(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 106022106 A
(43)申请公布日 2016.10.12

(21)申请号 201610369865.4

(22)申请日 2016.05.30

(71)申请人 努比亚技术有限公司
地址 518000 广东省深圳市南山区高新区北环大道9018号大族创新大厦A区6-8层、10-11层、B区6层、C区6-10层

(72)发明人 袁强

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 王花丽 张颖玲

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

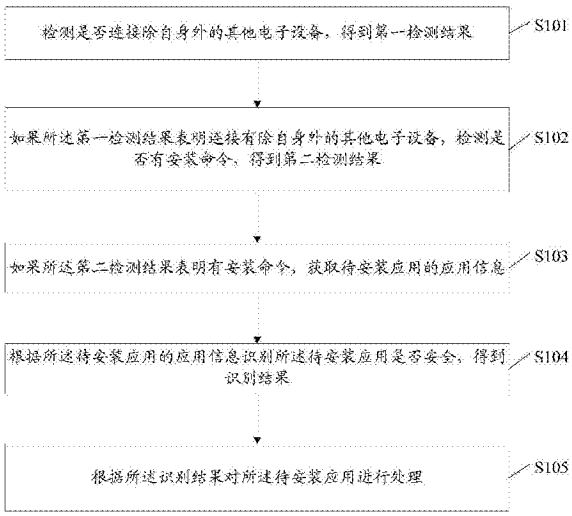
权利要求书2页 说明书14页 附图6页

(54)发明名称

一种应用安装方法及装置、终端

(57)摘要

本发明公开了一种应用安装方法及装置、终端，其中，所述方法包括：检测是否连接除自身外的其他电子设备，得到第一检测结果；如果所述第一检测结果表明连接有除自身外的其他电子设备，检测是否有安装命令，得到第二检测结果，所述安装命令用于安装应用；如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息；根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果；根据所述识别结果对所述待安装应用进行处理。



CN 106022106 A

1.一种应用安装方法,其特征在于,所述方法包括:

检测是否连接有除自身外的其他电子设备,得到第一检测结果;

如果所述第一检测结果表明连接有除自身外的其他电子设备,检测是否有安装命令,得到第二检测结果,所述安装命令用于安装应用;

如果所述第二检测结果表明有安装命令,获取待安装应用的应用信息;

根据所述待安装应用的应用信息识别所述待安装应用是否安全,得到识别结果;

根据所述识别结果对所述待安装应用进行处理。

2.根据权利要求1所述的方法,其特征在于,所述根据所述待安装应用的应用信息识别所述待安装应用是否安全,得到识别结果,包括:

将所述待安装应用的应用信息与黑名单中应用的信息进行比较,得到识别结果,所述识别结果表明当前安装的应用是否为黑名单中的应用。

3.根据权利要求1所述的方法,其特征在于,所述根据所述待安装应用的应用信息识别所述待安装应用是否安全,得到识别结果,包括:

根据所述待安装应用的应用信息生成查询请求,所述查询请求用于请求查询所述待安装应用是否安全;

将所述查询请求发送给服务器;

接收所述服务器发送的查询响应,所述查询响应中携带有识别结果;

解析所述查询响应,得到所述识别结果。

4.根据权利要求2所述的方法,其特征在于,所述黑名单以数据库或者XML文件形式存储在本地;所述方法还包括:

周期性或非周期性的更新所述黑名单。

5.根据权利要求1至4任一项所述的方法,其特征在于,所述根据所述识别结果对所述待安装应用进行处理,包括:

如果所述识别结果表明所述待安装应用安全时,安装所述待安装应用,或者;

如果所述识别结果表明所述待安装应用安全时,输出第一提示信息并且安装所述待安装应用,所述第一提示信息用于提示所述待安装应用为安全的应用。

6.根据权利要求1至4任一项所述的方法,其特征在于,所述根据所述识别结果对所述待安装应用进行处理,包括:

如果所述识别结果表明所述待安装应用不安全时,停止所述待安装应用并输出第二提示信息并且安装所述待安装应用,所述第二提示信息用于提示所述待安装应用不安全。

7.根据权利要求1至4任一项所述的方法,其特征在于,所述如果所述第二检测结果表明有安装命令,获取待安装应用的应用信息,包括:

如果所述第二检测结果表明有安装命令,缓存所述待安装应用;

解析所述待安装应用,得到待安装应用的应用信息。

8.根据权利要求1至4任一项所述的方法,其特征在于,所述检测是否连接有除自身外的其他电子设备,得到第一检测结果,包括:

检测是否有数据线插入预设的外部接口;

如果有数据线插入所述外部接口,则确定所述第一检测结果连接有除自身外的其他电子设备;如果没有数据线插入所述外部接口,则确定所述第一检测结果没有连接有除自身

外的其他电子设备。

9.一种应用安装装置，其特征在于，所述装置包括第一检测单元、第二检测单元、第一获取单元、识别单元和处理单元，其中：

所述第一检测单元，用于检测是否连接除自身外的其他电子设备，得到第一检测结果；

所述第二检测单元，用于如果所述第一检测结果表明连接除自身外的其他电子设备，检测是否有安装命令，得到第二检测结果，所述安装命令用于安装应用；

所述获取单元，用于如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息；

所述识别单元，用于根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果；

所述处理单元，用于根据所述识别结果对所述待安装应用进行处理。

10.一种移动终端，其特征在于，所述移动终端包括用于除自身外的其他电子设备的外部接口和处理器，所述处理器，用于：

检测是否通过所述外部接口连接除自身外的其他电子设备，得到第一检测结果；

如果所述第一检测结果表明连接有除自身外的其他电子设备，检测是否有安装命令，得到第二检测结果，所述安装命令用于安装应用；

如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息；

根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果；

根据所述识别结果对所述待安装应用进行处理。

一种应用安装方法及装置、终端

技术领域

[0001] 本发明涉及电子技术，尤其涉及一种应用安装方法及装置、终端。

背景技术

[0002] 随着移动互联网的发展和移动终端的普及，用户群越来越大，一些对移动终端的了解较少的用户也开始使用移动终端。这些用户群体往往对移动终端了解不是非常深入，所以常常由于安装了错误的软件或者在不适当的场所将移动终端连接电脑，从而导致移动终端被安装若干流氓应用，进而导致移动终端越来越慢、以及用户所使用的用户识别模块(SIM)卡会出现严重地扣费的情况。

[0003] 在现有的技术中，使用安卓(Android)系统的移动终端的用户往往使用一些移动终端助手类软件。以手机作为移动终端进行说明，这些手机助手类软件在个人电脑(PC)电脑上运行时，会检测是否有手机插入。如果有手机插入时，在电脑端弹出进行安全检测、垃圾清理等提示信息，这时，如果用户点击进行安全监测或垃圾清理时，则会在手机上安装一些未经用户确认的应用程序。更为过分的是某些应用的推广厂家会提供一些免费充电设备，在火车站等地方以提供免费充电的名义，从而诱导用户给用户安装某些推广的应用。

发明内容

[0004] 有鉴于此，本发明实施例为解决现有技术中存在的至少一个问题而提供一种应用安装方法及装置、终端，能够防止当移动终端与其他电子设备连接时而下载恶意的应用，从而保证移动终端的安全。

