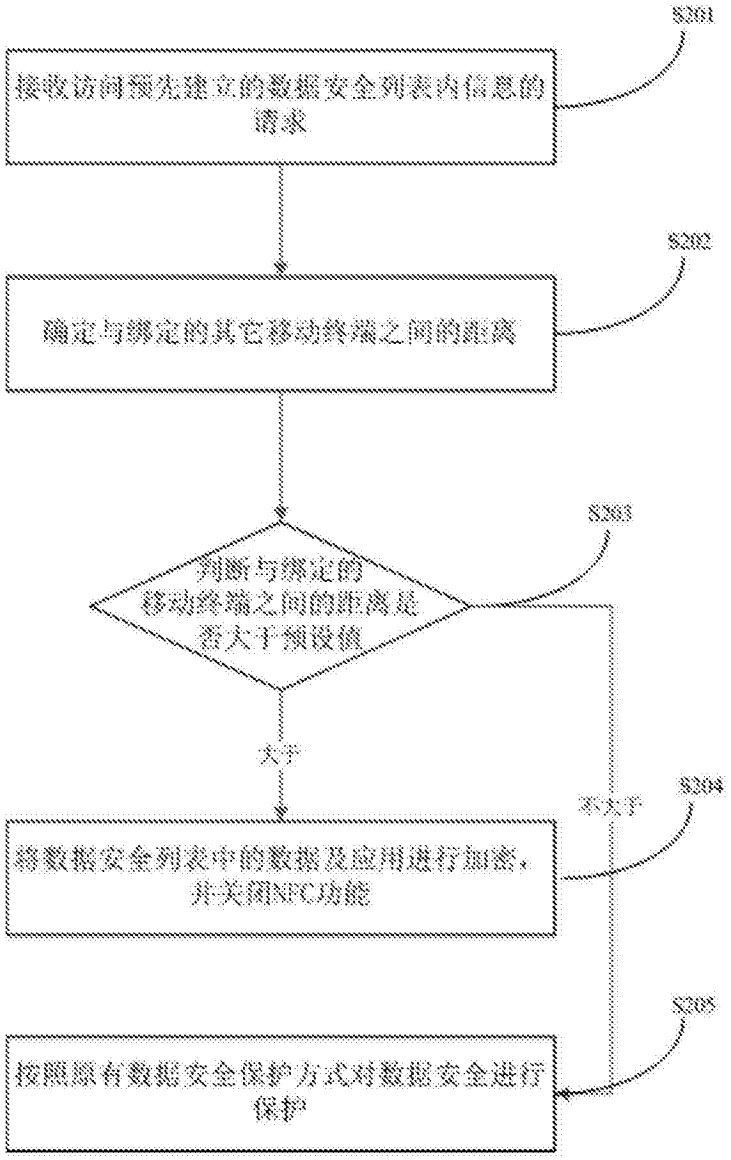

S201
接收访问预先建立的数据安全列表内信息的请求
S202
确定与绑定的其它移动终端之间的距离
S203
判断与绑定的移动终端之间的距离是否大于预设值
大于
不大于
S204
将数据安全列表中的数据及应用进行加密，并关闭NFC功能
S205
按照原有数据安全保护方式对数据安全进行保护

