(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 103491543 A
(43)申请公布日 2014.01.01

(21)申请号 201310461247.9

(22)申请日 2013.09.30

(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 倪杰 马齐

(74)专利代理机构 北京市浩天知识产权代理事务所 11276
代理人 宋菲 刘云贵

(51)Int.Cl.
H04W 12/12(2009.01)
H04L 29/06(2006.01)

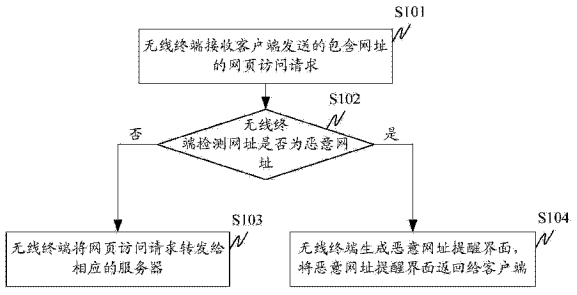
权利要求书2页 说明书10页 附图4页

(54)发明名称

通过无线终端检测恶意网址的方法、无线终端

(57)摘要

本发明公开了一种通过无线终端检测恶意网址的方法、无线终端。其中方法包括：无线终端接收客户端发送的包含网址的网页访问请求；无线终端通过查询固化在无线终端内的本地黑名单和/或本地白名单或者通过云端查询，检测网址是否为恶意网址；若无线终端检测出网址为恶意网址，则无线终端生成恶意网址提醒界面，而后将恶意网址提醒界面返回给客户端。本发明恶意网址检测功能是由无线终端来完成的，在一定情况下无线终端无需访问云端就可获知用户访问的网页是否为恶意网页，与将所有网址都去云端查询相比，本发明的检测效率更高。



CN 103491543 A

1. 一种通过无线终端检测恶意网址的方法，包括：

无线终端接收客户端发送的包含网址的网页访问请求；

所述无线终端通过查询固化在无线终端内的本地黑名单和/或本地白名单或者通过云端查询，检测所述网址是否为恶意网址；所述云端保存有及时更新的恶意网址库；

若所述无线终端检测出所述网址为恶意网址，则所述无线终端生成恶意网址提醒界面，而后将所述恶意网址提醒界面返回给所述客户端。

2. 根据权利要求 1 所述的方法，所述无线终端通过查询固化在无线终端内的本地黑名单和/或本地白名单或者通过云端查询，检测所述网址是否为恶意网址具体包括：

所述无线终端查询所述本地黑名单和/或本地白名单，判断所述网址是否属于所述本地黑名单和/或本地白名单；

若所述无线终端判断出所述网址属于所述本地黑名单，则检测出所述网址为恶意网址；

若所述无线终端判断出所述网址不属于所述本地黑名单和/或不属于所述本地白名单，则通过云端查询检测所述网址是否为恶意网址。

3. 根据权利要求 1 或 2 所述的方法，所述网页访问请求还包含用于反映客户端类型的信息；

所述无线终端生成恶意网址提醒界面具体包括：所述无线终端根据所述用于反映客户端类型的信息，确定所述客户端的类型；所述无线终端生成与所述客户端的类型对应的恶意网址提醒界面。

4. 根据权利要求 3 所述的方法，所述无线终端生成与所述客户端的类型对应的恶意网址提醒界面具体包括：

所述无线终端从服务器获取恶意网址的相关信息；

所述无线终端将所述恶意网址的相关信息插入到本地保存的恶意网址提醒界面模板中，生成所述恶意网址提醒界面。

5. 根据权利要求 3 所述的方法，所述用于反映客户端类型的信息为用户代理字符串或介质访问控制地址或动态主机配置协议信息。

6. 根据权利要求 1 所述的方法，在所述将恶意网址提醒界面返回给客户端之后还包括：

所述无线终端接收所述客户端发送的软件安装请求；

所述无线终端根据所述客户端的类型，向所述服务器请求软件安装页面或软件安装文件后返回给所述客户端。

7. 根据权利要求 1 所述的方法，所述无线终端向用户提供了用于启动/关闭恶意网址检测功能的设置接口；

在所述无线终端检测所述网址是否为恶意网址的步骤之前还包括：所述无线终端判断是否启动所述恶意网址检测功能；

若是，则所述无线终端执行检测所述网址是否为恶意网址的步骤。

8. 根据权利要求 1 所述的方法，所述恶意网址包括：钓鱼网址、欺诈网址、挂马网址或仿冒网址。

9. 一种无线终端，包括：

接收模块，用于接收客户端发送的包含网址的网页访问请求；

检测模块，用于通过查询固化在无线终端内的本地黑名单和／或本地白名单或者通过云端查询，检测所述网址是否为恶意网址；所述云端保存有及时更新的恶意网址库；

界面生成模块，用于在所述检测模块检测出所述网址为恶意网址的情况下，则生成恶意网址提醒界面，而后将所述恶意网址提醒界面返回给所述客户端。

10. 根据权利要求 9 所述的无线终端，所述检测模块包括：

查询单元，用于查询所述本地黑名单和／或本地白名单，判断所述网址是否属于所述本地黑名单和／或本地白名单，若判断出所述网址属于所述本地黑名单，则检测出所述网址为恶意网址；

云端查询请求单元，用于在所述查询单元判断出所述网址不属于所述本地黑名单和／或不属于所述本地白名单的情况下，通过云端查询检测所述网址是否为恶意网址。

通过无线终端检测恶意网址的方法、无线终端

技术领域

[0001] 本发明涉及互联网技术领域，具体涉及一种通过无线终端检测恶意网址的方法、无线终端。

背景技术

[0002] 钓鱼网站或者是欺诈网站等主要是通过仿冒真实网站的 URL 地址或是页面内容，伪装成银行及电子商务等类型的网站，或是利用真实网站服务器程序上的漏洞，在该网站的某些网页中插入危险的网页代码，以此来骗取用户银行或信用卡账号、密码等私人资料。钓鱼网页中包含着许多敏感的特征，例如，金融欺诈类的钓鱼网页会在文字、图片等方面仿冒官网，或是在真实网页中插入虚假票务、虚假中奖、假冒网银、虚假购物等信息，这些特征大多以文本串的形式出现在网页中。

