(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
2014 年 5 月 22 日 (22.05.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/075504 A1

(51) 国转 利分类号：
G06F 21/51 (2013.01) G06F 21/52 (2013.01)

(21) 国际申请号： PCT/CN2013/083621

(22) 国际申请日： 2013 年 9 月 17 日 (17.09.2013)

(25) 申飾 言： 中文

(26) 公布语言： 中文

(30) 优先权：
2012 10457164.8 2012 年 11 月 14 日 (14. 11.2012) CN

(71) 申请人 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。奇智软件 (北京) 有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED) [CN/CN] ;中国北京市朝阳区酒仙桥路 14 号兆维大厦 4 层东侧单元 ,Beijing 100016 (CN)。

(72) 发明人 温铭 (WEN, Ming); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 ,Beijing 100015 (CN) 。李宇 (LI, Yu); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。胡劲 (HU, Jin); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 ,Beijing 100015 (CN)。张家柱 (ZHANG, Jiazhu); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 Beijing 100015 (CN)。

(74) 代理人：北京智汇东方知识产权代理事务所 (普通合伙) (WISEAST INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区成府路 28 号优盛大厦 D-I 111 室 Beijing 100083 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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)。

本国际公布：
- 包括国际检索报告(条约第 21 条(3))。

(54) Title: SECURITY CONTROL METHOD AND DEVICE FOR RUNNING APPLICATION

(54) 发明名称：一种运行应用程序的安全控制方法和装置

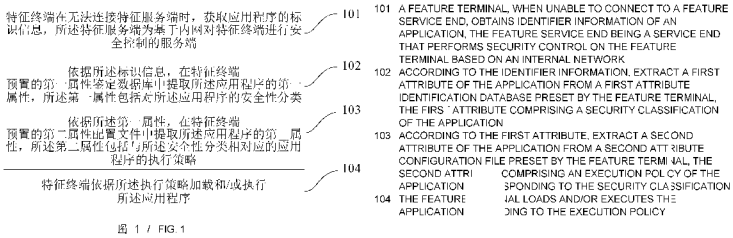

图 1 / FIG. 1

(57) Abstract: Disclosed are a security control method and device for running an application. The method comprises: a feature terminal, when unable to connect to a feature service end, obtaining identifier information of an application, the feature service end being a service end that performs security control on the feature terminal based on an internal network; according to the identifier information, extracting a first attribute of the application fi"om a first attribute identification database preset by the feature terminal, the first attribute comprising a security classification of the application; according to the first attribute, extracting a second attribute of the application fi"om a second attribute configuration file preset by the feature terminal, the second attribute comprising an execution policy of the application corresponding to the security classification; the feature terminal loading and/or executing the application according to the execution policy. The present invention can prevent running of the application from being affected by incapability of a terminal in connecting a private cloud.

(57) 摘要：本发明公开了一种运行应用程序的安全控制方法和装置。所述方法包括：特征终端在无法连接特征服务端时，获取应用程序的标识信息，所述特征服务端为基于内网对特征终端进行安全控制的服务端；依据所述标识信息，在特征终端预置的第一属性鉴定数据库中提取所述应用程序的第一属性，所述第一属性包括对所述应用程序的安全性分类；依据所述第一属性，在特征终端预置的第二属性配置文件中提取所述应用程序的第二属性，所述第二属性包括与所述安全性分类相对应的应用程序的执行策略；特征终端依据所述述执行策略加载和/或执行所述应用程序。本发明可以避免终端无法连接私有云时影响应用程序的运行。

WO 2014/075504 A1

一种运行应用程序的安全控制方法和装置

技术领域

本发明涉及计算机技术领域，尤其涉及一种运行应用程序的安全控制方法和装置。

背景技术

云是互联网、网络的一种比喻说法，表示互联网和底层基础设施的抽象，大致可以分为公有云和私有云。

公有云通常指第三方供应商通过自己的基础设施，直接向外部用户提供服务能够使用的云。私有云是放在私有环境中的，比如企业、政府等组织自己在机房中建立的，或者是运营商建设好，但是整体租给某一组织的。组织之外的用户无法访问或无法使用。私有云是一个组织单独使用构建的，因而可以提供对数据、安全性和服务质量的最有效控制。

可访问私有云的终端和私有云服务器处于同一个局域网，可以使用交换机、路由器等网络设备连接，当终端需要对文件进行操作时需要从私有云获取相应策略，具体而言，在终端访问某个程序时，需要请求私有云鉴定该程序是否可执行，接收到私有云的鉴定结果后，才进一步运行该程序或是不运行该程序。

