(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115333774 A
(43)申请公布日 2022.11.11

(21)申请号 202210790545.1

(22)申请日 2022.07.06

(71)申请人 阿里云计算有限公司
地址 310000 浙江省杭州市西湖区转塘科技经济区块12号

(72)发明人 曲宇辉

(74)专利代理机构 北京辰权知识产权代理有限公司 11619
专利代理师 李小朋

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/563(2022.01)
H04L 43/062(2022.01)

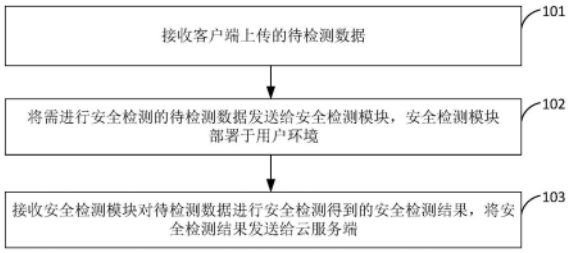
权利要求书2页 说明书12页 附图6页

(54)发明名称

安全检测的方法、系统、设备及存储介质

(57)摘要

本申请提出一种安全检测的方法、系统、设备及存储介质，该方法包括：通过应用本申请的技术方案，可以不由云服务端计算客户端的安全检测结果，而是由部署在用户环境下的代理模块以及安全检测模块共同实现计算客户端安全检测结果的目的，并在得到安全检测结果后将其上传给云服务端即可。以使一方面减少了客户端与云端的数据交互，降低了用户的流量开销。另一方面也可以节省云服务端的计算资源，避免其在处于高负荷状态下无法保证安全检测效果准确性与实时性的问题。再一方面还可以对客户端中存在的敏感性较强的隐私数据进行本地化安全检测，进而避免将隐私数据上传到云端中所导致的容易被窃取的问题。



CN 115333774 A

1.一种安全检测的方法,其特征在于,所述方法应用于部署在用户环境的代理模块,包括:

接收客户端上传的待检测数据;

将需进行安全检测的待检测数据发送给安全检测模块,所述安全检测模块部署于所述用户环境;

接收所述安全检测模块对所述待检测数据进行安全检测得到的安全检测结果,将所述安全检测结果发送给云服务端。

2.根据权利要求1所述的方法,其特征在于,在所述接收客户端上传的待检测数据之后,还包括:

基于所述云服务端下发的预设匹配规则,确定所述待检测数据是否需进行安全检测;

如果是,则将所述待检测数据发送给所述安全检测模块;

如果否,则丢弃所述待检测数据,并向所述云服务端发送本次丢弃事件的通知消息。

3.根据权利要求2所述的方法,其特征在于,所述预设匹配规则包括预设限流规则和预设转发规则,所述基于所述云服务端下发的预设匹配规则,确定所述待检测数据是否需进行安全检测,包括:

基于所述预设限流规则,确定是否需要对所述待检测数据进行限流;以及,

基于所述预设转发规则,确定是否需要对所述待检测数据进行安全检测。

4.根据权利要求3所述的方法,其特征在于,在所述获取所述云服务端发送的预设转发规则之后,还包括:

确定所述预设转发规则所包含的需要进行安全检测的数据标签;

确定所述待检测数据中,是否包含有与所述数据标签相对应的数据;

若包含,将所述待检测数据发送给所述安全检测模块;或,将所述数据标签对应的数据发送给所述安全检测模块。

5.根据权利要求1所述的方法,其特征在于,在所述接收客户端上传的待检测数据之前,还包括:

获取所述云服务端发送的预设转发规则,所述预设转发规则用于指示需要进行安全检测的类型以及对应的数据标签;

将所述预设转发规则发送给所述安全检测模块。

6.一种安全检测的方法,其特征在于,所述方法应用于部署在用户环境的安全检测模块,包括:

接收部署于所述用户环境的代理模块发送的待检测数据;

对所述待检测数据进行安全检测,得到安全检测结果;

将所述安全检测结果发送给所述代理模块,以使所述代理模块将所述安全检测结果转发给云服务端。

7.根据权利要求6所述的方法,其特征在于,在所述接收代理模块发送的待检测数据之前,还包括:

接收所述代理模块发送的预设转发规则,所述预设转发规则由云服务端下发给所述代理模块。

8.根据权利要求7所述的方法,其特征在于,在所述接收代理模块发送的待检测数据之

后,还包括:

基于所述预设转发规则,确定需要进行安全检测的数据标签;

从所述待检测数据中选取所述数据标签对应的待检测数据;

对所述数据标签对应的待检测数据进行安全检测,得到所述安全检测结果。

9.根据权利要求6所述的方法,其特征在于,所述方法还包括:

若确定所述待检测数据指向不存在安全隐患的安全检测结果时,不对所述不存在安全隐患的安全检测结果进行处理。

10.一种安全检测的方法,其特征在于,所述方法应用于云服务端,包括:

接收所述代理模块发送的安全检测结果,所述安全检测结果为安全检测模块对客户端的待检测数据进行安全检测得到的,所述代理模块及所述安全检测模块均部署于用户环境;

对所述安全检测结果进行展示。

11.根据权利要求10所述的方法,其特征在于,在所述接收所述代理模块发送的安全检测结果之前,还包括:

向所述代理模块下发预设转发规则,所述预设转发规则用于指示需要进行安全检测的类型以及对应的数据标签;以及,

向所述代理模块下发限流检测规则,所述限流检测规则用于指示所述代理模块根据网络环境确定是否对所述待检测数据进行限流。

12.一种安全检测的系统,其特征在于,所述系统包括:

部署在用户环境的客户端,用于向代理模块发送待检测数据;

部署在所述用户环境的所述代理模块,用于将接收到的待检测数据发送给安全检测模块,并在接收到所述安全检测模块基于所述待检测数据生成的安全检测结果后,将所述安全检测结果发送给云服务端;

部署在所述用户环境的所述安全检测模块,用于接收所述代理模块发送的待检测数据后,对所述待检测数据进行安全检测,得到安全检测结果,并将所述安全检测结果发送给所述代理模块;

所述云服务端,用于接收所述代理模块发送的安全检测结果后,对所述安全检测结果进行展示。

13.一种电子设备,包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序,其特征在于,所述处理器运行所述计算机程序以实现1-11任一项所述的方法。

14.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,所述程序被处理器执行实现1-11任一项所述的方法。

安全检测的方法、系统、设备及存储介质

技术领域

[0001] 本申请属于计算机技术领域，具体涉及一种安全检测的方法、系统、设备及存储介质。

背景技术

[0002] 随着互联网行业的外部环境不断变化以及云计算的快速发展，为了更好的适应环境的变换，许多工作平台纷纷将工作部署在云环境下以进行处理。

[0003] 相关技术中，对于云上数据的安全检测方式中，主要通过采集客户端上的实时数据上报到云端进行对应的安全规则匹配并最终生成检测结果。

[0004] 但是，相关技术中的安全检测方式涉及到客户端与云服务端的大量数据交互，包括机器软件包信息的采集与传输，检测数据的上传与下载，频繁的网络请求等，从而导致加大了云端设备之间的流量开销，从而增加了用户成本。

发明内容

[0005] 本申请提出一种安全检测的方法、系统、设备及存储介质，可以解决相关技术中出现的，云场景下客户端与云服务端大量数据交互所导致的增加云端设备之间的流量开销的问题。

