(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 9 月 21 日 (21.09.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/157192 A1

(51) 国际专利分类号:
G06F 21/55 (2013.01)

(21) 国际申请号: PCT/CN2017/075643

(22) 国际申请日: 2017 年 3 月 3 日 (03.03.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610145990.7 2016 年 3 月 15 日 (15.03.2016) CN

(71) 申请人: **华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: **张朋 (ZHANG, Peng)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **王季 (WANG, Ji)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **李辉 (LI, Hui)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **谢红亮 (XIE, Hongliang)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **王小璞 (WANG, Xiaopu)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: **北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS)**; 中国北京市海淀区知春路 7 号致真大厦 A1304-05 室, Beijing 100191 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: DATA INPUT METHOD, DEVICE AND USER EQUIPMENT

(54) **发明名称**: 一种数据输入方法、装置及用户设备

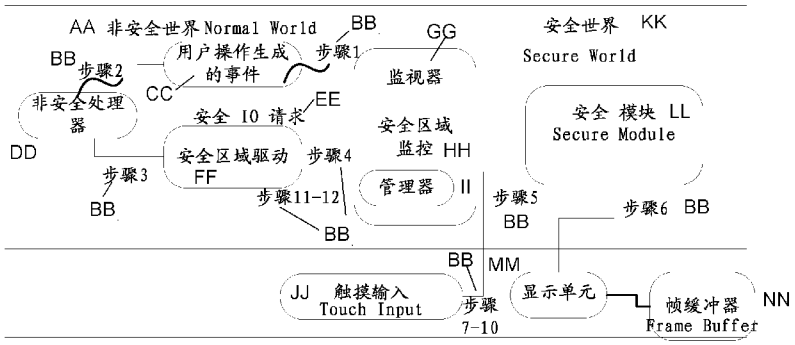

图 5

AA Normal world
BB Step
CC Event generated by user operation
DD Normal processor
EE Secure IO request
FF Secure zone driving
GG Monitor
HH Secure zone monitoring
II Manager
JJ Touch input
KK Secure world
LL Secure module
MM Display unit
NN Frame buffer

(57) **Abstract**: Disclosed are a data input method, a device and a user equipment. The method comprises: if it is determined that a user does not perform, in a preset display area, an operation on user equipment (UE), allocating an event corresponding to the operation to a first operating environment to be processed. The preset display area operates in a second operating environment of the UE, and a security level of the second operating environment is higher than a security level of the first operating environment. The present invention can increase the security of an event generated when a user operates a program running in a normal world of the UE, and realize direct operation of an event running in the normal world.

(57) **摘要**: 一种数据输入方法、装置及用户设备，该方法包括：在确定出用户未在预设的显示区域中对用户设备 UE 执行操作时，将与操作对应的事件分发至第一运行环境中进行处理；其中，预设的显示区域运行在 UE 的第二运行环境中，第二运行环境的安全级别高于第一运行环境。能够较好地提高用户在用户设备的非安全世界中运行的程序进行操作时生成的事件的安全性，实现直接对运行在非安全世界中的事件进行操作。

WO 2017/157192 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种数据输入方法、装置及用户设备

本申请要求在2016年3月15日提交中国专利局、申请号为201610145990.7、发明名称为“一种数据输入方法、装置及用户设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及通信技术领域，尤其是涉及一种数据输入方法、装置及用户设备。

背景技术

随着通信技术的不断发展，用户设备（user equipment，UE）能够提供的应用功能也越来与强大，个人财产、隐私等数据也就越来越多的存储在用户设备中。

用户设备的不断发展，其系统功能也不断增加，随着系统功能的增加，用户设备的系统中不可避免地出现安全漏洞，不法分子可以利用这些安全漏洞入侵用户设备的系统，获得用户设备中存储的数据，用户输入操作与终端显示的的安全性就无法得到保证。以用户通过用户设备实现费用支付为例，用户在通过用户设备提供的界面输入数据的过程中，不法分子可以通过截获用户的输入事件以及用户设备的显示内容获取该用户的输入数据，再通过分析用于费用支付的应用所对应的已经存储的历史数据，就可以得知用户的账号，进而加上获取的用户在用户设备中输入的口令，用户的资金就存在严重的风险。基于此，业界提出信任区域(Trust Zone)技术。该技术提出将用户设备的硬件组成分为安全世界(secure world）与非安全世界 (normal world)，且安全世界只有通过监视器（monitor）才可以传输数据。其中，在非安全世界中运行用户设备的操作系统，在安全世界中运行的程序的安全级别高于非安全世界中运行的程序，安全世界通过硬件与非安全世界隔离，安全世界有权访问非安全世界中的全部数据，但反之不行。用户设备启动时，会首先进入安全世界，然后由安全世界中的程序负责切换到非安全世界，启动用户设备的操作系统。Trust Zone 技术提出了安全世界和非安全世界的概念，用于解决用户设备中数据输入安全的问题，通过提供运行在安全世界中的数据输入环境，用户可以在提供的数据输入环境中进行操作，输入账号、口令等事件，但是通常情况下，在安全世界中运行的数据输入环境在显示和输入相关的内容时，这些显示出的内容一般会覆盖用户设备的整个显示区域，当用户需要进行其它事件的操作时，例如用户正在输入用户名和密码时出现短消息弹窗，用户需要查看该短消息，此时在用户查看短消息的指令下系统需要退出数据输入环境，造成之前已经进行操作的事件丢失。因此，Trust Zone 技术无法完全解决用户在用户设备的非安全世界中运行的程序进行操作时生成的事件的安全性，也无法直接对运行在非安全世界中的事件进行操作。

发明内容

本发明提供了一种数据输入方法、装置及用户设备，能够较好地提高用户在用户设备的非安全世界中运行的程序进行操作时生成的事件的安全性，实现直接对运行在非安全世界中的事件进行操作。

第一方面，提供了一种数据输入方法，包括：在确定出用户未在预设的显示区域中对

UE 执行操作时，将与所述操作对应的事件分发至第一运行环境中进行处理；其中，所述预设的显示区域运行在所述 UE 的第二运行环境中，所述第二运行环境的安全级别高于所述第一运行环境，能够较好地提高用户在用户设备的非安全世界中运行的程序进行操作时生成的事件的安全性，实现直接对运行在非安全世界中的事件进行操作。

结合第一方面，在第一方面的第一种可能的实现方式中，该方法还包括：接收用户在显示单元为用户呈现的输入区域中进行操作，生成与操作对应的事件；判断该用户在输入区域中操作生成的事件是否是安全输入事件；如果判断结果为是，启动预设的显示区域，通过显示单元将预设的显示区域呈现给用户。

结合第一方面的第一种可能的实现方式，在第一方面的第二种可能的实现方式中，启动预设的显示区域，包括：备份当前第一运行环境中的事件；触发第二运行环境中的中断，通过第二运行环境中的中断，启动预设的显示区域。

对用户在运行在第一运行环境中的输入区域进行操作生成的对应的事件进行判断，确定该事件是否是安全输入事件，在判断结果为是时，进行第一运行环境到第二运行环境的切换，即为用户展示预设的显示区域，以使用户在对用户设备进行操作生成的安全输入时间可以切换到第二运行环境中进行处理，这样，能够较好地保障用户在用户设备中操作时生成的事件的安全性。

结合第一方面至第一面方面的第二种可能的实现方式中的任一一种可能的实现方式，在第一面的第三种可能的实现方式中，预设的显示区域和输入区域，同时呈现在用户设备的屏幕中。

结合第一方面，在第一方面的第四种可能的实现方式中，将与所述操作对应的事件分发至第一运行环境中进行处理，包括：将与所述操作对应的事件存储至共享存储区中，其中所述共享存储区是所述第一运行环境和所述第二运行环境共同使用的存储区；通过触发所述第一运行环境中的中断，将所述共享存储区中存储的所述事件分发至第一运行环境中进行处理。

结合第一方面的第四种可能的实现方式，在第一方面的第五种可能的实现方式中，通过触发所述第一运行环境中的中断，将所述共享存储区中存储的所述事件分发至第一运行环境中进行处理，包括：触发所述第一运行环境中的中断，并调用所述第一安全环境中的守护线程，以通过所述守护线程将所述共享存储区中存储的所述事件分发至第一运行环境中进行处理。

结合第一方面至第一方面的第五种可能实现的方式中的任一一种可能 实现方式，在第一方面的第六种可能的实现方式中，在确定出用户未在预设的显示区域中对用户设备UE执行操作之前，还包括：在确定出与所述操作对应的事件是安全输入事件时，显示所述预设的显示区域，以使用户在所述预设的显示区域中进行操作，其中所述安全输入事件是具有权限验证属性的数据输入事件。

结合第一方面至第一方面的第六种可能实现的方式中的任一一种可能 实现方式，在第一方面的第七种可能的实现方式中，将与所述操作对应的事件分发至第一运行环境中进行处理之后，还包括：隐藏所述预设的显示区域。能够提高用户操作的灵活性。