以上现有技术中存在的问题是，如果私有云所属的局域网内出现网络故障，或者病毒爆发，致使终端和私有云无法连接，那么终端就无法判断程序是否可执行，会导致终端的所有程序都无法运行，影响终端的正常使用。

因此，目前需要本领域技术人员解决的一个技术问题就是，提供一种运行应用程序的安全控制机制，避免终端无法连接私有云时影响应用程序的运行。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决或者减缓上述问题的运行应用程序的安全控制方法和相应的运行应用程序的安全控制装置。

根据本发明的一个方面，提供了一种运行应用程序的安全控制方法，包括：

特征终端在无法连接特征服务端时，获取应用程序的标识信息，所述特征服务端为基于内网对特征终端进行安全控制的服务端；

依据所述标识信息，在特征终端预置的第一属性鉴定数据库中提取所述应用程序的第一属性，所述第一属性包括对所述应用程序的安全性分类；

依据所述第一属性，在特征终端预置的第二属性配置文件中提取所述应用程序的第二属性，所述第二属性包括与所述安全性分类相对应的应用程序的执行策略；

特征终端依据所述执行策略加载和/或执行所述应用程序。

根据本发明的另一个方面，提供了一种运行应用程序的安全控制装置，包括：

标识信息获取模块，适于特征终端在无法连接特征服务端时，获取应用程序的标识信息，所述特征服务端为基于内网对特定终端进行安全控制的服务端；

第一属性获取模块，适于依据所述标识信息，在特征终端预置的第一属性鉴定数据库中提取所述应用程序的第一属性，所述第一属性包括对所述应用程序的安全性分类；

第二属性获取模块，适于依据所述第一属性，在特征终端预置的第二属性配置文件中提取所述应用程序的第二属性，所述第二属性包括与所述安全性分类相对应的应用程序的执行策略；

加载模块，适于特征终端依据所述执行策略加载和/或执行所述应用程序。

根据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，当所述计算机可读代码在服务器上运行时，导致所述服务器执行根据权利要求 1-10 中的任一个所述的运行应用程序的安全控制方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了如权利要求 21 所述的计算机程序。

本发明的有益效果为：

依据本发明实施例，通过在终端预置第一属性鉴定数据库和第二属

性配置文件，终端在无法连接特征服务端时，可以直接在本地鉴定出应用程序的安全性分类对应的执行策略，进而可以依据执行策略来加载应用程序，从而使得终端无法连接私有云时，依然可以对应用程序进行鉴定，得出应用程序是否可以执行，不影响用户对应用程序的访问。

本发明实施例中，应用程序的安全性分类可以包括黑文件、白文件和灰文件等多种不同的属性，相应的，第二属性配置文件可以包括对多种不同的安全性分类分别对应的执行策略。用户可以按照自己不同的需求在私有云重新设置第二属性配置文件，然后对终端的第二属性配置文件进行更新。

本发明实施例在第一属性鉴定数据库不够完善，无法对应用程序的第一属性进行鉴定时，可以将该应用程序的安全性分类判定为灰文件，进而可以在第二属性配置文件中找到相应的执行策略，避免了第一属性鉴定数据库不够完善时，造成部分程序无法访问的问题。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述,各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示意性示出了根据本发明一个实施例的运行应用程序的安全控制方法的流程图；

图 2 示意性示出了根据本发明一个实施例的运行应用程序的安全控制装置的框图；

图 3 示意性地示出了用于执行根据本发明的方法的服务器的框图；以及

图 4 示意性地示出了用于保持或者携带实现根据本发明的方法的程序代码的存储单元。

具体实施例

下面结合附图和具体的实施方式对本发明作进一步的描述。

参考图 1,示出了本发明实施例的一种运行应用程序的安全控制方法实施例的步骤流程图，具体可以包括以下步骤：

步骤 101、特征终端在无法连接特征服务端时，获取应用程序的标识信息，所述特征服务端为基于内网对特征终端进行安全控制的服务端。

本发明实施例中，特征服务端为特定终端可访问的服务端，即私有云，可访问私有云的特征终端和私有云服务器处于同一个内网，在具体的实现中，私有云多架设在企业内网中，可以对内网的各个终端进行安全控制。

本发明实施例主要用于终端与私有云无法连接场景下，终端可以使用 http 数据包向私有云服务器发起请求，如果终端无法和私有云服务器连接，这个请求会立刻返回失败，终端从而判断处于无法连接私有云的环境。

本发明实施例中，所述应用程序可以是用户请求访问的应用程序，用户可以在终端通过点击应用程序的快捷方式或是程序文件等方式来请求访问该应用程序，终端接收到用户的点击之后，提取该应用程序的标识信息用于进一步进行鉴定。