[0006] 本申请第一方面实施例提出了一种安全检测的方法，所述方法应用于部署在用户环境的代理模块，包括：

[0007] 接收客户端上传的待检测数据；

[0008] 将需进行安全检测的待检测数据发送给安全检测模块，所述安全检测模块部署于所述用户环境；

[0009] 接收所述安全检测模块对所述待检测数据进行安全检测得到的安全检测结果，将所述安全检测结果发送给云服务端。

[0010] 本申请第二方面实施例提出了一种安全检测的方法，所述方法应用于部署在用户环境的安全检测模块，包括：

[0011] 接收部署于所述用户环境的代理模块发送的待检测数据；

[0012] 对所述待检测数据进行安全检测，得到安全检测结果；

[0013] 将所述安全检测结果发送给所述代理模块，以使所述代理模块将所述安全检测结果转发给云服务端。

[0014] 本申请第三方面实施例提出了一种安全检测的方法，所述方法应用于云服务端，包括：

[0015] 接收所述代理模块发送的安全检测结果，所述安全检测结果为安全检测模块对客户端的待检测数据进行安全检测得到的，所述代理模块及所述安全检测模块均部署于用户环境；

[0016] 对所述安全检测结果进行展示。

[0017] 本申请第四方面实施例提出了一种安全检测的系统，包括：

[0018] 部署在用户环境的客户端，用于向代理模块发送待检测数据；

[0019] 部署在所述用户环境的所述代理模块，用于将接收到的待检测数据发送给安全检测模块，并在接收到所述安全检测模块基于所述待检测数据生成的安全检测结果后，将所述安全检测结果发送给云服务端；

[0020] 部署在所述用户环境的所述安全检测模块，用于接收所述代理模块发送的待检测数据后，对所述待检测数据进行安全检测，得到安全检测结果，并将所述安全检测结果发送给所述代理模块；

[0021] 所述云服务端，用于接收所述代理模块发送的安全检测结果后，对所述安全检测结果进行展示。

[0022] 本申请第五方面的实施例提供了一种电子设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器运行所述计算机程序以实现上述第一方面、第二方面、第三方面所述的方法。

[0023] 本申请第六方面的实施例提供了一种计算机可读存储介质，其上存储有计算机程序，所述程序被处理器执行实现上述第一方面、第二方面、第三方面所述的方法。

[0024] 本申请实施例中提供的技术方案，至少具有如下技术效果或优点：

[0025] 在本申请实施例中，可以由部署在用户环境的客户端，用于向代理模块发送待检测数据；部署在用户环境的代理模块，用于将接收到的待检测数据发送给安全检测模块，并在接收到安全检测模块基于待检测数据生成的安全检测结果后，将安全检测结果发送给云服务端；部署在用户环境的安全检测模块，用于接收代理模块发送的待检测数据后，对待检测数据进行安全检测，得到安全检测结果，并将安全检测结果发送给代理模块；云服务端，用于接收代理模块发送的安全检测结果后，对安全检测结果进行展示。通过应用本申请的技术方案，可以不由云服务端计算客户端的安全检测结果，而是由部署在用户环境下的代理模块以及安全检测模块共同实现计算客户端安全检测结果的目的，并在得到安全检测结果后将其上传给云服务端即可。以使一方面减少了客户端与云端的数据交互，降低了用户的流量开销。另一方面也可以节省云服务端的计算资源，避免其在处于高负荷状态下无法保证安全检测效果准确性与实时性的问题。再一方面还可以对客户端中存在的敏感性较强的隐私数据进行本地化安全检测，进而避免将隐私数据上传到云端中所导致的容易被窃取的问题。

[0026] 本申请附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变的明显，或通过本申请的实践了解到。

附图说明

[0027] 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，而并不认为是对本申请的限制。而且在整个附图中，用相同的参考符号表示相同的部件。

[0028] 在附图中：

[0029] 图1示出了本申请一实施例所提供的一种安全检测的方法的示意图；

[0030] 图2示出了本申请一实施例所提供的一种安全检测的系统架构示意图；

[0031] 图3示出了本申请一实施例所提供的一种安全检测的方法的一个流程图；

[0032] 图4示出了本申请一实施例所提供的一种安全检测的方法的另一流程图；

[0033] 图5示出了本申请一实施例所提供的一种安全检测的方法的再一流程图；

[0034] 图6示出了本申请一实施例所提供的一种安全检测的系统流程图；

[0035] 图7示出了本申请一实施例所提供的还一种安全检测的装置的结构示意图；

[0036] 图8示出了本申请一实施例所提供的另一种安全检测的装置的结构示意图；

[0037] 图9示出了本申请一实施例所提供的另一种安全检测的装置的结构示意图；

[0038] 图10示出了本申请一实施例所提供的一种电子设备的结构示意图；

[0039] 图11示出了本申请一实施例所提供的一种存储介质的示意图。

具体实施方式

[0040] 下面将参照附图更详细地描述本申请的示例性实施方式。虽然附图中显示了本申请的示例性实施方式，然而应当理解，可以以各种形式实现本申请而不应被这里阐述的实施方式所限制。相反，提供这些实施方式是为了能够更透彻地理解本申请，并且能够将本申请的范围完整的传达给本领域的技术人员。

[0041] 需要注意的是，除非另有说明，本申请使用的技术术语或者科学术语应当为本申请所属领域技术人员所理解的通常意义。

[0042] 下面结合附图来描述根据本申请实施例提出的一种安全检测的方法、系统、设备及存储介质。

[0043] 本申请实施例提供了一种安全检测的方法，该方法可以由部署在用户环境的代理模块接收到待检测数据并发送给安全检测模块，并在接收到安全检测模块基于待检测数据生成的安全检测结果后，将安全检测结果发送给云服务端。

[0044] 参见图1，该方法应用于部署在用户环境的代理模块，具体包括以下步骤：

[0045] 步骤101：接收客户端上传的待检测数据。

[0046] 其中，本申请不对客户端上传的待检测数据进行具体限定。一种方式中，其可以为工作数据，该数据中包含了安全检测规则所对应的，需要进行安全检测的数据。例如包括系统数，rpm包数，进程数据以及版本号数据等等。

[0047] 作为示例的，客户端可以预先采集用户机器的多个工作数据并对不同类型的数据进行标签打标，从而区分出系统信息，rpm包信息，进程信息等不同数据类型的数据。

[0048] 一种方式中，本申请实施例不对客户端的数量进行具体限定，例如可以为一个，也可以为多个。其中，一个客户端可以上传一份待检测数据，也可以上传多份待检测数据。

[0049] 可以理解的，本申请实施例下，不用再使每台客户端都具备连通云上服务的能力，也无需采集用户机器原始数据向云服务端全量上报。而是在用户环境部署具有规则配置与转发能力的代理模块，以使每台客户端与代理模块建立tcp长连接，客户端数据通过长连接上报至代理模块即可。

[0050] 一种方式中，本申请中的代理模块可以为一个计算单元，也可以为一台服务器，还可以为多台服务器组成的服务器集群。作为示例的，若代理模块为多台服务器组成的服务器集群时，可以由一台代理模块负责接收某一区域或某一工作范围的客户端上传的待检测数据。

[0051] 步骤102:将需进行安全检测的待检测数据发送给安全检测模块,安全检测模块部署于用户环境。

[0052] 其中,本申请实施例不对安全检测模块进行具体限定,例如可以为用于检测数据漏洞的安全检测模块,也可以为用于检测告警信息的安全检测模块。还可以为用于检测文件合规的安全检测模块等等。

[0053] 一种方式中,安全检测模块的数量可以为一台,也可以为多台。本申请实施例中,代理模块在接收到待检测数据后,可以将其中需进行安全检测的待检测数据发送给其中一台安全检测模块。也可以根据安全检测的类型不同,选择将待检测数据发送到多个对应的安全检测模块中。