结合第一方面至第一方面的第六种可能实现的方式中的任一一种可能的 实现方式，在第一方面的第八种可能的实现方式中，所述预设的显示区域包含设定格式的输入编辑框。

结合第一方面的第八种可能的实现方式，在第一方面的第九种可能的实现方式中，所述设定格式的输入编辑框包含下述中的至少一种：设定的输入类型可以是九键盘数字类型、九键盘中文类型、九键盘字母类型、数字中文混合等输入类型。可以提高用户操作的便利性。

第二方面，提供一种数据输入装置，该数据输入装置具有实现上述第一方面和第一方面的第一种至第八种可能的实现方式中的任一种方法设计中终端行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块。

第三方面，提供了一种用户终端，该用户终端具有实现上述第一方面和第一方面的第一种至第八种可能的实现方式中的任一种方法设计中终端行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块。

结合第三方面，在第三方面的第一种可能的实现方式中，终端的结构包括存储器和处理器，其中，所述存储器用于存储一组程序，所述处理器用于调用所述存储器存储的程序以执行如上述第一方面和第一方面的第一种至第八种可能的实现方式中的任一种所述的方法。

第四方面，提供了一种计算机存储介质，用于储存为数据输入装置所用的计算机软件指令，其包含用于执行上述方面所设计的程序。

通过采用上述技术方案，在确定出用户未在预设的显示区域中对 UE 执行操作时，将与操作对应的事件分发至第一运行环境中进行处理，这样，用户在用户设备的非安全世界中运行的程序进行操作时，即使需要处理其它非安全事件，也能够保证用户在用户设备的非安全世界中运行的程序进行操作时生成的事件的安全性，实现直接对运行在非安全世界中的事件进行操作。

附图说明

图 1 本发明实施例提供的数据输入的方法应用的计算节点的逻辑结构示意图；

图 2 为本发明实施例提出的用户设备结构组成示意图；

图 3 为本发明实施例提出的用户设备结构组成示意图；

图 4 为本发明实施例提供的数据输入系统的安全世界硬件组成示意图；

图 5 为本发明实施例提出的数据输入方法流程图；

图 6 为本发明实施例提出的输入编辑框示意图；

图 7 为本发明实施例提出的预设的显示区域和输入区域示意图；

图 8 为本发明实施例提出的设定的输入类型示意图；

图 9 为本发明实施例提出的数据输入方法流程图；

图 10 为本发明实施例提出的数据输入装置结构组成示意图。

具体实施方式

针对 Trust Zone 技术无法完全解决用户在用户设备的非安全世界中运行的程序进行操作时生成的事件的安全性，也无法直接对运行在非安全世界中的事件进行操作的问题，本发明提出的技术方案中，在确定出用户未在预设的显示区域中对 UE 执行操作时，将与操

作对应的事件分发至第一运行环境中进行处理，其中，预设的显示区域运行在所述 UE 的第二运行环境中，第二运行环境的安全级别高于所述第一运行环境，从而能够较好地提高用户在用户设备的非安全世界中运行的程序进行操作时生成的事件的安全性，实现直接对运行在非安全世界中的事件进行操作。

下面将结合各个附图对本发明实施例技术方案的主要实现原理、具体实施方式及其对应能够达到的有益效果进行详细地阐述。

本发明实施例提出的技术方案中，以图 1 为例介绍本发明实施例提供的数据输入的方法应用的计算节点的逻辑结构。该计算节点可以是用户设备，该用户设备具体可以为桌面计算机、笔记本电脑、智能手机或平板电脑等。如图 1 所示，该用户设备的硬件层包括中央处理器（Center Processing Unit ，CPU）、图形处理器（Graphic Processing Unit，GPU）等，当然还可以包括存储器、输入/输出设备（Input Device）、网络接口等，输入设备可包括键盘、鼠标、触摸屏等，输出设备可包括显示设备如液晶显示器（Liquid Crystal Display， LCD）、阴极射线管(Cathode Ray Tube，CRT)、全息成像（Holographic）、投影（Projector）等。在硬件层之上可运行有操作系统（如 Android 等）以及一些应用程序。核心库层是操作系统的核心部分，包括输入/输出服务、核心服务、图形设备接口以及实现 CPU、GPU 图形处理的图形引擎（Graphics Engine）等。图形引擎可包括 2D 引擎、3D 引擎、合成器（Composition）、帧缓冲区（Frame Buffer）等。核心库层还包括输入法服务。其中，输入法服务包括终端自带的输入法服务。输入法服务还包含本发明实施例提出的数据输入方法。除此之外，该终端还包括驱动层、框架层和应用层。驱动层可包括 CPU 驱动（driver）、GPU 驱动、显示控制器驱动、安全区域驱动（Trust Zone Driver）等。框架层可包括图形服务（Graphic Service）、系统服务（System service）、网页服务（Web Service）和用户服务（Customer Service）等；图形服务中，可包括如微件（Widget）、画布（Canvas）、视图（Views）、Render Script 等。应用层可包括桌面（launcher）、媒体播放器（Media Player）、浏览器（Browser）等。

在 Trust Zone 技术中，用户设备的硬件和程序指令在运行时，可包含两个运行环境，分别是安全运行环境和非安全运行环境，非安全运行环境，也可以称之为非安全世界，对应本发明实施例提出的第一运行环境，安全运行环境，也可以称之为安全世界，对应本发明实施例提出的第二运行环境。在安全运行环境中运行的程序以及用户设备的硬件的安全级别要高于非安全运行环境中运行的程序以及用户设备的硬件的安全级别。其中，安全世界也可以是用户设备的操作系统中隔离出来的虚拟运行环境。

本发明实施例提出的数据输入方法所应用的用户设备，如图 2 所示，该用户设备 200 包括：至少一个处理器 201，至少一个网络接口 204 或者其他用户接口 203，存储器 205，至少一个通信总线 202。通信总线 202 用于实现这些组件之间的连接通信。该用户设备 200 可选的包含用户接口 203，包括显示器（例如图 1 所示的 LCD、CRT、全息成像（Holographic）或者投影（Projector）等），键盘或者点击设备（例如，鼠标，轨迹球（trackball），触感板或者触摸屏等）。

存储器 205 可以包括只读存储器和随机存取存储器，并向处理器 201 提供存储器 205 中存储的程序指令和数据。存储器 205 的一部分还可以包括非易失性随机存取存储器（NVRAM）。

在一些实施方式中，存储器 205 存储了如下的元素，可执行模块或者数据结构，或者

他们的子集，或者他们的扩展集:

操作系统 2051，包含各种系统程序指令，该程序指令可运行在例如图 1 所示的框架层、核心库层、驱动层等，用于实现各种基础业务以及处理基于硬件的任务。

其中，在本发明实施例提出的技术方案中，操作系统不仅看运行在第一运行环境中，操作系统还可运行在安全级别高于第一运行环境的第二运行环境中。

应用程序 2052，包含各种应用程序，例如图 1 所示的桌面(launcher)、媒体播放器(Media Player)、浏览器（ Browser ）以及输入法应用等，用于实现各种应用业务。

应用程序 2052 中的各种应用程序，可以应用在第一运行环境中，也可以运行在第二运行环境中，在本发明实施例上述提出的技术方案中，应用程序 2052 中 ，存储的实现数据输入方法的程序指令，该程序指令运行在第二运行环境中。

在本发明实施例中，存储器 205 也可以称之为存储区域，用于存储数据输入方法的程序，以及存储操作系统。

处理器 201 通过调用存储器 205 存储的程序指令，处理器 201 用于按照获得的程序指令执行: 在确定出用户未在预设的显示区域中对 UE 执行操作时，将与操作对应的事件分发至第一运行环境中进行处理。

可选地，作为一个实施例，处理器 201 还用于: 在确定出与操作对应的事件是安全输入事件时，显示预设的显示区域，以使用户在预设的显示区域中进行操作，其中安全输入事件是具有权限验证属性的数据输入事件。

进一步地，处理器 201 具体用于: 将与操作对应的事件存储至共享存储区中，其中共享存储区是第一运行环境和第二运行环境共同使用的存储区;

该用户设备还包括第一运行环境中的中断（图 2 中未示出），处理器 201 触发第一运行环境中的中断，第一运行环境中的中断将共享存储区中存储的事件分发至第一运行环境中进行处理。进一步地，处理器 201 具体用于: 触发第一运行环境中的中断，并调用第一安全环境中的守护线程，以通过守护线程将共享存储区中存储的事件分发至第一运行环境中进行处理。

进一步地，处理器 201 具体用于: 隐藏预设的显示区域。

本发明实施例提出的提出数据输入方法所应用的用户设备，该用户设备可以为手机、平板电脑、个人数字助理（ Personal Digital Assistant，PDA ）等。参考图 3 所示，为用户设备 300 的其中一种结构组成示意图。

该用户设备 300 主要包括，存储器 320、处理器 360 及输入单元 330，该输入单元 330 用于接收用户在终端上进行操作时的生成的事件。该存储器 320 用于存储操作系统和各种应用程序的程序指令。