本发明实施例中，所述应用程序也可以是特征终端安装的所有应用程序，特征终端确定无法连接特征服务器端时，可以提取所有应用程序的标识信息，在特征终端本地进行鉴定。

本发明实施例中，所述应用程序也可以是特征终端安装的需要与特征服务端保持连接的应用程序，终端确定无法连接特征服务器端时，提取该应用程序的标识信息，在特征终端本地进行鉴定。

在本发明的一种优选的实施例中，所述步骤 101 可以包括：

子步骤 SIl、特征终端提取应用程序对应的应用程序文件；

子步骤 S12、采用预设算法将所述应用程序文件转换为对应的标识信息。

本发明中，应用程序的标识信息可以通过对应用程序文件处理后得到，私有云终端安装有多个应用程序，每个程序对应有多个文件，其中包括有应用程序文件。应用程序文件即 PE（portable executable，可移植的可执行文件）格式的文件，PE 文件是微软 Windows 操作系统上的程序

文件，常见的 EXE、DLL, OCX, SYS、COM 都是 PE 文件，每个应用程序都有对应的 PE 文件。

具体的，PE 文件由 MS-DOS 可执行体、文件头、可选头、数据目录、节头以及节等结构组成，其中，文件头中包含如下结构：

1) "Machine（机器）"，用来指出该二进制文件预定运行于什么样的系统；

2) "NumberOf Sections（节数）"，它是紧跟在头后面的节的数目；

3) "TimeDateStamp（时间戳）"，用来给出文件建立的时间；

4-5) "PointerToSymbolTable（符号表指针）"和"NumberOfSymbols（符号数）"(都是 32 位）都用于调试信息的；

6) "SizeOfOptionalHeader（可选头大小）"只是"IMAGE— OPTIONAL— HEADER（可选头）"项的大小，可以用它去验证 PE 文件结构的正确性；

7) "Characteristics（特性）"是一个 16 位的，由许多标志位形成的集合组成，但大多数标志位只对目标文件和库文件有效。

本发明中可以通过 PE 文件的文件头中各个结构的关键词作为预设关键词，来判断应用程序对应的各个文件是否为应用程序文件。然后可以通过预设算法对应用程序文件进行转换，并将转换后的文件作为应用程序的标识信息。

通过对 PE 文件采用预设的算法进行转换可以得到对应的标识信息，本发明中，预设算法可以是 MD5 算法，即信息摘要算法 (Message-Digest Algorithm 5)，MD5 的作用是让大容量信息在用数字签名软件签署私人密钥前被"压缩"成一种保密的格式，就是把一个任意长度的字节串变换成一定长的十六进制数字串，可以确保信息传输完整一致。

步骤 102、依据所述标识信息，在特征终端预置的第一属性鉴定数据库中提取所述应用程序的第一属性，所述第一属性包括对所述应用程序的安全性分类。

本发明中，在终端预置了第一属性鉴定数据库，其中包括应用程序的标识信息和第一属性的对应关系，依据应用程序的标识信息便可以提取到相应的第一属性，第一属性可以包括对所述应用程序的安全性分类。

在本发明的一种实施例中，安全性分类可以分为三种，具体为黑文件、灰文件和白文件。若第一属性鉴定数据库构建的初期可能不够完善，

不存在该应用程序的标识信息时，为了避免影响用户使用该程序，可以该应用程序的安全性分类确定为灰文件，避免了第一属性鉴定数据库不够完善时，造成部分程序无法访问的问题。在具体的实现中，安全性分类的种类和个数也可以根据需要设定，本发明对此并不做限制。

进一步，本发明还可以包括：

若所述第一属性鉴定数据库中不存在所述应用程序的标识信息，则记录所述应用程序的标识信息。

对于鉴定为灰文件的应用程序，可以将记录下该应用程序的标识信息，在可以连接上私有云时，将该应用程序的标识信息发送到私有云进行鉴定，进一步，本发明实施例还可以包括：

在特征终端连接上特征服务端时，获取所述应用程序的标识信息发送到所述特征服务端进行鉴定。

进一步，本发明实施例还可以包括：

接收所述特征服务端返回的所述应用程序的第一属性，并将所述应用程序的标识信息和第一属性的对应关系保存在所述第一属性鉴定数据库中。

具体的，私有云构建有应用程序管理数据库，即私有黑白库，简称私有库，由私有云所在的企业组织内部自己定制，其中包括了各个应用程序的标识信息和第一属性的对应关系。私有云服务器接收到终端发送的应用程序的标识信息后，通过私有库对该应用程序的第一属性进行鉴定，并返回给终端，终端将该应用程序的第一属性与标识信息的对应关系保存在第一属性鉴定数据库中，下次可以直接利用本地的第一属性鉴定数据库确定该程序的第一属性，使得对应用程序的鉴定更为准确。

