(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 12 月 11 日 (11.12.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/194803 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2014/079076

(22) 国际申请日: 2014 年 6 月 3 日 (03.06.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310219053.8 2013 年 6 月 4 日 (04.06.2013) 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 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。

(72) 发明人: **孔庆龙 (KONG, Qinglong)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **姚彤 (YAO, Tong)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **张波 (ZHANG, Bo)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **刘智锋 (LIU, Zhifeng)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **江爱军 (JIANG, Aijun)**; 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 座-1111 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT,

[见续页]

(54) **Title**: CLOUD SECURITY-BASED FILE PROCESSING METHOD AND DEVICE

(54) **发明名称** : 基于云安全的文件处理方法及装置

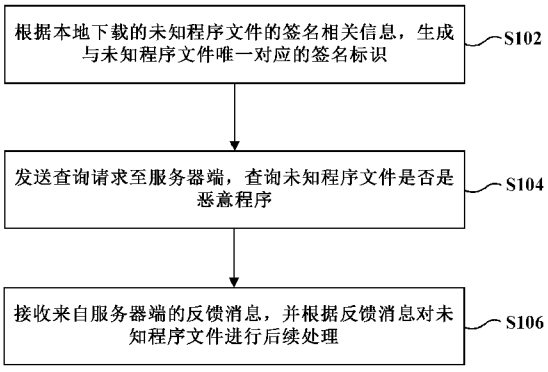

图 1/Fig.1

S102 According to signature relevant information about an unknown program file locally downloaded, generating a signature identifier uniquely corresponding to the unknown program file

S104 Sending a query request to a server end, to query whether the unknown program file is a malicious program or not

S106 Receiving a feedback message from the server end, and according to the feedback message, performing subsequent processing on the unknown program file

(57) **Abstract**: A cloud security-based file processing method and device. The method comprises: according to signature relevant information about an unknown program file locally downloaded, generating a signature identifier uniquely corresponding to the unknown program file; sending a query request to a server end, to query whether the unknown program file is a malicious program or not, wherein the query request carries the signature identifier of the unknown program file and some or all file features of the unknown program file; and receiving a feedback message from the server end, and according to the feedback message, performing subsequent processing on the unknown program file, wherein the server end generates the feedback message according to the signature identifier and the file features. The present invention solves the problem of breaking through the cloud killing by using a Trojan in the prior art and can reduce the time delay between discovering a malicious program and checking the malicious program as well, thereby accelerating the speed of attacking a newly arisen malicious program and reducing the information storage amount of the server, and thus guaranteeing the security of a client program.

(57) **摘要**:

[见续页]

WO 2014/194803 A1

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))。

一种基于云安全的文件处理方法及装置。该方法包括：根据本地下载的未知程序文件的签名相关信息，生成与未知程序文件唯一对应的签名标识；发送查询请求至服务器端，查询未知程序文件是否是恶意程序，其中，查询请求携带有未知程序文件的签名标识以及未知程序文件的部分或全部文件特征；接收来自服务器端的反馈消息，并根据反馈消息对未知程序文件进行后续处理，其中，服务器端根据签名标识以及文件特征生成反馈消息。解决了现有技术中利用木马突破云查杀的问题，同时也能够减少由发现恶意程序到查收恶意程序的时间，从而加快了对新生恶意程序的打击速度，也减少了服务器的信息存储量，进而保证了客户端程序的安全。

基于云安全的文件处理方法及装置

技术领域

本发明涉及信息安全领域，具体涉及基于云安全的文件处理方法及装置。

背景技术

目前，随着恶意程序的不断增长，传统的基于特征码查杀和定期更新病毒库的杀毒方式已经无法应对这种局面，这就促使了大量客户端跟踪、查杀恶意程序的云安全技术的兴起。

现有技术中的云安全技术大多采用客户端本地引擎与云安全服务器侧相结合的方式，具体通过如下方式对恶意程序进行查杀：

客户端本地引擎根据其内置的扫描位置进行扫描，并把本地无法识别的未知程序文件特征发送给云安全服务器，由云安全服务器对接收到的程序文件特征进行对比并判断是否为恶意程序，若为恶意程序，再由客户端本地引擎根据其预置的恶意程序处理方法对该恶意程序进行相应处理。