其中，本发明实施例提出的技术方案中，提出了第一运行环境和第二运行环境，相应地，存储器 320 可以划分为安全存储器（也可以称之为安全存储区）、非安全存储器（也可以称之为非安全存储区）和共享存储器（也可以称之为共享存储区）。非安全存储器设置在第一运行环境中，安全存储器设置在第二运行环境中，第二运行环境的安全级别高于第一运行环境。设置在第一运行环境中的处理器或中断，不能够直接访问第二运行环境中的安全存储器。在第二运行环境中的处理器或中断，可以访问设置在第一运行环境中的非安全处理器，以及访问非安全存储区。对于共享存储器，共享存储器中存储的数据，是第一运行环境和第二运行环境中的处理器或中断都可以访问的数据，即第一运行环境和第二

运行环境中的处理器，或中断，可以通过访问共享存储器，获得共享存储器中的数据。

可以理解的，处理器 360 的具体实现功能可参见上述处理器 201 的详细阐述，不再赘述。

存储器 320 可以是用户设备 300 的内存，该内存可以划分为三个存储空间，分别对应设置在第一运行环境中的安全内存、设置在第二环境中的非安全内存以及第一运行环境和第二运行环境中的应用程序或者硬件都可以访问的共享内存。安全内存、非安全内存以及共享内存的空间划分，可以划分相同的大小，也可以根据存储数据输入事件的不同，划分不同的大小。

用户设备中的输入单元 330 可用于接收用户输入的数字或字符信息，以及产生与用户设备 300 的用户设置以及功能控制有关的信号输入。具体地，本发明实施例中，该输入单元 330 可以包括触控面板 331。触控面板 331，可收集用户在其上（比如用户使用手指、触笔等任何适合的物体或附件在触控面板 331 上）的操作，并根据预先设定的程序指令，驱动与触控面板 331 相应的连接装置。可选的，触控面板 331 可包括触摸检测装置和触摸控制器两个部分。其中，触摸检测装置检测用户的触摸方位，并检测触摸操作带来的信号，将信号传送给触摸控制器；触摸控制器从触摸检测装置上接收触摸信息，并将它转换成触点坐标，再送给该处理器 360，并能接收处理器 360 发来的命令并加以执行。此外，可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触控面板 331。除了触控面板 331，输入单元 330 还可以包括其他输入设备 332，其他输入设备 332 可以包括但不限于物理键盘、功能键（比如音量控制按键、开关按键等）、轨迹球、鼠标、操作杆等中的一种或多种。

该用户设备 300 还可以包括显示单元 340，该显示单元 340 可用于显示由用户输入的信息或提供给用户的信息以及用户设备 300 的各种菜单界面。该显示单元 340 可包括显示面板 341，可选的，可以采用液晶显示器（Liquid Crystal Display，LCD）或有机发光二极管（Organic Light-Emitting Diode, OLED）等形式来配置显示面板 341。

请参考图 3 所示，本发明实施例中，该触控面板 331 覆盖该显示面板 341，形成触摸显示屏，触摸显示屏提供给用户预设的显示区域。当该触摸显示屏 7 检测到在其上或附近的触摸操作后，传送给处理器 360 以确定触摸事件的类型，随后处理器 360 根据触摸事件的类型在触摸显示屏上提供相应的视觉输出。

本发明实施例中，该触摸显示屏包括不同的显示区域。每一个显示区域可以包含至少一个应用程序的图标和/或 widget 桌面控件等界面元素。

该处理器 360 是用户设备 300 的控制中心，利用各种接口和线路连接整个手机的各个部分，通过运行或执行存储在该存储器 320 内的软件程序和/或模块，执行用户设备 300 的各种功能和处理数据，从而对用户设备 300 进行整体监控。

可以理解的，该处理器 360 初始化时，首先进入第二运行环境，在第二运行环境中进行操作系统的初始化设置，以保证操作系统的安全性。

其中，初始化设置包括监控模式的初始化。在系统初始化过程中，用户设备的操作系统中的所有内存（安全内存、非安全内存以及共享内存）处于第二运行环境中。然后将需要在第一运行环境中运行的操作系统镜像加载到非安全内存中，再转至运行第一运行环境中的系统镜像。

可选的该用户设备 300 还可以包括 RF 电路 310，用于提供无线连接的 WIFI 模块 380，

以及电源 390 和用于提供声音输入输出的音频电路 370。

基于图 3 所示的带有触摸显示屏的用户设备 300，本发明实施例提出的技术方案中，将数据输入方法的运行环境划分为非安全世界（第一运行环境）和安全世界(第二运行环境)。在硬件组成上，一个用户设备中的只有一套硬件结构。但是，该些硬件中，部分硬件是的安全属性是可以进行动态设置的，而其他硬件的安全属性是固定不变的。整个系统的安全是通过将片上系统（System on Chip， SoC）的硬件资源和软件资源划分到两个世界获得的。安全世界和非安全世界是安全子系统对应的安全世界，以及其他子系统对应的非安全世界。

如图 4 所示， SoC 系统包括处理器（Core）401。在处理器架构上，每个物理的处理器核提供两个虚拟核，一个是非安全核（Non-secure，NS），另一个是安全核（Secure），在非安全核和安全核之间切换的机制称之为监控（monitor）模式。非安全核只能访问 NS 的系统资源，而安全核能够访问用户设备中的所有资源。在 SoC 中，还包括直接内存访问（Direct Memory Access ，DMA）402、安全的随机存储器（Secure Random Access Memory，Secure RAM）403、用于启动的安全只读存储器（Secure Boot Read Only Memory，Secure Boot ROM）404、集成 Trust Zone 支持的可在第一运行环境与第二运行环境下工作的中断控制器（Generic Interrupt Controller，GIC）405，在实现上可能会单独实现一个 Trust Zone 中断控制器(Trust Zone Interrupt Controller ，TZIC)406。SoC 还包括用于支持安全中断的信任区域地址空间控制器（Trust Zone Address Space Controller，TZASC）407、信任区域地址空间保护控制器（Trust Zone Protection Controller，TZPC）408、动态内存控制器（Dynamic Memory Controller，DMC）409、动态 RAM(Dynamic RAM)410 等。TZPC 用于设置外围设备的安全属性，例如，它可设置显示单元属性为安全的，这样在第一运行环境中的操作就无法访问这些设置为安全的设备。TZASC 用于控制对 DRAM 的安全属性划分，它可将一部分 DRAM 设置为安全的，其余部分设为非安全的，如果处于第一运行环境中的处理器对安全的内存发起访问请求时该访问请求会被拒绝。第一运行环境中的 DMA 对安全内存的访问会被拒绝，这样保证了安全内存不被第一运行环境下的任何操作系统或硬件访问。GIC 负责控制所有中断信息，它可将某些中断设置为安全的，某些中断设置为普通的。

SoC 组件之间通过高速可拓展接口（Advanced eXtensible Interactive，AXI）411 相互连接。SoC 与外围设备是通过高速可拓展接口先进的可扩展的外围总线桥（Advanced eXtensible Interactive to Advanced Peripheral Bus Bridge ，AXI2APB）桥 412 进行通信，AXI2APB 可感知当前访问外围设备的事件的安全属性，当第一运行环境中的事件访问一个属性被设为安全的外围设备时，AXI2APB 会拒绝该访问。安全 RAM 与安全 ROM 利用软硬件机制进行隔离，它们用于存储第二运行环境中运行的操作系统。

本发明实施例提出的数据输入方法中，SoC 系统在上电后进行初始化，系统在启动时，首先进入第二运行环境，在第二运行环境中进行初始化设置。初始化设置包括第二运行环境中的操作系统的初始化。在系统初始化过程中，用户设备的操作系统中的所有内存处于第二运行环境中。然后将需要在第一运行环境中运行的操作系统镜像加载到内存，并给第一运行环境分配部分内存，为第一运行环境分配的部分内存的安全属性被设置为非安全的，再转至运行第一运行环境中的系统镜像。

下面详细阐述本发明实例提出的数据输入方法的处理流程，首先阐述将第一运行环境中的事件转入到第二运行环境中处理的具体实施过程，如图 5 所示:

步骤 1，显示单元为用户呈现输入区域，用户在该输入区域中进行操作，生成与操作对应的事件。

以用户在显示单元呈现的输入区域中输入数字类型的支付口令为例进行详细阐述。显示单元可以包含具有触摸性质的触控面板。用户通过触摸触控面板，在输入区域中输入支付账号，在输入支付账号后，继续输入支付口令。处理器接收用户操作触控面板生成的事件。具体地，可以是第一运行环境中的非安全核，接收用户操作触控面板生成的事件。

步骤 2，处理器判断该用户在输入区域中操作生成的事件是否是安全输入事件。如果确定出不是安全输入事件，用户继续在输入区域中进行操作，生成与操作对应的事件，处理器继续处理该事件。

安全输入事件，是指需要用户输入具有权限验证属性的口令生成的事件。例如，某一支付应用，在用户输入用户名之后，需要用户继续输入与该用户名对应的支付口令，在支付口令和用户名匹配之后，完成支付。则用户继续输入与该用户名对应的支付口令的操作对应的事件，即为安全输入事件。

