(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 103020118 A
(43)申请公布日 2013.04.03

(21)申请号 201210458968.X

(22)申请日 2012.11.14

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 奇智软件(北京)有限公司

(72)发明人 张家柱

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 苏培华

(51)Int.Cl.
G06F 17/30(2006.01)
H04L 29/08(2006.01)
H04L 29/06(2006.01)

权利要求书 3 页 说明书 11 页 附图 1 页

(54)发明名称

用于应用程序的安全属性识别方法和装置

(57)摘要

本发明实施例提供了一种更为可靠的用于应用程序的安全属性识别方法和装置，该装置包括特征文件接收模块，适于接收终端提交的应用程序的特征文件；判断模块，适于判断当前是否可以连接第二服务端，若是，则执行第二服务端识别模块，若否，则执行参考数据库识别模块；第二服务端识别模块，适于通过访问第二服务端，依据特征文件获取应用程序对应的安全属性；参考数据库识别模块，适于访问预置在第一服务端的参考数据库，依据特征文件获取应用程序对应的安全属性；其中，通过以下模块预置参考数据库：下载模块，适于访问第二服务端，下载参考数据库；保存模块，适于将参考数据库保存在第一服务端；参考数据库通过离线下载的方式进行更新。

CN 103020118 A

1. 一种用于应用程序的安全属性识别方法，包括：

接收终端提交的应用程序的特征文件；

判断当前是否可以连接第二服务端；

若是，则通过访问所述第二服务端，依据所述特征文件获取所述应用程序对应的安全属性；若否，则访问预置在第一服务端的参考数据库，依据所述特征文件获取所述应用程序对应的安全属性；

其中，所述第一服务端为与所述终端处于同一内网的服务端，所述第二服务端为设置在互联网中，所述终端通过互联网可访问的服务端；

其中，通过以下步骤预置所述参考数据库：

访问第二服务端，下载所述参考数据库，并将所述参考数据库保存在第一服务端中；

所述参考数据库通过离线下载的方式进行更新。

2. 如权利要求 1 所述的方法，还包括：

依据所述安全属性查找所述应用程序的安装文件，或将所述安全属性返回终端，由终端依据所述安全属性加载所述应用程序。

3. 如权利要求 1 所述的方法，所述第二服务端预置有应用程序管理数据库，所述应用程序管理数据库与所述参考数据库中均包括多个应用程序的特征文件，以及对应的安全属性；

