(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115146309 A
(43)申请公布日 2022.10.04

(21)申请号 202210740251.8

(22)申请日 2022.06.27

(71)申请人 京东科技信息技术有限公司
地址 100176 北京市大兴区经济技术开发区科创十一街18号院2号楼6层601

(72)发明人 刘一鑫 曹炜

(74)专利代理机构 北京品源专利代理有限公司 11332
专利代理师 孔凡红

(51)Int.Cl.
G06F 21/62(2013.01)

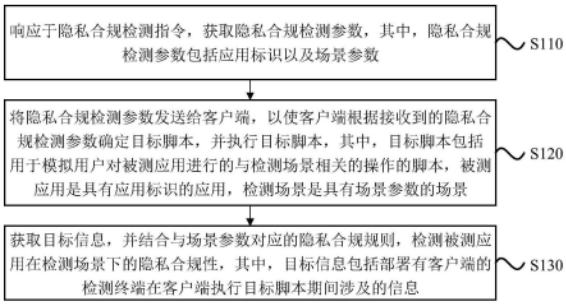
权利要求书3页 说明书14页 附图3页

(54)发明名称

隐私合规检测方法、装置、服务器、终端及存储介质

(57)摘要

本发明实施例公开了一种隐私合规检测方法、装置、服务器、终端及存储介质。应用于客户端的方法,可以包括:响应于隐私合规检测指令,获取包括被测应用的应用标识以及检测场景的场景参数的隐私合规检测参数;将隐私合规检测参数发送给客户端,以使客户端根据接收的隐私合规检测参数确定目标脚本,执行目标脚本,该目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本;获取目标信息,结合与场景参数对应的隐私合规规则,检测被测应用在检测场景下的隐私合规性,其中目标信息包括部署有客户端的检测终端在客户端执行目标脚本期间涉及的信息。本发明实施例的技术方案,可以自动化检测被测应用在检测场景下的隐私合规性。



CN 115146309 A

1.一种隐私合规检测方法,其特征在于,应用于服务端,所述方法包括:

响应于隐私合规检测指令,获取隐私合规检测参数,其中,所述隐私合规检测参数包括应用标识以及场景参数;

将所述隐私合规检测参数发送给客户端,以使所述客户端根据接收的所述隐私合规检测参数确定目标脚本,并执行所述目标脚本,其中,所述目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本,所述被测应用是具有所述应用标识的应用,所述检测场景是具有所述场景参数的场景;

获取目标信息,并结合与所述场景参数对应的隐私合规规则,检测所述被测应用在所述检测场景下的隐私合规性,其中,所述目标信息包括部署有所述客户端的检测终端在所述客户端执行所述目标脚本期间涉及的信息。

2.根据权利要求1所述的方法,其特征在于,所述获取目标信息,包括:

拦截所述检测终端在所述客户端执行所述目标脚本期间传输的传输信息,并将所述传输信息转发给待接收所述传输信息的接收设备;和/或,

拦截所述检测终端在所述客户端执行所述目标脚本期间待获取的获取信息,并将所述获取信息转发给所述检测终端;

将拦截到的所述传输信息和/或所述获取信息作为目标信息。

3.根据权利要求2所述的方法,其特征在于,所述隐私合规检测参数还包括用于定位部署有所述服务端的检测服务器上开启的代理端口的参数代理地址;

在所述将所述隐私合规检测参数发送给客户端之后,还包括:以使所述客户端将所述检测终端的终端系统代理,配置为接收的所述参数代理地址;

相应的,所述拦截所述检测终端在所述客户端执行所述目标脚本期间传输的传输信息,包括:基于所述代理端口,拦截所述检测终端在所述客户端执行所述目标脚本期间传输的传输信息;

所述拦截所述检测终端在所述客户端执行所述目标脚本期间待获取的获取信息,包括:基于所述代理端口,拦截所述检测终端在所述客户端执行所述目标脚本期间待获取的获取信息。

4.根据权利要求1所述的方法,其特征在于,所述目标信息包括所述检测终端在所述客户端执行所述目标脚本期间传输的传输信息和/或获取到的获取信息,所述隐私合规规则包括与获取或传输的用户隐私信息未存在于预先设置的隐私政策中时,所述被测应用在所述检测场景下隐私合规相关的规则;

所述结合与所述场景参数对应的隐私合规规则,检测所述被测应用在所述检测场景下的隐私合规性,包括:

确定所述目标信息中的所述用户隐私信息,并根据所述用户隐私信息是否存在于所述隐私政策中,检测所述被测应用在所述检测场景下的隐私合规性。

5.根据权利要求1所述的方法,其特征在于,所述检测终端是连接在终端管理服务器上的各候选终端中的一台,每台所述候选终端内均预先配置有隐私合规检测环境,在所述响应于隐私合规检测指令之后,还包括:

从与所述终端管理服务器连接的各所述候选终端中确定所述检测终端;

所述将所述隐私合规检测参数发送给客户端,包括:

将所述隐私合规检测参数发送给预先部署在所述检测终端上的客户端。

6.一种隐私合规检测方法,其特征在于,应用于客户端,所述方法包括:

接收服务端发送的隐私合规检测参数,其中,所述隐私合规检测参数包括应用标识以及场景参数;

根据接收到的所述隐私合规检测参数确定目标脚本,并执行所述目标脚本,以使所述服务端获取到目标信息,并结合与所述场景参数对应的隐私合规规则,检测被测应用在检测场景下的隐私合规性;

其中,所述目标脚本包括用于模拟用户对所述被测应用进行的与所述检测场景相关的操作的脚本,所述被测应用是具有所述应用标识的应用,所述检测场景是具有所述场景参数的场景,所述目标信息包括部署有所述客户端的检测终端在所述客户端执行所述目标脚本期间涉及的信息。

7.根据权利要求6所述的方法,其特征在于,还包括:

获取函数调用信息,其中,所述函数调用信息是安装在所述检测终端上的所述被测应用在所述客户端执行所述目标脚本期间调用的目标函数的标识信息;

获取预先设置的敏感函数库,并确定与所述函数调用信息对应的所述目标函数是否存在于所述敏感函数库中;

如果是,则将所述函数调用信息作为所述目标信息,发送给所述服务端。

8.根据权利要求7所述的方法,其特征在于,所述获取函数调用信息包括:

接收基于广播方式发送的函数调用信息,其中,所述函数调用信息是基于注册在所述被测应用所在的进程中的钩子脚本获取后发送的信息。

9.根据权利要求6所述的方法,其特征在于,所述隐私合规检测参数还包括所述被测应用的应用安装包在存储服务器中的存储地址;

在所述接收服务端发送的隐私合规检测参数之后,还包括:

根据接收到的所述应用标识确定所述检测终端上是否安装有所述被测应用;

如果是,则卸载安装在所述检测终端上的所述被测应用;

基于接收到的所述存储地址从所述存储服务器上下载所述应用安装包,并将已下载的所述应用安装包安装在所述检测终端上。

10.一种隐私合规检测装置,其特征在于,配置于服务端,所述装置包括:

隐私合规检测参数获取模块,用于响应于隐私合规检测指令,获取隐私合规检测参数,其中,所述隐私合规检测参数包括应用标识以及场景参数;

目标脚本第一执行模块,用于将所述隐私合规检测参数发送给客户端,以使所述客户端根据接收的所述隐私合规检测参数确定目标脚本,并执行所述目标脚本,其中,所述目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本,所述被测应用是具有所述应用标识的应用,所述检测场景是具有所述场景参数的场景;

隐私合规检测模块,用于获取目标信息,并结合与所述场景参数对应的隐私合规规则,检测所述被测应用在所述检测场景下的隐私合规性,其中,所述目标信息包括部署有所述客户端的检测终端在所述客户端执行所述目标脚本期间涉及的信息。

11.一种隐私合规检测装置,其特征在于,配置于客户端,所述装置包括:

隐私合规检测参数接收模块,用于接收服务端发送的隐私合规检测参数,其中,所述隐

私合规检测参数包括应用标识以及场景参数；

目标脚本第二执行模块，用于根据接收到的所述隐私合规检测参数确定目标脚本，并执行所述目标脚本，以使所述服务端获取到目标信息，结合与所述场景参数对应的隐私合规规则，检测被测应用在检测场景下的隐私合规性；

其中，所述目标脚本包括用于模拟用户对所述被测应用进行的与所述检测场景相关的操作的脚本，所述被测应用是具有所述应用标识的应用，所述检测场景是具有所述场景参数的场景，所述目标信息包括部署有所述客户端的检测终端在所述客户端执行所述目标脚本期间涉及的信息。

