(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
2018 年 9 月 20 日 (20.09.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/166142 A1

(51) 国际专利分类号:
G06F 21/52 (2013.01)

(21) 国际申请号: PCT/CN2017/098408

(22) 国际申请日: 2017 年 8 月 22 日 (22.08.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710157752.2 2017年3月16日 (16.03.2017) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 孙延均 (SUN, Yanjun); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。

(74) 代理人: 北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE); 中国北京市海淀区学清路8号B座1601A, Beijing 100192 (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, JO, 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,

(54) **Title:** AUTHENTICATION PROCESSING METHOD AND APPARATUS

(54) **发明名称**: 验证处理方法及装置

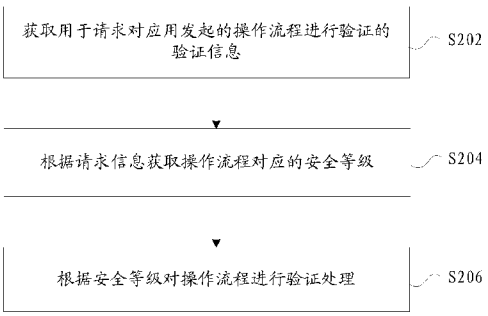

图 2

S202 Acquire authentication information used for requesting authentication of an operation process initiated by an application

S204 On the basis of the authentication information, acquire a security level corresponding to the operation process

S206 On the basis of the security level, perform authentication processing of the operation process

(57) **Abstract:** An authentication processing method, comprising: acquiring authentication information used for requesting authentication of an operation process initiated by an application; on the basis of the authentication information, acquiring a security level corresponding to the operation process; and, on the basis of the security level, performing authentication processing of the operation process.

(57) **摘要**: 一种验证处理方法包括: 获取用于请求对应用发起的操作流程进行验证的验证信息; 根据验证信息获取操作流程对应的安全等级; 根据安全等级对操作流程进行验证处理。

WO 2018/166142 A1

[见续页]

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)。

根据细则4.17的声明:

- 关于申请人有权申请并被授予专利(细则4.17(ii))
- 发明人资格(细则4.17(iv))

本国际公布:

- 包括国际检索报告(条约第21条(3))。

验证处理方法及装置

技术领域

本申请涉及但不限于通信领域，尤其是一种验证处理方法及装置。

背景技术

终端系统一般仅在应用程序启动时进行安全验证，也就是在用户点击应用图标想要启动应用的时候，会弹出一个密码验证界面。并且当前的验证方式是对于所有的应用都不加区别地采取完全一样的验证方式。

发明内容

以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

终端系统一般仅在应用程序启动时进行安全验证，也就是在用户点击应用图标想要启动应用的时候，会弹出一个密码验证界面，但是进入应用程序后，无法提供对于后续某一个界面或者操作的安全验证机制。并且当前的验证方式是对于所有的应用都不加区别地采取完全一样的验证方式。这样，如果应用没有在应用内部针对某一特定界面或者操作增加验证界面，那么就无法实施针对某一界面或者操作的安全验证机制，假如每个应用分别设计和实现，那么就大大增加了应用的开发难度，特别是对于提供高安全性的生物识别验证的界面由于涉及到操作系统权限的限制，第三方应用程序基本上不可能自行实现。

因此，如果仅在应用程序启动时进行安全验证，则无法对该应用的某一个界面或者操作进行安全验证，使得无法对应用进行精确的验证。

本文提供了一种验证处理方法及装置，能够避免如果仅在应用程序启动时进行安全验证，则无法对该应用的某一个界面或者操作进行安全验证。

本公开实施例提供了一种验证处理方法，包括：获取用于请求对应用发起的操作流程进行验证的请求信息；根据所述请求信息获取所述操作流程对

应的安全等级；根据所述安全等级对所述操作流程进行验证处理。

在一种示例性实施方式中，获取用于请求对所述应用发起的操作流程进行验证的所述请求信息包括：获取用于请求对所述应用发起的操作流程进行验证的第一请求信息，其中，所述第一请求信息携带有所述操作流程当前环境下对应的安全等级；或者，获取用于请求对所述应用发起的操作流程进行验证的第二请求信息，其中，所述第二请求信息携带有所述应用发起的所述操作流程的标识信息。

在一种示例性实施方式中，在获取用于请求对所述应用发起的操作流程进行验证的第二请求信息的情况下，根据所述第二请求信息获取所述操作流程对应的安全等级包括：根据所述第二请求信息携带的所述标识信息获取所述应用发起的操作流程；判断当前环境下是否存在与所述操作流程对应的安全等级；在判断结果为是的情况下，获取所述操作流程对应的安全等级。

在一种示例性实施方式中，根据所述安全等级对所述操作流程进行验证处理包括：根据所述安全等级确定与所述安全等级对应的安全验证序列；通过确定的安全验证序列验证输入的密令的合法性；在验证合法的情况下，确定所述操作流程合法。

在一种示例性实施方式中，在获取用于请求对所述应用发起的操作流程进行验证的所述请求信息之前，还包括：选择需要进行验证的所述操作流程；配置并保存所述操作流程的安全等级。

在一种示例性实施方式中，配置并保存所述操作流程的安全等级包括：本地配置并保存所述操作流程的安全等级；或者，通过网络侧配置并保存所述操作流程的安全等级。

本公开实施例还提供了一种验证处理装置，包括：接收模块，设置为：获取用于请求对应用发起的操作流程进行验证的请求信息；获取模块，设置为：根据所述请求信息获取所述操作流程对应的安全等级；处理模块，设置为：根据所述安全等级对所述操作流程进行验证处理。

在一种示例性实施方式中，所述接收模块，还设置为：获取用于请求对所述应用发起的操作流程进行验证的第一请求信息，其中，所述第一请求信息携带有所述操作流程当前环境下对应的安全等级；或者，获取用于请求对

所述应用发起的操作流程进行验证的第二请求信息，其中，所述第二请求信息携带有所述应用发起的所述操作流程的标识信息。

在一种示例性实施方式中，所述获取模块，还设置为：根据所述第二请求信息携带的所述标识信息获取所述应用发起的操作流程；判断当前环境下是否存在与所述操作流程对应的安全等级；在判断结果为是的情况下，获取所述操作流程对应的安全等级。

在一种示例性实施方式中，所述处理模块，还设置为：根据所述安全等级确定与所述安全等级对应的安全验证序列；通过确定的安全验证序列验证输入的密令的合法性；在验证合法的情况下，确定所述操作流程合法。

在一种示例性实施方式中，上述装置还包括：选择模块，设置为：选择需要进行验证的所述操作流程；确定模块，还设置为：配置并保存所述操作流程的安全等级。

在一种示例性实施方式中，所述确定模块，还设置为：本地配置并保存所述操作流程的安全等级；或者，通过网络侧配置并保存所述操作流程的安全等级。

本公开实施例还提供了一种存储介质。该存储介质设置为存储用于执行以下步骤的程序代码：获取用于请求对应用发起的操作流程进行验证的请求信息；根据所述请求信息获取所述操作流程对应的安全等级；根据所述安全等级对所述操作流程进行验证处理。

在一种示例性实施方式中，该存储介质设置为存储用于执行以下步骤的程序代码：获取用于请求对所述应用发起的操作流程进行验证的所述请求信息包括：获取对所述应用发起的操作流程进行验证的第一请求信息，其中，所述第一请求信息携带有所述操作流程当前环境下对应的安全等级；或者，获取用于请求对所述应用发起的操作流程进行验证的第二请求信息，其中，所述第二请求信息携带有所述应用发起的所述操作流程的标识信息。