所述安全属性包括不可执行的黑文件和可执行的白文件。

4. 如权利要求 3 所述的方法，所述终端通过以下步骤获取应用程序的特征文件：

扫描终端所有应用程序对应的所有文件，提取出其中的应用程序文件；

采用预设算法将所述应用程序文件转换为对应的程序特征文件。

5. 如权利要求 3 所述的方法，所述终端通过以下步骤获取应用程序的特征文件：

接收用户访问应用程序的请求；

依据所述请求提取对应的应用程序文件，并采用预设算法将所述应用程序文件转换为对应的程序特征文件。

6. 如权利要求 4 或 5 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。

7. 如权利要求 4 所述的方法，还包括：

依据各个应用程序的特征文件与可安全属性的对应关系，构建第一服务端的应用程序管理数据库。

8. 如权利要求 5 所述的方法，还包括：

将各个应用程序的特征文件与可安全属性的对应关系添加到第一服务端的应用程序管理数据库中。

9. 如权利要求 5 所述的方法，第一服务端部署有应用程序管理数据库，所述应用程序管理数据库保存有多个应用程序的特征文件，以及对应的安全属性；

所述方法还包括：

在第一服务端的应用程序管理数据库搜索是否存在所述应用程序的特征文件，若否，则执行判断当前是否可以连接第二服务端的步骤。

10. 如权利要求 5 所述的方法，还包括：

若所述应用程序文件的安全属性为黑文件，则生成不可执行的提示信息并返回给终端，终端接收提示信息后不加载所述应用程序；

若所述应用程序文件的安全属性为白文件，则生成可执行的提示信息并返回给终端，终端接收提示信息后开始加载所述应用程序。

11. 一种用于应用程序的安全属性识别装置，包括：

特征文件接收模块，适于接收终端提交的应用程序的特征文件；

判断模块，适于判断当前是否可以连接第二服务端，若是，则执行第二服务端识别模块，若否，则执行参考数据库识别模块；

第二服务端识别模块，适于通过访问所述第二服务端，依据所述特征文件获取所述应用程序对应的安全属性；

参考数据库识别模块，适于访问预置在第一服务端的参考数据库，依据所述特征文件获取所述应用程序对应的安全属性；

其中，所述第一服务端为与所述终端处于同一内网的服务端，所述第二服务端为设置在互联网中，所述终端通过互联网可访问的服务端；

其中，通过以下模块预置所述参考数据库：

下载模块，适于访问第二服务端，下载所述参考数据库；

保存模块，适于将所述参考数据库保存在第一服务端；

所述参考数据库通过离线下载的方式进行更新。

12. 如权利要求 11 所述的装置，还包括：

应用程序处理模块，适于依据所述安全属性查找所述应用程序的安装文件，或将所述安全属性返回终端，由终端依据所述安全属性加载所述应用程序。

13. 如权利要求 11 所述的装置，所述第二服务端预置有应用程序管理数据库，所述应用程序管理数据库与所述参考数据库中均包括多个应用程序的特征文件，以及对应的安全属性；

所述安全属性包括不可执行的黑文件和可执行的白文件。

14. 如权利要求 13 所述的装置，所述终端通过以下模块获取应用程序的特征文件：

应用程序文件提取模块，适于扫描终端所有应用程序对应的所有文件，提取出其中的应用程序文件；

第一转换模块，适于采用预设算法将所述应用程序文件转换为对应的程序特征文件。

15. 如权利要求 13 所述的装置，所述终端通过以下模块获取应用程序的特征文件：

请求接收模块，适于接收用户访问应用程序的请求；

第二转换模块，适于依据所述请求提取对应的应用程序文件，并采用预设算法将所述应用程序文件转换为对应的程序特征文件。

16. 如权利要求 14 或 15 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。

17. 如权利要求 14 所述的装置，还包括：

数据库构建模块，适于依据各个应用程序的特征文件与可安全属性的对应关系，构建第一服务端的应用程序管理数据库。

18. 如权利要求 15 所述的装置，还包括：

添加模块，适于将各个应用程序的特征文件与可安全属性的对应关系添加到第一服务端的应用程序管理数据库中。

19. 如权利要求 15 所述的装置，第一服务端部署有应用程序管理数据库，所述应用程序管理数据库保存有多个应用程序的特征文件，以及对应的安全属性；

所述装置还包括：

搜索模块，适于在第一服务端的应用程序管理数据库搜索是否存在所述应用程序的特征文件，若否，则执行判断当前是否可以连接第二服务端的步骤。

20. 如权利要求 15 所述的装置，还包括：

第一提示信息返回模块，适于若所述应用程序文件的安全属性为黑文件，则生成不可执行的提示信息并返回给终端，终端接收提示信息后不加载所述应用程序；

第二提示信息返回模块，适于若所述应用程序文件的安全属性为白文件，则生成可执行的提示信息并返回给终端，终端接收提示信息后开始加载所述应用程序。

用于应用程序的安全属性识别方法和装置

技术领域

[0001] 本申请涉及互联网技术领域，特别是涉及一种用于应用程序的安全属性识别方法和装置。

背景技术

[0002] 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。

[0003] 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。只要是注册用户、付费用户都可以通过互联网访问公有云以获得相应的网络服务，但并不拥有云计算资源。

[0004] 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。

[0005] 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，用于管理各个程序是否可执行。

[0006] 具体而言，私有库分为白库和黑库，白库包括可执行的程序，即白文件；黑库包括禁止运行程序，即黑文件。私有库可以由组织自己定制，决定哪些程序被禁止，哪些程序可以正常运行，一方面可以避免了企业内部一些专用系统文件被禁止；而另一方面可以把恶意病毒木马和企业禁止的正常软件都无法运行。

[0007] 终端请求访问一个程序时，可以依据私有库判断该程序是黑文件还是白文件，若是黑文件，则不允许访问该程序。

[0008] 以上现有技术中存在的问题是，私有云的私有库可能不够完善，特别是在刚部署完私有云时，私有库中可能并不存在用户请求访问的程序，进而无法判断是否执行该程序；虽然可以进行人工判断，但由于管理人员通常比较不熟悉业务，对这些程序没有认知，对该文件的可安全属性无法进行可靠的识别。

[0009] 因此，目前需要本领域技术人员解决的一个技术问题就是，提供一种更为可靠的应用程序安全属性的识别机制。

发明内容

[0010] 鉴于上述问题，本发明实施例提出了以便提供一种克服上述问题或者至少部分地解决上述问题的用于应用程序的安全属性识别方法和相应的用于应用程序的安全属性识别装置。