[0003] 目前对钓鱼 / 欺诈网页识别的方法，主要是通过人工审核，以收集一些简单的钓鱼网页的文本特征，供浏览器插件依据这些文本特征对网页内容进行判断，过滤掉这些已报告的攻击网站。但是，现今钓鱼网页的存活期越来越短，新的钓鱼网页层出不穷，需要审核的网页量太大；并且钓鱼网页的特征变化加快，按照传统的人工审核的方式，提取信息的效率会比较低。因此，如何有效的检测钓鱼 / 欺诈网页的 URL 是业内一直比较关注的问题。

发明内容

[0004] 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上述问题的无线终端以及通过无线终端检测恶意网址的方法。

[0005] 根据本发明的一个方面，提供了一种通过无线终端检测恶意网址的方法，包括：无线终端接收客户端发送的包含网址的网页访问请求；无线终端通过查询固化在无线终端内的本地黑名单和 / 或本地白名单或者通过云端查询，检测网址是否为恶意网址；云端保存有及时更新的恶意网址库；若无线终端检测出网址为恶意网址，则无线终端生成恶意网址提醒界面，而后将恶意网址提醒界面返回给客户端。

[0006] 根据本发明的另一方面，提供了一种无线终端，包括：接收模块，用于接收客户端发送的包含网址的网页访问请求；检测模块，用于通过查询固化在无线终端内的本地黑名单和 / 或本地白名单或者通过云端查询，检测所述网址是否为恶意网址，云端保存有及时更新的恶意网址库；界面生成模块，用于在检测模块检测出网址为恶意网址的情况下，则生成恶意网址提醒界面，而后将恶意网址提醒界面返回给客户端。

[0007] 根据本发明提供的通过无线终端检测恶意网址的方法、无线终端，在客户端通过无线终端发起网页请求的过程中，利用无线终端检测用户想要访问的网页是否为恶意网址，如果检测出为恶意网址，则生成恶意网址提醒界面返回给客户端。客户端将恶意网址提醒界面展示给用户，用以提醒用户当前访问的网页为恶意网页，从而避免了用户因访问恶意网页遭受不必要的损失，保证网页访问的安全性。而且，本发明与现有技术的主要区别是恶意网址检测功能是由无线终端来完成的，在一定情况下无线终端无需访问云端就可获知

用户访问的网页是否为恶意网页，与将所有网址都去云端查询相比，本发明的检测效率更高。

[0008] 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

[0009] 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：

[0010] 图 1 示出了本发明实施例中包含客户端、无线终端和云端的系统架构图；

[0011] 图 2 示出了根据本发明的一个实施例的通过无线终端检测恶意网址的方法的流程图；

[0012] 图 3 示出了根据本发明的另一个实施例的通过无线终端检测恶意网址的方法的流程图；

[0013] 图 4 示出了本发明实施例中恶意网址提醒界面的一个例子的示意图；

[0014] 图 5 示出了本发明实施例中恶意网址提醒界面的另一个例子的示意图；

[0015] 图 6 示出了根据本发明一个实施例的无线终端的结构框图。

具体实施方式

[0016] 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。

[0017] 图 1 示出了本发明实施例中包含客户端、无线终端和云端的系统架构图。如图 1 所示，客户端 100 包括但不仅限于各种 PC、平板设备、智能手机、电视机等，无线终端 300 可以为各种无线接入设备，例如无线路由器、无线上网卡、安全网关等，无线终端 300 具有无线覆盖功能，在该无线终端 300 的覆盖范围内的客户端 100 都可以通过该无线终端 300 接入云端 200 网络。本发明基于该系统架构内云端 200 和无线终端 300 的联动用于检测恶意网址。

[0018] 图 2 示出了根据本发明的一个实施例的通过无线终端检测恶意网址的方法的流程图。如图 2 所示，该方法包括如下步骤：

[0019] 步骤 S101，无线终端接收客户端发送的包含网址的网页访问请求。

[0020] 由于客户端通过无线终端接入云端网络，所以当用户通过客户端发起网页访问时，客户端生成网页访问请求发送给无线终端，如果该网页为正常网页，应由无线终端将该网页访问请求转发给云端服务器。

[0021] 步骤 S102，无线终端通过查询固化在无线终端内的本地黑名单和 / 或本地白名单或者通过云端查询，检测网址是否为恶意网址，若是，则执行步骤 S104；否则，执行步骤 S103。

[0022] 本发明实施例中，恶意网址包括但不限于钓鱼网址、欺诈网址、挂马网址或仿冒网址。无线终端内预先固化了网址 URL 的本地黑名单和 / 或本地白名单。该本地黑名单和 / 或本地白名单可以是无线终端从云端下载下来的，进一步的，无线终端还可以定期向云端请求更新该本地黑名单和 / 或本地白名单。

[0023] 如果无线终端内仅固化有本地白名单，在无线终端接收到客户端上报的网页访问请求并从中提取出网址 URL 之后，判断该 URL 是否属于本地白名单，若是，则判定该网址为正常网址，执行步骤 S103 ；若否，则将该 URL 发送给云端，进行云端查询。

[0024] 如果无线终端内仅固化有本地黑名单，在无线终端接收到客户端上报的网页访问请求并从中提取出网址 URL 之后，判断该 URL 是否属于本地黑名单，若是，则判定该网址为恶意网址，执行步骤 S104 ；若否，则将该 URL 发送给云端，进行云端查询。