[0005] 本发明实施例的技术方案是这样实现的：

[0006] 第一方面，本发明实施例提供一种应用安装方法，所述方法包括：

[0007] 检测是否连接有除自身外的其他电子设备，得到第一检测结果；

[0008] 如果所述第一检测结果表明连接有除自身外的其他电子设备，检测是否有安装命令，得到第二检测结果，所述安装命令用于安装应用；

[0009] 如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息；

[0010] 根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果；

[0011] 根据所述识别结果对所述待安装应用进行处理。

[0012] 第二方面，本发明实施例提供一种应用安装装置，所述装置包括第一检测单元、第二检测单元、第一获取单元、识别单元和处理单元，其中：

[0013] 所述第一检测单元，用于检测是否连接除自身外的其他电子设备，得到第一检测结果；

[0014] 所述第二检测单元，用于如果所述第一检测结果表明连接除自身外的其他电子设备，检测是否有安装命令，得到第二检测结果，所述安装命令用于安装应用；

[0015] 所述获取单元，用于如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息；

[0016] 所述识别单元，用于根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果；

[0017] 所述处理单元，用于根据所述识别结果对所述待安装应用进行处理。

[0018] 第三方面，本发明实施例提供一种移动终端，所述移动终端包括用于除自身外的其他电子设备的外部接口和处理器，所述处理器，用于：

[0019] 检测是否通过所述外部接口连接除自身外的其他电子设备，得到第一检测结果；

[0020] 如果所述第一检测结果表明连接有除自身外的其他电子设备，检测是否有安装命令，得到第二检测结果，所述安装命令用于安装应用；

[0021] 如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息；

[0022] 根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果；

[0023] 根据所述识别结果对所述待安装应用进行处理。

[0024] 本发明实施例提供的应用安装方法及装置、终端，其中：检测是否连接有除自身外的其他电子设备，得到第一检测结果；如果所述第一检测结果表明连接有除自身外的其他电子设备，检测是否有安装命令，得到第二检测结果，所述安装命令用于安装应用；如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息；根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果；根据所述识别结果对所述待安装应用进行处理；如此，能够防止当移动终端与其他电子设备连接时而下载恶意的应用，从而保证移动终端的安全。

附图说明

[0025] 图1-1为实现本发明各个实施例的一个可选的移动终端100的硬件结构示意图；

[0026] 图1-2为如图1-1所示的移动终端100的无线通信系统示意图；

[0027] 图1-3为本发明实施例一应用安装方法的实现流程示意图；

[0028] 图2为本发明实施例二应用安装方法的实现流程示意图；

[0029] 图3-1为本发明实施例一应用安装装置的组成结构示意图；

[0030] 图3-2为本发明实施例一应用安装方法的实现流程示意图；

[0031] 图4-1为本发明实施例四应用安装装置的组成结构示意图一；

[0032] 图4-2为本发明实施例四应用安装装置的组成结构示意图二。

具体实施方式

[0033] 应当理解，此处所描述的具体实施例仅仅用以解释本发明的技术方案，并不用于限定本发明的保护范围。

[0034] 现在将参考附图描述实现本发明各个实施例的移动终端。在后续的描述中，使用用于表示元件的诸如“模块”、“部件”或“单元”的后缀仅为了有利于本发明的说明，其本身并没有特定的意义。因此，“模块”与“部件”可以混合地使用。

[0035] 移动终端可以以各种形式来实施。例如，本发明中描述的终端可以包括诸如移动电话、智能电话、笔记本电脑、数字广播接收器、个人数字助理(PDA)、平板电脑(PAD)、便携式多媒体播放器(PMP)、导航装置等等的移动终端以及诸如数字TV、台式计算机等等的固定终端。下面，假设终端是移动终端。然而，本领域技术人员将理解的是，除了特别用于移动目

的的元件之外，根据本发明的实施方式的构造也能够应用于固定类型的终端。

[0036] 图1-1为实现本发明各个实施例的移动终端100的硬件结构示意，如图1-1所示，移动终端100可以包括无线通信单元110、音频/视频(A/V)输入单元120、用户输入单元130、感测单元140、输出单元150、存储器160、接口单元170、控制器180和电源单元190等等。图1-1示出了具有各种组件的移动终端100，但是应理解的是，并不要求实施所有示出的组件。可以替代地实施更多或更少的组件。将在下面详细描述移动终端100的元件。

[0037] 无线通信单元110通常包括一个或多个组件，其允许移动终端100与无线通信系统或网络之间的无线电通信。例如，无线通信单元110可以包括广播接收模块111、移动通信模块112、无线互联网模块113、短程通信模块114和位置信息模块115中的至少一个。

[0038] 广播接收模块111经由广播信道从外部广播管理服务器接收广播信号和/或广播相关信息。经由广播接收模块111接收的广播信号和/或广播相关信息可以存储在存储器160(或者其它类型的存储介质)中。

[0039] 移动通信模块112将无线电信号发送到基站(例如，接入点、节点B等等)、外部终端以及服务器中的至少一个和/或从其接收无线电信号。

[0040] 无线互联网模块113支持移动终端100的无线互联网接入。无线互联网模块113可以内部或外部地耦接到终端。

[0041] 短程通信模块114是用于支持短程通信的模块。短程通信技术的一些示例包括蓝牙™、射频识别(RFID)、红外数据协会(IrDA)、超宽带(UWB)、紫蜂™等等。

[0042] 位置信息模块115是用于检查或获取移动终端100的位置信息的模块。位置信息模块115的典型示例是全球定位系统(GPS)模块115。

[0043] A/V输入单元120用于接收音频或视频信号。A/V输入单元120可以包括相机121和麦克风122，相机121对在视频捕获模式或图像捕获模式中由图像捕获装置获得的静态图片或视频的图像数据进行处理。处理后的图像帧可以显示在显示单元151上。经相机121处理后的图像帧可以存储在存储器160(或其它存储介质)中或者经由无线通信单元110进行发送，可以根据移动终端100的构造提供两个或更多相机121。麦克风122可以在电话通话模式、记录模式、语音识别模式等等运行模式中经由麦克风接收声音(音频数据)，并且能够将这样的声音处理为音频数据。处理后的音频(语音)数据可以在电话通话模式的情况下转换为可经由移动通信模块112发送到移动通信基站的格式输出。麦克风122可以实施各种类型的噪声消除(或抑制)算法以消除(或抑制)在接收和发送音频信号的过程中产生的噪声或者干扰。

[0044] 用户输入单元130可以根据用户输入的命令生成键输入数据以控制移动终端100的各种操作。用户输入单元130允许用户输入各种类型的信息。特别地，当触摸板以层的形式叠加在显示单元151上时，可以形成触摸屏。

[0045] 感测单元140检测移动终端100的当前状态，(例如，移动终端100的打开或关闭状态)、移动终端100的位置、用户对于移动终端100的接触(即，触摸输入)的有无、移动终端100的取向、移动终端100的加速或减速移动和方向等等，并且生成用于控制移动终端100的操作的命令或信号。例如，当移动终端100实施为滑动型移动电话时，感测单元140可以感测该滑动型电话是打开还是关闭。另外，感测单元140能够检测电源单元190是否提供电力或者接口单元170是否与外部装置耦接。

[0046] 接口单元170用作至少一个外部装置与移动终端100连接可以通过的接口。例如，外部装置可以包括有线或无线头戴式耳机端口、外部电源(或电池充电器)端口、有线或无线数据端口、存储卡端口(典型示例是通用串行总线USB端口)、用于连接具有用户识别模块的装置的端口、音频输入/输出(I/O)端口、视频I/O端口、耳机端口等等。用户识别模块可以是存储用于验证用户使用移动终端100的各种信息并且可以包括客户识别模块(SIM)、通用客户识别模块(USIM)等等。

[0047] 接口单元170可以用于接收来自外部装置的输入(例如，数据信息、电力等等)并且将接收到的输入传输到移动终端100内的一个或多个元件或者可以用于在移动终端100和外部装置之间传输数据。

[0048] 另外，当移动终端100与外部底座连接时，接口单元170可以用作允许通过其将电力从底座提供到移动终端100的路径或者可以用作允许从底座输入的各种命令信号通过其传输到移动终端100的路径。从底座输入的各种命令信号或电力可以用作用于识别移动终端100是否准确地安装在底座上的信号。

[0049] 输出单元150被构造为以视觉、音频和/或触觉方式提供输出信号(例如，音频信号、视频信号、警报信号、振动信号等等)。输出单元150可以包括显示单元151、音频输出模块152、警报单元153等等。

[0050] 显示单元151可以显示在移动终端100中处理的信息。例如，当移动终端100处于电话通话模式时，显示单元151可以显示与通话或其它通信(例如，文本消息收发、多媒体文件下载等等)相关的用户界面(UI)或图形用户界面(GUI)。当移动终端100处于视频通话模式或者图像捕获模式时，显示单元151可以显示捕获的图像和/或接收的图像、示出视频或图像以及相关功能的UI或GUI等等。

[0051] 同时，当显示单元151和触摸板以层的形式彼此叠加以形成触摸屏时，显示单元151可以用作输入装置和输出装置；音频输出模块152可以包括扬声器、蜂鸣器等等。警报单元153可以提供输出以将事件的发生通知给移动终端100。典型的事件可以包括呼叫接收、消息接收、键信号输入、触摸输入等等。