[0011] 依据本发明实施例的一个方面，提供了一种用于应用程序的安全属性识别方法，包括：

[0012] 接收终端提交的应用程序的特征文件；

[0013] 判断当前是否可以连接第二服务端；

[0014] 若是，则通过访问所述第二服务端，依据所述特征文件获取所述应用程序对应的安全属性；若否，则访问预置在第一服务端的参考数据库，依据所述特征文件获取所述应用程序对应的安全属性；

[0015] 其中，所述第一服务端为与所述终端处于同一内网的服务端，所述第二服务端为设置在互联网中，所述终端通过互联网可访问的服务端；

[0016] 其中，通过以下步骤预置所述参考数据库：

[0017] 访问第二服务端，下载所述参考数据库，并将所述参考数据库保存在第一服务端中；

[0018] 所述参考数据库通过离线下载的方式进行更新。

[0019] 本发明实施例中，所述方法还包括：

[0020] 依据所述安全属性查找所述应用程序的安装文件，或将所述安全属性返回终端，由终端依据所述安全属性加载所述应用程序。

[0021] 本发明实施例中，所述第二服务端预置有应用程序管理数据库，所述应用程序管理数据库与所述参考数据库中均包括多个应用程序的特征文件，以及对应的安全属性；

[0022] 所述安全属性包括不可执行的黑文件和可执行的白文件。

[0023] 本发明实施例中，所述终端通过以下步骤获取应用程序的特征文件：

[0024] 扫描终端所有应用程序对应的所有文件，提取出其中的应用程序文件；

[0025] 采用预设算法将所述应用程序文件转换为对应的程序特征文件。

[0026] 本发明实施例中，所述终端通过以下步骤获取应用程序的特征文件：

[0027] 接收用户访问应用程序的请求；

[0028] 依据所述请求提取对应的应用程序文件，并采用预设算法将所述应用程序文件转换为对应的程序特征文件。

[0029] 本发明实施例中，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。

[0030] 本发明实施例中，所述方法还包括：

[0031] 依据各个应用程序的特征文件与可安全属性的对应关系，构建第一服务端的应用程序管理数据库。

[0032] 本发明实施例中，所述方法还包括：

[0033] 将各个应用程序的特征文件与可安全属性的对应关系添加到第一服务端的应用程序管理数据库中。

[0034] 本发明实施例中，第一服务端部署有应用程序管理数据库，所述应用程序管理数据库保存有多个应用程序的特征文件，以及对应的安全属性；

[0035] 所述方法还包括：

[0036] 在第一服务端的应用程序管理数据库搜索是否存在所述应用程序的特征文件，若否，则执行判断当前是否可以连接第二服务端的步骤。

[0037] 本发明实施例中，所述方法还包括：

[0038] 若所述应用程序文件的安全属性为黑文件，则生成不可执行的提示信息并返回给终端，终端接收提示信息后不加载所述应用程序；

[0039] 若所述应用程序文件的安全属性为白文件，则生成可执行的提示信息并返回给终

端，终端接收提示信息后开始加载所述应用程序。

[0040] 根据本发明实施例的另一方面，提供了一种用于应用程序的安全属性识别装置，包括：

[0041] 特征文件接收模块，适于接收终端提交的应用程序的特征文件；

[0042] 判断模块，适于判断当前是否可以连接第二服务端，若是，则执行第二服务端识别模块，若否，则执行参考数据库识别模块；

[0043] 第二服务端识别模块，适于通过访问所述第二服务端，依据所述特征文件获取所述应用程序对应的安全属性；

[0044] 参考数据库识别模块，适于访问预置在第一服务端的参考数据库，依据所述特征文件获取所述应用程序对应的安全属性；

[0045] 其中，所述第一服务端为与所述终端处于同一内网的服务端，所述第二服务端为设置在互联网中，所述终端通过互联网可访问的服务端；

[0046] 其中，通过以下模块预置所述参考数据库：

[0047] 下载模块，适于访问第二服务端，下载所述参考数据库；

[0048] 保存模块，适于将所述参考数据库保存在第一服务端；

[0049] 所述参考数据库通过离线下载的方式进行更新。

[0050] 本发明实施例中，所述装置还包括：

[0051] 应用程序处理模块，适于依据所述安全属性查找所述应用程序的安装文件，或将所述安全属性返回终端，由终端依据所述安全属性加载所述应用程序。

[0052] 本发明实施例中，所述第二服务端预置有应用程序管理数据库，所述应用程序管理数据库与所述参考数据库中均包括多个应用程序的特征文件，以及对应的安全属性；

[0053] 所述安全属性包括不可执行的黑文件和可执行的白文件。