12.一种检测服务器，其特征在于，包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的计算机程序，所述计算机程序被所述至少一个处理器执行，以使所述至少一个处理器执行如权利要求1-5中任一项所述的隐私合规检测方法。

13.一种检测终端，其特征在于，包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的计算机程序，所述计算机程序被所述至少一个处理器执行，以使所述至少一个处理器执行如权利要求6-9中任一项所述的隐私合规检测方法。

14.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有计算机指令，所述计算机指令用于使处理器执行时实现如权利要求1-9中任一所述的隐私合规检测方法。

隐私合规检测方法、装置、服务器、终端及存储介质

技术领域

[0001] 本发明实施例涉及计算机应用技术领域，尤其涉及一种隐私合规检测方法、装置、服务器、终端及存储介质。

背景技术

[0002] 某应用程序(Application,APP)的隐私合规检测过程可以理解为检测该APP在运行过程中的获取或传输的信息是否符合相关的隐私合规政策的过程。目前，主要是通过人工方式实现APP隐私合规的检测。

[0003] 在实现本发明的过程中，发明人发现现有技术中存在以下技术问题：检测效率低下、检测准确度难以保证和检测成本较高。

发明内容

[0004] 本发明实施例提供了一种隐私合规检测方法、装置、服务器、终端及存储介质，通过对被测应用在检测场景下的隐私合规的自动化检测的方式，解决了人工检测中存在的检测效率低下、检测准确度难以保证和检测成本较高的问题。

[0005] 根据本发明的一方面，提供了一种隐私合规检测方法，应用于服务端，可包括：

[0006] 响应于隐私合规检测指令，获取隐私合规检测参数，其中，隐私合规检测参数包括应用标识以及场景参数；

[0007] 将隐私合规检测参数发送给客户端，以使客户端根据接收的隐私合规检测参数确定目标脚本，并执行目标脚本，其中，目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，被测应用是具有应用标识的应用，检测场景是具有场景参数的场景；

[0008] 获取目标信息，并结合与场景参数对应的隐私合规规则，检测被测应用在检测场景下的隐私合规性，其中，目标信息包括部署有客户端的检测终端在客户端执行目标脚本期间涉及的信息。

[0009] 根据本发明的另一方面，提供了一种隐私合规检测方法，应用于客户端，可以包括：

[0010] 接收服务端发送的隐私合规检测参数，其中，隐私合规检测参数包括应用标识以及场景参数；

[0011] 根据接收到的隐私合规检测参数确定目标脚本，执行目标脚本，以使服务端获取到目标信息，并结合与场景参数对应的隐私合规规则，检测被测应用在检测场景下的隐私合规性；

[0012] 其中，目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，被测应用是具有应用标识的应用，检测场景是具有场景参数的场景，目标信息包括部署有客户端的检测终端在客户端执行目标脚本期间涉及的信息。

[0013] 根据本发明的另一方面，提供了一种隐私合规检测装置，配置于服务端，可以包

括：

[0014] 隐私合规检测参数获取模块，用于响应于隐私合规检测指令，获取隐私合规检测参数，其中，隐私合规检测参数包括应用标识以及场景参数；

[0015] 目标脚本第一执行模块，用于将隐私合规检测参数发送给客户端，以使客户端根据接收的隐私合规检测参数确定目标脚本，执行目标脚本，其中，目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，被测应用是具有应用标识的应用，检测场景是具有场景参数的场景；

[0016] 隐私合规检测模块，用于获取目标信息，并结合与场景参数对应的隐私合规规则，检测被测应用在检测场景下的隐私合规性，其中，目标信息包括部署有客户端的检测终端在客户端执行目标脚本期间涉及的信息。

[0017] 根据本发明的另一方面，提供了一种隐私合规检测装置，配置于客户端，可以包括：

[0018] 隐私合规检测参数接收模块，用于接收服务端发送的隐私合规检测参数，其中，隐私合规检测参数包括应用标识以及场景参数；

[0019] 目标脚本第二执行模块，用于根据接收的隐私合规检测参数确定目标脚本，并执行目标脚本，以使服务端获取到目标信息，结合与场景参数对应的隐私合规规则，检测被测应用在检测场景下的隐私合规性；

[0020] 其中，目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，被测应用是具有应用标识的应用，检测场景是具有场景参数的场景，目标信息包括部署有客户端的检测终端在客户端执行目标脚本期间涉及的信息。

[0021] 根据本发明的另一方面，提供了一种检测服务器，可以包括：

[0022] 至少一个处理器；以及

[0023] 与至少一个处理器通信连接的存储器；其中，

[0024] 存储器存储有可被至少一个处理器执行的计算机程序，计算机程序被至少一个处理器执行，以使至少一个处理器执行时实现本发明任意实施例所提供的应用于服务端的隐私合规检测方法。

[0025] 根据本发明的另一方面，提供了一种检测终端，可以包括：

[0026] 至少一个处理器；以及

[0027] 与至少一个处理器通信连接的存储器；其中，

[0028] 存储器存储有可被至少一个处理器执行的计算机程序，计算机程序被至少一个处理器执行，以使至少一个处理器执行时实现本发明任意实施例所提供的应用于客户端的隐私合规检测方法。

[0029] 根据本发明的另一方面，提供了一种计算机可读存储介质，其上存储有计算机指令，该计算机指令用于使处理器执行时实现本发明任意实施例所提供的隐私合规检测方法。

[0030] 本发明实施例中的技术方案，服务端通过响应于隐私合规检测指令，获取包括被测应用的应用标识和检测场景的场景参数的隐私合规检测参数，该隐私合规检测参数可以体现出是对什么应用在什么场景下的隐私合规性进行检测；进而，将隐私合规检测参数发送给客户端，以使客户端根据接收到的隐私合规检测参数确定目标脚本，并执行目标脚本，

该目标脚本是用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，由此实现了自动化模拟检测场景的效果；然后，获取部署有客户端的检测终端在客户端执行目标脚本期间涉及的目标信息，并结合与场景参数对应的预先设置的隐私合规规则，检测被测应用在检测场景下的隐私合规性，由此实现了自动化判断隐私合规性的效果。上述技术方案，可以自动化检测被测应用在检测场景下的隐私合规性，由此提高了检测效率、保证了检测准确性并且降低了检测成本。

[0031] 应当理解，本部分所描述的内容并非旨在标识本发明的实施例的关键或是重要特征，也不用于限制本发明的范围。本发明的其它特征将通过以下的说明书而变得容易理解。

附图说明

[0032] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0033] 图1是根据本发明实施例提供的一种隐私合规检测方法的流程图；

[0034] 图2是根据本发明实施例提供的另一种隐私合规检测方法的流程图；

[0035] 图3是根据本发明实施例提供的另一种隐私合规检测方法的时序图；

[0036] 图4是根据本发明实施例提供的一种隐私合规检测装置的结构框图；

[0037] 图5是根据本发明实施例提供的另一种隐私合规检测装置的结构框图；

[0038] 图6是实现本发明实施例的隐私合规检测方法的检测服务器或是检测终端的结构示意图。

具体实施方式

[0039] 为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

[0040] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“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。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。“目标”、“原始”等的情况类似，在此不再赘述。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0041] 图1是本发明实施例中提供的一种隐私合规检测方法的流程图。本实施例可适用于自动化检测被测应用在检测场景下的隐私合规性的情况。该方法可以由本发明实施例提供的隐私合规检测装置来执行，该装置可以由软件和/或硬件的方式实现，该装置可以集成在检测服务器上。

[0042] 参见图1,本发明实施例的方法具体包括如下步骤:

[0043] S110、响应于隐私合规检测指令,获取隐私合规检测参数,其中,隐私合规检测参数包括应用标识以及场景参数。

[0044] 其中,隐私合规检测指令可以包括用于检测被测应用在检测场景下的隐私合规性的指令,响应于该隐私合规检测指令,获取隐私合规检测参数,该隐私合规检测参数可以包括应用标识以及场景参数,该应用标识可以是被测应用的标识,该场景参数可以是检测场景的参数,由此通过该隐私合规检测参数可以确定是对什么应用在什么场景下的隐私合规性进行检测。