步骤 103、依据所述第一属性，在特征终端预置的第二属性配置文件中提取所述应用程序的第二属性，所述第二属性包括与所述安全性分类相对应的应用程序的执行策略。

在具体的实现中，特征终端可以安装有客户端软件，第二属性配置文件是可以内置在客户端软件的安装包中。本发明中，第二属性配置文件包括了应用程序的第一属性和第二属性的对应关系，第二属性可以包括与所述安全性分类相对应的应用程序的执行策略。在本发明的一种优选实施例中，应用程序的安全性分类与执行属性可以有如下对应关系：

所述应用程序的安全性分类为黑文件时，对应的执行策略为加载并执行所述应用程序；

所述应用程序的安全性分类为白文件时，对应的执行策略为不加载所述应用程序；

所述应用程序的安全性分类为灰文件时，对应的执行策略为执行所述应用程序的部分应用功能。

在具体的实现中，应用程序安全性分类和执行策略的对应关系可以根据应用环境和需求灵活设置。并且，用户可以按照自己不同的需求在特征服务端重新设置第二属性配置文件，然后对特征终端的第二属性配置文件进行更新，所述方法进一步还包括：

依据特征服务端的第二属性配置文件，对特征终端的第二属性配置文件进行更新。

步骤 104、特征终端依据所述执行策略加载和/或执行所述应用程序。

执行策略中包含了针对各种安全性分类，对应的加载或执行的方式，特征终端对应用程序的执行策略鉴定完后，可以依据执行策略决定是否加载该应用程序。

综上所述，依据本发明，通过在终端预置第一属性鉴定数据库和第二属性配置文件，终端在无法连接特征服务端时访问应用程序时，可以直接在本地鉴定出应用程序的安全性分类对应的执行策略，进而可以依据执行策略来加载应用程序，从而使得终端无法连接私有云时，终端依然可以对应用程序进行鉴定，得出应用程序是否可以执行，不影响用户对应用程序的访问。

本发明中，应用程序的安全性分类可以包括黑文件、白文件和灰文件等多种不同的属性，相应的，第二属性配置文件可以包括对多种不同的安全性分类分别对应的执行策略。客户可以按照自己不同的需求在私有云重新设置第二属性配置文件，然后对终端的第二属性配置文件进行更新。

本发明在第一属性鉴定数据库不够完善，无法对应用程序的第一属性进行鉴定时，可以将该应用程序的安全性分类判定为灰文件，进而可以在第二属性配置文件中找到相应的执行策略，避免了第一属性鉴定数

据库不够完善时，造成部分程序无法访问的问题。

参考图2，示出了本发明实施例的一种运行应用程序的安全控制装置实施例的结构框图，具体可以包括以下模块：

标识信息获取模块201，适于特征终端在无法连接特征服务端时，获取应用程序的标识信息；

第一属性获取模块202，适于依据所述标识信息，在特征终端预置的第一属性鉴定数据库中提取所述应用程序的第一属性，所述第一属性包括对所述应用程序的安全性分类；

第二属性获取模块203，适于依据所述第一属性，在特征终端预置的第二属性配置文件中提取所述应用程序的第二属性，所述第二属性包括与所述安全性分类相对应的应用程序的执行策略；

运行模块204，适于特征终端依据所述执行策略加载和/或执行所述应用程序。

本发明实施例中，所述应用程序可以包括请求访问的应用程序、或特征终端安装的所有应用程序、或特征终端安装的需要与特征服务端保持连接的应用程序。

在本发明的一种优选实施例中，所述第一属性鉴定数据库可以包括应用程序的标识信息和第一属性的对应关系，所述第二属性配置文件可以包括应用程序的第一属性和第二属性的对应关系。