在一种示例性实施方式中，该存储介质设置为存储用于执行以下步骤的程序代码：在获取用于请求对所述应用发起的操作流程进行验证的第二请求信息的情况下，根据所述第二请求信息获取所述操作流程对应的安全等级包括：根据所述第二请求信息携带的所述标识信息获取所述应用发起的操作流

程；判断当前环境下是否存在与所述操作流程对应的安全等级；在判断结果为是的情况下，获取所述操作流程对应的安全等级。

在一种示例性实施方式中，该存储介质设置为存储用于执行以下步骤的程序代码：根据所述安全等级对所述操作流程进行验证处理包括：根据所述安全等级确定与所述安全等级对应的安全验证序列；通过确定的安全验证序列验证输入的密令的合法性；在验证合法的情况下，确定所述操作流程合法。

在一种示例性实施方式中，该存储介质设置为存储用于执行以下步骤的程序代码：在获取用于请求对所述应用发起的操作流程进行验证的所述请求信息之前，还包括：选择需要进行验证的所述操作流程；配置并保存所述操作流程的安全等级。

在一种示例性实施方式中，该存储介质设置为存储用于执行以下步骤的程序代码：配置并保存所述操作流程的安全等级包括：本地配置并保存所述操作流程的安全等级；或者，通过网络侧配置并保存所述操作流程的安全等级。

本公开实施例还提供了一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令被执行时实现上述验证处理方法。

通过本公开实施例，获取用于请求对应用发起的操作流程进行验证的请求信息；根据所述请求信息获取所述操作流程对应的安全等级；根据所述安全等级对所述操作流程进行验证处理。由于根据操作的安全等级对应用发起的操作进行验证处理，使得应用的不同操作可以采用相应等级的安全验证方式。因此，可以避免如果仅在应用程序启动时进行安全验证，则无法对该应用的某一个界面或者操作进行安全验证，以及避免如果验证的方式都是单一的安全验证方式，则没有一种安全分级策略；提高了对应用安全验证的精确度。

在阅读并理解了附图和详细描述后，可以明白其他方面。

附图概述

图 1 是根据本公开实施例的一种验证处理方法的移动终端的硬件结构框

图；

图 2 是根据本公开实施例的验证处理方法的流程图；

图 3 是根据本公开实施例的操作流程安全分级保护框架示意图；

图 4 是根据本公开实施例的操作流程安全分级保护方法流程图；

图 5 是根据本公开实施例的安全验证控制模块的请求流程示意图；

图 6 是根据本公开实施例的安全验证序列的执行流程示意图；

图 7 是根据本公开实施例的安全策略模块确立操作流程安全等级的流程示意图；

图 8 是根据本公开实施例的验证处理装置的结构框图；

图 9 是根据本公开实施例的可选验证处理装置的结构框图。

本公开的较佳实施方式

下面结合附图对本公开的实施方式进行描述。

需要说明的是，本文中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

本申请实施例所提供的方法实施例可以在移动终端、计算机终端或者类似的运算装置中执行。以运行在移动终端上为例，图 1 是根据本公开实施例的一种验证处理方法的移动终端的硬件结构框图。如图 1 所示，移动终端 10 可以包括一个或多个（图中仅示出一个）处理器 102（处理器 102 可以包括但不限于微处理器 MCU（Micro Controller Unit，微控制器单元）或可编程逻辑器件 FPGA（Field Programmable Gate Array，现场可编程门阵列）等的处理装置）、设置为存储数据的存储器 104、以及设置为通信功能的传输装置 106。本领域普通技术人员可以理解，图 1 所示的结构仅为示意，其并不对上述电子装置的结构造成限定。例如，移动终端 10 还可包括比图 1 中所示更多或者更少的组件，或者具有与图 1 所示不同的配置。

存储器 104 可设置为：存储应用软件的软件程序以及模块，如本公开实施例中的验证处理方法对应的程序指令/模块，处理器 102 可设置为：通过运行存储在存储器 104 内的软件程序以及模块，从而执行各种功能应用以及数

据处理，即实现上述的方法。存储器 104 可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器 104 还可包括相对于处理器 102 远程设置的存储器，这些远程存储器可以通过网络连接至移动终端 10。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

传输装置 106 可设置为：经由一个网络接收或者发送数据。上述的网络实例可包括移动终端 10 的通信供应商提供的无线网络。在一个实例中，传输装置 106 包括一个网络适配器（Network Interface Controller，NIC），其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中，传输装置 106 可以为射频（Radio Frequency，RF）模块，其设置为：通过无线方式与互联网进行通讯。

在本实施例中提供了一种运行于上述移动终端的验证处理方法，图 2 是根据本公开实施例的验证处理方法的流程图，如图 2 所示，该流程包括如下步骤：

步骤 S202，获取用于请求对应用发起的操作流程进行验证的验证信息；

步骤 S204，根据请求信息获取操作流程对应的安全等级；

步骤 S206，根据安全等级对操作流程进行验证处理。

通过上述步骤，由于根据操作的安全等级对应用发起的操作进行验证处理，使得应用的不同操作可以采用相应等级的安全验证方式。因此，可以避免如果仅在应用程序启动时进行安全验证，则无法对该应用的某一个界面或者操作进行安全验证，以及避免如果验证的方式都是单一的安全验证方式，则没有一种安全分级策略；提高了对应用安全验证的精确度。可以支持对于更细粒度的操作的安全验证，可以更精确地保护敏感操作。

可选地，上述操作包括但不限于界面的显示、隐藏，按键或视图的点击、滑动等一切系统中可控的处理。

可选地，获取用于请求对应用发起的操作流程进行验证的请求信息包括：获取用于请求对应用发起的操作流程进行验证的第一请求信息，其中，第一请求信息携带有操作流程当前环境下对应的安全等级。例如，接收应用程序

主动请求安全验证控制模块提供的安全验证接口，并向该安全验证接口传入所需的安全等级参数。

可选地，获取用于请求对应用发起的操作流程进行验证的请求信息包括：获取用于请求对应用发起的操作流程进行验证的第二请求信息，其中，第二请求信息携带有应用发起的操作流程的标识信息。例如，由于当前用户的操作流程满足了安全策略库设置的安全策略而请求对操作流程进行验证的情况。

可选地，在获取用于请求对应用发起的操作流程进行验证的第二请求信息的情况下，根据第二请求信息获取操作流程对应的安全等级包括：根据第二请求信息携带的标识信息获取应用发起的操作流程；判断当前环境下是否存在与操作流程对应的安全等级；在判断结果为是的情况下，获取操作流程对应的安全等级。

可选地，根据安全等级对操作流程进行验证处理包括：根据安全等级确定与安全等级对应的安全验证序列；通过确定的安全验证序列验证输入的密令的合法性；在验证合法的情况下，确定操作流程合法。例如，可以根据操作流程的安全敏感程度的不同，提供不同的安全等级，不同安全等级对应不同的安全验证序列，而该安全验证序列可以包括对于数字密码、字符密码、指纹、声纹等多种密令的串行验证流程，可通过判断输入的密令是否与安全验证序列相一致，确定操作是否合法。通过上述步骤，使得密令验证方式不再单一，可以根据安全敏感程度的不同，使用包括数字密码、字符密码、指纹、声纹等多于一种的验证方式来确保安全，避免应用程序的保护方式比较单一，基本上都只是提供数字密码、字符密码、手势密码等的某一种密码验证方式。