[0054] 一种方式中,本申请中的安全检测模块可以为一个计算单元,也可以为一台服务器,还可以为多台服务器组成的服务器集群。作为示例的,安全检测模块和代理模块可以为一个计算单元或一台服务器(即同台服务器中的不同功能区域部署),也可以为不同的计算单元或不同的服务器。本申请对此不作限定。

[0055] 一种方式中,以安全检测模块为数据漏洞检测服务器为例,相关技术中,对于云上Saas化漏洞检测产品的检测方式,主要包括通过采集客户端上的实时数据上报到云端进行规则匹配;下发脚本到用户环境,在机器上执行检测脚本进行本地检测,最后将检测结果上报云端;或,通过扫描器构造网络流量对用户公网暴露的资产进行远程扫描等。

[0056] 进一步的,在混合云场景下,需要将用户环境与云上产品进行打通,用户可通过部署代理或拉专线的方式来实现,最终可以实现像云上机器检测一样的检测效果。

[0057] 但是漏洞检测方式涉及到大量的数据交互,包括机器软件包信息的采集与传输,检测脚本的上传与下载,频繁的网络请求等。因此在云场景下会带来一系列问题。例如机器数据上传云端是否合规,大量依赖公网的数据交互带来的潜在流量开销,网络质量对系统的检测效果影响,专线的成本问题等。

[0058] 基于上述问题,本申请提出一种安全检测的方法,通过将云端的漏洞检测逻辑(或其他安全检测逻辑)下沉到用户环境,从而实现直接在用户环境进行数据采集,转发与安全检测,并由代理模块将检测结果进行上报的方案。

[0059] 步骤103:接收安全检测模块对待检测数据进行安全检测得到的安全检测结果,将安全检测结果发送给云服务端。

[0060] 一种方式中,如图2所示,为本申请提出的安全检测的系统架构图,其中包括客户端(client),部署在用户环境的代理模块(proxy),部署在用户环境的安全检测模块(vul-engine)以及云端中的云服务端(server)。

[0061] 由图2可以看出,本申请实施例中的客户端无需如现有技术一样,需要具备连通云上服务的能力,也无需采集用户机器原始数据向云服务端全量上报。而是在用户环境部署具有规则配置与转发能力的代理模块,以使每台客户端与代理模块建立tcp长连接,客户端数据通过长连接上报至代理模块即可。

[0062] 进一步的,本申请实施例下的代理模块作为用户环境的出口,需要具备连通云服务端的能力。一种方式中,可以由每台客户端与代理模块建立长连接后,每个客户端通过这样一条双向连接来实现待检测数据的透明代理与转发。

[0063] 一种方式中,代理模块需要与云服务端维护一条独立的长连接,来作为代理自身

的通道，通过维护这样一条通道来实现接收云服务端下发的预设匹配规则(即包括预设限流规则以及预设转发规则等)。

[0064] 另外，该通道与用于由代理模块将安全检测结果进行上报的数据通道。作为示例的，为了实现用户环境的安全检测，安全检测模块需要与代理模块一同部署。其中，二者可以部署为同一台服务器，也可以部署在不同的服务器上。本申请对此不作限定。

[0065] 一种方式中，代理模块通过长连接接收到客户端上报的待检测数据后，可以将根据预设转发规则过滤后的所需待检测数据转发至安全检测模块。并在后续把最终的安全检测结果上报到云服务端。

[0066] 可以理解的，本申请实施例中通过将安全检测的步骤下沉到用户环境，大大减少了数据上报，同时降低了服务端数据存储与计算的压力。另外，也减少了网络数据传输，更低的带宽占用，降低了用户的部署成本，同时也减轻了云服务端的存储与计算压力。再者，由于系统自身具备流量统计，带宽控制，支持配置化的数据限流，转发功能。还可以实现便于扩展，方便用户进行数据接入，打造客户自己的检测平台等目的。

[0067] 在本申请实施例中，可以由部署在用户环境的客户端，用于向代理模块发送待检测数据；部署在用户环境的代理模块，用于将接收到的待检测数据发送给安全检测模块，并在接收到安全检测模块基于待检测数据生成的安全检测结果后，将安全检测结果发送给云服务端；部署在用户环境的安全检测模块，用于接收代理模块发送的待检测数据后，对待检测数据进行安全检测，得到安全检测结果，并将安全检测结果发送给代理模块；云服务端，用于接收代理模块发送的安全检测结果后，对安全检测结果进行展示。通过应用本申请的技术方案，可以不由云服务端计算客户端的安全检测结果，而是由部署在用户环境下的代理模块以及安全检测模块共同实现计算客户端安全检测结果的目的，并在得到安全检测结果后将其上传给云服务端即可。以使一方面减少了客户端与云端的数据交互，降低了用户的流量开销。另一方面也可以节省云服务端的计算资源，避免其在处于高负荷状态下无法保证安全检测效果准确性与实时性的问题。

[0068] 可选的一种实施例中，本申请在接收客户端上传的待检测数据之后，还包括：

[0069] 基于云服务端下发的预设匹配规则，确定待检测数据是否需进行安全检测；

[0070] 如果是，则将待检测数据发送给安全检测模块；

[0071] 如果否，则丢弃待检测数据，并向云服务端发送本次丢弃事件的通知消息。

[0072] 一种方式中，代理模块在采集到客户端上传的待检测数据后，需要基于云服务端下发的预设匹配规则来确定其是否需要进行安全检测。

[0073] 作为一种示例，若需要进行安全检测则将待检测数据发送给安全检测模块。作为另一种示例，如果不需要，那么为了避免与安全检测模块的无谓交互，代理模块即可对其进行丢弃或失效处理。一种方式中，其需要向云服务端发送本次丢弃事件的通知消息以使服务端及时获知客户端的采集状态。

[0074] 可选的一种实施例中，本申请在预设匹配规则包括预设限流规则和预设转发规则，基于云服务端下发的预设匹配规则，确定待检测数据是否需进行安全检测，包括：

[0075] 基于预设限流规则，确定是否需要对待检测数据进行限流；以及，

[0076] 基于预设转发规则，确定是否需要对待检测数据进行安全检测。

[0077] 一种方式中，对于限流匹配来说，代理模块可以根据该预设限流规则来对当前其

自身的网络环境进行流量检测，从而确定当前网络环境是否能够进行数据转发。可以理解的，若能够，则确定不需要对待检测数据进行限流。反之则确定需要对待检测数据进行限流。

[0078] 另一种方式中，对于转发匹配来说，代理模块可以根据该预设转发规则来对待检测数据是否有需要进行安全检测的数据来进行数据匹配。可以理解的，若不包含，则确定不需要对待检测数据进行转发至安全检测模块的步骤。反之则确定需要对待检测数据进行转发至安全检测模块的步骤。

[0079] 一种方式中，代理模块为每个客户端维护一条双向连接，通过集群部署实现负载均衡，根据服务端下发的规则对客户端上报的原始数据进行限流，直接上报或转发。

[0080] 作为示例的，在一定的时间窗口内，代理模块会统计对应的事件数，并采集例如自身的水位信息等用于表征自身工作负载状态的信息进行上报至云服务器的步骤。对于客户端上报的每一类工作数据，可根据标签配置对应的规则，限流规则支持带宽和QPS，转发规则支持转发至本地扫描引擎或上报云端，或写入本地文件等方式，便于用户自己进行数据接入，打造自己的管理平台。