[0054] 本发明实施例中，所述终端通过以下模块获取应用程序的特征文件：

[0055] 应用程序文件提取模块，适于扫描终端所有应用程序对应的所有文件，提取出其中的应用程序文件；

[0056] 第一转换模块，适于采用预设算法将所述应用程序文件转换为对应的程序特征文件。

[0057] 本发明实施例中，所述终端通过以下模块获取应用程序的特征文件：

[0058] 请求接收模块，适于接收用户访问应用程序的请求；

[0059] 第二转换模块，适于依据所述请求提取对应的应用程序文件，并采用预设算法将所述应用程序文件转换为对应的程序特征文件。

[0060] 本发明实施例中，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。

[0061] 本发明实施例中，所述装置还包括：

[0062] 数据库构建模块，适于依据各个应用程序的特征文件与可安全属性的对应关系，构建第一服务端的应用程序管理数据库。

[0063] 本发明实施例中，所述装置还包括：

[0064] 添加模块，适于将各个应用程序的特征文件与可安全属性的对应关系添加到第一服务端的应用程序管理数据库中。

[0065] 本发明实施例中，第一服务端部署有应用程序管理数据库，所述应用程序管理数据库保存有多个应用程序的特征文件，以及对应的安全属性；

[0066] 所述装置还包括：

[0067] 搜索模块，适于在第一服务端的应用程序管理数据库搜索是否存在所述应用程序的特征文件，若否，则执行判断当前是否可以连接第二服务端的步骤。

[0068] 本发明实施例中，所述装置还包括：

[0069] 第一提示信息返回模块，适于若所述应用程序文件的安全属性为黑文件，则生成不可执行的提示信息并返回给终端，终端接收提示信息后不加载所述应用程序；

[0070] 第二提示信息返回模块，适于若所述应用程序文件的安全属性为白文件，则生成可执行的提示信息并返回给终端，终端接收提示信息后开始加载所述应用程序

[0071] 根据本发明实施例的用于应用程序的安全属性识别方法，在私有云的私有库不够完善时，首先判断是否可连接目标公有云，进而选择通过目标公有云或是预置在私有云的参考数据库，来判断终端提交的应用程序是是黑文件还是白文件，从而可以在私有库不完善时，对应用程序进行比较可靠的识别。

[0072] 本发明可以进一步将目标公有云或参考数据库对应用程序的识别结果保存在私有云私有库中，从而可以完善私有库。

[0073] 利用本发明的方法可以在私有云刚部署完时，对终端的所有应用程序进行识别，并依据识别结果来建立私有库，从而使得私有云的私有库的建立有效、快速、可靠。

[0074] 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

[0075] 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：

[0076] 图 1 示出了根据本发明实施例一种用于应用程序的安全属性识别方法实施例的步骤流程图；

[0077] 图 2 示出了根据本发明实施例一种用于应用程序的安全属性识别装置实施例的结构框图。

具体实施方式

[0078] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0079] 本发明实施例可以应用于计算机系统 / 服务器，其可与众多其它通用或专用计算系统环境或配置一起操作。适于与计算机系统 / 服务器一起使用的众所周知的计算系统、环境和 / 或配置的例子包括但不限于：个人计算机系统、服务器计算机系统、瘦客户机、厚

客户机、手持或膝上设备、基于微处理器的系统、机顶盒、可编程消费电子产品、网络个人电脑、小型计算机系统、大型计算机系统和包括上述任何系统的分布式云计算技术环境，等等。

[0080] 计算机系统/服务器可以在由计算机系统执行的计算机系统可执行指令(诸如程序模块)的一般语境下描述。通常，程序模块可以包括例程、程序、目标程序、组件、逻辑、数据结构等等，它们执行特定的任务或者实现特定的抽象数据类型。计算机系统/服务器可以在分布式云计算环境中实施，分布式云计算环境中，任务是由通过通信网络链接的远程处理设备执行的。在分布式云计算环境中，程序模块可以位于包括存储设备的本地或远程计算系统存储介质上。

[0081] 参考图1，示出了本发明实施例的一种用于应用程序的安全属性识别方法实施例1的步骤流程图，具体可以包括以下步骤：

[0082] 步骤101、接收终端提交的应用程序的特征文件。

[0083] 第一服务端是与终端处于同一内网的服务端，在本发明中即为私有云，终端和私有云服务器处于同一个局域网中，终端可以安装有私有云客户端软件，可以由客户端软件执行向私有云提交应用程序的特征文件的操作。