可选地，在获取用于请求对应用发起的操作流程进行验证的请求信息之前，还包括：选择需要进行验证的操作流程；配置并保存操作流程的安全等级。通过上述步骤，使得可以根据用户需要选择需要进行验证的操作，确定并保存该操作的安全等级，提高了用户的体验度。

可选地，配置并保存操作流程的安全等级包括：本地配置并保存操作流程的安全等级；或者，通过网络侧配置并保存操作流程的安全等级。

应用程序安全验证界面可以由每个应用分别设计和实现，特别是对于生物识别验证的界面，由于涉及到操作系统权限的限制，第三方应用程序基本上不可能自行实现声纹、眼纹等生物识别安全验证。本公开实施例的系统框架层级提供一个统一的安全验证接口对于移动终端来说很有必要，可以让所有应用有统一的验证方式，能够为不同应用程序提供统一的、方便调用的安全验证接口。

图 3 是根据本公开实施例的操作流程安全分级保护框架示意图，为了方便理解上述实施例，以如图 3 所示的操作流程安全分级保护框架进行详细说明，如图 3 所示，显示了操作流程安全分级保护框架（以下简称安全分级框架）的结构，以及与该安全分级框架所运行系统的其他相关模块的交互关系，其中其他相关模块可包括（1）系统中所有应用程序组成的应用层；（2）对应用发起的各种操作流程进行处理的操作流程处理模块，可包括但不限于界面管理器、事件分发管理器等对系统中不同类型的操作流程进行处理的子模块。

如图 3 所示，操作流程安全分级保护框架可包括安全验证控制模块、安全策略模块、操作流程安全等级设置模块、密令验证模块四个模块。

（1）操作流程安全等级设置模块设置为：提供给用户设置操作流程等级的选项，并接收用户对于设置选项值的设定操作。

（2）安全策略模块设置为：保存系统预置的和用户设置的安全策略。

（3）密令验证模块设置为：接收安全验证控制模块发送的请求，并根据请求类型显示对应类型的密令验证界面，并返回用户输入的密令验证结果。

（4）安全验证控制模块设置为：接收当前该安全分级框架运行的系统的操作流程验证请求，并根据从安全策略模块读取到的安全等级，进行相应安全等级的密令验证流程。其中操作流程验证请求可包括主动请求和被动请求，主动请求可以是指应用程序主动调用安全验证控制模块提供的安全验证接口，并向该安全验证接口传入所需的安全等级参数；被动请求可以是指当前该安全分级框架运行的系统由于当前用户的操作流程满足了安全策略库设置的安全策略而向应用程序请求对该操作流程进行验证的情况。

图 4 是根据本公开实施例的操作流程安全分级保护方法流程图，该流程

可包括以下步骤:

步骤 S401: 应用发起操作流程; 应用主动请求安全验证, 直接执行步骤 S404;

步骤 S402: 操作流程处理模块请求安全验证控制模块验证操作合法性;

步骤 S403: 安全验证控制模块请求查询该操作在安全策略模块中定义的安全等级;

步骤 S404: 安全验证控制模块根据安全等级, 发送串行的安全验证序列给密令验证模块;

步骤 S405: 安全验证控制模块返回安全验证序列验证成功与否的结果给应用或者操作流程控制模块;

步骤 S406: 应用或者操作流程控制模块根据安全验证序列验证成功与否的结果来继续或终止操作流程。

为了更清楚地阐述如图 3 所示的操作流程安全分级保护框架中的安全验证控制模块、安全策略模块、操作流程安全等级设置模块、密令验证模块四个模块, 下面分别对这四个模块进行详细的说明。

安全验证控制模块

安全验证控制模块大致可设置为: 接收应用直接下发的主动安全验证请求, 或者操作流程处理模块的验证操作合法性的请求。图 5 是根据本公开实施例的安全验证控制模块的请求流程示意图, 如图 5 所示。请求流程可包括:

在应用主动下发安全验证请求的情况下, 请求流程可包括: 应用调用本模块的对外的安全验证应用程序编程接口 (Application Programming Interface, 简称为 API), 并向该安全验证 API 传入所需的安全等级, 安全验证控制模块根据请求传入的安全等级,执行安全等级对应的安全验证序列, 然后将验证序列验证成功与否的结果返回给应用。

在操作流程处理模块下发验证操作合法性的请求的情况下, 请求流程可包括: 操作流程处理模块调用安全验证控制模块的操作流程合法性验证 API, 安全验证控制模块发送请求给安全策略模块, 查询操作流程的安全等级, 如果安全策略模块存储了当前操作流程的安全等级记录, 返回该操作流程对应

的安全等级，然后执行安全等级对应的安全验证序列，然后将验证序列验证成功与否的结果返回给操作流程处理模块；否则说明当前操作流程没有设置任何安全验证策略，直接返回验证结果成功给操作流程处理模块。

图 6 是根据本公开实施例的安全验证序列的执行流程示意图，如图 6 所示，上述请求流程中安全等级可以根据实际情况划分为任意多的等级，每个等级所对应的安全验证序列包含的密令组合也是可以自由选择的。安全验证序列的验证流程可以是串行执行的，即密令 1 验证成功后进入密令 2 验证流程，密令 2 验证成功后进入密令 3 验证流程，以此类推，直至该安全验证序列中所有的密令被验证完成为止，返回结果为成功；否则只要其中任何的一个密令验证失败，返回结果为失败。

本实施例中提供了三个等级的安全验证的例子，每个安全验证等级都有一个相对应的安全验证序列。安全验证等级 1 对应的安全验证序列只包含字符密令；安全验证等级 2 对应的安全验证序列包含字符密令和指纹密令；安全验证等级 3 对应的安全验证序列包含字符密令、指纹密令、眼纹密令。

密令验证模块

密令验证模块的流程步骤可包括:

（1）接收安全验证控制模块发送的请求;

（2）根据请求类型显示对应类型的密令验证界面;

（3）返回用户输入的密令验证结果。

其中各种类型的密令（包括字符密码、指纹、眼纹等）都是存储在本地安全可信分区中的，此区域可保证在其内部存储、处理的数据是独立于外部环境的，并且此区域可以是一个授信环境，这样就确保了密令存储的安全性。

操作流程等级设置模块

操作流程等级设置模块的流程步骤可包括:

（1）用户选择想要设置安全验证的操作流程;

（2）用户设置该操作流程的安全等级;

（3）将设置结果保存至安全策略模块。

安全策略模块

图 7 是根据本公开实施例的安全策略模块确立操作流程安全等级的流程示意图，如图 7 所示，该流程步骤可包括:

（1）判断当前请求的操作流程是否加入了安全策略模块中，如果安全策略模块没有当前请求的操作流程的安全策略记录，就直接返回无安全等级标识。

（2）判断当前请求的操作流程，用户是否通过操作流程等级设置模块主动设置了安全等级，如果设置了，就返回用户设置的安全等级。

（3）对于用户没有主动设置安全等级的预置操作流程。通过安全策略模块智能学习算法来动态地确定操作流程的安全等级，并返回计算出的安全等级。

本实施例所述预置操作流程，可以是根据大数据用户统计分析，得出较常用的需要安全验证保护的操作流程。并且可以通过连接至云端安全策略服务器，实时更新本地终端系统中的预置操作流程，从而保证本地安全策略的时效性。