[0081] 可选的一种实施例中，本申请在获取云服务端发送的预设转发规则之后，还包括：

[0082] 确定预设转发规则所包含的需要进行安全检测的数据标签；

[0083] 确定待检测数据中，是否包含有与数据标签相对应的数据；

[0084] 若包含，将待检测数据发送给安全检测模块；或，将数据标签对应的数据发送给安全检测模块。

[0085] 一种方式中，代理模块可以通过长连接接收到客户端上报的待检测数据后，将根据预设转发规则过滤后的所需数据(即数据标签相对应的数据，例如数据标签指向预设版本时，该预设版本下的数据即为数据标签相对应的数据)或待检测数据的全部数据转发至安全检测模块。并在后续把最终检测结果上报到云服务。通过将扫描引擎下沉到用户环境，大大减少了数据上报，同时降低了服务端数据存储与计算的压力

[0086] 可选的一种实施例中，本申请在接收客户端上传的待检测数据之前，还包括：

[0087] 获取云服务端发送的预设转发规则，预设转发规则用于指示需要进行安全检测的类型以及对应的数据标签；

[0088] 将预设转发规则发送给安全检测模块。

[0089] 一种方式中，如图3所示，为本申请提出的一种安全检测的方法的示意图，其中以代理模块为混合云代理模块，安全检测模块为漏洞检测服务器(vul-engine)为例进行说明，其中：

[0090] 首先，需要由客户端采集自身的主机数据并对不同类型的数据进行打标，从而区分出系统信息，rpm包信息，进程信息等不同数据类型，生成待检测数据。

[0091] 另外，客户端将待检测数据上报到代理模块之后，混合云代理模块通过识别数据标签进行预设匹配规则判断，如果触发了限流规则，将对待检测数据进行丢弃并记录事件；如果是漏洞检测服务器需要关注的数据类型，需要进行转发值漏洞检测服务器的步骤。

[0092] 进一步的，漏洞检测服务器对待检测数据进行漏洞规则匹配后产出漏洞并由代理模块上报至云端。作为示例的，如果是目前无需关注的数据类型或不存在安全隐患的待检测数据，可以直接进行丢弃并记录事件即可。

[0093] 通过应用本申请的技术方案，可以不由云服务端计算客户端的安全检测结果，而是由部署在用户环境下的代理模块以及安全检测模块共同实现计算客户端安全检测结果的目的，并在得到安全检测结果后将其上传给云服务端即可。以使一方面减少了客户端与云端的数据交互，降低了用户的流量开销。另一方面也可以节省云服务端的计算资源，避免其在处于高负荷状态下无法保证安全检测效果准确性与实时性的问题。

[0094] 参见图4，本申请实施例还提供了一种安全检测的方法，该方法应用于部署在用户环境的安全检测模块，包括：

[0095] 步骤201：接收部署于用户环境的代理模块发送的待检测数据。

[0096] 其中，本申请实施例不对安全检测模块进行具体限定，例如可以为用于检测数据漏洞的安全检测模块，也可以为用于检测告警信息的安全检测模块。还可以为用于检测文件合规的安全检测模块等等。

[0097] 一种方式中，安全检测模块的数量可以为一台，也可以为多台。本申请实施例中，代理模块在接收到待检测数据后，可以将其中需进行安全检测的待检测数据发送给其中一台安全检测模块。也可以根据安全检测的类型不同，选择将待检测数据发送到多个对应的安全检测模块中。

[0098] 步骤202：对待检测数据进行安全检测，得到安全检测结果。

[0099] 步骤203：将安全检测结果发送给代理模块，以使代理模块将安全检测结果转发给云服务端。

[0100] 一种方式中，安全检测模块需要根据云服务端下发的转发规则来确定自身需要进行安全检测的数据标签(该数据标签可以为管理人员根据需要设定，例如为系统类型，rpm软件包版本信息等)。并依赖客户端上报的待检测数据中包含的对应系统类型，rpm软件包版本信息，进程关联的相关中间件版本信息等等数据(即数据标签对应的待检测数据)来实现对待检测数据进行安全检测，从而得到安全检测结果。

[0101] 进一步说明，同样的，首先需要由客户端采集自身的主机数据并对不同类型的数据进行打标，从而区分出系统信息，rpm包信息，进程信息等不同数据类型，生成待检测数据。

[0102] 另外，客户端将待检测数据上报到代理模块之后，云代理模块通过识别数据标签进行预设匹配规则判断，如果触发了限流规则，将对待检测数据进行丢弃并记录事件；如果是安全检测模块需要关注的数据类型，需要进行转发值漏洞检测服务器的步骤。

[0103] 进一步的，安全检测模块对待检测数据进行安全规则匹配后产出安全结果并由代理模块上报至云端。作为示例的，如果是目前无需关注的数据类型或不存在安全隐患的待检测数据，安全检测模块可以直接将其进行丢弃并记录事件即可。

[0104] 通过应用本申请的技术方案，可以不由云服务端计算客户端的安全检测结果，而是由部署在用户环境下的代理模块以及安全检测模块共同实现计算客户端安全检测结果的目的，并在得到安全检测结果后将其上传给云服务端即可。以使一方面减少了客户端与云端的数据交互，降低了用户的流量开销。另一方面也可以节省云服务端的计算资源，避免其在处于高负荷状态下无法保证安全检测效果准确性与实时性的问题。

[0105] 可选的一种实施例中，本申请在接收代理模块发送的待检测数据之前，还包括：

[0106] 接收代理模块发送的预设转发规则，预设转发规则由云服务端下发给代理模块。

[0107] 可选的一种实施例中，本申请在接收代理模块发送的待检测数据之后，还包括：

[0108] 基于预设转发规则，确定需要进行安全检测的数据标签；

[0109] 从待检测数据中选取数据标签对应的待检测数据；

[0110] 对数据标签对应的待检测数据进行安全检测，得到安全检测结果。

[0111] 一种方式中，对于转发匹配来说，安全检测模块可以根据该预设转发规则来对待检测数据是进行对应的安全检测。即首先根据预设转发规则中的数据标签确定相对应的待检测数据。并在后续对该数据标签确定相对应的待检测数据进行安全检测，得到安全检测结果。

[0112] 作为示例的，例如数据标签指向系统A的1.0版本时，客户端发送的待检测数据中，所有属于系统A的1.0版本下的数据即为数据标签相对应的数据，安全检测模块即对该系统A的1.0版本下的数据进行安全检测，得到安全检测结果后发送给代理模块。

[0113] 可选的一种实施例中，本申请若确定待检测数据指向不存在安全隐患的安全检测结果时，不对不存在安全隐患的安全检测结果进行处理。

[0114] 作为一种示例，若待检测数据指向存在安全隐患的安全检测结果时，需要立即将其发送给代理模块以使后续反馈给云服务端。

[0115] 作为另一种示例，如果待检测数据指向不存在安全隐患的安全检测结果时，那么为了避免与代理模块的无谓交互，安全检测模块即可对其进行丢弃或失效处理。一种方式中，其需要记录该丢弃事件以在后续提供给用户查看。

[0116] 参见图5，本申请实施例还提供了一种安全检测的方法，该方法应用于云服务端，包括：

[0117] S301，接收代理模块发送的安全检测结果，安全检测结果为安全检测模块对客户端的待检测数据进行安全检测得到的，代理模块及安全检测模块均部署于用户环境。

[0118] S302，对安全检测结果进行展示。

[0119] 本申请实施例中的云服务端可以包括向代理模块下发的密钥管理，规则配置管理，检测统计，以及安全检测结果的展示等等。

[0120] 其中，密钥管理主要涉及到客户端数据上报的待检测数据加解密，从而避免数据的明文传输。规则配置是指在代理侧生效的相关规则，包括预设限流规则，预设转发规则等。