[0052] 存储器160可以存储由控制器180执行的处理和控制操作的软件程序等等，或者可以暂时地存储已经输出或将要输出的数据(例如，电话簿、消息、静态图像、视频等等)。而且，存储器160可以存储关于当触摸施加到触摸屏时输出的各种方式的振动和音频信号的数据。

[0053] 存储器160可以包括至少一种类型的存储介质，而且，移动终端100可以与通过网络连接执行存储器160的存储功能的网络存储装置协作。

[0054] 控制器180通常控制移动终端100的总体操作。例如，控制器180执行与语音通话、数据通信、视频通话等等相关的控制和处理。另外，控制器180可以包括用于再现或回放多媒体数据的多媒体模块181，多媒体模块181可以构造在控制器180内，或者可以构造为与控制器180分离。控制器180可以执行模式识别处理，以将在触摸屏上执行的手写输入或者图片绘制输入识别为字符或图像。

[0055] 电源单元190在控制器180的控制下接收外部电力或内部电力并且提供操作各元件和组件所需的适当的电力。

[0056] 这里描述的各种实施方式可以以使用例如计算机软件、硬件或其任何组合的计算

机可读介质来实施。对于硬件实施，这里描述的实施方式可以通过使用特定用途集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理装置(DSPD)、可编程逻辑装置(PLD)、现场可编程门阵列(FPGA)、处理器、控制器、微控制器、微处理器、被设计为执行这里描述的功能的电子单元中的至少一种来实施，在一些情况下，这样的实施方式可以在控制器180中实施。对于软件实施，诸如过程或功能的实施方式可以与允许执行至少一种功能或操作的单独的软件模块来实施。软件代码可以由以任何适当的编程语言编写的软件应用程序(或程序)来实施，软件代码可以存储在存储器160中并且由控制器180执行。

[0057] 至此，已经按照其功能描述了移动终端100。下面，为了简要起见，将描述诸如折叠型、直板型、摆动型、滑动型移动终端100等等的各种类型的移动终端100中的滑动型移动终端100作为示例。因此，本发明能够应用于任何类型的移动终端100，并且不限于滑动型移动终端100。

[0058] 如图1-1中所示的移动终端100可以被构造为利用经由帧或分组发送数据的诸如有线和无线通信系统以及基于卫星的通信系统来操作。

[0059] 现在将参考图1-2描述其中根据本发明的移动终端100能够操作的通信系统。

[0060] 这样的通信系统可以使用不同的空中接口和/或物理层。例如，由通信系统使用的空中接口包括例如频分多址(FDMA)、时分多址(TDMA)、码分多址(CDMA)和通用移动通信系统(UMTS)(特别地，长期演进(LTE))、全球移动通信系统(GSM)等等。作为非限制性示例，下面的描述涉及CDMA通信系统，但是这样的教导同样适用于其它类型的系统。

[0061] 参考图1-2，CDMA无线通信系统可以包括多个移动终端100、多个基站(BS)270、基站控制器(BSC)275和移动交换中心(MSC)280。MSC 280被构造为与公共电话交换网络(PSTN)290形成接口。MSC 280还被构造为与可以经由回程线路耦接到基站270的BSC 275形成接口。回程线路可以根据若干已知的接口中的任一种来构造，所述接口包括例如E1/T1、ATM、IP、PPP、帧中继、HDSL、ADSL或xDSL。将理解的是，如图1-2中所示的系统可以包括多个BSC 2750。

[0062] 每个BS 270可以服务一个或多个分区(或区域)，由多向天线或指向特定方向的天线覆盖的每个分区放射状地远离BS 270。或者，每个分区可以由用于分集接收的两个或更多天线覆盖。每个BS 270可以被构造为支持多个频率分配，并且每个频率分配具有特定频谱(例如，1.25MHz，5MHz等等)。

[0063] 分区与频率分配的交叉可以被称为CDMA信道。BS 270也可以被称为基站收发器子系统(BTS)或者其它等效术语。在这样的情况下，术语“基站”可以用于笼统地表示单个BSC 275和至少一个BS 270。基站也可以被称为“蜂窝站”。或者，特定BS 270的各分区可以被称为多个蜂窝站。

[0064] 如图1-2中所示，广播发射器(BT)295将广播信号发送给在系统内操作的移动终端100。如图1-1中所示的广播接收模块111被设置在移动终端100处以接收由BT295发送的广播信号。在图1-2中，示出了几个卫星300，例如可以采用全球定位系统(GPS)卫星300。卫星300帮助定位多个移动终端100中的至少一个。

[0065] 在图1-2中，描绘了多个卫星300，但是理解的是，可以利用任何数目的卫星获得有用的定位信息。如图1-1中所示的GPS模块115通常被构造为与卫星300配合以获得想要的定位信息。替代GPS跟踪技术或者在GPS跟踪技术之外，可以使用可以跟踪移动终端100的位置

的其它技术。另外，至少一个GPS卫星300可以选择性地或者额外地处理卫星DMB传输。

[0066] 作为无线通信系统的一个典型操作，BS 270接收来自各种移动终端100的反向链路信号。移动终端100通常参与通话、消息收发和其它类型的通信。特定基站270接收的每个反向链路信号被在特定BS 270内进行处理。获得的数据被转发给相关的BSC 275。BSC提供通话资源分配和包括BS 270之间的软切换过程的协调的移动管理功能。BSC275还将接收到的数据路由到MSC 280，其提供用于与PSTN 290形成接口的额外的路由服务。类似地，PSTN 290与MSC 280形成接口，MSC与BSC 275形成接口，并且BSC 275相应地控制BS 270以将正向链路信号发送到移动终端100。

[0067] 移动终端中无线通信单元110的移动通信模块112基于移动终端内置的接入移动通信网络(如2G/3G/4G等移动通信网络)的必要数据(包括用户识别信息和鉴权信息)接入移动通信网络为移动终端用户的网页浏览、网络多媒体播放等业务传输移动通信数据(包括上行的移动通信数据和下行的移动通信数据)。

[0068] 无线通信单元110的无线互联网模块113通过运行无线热点的相关协议功能而实现无线热点的功能，无线热点支持多个移动终端(移动终端之外的任意移动终端)接入，通过复用移动通信模块112与移动通信网络之间的移动通信连接为移动终端用户的网页浏览、网络多媒体播放等业务传输移动通信数据(包括上行的移动通信数据和下行的移动通信数据)，由于移动终端实质上是复用移动终端与通信网络之间的移动通信连接传输移动通信数据的，因此移动终端消耗的移动通信数据的流量由通信网络侧的计费实体计入移动终端的通信资费，从而消耗移动终端签约使用的通信资费中包括的移动通信数据的数据流量。

[0069] 基于上述移动终端100硬件结构以及通信系统，提出本发明方法各个实施例。

[0070] 为了解决背景技术中存在的问题，本发明实施例提供一种应用安装方法及装置、设备，其中，移动终端检测应用的安装命令，当移动终端检测到安装应用的命令时，首先对应用进行解析，获取应用的包名等应用信息，并将包名等应用信息与黑名单中应用的信息进行比较，得出识别结果，所述识别结果用于表明安装的应用是否为黑名单中的应用。如果识别结果表明安装的应用是黑名单中的应用，则直接停止安装流程，禁止该当前安装的应用进行安装；如果识别结果表明当前安装的应用不是黑名单应用，则弹出提示框进行安装确认或者直接进行安装操作。其中，黑名单存储在移动终端中，黑名单可以通过联网等方式进行更新。

[0071] 下面结合附图和具体实施例对本发明的技术方案进一步详细阐述。

[0072] 实施例一

[0073] 为了解决前述的技术问题，本发明实施例提供一种应用安装方法，该方法应用于移动终端，该方法所实现的功能可以通过移动终端中的处理器调用程序代码来实现，当然程序代码可以保存在计算机存储介质中，可见，该移动终端至少包括处理器和存储介质。