在本发明的一种优选实施例中，所述安全性分类可以包括黑文件、白文件和灰文件，所述第一属性鉴定模块可以包括：

灰文件鉴定子模块，适于若所述第一属性鉴定数据库中不存在所述应用程序的标识信息，则判断所述应用程序的安全性分类为灰文件。

在本发明的一种优选实施例中，所述

应用程序的安全性分类为黑文件时，对应的执行策略为加载并执行所述应用程序；

所述应用程序的安全性分类为白文件时，对应的执行策略为不加载所述应用程序；

所述应用程序的安全性分类为灰文件时，对应的执行策略为执行所述应用程序的部分应用功能。

在本发明的一种优选实施例中，所述装置还可以包括：

记录模块，适于若所述第一属性鉴定数据库中不存在所述应用程序的标识信息，则记录所述应用程序的标识信息。

进一步，在该实施例中，所述装置还可以包括：

鉴定模块，适于在特征终端连接上特征服务端时，将所述应用程序的标识信息发送到所述特征服务端进行鉴定。

进一步，在该实施例中，所述装置还可以包括：

保存模块，适于接收所述特征服务端返回的所述应用程序的第一属性，并将所述应用程序的标识信息和第一属性的对应关系保存在所述第一属性鉴定数据库中。

在本发明的一种优选实施例中，所述装置还可以包括：

更新模块，适于依据特征服务端的第二属性配置文件，对特定终端的第二属性配置文件进行更新。

在本发明的一种优选实施例中，所述标识信息获取模块可以包括：

应用程序文件提取子模块，适于特征终端提取所述应用程序对应的应用程序文件；

转换子模块，适于采用预设算法将所述应用程序文件转换为对应的标识信息。

在本发明的一种优选实施例中，所述应用程序文件的文件头中可以包含预设关键词；所述预设算法可以包括信息摘要算法。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的运行应用程序的安全控制装置中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 3 示出了可以实现根据本发明的运行应用程序的安全控制方法的服务器，例如应用服务器。该服务器传统上包括处理器 310 和以存储器 320 形式的计算机程序产品或者计算机可读介质。存储器 320 可

以是诸如闪存、EEPROM （电可擦除可编程只读存储器）、EPROM 、硬盘或者 ROM 之类的电子存储器。存储器 320 具有用于执行上述方法中的任何方法步骤的程序代码 331 的存储空间 330。例如，用于程序代码的存储空间 330 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 331。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘 （CD) 、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图 4 所述的便携式或者固定存储单元。该存储单元可以具有与图 3 的服务器中的存储器 320 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 331'，即可以由例如诸如 310 之类的处理器读取的代码，这些代码当由服务器运行时，导致该服务器执行上面所描述的方法中的各个步骤。

本文中所称的"一个实施例"、"实施例"或者"一个或者多个实施例"意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里"在一个实施例中"的词语例子不一定全指同一个实施例。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下被实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词"包含"不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词"一"或"一个"不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。

因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求

1、一种运行应用程序的安全控制方法，包括：

特征终端在元法连接特征服务端时，获取应用程序的标识信息，所还特征服务端为基于内网对特征终端进行安全控制的服务端；

依据所述标识信息，在特征终端预置的第一属性鉴定数据库中提取所述应用程序的第一属性，所述第一属性包括对所述应用程序的安全性分类：

依据所述第一属性，在特征终端预置的第二属性配置文件中提取所述应用程序的第二属性，所述第二属性包括与所述安全性分类相对应的应用程序的执行策略；

特征终端依据所述执行策略加载和/或执行所述应用程序。

2、如权利要求1所述的方法，所述应用程序包括请求访问的应用程序、或特征终端安装的所有应用程序、或特征终端安装的需要与特征服务端保持连接的应用程序。

3、如权利要求1所述的方法，所述安全性分类包括黑文件、白文件和灰文件，若所述第一属性鉴定数据库中不存在所述应用程序的标识信息，则判断所述应用程序的安全性分类为灰文件。

4、如权利要求3所述的方法，所述应用程序的安全性分类为黑文件时，对应的执行策略为加载并执行所述应用程序；

所述应用程序的安全性分类为白文件时，对应的执行策略为不加载所述应用程序；

所述应用程序的安全性分类为灰文件时，对应的执行策略为执行所述应用程序的部分应用功能。

5、如权利要求1所述的方法，还包括：

若所述第一属性鉴定数据库中不存在所述应用程序的标识信息，则记录所述应用程序的标识信息。

6、如权利要求1或5所述的方法，还包括：

在特征终端连接上特征服务端时，获取应用程序的标识信息发送到所述特征服务端进行签定。

7、如权利要求6所述的方法，还包括：

接收特征服务端返回的所述应用程序的第一属性，并将所述应用程

序的标识信息和第一属性的对应关系保存在所述第一属性鉴定数据库中。

8、如权利要求]所迷的方法，还包括：

依据特征服务端的第二属性配置文件，对特征终端的第二属性配置文件进行更新。

9、如权利要求 1所述的方法，所述特征终端获取应用程序的标识信息的步璨包括：

特征终端提取应用程序对应的应用程序文件；

采用预设算法将所述应用程序文件转换为对应的标识信息。

10、如权利要求 9 所述的方法，所述应用程序文件的文件头中包含预设关键词：所述预设算法包括信息摘要算法。

11、一种运行应用程序的安全控制装置，包括：

标识信息获取模块，适于特征终端在无法连接特征服务端时，获取应用程序的标识信息，所迷特征服务端为基于内网对特定终端进行安全控制的服务端；

第一属性获取模块，适于依据所述标识信息，在特征终端预置的第一属性鉴定数据库中提取所迷应用程序的第一属性，所迷第一属性包括对所述应用程序的安全性分类：

第二属性获取模块，追于依据所述第一属性，在特征终端预置的第二属性配置文件中提取所述应用程序的第二属性，所述第二属性包括与所述安全性分类相对应的应用程序的执行策略；