[0045] 在实际应用中,可选的,隐私合规检测指令可以在如下情况下获取:针对于与服务端对应的前端,用户可以在前端显示的前端页面上选择被测应用(或上传被测应用的应用安装包)和检测场景,并在点击检测选项后,服务端接收到前端触发的隐私合规检测指令。可选的,应用标识可以是应用安装包的包名,具体来说可以是对用户上传的应用安装包的包名进行反编译后得到的被测应用在检测终端(即安装有被测应用的终端)的运行系统下的包名。再可选的,当运行系统是安卓(Android)系统时,服务端可以将获取到的隐私合规检测参数封装为Android调试桥(Android Debug Bridge,adb)命令进行应用,即将adb命令作为隐私合规检测参数进行应用,这非常适合于自动化检测的应用场景。

[0046] S120、将隐私合规检测参数发送给客户端,以使客户端根据接收到的隐私合规检测参数确定目标脚本,并执行目标脚本,其中,目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本,被测应用是具有应用标识的应用,检测场景是具有场景参数的场景。

[0047] 其中,将隐私合规检测参数发送给客户端,以使客户端根据接收到的隐私合规检测参数确定服务端需要对什么应用在什么场景下的隐私合规性进行检测,进而确定自身需要模拟用户对什么应用进行与什么场景有关的操作。具体的,由于客户端接收到的隐私合规检测参数包括应用标识和场景参数,因此其由此确定出的目标脚本可以包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本,进而通过执行该目标脚本来模拟用户进行上述操作的过程,由此实现了根据检测场景自动化操作被测应用的效果。

[0048] 示例性的,检测场景可以是同意隐私政策前不可获取或传输用户隐私信息(即用户个人信息);被测应用未向用户告知且未经用户同意,频繁自启动;同意隐私政策后,不可使用隐私政策中未声明的用户个人信息;等等。模拟的操作可以是同意隐私政策前、点击同意隐私政策、用户登录、开关推送等按钮、复制粘贴文本、输入用户个人信息等。具体的,如果检测场景是同意隐私政策前不可获取或传输用户个人信息,那么模拟的操作可以是操作被测应用,直至在根据应用页面元素判断出现同意按钮时结束;如果检测场景是同意隐私政策后,不可使用隐私政策中未声明的用户个人信息,那么模拟的操作可以是查找隐私政策页面的同意按钮,对其进行点击;如果被测应用未向用户告知且未经用户同意,频繁自启动,那么模拟的操作可以是在启动被测应用后,杀死被测应用的进程;等等。

[0049] S130、获取目标信息,并结合与场景参数对应的隐私合规规则,检测被测应用在检测场景下的隐私合规性,其中,目标信息包括部署有客户端的检测终端在客户端执行目标脚本期间涉及的信息。

[0050] 其中,获取目标信息,该目标信息可以是部署有客户端的检测终端(亦是部署有被

测应用的检测终端)在客户端执行目标脚本期间涉及的信息,如检测终端向外传输的传输信息、获取得到的获取信息、其中的被测应用调用的目标函数的函数调用信息等,在此未做具体限定。实际应用中,可选的,传输信息和/或获取信息可能是被测应用涉及的信息,也可能是检测终端内除被测应用之外的其余应用涉及的信息,在此未做具体限定。隐私合规规则可以是用于表示目标信息满足什么条件时,被测应用在检测场景下具有或是未具有隐私合规性的规则,如与获取或传输的用户隐私信息未存在于预先设置的隐私政策中时,被测应用在检测场景下隐私合规相关的规则;与目标函数未存在于预先设置的敏感函数库中时,被测应用在检测场景下隐私合规相关的规则;等等。因此,可以根据目标信息和隐私合规规则,实现被测应用在检测场景中的隐私合规性的自动化检测的效果。

[0051] 需要说明的是,上述技术方案,一方面,通过自动化模拟在检测场景下的隐私合规性的自动检测的效果。检测场景(即自动化模拟用户对于被测应用进行的与检测场景有关的操作),然后根据由此获取的目标信息自动化判断被测应用在检测场景下的隐私合规性,由此提高了检测效率并且降低了检测成本。另一方面,虽然现有隐私合规政策复杂繁多,晦涩难懂,而且检测机构对于隐私合规政策的解读力度更新速度较快(如有时严格一些,有时松弛一些),但通过基于隐私合规政策预先设置隐私合规规则的方式,可以在检测过程中及时并且自动地应用最新的隐私合规政策,由此保证了检测效率和检测准确性。除此外,通过被测应用在运行过程中获取的目标信息进行自动化检测,这种动态检测方式亦有效保证了检测准确性。

[0052] 本发明实施例中的技术方案,服务端通过响应于隐私合规检测指令,获取包括被测应用的应用标识和检测场景的场景参数的隐私合规检测参数,该隐私合规检测参数可以体现出是对什么应用在什么场景下的隐私合规性进行检测;进而,将隐私合规检测参数发送给客户端,以使客户端根据接收到的隐私合规检测参数确定目标脚本,并执行目标脚本,该目标脚本是用于模拟用户对被测应用进行的与检测场景相关的操作的脚本,由此实现了自动化模拟检测场景的效果;然后,获取部署有客户端的检测终端在客户端执行目标脚本期间涉及的目标信息,并结合与场景参数对应的预先设置的隐私合规规则,检测被测应用在检测场景下的隐私合规性,由此实现了自动化判断隐私合规性的效果。上述技术方案,可以自动化检测被测应用在检测场景下的隐私合规性,由此提高了检测效率、保证了检测准确性并且降低了检测成本。

[0053] 一种可选的技术方案,获取目标信息,可以包括:拦截检测终端在客户端执行目标脚本期间传输的传输信息,将传输信息转发给待接收传输信息的接收设备;和/或,拦截检测终端在客户端执行目标脚本期间待获取的获取信息,将获取信息转发给检测终端;将拦截到的传输信息和/或获取信息作为目标信息。其中,检测终端在客户端执行目标脚本期间传输的传输信息和/或获取的获取信息均是检测被测应用的隐私合规性的重要依据,因此服务端可以拦截这些信息,并将拦截到的这些信息作为目标信息。需要说明的是,服务端拦截到目标信息后,这意味着本来待接收目标信息的接收设备和/或检测终端将无法接收到目标信息,影响了被测应用的有效运行。因此,当服务端拦截到传输信息后,可以将该传输信息转发给相应的接收设备,由此实现了检测终端和接收设备之间的信息交互过程;当服务端拦截到获取信息后,可将该获取信息转发给检测终端,由此实现了检测终端和发送该获取信息的发送设备间的信息交互过程。在此基础上,可选的,接收设备和发送设备均可以

是与被测应用对应的应用服务器;再可选的,服务端拦截到的目标信息可能是加密信息,如HTTPS加密信息,其中可能包括用户个人信息,具体说可以是IMEI、ip、mac地址等,因此在拦截到加密信息后,可以对其进行解密,将解密结果作为隐私合规性检测的依据,并将解密前(即拦截到)的目标信息进行转发。上述技术方案,即保证了服务端可以拦截到用于隐私合规性检测的目标信息,又不会影响到被测应用的有效运行,需要说明的,被测应用的有效运行亦是隐私合规性检测实现的重要前提。

[0054] 在此基础上,可选的,隐私合规检测参数还包括用于定位部署有服务端的检测服务器上开启的代理端口的参数代理地址,在将隐私合规检测参数发送给客户端之后,上述隐私合规检测方法,还可以包括:以使客户端将检测终端的终端系统代理,配置为接收的参数代理地址;拦截检测终端在客户端执行目标脚本期间传输的传输信息,可以包括:基于代理端口,拦截检测终端在客户端执行目标脚本期间传输的传输信息;拦截检测终端在客户端执行目标脚本期间待获取的获取信息,可包括:基于代理端口,拦截检测终端在客户端执行目标脚本期间待获取的获取信息。其中,代理端口可以是检测服务器上开启的用于实现代理功能的端口,如检测服务器上开启的中间人代理(mitmproxy)的端口。参数代理地址可以是用于定位检测服务器上的代理端口的地址,在实际应用中,可选的,其可以包括检测服务器的网际协议地址(Internet Protocol Address,IP)以及代理端口的端口地址,由此可以唯一定位到这个检测服务器上的这个代理端口。当参数代理地址作为隐私合规检测参数中的一部分发送给客户端之后,客户端可以将检测终端的终端系统代理配置为参数代理地址,由此代理端口和检测终端关联在一起,从而服务端可以基于代理端口拦截到传输信息和/或获取信息,由此实现了服务器代理拦截传输信息和/或获取信息的自动化。