[0121] 可选的，代理模块可以实时的采集限流事件，客户端连接数，机器水位等相关检测信息上报至云服务端。以使由云服务端统一管理，从而保证代理模块的稳定性。一种方式中，作为安全检测模块，需要把安全检测结果进行透出，云服务端需要把代理模块上报的最终安全检测结果进行最终处理(例如保存、筛除重复等操作)后，进行控制台展示。

[0122] 一种可能的实施方式中，在用户环境下，代理模块可以对客户端进行事件统计，网络限流，连接管理，透明代理，规则管理，密钥管理，负载均衡，配置转发等主要功能。

[0123] 可选的一种实施例中，本申请在接收代理模块发送的安全检测结果之前，还包括：

[0124] 向代理模块下发预设转发规则，预设转发规则用于指示需要进行安全检测的类型以及对应的数据标签；以及，

[0125] 向代理模块下发限流检测规则，限流检测规则用于指示代理模块根据网络环境确定是否对待检测数据进行限流。

[0126] 通过应用本申请的技术方案，可以不由云服务端计算客户端的安全检测结果，而是由部署在用户环境下的代理模块以及安全检测模块共同实现计算客户端安全检测结果的目的，并在得到安全检测结果后将其上传给云服务端即可。以使一方面减少了客户端与云端的数据交互，降低了用户的流量开销。另一方面也可以节省云服务端的计算资源，避免其在处于高负荷状态下无法保证安全检测效果准确性与实时性的问题。

[0127] 本申请实施例还提供一种安全检测的系统，该系统用于执行上述任一实施例提供的安全检测的方法中代理模块、安全检测模块以及客户端所执行的操作。其中，该系统包括：

[0128] 部署在用户环境的客户端，用于向代理模块发送待检测数据；

[0129] 部署在所述用户环境的所述代理模块，用于将接收到的待检测数据发送给安全检测模块，并在接收到所述安全检测模块基于所述待检测数据生成的安全检测结果后，将所述安全检测结果发送给云服务端；

[0130] 部署在所述用户环境的所述安全检测模块，用于接收所述代理模块发送的待检测数据后，对所述待检测数据进行安全检测，得到安全检测结果，并将所述安全检测结果发送给所述代理模块；

[0131] 所述云服务端，用于接收所述代理模块发送的安全检测结果后，对所述安全检测结果进行展示。

[0132] 如图6所示，为本申请提出的一种利用安全检测的系统执行上述任一实施例提供的安全检测的方法中代理模块、安全检测模块以及客户端所执行的操作的示意图，其中：

[0133] 首先，需要由客户端采集自身的主机数据并对不同类型的数据进行打标，从而区分出系统信息，rpm包信息，进程信息等不同数据类型，生成待检测数据。

[0134] 另外，客户端将待检测数据上报到代理模块之后，混合云代理模块通过识别数据标签进行预设匹配规则判断，如果触发了限流规则，将对待检测数据进行丢弃并记录事件；如果是漏洞检测服务器需要关注的数据类型，需要进行转发值漏洞检测服务器的步骤。

[0135] 进一步的，漏洞检测服务器对待检测数据进行漏洞规则匹配后产出漏洞并由代理模块上报至云端。作为示例的，如果是目前无需关注的数据类型或不存在安全隐患的待检测数据，可以直接进行丢弃并记录事件即可。

[0136] 通过应用本申请的技术方案，可以不由云服务端计算客户端的安全检测结果，而是由部署在用户环境下的代理模块以及安全检测模块共同实现计算客户端安全检测结果的目的，并在得到安全检测结果后将其上传给云服务端即可。以使一方面减少了客户端与云端的数据交互，降低了用户的流量开销。另一方面也可以节省云服务端的计算资源，避免其在处于高负荷状态下无法保证安全检测效果准确性与实时性的问题。

[0137] 本申请的上述实施例提供的安全检测的装置与本申请实施例提供的安全检测的方法出于相同的发明构思，具有与其存储的应用程序所采用、运行或实现的方法相同的有益效果。

[0138] 本申请实施例还提供一种安全检测的装置，该装置用于执行上述任一实施例提供的安全检测的方法中所执行的操作。如图7所示，该装置应用于部署在用户环境的代理模块，包括：

[0139] 第一接收模块301，用于接收客户端上传的待检测数据；

[0140] 第一发送模块302，用于将需进行安全检测的待检测数据发送给安全检测模块，所述安全检测模块部署于所述用户环境；

[0141] 第二接收模块303，用于接收所述安全检测模块对所述待检测数据进行安全检测得到的安全检测结果，将所述安全检测结果发送给云服务端。

[0142] 在本申请的另外一种实施方式中，第一发送模块302，被配置执行的步骤包括：

[0143] 基于所述云服务端下发的预设匹配规则，确定所述待检测数据是否需进行安全检测；

[0144] 如果是，则将所述待检测数据发送给所述安全检测模块；

[0145] 如果否，则丢弃所述待检测数据，并向所述云服务端发送本次丢弃事件的通知消息。

[0146] 在本申请的另外一种实施方式中，第一发送模块302，被配置执行的步骤包括：

[0147] 基于所述预设限流规则，确定是否需要对所述待检测数据进行限流；以及，

[0148] 基于所述预设转发规则，确定是否需要对所述待检测数据进行安全检测。

[0149] 在本申请的另外一种实施方式中，第一发送模块302，被配置执行的步骤包括：

[0150] 确定所述预设转发规则所包含的需要进行安全检测的数据标签；

[0151] 确定所述待检测数据中，是否包含有与所述数据标签相对应的数据；

[0152] 若包含，将所述待检测数据发送给所述安全检测模块；或，将所述数据标签对应的数据发送给所述安全检测模块。

[0153] 在本申请的另外一种实施方式中，第一发送模块302，被配置执行的步骤包括：

[0154] 获取所述云服务端发送的预设转发规则，所述预设转发规则用于指示需要进行安全检测的类型以及对应的数据标签；

[0155] 将所述预设转发规则发送给所述安全检测模块。

[0156] 本申请实施例还提供一种安全检测的装置，该装置用于执行上述任一实施例提供的安全检测的方法中所执行的操作。如图8所示，该装置应用于部署在用户环境的安全检测模块，包括：

[0157] 第二接收模块304，用于接收部署于所述用户环境的代理模块发送的待检测数据；

[0158] 检测模块305，用于对所述待检测数据进行安全检测，得到安全检测结果；

[0159] 第三发送模块306，用于将所述安全检测结果发送给所述代理模块，以使所述代理模块将所述安全检测结果转发给云服务端。

[0160] 在本申请的另外一种实施方式中，检测模块305，被配置执行的步骤包括：

[0161] 接收所述代理模块发送的预设转发规则，所述预设转发规则由云服务端下发给所述代理模块。

[0162] 在本申请的另外一种实施方式中，检测模块305，被配置执行的步骤包括：

[0163] 基于所述预设转发规则，确定需要进行安全检测的数据标签；

[0164] 从所述待检测数据中选取所述数据标签对应的待检测数据；

[0165] 对所述数据标签对应的待检测数据进行安全检测，得到所述安全检测结果。

[0166] 在本申请的另外一种实施方式中，检测模块305，被配置执行的步骤包括：

[0167] 若确定所述待检测数据指向不存在安全隐患的安全检测结果时，不对所述不存在安全隐患的安全检测结果进行处理。

[0168] 本申请实施例还提供一种安全检测的装置，该装置用于执行上述任一实施例提供的安全检测的方法中所执行的操作。如图9所示，该装置应用于部署在用户环境的安全检测模块，包括：