[0074] 图1-3为本发明实施例一应用安装方法的实现流程示意图，如图1-3所示，该应用安装方法包括：

[0075] 步骤S101，检测是否连接除自身外的其他电子设备，得到第一检测结果；

[0076] 这里，本发明实施例至少针对于下面两种场景：

[0077] 第一种场景：用户需要将移动终端上的文件如照片导出到其他的电子设备如PC等

时，安装在电子设备上如PC的手机助手类软件在PC电脑上运行时，手机助手类软件会检测是否有手机插入，如果有手机插入时，在电脑端弹出进行安全检测、垃圾清理等提示信息，这时，如果用户点击进行安全监测或垃圾清理时，则会在手机上安装一些未经用户确认的应用程序，而本实施例提供的方法将针对这类的应用程序进行检测。

[0078] 第二种场景：某些应用的推广厂家会提供一些免费充电设备，在火车站等地方以提供免费充电的名义，从而诱导用户给用户安装某些推广的应用，本实施例提供的方法也针对这类的应用程序进行检测。

[0079] 这里，移动终端检测自身是否连接有除自身外的其他电子设备包括检测通过有线和无线方式连接的其他电子设备，其中无线方式包括蓝牙、红外等无线连接方式，下面以有线连接进行说明，在本发明的其他实施例中，所述步骤S101，所述检测是否连接有除自身外的其他电子设备，得到第一检测结果，包括：

[0080] 步骤S111，检测是否有数据线插入预设的外部接口；

[0081] 步骤S112，如果有数据线插入所述外部接口，则确定所述第一检测结果连接有除自身外的其他电子设备；如果没有数据线插入所述外部接口，则确定所述第一检测结果没有连接有除自身外的其他电子设备。

[0082] 步骤S102，如果所述第一检测结果表明连接有除自身外的其他电子设备，检测是否有安装命令，得到第二检测结果，所述安装命令用于安装应用；

[0083] 这里，所述安装命令针对不同的操作系统，安装命令的具体格式可能不同，例如以安卓操作系统为例进行说明，安装命令包括adb push和adb install。

[0084] 步骤S103，如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息；

[0085] 步骤S104，根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果；

[0086] 步骤S105，根据所述识别结果对所述待安装应用进行处理。

[0087] 本发明实施例中，所述步骤S105，所述根据所述识别结果对所述待安装应用进行处理，包括：

[0088] 步骤S151，如果所述识别结果表明所述待安装应用安全时，安装所述待安装应用，或者；如果所述识别结果表明所述待安装应用安全时，输出第一提示信息并且安装所述待安装应用，所述第一提示信息用于提示所述待安装应用为安全的应用。

[0089] 步骤S152，如果所述识别结果表明所述待安装应用不安全时，停止所述待安装应用并输出第二提示信息并且安装所述待安装应用，所述第二提示信息用于提示所述待安装应用不安全。

[0090] 在本发明的其他实施例中，所述步骤S104包括：所述根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果，包括：将所述待安装应用的应用信息与黑名单中应用的信息进行比较，得到识别结果，所述识别结果表明当前安装的应用是否为黑名单中的应用。

[0091] 这里，在实施的过程中，所述黑名单以数据库或者XML文件形式存储在本地；所述方法还包括：周期性或非周期性的更新所述黑名单。该实施例中，识别结果是移动终端自身识别的，因此具有快速的优点，而且不需要网络即可实现。

[0092] 本发明实施例中，步骤S103，所述如果所述第二检测结果表明有安装命令，获取待

安装应用的应用信息，包括：如果所述第二检测结果表明有安装命令，缓存所述待安装应用；解析所述待安装应用，得到待安装应用的应用信息。

[0093] 在本发明的其他实施例中，移动终端检测到安装命令后，根据不同安装命令，将安装的应用进行缓存等处理后，首先对应用进行解析，从中获取应用的包名等应用信息，并将该应用的包名等应用信息与黑名单中应用的信息进行比较，得到识别结果，所述识别结果表明当前安装的应用是否为黑名单中的应用。如果识别结果表明安装的应用是黑名单应用，则直接停止安装流程，禁止该应用的安装，避免用户由于不熟悉而被误装应用；如果识别结果表明当前安装的应用不是黑名单的应用，则弹出提示框提示用户进行安装确认或者直接进行安装处理。其中，黑名单可以以数据库或者XML文件等形式存储在移动中，可以通过联网、FOTA升级等方式对黑名单进行维护和升级等处理。

[0094] 实施例二

[0095] 基于前述的实施例，本发明实施例再提供一种应用安装方法，图2为本发明实施例二应用安装方法的实现流程示意图，如图2所示，该方法包括：

[0096] 步骤S201，移动终端检测是否连接除自身外的其他电子设备，得到第一检测结果；

[0097] 步骤S202，如果所述第一检测结果表明连接有除自身外的其他电子设备，移动终端检测是否有安装命令，得到第二检测结果，所述安装命令用于安装应用；

[0098] 步骤S203，如果所述第二检测结果表明有安装命令，移动终端获取待安装应用的应用信息；

[0099] 步骤S204，移动终端根据所述待安装应用的应用信息生成查询请求，所述查询请求用于请求查询所述待安装应用是否安全；

[0100] 步骤S205，移动终端将所述查询请求发送给服务器；

[0101] 步骤S206，服务器接收到所述查询请求后，解析所述查询请求，得到所述待安装应用的应用信息；

[0102] 步骤S207，所述服务器将所述待安装应用的应用信息与黑名单中应用的信息进行比较，得到识别结果；

[0103] 这里，所述识别结果表明当前安装的应用是否为黑名单中的应用；

[0104] 步骤S208，所述服务器将所述识别结果携带于查询响应中，将所述查询响应发送给移动终端。

[0105] 步骤S209，移动终端接收所述服务器发送的查询响应，所述查询响应中携带有识别结果；

[0106] 步骤S210，移动终端解析所述查询响应，得到所述识别结果。

[0107] 步骤S211，移动终端根据所述识别结果对所述待安装应用进行处理。

[0108] 本发明实施例中，所述如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息，包括：如果所述第二检测结果表明有安装命令，缓存所述待安装应用；解析所述待安装应用，得到待安装应用的应用信息。

[0109] 本发明实施例中，所述根据所述识别结果对所述待安装应用进行处理，包括：

[0110] 如果所述识别结果表明所述待安装应用安全时，安装所述待安装应用，或者；如果所述识别结果表明所述待安装应用安全时，输出第一提示信息并且安装所述待安装应用，所述第一提示信息用于提示所述待安装应用为安全的应用；

[0111] 如果所述识别结果表明所述待安装应用不安全时，停止所述待安装应用并输出第二提示信息并且安装所述待安装应用，所述第二提示信息用于提示所述待安装应用不安全。

[0112] 上述的S204至步骤S210实际上提供一种实现实施例一种步骤S104的方式，在本实施例中，识别结果是服务器基于移动终端的请求而发送的，即识别结果是服务器识别的，由于服务器上黑名单的更新会比较及时，而且数据量比较大，因此该方法具有准确的优点。

[0113] 实施例三

[0114] 本实施例提供了一种应用安装装置，图3-1为本发明实施例三应用安装装置的组成结构示意图，如图3-1所示，该装置包括检测模块101、识别模块102和处理模块103，其中：

[0115] 检测模块101用于检测移动终端的安装应用的操作。

[0116] 对于安卓操作系统的移动终端而言，通过数据线进行应用安装的方式包括以下两种：adb push应用进/system/priv-app/或/system/app/目录进行安装应用、通过pc端的adb install操作进行安装应用。

[0117] 检测模块101在相应的代码中做出一定的扩展即可实现对应用安装的检测。以安卓操作系统为例进行说明，对于adb push应用进/system/priv-app/或/system/app/进行安装的方式，只需要监听push命令的内容，在框架层中进行扩展，同样，对于通过adb install进行的安装则对框架层(frameworks)中的pm.java进行相应的扩展，可在处理adb install的函数中增加相应的代码。当检测模块101检测到应用的安装操作后，通知识别模块102对安装的应用进行识别处理。