[0055] 另一种可选的技术方案,目标信息包括检测终端在客户端执行目标脚本期间传输的传输信息和/或获取到的获取信息,隐私合规规则包括与获取或传输的用户隐私信息未存在于预先设置的隐私政策中时,被测应用在检测场景下隐私合规相关的规则;结合与场景参数对应的隐私合规规则,检测被测应用在检测场景下的隐私合规性,可以包括:确定目标信息中的用户隐私信息,并根据用户隐私信息是否存在于隐私政策中,检测被测应用在检测场景下的隐私合规性。其中,与上述隐私合规规则匹配的检测场景可以是同意隐私政策后,不可使用隐私政策中未声明的用户隐私信息,因此可以通过确定目标信息中的用户隐私信息,并根据用户隐私信息是否存在于隐私政策中,检测被测应用在检测场景下的隐私合规性。例如,当用户隐私信息存在于隐私政策中(即与隐私政策中声明使用的用户隐私信息相匹配)时,被测应用在检测场景下具备隐私合规性;否则,其不具备隐私合规性。上述技术方案,可以准确检测隐私合规性。

[0056] 另一种可选的技术方案,检测终端是连接在终端管理服务器上的各候选终端中的一台,每台候选终端内均预先配置有隐私合规检测环境,在响应于隐私合规检测指令之后,上述隐私合规检测方法,还可包括:从与终端管理服务器连接的各候选终端中确定检测终端;将隐私合规检测参数发送给客户端,包括:将隐私合规检测参数发送给预先部署在检测终端上的客户端。其中,为了部署在检测终端上的客户端可以实现上述任一的隐私合规检测过程,该检测终端内需预先配置有隐私合规检测环境,如root环境、xposed框架、system分区解锁、证书安装等,该隐私合规检测环境的配置过程较为耗时,而且需要具备一定的技术专业背景,门槛较高。在此基础上,为了降低隐私合规检测的实现难度并且提高其的实现

效率，可以预先准备有至少两台已配置有隐私合规检测环境的候选终端，并将各候选终端连接在终端管理服务器上(如通过数据线进行连接)，以使这些候选终端可以被终端管理服务器发现。由此，服务端响应于隐私合规检测指令，可以从与终端管理服务器连接的各候选终端中确定检测终端，然后将隐私合规检测参数发送给预先部署在检测终端上的客户端。这样一来，用户在进行检测前，无需自己配置隐私合规检测环境，可以直接应用已配置好隐私合规检测环境的候选终端，从而解决了隐私合规检测的实现难度大且实现效率低的问题。实际应用中，可选的，候选终端可以是虚拟终端(如虚拟机)，也可以是实际终端(即真机)，在此未做具体限定。再可选的，由于各候选终端均连接在终端管理服务器上，因此候选终端也可以称为云终端，这是一种云端控制方式，可以大幅提升动态检测能力。

[0057] 图2是本发明实施例中提供的另一种隐私合规检测方法的流程图。本实施例可已适用于自动化检测被测应用在检测场景下的隐私合规性的情况。该方法可以由本发明实施例提供的隐私合规检测装置来执行，该装置可以由软件和/或硬件的方式实现，该装置可以集成在检测终端上。

[0058] 参见图2，本实施例的方法具体可以包括如下步骤：

[0059] S210、接收服务端发送的隐私合规检测参数，其中，隐私合规检测参数包括应用标识以及场景参数。

[0060] 其中，客户端接收服务端发送的隐私合规检测参数，该隐私合规检测参数可以包括应用标识以及场景参数，该应用标识可以是被测应用的标识，该场景参数可以是检测场景的参数，这意味着客户端根据接收到的隐私合规检测参数可以确定服务端是对什么应用在什么场景下的隐私合规性进行检测，进而确定自身需要模拟用户对什么应用进行与什么场景有关的操作。

[0061] S220、根据接收到的隐私合规检测参数确定目标脚本，并执行目标脚本，以使服务端获取到目标信息，并结合与场景参数对应的隐私合规规则，检测被测应用在检测场景下的隐私合规性，其中，目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，被测应用是具有应用标识的应用，检测场景是具有场景参数的场景，目标信息包括部署有客户端的检测终端在客户端执行目标脚本期间涉及的信息。

[0062] 其中，由于客户端接收到的隐私合规检测参数包括应用标识和场景参数，因此其由此确定出的目标脚本可以包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，进而通过执行该目标脚本来模拟用户进行上述操作的过程，由此实现了根据检测场景自动化操作被测应用的效果。进一步，服务端可以获取到检测终端在客户端执行目标脚本期间涉及的目标信息，从而结合与场景参数对应的隐私合规规则，可以实现被测应用在检测场景中的隐私合规性的自动化检测的效果。

[0063] 本发明实施例中的技术方案，客户端通过接收服务端发送的包括被测应用的应用标识和检测场景的场景参数的隐私合规检测参数，该隐私合规检测参数可以体现出服务端需对什么应用在什么场景下的隐私合规性进行检测；进而，根据接收到的隐私合规检测参数确定目标脚本，并执行目标脚本，该目标脚本是用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，由此实现了自动化模拟检测场景的效果，这样一来，服务端可以获取到部署有该客户端的检测终端在客户端执行目标脚本期间涉及的目标信息，并结合与场景参数对应的预先设置的隐私合规规则，检测被测应用在检测场景下的隐私合规性，由此

实现了自动化判断隐私合规性的效果。上述技术方案，实现了被测应用在检测场景下的隐私合规性的自动化检测，由此提高了检测效率、保证了检测准确性并且降低了检测成本。

[0064] 一种可选的技术方案，上述隐私合规检测方法，还可包括：获取函数调用信息，其中，函数调用信息是安装在检测终端上的被测应用在客户端执行目标脚本期间调用的目标函数的标识信息；获取预先设置的敏感函数库，并确定与函数调用信息对应的目标函数是否存在于敏感函数库中；如果是，则将函数调用信息作为目标信息，发送给服务端。其中，函数调用信息可以表示出安装在检测终端上的被测应用在客户端执行目标脚本期间调用了什么函数(这里称为目标函数)，敏感函数库可以是预先设置的用于存储敏感函数的库，该敏感函数可以理解为用于获取或是传输用户隐私信息的函数。客户端获取函数调用信息后，可以将与其对应的目标函数与存储在敏感数据库中的敏感函数进行对比，如果目标函数是敏感函数，则可以将函数调用信息作为目标信息发送给服务端。这样一来，当隐私合规规则是与目标函数未存在于敏感函数库中时，被测应用在检测场景下隐私合规相关的规则时，这时的检测场景可以是同意隐私政策前不可获取或传输用户隐私信息，服务端根据获取的目标信息可以确定被测应用调用了敏感函数，那么由此可以确定被测应用在检测场景下未具备隐私合规性，由此实现了隐私合规性的准确检测的效果。在实际应用中，可选的，上述敏感函数库可以通过如下方式中的至少一种进行收集：通过爬虫从官方网站获取用于收集用户隐私信息的函数、通过用户线上反馈机制收集、及通过对监管机构公布的隐私合规政策进行解读分析后收集等。

[0065] 在此基础上，可选的，获取函数调用信息，可以包括：接收基于广播方式发送的函数调用信息，其中，函数调用信息是基于注册在被测应用所在的进程中的钩子脚本获取后发送的信息。其中，钩子脚本可以是与钩子(Hook)函数相关的脚本，钩子函数实际上是一个处理消息的程序段，通过终端系统的调用，可以将其挂到终端系统。钩子脚本被预先注册在被测应用所在的进程中，这样才能基于钩子脚本获取到函数调用信息，但是这也意味着钩子脚本所在的进程与客户端所在的进程并非是同一个进程，而两个不同进程间无法直接进行信息交互。因此，基于钩子脚本获取到的函数调用信息可以通过广播方式进行发送，由此客户端所在的进程可以基于reciever接收到该函数调用信息，由此实现了函数调用信息的有效接收的效果。