图2

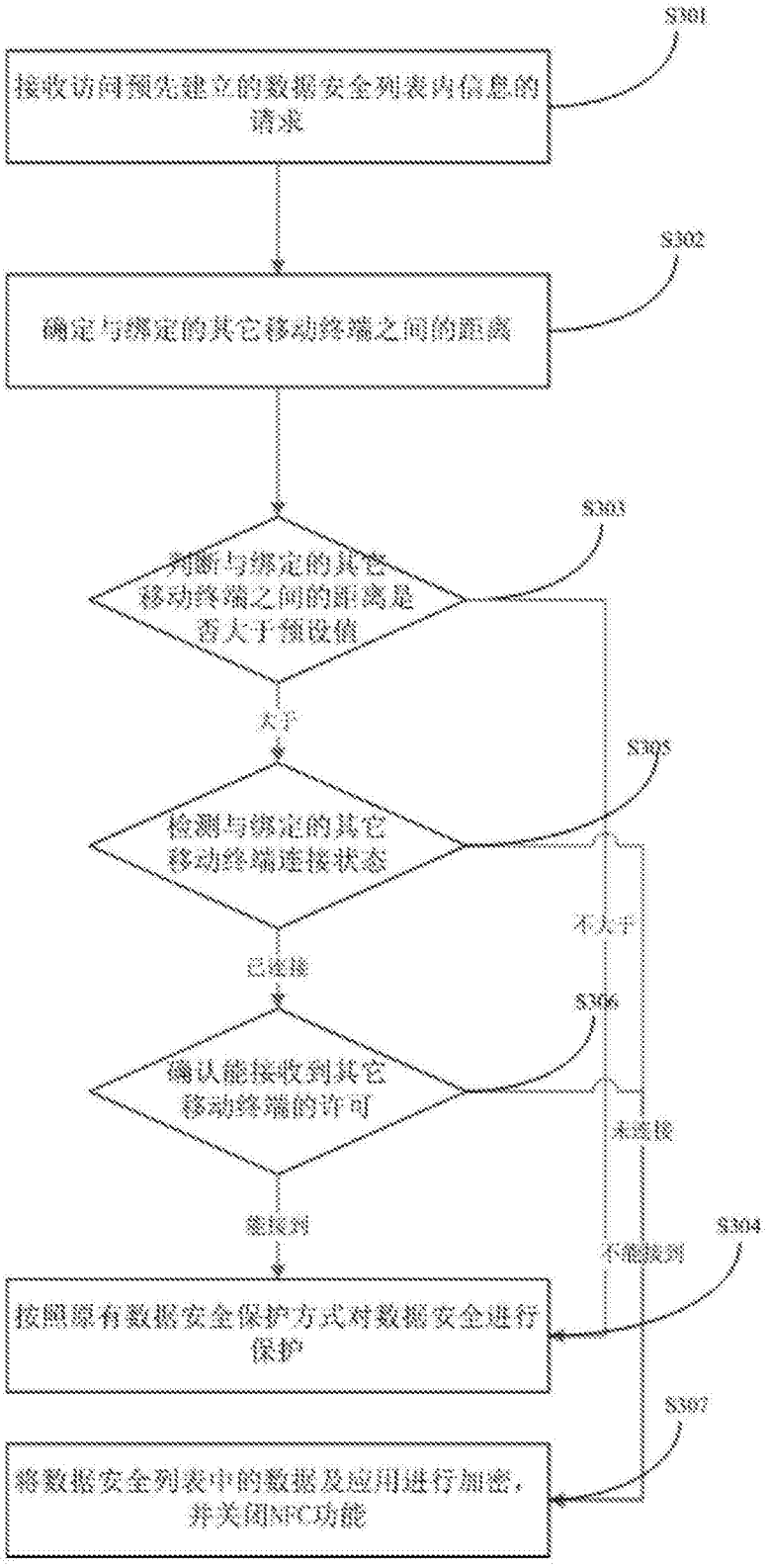

S301
接收访问预先建立的数据安全列表内信息的请求
S302
确定与绑定的其它移动终端之间的距离
S303
判断与绑定的其它移动终端之间的距离是否大于预设值
大于
S305
检测与绑定的其它移动终端连接状态
不大于
已连接
S306
确认能接收到其它移动终端的许可
未连接
能接收到
不能接收到
S304
按照原有数据安全保护方式对数据安全进行保护
S307
将数据安全列表中的数据及应用进行加密，并关闭NFC功能