[0169] 第三接收模块307，用于接收所述代理模块发送的安全检测结果，所述安全检测结果为安全检测模块对客户端的待检测数据进行安全检测得到的，所述代理模块及所述安全检测模块均部署于用户环境；

[0170] 展示模块308，用于对所述安全检测结果进行展示。

[0171] 在本申请的另外一种实施方式中，展示模块308，被配置执行的步骤包括：

[0172] 向所述代理模块下发预设转发规则，所述预设转发规则用于指示需要进行安全检测的类型以及对应的数据标签；以及，

[0173] 向所述代理模块下发限流检测规则，所述限流检测规则用于指示所述代理模块根据网络环境确定是否对所述待检测数据进行限流。

[0174] 本申请的上述实施例提供的安全检测的装置与本申请实施例提供的安全检测的方法出于相同的发明构思，具有与其存储的应用程序所采用、运行或实现的方法相同的有益效果。

[0175] 本申请实施方式还提供一种电子设备，以执行上述安全检测的方法。请参考图10，其示出了本申请的一些实施方式所提供的一种电子设备的示意图。如图10所示，电子设备4包括：处理器400，存储器401，总线402和通信接口403，所述处理器400、通信接口403和存储器401通过总线402连接；所述存储器401中存储有可在所述处理器400上运行的计算机程序，所述处理器400运行所述计算机程序时执行本申请前述任一实施方式所提供的安全检测的方法。

[0176] 其中，存储器401可能包含高速随机存取存储器(RAM:Random Access Memory)，也可能还包括非不稳定的存储器(non-volatile memory)，例如至少一个磁盘存储器。通过至少一个通信接口403(可以是有线或者无线)实现该装置网元与至少一个其他网元之间的通信连接，可以使用互联网、广域网、本地网、城域网等。

[0177] 总线402可以是ISA总线、PCI总线或EISA总线等。所述总线可以分为地址总线、数据总线、控制总线等。其中，存储器401用于存储程序，所述处理器400在接收到执行指令后，执行所述程序，前述本申请实施例任一实施方式揭示的所述安全检测的方法可以应用于处理器400中，或者由处理器400实现。

[0178] 处理器400可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器400中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器400可以是通用处理器，包括处理器(Central Processing Unit，简称CPU)、网络处理器(Network Processor，简称NP)等；还可以是数字信号处理器(DSP)、专用集成电路(ASIC)、现成可编程门阵列(FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于

存储器401，处理器400读取存储器401中的信息，结合其硬件完成上述方法的步骤。

[0179] 本申请实施例提供的电子设备与本申请实施例提供的安全检测的方法出于相同的发明构思，具有与其采用、运行或实现的方法相同的有益效果。

[0180] 本申请实施方式还提供一种与前述实施方式所提供的安全检测的方法对应的计算机可读存储介质，请参考图11，其示出的计算机可读存储介质为光盘50，其上存储有计算机程序(即程序产品)，所述计算机程序在被处理器运行时，会执行前述任意实施方式所提供的安全检测的方法。

[0181] 需要说明的是，所述计算机可读存储介质的例子还可以包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他光学、磁性存储介质，在此不再一一赘述。

[0182] 本申请的上述实施例提供的计算机可读存储介质与本申请实施例提供的安全检测的方法出于相同的发明构思，具有与其存储的应用程序所采用、运行或实现的方法相同的有益效果。

[0183] 需要说明的是：

[0184] 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，本申请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结构和技术，以便不模糊对本说明书的理解。

[0185] 类似地，应当理解，为了精简本申请并帮助理解各个发明方面中的一个或多个，在上面对本申请的示例性实施例的描述中，本申请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示意图：即所要求保护的本申请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申请的单独实施例。

[0186] 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申请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。

[0187] 以上所述，仅为本申请较佳的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

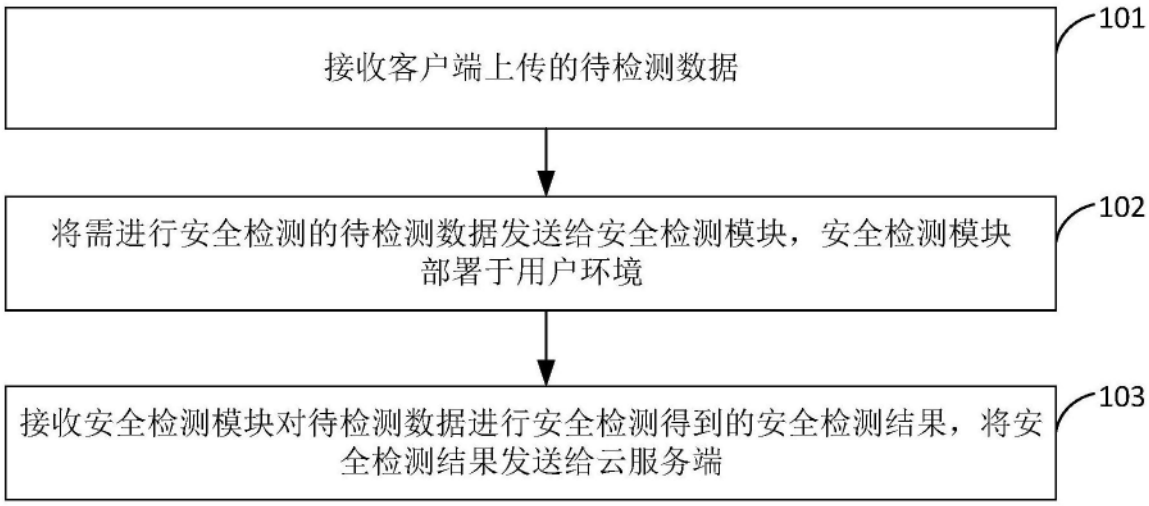

接收客户端上传的待检测数据
101
将需进行安全检测的待检测数据发送给安全检测模块，安全检测模块部署于用户环境
102
接收安全检测模块对待检测数据进行安全检测得到的安全检测结果，将安全检测结果发送给云服务端
103