[0118] 识别模块102用于对检测模块101所安装的应用进行识别处理。

[0119] 这里，识别模块102首先对安装的应用进行解析，得到安装应用的包名等应用信息，之后，将这些应用信息与黑名单中的进行比较，得到识别结果，所述识别结果用于表明安装的应用是否为黑名单中的应用。识别模块102将识别结果发送处理模块103进行相应的处理。其中，黑名单可以以可扩展标记语言(XML，Extensible Markup Language)文件、数据库等形式内置在移动终端中，以后通过移动终端的空中下载软件升级(FOTA，Firmware Over-The-Air)升级、网络升级等方式进行维护更新。其中FOTA升级是指通过云端升级技术，为具有连网功能的设备：例如手机、平板电脑、便携式媒体播放器、移动互联网设备等提供固件升级服务，用户使用网络以按需、易扩展的方式获取智能终端系统升级包，并通过FOTA进行云端升级，完成系统修复和优化。

[0120] 处理模块103用于根据所述识别结果对识别后的应用进行相应的处理。如果所述识别结果表明安装的应用是黑名单中的应用，则直接停止安装流程并删除缓存中的安装文件；如果识别结果表明安装的应用不是黑名单中的应用，则以提示框的形式提示用户确认安装操作或直接进行静默安装。

[0121] 下面介绍一下安卓操作系统中的两个安装命令，即adb push安装命令和adb install安装命令，的使用区别：在安卓操作系统实际开发中，经常会使用adb命令，安装应用程序可以使用adb push安装命令或者adb install安装命令，它们的区别在于：

[0122] adb push安装命令能够指定安装目录。比如执行命令“adb push xxx.apk system/app”后，xxx.apk被安装到了system/app目录下，此目录下的软件为系统应用(system application)其中，“xxx”为安卓安装包(APK，Android Package)，小写的apk含义

也是安卓安装包，因为在代码或命令中采用小写来表示。需要说明的是，system/app是只读的，所以只有用于根或系统(root)权限才能push apk进去，而且在push进去的APK会把原本的APK覆盖掉。adb push本身的意思是将文件复制到系统中的某个文件夹下，但是将apk push到system/app下并且重启手机以后会注册应用程序。

[0123] adb install用此命令安装的软件位于data/app目录，带有参数-r才能强制安装，为用户应用或用户程序(user application)。

[0124] 由以上可知，adb install和adb push的apk主要区别见表1：

[0125] 表1

[0126]

命令	adb push	adb install
目录	system/app	data/app
权限	系统级(权限全开)	用户级(没全开)
卸载	root后删除	可卸载
大小	无限制，自定义	有限制
安装	pm重新注册	不会重新弄注册

[0127] 基于前述的图3-1所示的实施例，本发明实施例再提供一种应用安装方法，图3-2为本发明实施例三应用安装方法的实现流程示意图，如图3-2所示，该方法包括：

[0128] 步骤S301：检测模块101用于检测移动终端的安装应用的操作；当检测模块101检测到应用的安装操作后，进入步骤S302；

[0129] 这里，对于使用数据线的形式进行安装，检测adb push应用进/system/priv-app/或/system/app/目录进行文件安装、通过pc端的adb install操作即可实现对数据线安装应用的检测，在安卓操作系统中，可以通过对框架层添加代码实现检测的流程。

[0130] 步骤S302：识别模块102对安装的应用进行解析，获取当前应用的包名等应用信息。

[0131] 这里，识别模块102将通过安装命令adb push进目录“/system/priv-app/”或“/system/app/”目录的应用，或通过安装命令adb install的应用进行缓存处理，以便于解析，一般而言，可以通过解析AndroidManifest实现对包名的获取；其中，每个安卓操作系统的应用程序必须有一个AndroidManifest.xml文件，在其根目录res下，它在简单的Android系统的应用提出了重要的信息，它可以运行任何应用程序的代码。

[0132] 步骤S303：识别模块102将获取的包名等信息与黑名单中的进行比较，得到识别结果，所述识别结果用于表明安装的应用是否为黑名单中的应用。如果识别结果表明安装的应用为黑名单中的应用，则进入步骤S304，如果识别结果表明安装的应用不是黑名单中的应用，则进入步骤S305；

[0133] 步骤S304：处理模块103对识别为黑名单中的应用进行相应的处理，处理的方式包括但不仅限于直接停止应用的安装流程等；

[0134] 步骤S305：处理模块103对识别为非黑名单中的应用进行相应的处理，处理的方式包括但不仅限于提示用户以确认安装流程的进行、以静默的方式进行应用的安装等。

[0135] 本发明通过检测应用的安装流程实现对应用安装的监控。目前，常见的安卓操作系统上通过数据线进行应用安装的方式有以下两种：通过PC端的adb push命令将应用push

进“/system/priv-app/”或“/system/app/”目录进行文件安装、通过PC端的adb install操作实现应用的安装，但此两种方式在框架层中都有所体现。本发明实施例通过对应用安装的监控，可以避免非专业用户被安装恶意应用导致手机出现吸费、移动终端变慢等情况；而且在一定程度上可以加强初级用户、老人等特殊群体的用户体验。

[0136] 实施例四

[0137] 基于前述的实施例，本发明实施例在提供一种应用安装装置，该装置中所包括的各单元，以及各单元所包括的各模块，都可以通过移动终端中的处理器来实现；当然也可通过具体的逻辑电路实现；在具体实施例的过程中，处理器可以为中央处理器(CPU)、微处理器(MPU)、数字信号处理器(DSP)或现场可编程门阵列(FPGA)等。

[0138] 这里，所述移动终端设备在具体实施例的过程中可以为各种类型的具有信息处理能力的移动设备，例如可以包括手机、平板电脑、个人数字助理、导航仪、数字电话等。

[0139] 图4-1为本发明实施例四应用安装装置的组成结构示意图一，如图4-1所示，该装置400包括第一检测单元401、第二检测单元402、第一获取单元403、识别单元404和处理单元405，其中：

[0140] 所述第一检测单元401，用于检测是否连接除自身外的其他电子设备，得到第一检测结果；

[0141] 所述第二检测单元402，用于如果所述第一检测结果表明连接有除自身外的其他电子设备，检测是否有安装命令，得到第二检测结果，所述安装命令用于安装应用；

[0142] 所述获取单元403，用于如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息；

[0143] 所述识别单元404，用于根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果；

[0144] 所述处理单元405，用于根据所述识别结果对所述待安装应用进行处理。

[0145] 在本发明的其他实施例中，所述识别单元，用于将所述待安装应用的应用信息与黑名单中应用的信息进行比较，得到识别结果，所述识别结果表明当前安装的应用是否为黑名单中的应用。

[0146] 在本发明的其他实施例中，如图4-2所示，所述识别单元404包括生成模块441、发送模块442、接收模块443和解析模块444，其中：

[0147] 所述生成模块，用于根据所述待安装应用的应用信息生成查询请求，所述查询请求用于请求查询所述待安装应用是否安全；

[0148] 所述发送模块，用于将所述查询请求发送给服务器；

[0149] 所述接收模块，用于接收所述服务器发送的查询响应，所述查询响应中携带有识别结果；

[0150] 所述解析模块，用于解析所述查询响应，得到所述识别结果。

[0151] 这里，本实施例中，如果服务器接收到所述查询请求后，解析所述查询请求，得到所述待安装应用的应用信息，然后所述服务器将所述待安装应用的应用信息与黑名单中应用的信息进行比较，得到识别结果，所述识别结果表明当前安装的应用是否为黑名单中的应用；然后所述服务器将所述识别结果携带于查询响应中，最终所述服务器将所述查询响应发送给移动终端。

[0152] 在本发明的其他实施例中，所述黑名单以数据库或者XML文件形式存储在本地；所述装置还包括更新单元，用于周期性或非周期性的更新所述黑名单。

[0153] 在本发明的其他实施例中，所述处理单元用于如果所述识别结果表明所述待安装应用安全时，安装所述待安装应用，或者；如果所述识别结果表明所述待安装应用安全时，输出第一提示信息并且安装所述待安装应用，所述第一提示信息用于提示所述待安装应用为安全的应用。

[0154] 在本发明的其他实施例中，所述处理单元，用于如果所述识别结果表明所述待安装应用不安全时，停止所述待安装应用并输出第二提示信息并且安装所述待安装应用，所述第二提示信息用于提示所述待安装应用不安全。

[0155] 在本发明的其他实施例中，所述获取单元包括缓存模块和解析模块，其中：

[0156] 所述缓存模块，用于如果所述第二检测结果表明有安装命令，缓存所述待安装应用；

[0157] 所述解析模块，用于解析所述待安装应用，得到待安装应用的应用信息。

[0158] 这里需要指出的是：以上装置实施例的描述，与上述方法实施例的描述是类似的，具有同方法实施例相似的有益效果，因此不做赘述。对于本发明装置实施例中未披露的技术细节，请参照本发明方法实施例的描述而理解，为节约篇幅，因此不再赘述。