然而，恶意程序的作者在对抗安全软件时，恶意软件为了躲避安全防护软件的检测，会找到操作系统中新的可利用点或者找到安全软件所忽视的点，从而绕过安全软件的检测和查杀。这就需要安全厂商需要针对新兴的恶意程序样本进行分析，以对客户端安全软件进行更新。但是，在对安全软件升级的程中，恶意程序已经广泛蔓延。可见，现有技术的方法，并不能及时地对恶意程序进行检测和查杀。

发明内容

鉴于上述问题，本发明提供一种基于云安全的文件处理方法及装置，以便克服上述问题或者至少部分地解决上述问题。

依据本发明的一个方面，提供了一种基于云安全的文件处理方法，该方法包括：

根据本地下载的未知程序文件的签名相关信息，生成与未知程序文件唯一对应的签名标识；

发送查询请求至服务器端，查询未知程序文件是否是恶意程序，其中，查询请求携带有未知程序文件的签名标识以及未知程序文件的部分或全部文件特征；

接收来自服务器端的反馈消息，并根据反馈消息对未知程序文件进行后续处理，其中，服务器端根据签名标识以及文件特征生成反馈消息。

可选地，按照如下步骤获得签名相关信息以及文件特征，包括：

扫描未知程序文件，获取文件特征；

从文件特征中提取签名相关信息。

可选地，文件特征包括下列至少之一：

MD5（Message Digest Algorithm 5，消息摘要算法）、SHA1（Secure Hash Algorithm，哈希算法）、从文件中抽取部分内容计算出的特征值。