其中，可以预先对显示单元呈现的输入区域的安全属性进行编辑。将输入区域设置为运行在第一运行环境中的非安全显示区域和运行在第二运行环境中的安全显示区域。例如，在具体实施过程中，如图 6 所示，第一运行环境中的输入区域可以是一个具有固定形状和大小的输入编辑框，输入编辑框可以是任何形状，如图 6 所示，仅以方形为例进行示意。在进行设置时，可以对该输入编辑框增加一个安全属性，并对安全属性进行设置。例如，安全属性设置为数字属性，即当接收到的用户在该输入编辑框中操作的事件是触发数字输入时，判断该事件是安全输入事件。

后文将继续以用户输入数字类型的支付口令为例进行详细阐述。在用户将要输入数字类型的支付口令时，例如用户支付口令为 12345678，用户触发数字时，确定用户操作的数据输入事件是安全输入事件。

步骤 3，处理器在确定出用户操作的数据输入事件是安全输入事件时，触发 TZ driver。TZ driver 触发第一运行环境和第二运行环境之间进行切换所使用的监控（monitor）模式，处理器将通过 monitor，进入到第二运行环境。

步骤 4，处理器在 monitor 模式中备份当前第一运行环境中的事件。处理器触发第一运行环境中的中断，将当前确定出的安全输入事件保存才共享存储区中。在安全输入事件存储完毕之后，monitor 模式下触发第二运行环境中的中断，通过第二运行环境中的中断，触发第二运行环境中的处理器，即安全核。

步骤 5，安全核（即第二运行环境中的处理器）触发中断，启动预设的显示区域，通过显示单元将预设的显示区域呈现给用户。用户之后的操作，将在预设的显示区域中进行操作。

预设的显示区域，运行在第二运行环境中，该预设的显示区域可以是用户设备屏幕中的一部分，用户可以在该预设的显示区域中进行输入操作。相应地，该预设的显示区域可以是具有固定形状和大小，以及具备安全属性的输入编辑框。如图 7 所示，启动预设的显示区域，该预设的显示区域和输入区域，可以同时呈现在用户设备的屏幕中。预设的显示区域可以覆盖部分输入区域，叠加在部分输入区域之上。预设的显示区域，可以包括设定的输入类型。如图 8 所示，设定的输入类型可以是九键盘数字类型、九键盘中文类型（图 8 中未示出）、九键盘字母类型、数字中文混合等输入类型（图 8 中未示出）。

例如，启动预设的显示区域，假设设定的输入类型是九键盘数字类型的显示区域，在显示单元中，将九键盘数字类型的显示区域展示给用户，用户在九键盘数字类型的预设的显示区域中输入支付口令。

步骤 6，处理器将事件转入到第二运行环境中进行处理。

通过采用上述技术方案，对用户在运行在第一运行环境中的输入区域进行操作生成的对应的事件进行判断，确定该事件是否是安全输入事件，在判断结果为是时，进行第一运行环境到第二运行环境的切换，即为用户展示预设的显示区域，以使用户在对用户设备进行操作生成的安全输入时间可以切换到第二运行环境中进行处理，这样，能够较好地保障用户在用户设备中操作时生成的事件的安全性。

其次阐述将第二运行环境中的事件分发到第一运行环境中处理的具体实施过程，如图 5 所示：

步骤 7，用户在用户设备的预设的显示区域中进行操作。

步骤 8，第二运行环境中的处理器获得与该操作对应的事件。

预设的显示区域的详细阐述请参见上述步骤 5 中的详细阐述，不再赘述。

同样以用户输入数字类型的支付口令为例进行阐述。在步骤 8 中，用户预设的显示区域中输入支付口令。

步骤 9，处理器判断用户是否在预设的显示区域中对 UE 进行操作，如果判断结果为是，执行步骤 10，反之，执行步骤 12。

具体地，用户在显示单元的预设的显示区域中进行操作，也可以在预设的显示区域之外进行操作。与用户的操作生成的对应的事件，传输到安全核中，安全核判断该事件是否对应落入在预设的显示区域中的操作。例如用户预设的显示区域，输入支付口令，安全核确定用户的触摸点是否在预设的显示区域中。用户在操作时，如用户又触发输入账号类目时（即在输入区域中操作），则确定该用户未在预设的显示区域中进行操作，反之，确定该用户是在预设的显示区域中进行操作。例如，用户通过预设的显示区域输入支付口令 12345678，用户输入了 123，此时，用户设备接收到短消息展示、或者来电展示时，用户点击该短消息展示，此时用户对用户设备的操作落在短消息展示框中，该种情况下即确定用户未在预设的显示区域中对 UE 执行操作。

步骤 10，继续接收用户在预设的显示区域中对用户设备执行操作生成的事件。

步骤 11，处理器在确定出用户结束操作时，对接收到的事件进行验证处理，并转入到第一运行环境中，将验证处理结果反馈给用户。

例如，当用户结束输入支付口令时，在第二运行环境中，对接收到的支付口令进行验证，将验证结果反馈给用户。

步骤 12，处理器在确定出用户未在预设的显示区域中对用户设备执行操作时，将与该操作对应的事件分发至第一运行环境中进行处理。

其中，将与操作对应的事件分发至第一运行环境中进行处理，其实施方式可以包含下述两种方式：

第一种方式：可以通过触发中断，实现将与操作对应的事件分发至第一运行环境中进行处理。

上述第一种方式中，处理器可以触发第二运行环境中的中断，通过第二运行环境中的中断，将与用户的操作对应的事件存储至共享存储区中。此时，处理器在 monitor 模式中，

通过触发第一运行环境中的中断，将共享存储区中存储的事件分发至第一运行环境中进行处理。

例如，处理器触发快速中断请求（Fast Interrupt Reques, FIQ），将与用户的操作对应的事件存储至共享存储区中，然后处理器在 monitor 模式中，触发第一运行环境中的中断，在共享存储区中获得存储的事件，第一运行环境中的中断将获得的事件分发至第一运行环境中进行处理。

第二种方式：通过守护线程实现将与操作对应的事件分发至第一运行环境中进行处理。

上述第二种方式中，守护进程，是一个生存期较长的进程，通常独立于用户设备并且周期性地执行某种任务或等待处理某些发生的事件。守护进程一般在系统引导装入时启动，在系统关闭时终止。在上述第二种方式中，处理器可以通过触发第二运行环境中的中断，将与用户的操作对应的事件存储至共享存储区中，然后在 monitor 模式中，通过触发第一运行环境中的中断，通过第一运行环境中的中断，触发第一运行环境中的守护线程，守护线程在共享存储区中获得存储的事件，守护线程将获得的事件发送给第一运行环境中进行处理。

在上述两种将与操作对应的事件分发至第一运行环境中进行处理的具体实施方式中，在将事件进行分发之前，需要将当前事件保存到共享存储区中，此时，可以通过触发第二运行环境中的中断，通过第二环境中运行的中断，将事件存储在共享存储区中。也可以是显示单元驱动将事件传输给上层应用，通过上层应用将事件存储在共享存储区中。

可选地，在将与操作对应的事件分发至第一运行环境中进行处理之后，还包括：隐藏预设的显示区域。

例如，用户在输入 12345678 之后，不需要再进行任何输入，此时处理器隐藏预设的显示区域。

相应地，本发明实施例还提出一种数据输入方法，如图 9 所示，其具体处理流程如下述：

步骤 91，用户在用户设备的预设的显示区域中进行操作。

步骤 92，第二运行环境中的处理器获得与该操作对应的事件。

预设的显示区域的详细阐述请参见上述步骤 5 中的详细阐述，这里不再赘述。

同样以用户输入数字类型的支付口令为例进行阐述。用户在预设的显示区域中输入支付口令。

步骤 93，处理器判断用户是否在预设的显示区域中对 UE 进行操作，如果判断结果为是，执行步骤 94，反之，执行步骤 96。

步骤 94，继续接收用户在预设的显示区域中对用户设备执行操作生成的事件。

步骤 95，处理器在确定出用户结束操作时，对接收到的事件进行验证处理，并转入到第一运行环境中，将验证处理结果反馈给用户。

例如，当用户结束输入支付口令时，在第二运行环境中，对接收到的支付口令进行验证，将验证结果反馈给用户。

步骤 96，处理器在确定出用户未在预设的显示区域中对用户设备执行操作时，将与该操作对应的事件分发至第一运行环境中进行处理。

其中，将与操作对应的事件分发至第一运行环境中进行处理，其实施方式可以包含下

述两种方式:

第一种方式:可以通过触发中断,实现将与操作对应的事件分发至第一运行环境中进行处理。

上述第一种方式中,处理器可以触发第二运行环境中的中断,通过第二运行环境中的中断,将与用户的操作对应的事件存储至共享存储区中。此时,处理器在 monitor 模式中,通过触发第一运行环境中的中断,将共享存储区中存储的事件分发至第一运行环境中进行处理。

例如,处理器触发快速中断请求(Fast Interrupt Reques, FIQ),将与用户的操作对应的事件存储至共享存储区中,然后处理器在 monitor 模式中,触发第一运行环境中的中断,在共享存储区中获得存储的事件,第一运行环境中的中断将获得的事件分发至第一运行环境中进行处理。