[0066] 另一可选的技术方案，隐私合规检测参数还包括被测应用的应用安装包在存储服务器中的存储地址，在接收服务端发送的隐私合规检测参数之后，上述隐私合规检测方法，还可以包括：根据接收到的应用标识确定检测终端上是否安装有被测应用；如果是，则卸载安装在检测终端上的被测应用；基于接收到的存储地址从存储服务器上下载应用安装包，并将已下载的应用安装包安装在检测终端上。其中，考虑到本发明实施例可能涉及到的应用场景，被测应用在首次运行时，可能是需要将一些应用信息存储到某应用文件中。那么，当检测场景与应用信息和/或应用文件有关时，被测应用在被检测前，不能发生过运行，以保证其在检测过程中是首次运行。为此，客户端在接收到应用标识后，可以确定检测终端上是否安装有与其对应的被测应用；如果是(这说明被测试应用很可能已被运行过)，则卸载安装在检测终端上的被测应用，并基于接收到的存储地址从存储服务器上下载被测应用的应用安装包，然后将已下载的应用安装包安装在检测终端上，由此保证了检测过程中运行的被测应用是首次运行。在此基础上，可选的，用于存储应用安装包的存储服务器和检测服

务器可以是相同或不同的服务器，在此未做具体限定。当二者不同时，服务端可以从存储服务器中获取到应用安装包在存储服务器中的存储地址。再可选的，终端系统是Android系统时，上述应用安装包可以称为APK(Android Application Package)，这是专为在平台上分发Android应用程序而设计的文件格式。

[0067] 图3是本发明实施例中提供的另一种隐私合规检测方法的时序图。本实施例以上述各技术方案为基础进行优化。其中，与上述各实施例相同或是相应的术语的解释在此不再赘述。

[0068] 参见图3，本实施例的方法具体可以包括如下步骤：

[0069] S1、服务端响应于隐私合规检测指令，获取隐私合规检测参数，其中隐私合规检测参数包括被测应用的应用包名、检测场景的场景参数、用于定位部署有服务端的检测服务器上开启的代理端口的参数代理地址、及被测应用的apk在检测服务器中的存储地址。

[0070] 其中，针对于与服务端对应的前端，用户可以通过前端显示的前端页面将apk上传到存储服务器上，并选择检测场景，然后点击检测控件。由此，服务端可以接收到前端触发的隐私合规检测指令，自动检测过程启动。

[0071] S2、服务端从连接在终端管理服务器上的各候选终端中确定检测终端，并根据隐私合规检测参数生成adb命令，将adb命令发送给预先部署在检测终端上的客户端，其中，每台候选终端内均预先配置有隐私合规检测环境。

[0072] S3、客户端通过预先设置的接口接收到adb命令，并从adb命令中获取到隐私合规检测参数。

[0073] S4、客户端根据应用包名确定检测终端上是否安装有被测应用，如果是，则将安装在检测终端上的被测应用进行卸载，并基于存储地址从检测服务器上下载apk，将已下载的apk安装在检测终端上。

[0074] S5、客户端将检测终端的终端系统代理配置为参数代理地址，然后启动已安装的被测应用，启动钩子脚本，其中，钩子脚本包括注册在被测应用所在的进程中的用于获取被测应用在客户端执行目标脚本期间调用的目标函数的函数调用信息，该函数调用信息通过广播方式向外发送。

[0075] S6、客户端根据应用包名和场景参数确定目标脚本，并执行目标脚本，其中，目标脚本是用于模拟用户对被测应用进行的与检测场景相关的操作的脚本。

[0076] S7、客户端接收基于广播方式发送的函数调用信息。

[0077] S8、客户端获取预先设置的敏感函数库，确定与函数调用信息对应的目标函数是否存在于敏感函数库中，如果是，则将函数调用信息作为目标信息发送给服务端。

[0078] 其中，本步骤可以在目标脚本执行期间执行，也可以在目标脚本执行结束后执行，在此未做具体限定。

[0079] S9、服务端基于代理端口，拦截检测终端在客户端执行目标脚本期间传输的传输信息以及待获取的获取信息，并将拦截到的传输信息转发给待接收传输信息的接收设备以及拦截到的获取信息转发给检测终端。

[0080] S10、服务端将函数调用信息、传输信息和获取信息作为目标信息，并结合与场景参数对应的隐私合规规则，检测被测应用在检测场景下的隐私合规性。

[0081] 需要说明的是，在上述技术方案中，客户端执行了很多动作，如确定检测终端上是

否安装有被测应用、卸载已安装的被测应用、下载apk、安装已下载的apk、确定目标脚本、执行目标脚本和发送目标信息等，这些动作可以在服务端发送给客户端的adb命令中一次体现出来，这就是异步操作，由此降低了服务端阻塞耗时的可能；当然，每个动作也可以分别通过各自的adb命令体现出来，这就是同步操作，在此未做具体限定。

[0082] 本发明实施例的技术方案，通过上述各步骤相互配合，可以实现被测应用在检测场景下的隐私合规性的自动化检测，由此提高了检测效率、保证了检测准确性并且降低了检测成本。

[0083] 在实际应用中，可选的，上述技术方案的实现框架可以包括如下四个模块：检测终端模块、函数调用模块、信息拦截模块以及场景模拟模块。其中，检测终端模块还可以称为云真机，可以用于实现隐私合规检测环境配置和adb命令下达等功能。函数调用模块还可以称为客户端函数hook，可用于实现函数调用信息获取和敏感函数比对等功能。信息拦截模块还可以称为流量拦截模块，可用于实现代理链接和流量拦截转发等功能。场景模拟模块还可以称为场景自动化模块，可以用于实现检测场景模拟和隐私合规判断等功能。

[0084] 图4为本发明实施例提供的隐私合规检测装置的结构框图，该装置可用于执行上述任意实施例所提供的隐私合规检测方法。该装置与上述各个实施例的隐私合规检测方法属于同一个发明构思，在隐私合规检测装置的实施例中未详尽描述的细节内容，可以参考上述隐私合规检测方法的实施例。参见图4，该装置配置于服务端，可包括：隐私合规检测参数获取模块410、目标脚本第一执行模块420和隐私合规检测模块430。

[0085] 其中，隐私合规检测参数获取模块410，用于响应于隐私合规检测指令，获取隐私合规检测参数，其中，隐私合规检测参数包括应用标识以及场景参数；

[0086] 目标脚本第一执行模块420，用于将隐私合规检测参数发送给客户端，以使客户端根据接收的隐私合规检测参数确定目标脚本，并执行目标脚本，其中，目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，被测应用是具有应用标识的应用，检测场景是具有场景参数的场景；

[0087] 隐私合规检测模块430，用于获取目标信息，并结合与场景参数对应的隐私合规规则，检测被测应用在检测场景下的隐私合规性，其中，目标信息包括部署有客户端的检测终端在客户端执行目标脚本期间涉及的信息。

[0088] 可选的，隐私合规检测模块430，可以包括：

[0089] 传输信息拦截转发单元，用于拦截检测终端在客户端执行目标脚本期间传输的传输信息，并将传输信息转发给待接收传输信息的接收设备；和/或，

[0090] 获取信息拦截转发单元，用于拦截检测终端在客户端执行目标脚本期间待获取的获取信息，并将获取信息转发给检测终端；

[0091] 目标信息得到单元，用于将拦截到的传输信息和/或获取信息作为目标信息。

[0092] 在此基础上，可选的，隐私合规检测参数还包括用于定位部署有服务端的检测服务器上开启的代理端口的参数代理地址；

[0093] 上述隐私合规检测装置，还可以包括：

[0094] 终端系统代理配置模块，用于在将隐私合规检测参数发送给客户端之后，以使客户端将检测终端的终端系统代理，配置为接收的参数代理地址；

[0095] 相应的，传输信息拦截转发单元，可以包括：传输信息拦截子单元，用于基于代理

端口，拦截检测终端在客户端执行目标脚本期间传输的传输信息；

[0096] 获取信息拦截转发单元，可以包括：获取信息拦截子单元，用于基于代理端口，拦截检测终端在客户端执行目标脚本期间待获取的获取信息。

[0097] 可选的，目标信息包括检测终端在客户端执行目标脚本期间传输的传输信息和/或获取到的获取信息，隐私合规规则包括与获取或传输的用户隐私信息未存在于预先设置的隐私政策中时，被测应用在检测场景下隐私合规相关的规则；