[0159] 实施例五

[0160] 基于前述的实施例，本发明实施例在提供一种移动终端，所述移动终端包括用于连接除自身外的其他电子设备的外部接口(可以是图1-1中的接口单元170)和处理器，所述处理器，用于：

[0161] 检测是否连接除自身外的其他电子设备，得到第一检测结果；

[0162] 如果所述第一检测结果表明连接有除自身外的其他电子设备，检测是否有安装命令，得到第二检测结果，所述安装命令用于安装应用；

[0163] 如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息；

[0164] 根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果；

[0165] 根据所述识别结果对所述待安装应用进行处理。

[0166] 在本发明的其他实施例中，所述根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果，包括：

[0167] 将所述待安装应用的应用信息与黑名单中应用的信息进行比较，得到识别结果，所述识别结果表明当前安装的应用是否为黑名单中的应用。

[0168] 在本发明的其他实施例中，所述根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果，包括：

[0169] 根据所述待安装应用的应用信息生成查询请求，所述查询请求用于请求查询所述待安装应用是否安全；

[0170] 将所述查询请求发送给服务器；

[0171] 接收所述服务器发送的查询响应，所述查询响应中携带有识别结果；

[0172] 解析所述查询响应，得到所述识别结果。

[0173] 在本发明的其他实施例中，所述黑名单以数据库或者XML文件形式存储在本地；所述处理器还用于：周期性或非周期性的更新所述黑名单。

[0174] 在本发明的其他实施例中，所述根据所述识别结果对所述待安装应用进行处理，包括：

[0175] 如果所述识别结果表明所述待安装应用安全时，安装所述待安装应用，或者；如果所述识别结果表明所述待安装应用安全时，输出第一提示信息并且安装所述待安装应用，所述第一提示信息用于提示所述待安装应用为安全的应用；

[0176] 如果所述识别结果表明所述待安装应用不安全时，停止所述待安装应用并输出第二提示信息并且安装所述待安装应用，所述第二提示信息用于提示所述待安装应用不安全。

[0177] 在本发明的其他实施例中，所述如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息，包括：

[0178] 如果所述第二检测结果表明有安装命令，缓存所述待安装应用；

[0179] 解析所述待安装应用，得到待安装应用的应用信息。

[0180] 这里需要指出的是：以上终端实施例的描述，与上述方法实施例的描述是类似的，具有同方法实施例相似的有益效果，因此不做赘述。对于本发明终端实施例中未披露的技术细节，请参照本发明方法实施例的描述而理解，为节约篇幅，因此不再赘述。

[0181] 应理解，说明书通篇中提到的“一个实施例”或“一实施例”意味着与实施例有关的特定特征、结构或特性包括在本发明的至少一个实施例中。因此，在整个说明书各处出现的“在一个实施例中”或“在一实施例中”未必一定指相同的实施例。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。应理解，在本发明的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。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。

[0182] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0183] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性的、机械的或其它形式的。

[0184] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显示的部件可以是、或也可以不是物理单元；既可以位于一个地方，也可以分布到多个网络单元上；可以根据实际的需要选择其中的部分或全部单元来实现本实施例方案的目的。

[0185] 另外，在本发明各实施例中的各功能单元可以全部集成在一个处理单元中，也可以是各单元分别单独作为一个单元，也可以两个或两个以上单元集成在一个单元中；上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0186] 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:移动存储设备、只读存储器(Read Only Memory,ROM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0187] 或者,本发明上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时,也可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明实施例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一个存储介质中,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方法的全部或部分。而前述的存储介质包括:移动存储设备、ROM、磁碟或者光盘等各种可以存储程序代码的介质。

[0188] 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以所述权利要求的保护范围为准。

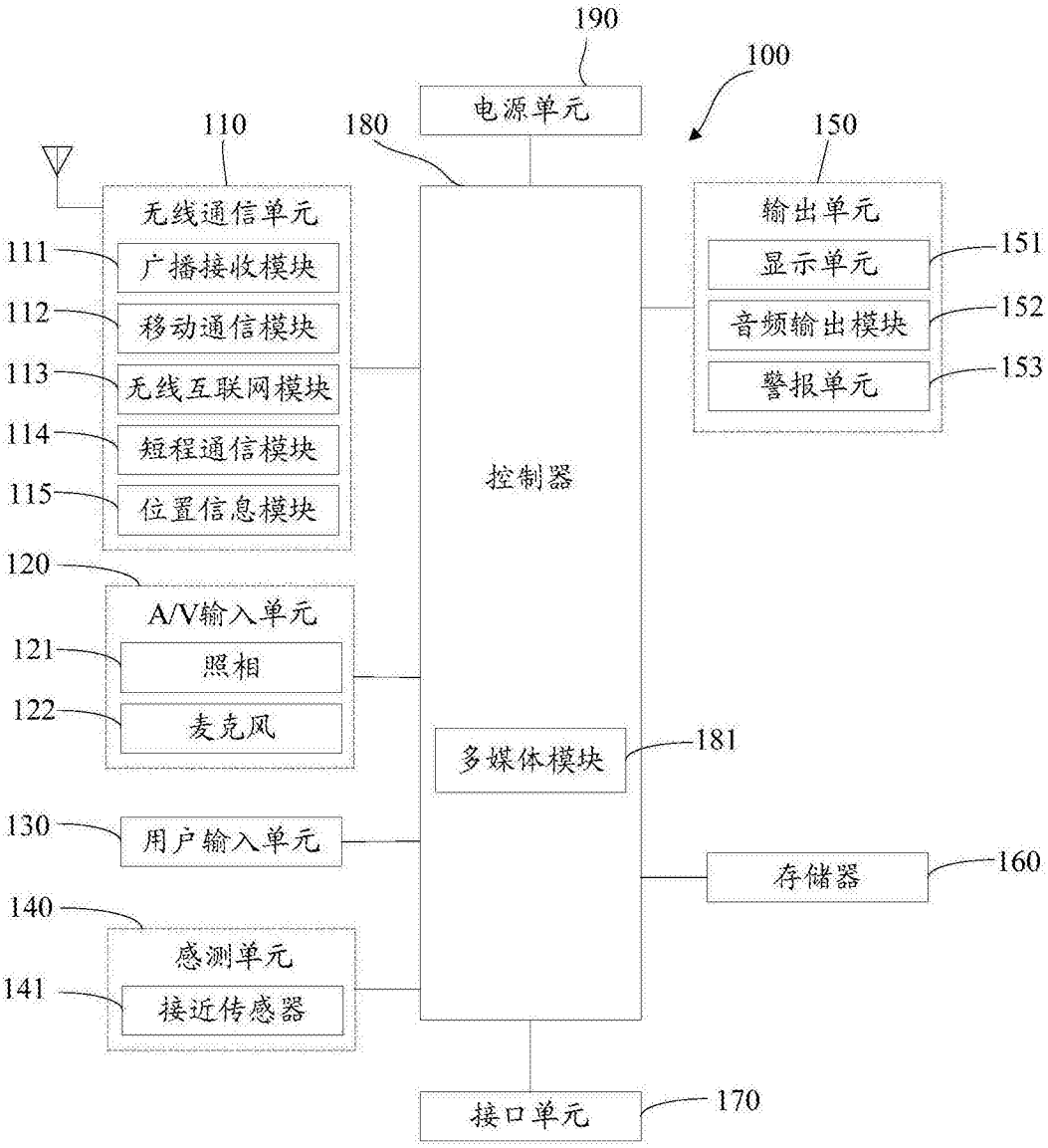

190
100
电源单元
110
180
150
无线通信单元
输出单元
111
广播接收模块
显示单元
151
112
移动通信模块
音频输出模块
152
113
无线互联网模块
警报单元
153
114
短程通信模块
控制器
115
位置信息模块
120
A/V输入单元
121
照相
122
麦克风
多媒体模块
181
130
用户输入单元
存储器
160
140
感测单元
141
接近传感器
接口单元
170