[0025] 如果无线终端内固化有本地白名单和本地黑名单，在无线终端接收到客户端上报的网页访问请求并从中提取出网址 URL 之后，判断该 URL 是否属于本地白名单和本地黑名单，若属于本地白名单，则判定该网址为正常网址，执行步骤 S103 ；若属于本地黑名单，则判定该网址为恶意网址，执行步骤 S104 ；若既不属于本地白名单也不属于本地黑名单，则将该 URL 发送给云端，进行云端查询。

[0026] 云端的主要工作包括 ：全网蜘蛛服务器集群爬取网页和接收客户端上报的网页。全网蜘蛛服务器集群的职责包括 ：①完成对已知活动网页的变化监测，其中活动网页的判断依据是看是否有人使用。②完成对新增 HOST 和网页的发现。③监测的变化信息和发现的新增网页及时推送给 HOST\URL 处理服务器。④日均监测的网页 200 亿，日均新发现网页量 10-20 亿。整个集群的任务处理量与做网页搜索服务是一个量级。对于全网蜘蛛服务器集群无法覆盖的网页，需要客户端上报来解决。

[0027] 上述接收爬取的网页和上报的网页的服务器是 HOST\URL 处理服务器。HOST\URL 处理服务器具有恶意网址库及其管理平台，主要工作包括 ：

[0028] ①接收和存储 Q3W 人工智能引擎的预判为黑的网址结果。Q3W 人工智能引擎预判的方法可以为 ：1）验明正身（网页快照）：如，金融欺诈网页会在文字、图片等方面仿冒官网。2）查家庭背景（服务器信息）：如，HOST 和 IP 下有恶意网页，那么当前网页是恶意的可能性极高。3）查祖上三代（ICP 备案信息、WHOIS 信息）：如，一个网页能售卖机票，但备案信息无票务经营，那么欺诈的可能性很大 ；再如，注册商名下网站经常出恶意网页，信任记录很差，那么新出的网页是恶意的概率比较高。

[0029] ②由于机器学习基本是每隔 15 分钟进行一轮。中间可能会出现除误报的情况，此时，需要恶意网址库更新记录，保持和引擎判断一致。

[0030] ③恶意网址库配套管理平台，方便人工增、删、改、查恶意网址。对于误报的网页，能够及时剔除。对于漏报的网页，能够强行入库。

[0031] ④恶意网址库的所有更改、实时同步到恶意网址云查询引擎。

[0032] 云端查询指的就是无线终端将 URL 上报给上述恶意网址云查询引擎，恶意网址云查询引擎判断该 URL 是否属于恶意网址库，若属于，则判定该 URL 为恶意网址，并将该判定结果返回给无线终端。

[0033] 进一步的，无线终端通过云端查询获知某个网址 URL 为恶意网址后，可以将该网址 URL 加入本地黑名单，这样在无线终端的无线覆盖范围内的客户端再次访问该 URL 时，无

需云端查询就可确定该 URL 为恶意网址。

[0034] 步骤 S103，无线终端将网页访问请求转发给相应的服务器。

[0035] 通过上述步骤 S102 判定网址不属于恶意网址，那么无线终端按照现有的方式将网页访问请求转发给相应的服务器，并将服务器反馈的网页返回给客户端，实现用户正常的网页访问。

[0036] 步骤 S104，无线终端生成恶意网址提醒界面，将恶意网址提醒界面返回给客户端。

[0037] 客户端接收到恶意网址提醒界面之后，将恶意网址提醒界面展示给用户，用以提醒用户当前访问的网页为恶意网页。

[0038] 根据本发明上述实施例提供的方法，在客户端通过无线终端发起网页请求的过程中，利用无线终端检测用户想要访问的网页是否为恶意网址，如果检测出为恶意网址，则生成恶意网址提醒界面返回给客户端。客户端将恶意网址提醒界面展示给用户，用以提醒用户当前访问的网页为恶意网页，从而避免了用户因访问恶意网页遭受不必要的损失，保证网页访问的安全性。而且，本发明与现有技术的主要区别是恶意网址检测功能是由无线终端来完成的，在一定情况下无线终端无需访问云端就可获知用户访问的网页是否为恶意网页，与将所有网址都去云端查询相比，本发明的检测效率更高。

[0039] 图 3 示出了根据本发明的另一个实施例的通过无线终端检测恶意网址的方法的流程图。如图 3 所示，该方法包括如下步骤：

[0040] 步骤 S201，无线终端接收客户端发送的包含网址的网页访问请求。

[0041] 由于客户端通过无线终端接入云端网络，所以当用户通过客户端发起网页访问时，客户端生成网页访问请求发送给无线终端，如果该网页为正常网页，应由无线终端将该网页访问请求转发给云端服务器。

[0042] 步骤 S202，无线终端通过查询固化在无线终端内的本地黑名单和 / 或本地白名单或者通过云端查询，检测网址是否为恶意网址，若是，则执行步骤 S204；否则，执行步骤 S203。关于本步骤的具体内容可参见上述实施例的描述，在此不再赘述。

[0043] 步骤 S203，无线终端将网页访问请求转发给相应的服务器，方法结束。

[0044] 通过上述步骤 S202 判定网址不属于恶意网址，那么无线终端按照现有的方式将网页访问请求转发给相应的服务器，并将服务器反馈的网页返回给客户端，实现用户正常的网页访问。

[0045] 步骤 S204，无线终端根据网页访问请求中所包含的用于反映客户端类型的信息，确定客户端的类型。

[0046] 本发明实施例中，网页访问请求中携带有用于反映客户端类型的信息。由于在一个无线终端的无线覆盖范围内可能包括多种不同类型的客户端，比如 PC、平板电脑、智能手机和电视机都属于不同类型。无线终端可以根据网页访问请求中携带的用于反映客户端类型的信息来判别当前发起网页访问的请求属于哪种类型。