可选地，根据本地下载的未知程序文件的签名相关信息，生成与未知程序文件唯一对应的签名标识，包括：

获取可移植的执行体 PE 文件的可计算字段，可计算字段为 PE 文件中除去 PE 校验段、签名段以及签名内容剩余部分；

对可计算字段进行计算，将计算结果作为签名标识。

可选地，根据反馈消息进行后续处理，包括：

签名标识在服务器端匹配成功时，接收服务器端反馈的、与签名标识相对应的查杀方法。

可选地，接收服务器端反馈的查杀方式之后，包括：

从服务器端下载预设的、针对未知程序文件的信息参数的检测条件，判断未知程序文件是否满足检测条件；

将判断结果上传服务器端，并根据服务器端的指令执行后续处理。

可选地，检测条件包括下列至少一项：

PE 加载的特定文件是否具有特定公司的有效签名；

PE 加载的特定文件的内部名称、产品名称及公司名称是否为指定的名称；

系统中是否挂有特定的钩子；

特定的进程中是否具有特定的填充数据 Shellcode；

系统中是否有特定驱动模块或者设备对象存在；

特定的注册表是否指向特定的文件或者特定的唯一标识 CLSID 或者匹配特定的模式；

PE 加载的进程链中是否存在安全性未知的文件。

可选地，根据服务器端的指令执行后续处理，包括：

接收来自服务器端的未知程序文件可能感染恶意程序的提醒消息；和/或

接收来自服务器端的对未知程序文件进行查杀的查杀命令时，对未知程序文件进行查杀；和/或在接收到用户界面触发的查杀指令时，通过服务端对未知程序文件进行查杀。

可选地，查杀方法包括：扫描/判定动作和/或修复动作。

依据本发明的一个方面，还提供了一种基于云安全的文件处理方法，该方法包括：

接收来自客户端的查询请求，其中，查询请求包括未知程序文件的签名标识以及未知程序文件的部分或全部文件特征；

根据签名标识以及文件特征生成反馈消息；

将反馈消息发送至客户端，其中，客户端根据反馈消息对未知程序文件进行后

续处理。

可选地，将反馈消息发送至客户端，包括：

在数据库中，对签名标识进行匹配；

将匹配得到的查杀方法返回给客户端。

可选地，数据库包括：本地数据库和/或云端数据库。

可选地，接收来自客户端的查询请求之前，包括：接收来自客户端的、未知程序文件的文件特征。

可选地，将匹配得到的查杀方法返回给客户端之后，还包括：

将预设的、针对未知程序文件的信息参数的检测条件发送至客户端；以及

接收来自客户端的检测结果；

根据检测结果发送相应指令。

可选地，根据检测结果发送相应指令，包括：

根据检测结果发送未知程序文件可能感染恶意程序的提醒消息至客户端；和/或

根据检测结果发送相应命令，其中，相应命令包括对未知程序文件进行查杀的查杀命令，以及，对安全文件进行放行的命令。

根据本发明的另一方面，提供了一种基于云安全的文件处理装置，该装置包括：

生成模块，配置为根据本地下载的未知程序文件的签名相关信息，生成与未知程序文件唯一对应的签名标识；

查询模块，配置为发送查询请求至服务器端，查询未知程序文件是否是恶意程序，其中，查询请求携带有未知程序文件的签名标识以及未知程序文件的部分或全部文件特征；

处理模块，配置为接收来自服务器端的反馈消息，并根据反馈消息对未知程序文件进行后续处理，其中，服务器端根据签名标识以及文件特征生成反馈消息。

可选地，上述装置还包括：

提取模块，配置为扫描未知程序文件，获取文件特征；从文件特征中提取签名相关信息。

可选地，文件特征包括下列至少之一：

MD5、SHA1、从文件中抽取部分内容计算出的特征值。

可选地，生成模块还配置为：

获取可移植的执行体 PE 文件的可计算字段，可计算字段为 PE 文件中除去 PE 校验段、签名段以及签名内容剩余部分；

对可计算字段进行计算，将计算结果作为签名标识。

可选地，处理模块还配置为：

签名标识在服务器端匹配成功时，接收服务器端反馈的、与签名标识相对应的

查杀方法。

可选地，处理模块还配置为：

从服务器端下载预设的、针对未知程序文件的信息参数的检测条件，判断未知程序文件是否满足检测条件；

将判断结果上传服务器端，并根据服务器端的指令执行后续处理。

可选地，处理模块还配置为：

接收来自服务器端的未知程序文件可能感染恶意程序的提醒消息；和/或

接收来自服务器端的对未知程序文件进行查杀的查杀命令时，对未知程序文件进行查杀；和/或

在接收到用户界面触发的查杀指令时，通过服务端对未知程序文件进行查杀。

可选地，查杀方法包括：对未知程序文件进行扫描/判定动作和/或修复动作。

根据本发明的另一方面，还提供了一种基于云安全的文件处理装置，该装置包括：

接收模块，配置为接收来自客户端的查询请求，其中，查询请求包括未知程序文件的签名标识以及未知程序文件的部分或全部文件特征；

发送模块，配置为根据签名标识以及文件特征生成反馈消息，并将反馈消息发送至客户端，其中，客户端根据反馈消息对未知程序文件进行后续处理。

可选地，发送模块包括：

匹配单元，配置为在数据库中，对签名标识进行匹配；

发送单元，配置为将匹配得到的查杀方法发送给客户端。

可选地，数据库包括：本地数据库和/或云端数据库。

可选地，接收模块还配置为接收来自客户端的、未知程序文件的文件特征。

可选地，发送模块，还配置为预设的、针对未知程序文件的信息参数的检测条件发送至客户端；以及

接收模块，还配置为接收来自客户端的检测结果；

发送模块，还配置为根据检测结果发送相应指令。

可选地，发送模块还配置为：

根据检测结果发送未知程序文件可能感染恶意程序的提醒消息至客户端；和/或

根据检测结果发送相应命令，其中，相应命令包括对未知程序文件进行查杀的查杀命令，以及，对安全文件进行放行的命令。

根据本发明的又一个方面，提供了一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 1-9 中的任一个所述的基于云安全的文件处理方法，和/或，根据权利要求 10-15 任一个所述的基于云安全的文件处理方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了如上所述

的计算机程序。

本发明的有益效果为：

本发明提供的了一种基于云安全的文件处理方法及装置。通过本发明，使得客户端能够及时获取到本地的未知程序文件，并生成与该程序文件唯一对应的签名标识发送给服务器端，服务器端能够根据接收的签名标签获取对应的反馈消息并返回给客户端，客户端根据反馈消息对该未知程序文件进行相应地处理。