图3

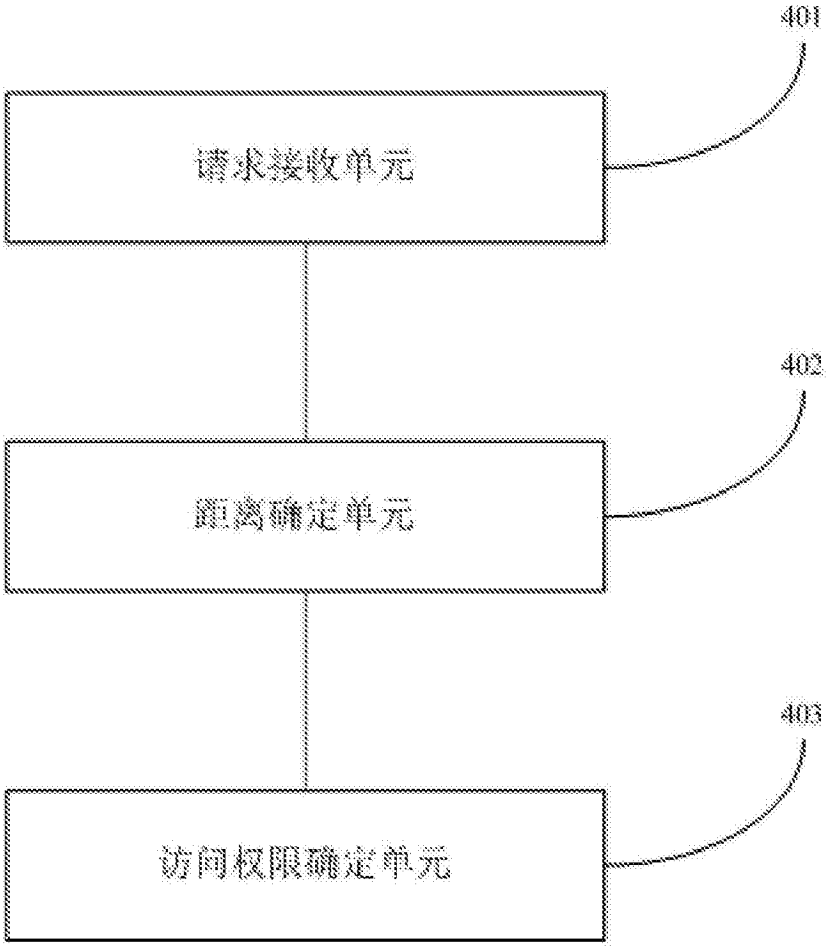


图4

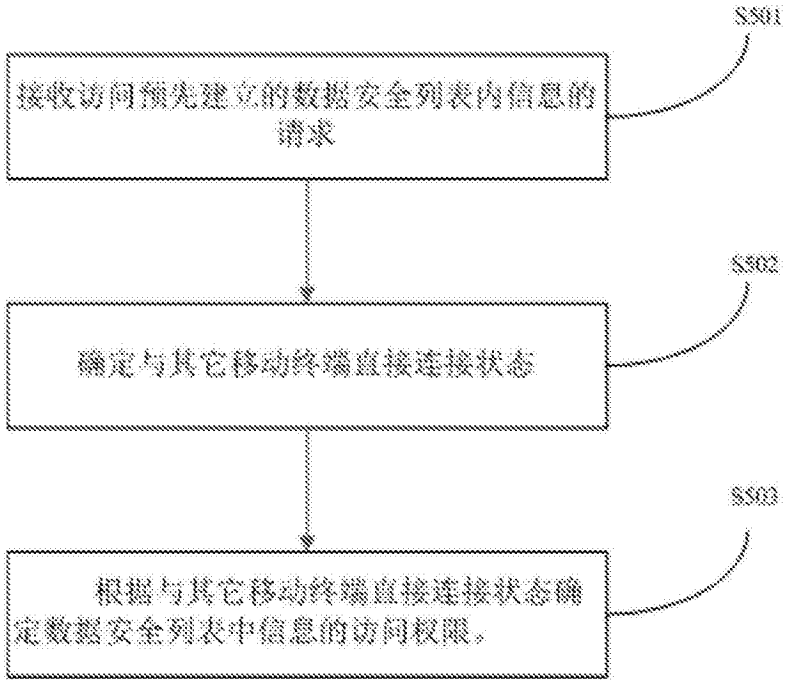

S501
接收访问预先建立的数据安全列表内信息的请求
S502
确定与其它移动终端直接连接状态
S503
根据与其它移动终端直接连接状态确定数据安全列表中信息的访问权限。