[0047] 可选地，用于反映客户端类型的信息可以为用户代理字符串（User Agent）或介质访问控制地址（MAC）或动态主机配置协议信息（DHCP）。

[0048] 举例来说，用户通过浏览器访问网站时，浏览器会向云端服务器发送 UA，即 User Agent。它是一个特殊字符串头，使得云端服务器能够识别客户使用的操作系统及版本、CPU 类型、浏览器及版本、浏览器渲染引擎、浏览器语言、浏览器插件等。不同浏览器、同一浏览

器的不同版本、手机浏览器、电脑端的浏览器的 UA 是不一样的，因此无线终端通过 UA 能够判断客户端的类型。

[0049] 以 IE 的 User Agent 为例，其包括如下信息：

[0050] Compatible：相容性标志（“兼容”），是使用最先进的浏览器。它表明，互联网浏览器是一套通用的功能兼容。

[0051] Version token：该版本浏览器和识别标记包含版本号，例如版本“MSIE7.0”标记标识的 Internet Explorer 7。

[0052] Platform token：该平台令牌识别用户的操作系统，并包含版本号。例如平台“Windows NT 的 6.0”令牌表示 Windows Vista。

[0053] MAC 地址通常是由客户端生产厂家烧入的 EPROM（一种闪存芯片，通常可以通过程序擦写），MAC 地址就如同我们身份证上的身份证号码，具有全球唯一性。通过 MAC 地址中的生产厂家的信息也可以判定客户端类型。

[0054] DHCP 信息携带有客户端的操作系统的信息，根据该操作系统的信息也可以判定客户端的类型。

[0055] 步骤 S205，无线终端生成与客户端的类型对应的恶意网址提醒界面。

[0056] 本实施例中，对于不同的客户端类型，无线终端所生成的恶意网址提醒界面是不同的，这具体是与不同类型的客户端的显示屏幕的尺寸有关。图 4 示出了本发明实施例中恶意网址提醒界面的一个例子的示意图，图 5 示出了本发明实施例中恶意网址提醒界面的另一个例子的示意图。如果通过步骤 S204 确定的客户端的类型为智能手机，那么无线终端生成如图 4 所示的恶意网址提醒界面；如果通过步骤 S204 确定的客户端的类型为 PC、平板电脑或电视机，那么无线终端生成如图 5 所示的恶意网址提醒界面。需要说明的是，图 4 和图 5 仅为两个示例，本发明不仅限于此。

[0057] 具体地，无线终端本地保存有恶意网址提醒界面模板，不同类型的客户端可以对应不同的或相同的恶意网址提醒界面模板。无线终端从服务器获取恶意网址的相关信息，将恶意网址的相关信息插入到本地保存的恶意网址提醒界面模板中，生成恶意网址提醒界面。如图 4 和图 5 所示，用“下划线”标注的信息是从服务器获取的恶意网址的相关信息，没有用“下划线”标注的信息都属于恶意网址提醒界面模板的信息。可选地，无线终端本地保存的恶意网址提醒界面模板为 HTML 语言文件，无线终端将获取的恶意网址的相关信息以 JS 代码的方式复制到 HTML 语言文件的预定位置，即可实现上述插入处理。

[0058] 步骤 S206，无线终端将恶意网址提醒界面返回给客户端。

[0059] 客户端接收到恶意网址提醒界面之后，将恶意网址提醒界面展示给用户，用以提醒用户当前访问的网页为恶意网页。

[0060] 进一步的，如图 4 和图 5 所示，恶意网址提醒界面上还可呈现“安装安全软件”的链接。用户根据提示选择点击“安装安全软件”的链接，客户端根据用户的点击动作触发向无线终端发送软件安装的请求。在上述步骤 S206 之后，该方法还包括：

[0061] 步骤 S207，无线终端接收客户端发送的软件安装请求。

[0062] 步骤 S208，无线终端根据客户端的类型，向服务器请求软件安装页面或软件安装文件后返回给客户端。具体地，对于 PC，无线终端直接向服务器请求软件安装页面，例如软件官网，将软件安装页面返回给 PC；对于智能手机或平板电脑，无线终端可以直接向服务

器请求软件安装文件后返回给客户端。

[0063] 为了进一步完善无线终端所提供的恶意网址的检测功能，无线终端可以向用户提供用于启动 / 关闭恶意网址检测功能的设置接口。即，用户可以通过该设置接口来设置是否启动上述实施例提供的恶意网址检测功能。对于上述方法来说，在步骤 S102 或步骤 S202 之前，无线终端首先判断是否启动恶意网址检测功能。如果判断结果为是，则执行上述步骤 S102 或步骤 S202 ；如果判断结果为否，则不执行上述步骤 S102 或步骤 S202，无线终端按照现有的方法转发客户端和服务器交互的信息。

[0064] 根据本发明上述实施例提供的方法，在客户端通过无线终端发起网页请求的过程中，利用无线终端检测用户想要访问的网页是否为恶意网址，如果检测出为恶意网址，则生成恶意网址提醒界面返回给客户端。客户端将恶意网址提醒界面展示给用户，用以提醒用户当前访问的网页为恶意网页，从而避免了用户因访问恶意网页遭受不必要的损失，保证网页访问的安全性。而且，本发明与现有技术的主要区别是恶意网址检测功能是由无线终端来完成的，在一定情况下无线终端无需访问云端就可获知用户访问的网页是否为恶意网页，与将所有网址都去云端查询相比，本发明的检测效率更高。而且，无线终端通过判定客户端的类型，为不同类型的客户端提供不同的恶意网址提醒界面，使得本方法对各种类型的客户端都具有适用性。

[0065] 图 6 示出了根据本发明一个实施例的无线终端的结构框图。如图 6 所示，该无线终端包括 ：接收模块 301、检测模块 302、界面生成模块 303。

[0066] 接收模块 301，用于接收客户端发送的包含网址的网页访问请求。由于客户端通过无线终端接入云端网络，所以当用户通过客户端发起网页访问时，客户端生成网页访问请求发送给无线终端的接收模块 301，如果该网页为正常网页，应由无线终端将该网页访问请求转发给云端服务器。