第二种方式:通过守护线程实现将与操作对应的事件分发至第一运行环境中进行处理。

上述第二种方式中,守护进程,是一个生存期较长的进程,通常独立于用户设备并且周期性地执行某种任务或等待处理某些发生的事件。守护进程一般在系统引导装入时启动,在系统关闭时终止。在上述第二种方式中,处理器可以通过触发第二运行环境中的中断,将与用户的操作对应的事件存储至共享存储区中,然后在 monitor 模式中,通过触发第一运行环境中的中断,通过第一运行环境中的中断,触发第一运行环境中的守护线程,守护线程在共享存储区中获得存储的事件,守护线程将获得的事件发送给第一运行环境中进行处理。

在上述两种将与操作对应的事件分发至第一运行环境中进行处理的具体实施方式中,在将事件进行分发之前,需要将当前事件保存到共享存储区中,此时,可以通过触发第二运行环境中的中断,通过第二环境中运行的中断,将事件存储在共享存储区中。也可以是显示单元驱动将事件传输给上层应用,通过上层应用将事件存储在共享存储区中。

可选地,在将与操作对应的事件分发至第一运行环境中进行处理之后,还包括:隐藏预设的显示区域。

例如,用户在输入 12345678 之后,不需要再进行任何输入,此时处理器隐藏预设的显示区域。

相应地,本发明实施例还提出一种数据输入装置,如图 10 所示,其结构组成包括:

接收单元 1001,用于接收用户在预设的显示区域中对 UE 执行操作生成的事件。

判断单元 1002,用于确定用户是否在预设的显示区域中 UE 执行操作。

执行单元 1003,用于在确定出用户未在预设的显示区域中对 UE 执行操作时,将与操作对应的事件分发至第一运行环境中进行处理。

其中,预设的显示区域运行在 UE 的第二运行环境中,第二运行环境的安全级别高于第一运行环境。

可选地,上述装置中,所述执行单元 1003,具体用于将与所述操作对应的事件存储至共享存储区中,其中所述共享存储区是所述第一运行环境和所述第二运行环境共同使用的存储区;通过触发所述第一运行环境中的中断,将所述共享存储区中存储的所述事件分发至第一运行环境中进行处理。

具体地,所述执行单元 1003,具体用于触发所述第一运行环境中的中断,并调用所述

第一安全环境中的守护线程，以通过所述守护线程将所述共享存储区中存储的所述事件分发至第一运行环境中进行处理。

具体地，所述执行单元 1003，还用于在确定出与所述操作对应的事件是安全输入事件时，显示所述预设的显示区域，以使用户在所述预设的显示区域中进行操作，其中所述安全输入事件是具有权限验证属性的数据输入事件。

具体地，所述执行单元 1003，还用于将与所述操作对应的事件分发至第一运行环境中进行处理之后，隐藏所述预设的显示区域。

具体地，上述预设的显示区域包含具有安全属性的输入编辑框。

本发明还提供了一种计算机存储介质，用于储存为上述方面所述的数据输入装置所用的计算机软件指令，其包含用于执行上述方面所设计的程序。

本领域的技术人员应明白，本发明的实施例可提供为方法、装置（设备）、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、只读光盘、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、装置（设备）和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求

1、一种数据输入方法，其特征在于，包括:

在确定出用户未在预设的显示区域中对用户设备 UE 执行操作时，将与所述操作对应的事件分发至第一运行环境中进行处理;

其中，所述预设的显示区域运行在所述 UE 的第二运行环境中，所述第二运行环境的安全级别高于所述第一运行环境。

2、如权利要求 1 所述的方法，其特征在于，将与所述操作对应的事件分发至第一运行环境中进行处理，包括:

将与所述操作对应的事件存储至共享存储区中，其中所述共享存储区是所述第一运行环境和所述第二运行环境共同使用的存储区;

通过触发所述第一运行环境中的中断，将所述共享存储区中存储的所述事件分发至第一运行环境中进行处理。

3、如权利要求 2 所述的方法，其特征在于，通过触发所述第一运行环境中的中断，将所述共享存储区中存储的所述事件分发至第一运行环境中进行处理，包括:

触发所述第一运行环境中的中断，并调用所述第一安全环境中的守护线程，以通过所述守护线程将所述共享存储区中存储的所述事件分发至第一运行环境中进行处理。

4、如权利要求 1~3 任一所述的方法，其特征在于，在确定出用户未在预设的显示区域中对用户设备 UE 执行操作之前，还包括:

在确定出与所述操作对应的事件是安全输入事件时，显示所述预设的显示区域，以使用户在所述预设的显示区域中进行操作，其中所述安全输入事件是具有权限验证属性的数据输入事件。

5、如权利要求 1~3 任一所述的方法，其特征在于，将与所述操作对应的事件分发至第一运行环境中进行处理之后，还包括:

隐藏所述预设的显示区域。

6、如权利要求 1~5 任一所述的方法，其特征在于，所述预设的显示区域包含设定格式的输入编辑框。

7、一种数据输入装置，其特征在于，包括:

接收单元，用于接收用户在预设的显示区域中对 UE 执行操作生成的事件;

判断单元，用于确定用户是否在预设的显示区域中 UE 执行操作;

执行单元，用于在所述判断单元确定出用户未在预设的显示区域中对用户设备 UE 执行操作时，将与所述操作对应的事件分发至第一运行环境中进行处理; 其中，所述预设的显示区域运行在所述 UE 的第二运行环境中，所述第二运行环境的安全级别高于所述第一运行环境。

8、如权利要求 7 所述的装置，其特征在于，所述执行单元，具体用于将与所述操作对应的事件存储至共享存储区中，其中所述共享存储区是所述第一运行环境和所述第二运行环境共同使用的存储区; 通过触发所述第一运行环境中的中断，将所述共享存储区中存储的所述事件分发至第一运行环境中进行处理。

9、如权利要求 8 所述的装置，其特征在于，所述执行单元，具体用于触发所述第一运行环境中的中断，并调用所述第一安全环境中的守护线程，以通过所述守护线程将所述

共享存储区中存储的所述事件分发至第一运行环境中进行处理。

10、如权利要求 7~9 任一所述的装置，其特征在于，所述执行单元，还用于在确定出与所述操作对应的事件是安全输入事件时，显示所述预设的显示区域，以使用户在所述预设的显示区域中进行操作，其中所述安全输入事件是具有权限验证属性的数据输入事件。

11、如权利要求 7~9 任一所述的装置，其特征在于，所述执行单元，还用于隐藏所述预设的显示区域。

12、一种用户设备，其特征在于，包括:

存储器，用于存储程序指令;

处理器，用于在所述存储器中获得存储的程序指令，按照获得的程序执行: 在确定出用户未在预设的显示区域中对用户设备 UE 执行操作时，将与所述操作对应的事件分发至第一运行环境中进行处理;

其中，所述预设的显示区域运行在所述 UE 的第二运行环境中，所述第二运行环境的安全级别高于所述第一运行环境。

13、如权利要求 12 所述的用户设备，其特征在于，所述处理器，具体用于将与所述操作对应的事件存储至共享存储区中，其中所述共享存储区是所述第一运行环境和所述第二运行环境共同使用的存储区;

所述用户设备还包括第一运行环境中的中断;

所述处理器，具体用于触发所述第一运行环境中的中断;

所述第一运行环境中的中断，用于将所述共享存储区中存储的所述事件分发至第一运行环境中进行处理。

14、如权利要求 13 所述的用户设备，其特征在于，所述处理器，具体用于触发所述第一运行环境中的中断，并调用所述第一安全环境中的守护线程，以通过所述守护线程将所述共享存储区中存储的所述事件分发至第一运行环境中进行处理。

15、如权利要求 12~14 任一所述的用户设备，其特征在于，所述处理器，还用于在确定出与所述操作对应的事件是安全输入事件时，显示所述预设的显示区域，以使用户在所述预设的显示区域中进行操作，其中所述安全输入事件是具有权限验证属性的数据输入事件。