可见，本发明提供的方法及装置使得客户端能够实时地、动态地从服务器侧获取针对未知程序文件的处理方法，并能够及时地对恶意程序进行查杀，解决了现有技术中利用木马突破云查杀的问题。另外，与现有技术中，通过升级本地特征库和引擎程序文件才能检测并查杀新生恶意程序相比，本发明还减少了由发现恶意程序到查杀恶意程序的时间，从而加快了对新生恶意程序的打击速度，也减少了服务器的信息存储量，进而保证了客户端程序的安全。

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 示出了根据本发明一个实施例的一种基于云安全的文件处理方法流程图；

图 2 示出了根据本发明一个实施例的另一种基于云安全的文件处理方法流程图以及

图 3 示出了根据本发明另一个实施例的一种基于云安全的文件处理方法流程图；

图 4 示出了根据本发明一个实施例的一种基于云安全的文件处理装置结构框图；

图 5 示出了根据本发明一个实施例的另一种基于云安全的文件处理装置结构框图；

图 6 示意性地示出了用于执行根据本发明的基于云安全的文件处理方法的计算设备的框图；以及

图 7 示意性地示出了用于保持或者携带实现根据本发明的基于云安全的文件处理方法的程序代码的存储单元。

具体实施方式

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。

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。

本发明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。

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连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。

实施例一

图 1 出示了根据本发明一个实施例的一种基于云安全的文件处理方法流程图。在该方法中，对用于处理本地程序的客户端进行了改进，该方法具体包括步骤 S102 至 S106。

S102，根据本地下载的未知程序文件的签名相关信息，生成与未知程序文件唯一对应的签名标识。

S104，发送查询请求至服务器端，查询未知程序文件是否是恶意程序。其中，查询请求携带有未知程序文件的签名标识以及未知程序文件的部分或全部文件特征。

其中，本实施例中的文件特征可以包括文件的 MD5 值、SHA1 值，或者是从文件中抽取部分内容计算出的特征值。还可以包括该文件可能加载的 DLL（Dynamic Link Library，动态链接库）信息及 DLL 的描述信息，该文件是否被木马感染成一个安全性未知的或者危险的文件；或者包括判断指定文件/目录是否存在，文件属性是否满足条件（如文件的 MD5 是否为指定的值），指定注册表键/值是否存在，注册表键/值内容是否满足条件，指定进程/服务是否存在等。

其中，服务器端预先保存有文件特征值和安全级别信息的对应关系，服务器端确定的安全级别信息可以自定义，例如包括安全、危险、未知等级别，也可以采用

一级、二级、三级等方式来进行区分，只要能够体现出各模块是否安全状态即可。或者，所述安全级别信息包括：安全等级、未知等级、可疑等级、高度可疑等级和恶意等级，其中，恶意等级为最高等级，安全等级为最低等级。例如，可以设置等级为 10-20 时为安全等级，等级为 30-40 时为未知等级，等级为 50-60 时为可疑等级和高度可疑等级，等级大于 70 时为恶意等级。

S106，接收来自服务器端的反馈消息，并根据反馈消息对未知程序文件进行后续处理。其中，服务器端根据签名标识以及文件特征生成反馈消息。

本实施例中，反馈消息为服务器端反馈的、与所述签名标识相对应的查杀方法，以使客户端能够根据该查杀方法对未知文件进行相应处理。

本发明实施例提供的基于云安全的文件处理方法，使得客户端能够及时获取到本地的未知程序文件，并生成与该程序文件唯一对应的签名标识发送给服务器端，并从服务器端获取对应的反馈消息，并根据反馈消息对该未知程序文件进行相应地处理。

可见，本发明实施例提供的方法使得客户端能够实时地、动态地从服务器侧获取针对未知程序文件的处理方法，并能够及时地对恶意程序进行查杀，解决了现有技术中利用木马突破云查杀的问题。另外，与现有技术中，通过升级本地特征库和引擎程序文件才能检测并查杀新生恶意程序相比，本方法还减少了由发现恶意程序到查杀恶意程序的时间，从而加快了对新生恶意程序的打击速度，也减少了服务器的信息存储量，进而保证了客户端程序的安全。