本实施例所述智能学习算法，简单的说，就是通过以下三种影响因子的加权平均计算得出操作流程的安全等级：操作流程状态因子（包括连续几次该操作流程验证未验证通过，付款流程中付款额度等），时间因子（包括上次使用时间等），操作环境因子（包括是否常用的网络环境，是否常用的客户识别模块（Subscriber Identification Module，简称为 SIM）卡等）。计算公式为: $f(N)=\sum_{i=1}^{N}(P_i \times \alpha_i)/N$，其中$P_i$为第 i 个影响因子的权重，满足 $0<P_i<1$，$\sum_{i=1}^{N} P_i =1$；α_i为第 i 个影响因子值，满足$0 \le \alpha_i \le 1$ ，其中 i 的取值集合例如为{1,2,3}，N 为影响因子的个数，例如为 3。此处举例说明一下影响因子是如何起作用的，（1）比如，当前用户处于支付界面，点击界面上的“付款”按钮，此时通过动态检测输入框中的付款金额，就会动态计算出操作流程状态因子的比重，当为小额付款时，会执行安全等级 2 的验证流程，当为大额付款时，会执行安全等级 3 的验证流程。（2）再比如，安全短信发送操作，在正常使用的情况下，会在用户点击发送按钮的时候执行安全等级 1 的验证流程，但是当检测到用户当前使用的 SIM 卡属于新的 SIM 卡时，会提高操

作环境因子的比重，执行安全等级 2 的验证流程。

本公开实施例提供了一种对于操作流程安全提供分级保护的方法，本地可预先配置安全分级策略或者通过连接至云端安全策略服务器，实时更新本地终端系统中的预置操作流程，可根据智能检测、用户设置等来动态决策当前操作的安全等级，从而采取相应等级的安全验证方式。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，本公开实施例的技术方案本质上或者说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（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端设备（可以是手机，计算机，服务器，或者网络设备等）执行本公开实施例所述的方法。

本公开实施例还提供了一种验证处理装置，该装置设置为实现上述实施例及可选实施方式，已经进行过说明的不再赘述。如以下所使用的，术语“模块”可以实现预定功能的软件的组合、或者硬件的组合、或者软件和硬件的组合。尽管以下实施例所描述的装置可以以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

图 8 是根据本公开实施例的验证处理装置的结构框图，如图 8 所示，该装置包括：

接收模块 82，设置为：获取用于请求对应用发起的操作流程进行验证的请求信息；

获取模块 84，连接至上述接收模块 82，设置为：根据请求信息获取操作流程对应的安全等级；

处理模块 86，连接至上述获取模块 84，设置为：根据安全等级对操作流程进行验证处理。

可选地，接收模块 82，还设置为：获取用于请求对应用发起的操作流程进行验证的第一请求信息，其中，第一请求信息携带有操作流程当前环境下对应的安全等级；或者，获取用于请求对应用发起的操作流程进行验证的第

二请求信息，其中，第二请求信息携带有应用发起的操作流程的标识信息。

可选地，获取模块 84，还设置为：根据第二请求信息携带的标识信息获取应用发起的操作流程；判断当前环境下是否存在与操作流程对应的安全等级；在判断结果为是的情况下，获取操作流程对应的安全等级。

可选地，处理模块 86，还设置为：根据安全等级确定与安全等级对应的安全验证序列；通过确定的安全验证序列验证输入的密令的合法性；在验证合法的情况下，确定操作流程合法。

图 9 是根据本公开实施例的可选验证处理装置的结构框图，如图 9 所示，该装置除包括图 8 所示的所有模块外，还可包括：

选择模块 92，设置为：选择需要进行验证的操作流程；

确定模块 94，连接至上述选择模块 92，设置为：配置并保存操作流程的安全等级。

可选地，确定模块 94，还设置为：本地配置并保存操作流程的安全等级；或者，通过网络侧配置并保存操作流程的安全等级。

需要说明的是，上述模块是可以通过软件或硬件来实现的，对于后者，可以通过以下方式实现，但不限于此：上述模块均位于同一处理器中；或者，上述模块以任意组合的形式分别位于不同的处理器中。

本公开的实施例还提供了一种存储介质。可选地，在本实施例中，上述存储介质可以被设置为存储用于执行以下步骤的程序代码：

S1，获取用于请求对应用发起的操作流程进行验证的请求信息；

S2，根据请求信息获取操作流程对应的安全等级；

S3，根据安全等级对操作流程进行验证处理。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：获取用于请求对应用发起的操作流程进行验证的请求信息包括：

S1，获取用于请求对应用发起的操作流程进行验证的第一请求信息，其中，第一请求信息携带有操作流程当前环境下对应的安全等级；或者

S2，获取用于请求对应用发起的操作流程进行验证的第二请求信息，其

中，第二请求信息携带有应用发起的操作流程的标识信息。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：在获取用于请求对应用发起的操作流程进行验证的第二请求信息的情况下，根据第二请求信息获取操作流程对应的安全等级包括：

S1，根据第二请求信息携带的标识信息获取应用发起的操作流程；

S2，判断当前环境下是否存在与操作流程对应的安全等级；

S3，在判断结果为是的情况下，获取操作流程对应的安全等级。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：根据安全等级对操作流程进行验证处理包括：

S1，根据安全等级确定与安全等级对应的安全验证序列；

S2，通过确定的安全验证序列验证输入的密令的合法性；

S3，在验证合法的情况下，确定操作流程合法。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：在获取用于请求对应用发起的操作流程进行验证的请求信息之前，还包括：

S1，选择需要进行验证的操作流程；

S2，配置并保存操作流程的安全等级。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：配置并保存操作流程的安全等级包括：

S1，本地配置并保存操作流程的安全等级；或者，

S2，通过网络侧配置并保存操作流程的安全等级。

可选地，上述存储介质可以包括但不限于：U 盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

可选地，处理器根据存储介质中已存储的程序代码执行：获取请求对应用发起的操作流程进行验证的请求信息；根据请求信息获取操作流程对应的安全等级；根据安全等级对操作流程进行验证处理。

可选地，处理器根据存储介质中已存储的程序代码执行：获取用于请求

对应用发起的操作流程进行验证的请求信息包括：获取用于请求对应用发起的操作流程进行验证的第一请求信息，其中，第一请求信息携带有操作流程当前环境下对应的安全等级；或者，获取用于请求对应用发起的操作流程进行验证的第二请求信息，其中，第二请求信息携带有应用发起的操作流程的标识信息。

可选地，处理器根据存储介质中已存储的程序代码执行：在获取用于请求对应用发起的操作流程进行验证的第二请求信息的情况下，根据第二请求信息获取操作流程对应的安全等级包括：根据第二请求信息携带的标识信息获取应用发起的操作流程；判断当前环境下是否存在与操作流程对应的安全等级；在判断结果为是的情况下，获取操作流程对应的安全等级。

可选地，处理器根据存储介质中已存储的程序代码执行：根据安全等级对操作流程进行验证处理包括：根据安全等级确定与安全等级对应的安全验证序列；通过确定的安全验证序列验证输入的密令的合法性；在验证合法的情况下，确定操作流程合法。

可选地，处理器根据存储介质中已存储的程序代码执行：在获取请求对应用发起的操作流程进行验证的请求信息之前，还包括：选择需要进行验证的操作流程；配置并保存操作流程的安全等级。