16、如权利要求 12~14 任一所述的用户设备，其特征在于，所述处理器，还用于隐藏所述预设的显示区域。

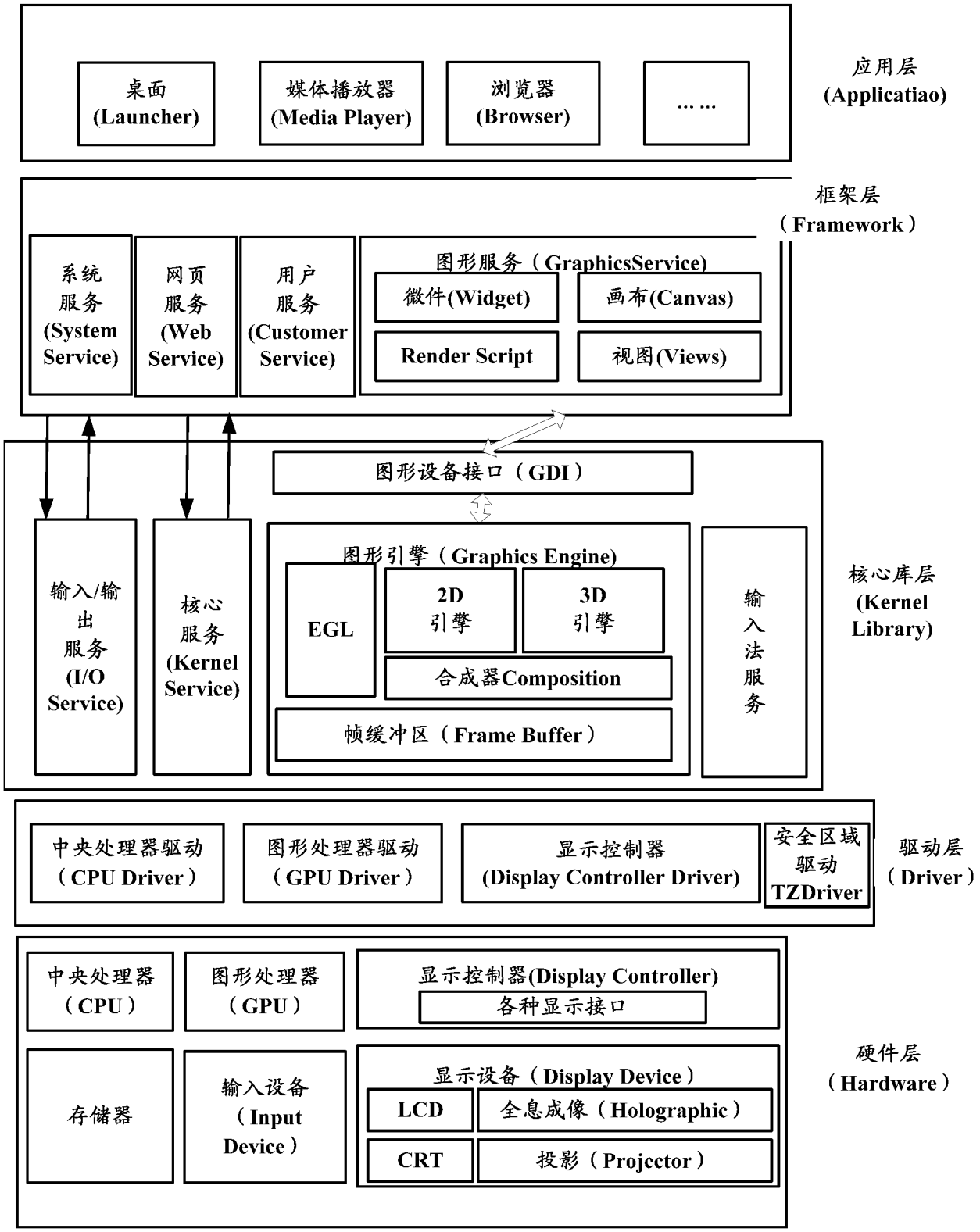
桌面
(Launcher)
媒体播放器
(Media Player)
浏览器
(Browser)
... ...
应用层
(Applicatiao)
框架层
（Framework）
系统
服务
(System
Service)
网页
服务
(Web
Service)
用户
服务
(Customer
Service)
图形服务（GraphicsService)
微件(Widget)
画布(Canvas)
Render Script
视图(Views)
图形设备接口（GDI）
输入/输
出
服务
(I/O
Service)
核心
服务
(Kernel
Service)
图形引擎（Graphics Engine)
EGL
2D
引擎
3D
引擎
合成器Composition
帧缓冲区（Frame Buffer）
输
入
法
服
务
核心库层
(Kernel
Library)
中央处理器驱动
（CPU Driver）
图形处理器驱动
（GPU Driver）
显示控制器
(Display Controller Driver)
安全区域
驱动
TZDriver
驱动层
（Driver）
中央处理器
（CPU）
图形处理器
（GPU）
显示控制器(Display Controller)
各种显示接口
存储器
输入设备
（Input
Device）
显示设备（Display Device）
LCD
全息成像（Holographic）
CRT
投影（Projector）
硬件层
（Hardware）

图 1

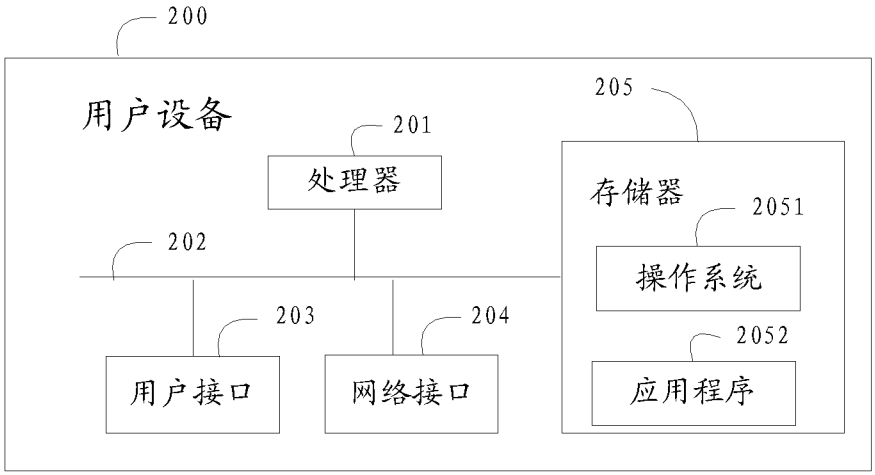
200
用户设备
201
处理器
205
存储器
2051
操作系统
202
203
204
2052
用户接口
网络接口
应用程序

图 2

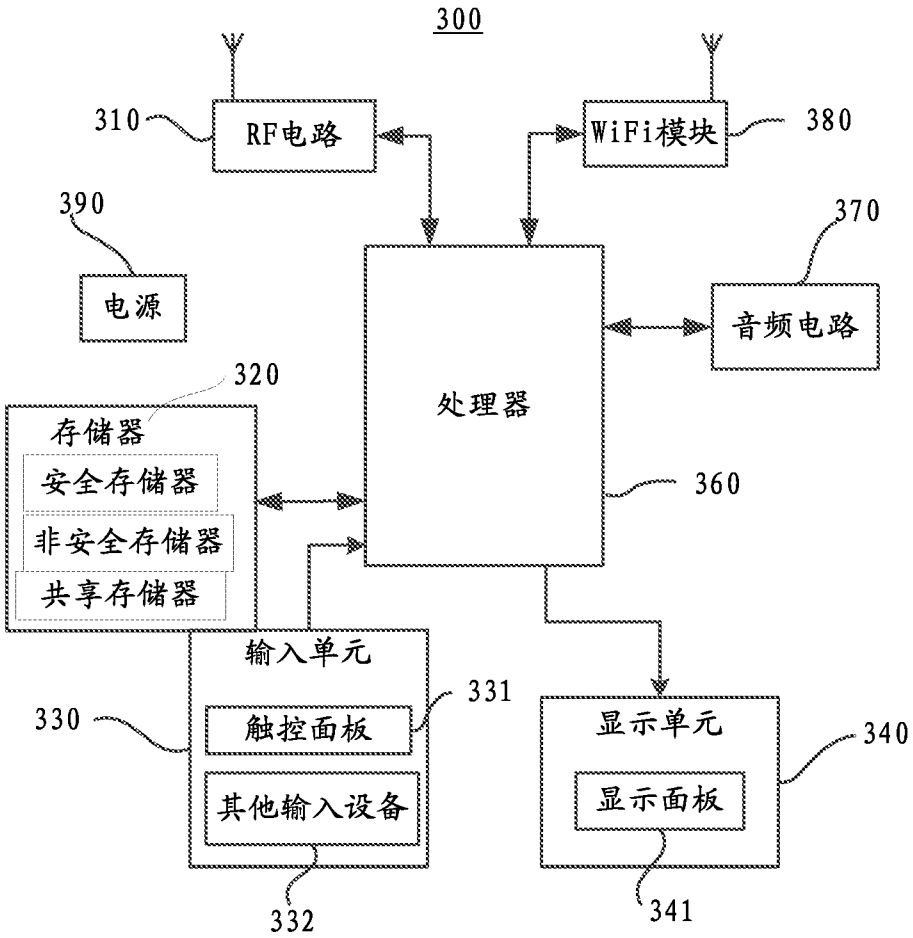
300
310
RF电路
WiFi模块
380
390
电源
370
音频电路
320
存储器
处理器
安全存储器
非安全存储器
共享存储器
360
输入单元
331
330
触控面板
显示单元
340
其他输入设备
显示面板
332
341