图1

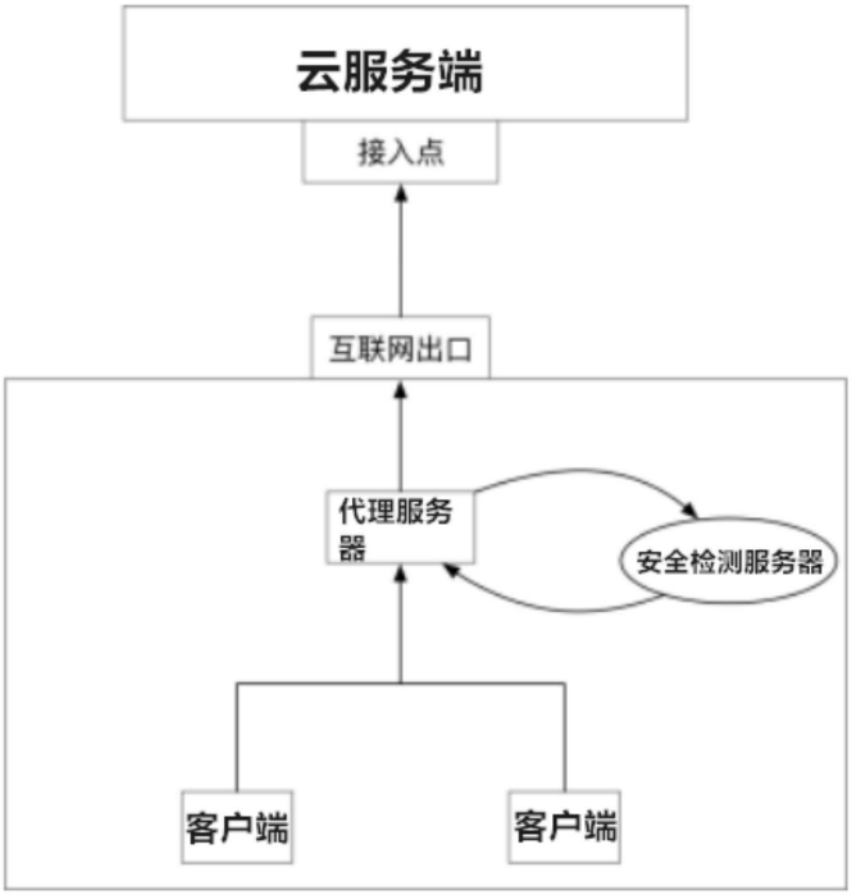

云服务端
接入点
互联网出口
代理服务器
安全检测服务器
客户端
客户端

图2

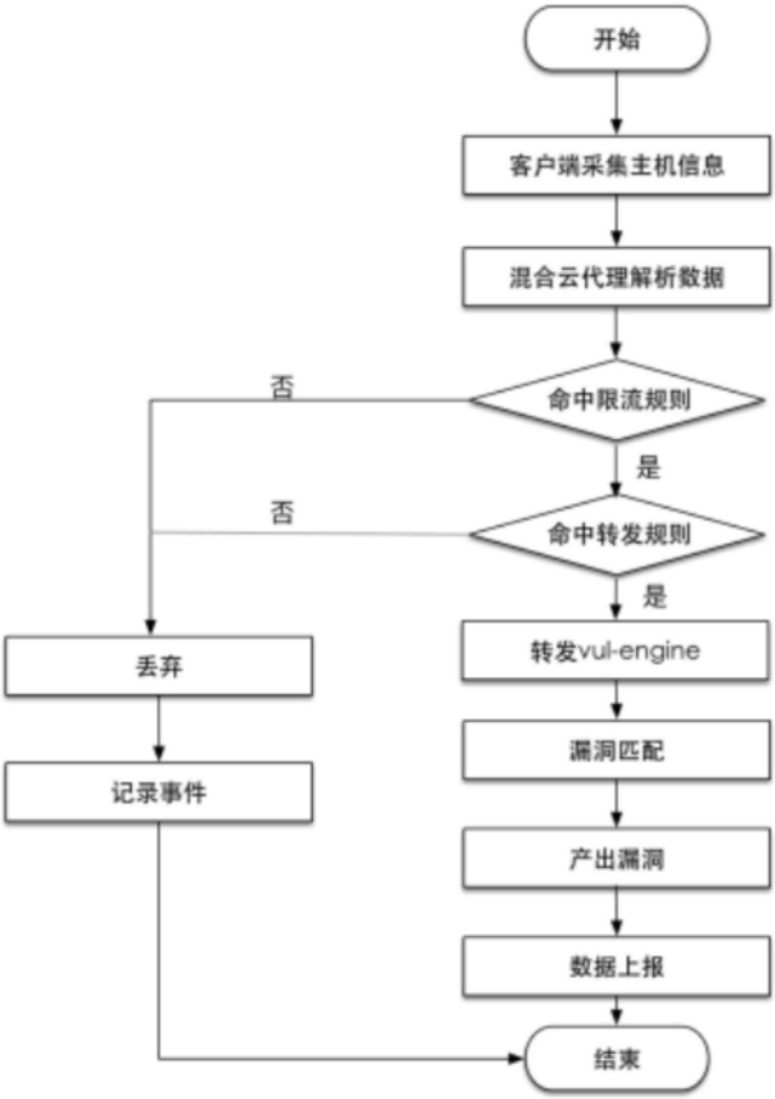

开始
客户端采集主机信息
混合云代理解析数据
命中限流规则
否
是
命中转发规则
否
是
丢弃
记录事件
转发vul-engine
漏洞匹配
产出漏洞
数据上报
结束

图3

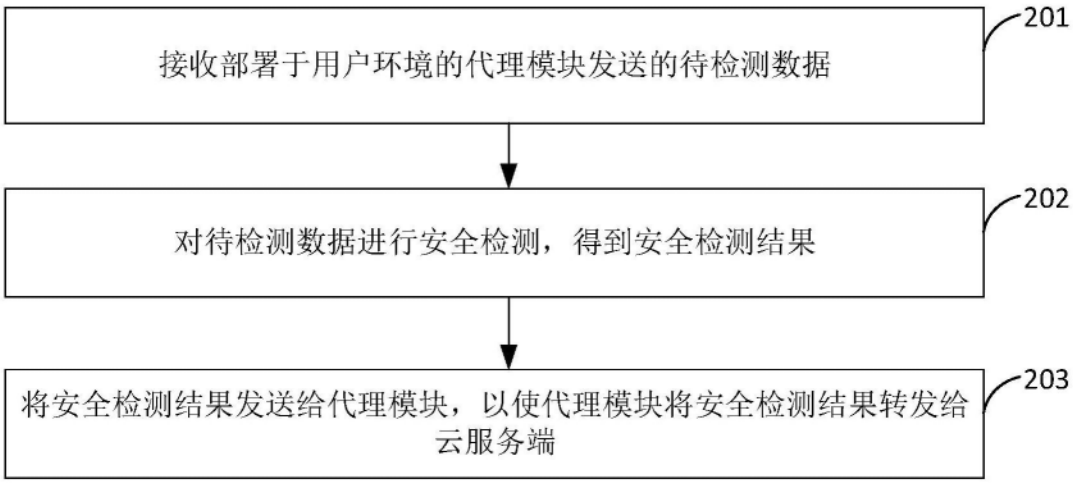

接收部署于用户环境的代理模块发送的待检测数据
201
对待检测数据进行安全检测，得到安全检测结果
202
将安全检测结果发送给代理模块，以使代理模块将安全检测结果转发给云服务端
203

图4

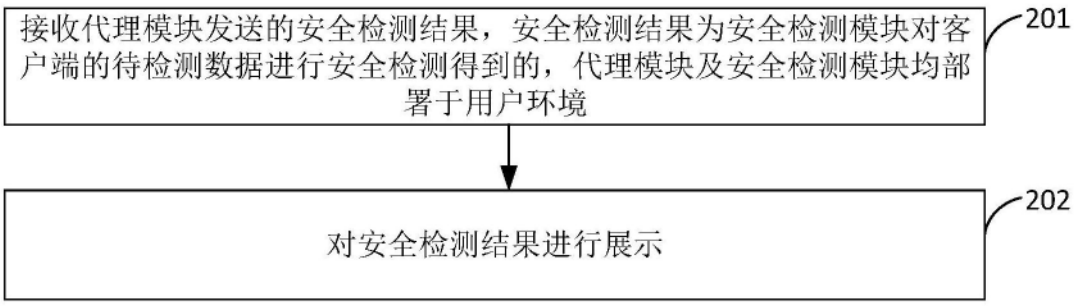

接收代理模块发送的安全检测结果，安全检测结果为安全检测模块对客户端的待检测数据进行安全检测得到的，代理模块及安全检测模块均部署于用户环境
201
对安全检测结果进行展示
202