[0084] 本发明实施例中，应用程序的特征文件可以通过对应用程序文件处理后得到，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。本发明可以通过对PE文件进行如下的处理得到应用程序对应的特征文件。

[0085] 在本发明的一种优选实施例中，在私有云刚刚部署完成，私有云的应用程序管理数据库还未建立的情况下，可以对多个应用程序进行识别，所述终端可以通过以下步骤获取应用程序的特征文件：

[0086] 子步骤S21、扫描终端所有应用程序对应的所有文件，提取出其中的应用程序文件；

[0087] 子步骤S22、采用预设算法将所述应用程序文件转换为对应的程序特征文件。

[0088] 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。客户端软件可以针对每个应用程序所对应的所有文件进行扫描，找出其中的应用程序文件，具体的，应用程序文件包括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：

[0089] 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；

[0090] 2)“NumberOfSections(节数)”，它是紧跟在头后面的节的数目；

[0091] 3)“TimeDateStamp(时间戳)”，用来给出文件建立的时间；

[0092] 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；

[0093] 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；

[0094] 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。

[0095] 本发明中可以通过应用程序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特征文件。在本发明的一种优选的实施例中，可以采用信息摘要算法对应用程序文件进行转换，信息摘要算法即 MD5（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。

[0096] 在本发明的另一种实施例中，用户可以在终端向第一服务端，提交对应用程序的识别请求，其中包括应用程序的特征文件。该应用程序可以是用户请求访问或请求安装的某个应用程序。

[0097] 本发明的一种应用场景下，用户需要在终端安装某个应用程序时，则可以在终端提交应用程序的特征文件，对特征文件识别后，进一步决定是否返回该应用程序的安装文件。

[0098] 在本发明的另一种应用场景下，用户需要在终端访问某个应用程序时，则可以在终端提交应用程序的特征文件，判断出该应用程序的安全属性后，可以返回给终端，由终端进一步加载该程序。

[0099] 在此应用场景下，所述终端可以通过以下步骤获取应用程序的特征文件：

[0100] 子步骤 S31、接收用户访问应用程序的请求；

[0101] 子步骤 S32、依据所述请求提取对应的应用程序文件，并采用预设算法将所述应用程序文件转换为对应的程序特征文件。

[0102] 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来请求访问该应用程序，终端接收到用户的点击之后，可以提取对应的应用程序文件，然后采用预设的算法对应用程序文件进行转换，得到特征文件，与上个实施例相同，本实施例中，也可以通过预设关键字来查找该程序对应的应用程序文件，预设算法可以是 MD5 算法。

[0103] 步骤 102、判断当前是否可以连接第二服务端，若是，则执行步骤 103，若否，则执行步骤 104；

[0104] 步骤 103、通过访问所述第二服务端，依据所述特征文件获取所述应用程序对应的安全属性。

[0105] 第二服务端为设置在互联网中，终端通过互联网即可访问的服务端，在本发明中，即为公有云，可以预先选取某个公有云作为目标公有云，公有云可以预置有应用程序管理数据库，所述应用程序管理数据库包括多个应用程序的特征文件以及对应的安全属性。依据应用程序的特征文件，可以在应用程序管理数据库中查找到相应的安全属性。

[0106] 私有云接收到终端发送的应用程序的特征文件后，可以进一步判断是否可以连接目标公有云，即是否可以连接上目标公有云的服务器。若可以连接上，则可以利用公有云的应用程序管理数据库，来判断应用程序的安全属性。

[0107] 所述应用程序管理数据库中可以包括多个应用程序的特征文件，以及对应的安全属性。安全属性包括不可执行的黑文件和可执行的白文件，若某个应用程序的安全属性为黑文件，则表明该应用程序在终端是被禁止执行的不安全程序或是需要屏蔽的程序，反之，若是白文件，则可以执行。具体的，某个应用程序是否可以执行，可以在预置参考数据库时，

根据用户的应用环境和需求来自定。

[0108] 在具体的实现中，所述应用程序管理数据库可以包括黑库和白库，若在黑库中搜索到特征文件，则表明该应用程序的安全属性为黑文件；若在白库中搜索到特征文件，则表明该应用程序的安全属性为白文件。

[0109] 所述应用程序管理数据库也可以只包括黑库，若在黑库中搜索到特征文件，则表明该应用程序的安全属性为黑文件。所述应用程序管理数据库也可以只包括白库，若在库中搜索到特征文件，则表明该应用程序的安全属性为白文件。