[0098] 隐私合规检测模块430，可以包括：

[0099] 隐私合规检测单元，用于确定目标信息中的用户隐私信息，并根据用户隐私信息是否存在于隐私政策中，检测被测应用在检测场景下的隐私合规性。

[0100] 可选的，检测终端是连接在终端管理服务器上的各个候选终端中的一台，每台候选终端内均预先配置有隐私合规检测环境；

[0101] 上述隐私合规检测装置，还可以包括：

[0102] 检测终端确定模块，用于在响应于隐私合规检测指令之后，从与终端管理服务器连接的各候选终端中确定检测终端；

[0103] 目标脚本第一执行模块420，可以包括：

[0104] 隐私合规检测参数发送单元，用于将隐私合规检测参数发送给预先部署在检测终端上的客户端。

[0105] 本发明实施例所提供的隐私合规检测装置，服务端通过隐私合规检测参数获取模块响应于隐私合规检测指令，获取包括被测应用的应用标识和检测场景的场景参数的隐私合规检测参数，其中隐私合规检测参数可以体现出是对什么应用在什么场景下的隐私合规性进行检测；进而，通过目标脚本第一执行模块将隐私合规检测参数发送给客户端，以使客户端根据接收的隐私合规检测参数确定目标脚本，并执行目标脚本，该目标脚本是用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，由此实现了自动化模拟检测场景的效果；然后，通过隐私合规检测模块获取部署有客户端的检测终端在客户端执行目标脚本期间涉及的目标信息，并结合与场景参数对应的预先设置的隐私合规规则，检测被测应用在检测场景下的隐私合规性，由此实现了自动化判断隐私合规性的效果。上述装置，可自动化检测被测应用在检测场景下的隐私合规性，由此提高了检测效率、保证了检测准确性并且降低了检测成本。

[0106] 本发明实施例所提供的隐私合规检测装置可执行本发明任意实施例所提供的隐私合规检测方法，具备执行方法相应的功能模块和有益效果。

[0107] 值得注意的是，上述隐私合规检测装置的实施例中，所包括的各个单元和模块只是按照功能逻辑进行划分的，但并不局限于上述的划分，只要能够实现相应的功能即可；另外，各功能单元的具体名称也只是为了便于相互区分，并不用于限制本发明的保护范围。

[0108] 图5为本发明实施例提供的隐私合规检测装置的结构框图，该装置可用于执行上述任意实施例所提供的隐私合规检测方法。该装置与上述各个实施例的隐私合规检测方法属于同一个发明构思，在隐私合规检测装置的实施例中未详尽描述的细节内容，可以参考上述隐私合规检测方法的实施例。参见图5，该装置配置于客户端，具体可包括：隐私合规检测参数接收模块510和目标脚本第二执行模块520。

[0109] 其中，隐私合规检测参数接收模块510，用于接收服务端发送的隐私合规检测参

数，其中，隐私合规检测参数包括应用标识以及场景参数；

[0110] 目标脚本第二执行模块520，用于根据接收的隐私合规检测参数确定目标脚本，并执行目标脚本，以使服务端获取到目标信息，并结合与场景参数对应的隐私合规规则，检测被测应用在检测场景下的隐私合规性；

[0111] 其中，目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，被测应用是具有应用标识的应用，检测场景是具有场景参数的场景，目标信息包括部署有客户端的检测终端在客户端执行目标脚本期间涉及的信息。

[0112] 可选的，上述隐私合规检测装置，还可以包括：

[0113] 函数调用信息获取模块，用于获取函数调用信息，函数调用信息是安装在检测终端上的被测应用在客户端执行目标脚本期间调用的目标函数的标识信息；

[0114] 目标函数确定模块，用于获取预先设置的敏感函数库，并确定与函数调用信息对应的目标函数是否存在于敏感函数库中；

[0115] 目标信息发送模块，用于如果是，则将函数调用信息作为目标信息，发送给服务端。

[0116] 在此基础上，可选的，函数调用信息获取模块，可以包括：

[0117] 函数调用信息接收单元，用于接收基于广播方式发送的函数调用信息，其中，函数调用信息是基于注册在被测应用所在的进程中的钩子脚本获取后发送的信息。

[0118] 可选的，隐私合规检测参数还包括被测应用的应用安装包在存储服务器中的存储地址；

[0119] 隐私合规检测装置，还可以包括：

[0120] 被测应用确定模块，用于在接收服务端发送的隐私合规检测参数后，根据接收到的应用标识确定检测终端上是否安装有被测应用；

[0121] 被测应用卸载模块，用于如果是，则卸载安装在检测终端上的被测应用；

[0122] 应用安装包安装模块，用于基于接收到的存储地址从存储服务器上下载应用安装包，并将已下载的应用安装包安装在检测终端上。

[0123] 本发明实施例所提供的隐私合规检测装置，客户端通过隐私合规检测参数接收模块接收服务端发送的包括被测应用的应用标识和检测场景的场景参数的隐私合规检测参数，其中隐私合规检测参数可以体现出服务端需对什么应用在什么场景下的隐私合规性进行检测；进而，通过目标脚本第二执行模块根据接收到的隐私合规检测参数确定目标脚本，并执行目标脚本，该目标脚本是用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，由此实现了自动化模拟检测场景的效果，这样一来，服务端可以获取到部署有该客户端的检测终端在客户端执行目标脚本期间涉及的目标信息，并结合与场景参数对应的预先设置的隐私合规规则，检测被测应用在检测场景下的隐私合规性，由此实现了自动化判断隐私合规性的效果。上述装置，可以实现被测应用在检测场景下的隐私合规性的自动化检测，由此提高了检测效率、保证了检测准确性并且降低了检测成本。

[0124] 本发明实施例所提供的隐私合规检测装置可执行本发明任意实施例所提供的隐私合规检测方法，具备执行方法相应的功能模块和有益效果。

[0125] 值得注意的是，上述隐私合规检测装置的实施例中，所包括的各个单元和模块只是按照功能逻辑进行划分的，但并不局限于上述的划分，只要能够实现相应的功能即可；另

外，各功能单元的具体名称也只是为了便于相互区分，并不用于限制本发明的保护范围。

[0126] 图6示出了可以用来实施本发明的实施例的检测服务器或检测终端(后文统称为电子设备)10的结构示意图。电子设备旨在表示各种形式的数字计算机，诸如，膝上型计算机、台式计算机、工作台、个人数字助理、服务器、刀片式服务器、大型计算机、和其它适合的计算机。电子设备还可以表示各种形式的移动装置，诸如，个人数字处理、蜂窝电话、智能电话、可穿戴设备(如头盔、眼镜、手表等)和其它类似的计算装置。本文所示的部件、它们的连接和关系、以及它们的功能仅仅作为示例，并且不意在限制本文中描述的和/或者要求的本发明的实现。

[0127] 如图6所示，电子设备10包括至少一个处理器11，以及与至少一个处理器11通信连接的存储器，如只读存储器(ROM)12、随机访问存储器(RAM)13等，其中，存储器存储有可被至少一个处理器执行的计算机程序，处理器11可以根据存储在只读存储器(ROM)12中的计算机程序或从存储单元18加载到随机访问存储器(RAM)13中的计算机程序，来执行各种适当的动作和处理。在RAM 13中，还可存储电子设备10操作所需的各种程序和数据。处理器11、ROM 12以及RAM 13通过总线14彼此相连。输入/输出(I/O)接口15也连接至总线14。

[0128] 电子设备10中的多个部件连接至I/O接口15，包括：输入单元16，例如键盘、鼠标等；输出单元17，例如各种类型的显示器、扬声器等；存储单元18，如磁盘、光盘等；以及通信单元19，例如网卡、调制解调器、无线通信收发机等。通信单元19允许电子设备10通过诸如因特网的计算机网络和/或各种电信网络与其他设备交换信息/数据。

[0129] 处理器11可以是各种具有处理和计算能力的通用和/或专用处理组件。处理器11的一些示例包括但不限于中央处理单元(CPU)、图形处理单元(GPU)、各种专用的人工智能(AI)计算芯片、各种运行机器学习模型算法的处理器、数字信号处理器(DSP)、以及任何适当的处理器、控制器、微控制器等。处理器11执行上文所描述的各个方法和处理，例如隐私合规检测方法。

[0130] 在一些实施例中，隐私合规检测方法可被实现为计算机程序，其被有形地包含于计算机可读存储介质，例如存储单元18。在一些实施例中，计算机程序的部分或者全部可以经由ROM 12和/或通信单元19而被载入和/或安装到电子设备10上。当计算机程序加载到RAM 13并由处理器11执行时，可以执行上文描述的隐私合规检测方法的一个或多个步骤。备选地，在其他实施例中，处理器11可通过其他任何适当的方式(例如，借助于固件)而被配置为执行隐私合规检测方法。