可选地，处理器根据存储介质中已存储的程序代码执行：配置并保存操作流程的安全等级包括：本地配置并保存操作流程的安全等级；或者，通过网络侧配置并保存操作流程的安全等级。

可选地，处理器根据存储介质中已存储的程序代码执行步骤流程的示例可以参考上述方法及装置实施例及可选实施方式中所描述的示例，在此不再赘述。

本公开实施例还提供了一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令被执行时实现上述验证处理方法。

本领域的技术人员可以明白，上述的本公开实施例的模块或步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算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，并且在

某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成不同集成电路模块，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，本公开实施例不限制于任何特定的硬件和软件结合。

本领域普通技术人员可以理解上述实施例的全部或部分步骤可以使用计算机程序流程来实现，所述计算机程序可以存储于一计算机可读存储介质中，所述计算机程序在相应的硬件平台上（如系统、设备、装置、器件、处理器等）执行，在执行时，包括方法实施例的步骤之一或其组合。

可选地，上述实施例的全部或部分步骤也可以使用集成电路来实现，这些步骤可以被分别制作成一个个集成电路模块，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。

上述实施例中的装置/功能模块/功能单元可以采用通用的计算装置来实现，它们可以集中在单个的计算装置上，也可以分布在多个计算装置所组成的网络上。

上述实施例中的装置/功能模块/功能单元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，可以存储在一个计算机可读取存储介质中。上述提到的计算机可读取存储介质可以是只读存储器，磁盘或光盘等。

本领域的普通技术人员可以理解，可以对本申请的技术方案进行修改或者等同替换，而不脱离本申请技术方案的精神和范围。本申请的保护范围以权利要求所定义的范围为准。

工业实用性

通过本公开实施例，获取用于请求对应用发起的操作流程进行验证的请求信息；根据所述请求信息获取所述操作流程对应的安全等级；根据所述安全等级对所述操作流程进行验证处理。由于根据操作的安全等级对应用发起的操作进行验证处理，使得应用的不同操作可以采用相应等级的安全验证方式。因此，可以避免如果仅在应用程序启动时进行安全验证，则无法对该应用的某一个界面或者操作进行安全验证，以及避免如果验证的方式都是单一的安全验证方式，则没有一种安全分级策略；提高了对应用安全验证的精确度。

权 利 要 求 书

1、一种验证处理方法，包括:

获取用于请求对应用发起的操作流程进行验证的请求信息;

根据所述请求信息获取所述操作流程对应的安全等级;

根据所述安全等级对所述操作流程进行验证处理。

2、根据权利要求 1 所述的方法，获取用于请求对所述应用发起的操作流程进行验证的所述请求信息包括:

获取用于请求对所述应用发起的操作流程进行验证的第一请求信息，其中，所述第一请求信息携带有所述操作流程当前环境下对应的安全等级;

或者，

获取用于请求对所述应用发起的操作流程进行验证的第二请求信息，其中，所述第二请求信息携带有所述应用发起的所述操作流程的标识信息。

3、根据权利要求 2 所述的方法，在获取用于请求对所述应用发起的操作流程进行验证的第二请求信息的情况下，根据所述第二请求信息获取所述操作流程对应的安全等级包括:

根据所述第二请求信息携带的所述标识信息获取所述应用发起的操作流程;

判断当前环境下是否存在与所述操作流程对应的安全等级;

在判断结果为是的情况下，获取所述操作流程对应的安全等级。

4、根据权利要求 1 所述的方法，根据所述安全等级对所述操作流程进行验证处理包括:

根据所述安全等级确定与所述安全等级对应的安全验证序列;

通过确定的安全验证序列验证输入的密令的合法性;

在验证合法的情况下，确定所述操作流程合法。

5、根据权利要求 1 至 4 中任一项所述的方法，在获取用于请求对所述应用发起的操作流程进行验证的所述请求信息之前，还包括:

选择需要进行验证的所述操作流程;

配置并保存所述操作流程的安全等级。

6、根据权利要求 5 所述的方法，配置并保存所述操作流程的安全等级包括:

本地配置并保存所述操作流程的安全等级；或者，

通过网络侧配置并保存所述操作流程的安全等级。

7、一种验证处理装置，包括:

接收模块，设置为：获取用于请求对应用发起的操作流程进行验证的请求信息;

获取模块，设置为：根据所述请求信息获取所述操作流程对应的安全等级;

处理模块，设置为：根据所述安全等级对所述操作流程进行验证处理。

8、根据权利要求 7 所述的装置，所述接收模块，还设置为：获取用于请求对所述应用发起的操作流程进行验证的第一请求信息，其中，所述第一请求信息携带有所述操作流程当前环境下对应的安全等级；或者，获取用于请求对所述应用发起的操作流程进行验证的第二请求信息，其中，所述第二请求信息携带有所述应用发起的所述操作流程的标识信息。

9、根据权利要求 8 所述的装置，所述获取模块，还设置为：根据所述第二请求信息携带的所述标识信息获取所述应用发起的操作流程；判断当前环境下是否存在与所述操作流程对应的安全等级;在判断结果为是的情况下，获取所述操作流程对应的安全等级。

10、根据权利要求 7 所述的装置，所述处理模块，还设置为：根据所述安全等级确定与所述安全等级对应的安全验证序列；通过确定的安全验证序列验证输入的密令的合法性；在验证合法的情况下，确定所述操作流程合法。

11、根据权利要求 7 至 10 中任一项所述的装置，还包括:

选择模块，设置为：选择需要进行验证的所述操作流程;

确定模块，设置为：配置并保存所述操作流程的安全等级。

12、根据权利要求 11 所述的装置，所述确定模块，还设置为：本地配置并保存所述操作流程的安全等级；或者，通过网络侧配置并保存所述操作流程的安全等级。

13、一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令被执行时实现如权利要求 1 至 6 中任一权利要求所述的验证处理方法。