运行模块，逸于特征终端依据所述执行策略加载和/或执行所述应用程序。

12、如权利要求 11 所述的装置，所述应用程序包括请求访问的应用程序、或特征终端安装的所有应用程序、或特征终端安装的需要与特征服务端保持连接的应用程序。

13、如权利要求 11 所述的装置，所述安全性分类包括黑文件、白文件和灰.文件，所述第一属性鉴定模块包括：

灰文件鉴定子模块，适于若所述第一属性鉴定数据库中不存在所述应用程序的标识信息，则判断所述应用程序的安全性分类为灰文件。

14、如权利要求 13 所述的装置，所述应用程序的安全性分类为嚴文件时，对应的执行策略为加截并执疔所述应用程序；

所述应用程序的安全性分类为白文件时，对应的执行策略为不加载所述应用程序；

所述应用程序的安全性分类为灰文件时，对应的执行策略为执行所述应用程序的部分应用功能。

15、如权利要求 11 所述的装置，还包括：

记录模块，适于若所述第一属性鉴定数据库中不存在所述应用程序的标识信息，则记录所述应用程序的标识信息。

16、如权利要求 11 或 15 所述的装置，还包括：

鉴定模块，适于在特征终端连接上特征服务端时，，获取所述应用程序的标识信息发送到所述特征服务端进行鉴定。

17、如权利要求 16 所述的装置，还包括：

保存模块，适于接收所述特征服务端返回的所述应用程序的第一属性，并将所述应用程序的标识信息和第一属性的对应关系保存在所述第一属性鉴定数据库中。

18、如权利要求 11 所述的装置，还包括：

更新模块，适于依据特征服务端的第二属性配置文件，对特征终端的第二属性配置文件进行更新。

19、如权利要求 11 所述的装置，所述标识信息获取模块包括：

应用程序文件提取子模块，适于特征終端提取应用程序对应的应用程序文件；

转换子模块，适于采用预设算法将所述应用程序文件转换为对应的标识信息。

20、如权利要求 19 所述的装置，所述应用程序文件的文件头中包含预设关键词；所述预设算法包括信息摘要算法。

21、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在服务器上运行时，导致所述服务器执行根据权利要求 1-10 中的任一个所述的运行应用程序的安全控制方法。

22、一种计算机可读介质，其中存储了如权利要求 21 所述的计算机程序。

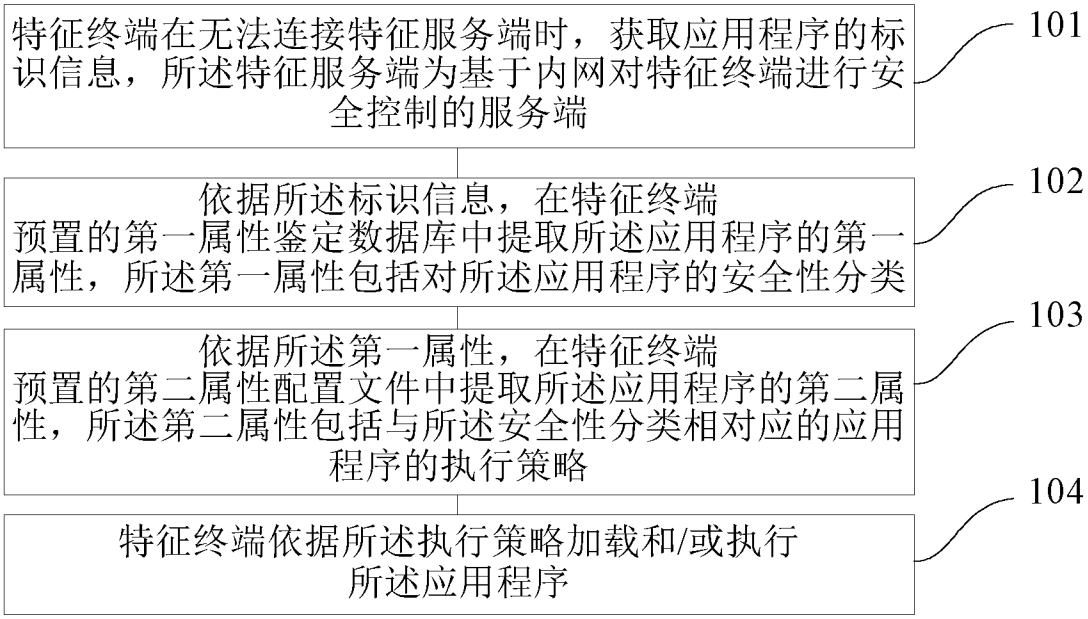
特征终端在无法连接特征服务端时，获取应用程序的标识信息，所述特征服务端为基于内网对特征终端进行安全控制的服务端
101
依据所述标识信息，在特征终端预置的第一属性鉴定数据库中提取所述应用程序的第一属性，所述第一属性包括对所述应用程序的安全性分类
102
依据所述第一属性，在特征终端预置的第二属性配置文件中提取所述应用程序的第二属性，所述第二属性包括与所述安全性分类相对应的应用程序的执行策略
103
特征终端依据所述执行策略加载和/或执行所述应用程序
104