[0110] 若在所述应用程序管理数据库中搜索不到所述特征文件，则可以认为该应用程序文件为黑文件，或者将该应用程序文件作为未知安全属性的灰文件，上报到终端，供技术人员查看和分析。

[0111] 步骤 104、访问预置在第一服务端参考数据库，依据所述特征文件获取所述应用程序对应的安全属性。

[0112] 本发明中，私有云预置有参考数据库，其中也包含了多个应用程序的特征文件以及对应的安全属性。在公有云无法连接的情况下，可以通过预置的参考数据库来对应用程序进行识别。

[0113] 在本发明的一种优选的实施例中，可以通过以下步骤预置所述参考数据库：

[0114] 子步骤 S11、访问第二服务端，下载所述参考数据库；

[0115] 子步骤 S12、将所述参考数据库保存在第一服务端；

[0116] 其中，所述参考数据库通过离线下载的方式进行更新。

[0117] 参考数据库可以从第二服务端即公有云下载，相当于离线状态下的公有云应用程序管理数据库，下载后保存在私有云。参考数据库可以按照预设的频率，通过离线下载的方式进行更新。

[0118] 所述参考数据库中可以包括多个程序特征文件，以及对应的安全属性。与所述应用程序管理数据库类似，在具体的实现中，所述参考数据库可以包括黑库和白库中的一种或多种。

[0119] 在本发明的一种优选实施例中，在获取了应用程序的安全属性之后，所述方法还可以包括：

[0120] 在依据所述安全属性查找所述应用程序的安装文件，或将所述安全属性返回终端，由终端依据所述安全属性加载所述应用程序。

[0121] 应用程序的安全属性表明了该程序是可被执行的黑文件或是不可被执行的白文件，在本发明的一种应用场景下，用户需要在终端访问某个应用程序时，则可以在终端提交应用程序的特征文件，判断出该应用程序的安全属性后，可以返回给终端，由终端进一步加载该程序。具体而言，若该程序的安全属性为黑文件，则终端将进一步加载该程序；若是白文件，则终端不加载该程序。

[0122] 本发明的另一种应用场景下，用户需要在终端安装某个应用程序时，则可以在终端提交应用程序的特征文件，若识别该应用程序的安全属性是白文件，则可以向终端返回该程序的安装文件。在具体的实现中，私有云的网络管理的控制台或控制终端上，可以记录各个终端所安装的应用程序，具体的，可以记录特征文件和安装该应用程序的终端的对应关系，判断用户请求安装的应用程序可执行后，若该应用程序的特征文件存在于上述记录

中，则可以向对应的终端发送请求，将安装文件共享给请求该应用程序的安装终端；若用户请求安装的应用程序不可执行，网络管理的控制台或控制终端可以进行报警处理。

[0123] 在本发明的一种实施例中，在私有云的应用程序管理数据库还未建立的情况下，还可以依据各个应用程序的特征文件与可安全属性的对应关系，构建第一服务端即私有云的应用程序管理数据库。按照各个应用程序的可安全属性可以构建应用程序管理数据库，具体的，可以将可安全属性为白文件的特征文件构建白库，也可以将可安全属性为黑文件的特征文件构建黑库，也可以同时构建白库和黑库，使用本发明的方法可以使得私有云的私有库的建立有效、快速、可靠。

[0124] 在本发明的另一种实施例中，私有云已经部署有应用程序管理数据库，所述应用程序管理数据库可以保存有多个应用程序的特征文件，以及对应的安全属性。

[0125] 在该实施例中，在判断是否可以连接第二服务端之前，所述方法还可以包括：

[0126] 在第一服务端的应用程序管理数据库搜索是否存在所述应用程序的特征文件，若否，则执行判断当前是否可以连接第二服务端的步骤。

[0127] 由于私有云已经部署有应用程序管理数据库，即私有库，因此，在利用公有云或参考数据库对程序特征文件进行识别之前，可以先在私有云的应用程序管理数据库中搜索是否存在该程序的特征文件，若不存在，再进一步连接公有云或参考数据库进行判断。

[0128] 在该实施例中，在对应用程序的安全属性进行识别之后，所述方法还可以包括：

[0129] 若所述应用程序文件的安全属性为黑文件，则生成不可执行的提示信息并返回给终端，终端接收提示信息后不加载所述应用程序；

[0130] 若所述应用程序文件的安全属性为白文件，则生成可执行的提示信息并返回给终端，终端接收提示信息后开始加载所述应用程序。

[0131] 本实施例中，私有库已构建，用户请求访问某个程序时，终端上传该程序的特征文件到私有云，私有云通过私有库或公有云或参考数据库进行识别，若该程序安全属性的识别结果，即安全属性为黑文件，则会不可执行的提示信息，返回到终端，终端则会拦截并停止加载该程序；若是白文件，则可以开始加载应用程序。