图5

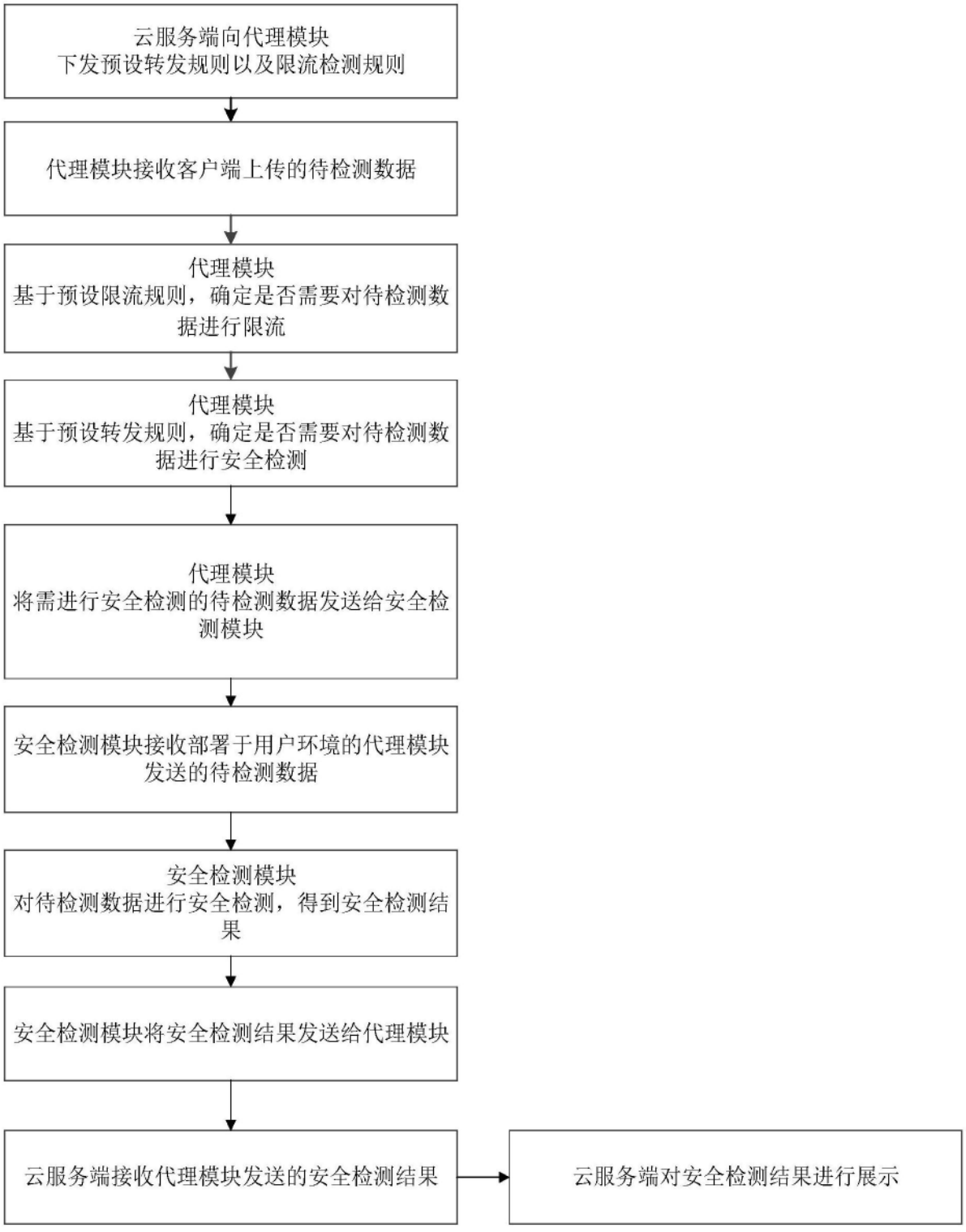

云服务端向代理模块
下发预设转发规则以及限流检测规则
代理模块接收客户端上传的待检测数据
代理模块
基于预设限流规则，确定是否需要对待检测数据进行限流
代理模块
基于预设转发规则，确定是否需要对待检测数据进行安全检测
代理模块
将需进行安全检测的待检测数据发送给安全检测模块
安全检测模块接收部署于用户环境的代理模块发送的待检测数据
安全检测模块
对待检测数据进行安全检测，得到安全检测结果
安全检测模块将安全检测结果发送给代理模块
云服务端接收代理模块发送的安全检测结果
云服务端对安全检测结果进行展示

图6

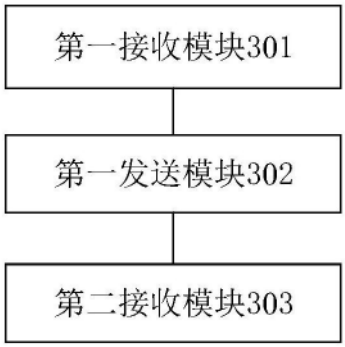

第一接收模块301
第一发送模块302
第二接收模块303

图7

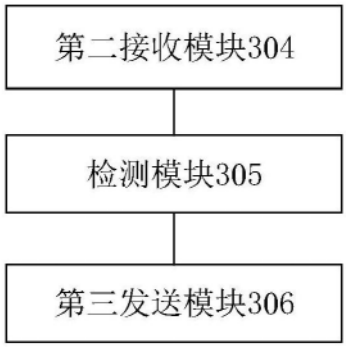

第二接收模块304
检测模块305
第三发送模块306

图8


第三接收模块307
展示模块308

图9

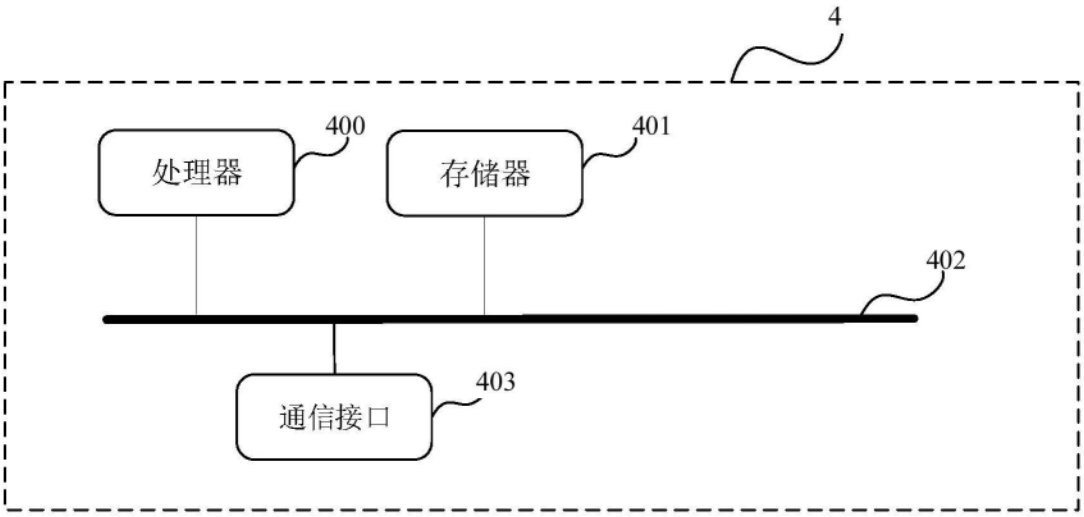


图10

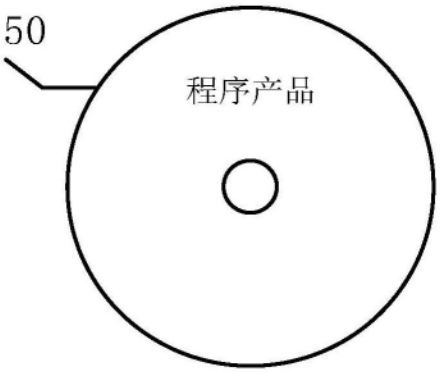


图11