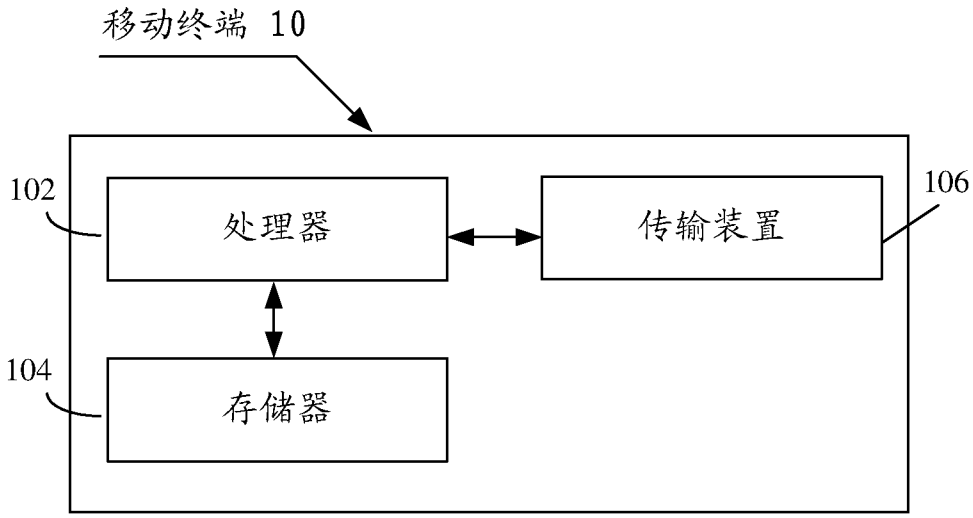

图 1

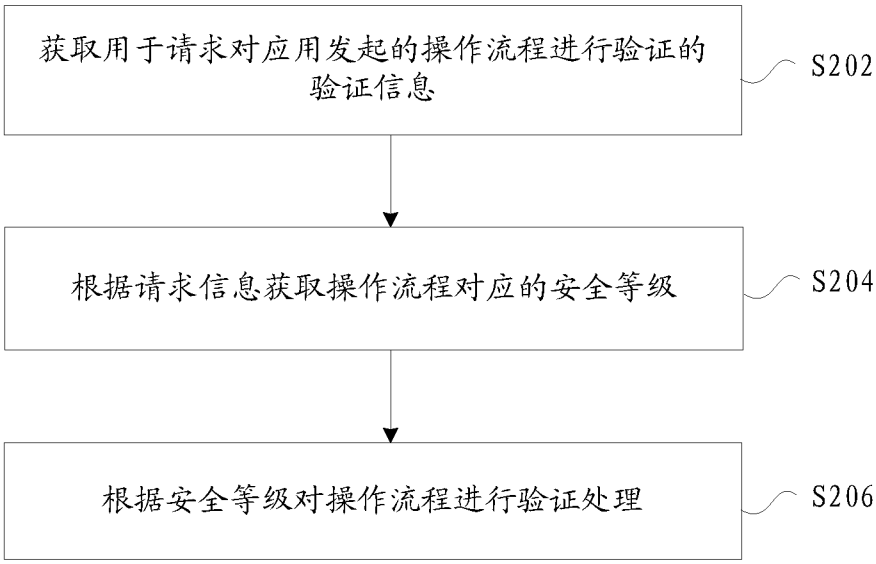
获取用于请求对应用发起的操作流程进行验证的验证信息
S202
根据请求信息获取操作流程对应的安全等级
S204
根据安全等级对操作流程进行验证处理
S206

图 2

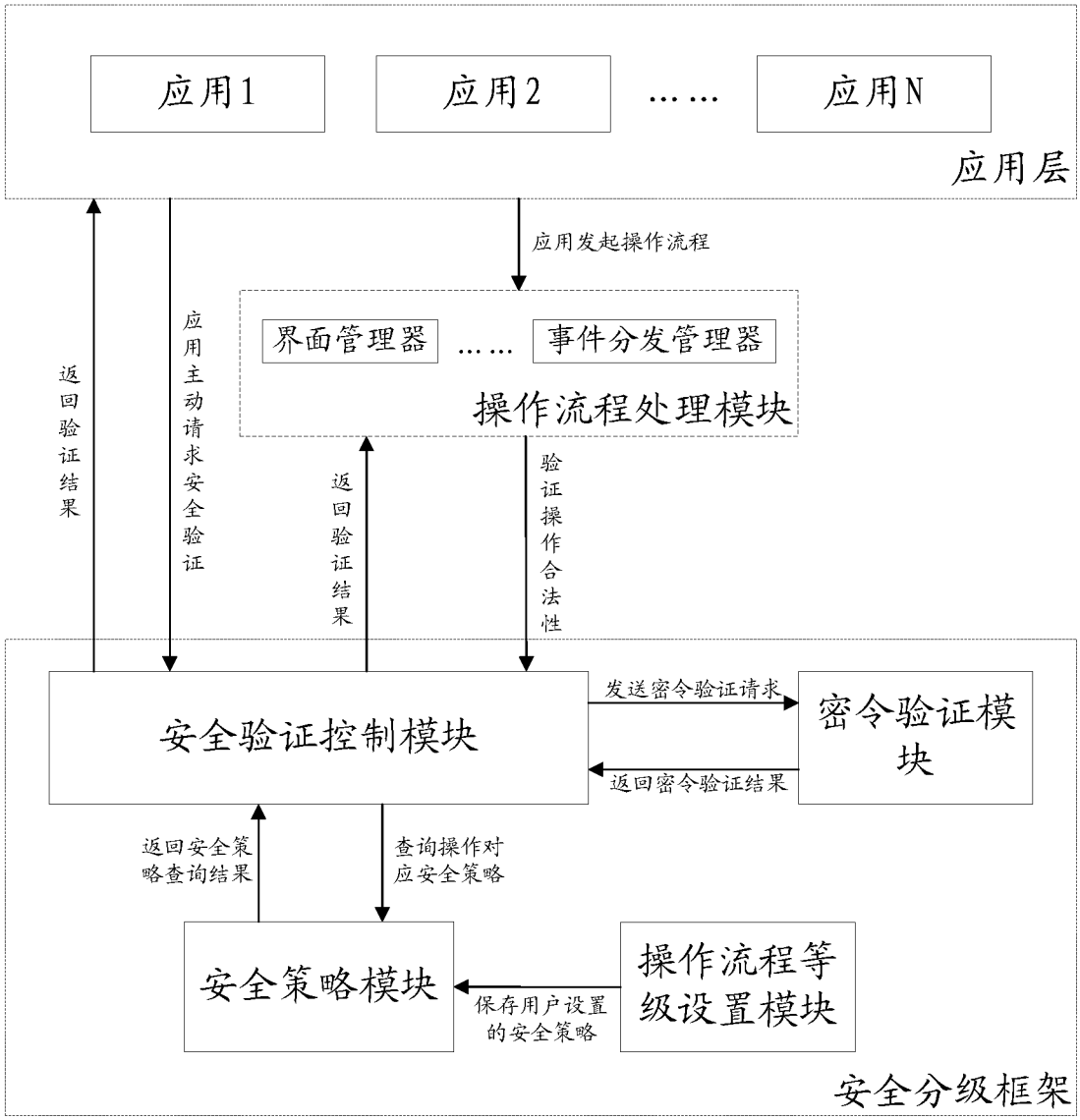
应用1
应用2
……
应用N
应用层
应用发起操作流程
界面管理器
……
事件分发管理器
操作流程处理模块
返回验证结果
应用主动请求安全验证
返回验证结果
验证操作合法性
安全验证控制模块
发送密令验证请求
返回密令验证结果
密令验证模块
返回安全策略查询结果
查询操作对应安全策略
安全策略模块
保存用户设置的安全策略
操作流程等级设置模块
安全分级框架