图 3

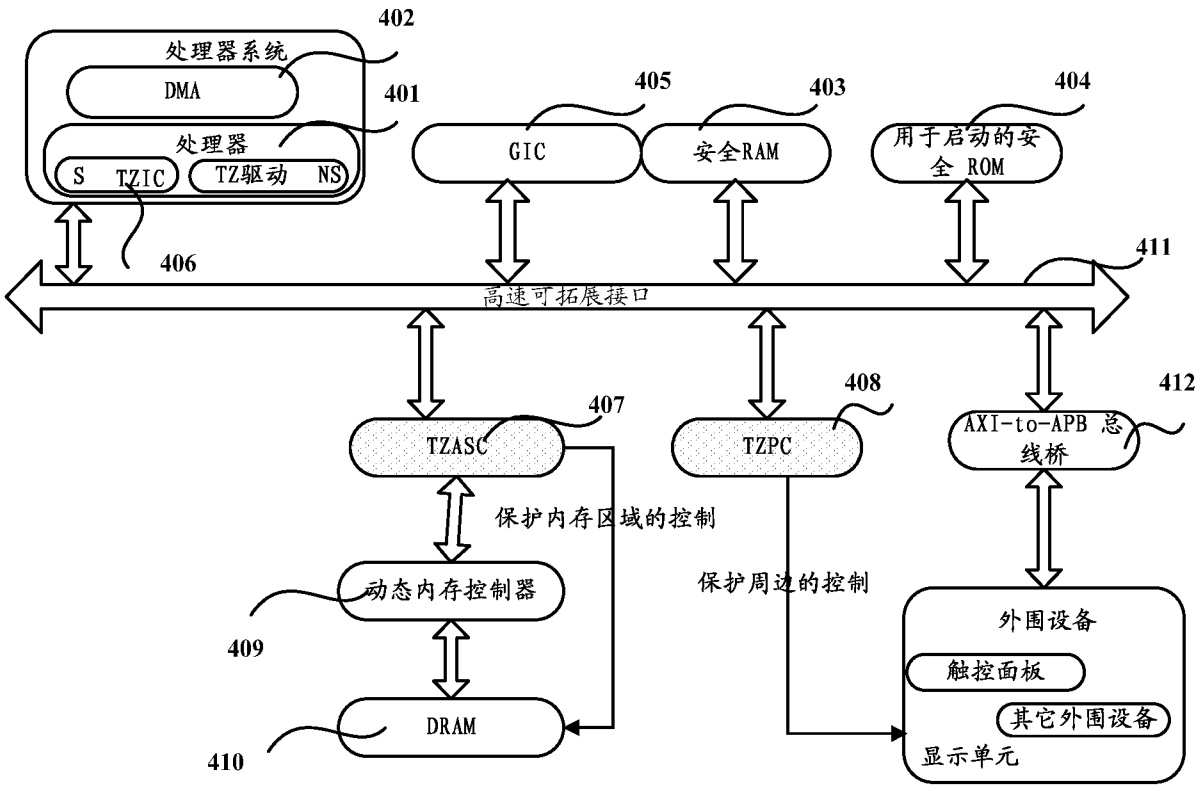
402
处理器系统
DMA
401
处理器
S TZIC
TZ驱动 NS
405
GIC
403
安全RAM
404
用于启动的安全 ROM
406
411
高速可拓展接口
407
TZASC
408
TZPC
412
AXI-to-APB 总线桥
保护内存区域的控制
动态内存控制器
409
DRAM
410
保护周边的控制
外围设备
触控面板
其它外围设备
显示单元

图 4

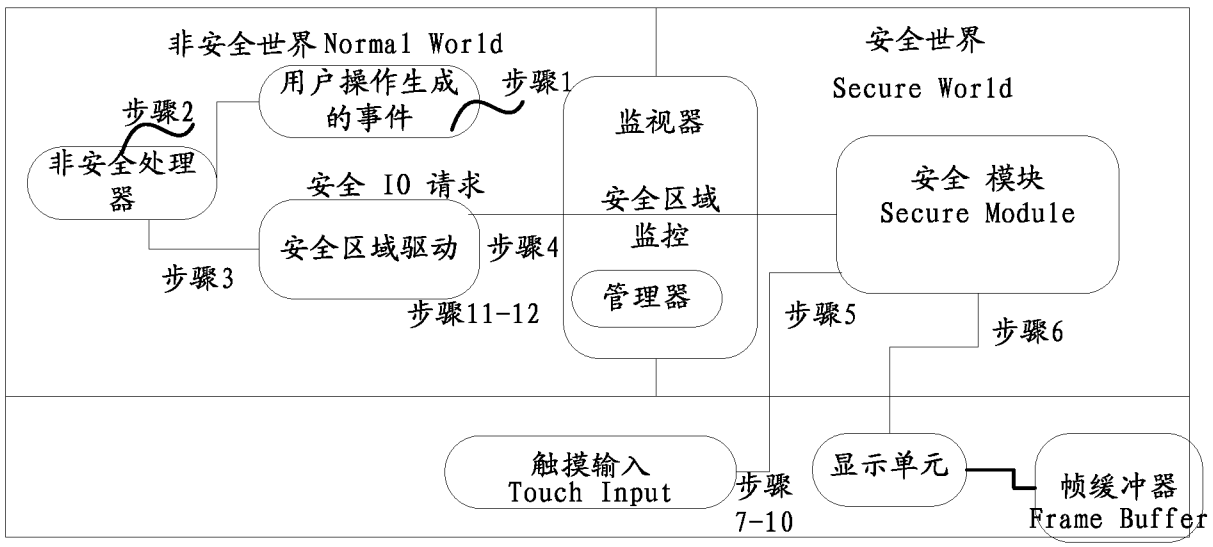
非安全世界 Normal World
安全世界
Secure World
用户操作生成的事件
步骤1
步骤2
非安全处理器
监视器
安全 IO 请求
安全区域监控
安全 模块
Secure Module
安全区域驱动
步骤4
步骤3
管理器
步骤11-12
步骤5
步骤6
触摸输入
Touch Input
步骤7-10
显示单元
帧缓冲器
Frame Buffer

图 5

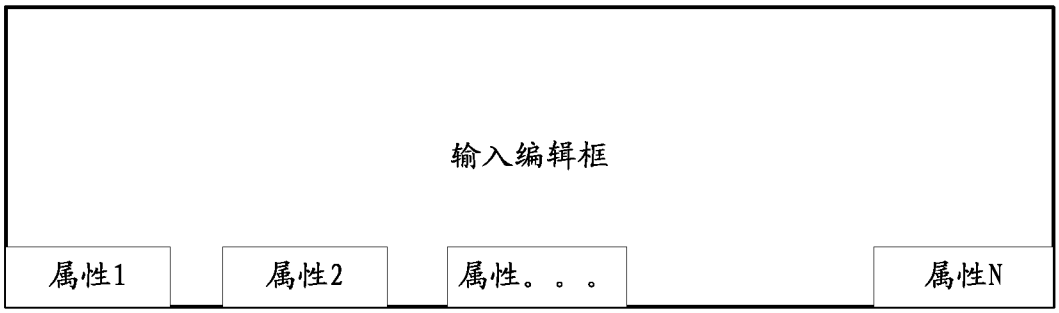

图 6

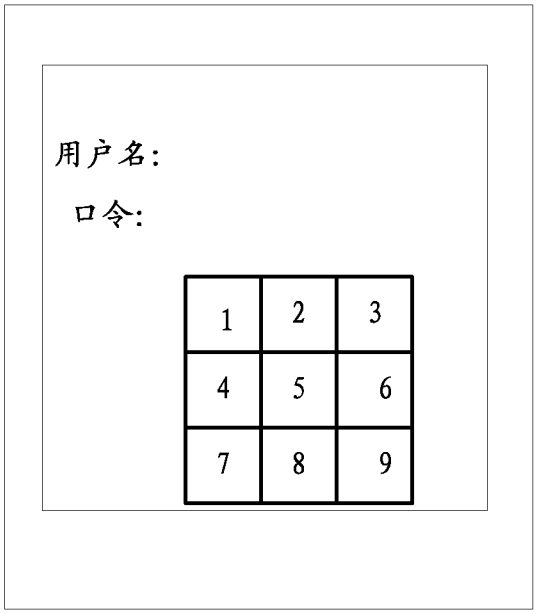

图 7

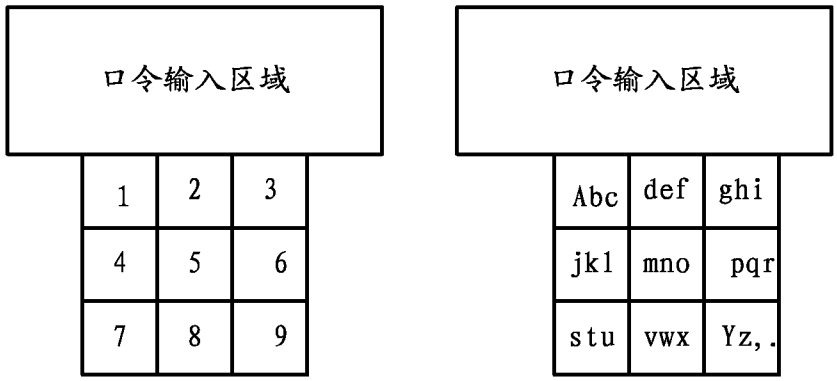
口令输入区域
1
2
3
4
5
6
7
8
9
口令输入区域
Abc
def
ghi
jkl
mno
pqr
stu
vwx
Yz,.