[0132] 进一步的，若私有云的应用程序管理数据库已经构建，所述方法还可以包括：

[0133] 将各个应用程序的特征文件与可安全属性的对应关系添加到第一服务端的应用程序管理数据库中。

[0134] 将依据公有云或参考数据库识别结果添加到私有云的应用程序管理数据库中，可以对私有云的应用程序管理数据库进行完善。

[0135] 综上所述，根据本发明实施例的一种应用程序安全属性的识别方法，在私有云的私有库不够完善时，首先判断是否可连接目标公有云，进而选择通过目标公有云或是预置在私有云的参考数据库，来判断终端提交的应用程序是是黑文件还是白文件，从而可以在私有库不完善时，对应用程序的安全属性进行比较可靠的识别。

[0136] 本发明可以进一步将目标公有云或参考数据库对应用程序安全属性的识别结果保存在私有云私有库中，从而可以完善私有库。

[0137] 利用本发明的方法可以在私有云刚部署完时，对终端的所有应用程序的安全属性进行识别，并依据安全属性识别结果来建立私有库，从而使得私有云的私有库的建立有效、快速、可靠。

[0138] 本说明书中的各个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

[0139] 需要说明的是，在本发明实施例中，所述硬件是指用户设备中的硬件，所述用户设备包括计算机、手机、PDA 等，所述硬件包括 CPU、主板、显卡、显示器、内存、硬盘、光驱、声卡、电池、网卡、鼠标键盘和 / 或摄像头等。本发明实施例不仅可以应用于单台设备的应用环境中，还可以应用于服务器 - 终端的应用环境，或者进一步应用于基于云技术的应用环境中。

[0140] 对于方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

[0141] 参考图 2，示出了本发明实施例的一种用于应用程序的安全属性识别装置实施例的结构框图，具体可以包括以下模块：

[0142] 特征文件接收模块 201，适于接收终端提交的应用程序的特征文件；

[0143] 判断模块 202，适于判断当前是否可以连接第二服务端，若是，则执行第二服务端识别模块，若否，则执行参考数据库识别模块；

[0144] 第二服务端识别模块 203，适于通过访问所述第二服务端，依据所述特征文件获取所述应用程序对应的安全属性；

[0145] 参考数据库识别模块 204，适于访问预置在第二服务端的参考数据库，依据所述特征文件获取所述应用程序对应的安全属性；

[0146] 其中，所述第一服务端为与所述终端处于同一内网的服务端，所述第二服务端为设置在互联网中，所述终端通过互联网可访问的服务端。

[0147] 在本发明的一种优选的实施例中，所述第二服务端可以预置有应用程序管理数据库，所述应用程序管理数据库与所述参考数据库中可以均包括多个应用程序的特征文件，以及对应的安全属性；