图 3

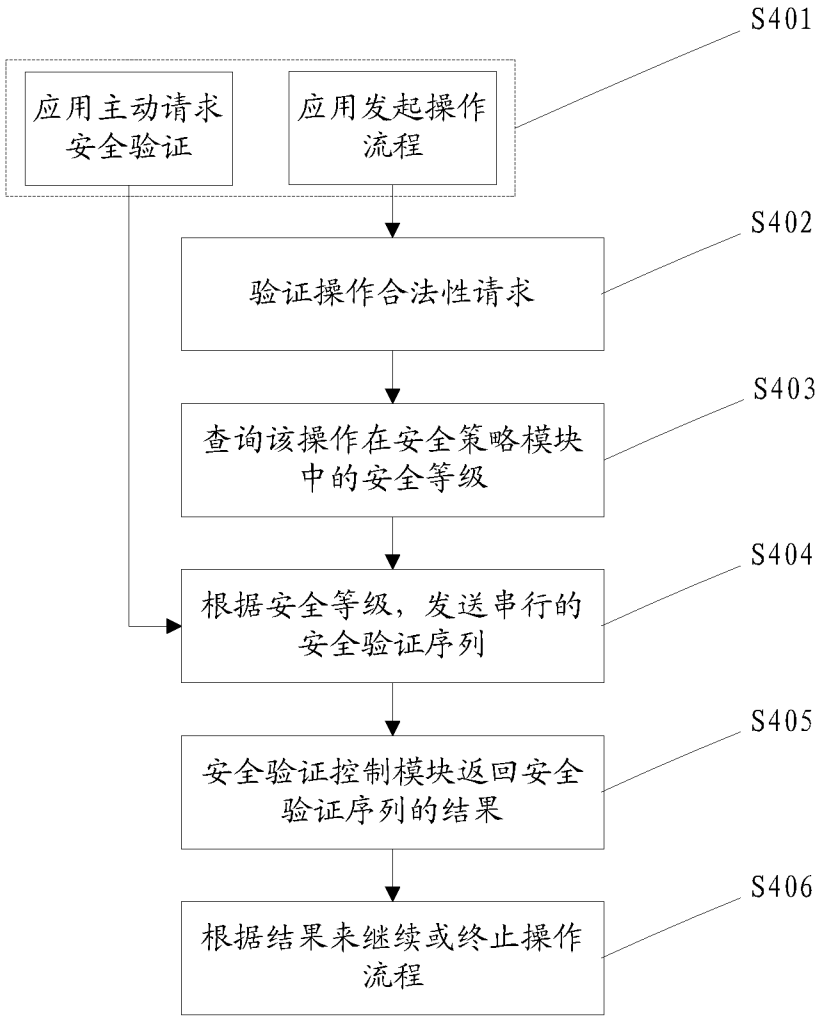
S401
应用主动请求安全验证
应用发起操作流程
S402
验证操作合法性请求
S403
查询该操作在安全策略模块中的安全等级
S404
根据安全等级，发送串行的安全验证序列
S405
安全验证控制模块返回安全验证序列的结果
S406
根据结果来继续或终止操作流程

图 4

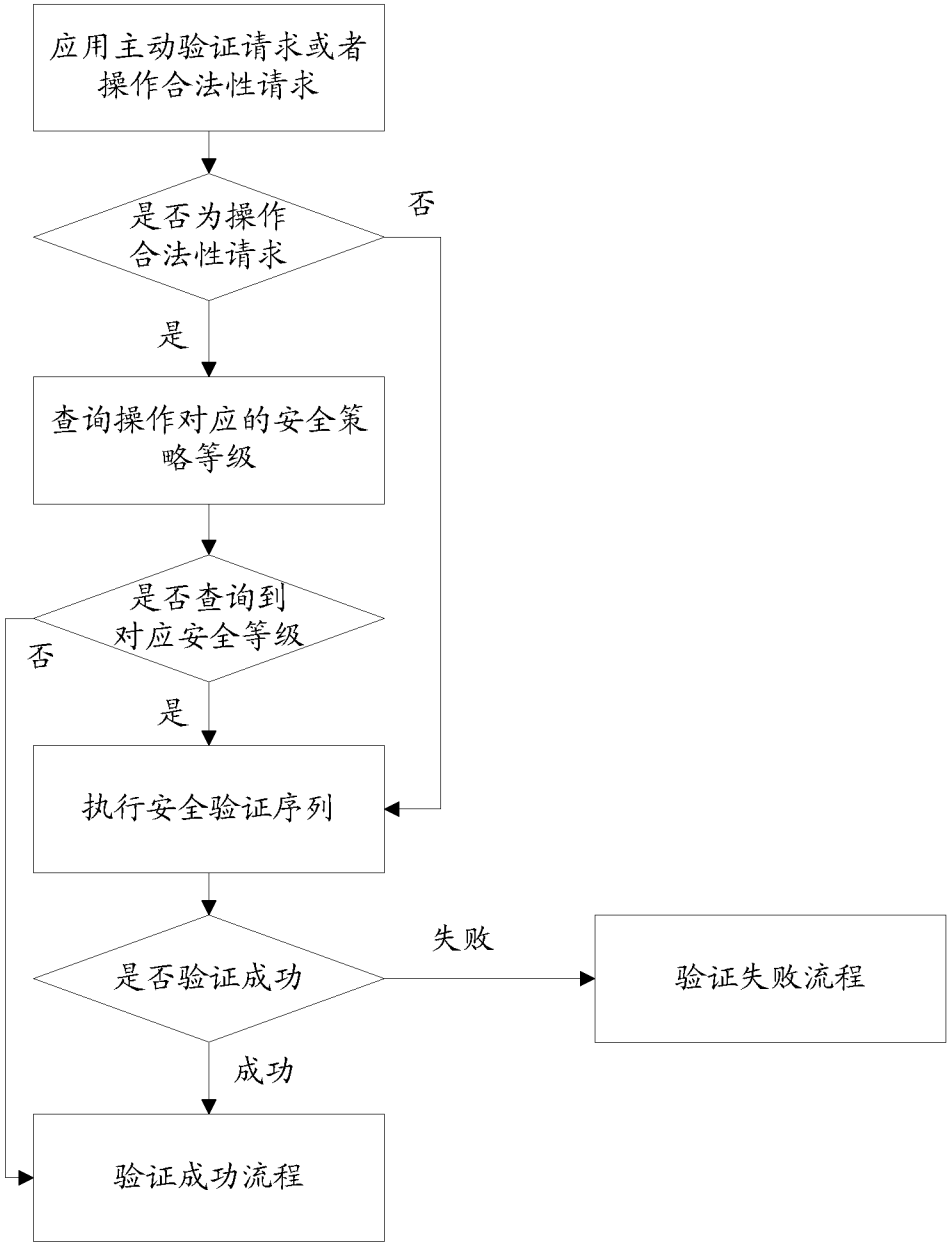
应用主动验证请求或者操作合法性请求
是否为操作合法性请求
否
是
查询操作对应的安全策略等级
是否查询到对应安全等级
否
是
执行安全验证序列
是否验证成功
失败
验证失败流程
成功
验证成功流程

图 5

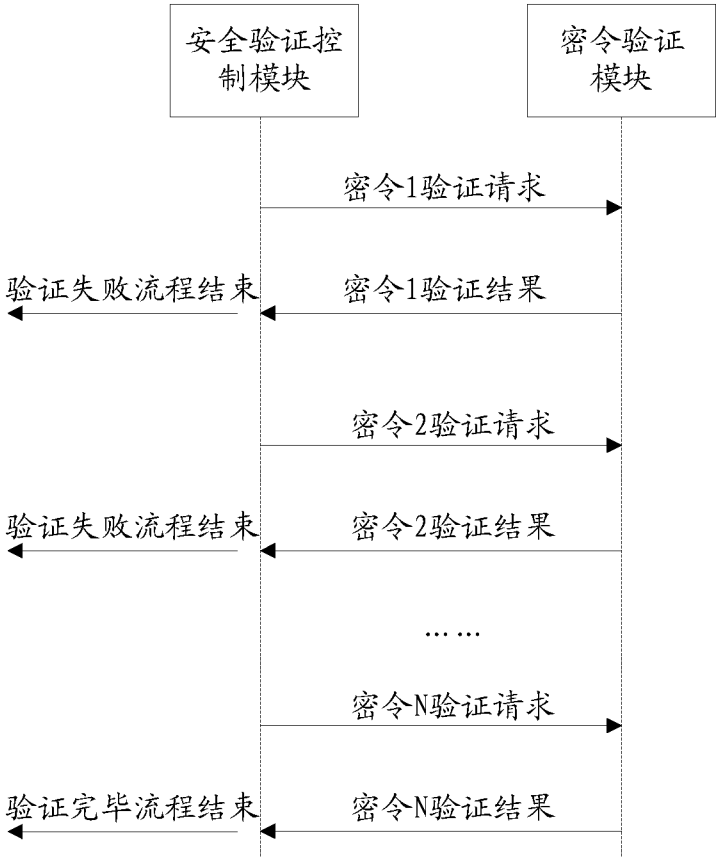
安全验证控制模块
密令验证模块
密令1验证请求
验证失败流程结束
密令1验证结果
密令2验证请求
验证失败流程结束
密令2验证结果
……
密令N验证请求
验证完毕流程结束
密令N验证结果