图1-1

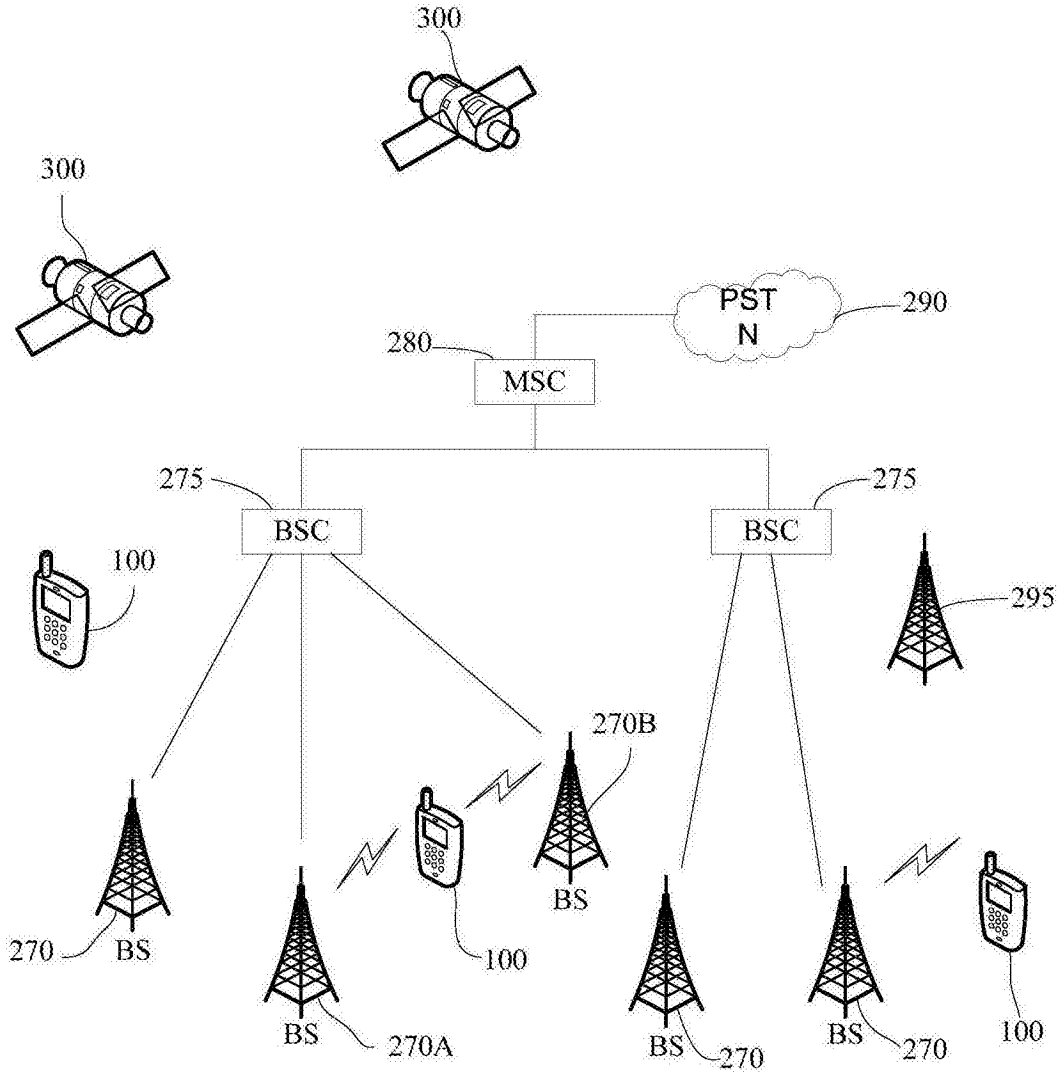

300
300
PST
N
290
280
MSC
275
BSC
275
BSC
100
295
270B
BS
270
BS
100
BS
270A
BS
270
BS
270
100

图1-2

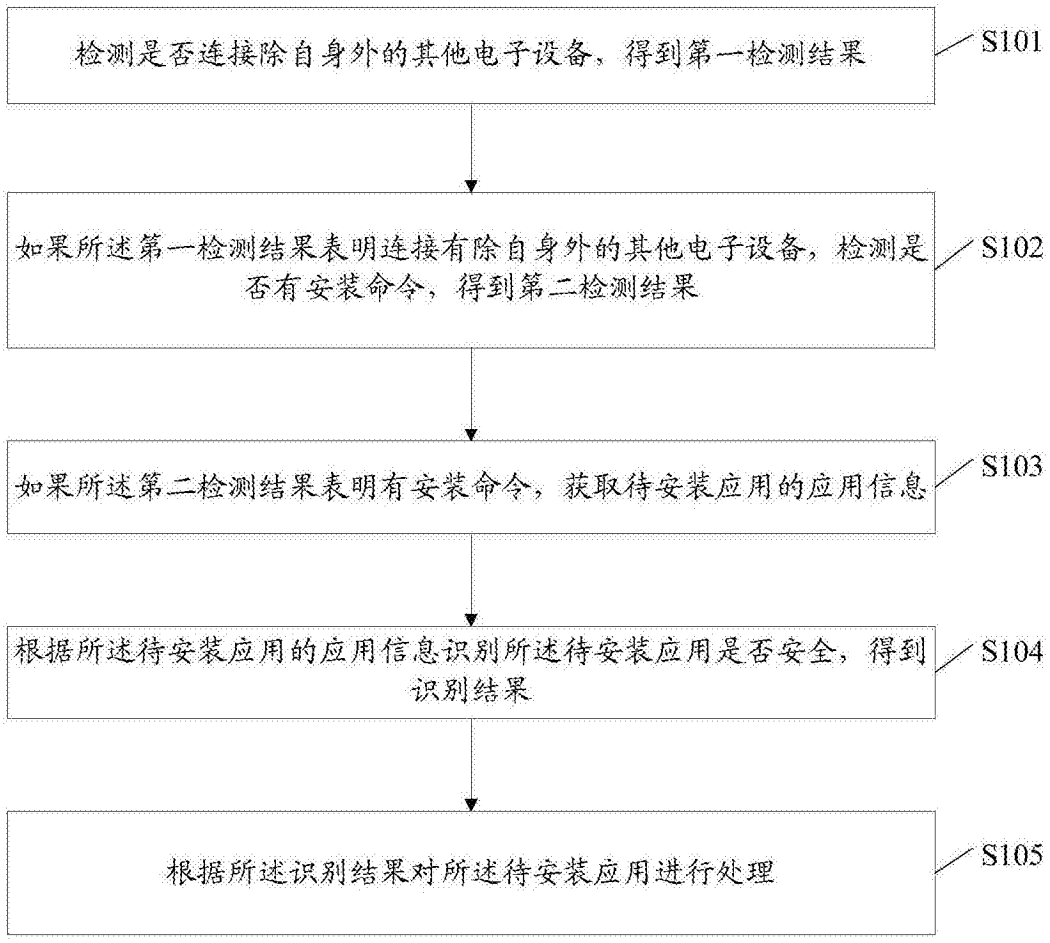

检测是否连接除自身外的其他电子设备，得到第一检测结果
S101
如果所述第一检测结果表明连接有除自身外的其他电子设备，检测是否有安装命令，得到第二检测结果
S102
如果所述第二检测结果表明有安装命令，获取待安装应用的应用信息
S103
根据所述待安装应用的应用信息识别所述待安装应用是否安全，得到识别结果
S104
根据所述识别结果对所述待安装应用进行处理
S105