[0067] 检测模块 302，用于通过查询固化在无线终端内的本地黑名单和 / 或本地白名单或者通过云端查询，检测网址是否为恶意网址。本发明实施例中，恶意网址包括但不限于钓鱼网址、欺诈网址、挂马网址或仿冒网址。无线终端内预先固化了网址 URL 的本地黑名单和 / 或本地白名单。该本地黑名单和 / 或本地白名单可以是无线终端从云端下载下来的，进一步的，无线终端还可以定期向云端请求更新该本地黑名单和 / 或本地白名单。

[0068] 进一步的，检测模块 302 包括 ：查询单元 304 和云端查询请求单元 305。

[0069] 查询单元 304，用于查询本地黑名单和 / 或本地白名单，判断网址是否属于本地黑名单和 / 或本地白名单，若判断出网址属于本地黑名单，则检测出网址为恶意网址。如果无线终端内仅固化有本地白名单，在接收模块 301 接收到客户端上报的网页访问请求并从中提取出网址 URL 之后，查询单元 304 判断该 URL 是否属于本地白名单，若是，则判定该网址为正常网址 ；若否，则由云端查询请求单元 305 将该 URL 发送给云端，进行云端查询。如果无线终端内仅固化有本地黑名单，在接收模块 301 接收到客户端上报的网页访问请求并从中提取出网址 URL 之后，查询单元 304 判断该 URL 是否属于本地黑名单，若是，则判定该网址为恶意网址 ；若否，则由云端查询请求单元 305 将该 URL 发送给云端，进行云端查询。如果无线终端内固化有本地白名单和本地黑名单，在接收模块 301 接收到客户端上报的网页访问请求并从中提取出网址 URL 之后，查询单元 304 判断该 URL 是否属于本地白名单和本地黑名单，若属于本地白名单，则判定该网址为正常网址 ；若属于本地黑名单，则判定该网

址为恶意网址；若既不属于本地白名单也不属于本地黑名单，则由云端查询请求单元 305 将该 URL 发送给云端，进行云端查询。

[0070] 云端查询请求单元305，用于在查询单元304判断出网址不属于本地黑名单和/或不属于本地白名单的情况下，通过云端查询检测网址是否为恶意网址。有关云端查询的描述可参见方法实施例。

[0071] 界面生成模块 303，用于在检测模块 302 检测出网址为恶意网址的情况下，则生成恶意网址提醒界面，而后将恶意网址提醒界面返回给客户端。

[0072] 进一步的，界面生成模块 303 包括：类型确定单元 306 和界面生成单元 307。

[0073] 类型确定单元 306 用于根据用于反映客户端类型的信息，确定客户端的类型。本发明实施例中，网页访问请求中携带有用于反映客户端类型的信息。由于在一个无线终端的无线覆盖范围内可能包括多种不同类型的客户端，比如 PC、平板电脑、智能手机和电视机都属于不同类型。类型确定单元 306 可以根据网页访问请求中携带的用于反映客户端类型的信息来判别当前发起网页访问的请求属于哪种类型。可选地，用于反映客户端类型的信息可以为用户代理字符串(User Agent)或介质访问控制地址(MAC)或动态主机配置协议信息(DHCP)。有关这些信息的描述可参见方法实施例。

[0074] 界面生成单元 307 用于生成与客户端的类型对应的恶意网址提醒界面。本实施例中，对于不同的客户端类型，界面生成单元 307 所生成的恶意网址提醒界面是不同的，这具体是与不同类型的客户端的显示屏幕的尺寸有关。具体可参见图 4 和图 5。界面生成单元 307 进一步用于：从服务器获取恶意网址的相关信息；将恶意网址的相关信息插入到本地保存的恶意网址提醒界面模板中，生成恶意网址提醒界面。具体地，无线终端本地保存有恶意网址提醒界面模板，不同类型的客户端可以对应不同的或相同的恶意网址提醒界面模板。界面生成单元 307 从服务器获取恶意网址的相关信息，将恶意网址的相关信息插入到本地保存的恶意网址提醒界面模板中，生成恶意网址提醒界面。如图 4 和图 5 所示，用“下划线”标注的信息是从服务器获取的恶意网址的相关信息，没有用“下划线”标注的信息都属于恶意网址提醒界面模板的信息。可选地，无线终端本地保存的恶意网址提醒界面模板为 HTML 语言文件，界面生成单元 307 将获取的恶意网址的相关信息以 JS 代码的方式复制到 HTML 语言文件的预定位置，即可实现上述插入处理。

[0075] 进一步的，如图 4 和图 5 所示，恶意网址提醒界面上还可呈现“安装安全软件”的链接。用户根据提示选择点击“安装安全软件”的链接，客户端根据用户的点击动作触发向无线终端发送软件安装的请求。接收模块 301 还用于接收客户端发送的软件安装请求。无线终端还包括：传输模块 308，用于根据客户端的类型，向服务器请求软件安装页面或软件安装文件后返回给客户端。具体地，对于 PC，传输模块 308 直接向服务器请求软件安装页面，例如软件官网，将软件安装页面返回给 PC；对于智能手机或平板电脑，传输模块 308 可以直接向服务器请求软件安装文件后返回给客户端。

[0076] 为了进一步完善无线终端所提供的恶意网址的检测功能，无线终端还包括：用户设置接口 309，是用于向用户提供启动/关闭恶意网址检测功能的接口。即，用户可以通过该用户设置接口 309 来设置是否启动上述实施例提供的恶意网址检测功能。上述检测模块 302 具体用于在判断出启动恶意网址检测功能的情况下，检测网址是否为恶意网址。