图 6

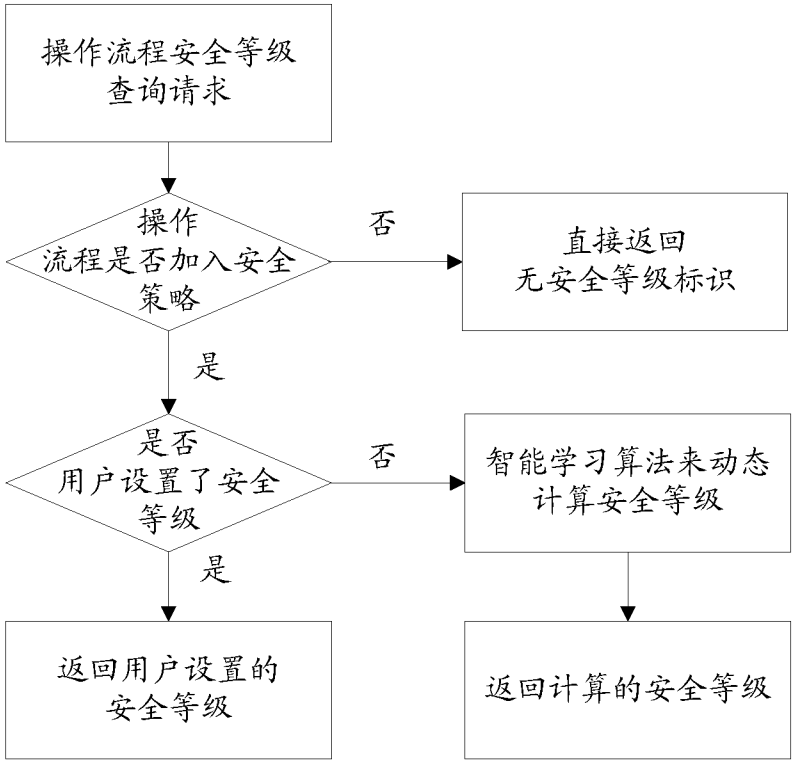
操作流程安全等级查询请求
操作流程是否加入安全策略
否
直接返回无安全等级标识
是
是否用户设置了安全等级
否
智能学习算法来动态计算安全等级
是
返回用户设置的安全等级
返回计算的安全等级

图 7

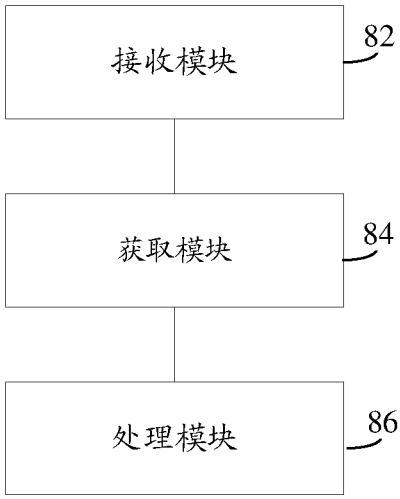
接收模块
82
获取模块
84
处理模块
86

图 8

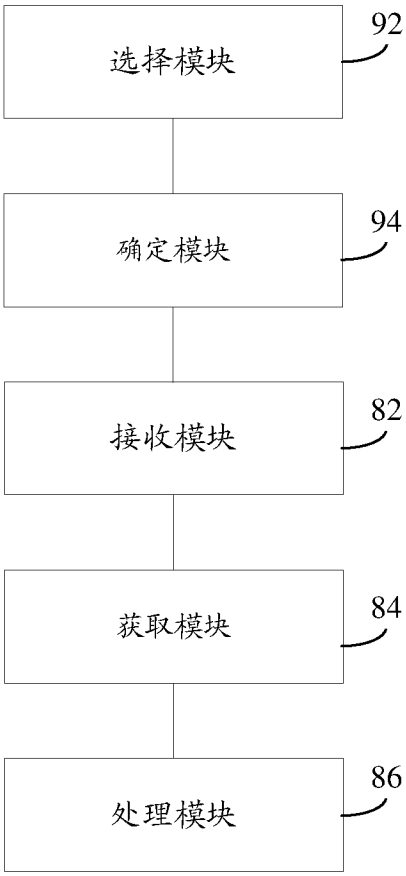

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/098408

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/52 (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 21/-

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)

MOABS; CPRSABS; CNABS; DWPI; HKABS; TWABS: 应用, 验证, 安全等级, application, verify+, safety level

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102255913 A (BEIJING BAIDU NETCOM SCIENCE AND TECHNOLOGY CO., LTD.) 23 November 2011 (23.11.2011), claims 1-6	1-13
Y	CN 105094996 A (UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA) 25 November 2015 (25.11.2015), claims 1-3	1-13
A	CN 105959317 A (SHENZHEN GIONEE COMMUNICATION EQUIPMENT CO., LTD.) 21 September 2016 (21.09.2016), entire document	1-13
A	CN 102957682 A (BEIJING BAIDU NETCOM SCIENCE AND TECHNOLOGY CO., LTD.) 06 March 2013 (06.03.2013), entire document	1-13

☐ 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
28 September 2017	11 October 2017

Name and mailing address of the ISA
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
HAN, Xianping
Telephone No. (86-10) 62411841

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/098408

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102255913 A	23 November 2011	None	
CN 105094996 A	25 November 2015	None	
CN 105959317 A	21 September 2016	None	
CN 102957682 A	06 March 2013	WO 2013029319 A1	07 March 2013

国际检索报告

国际申请号 PCT/CN2017/098408

A. 主题的分类

G06F 21/52(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)

G06F21/-

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）)

MOABS;CPRSABS;CNABS;DWPI;HKABS;TWABS:应用，验证，安全等级，application，verify+，safety level

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
Y	CN 102255913 A (北京百度网讯科技有限公司) 2011年 11月 23日 (2011-11-23) 权利要求1-6	1-13
Y	CN 105094996 A (电子科技大学) 2015年 11月 25日 (2015-11-25) 权利要求1-3	1-13
A	CN 105959317 A (深圳市金立通信设备有限公司) 2016年 9月 21日 (2016-09-21) 全文	1-13
A	CN 102957682 A (北京百度网讯科技有限公司) 2013年 3月 6日 (2013-03-06) 全文	1-13

☐ 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 9月 28日	2017年 10月 11日

ISA/CN的名称和邮寄地址	受权官员
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	韩鲜萍
传真号 (86-10)62019451	电话号码 (86-10)62411841

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/CN2017/098408

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 102255913 A	2011年 11月 23日	无	
CN 105094996 A	2015年 11月 25日	无	
CN 105959317 A	2016年 9月 21日	无	
CN 102957682 A	2013年 3月 6日	WO 2013029319 A1	2013年 3月 7日