相应地，图 2 出示了根据本发明一个实施例的另一种基于云安全的文件处理方法流程图。在该方法中，对用于查杀恶意程序的服务器进行了改进，该服务器为上述客户端的云安全服务器，该方法具体包括步骤 S202 至 S206。

S202，接收来自客户端的查询请求。其中，查询请求包括未知程序文件的签名标识以及未知程序文件的部分或全部文件特征。本实施例中的文件特征已经在上述方法中进行过具体介绍，在此不再赘述。

S204，根据签名标识以及文件特征生成反馈消息。

S206，将反馈消息发送至客户端。其中，客户端根据反馈消息对未知程序文件进行后续处理。

例如，本实施例中，当客户端迅雷 ThundPlatform.exe 加载 minizip.dll(minizip.dll 被替换成木马)，且检测到 minizip 非白文件（也成白程序或可信程序），时，由服务器返回删除木马的命令，执行修复迅雷软件的操作，可以由客户端执行该操作。

本发明实施例提供的基于云安全的文件处理方法，使得服务器能够根据客户端发送的未知程序文件的签名标签获取对应的反馈消息，且返回给客户端，并由客户端根据反馈消息对该未知程序文件进行相应地处理。

可见，本发明实施例提供的方法使得服务器能够实时地、动态地获取针对客户

端未知程序文件的处理方法，并由客户端对恶意程序进行查杀，解决了现有技术中利用木马突破云查杀的问题。另外，与现有技术中，通过升级本地特征库和引擎程序文件才能检测并查杀新生恶意程序相比，本方法还减少了由发现恶意程序到查杀恶意程序的时间，从而加快了对新生恶意程序的打击速度，也减少了服务器的信息存储量，进而保证了客户端程序的安全。

实施例二

本实施例为上述实施例一的一种具体应用场景，通过本实施例，能够更加清楚、具体地阐述本发明所提供的方法。

图 3 出示了本发明一个实施例的一种基于云安全的文件处理方法流程图。该方法具体包括步骤 S302 至 S316。

S302，客户端根据本地下载的未知程序文件的签名相关信息，生成与未知程序文件唯一对应的签名标识。

需要说明的是，本实施例中，客户端在执行本地程序文件时，会判断每个程序文件是否为本地可知程序文件，以保证客户端对本地程序的可知性，同时也确保了本地程序的安全性。其中，客户端中会存储有程序文件列表，当所扫描到的程序文件不在程序文件列表中时，客户端判定该程序文件为未知程序文件。

可选地，该步骤的具体实现方式包括：

首先，扫描该未知程序文件，获取其文件特征。

其中，文件特征已在上述实施例中进行过具体介绍，在此不再赘述。

其次，从获取的文件特征中提取签名相关信息。

其中，签名相关信息为文件特征的可计算字段，可计算字段包括 PE 文件中除去 PE 校验段、签名段以及签名内容剩余部分。其中，当获取的上述文件长度未达到 8 的整数倍时，将其所差的位数用 0 补齐，以便于对其进行计算。

再次，对可计算字段进行计算，将计算结果作为签名标识。

可选地，本实施例中，将可计算字段作为摘要值，采用 SHA1 算法对其进行计算，得到与未知程序文件唯一对应的签名标识。

客户端在生成未知程序文件的签名标识后，执行步骤 S304，即发送查询请求至服务器端。其中，查询请求携带有该未知程序文件的签名标识以及该未知程序文件的部分或全部文件特征。

服务器端接收到查询请求后，执行步骤 S306，即在数据库中对查询请求中的签名标识进行匹配，获取与签名标识相对应的查杀方法。

需要说明的是，本实施例中的数据库包括本地数据库和/或云端数据库。

可选地，本实施例中的查杀方法可以包括扫描/判定动作和修复动作等。其中，扫描/判定动作包括对程序文件属性及程序文件的上下文环境的扫描和判定，并当判

定为恶意程序时，执行相应的修复操作。可选地，该修复操作可以包括删除指定的注册表键/值、修改注册表键/值为指定内容、删除指定系统服务项、修复/删除指定程序文件等，还包括引导用户启动急救箱等，例如，在急救箱的模式下对恶意程序进行查杀，采用计算机基本输入输出系统→硬盘主引导记录→操作系统驱动层→操作系统应用层的多层检测和清除方式，从底层开始对病毒进行检测和清除处理，可以确保彻底清除存在于应用层到驱动层各层中的病毒，提高了检测和清除计算机病毒的能力，保证了计算机系统的安全。