图 1


标识信息获取模块201
第一属性获取模块202
第二属性获取模块203
运行模块204

图 2

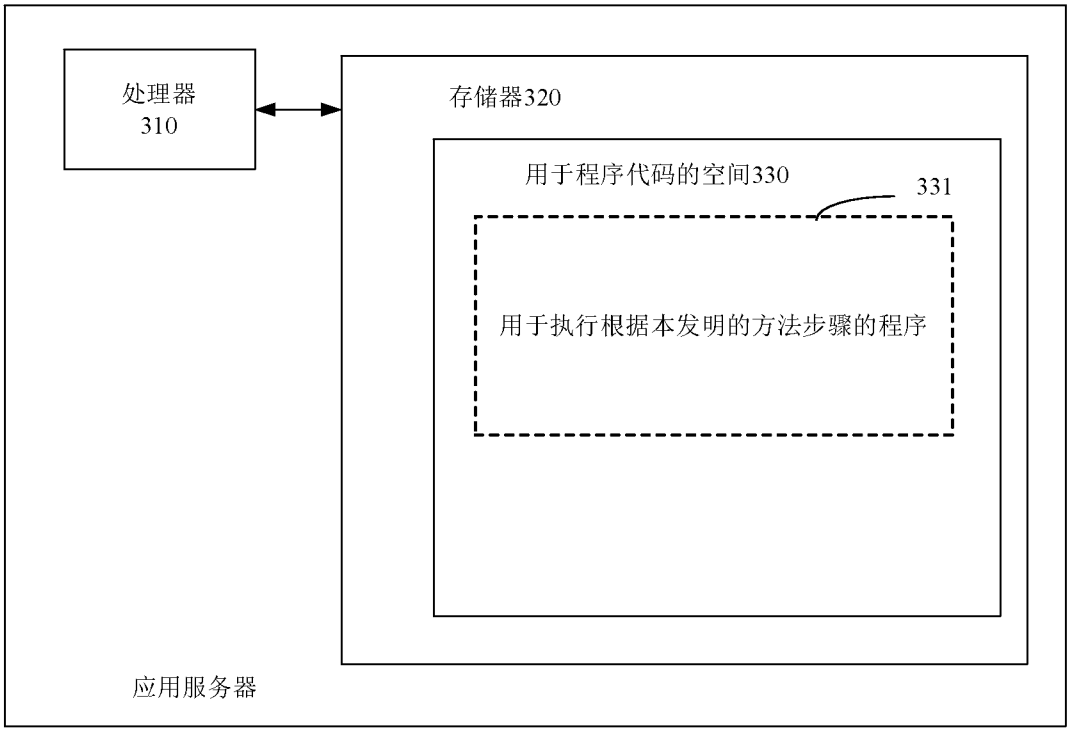
处理器
310
存储器320
用于程序代码的空间330
331
用于执行根据本发明的方法步骤的程序
应用服务器