[0148] 所述安全属性可以包括不可执行的黑文件和可执行的白文件。

[0149] 在本发明的一种优选的实施例中，可以通过以下模块预置所述参考数据库：

[0150] 下载模块，适于访问第二服务端，下载所述参考数据库；

[0151] 保存模块，适于将所述参考数据库保存在第一服务端；

[0152] 所述参考数据库通过离线下载的方式进行更新。

[0153] 本发明实施例中，所述装置还可以包括：

[0154] 应用程序处理模块，适于依据所述安全属性查找所述应用程序的安装文件，或将所述安全属性返回终端，由终端依据所述安全属性加载所述应用程序。

[0155] 在本发明的一种优选的实施例中，所述终端可以通过以下模块获取应用程序的特征文件：

[0156] 应用程序文件提取模块，适于扫描终端所有应用程序对应的所有文件，提取出其中的应用程序文件；

[0157] 第一转换模块，适于采用预设算法将所述应用程序文件转换为对应的程序特征文件。

[0158] 相应的，所述装置还可以包括：

[0159] 数据库构建模块，适于依据各个应用程序的特征文件与可安全属性的对应关系，构建第一服务端的应用程序管理数据库。

[0160] 在本发明的另一种优选的实施例中，所述终端可以通过以下模块获取应用程序的特征文件：

[0161] 请求接收模块，适于接收用户访问应用程序的请求；

[0162] 第二转换模块，适于依据所述请求提取对应的应用程序文件，并采用预设算法将所述应用程序文件转换为对应的程序特征文件。

[0163] 相应的，所述装置还可以包括：

[0164] 添加模块，适于将各个应用程序的特征文件与可安全属性的对应关系添加到第一服务端的应用程序管理数据库中。

[0165] 在具体的实现中，第一服务端上可以部署有应用程序管理数据库，所述应用程序管理数据库可以保存有多个应用程序的特征文件，以及对应的安全属性；

[0166] 所述装置还可以包括：

[0167] 搜索模块，适于在第一服务端的应用程序管理数据库搜索是否存在所述应用程序的特征文件，若否，则执行判断当前是否可以连接第二服务端的步骤。

[0168] 在对应用程序进行识别后，还可以依据识别结果生成相应的提示信息，用于终端进行进一步的操作，具体的，所述装置还可以包括：

[0169] 第一提示信息返回模块，适于若所述应用程序文件的安全属性为黑文件，则生成不可执行的提示信息并返回给终端，终端接收提示信息后不加载所述应用程序；

[0170] 第二提示信息返回模块，适于若所述应用程序文件的安全属性为白文件，则生成可执行的提示信息并返回给终端，终端接收提示信息后开始加载所述应用程序。

[0171] 在本发明的一种优选的实施例中，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。

[0172] 对于上述装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见图 1 所示方法实施例的部分说明即可。

[0173] 本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

[0174] 本领域技术人员易于想到的是：上述各个实施例的任意组合应用都是可行的，故上述各个实施例之间的任意组合都是本申请的实施方案，但是由于篇幅限制，本说明书在此就不一一详述了。

[0175] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0176] 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。

[0177] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0178] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和／或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0179] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0180] 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应用程序安全属性的识别设备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。

[0181] 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。

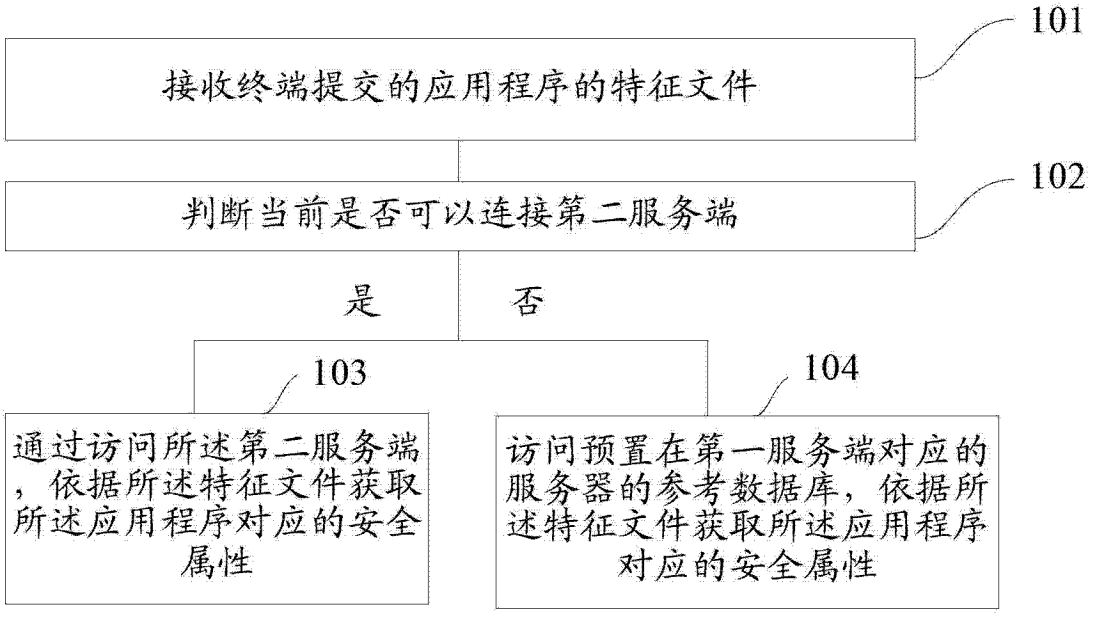
101
接收终端提交的应用程序的特征文件
102
判断当前是否可以连接第二服务端
是
否
103
通过访问所述第二服务端，依据所述特征文件获取所述应用程序对应的安全属性
104
访问预置在第一服务端对应的服务器的参考数据库，依据所述特征文件获取所述应用程序对应的安全属性

图 1


特征文件接收模块201
判断模块202
第二服务端识别模块203
参考数据库识别模块204

图 2