[0077] 根据本发明上述实施例提供的无线终端，在客户端通过无线终端发起网页请求的

过程中，利用无线终端检测用户想要访问的网页是否为恶意网址，如果检测出为恶意网址，则生成恶意网址提醒界面返回给客户端。客户端将恶意网址提醒界面展示给用户，用以提醒用户当前访问的网页为恶意网页，从而避免了用户因访问恶意网页遭受不必要的损失，保证网页访问的安全性。而且，本发明与现有技术的主要区别是恶意网址检测功能是由无线终端来完成的，在一定情况下无线终端无需访问云端就可获知用户访问的网页是否为恶意网页，与将所有网址都去云端查询相比，本发明的检测效率更高。而且，无线终端通过判定客户端的类型，为不同类型的客户端提供不同的恶意网址提醒界面，使得本方法对各种类型的客户端都具有适用性。

[0078] 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。

[0079] 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。

[0080] 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。

[0081] 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。

[0082] 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。

[0083] 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无线终端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。

[0084] 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。

[0085] 本发明公开了:A1、一种通过无线终端检测恶意网址的方法,包括:

[0086] 无线终端接收客户端发送的包含网址的网页访问请求;

[0087] 所述无线终端通过查询固化在无线终端内的本地黑名单和/或本地白名单或者通过云端查询,检测所述网址是否为恶意网址;所述云端保存有及时更新的恶意网址库;

[0088] 若所述无线终端检测出所述网址为恶意网址,则所述无线终端生成恶意网址提醒界面,而后将所述恶意网址提醒界面返回给所述客户端。

[0089] A2、根据A1所述的方法,所述无线终端通过查询固化在无线终端内的本地黑名单和/或本地白名单或者通过云端查询,检测所述网址是否为恶意网址具体包括:

[0090] 所述无线终端查询所述本地黑名单和/或本地白名单,判断所述网址是否属于所述本地黑名单和/或本地白名单;

[0091] 若所述无线终端判断出所述网址属于所述本地黑名单,则检测出所述网址为恶意网址;

[0092] 若所述无线终端判断出所述网址不属于所述本地黑名单和/或不属于所述本地白名单,则通过云端查询检测所述网址是否为恶意网址。

[0093] A3、根据A1或A2所述的方法,所述网页访问请求还包含用于反映客户端类型的信息;

[0094] 所述无线终端生成恶意网址提醒界面具体包括:所述无线终端根据所述用于反映客户端类型的信息,确定所述客户端的类型;所述无线终端生成与所述客户端的类型对应的恶意网址提醒界面。

[0095] A4、根据A3所述的方法,所述无线终端生成与所述客户端的类型对应的恶意网址提醒界面具体包括:

[0096] 所述无线终端从服务器获取恶意网址的相关信息;

[0097] 所述无线终端将所述恶意网址的相关信息插入到本地保存的恶意网址提醒界面模板中,生成所述恶意网址提醒界面。

[0098] A5、根据A3所述的方法,所述用于反映客户端类型的信息为用户代理字符串或介质访问控制地址或动态主机配置协议信息。

[0099] A6、根据A1所述的方法,在所述将恶意网址提醒界面返回给客户端之后还包括:

[0100] 所述无线终端接收所述客户端发送的软件安装请求;

[0101] 所述无线终端根据所述客户端的类型，向所述服务器请求软件安装页面或软件安装文件后返回给所述客户端。

[0102] A7、根据 A1 所述的方法，所述无线终端向用户提供了用于启动 / 关闭恶意网址检测功能的设置接口；

[0103] 在所述无线终端检测所述网址是否为恶意网址的步骤之前还包括：所述无线终端判断是否启动所述恶意网址检测功能；

[0104] 若是，则所述无线终端执行检测所述网址是否为恶意网址的步骤。

[0105] A8、根据 A1 所述的方法，所述恶意网址包括：钓鱼网址、欺诈网址、挂马网址或仿冒网址。

[0106] 本发明还公开了：B9、一种无线终端，包括：

[0107] 接收模块，用于接收客户端发送的包含网址的网页访问请求；

[0108] 检测模块，用于通过查询固化在无线终端内的本地黑名单和 / 或本地白名单或者通过云端查询，检测所述网址是否为恶意网址；所述云端保存有及时更新的恶意网址库；

[0109] 界面生成模块，用于在所述检测模块检测出所述网址为恶意网址的情况下，则生成恶意网址提醒界面，而后将所述恶意网址提醒界面返回给所述客户端。

[0110] B10、根据 B9 所述的无线终端，所述检测模块包括：

[0111] 查询单元，用于查询所述本地黑名单和 / 或本地白名单，判断所述网址是否属于所述本地黑名单和 / 或本地白名单，若判断出所述网址属于所述本地黑名单，则检测出所述网址为恶意网址；

[0112] 云端查询请求单元，用于在所述查询单元判断出所述网址不属于所述本地黑名单和 / 或不属于所述本地白名单的情况下，通过云端查询检测所述网址是否为恶意网址。

[0113] B11、根据 B9 或 B10 所述的无线终端，所述网页访问请求还包含用于反映客户端类型的信息；

[0114] 所述界面生成模块包括：

[0115] 类型确定单元，用于根据所述用于反映客户端类型的信息，确定所述客户端的类型；

[0116] 界面生成单元，用于生成与所述客户端的类型对应的恶意网址提醒界面。

[0117] B12、根据 B11 所述的无线终端，所述界面生成单元具体用于：从服务器获取恶意网址的相关信息；将所述恶意网址的相关信息插入到本地保存的恶意网址提醒界面模板中，生成所述恶意网址提醒界面。