[0131] 本文中以上描述的系统和技术的各种实施方式可以在数字电子电路系统、集成电路系统、场可编程门阵列(FPGA)、专用集成电路(ASIC)、专用标准产品(ASSP)、芯片上系统的系统(SOC)、负载可编程逻辑设备(CPLD)、计算机硬件、固件、软件、和/或它们的组合中实现。这些各种实施方式可以包括：实施在一个或者多个计算机程序中，该一个或者多个计算机程序可在包括至少一个可编程处理器的可编程系统上执行和/或解释，该可编程处理器可以是专用或者通用可编程处理器，可以从存储系统、至少一个输入装置、以及至少一个输出装置接收数据和指令，并且将数据和指令传输至该存储系统、该至少一个输入装置、以及该至少一个输出装置。

[0132] 用于实施本发明的方法的计算机程序可以采用一个或多个编程语言的任何组合来编写。这些计算机程序可以提供给通用计算机、专用计算机或是其他可编程数据处理装

置的处理器，使得计算机程序当由处理器执行时使流程图和/或框图中所规定的功能/操作被实施。计算机程序可以完全在机器上执行、部分地在机器上执行，作为独立软件包部分地在机器上执行并且部分地在远程机器上执行或完全在远程机器或服务器上执行。

[0133] 在本发明的上下文中，计算机可读存储介质可以是有形的介质，其可以包含或存储以供指令执行系统、装置或设备使用或与指令执行系统、装置或设备结合地使用的计算机程序。计算机可读存储介质可以包括但不限于电子的、磁性的、光学的、电磁的、红外的、或半导体系统、装置或设备，或者上述内容的任何合适组合。备选地，计算机可读存储介质可以是机器可读信号介质。机器可读存储介质的更具体示例会包括基于一个或多个线的电气连接、便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或快闪存储器)、光纤、便捷式紧凑盘只读存储器(CD-ROM)、光学储存设备、磁储存设备、或上述内容的任何合适组合。

[0134] 为了提供与用户的交互，可以在电子设备上实施此处描述的系统和技术，该电子设备具有：用于向用户显示信息的显示装置(例如，CRT(阴极射线管)或者LCD(液晶显示器)监视器)；以及键盘和指向装置(例如，鼠标或者轨迹球)，用户可以通过该键盘和该指向装置来将输入提供给电子设备。其它种类的装置还可以用于提供与用户的交互；例如，提供给用户的反馈可以是任何形式的传感反馈(例如，视觉反馈、听觉反馈、或者触觉反馈)；并且可以用任何形式(包括声输入、语音输入或者、触觉输入)来接收来自用户的输入。

[0135] 可以将此处描述的系统和技术实施在包括后台部件的计算系统(例如，作为数据服务器)、或者包括中间件部件的计算系统(例如，应用服务器)、或者包括前端部件的计算系统(例如，具有图形用户界面或者网络浏览器的用户计算机，用户可以通过该图形用户界面或者该网络浏览器来与此处描述的系统和技术的实施方式交互)、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信(例如，通信网络)来将系统的部件相互连接。通信网络的示例包括：局域网(LAN)、广域网(WAN)、区块链网络和互联网。

[0136] 计算系统可以包括客户端和服务器。客户端和服务器一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务器关系的计算机程序来产生客户端和服务器的关系。服务器可以是云服务器，又称为云计算服务器或云主机，是云计算服务体系中的一项主机产品，以解决了传统物理主机与VPS服务中，存在的管理难度大，业务扩展性弱的缺陷。

[0137] 应该理解，可以使用上面所示的各种形式的流程，重新排序、增加或删除步骤。例如，本发明中记载的各步骤可以并行地执行也可以顺序地执行也可以不同的次序执行，只要能够实现本发明的技术方案所期望的结果，本文在此不进行限制。

[0138] 上述具体实施方式，并不构成对本发明保护范围的限制。本领域技术人员应该明白的是，根据设计要求和其他因素，可以进行各种修改、组合、子组合和替代。任何在本发明的精神和原则之内所作的修改、等同替换和改进等，均应包含在本发明保护范围之内。

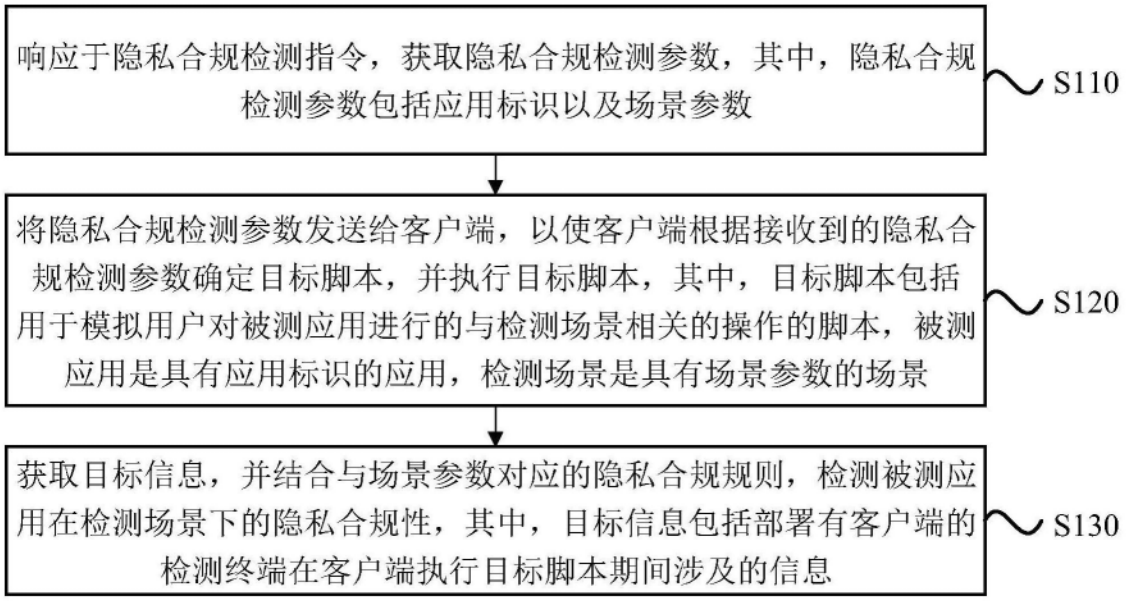

响应于隐私合规检测指令，获取隐私合规检测参数，其中，隐私合规检测参数包括应用标识以及场景参数
S110
将隐私合规检测参数发送给客户端，以使客户端根据接收到的隐私合规检测参数确定目标脚本，并执行目标脚本，其中，目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，被测应用是具有应用标识的应用，检测场景是具有场景参数的场景
S120
获取目标信息，并结合与场景参数对应的隐私合规规则，检测被测应用在检测场景下的隐私合规性，其中，目标信息包括部署有客户端的检测终端在客户端执行目标脚本期间涉及的信息
S130

图1

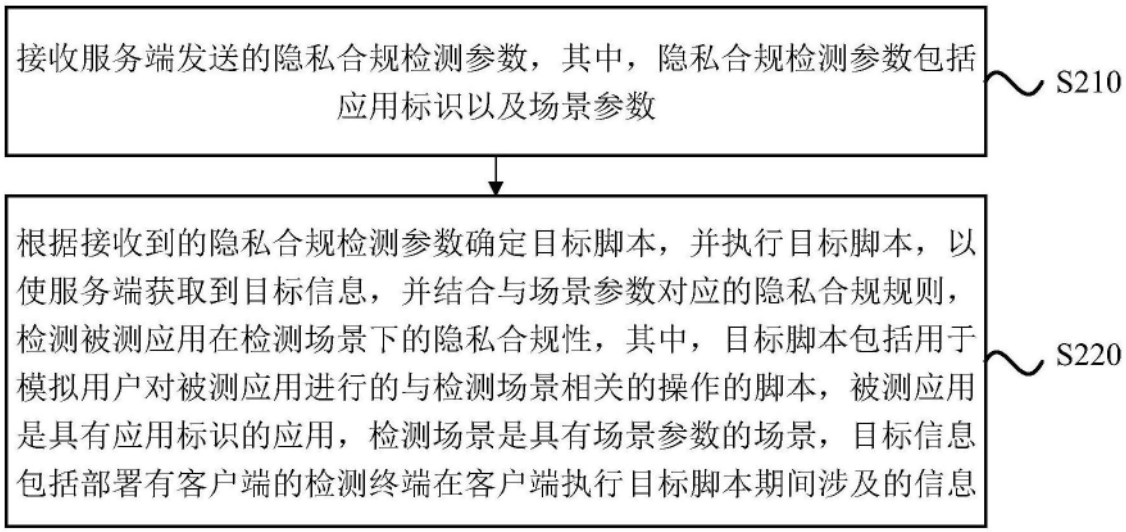

接收服务端发送的隐私合规检测参数，其中，隐私合规检测参数包括应用标识以及场景参数
S210
根据接收到的隐私合规检测参数确定目标脚本，并执行目标脚本，以使服务端获取到目标信息，并结合与场景参数对应的隐私合规规则，检测被测应用在检测场景下的隐私合规性，其中，目标脚本包括用于模拟用户对被测应用进行的与检测场景相关的操作的脚本，被测应用是具有应用标识的应用，检测场景是具有场景参数的场景，目标信息包括部署有客户端的检测终端在客户端执行目标脚本期间涉及的信息
S220