图 3

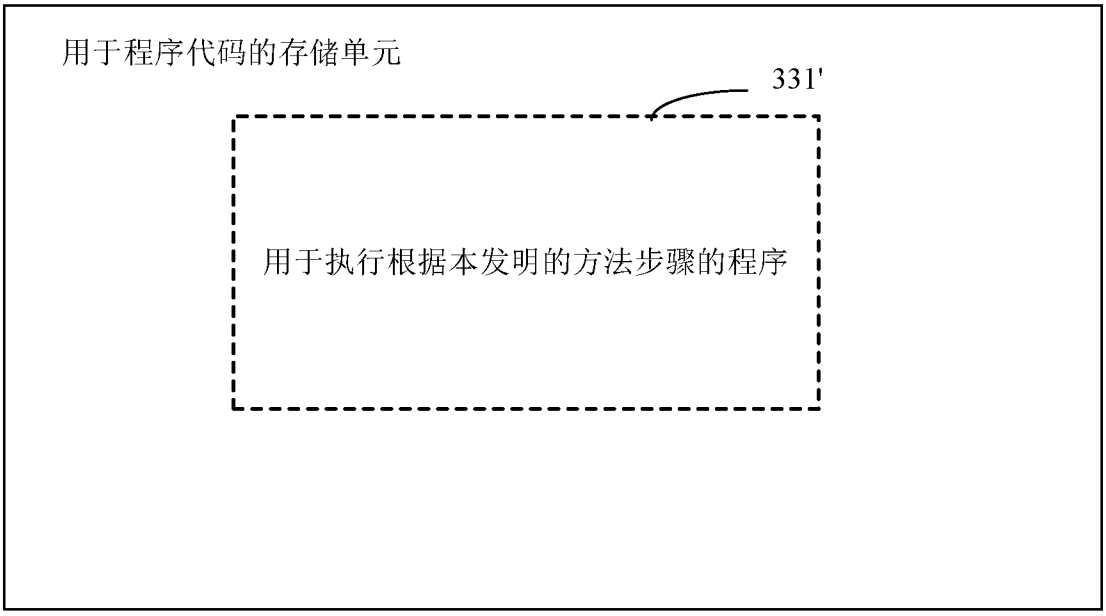
用于程序代码的存储单元
331'
用于执行根据本发明的方法步骤的程序

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/083621

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

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)

IPC: G06F; H04L

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, IEEE, GOOGLE: application, server, attribute, identity, security, run, execute, database, cloud, policy

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 1900941 A (FU, Yusheng) 24 January 2007 (24.01.2007) description, page 1, line 17 to 23, page 3, line 13 to page 5, line 7	1-22
PX	CN 102982275 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 20 March 2013 (20.03.2013) description, paragraphs [0007] -[0056]	1-22
A	US 2005/0125494 A1 (TSUBASA SYSTEM CO., LTD.) 09 June 2005 (09.06.2005) the whole document	1-22

☐ 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
29 November 2013 (29.11.2013)	19 December 2013 (19.12.2013)

[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
WANG, Liang
Telephone No. (86-10) 62412608

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN20 13/083621

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1900941 A	24.01.2007	None	
CN 102982275 A	20.03.2013	None	
US 2005/0125494 A l	09.06.2005	CN 1625125 A	08.06.2005
		JP 2005165874 A	23.06.2005
		KR 20050054435 A	10.06.2005

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN201 3/083621

A. CLASSIFICATION O F SUBJECT MATTER

G06 F 21/51 (2013.01) i

G06 F 21/52 (2013.01) i

国际检索报告

国际申请号
PCT/CN20 13/083621

A. 主题的分类

参见附加页

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)

IPC: G06F, H04L

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,IEEE, GOOGLE: 应用,程序,服务端,属性,标识,安全,执行,运行,加载,数据库,云,策略,application, server, attribute, identity, security, run, execute, database, cloud, policy

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	CN1900941 A (傅玉生)24. 1 月 2007(24.01.2007) 说明书第 1 页第 17 行至 23 行,第 3 页第 13 行至第 5 页第 7 行	1-22
PX	CN102982275 A (北京奇虎科技有限公司等)20.3 月 2013(20.03.2013 ,说明书 [0007]-[0056] 段	1-22
A	US2005/0 125494 A1(TSUBASA SYSTEM CO., LTD.)09.6 月 2005(09.06.2005)全文	1-22

☐ 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¾¾¾¾§ 公布i¾ P先申¾¾¾

"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
29. 11 月 2013(29. 11.2013)	19.12 月 2013 (19.12.2013)
ISA/CN 的名称和邮寄地址: 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 10008S 传真号: (86-10)62019451	受权官员 王亮 电话号码: (86-10) 62412608

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2013/083621

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1900941 A	24.01.2007	无	
CN102982275 A	20.03.2013	无	
US2005/0125494 A l	09.06.2005	CN1625125 A	08.06.2005
		JP2005 165874 A	23.06.2005
		KR20050054435 A	10.06.2005

国际检索报告

国际申请号
PCT/CN2013/083621

A. 主题的分类

G06F 21/51 (2013.01)i

G06F 21/52 (2013.01)i