图5

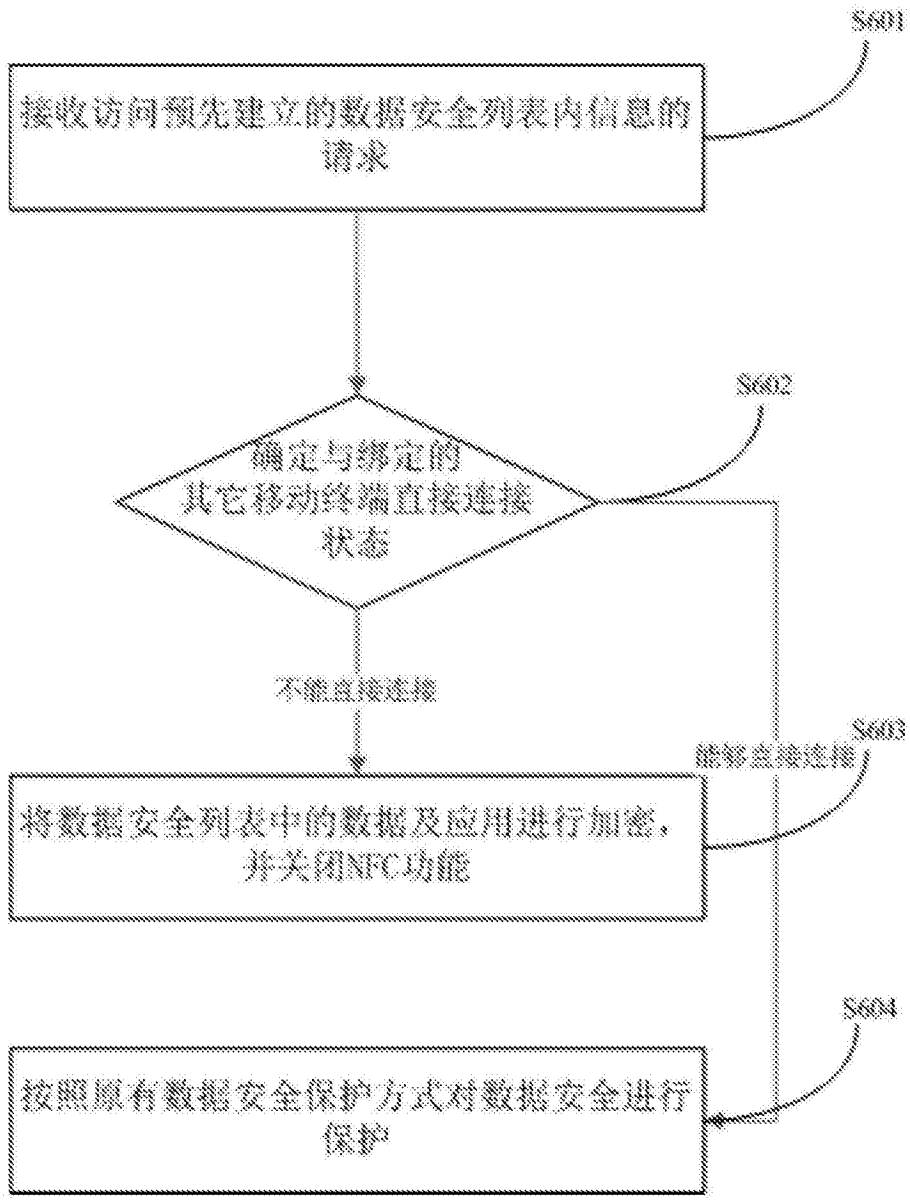

S601
接收访问预先建立的数据安全列表内信息的请求
S602
确定与绑定的其它移动终端直接连接状态
不能直接连接
能够直接连接
S603
将数据安全列表中的数据及应用进行加密，并关闭NFC功能
S604
按照原有数据安全保护方式对数据安全进行保护