图2

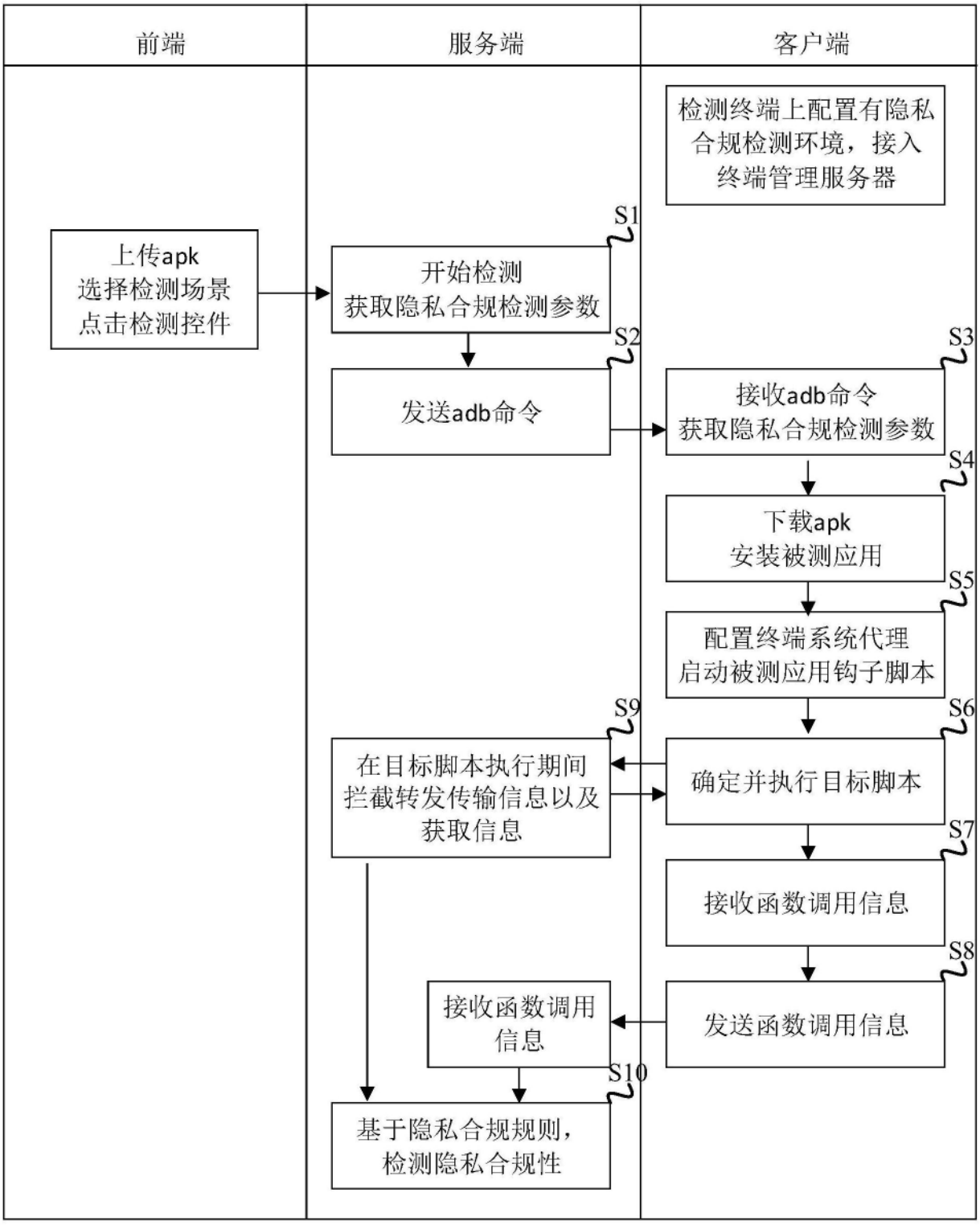

前端
服务端
客户端
检测终端上配置有隐私合规检测环境，接入终端管理服务器
S1
上传apk
选择检测场景
点击检测控件
开始检测
获取隐私合规检测参数
S2
S3
发送adb命令
接收adb命令
获取隐私合规检测参数
S4
下载apk
安装被测应用
S5
配置终端系统代理
启动被测应用钩子脚本
S9
S6
在目标脚本执行期间
拦截转发传输信息以及
获取信息
确定并执行目标脚本
S7
接收函数调用信息
S8
接收函数调用
信息
发送函数调用信息
S10
基于隐私合规规则，
检测隐私合规性

图3

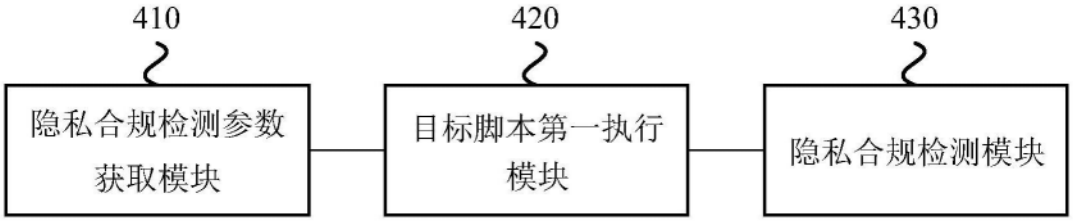

410
420
430
隐私合规检测参数获取模块
目标脚本第一执行模块
隐私合规检测模块

图4

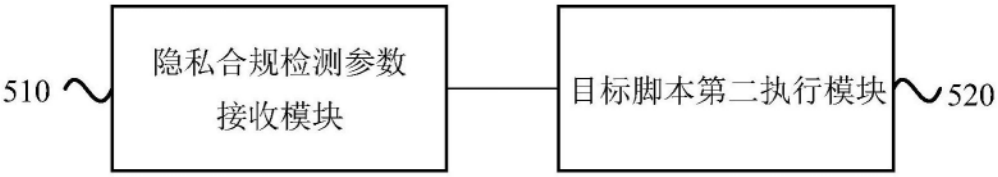

510
隐私合规检测参数接收模块
目标脚本第二执行模块
520

图5

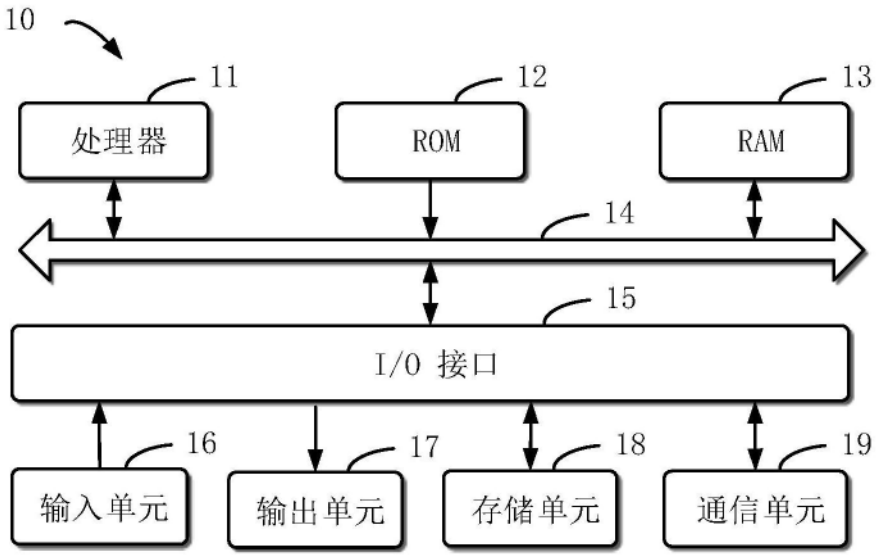

10
11
12
13
处理器
ROM
RAM
14
15
I/O 接口
16
17
18
19
输入单元
输出单元
存储单元
通信单元

图6