图1-3

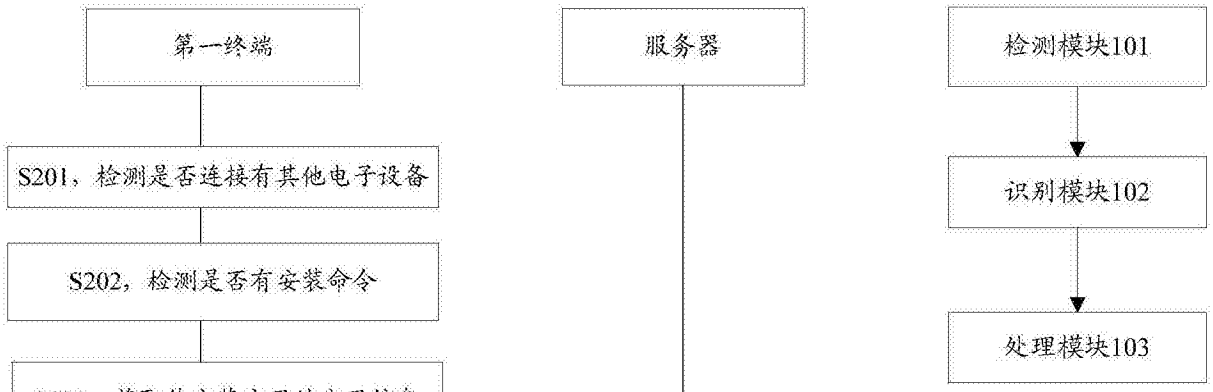

检测模块101
识别模块102
处理模块103

图3-1

第一终端
服务器
S201，检测是否连接有其他电子设备
S202，检测是否有安装命令
S203，获取待安装应用的应用信息
S204，生成查询请求
S205，查询请求
S206，解析所述查询请求
S207，得到识别结果
S208，查询响应
S209，接收所述服务器发送的查询响应
S210，解析所述查询响应
S211，据识别结果对待安装应用进行处理

图2

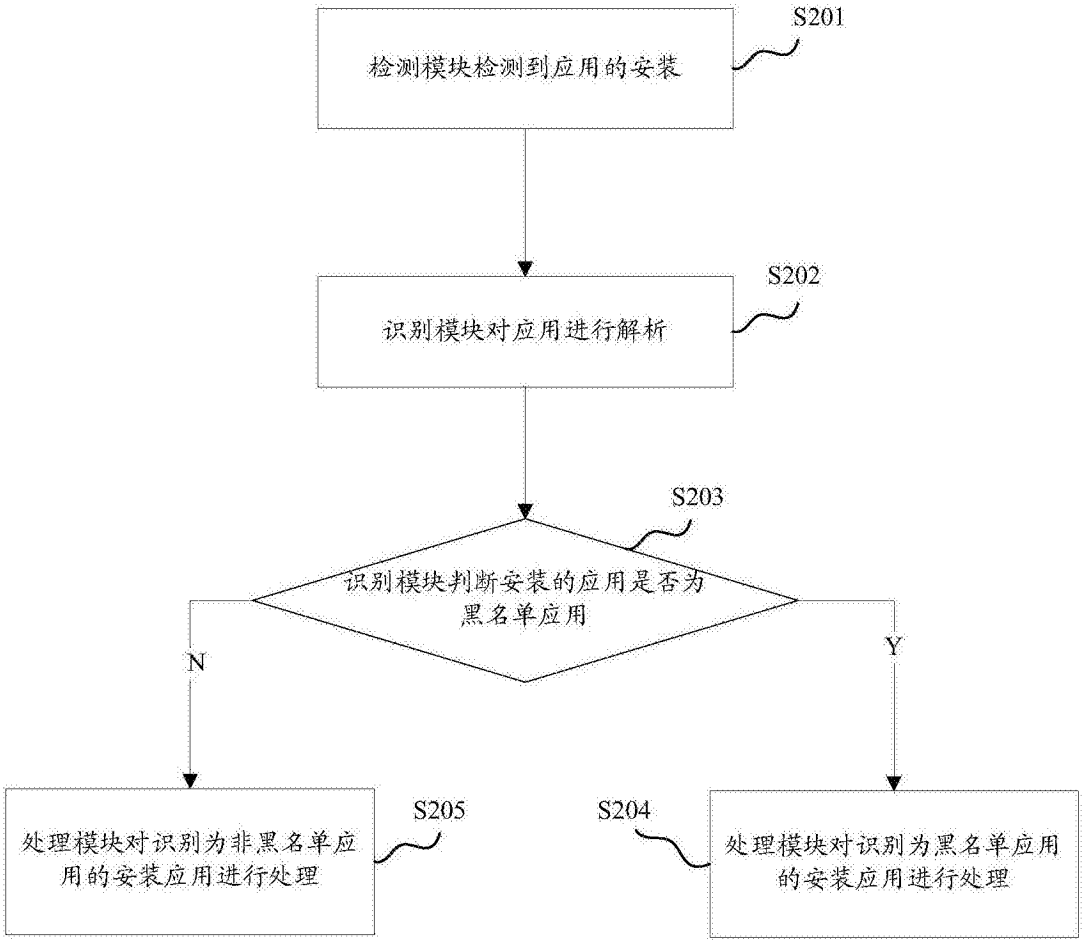

S201
检测模块检测到应用的安装
S202
识别模块对应用进行解析
S203
识别模块判断安装的应用是否为黑名单应用
N
Y
S205
处理模块对识别为非黑名单应用的安装应用进行处理
S204
处理模块对识别为黑名单应用的安装应用进行处理

图3-2

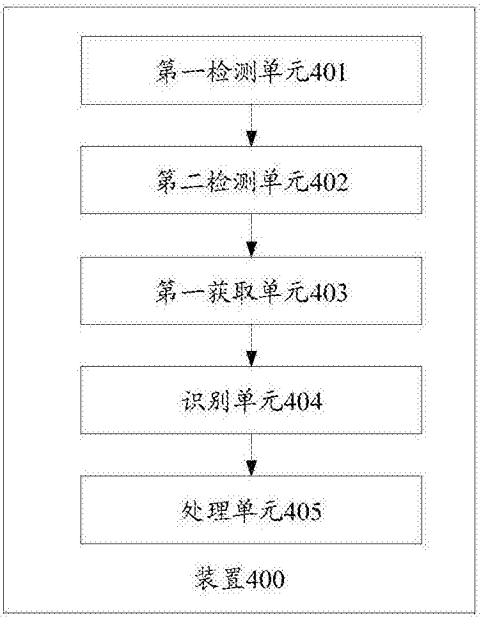

第一检测单元401
第二检测单元402
第一获取单元403
识别单元404
处理单元405
装置400

图4-1

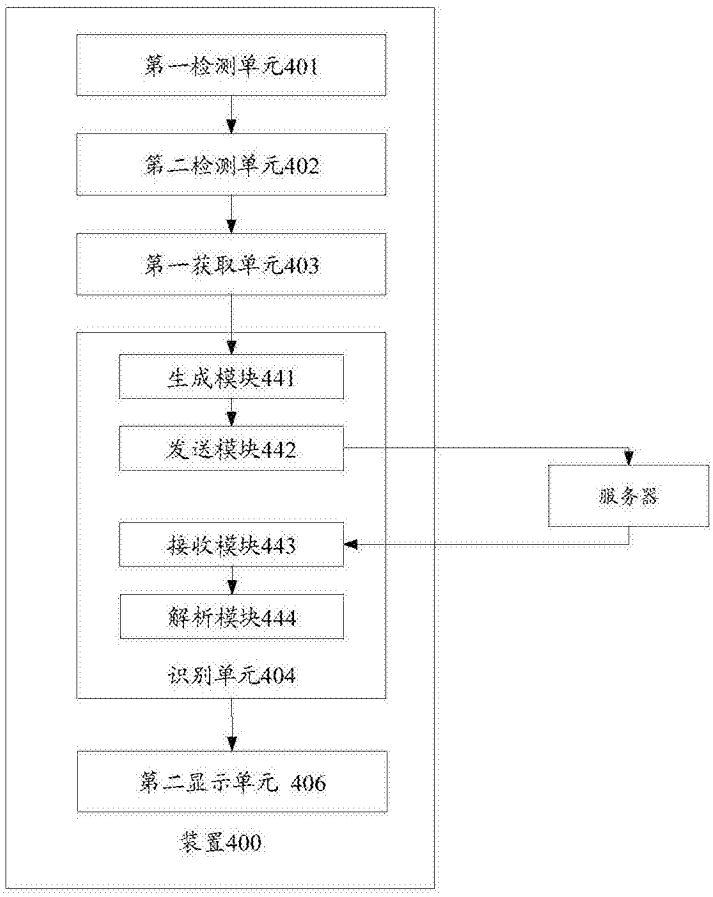

第一检测单元401
第二检测单元402
第一获取单元403
生成模块441
发送模块442
服务器
接收模块443
解析模块444
识别单元404
第二显示单元 406
装置400

图4-2