[0118] B13、根据 B9 所述的无线终端，所述接收模块还用于接收所述客户端发送的软件安装请求；

[0119] 所述无线终端还包括：传输模块，用于根据所述客户端的类型，向所述服务器请求软件安装页面或软件安装文件后返回给所述客户端。

[0120] B14、根据 B9 所述的无线终端，还包括：用户设置接口，是用于向用户提供启动 / 关闭恶意网址检测功能的接口；

[0121] 所述检测模块具体用于在判断出启动恶意网址检测功能的情况下，检测所述网址是否为恶意网址。

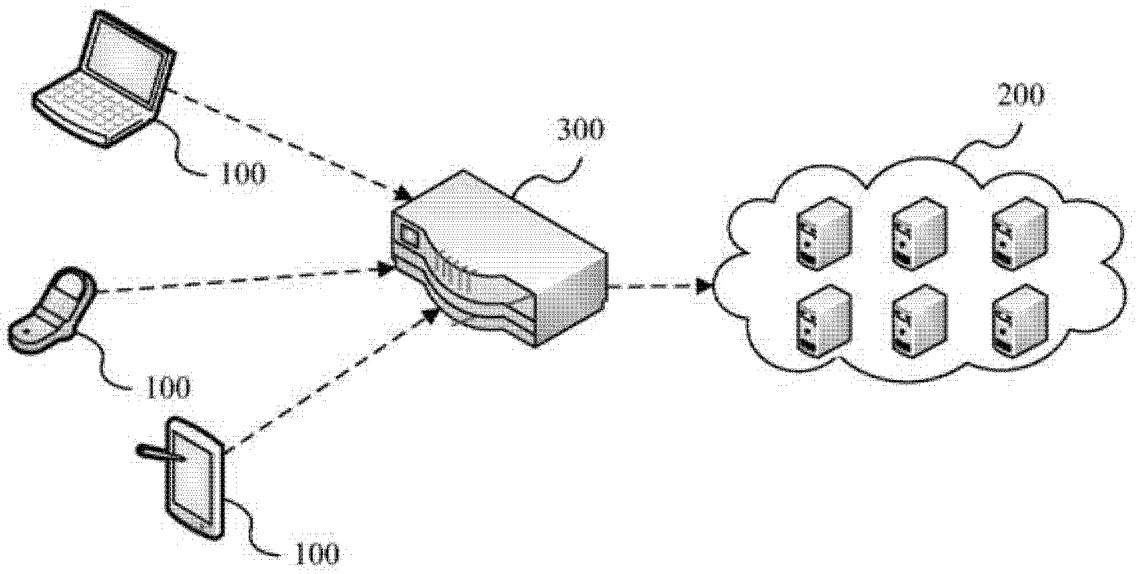

100
300
200
100
100

图 1

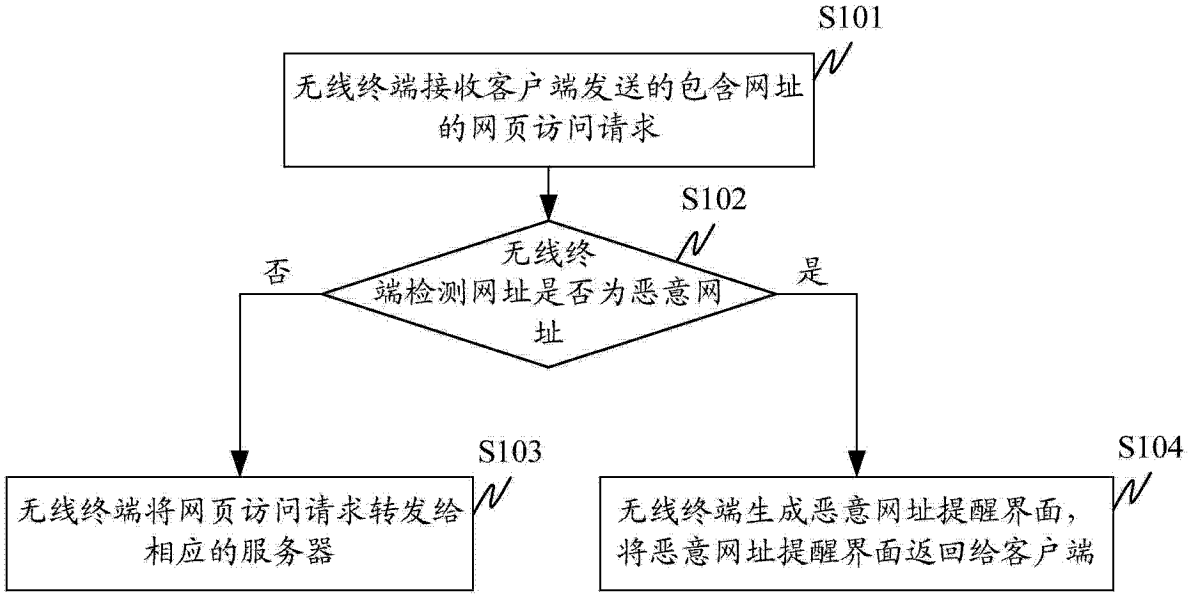

S101
无线终端接收客户端发送的包含网址的网页访问请求
S102
无线终端检测网址是否为恶意网址
否
是
S103
无线终端将网页访问请求转发给相应的服务器
S104
无线终端生成恶意网址提醒界面，将恶意网址提醒界面返回给客户端