图 8

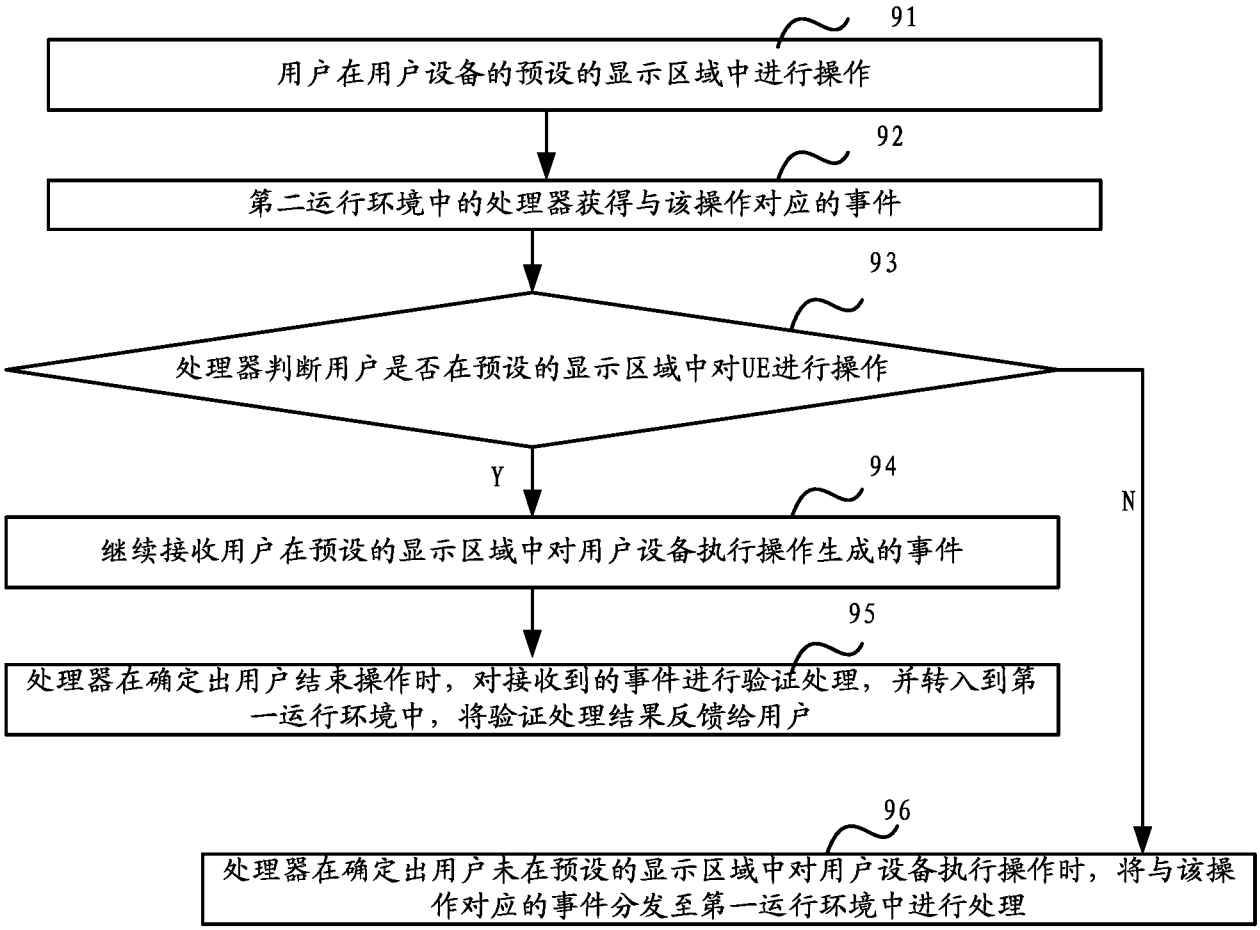
91
用户在用户设备的预设的显示区域中进行操作
92
第二运行环境中的处理器获得与该操作对应的事件
93
处理器判断用户是否在预设的显示区域中对UE进行操作
Y
N
94
继续接收用户在预设的显示区域中对用户设备执行操作生成的事件
95
处理器在确定出用户结束操作时，对接收到的事件进行验证处理，并转入到第一运行环境中，将验证处理结果反馈给用户
96
处理器在确定出用户未在预设的显示区域中对用户设备执行操作时，将与该操作对应的事件分发至第一运行环境中进行处理

图 9

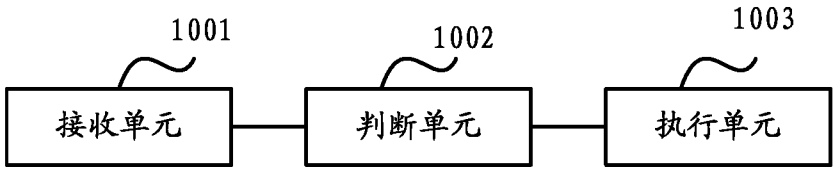

图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/075643

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/55 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, GOOGLE: non-secure zone, non-secure mode, untrusted zone, security zone, normal zone, security mode, normal mode, trust zone, normal zone, switch, virtual keyboard, security keyboard, password, sensitive information, input

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104239783 A (NEUSOFT CORPORATION), 24 December 2014 (24.12.2014), description, paragraphs [0003], [0048]-[0050] and [0053]-[0054], and figures 1-4	1-16
PX	CN 105825128 A (HUAWEI TECHNOLOGIES CO., LTD.), 03 August 2016 (03.08.2016), claims 1-16	1-16
A	CN 104115152 A (SAMSUNG SDI CO., LTD.), 22 October 2014 (22.10.2014), the whole document	1-16
A	US 2014101755 A1 (RESEARCH IN MOTION LIMITED), 10 April 2014 (10.04.2014), the whole document	1-16
A	CN 103714276 A (NXP B.V.), 09 April 2014 (09.04.2014), the whole document	1-16
A	CN 104933361 A (INSPUR ELECTRONIC INFORMATION INDUSTRY CO., LTD.), 23 September 2015 (23.09.2015), the whole document	1-16

☐ Further documents are listed in the continuation of Box C. ☒See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 May 2017 (25.05.2017)	**05 June 2017 (05.06.2017)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **DONG, Libo** Telephone No.:(86-10) **61648110**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/075643

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104239783 A	24 December 2014	JP 2016062581 A	25 April 2016
		US 2016088471A1	24 March 2016
CN 105825128 A	03 August 2016	None	
CN 104115152 A	22 October 2014	US 2013219507 A1	22 August 2013
		TW 201349008 A	01 December 2013
		WO 2013122443 A1	22 August 2013
		KR 20130101628 A	16 September 2013
		US 2015371051 A1	24 December 2015
		EP 2815347 A1	24 December 2014
US 2014101755 A1	10 April 2014	None	
CN 103714276 A	09 April 2014	US 2014096222 A1	03 April 2014
		EP 2713304 A1	02 April 2014
CN 104933361 A	23 September 2015	None	

国际检索报告

国际申请号 PCT/CN2017/075643

A. 主题的分类

G06F 21/55(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT, CNKI, WPI, EPODOC, GOOGLE: 安全区，非安全区，安全模式，非安全模式，可信区域，不可信区域，切换，虚拟键盘，安全键盘，密码，口令，敏感信息，输入，security zone, normal zone, security mode, normal mode, trust zone, normal zone, switch, virtual keyboard, security keyboard, password, sensitive information, input

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 104239783 A (东软集团股份有限公司) 2014年 12月 24日 (2014-12-24) 说明书第[0003], [0048]-[0050], [0053]-[0054]段，附图1-4	1-16
PX	CN 105825128 A (华为技术有限公司) 2016年 8月 3日 (2016-08-03) 权利要求1-16	1-16
A	CN 104115152 A (三星电子株式会社) 2014年 10月 22日 (2014-10-22) 全文	1-16
A	US 2014101755 A1 (RESEARCH IN MOTION LIMITED) 2014年 4月 10日 (2014-04-10) 全文	1-16
A	CN 103714276 A (NXP股份有限公司) 2014年 4月 9日 (2014-04-09) 全文	1-16
A	CN 104933361 A (浪潮电子信息产业股份有限公司) 2015年 9月 23日 (2015-09-23) 全文	1-16

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 5月 25日	2017年 6月 5日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 董立波 电话号码 (86-10)61648110

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/075643

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104239783	A	2014年 12月 24日	JP	2016062581	A	2016年 4月 25日
				US	2016088471	A1	2016年 3月 24日
CN	105825128	A	2016年 8月 3日		无		
CN	104115152	A	2014年 10月 22日	US	2013219507	A1	2013年 8月 22日
				TW	201349008	A	2013年 12月 1日
				WO	2013122443	A1	2013年 8月 22日
				KR	20130101628	A	2013年 9月 16日
				US	2015371051	A1	2015年 12月 24日
				EP	2815347	A1	2014年 12月 24日
US	2014101755	A1	2014年 4月 10日		无		
CN	103714276	A	2014年 4月 9日	US	2014096222	A1	2014年 4月 3日
				EP	2713304	A1	2014年 4月 2日
CN	104933361	A	2015年 9月 23日		无		