图6

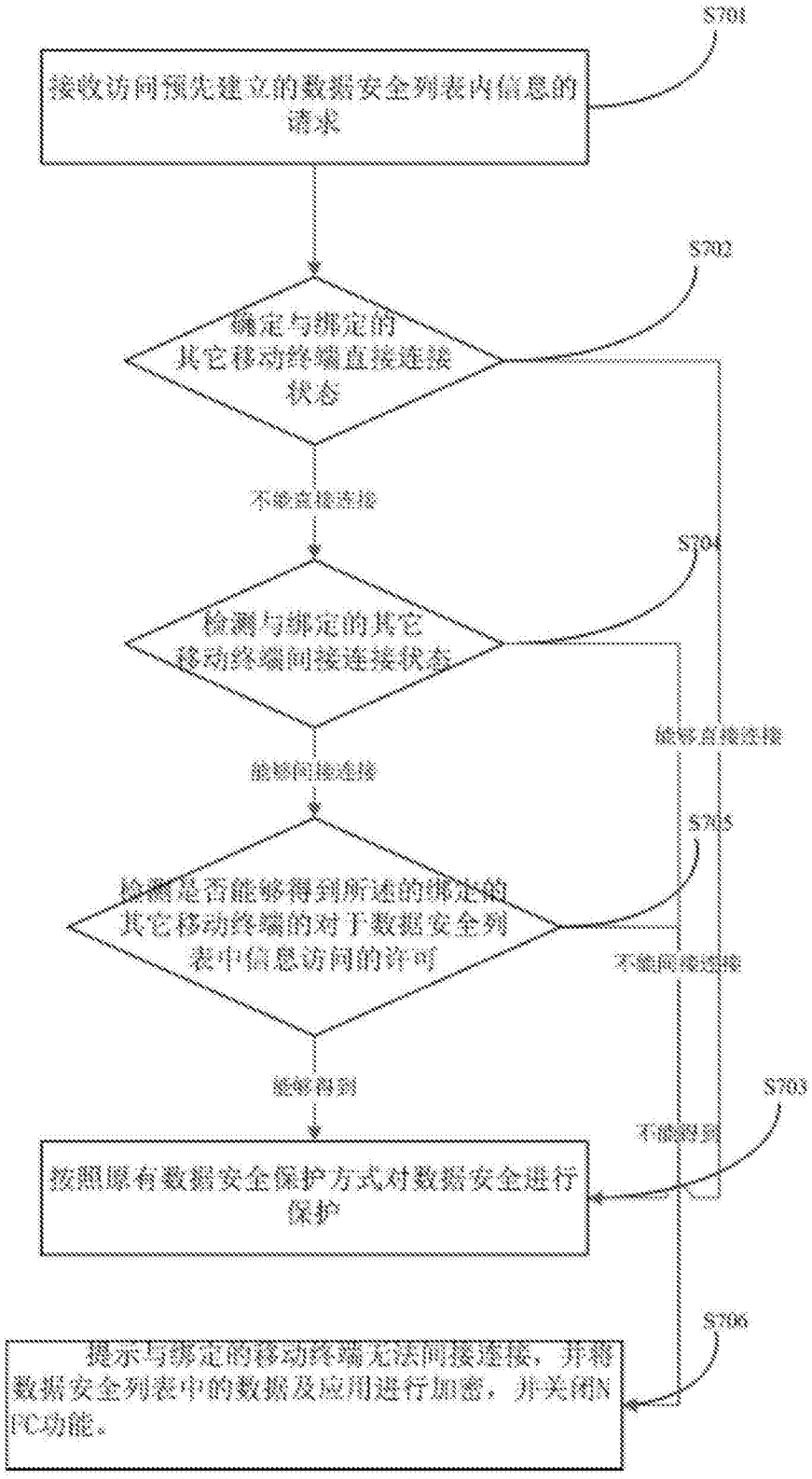

S701
接收访问预先建立的数据安全列表内信息的请求
S702
确定与绑定的其它移动终端直接连接状态
不能直接连接
S704
检测与绑定的其它移动终端间接连接状态
能够直接连接
能够间接连接
S705
检测是否能够得到所述的绑定的其它移动终端的对于数据安全列表中信息访问的许可
不能间接连接
能够得到
S703
不能得到
按照原有数据安全保护方式对数据安全进行保护
S706
提示与绑定的移动终端无法间接连接，并将数据安全列表中的数据及应用进行加密，并关闭NFC功能。

图7

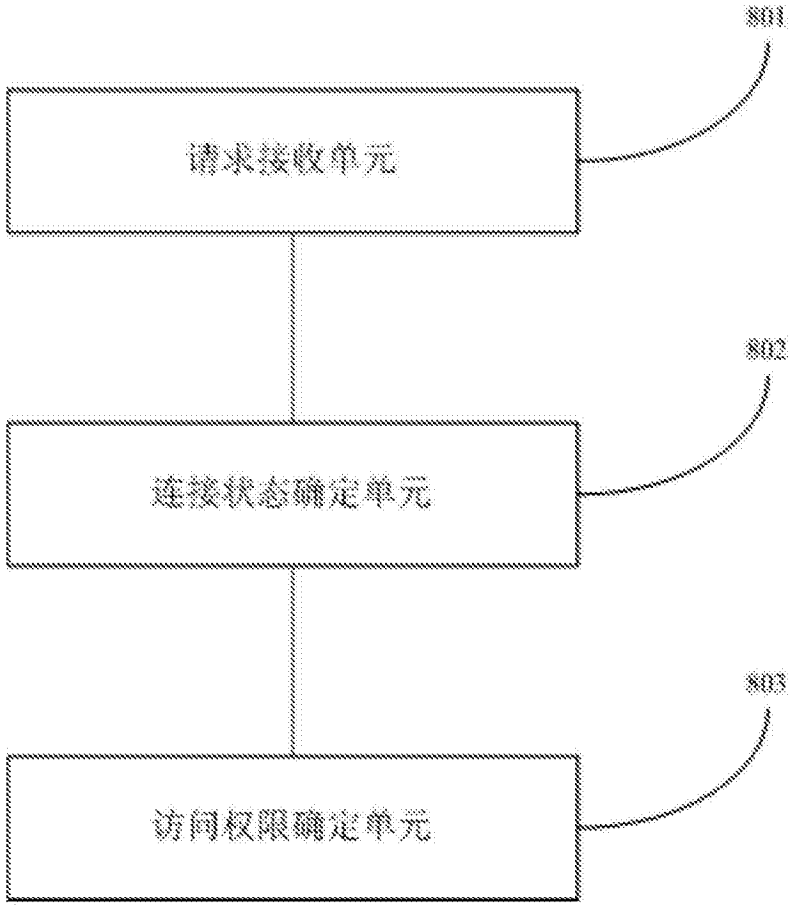


图8