图 2

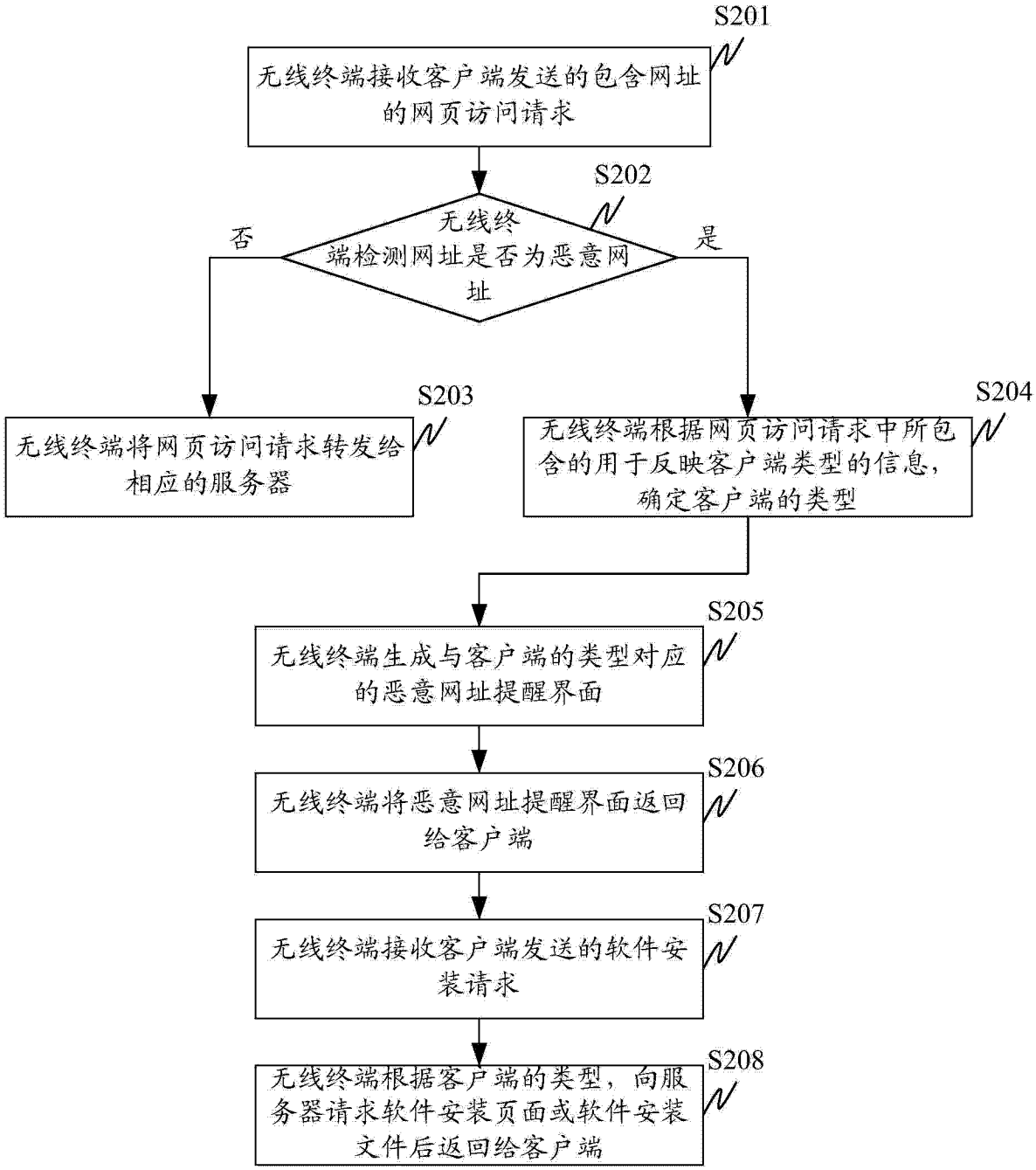

S201
无线终端接收客户端发送的包含网址的网页访问请求
S202
无线终端检测网址是否为恶意网址
否
是
S203
无线终端将网页访问请求转发给相应的服务器
S204
无线终端根据网页访问请求中所包含的用于反映客户端类型的信息，确定客户端的类型
S205
无线终端生成与客户端的类型对应的恶意网址提醒界面
S206
无线终端将恶意网址提醒界面返回给客户端
S207
无线终端接收客户端发送的软件安装请求
S208
无线终端根据客户端的类型，向服务器请求软件安装页面或软件安装文件后返回给客户端

图 3


无线终端提醒您
您当前访问的网站为:
钓鱼网站
您访问的网址为:
9999pt.com
忽略警告，继续访问
安装安全软件，保护您的移动生活

图 4


无线终端提醒您
经互联网安全中心确认，您访问的网站为:
虚假的金融证券网站
您访问的网址为:
Http://dribbble.com/slerts/776053-Activity-Prefile-UI-UX/attachment/77205
忽略警告，继续访问
安装安全软件
杀木马，防欺诈

图 5

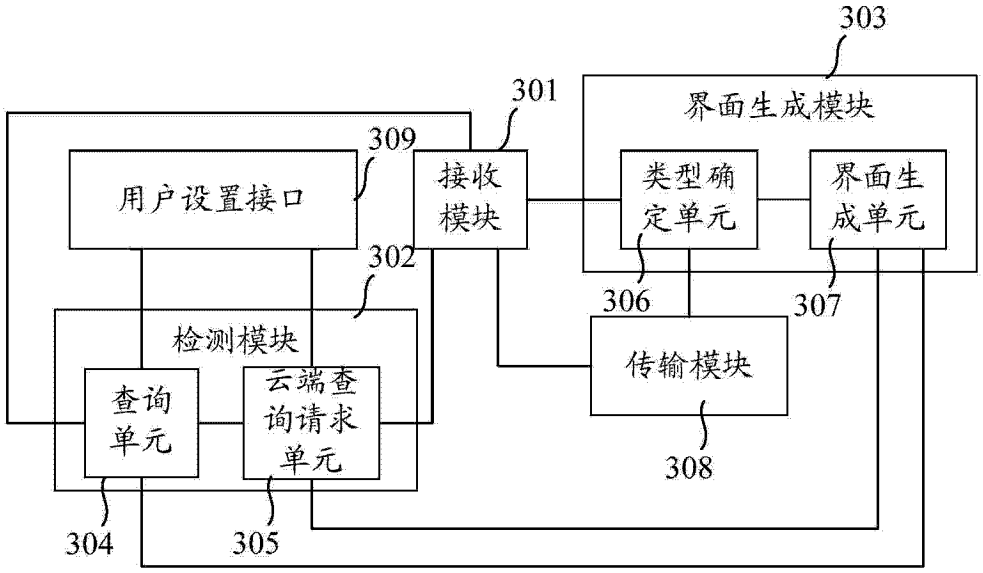

303
界面生成模块
301
309
用户设置接口
接收模块
类型确定单元
界面生成单元
302
306
307
检测模块
传输模块
查询单元
云端查询请求单元
308
304
305

图 6