S308，服务器将匹配得到的查杀方法发送给客户端。

客户端接收到服务器发送的查杀方法后，执行步骤 S310，即从服务器侧下载针对未知程序文件的信息参数的检测条件。其中，检测条件由服务器侧根据接收到的未知程序文件信息参数（如文件特征）生成。

客户端下载到检测条件后，执行步骤 S312，即判断该未知程序文件是否满足检测条件，并将判断结果发送至服务器。

可选地，本实施例中的检测条件至少包括如下列举的一种：

1）PE 加载的特定文件是否具有特定公司的有效签名。2）PE 加载的特定文件的内部名称、产品名称及公司名称是否为指定的名称。3）系统中是否挂有特定的钩子。4）特定的进程中是否具有特定的填充数据。5）系统中是否有特定驱动模块或者设备对象存在，其中，特定的驱动模块或者设备对象是指由本地未知程序所加载的驱动模块或者设备对象。6）特定的注册表是否指向特定的文件或者特定的 CLSID 或者匹配特定的模式，其中，特定的注册表、特定的文件、特定的 CLSID 及特定的模式均由未知程序在加载时生成，当该程序运行时，由特定的注册表利用该特定的文件和特定的 CLSID 在特定的模式下运行该程序。7）PE 加载的进程链中是否存在本地未知的文件（未能判断安全等级是否为可信的文件，主要根据每个文件对应的文件安全等级判断）等。PE 加载的进程链主要是需要分析进程链信息。

进程链包括运行所述程序操作的所有父子进程，例如，一种进程链的示例为：进程 1→进程 2→进程 3，即所述进程 2 为进程 3 的父进程，进程 1 为进程 2 的父进程，进程 2 为进程 1 的子进程，进程 3 为进程 2 的子进程。提取进程链上所有进程的名称，确定是否存在本地未知的文件。关于父进程和子进程，创建一个进程时，被创建的函数就是创建函数的子进程。所述进程的信息还可以包括其他信息，例如会话 ID、优先级、拥有的线程、用户 ID、句柄、进程内存计数器、进程路径、进程命令行参数、进程名称、进程创建者、创建时间、退出时间、内核时间等，本发明对此不再详细介绍。从当前进程开始，依据所述创建关系追溯对应所述当前进程的进程链，依次在该进程链中查找该进程的每一级父进程，并获取所述父进程的文件等级；根据获取到的文件等级从而可以获知 PE 加载的进程链中是否存在本地未知的文件。

对于上述第一类检测条件，可以查询到例如暴风影音 StoreUpdate.exe 加载 StormUpdate.dll,StormUpdated.dll 具有“北京暴风网际科技有限公司”的签名信息。

对于上述第二类检测条件，例如检测到加载 kernel32.dll 内部名称为 kernel32, 公司名称为 microsoft，产品名称为 Microsoft@Windows@Operating System 等。

对于上述系统中是否挂有特定的钩子这种检测条件，例如关机回调钩子函数，是 windows 关机时会调用的一个或多个回调函数，木马注册后，可以在关机时将自身从内存写到磁盘并设置自启动，以便下次开机仍然能够加载。 常见的一个木马样本 Unifade 就是通过注册关机回调钩子反复感染的。

又例如，对于上述系统中是否有特定驱动模块或者设备对象存在的检测条件，svchost.exe 是个常见的系统服务进程，木马会将自身模块远程注入到该进程中，并将自身的文件删除，达到隐形的目的，关机时在将自身写入到磁盘中以便下次开机加载。 分析人员可以根据木马的特征提取一些二进制串，用这些二进制串和 svchost.exe 进程的内存进行匹配从而发现木马。

又例如，对于上述特定的注册表是否指向特定的文件或者特定的 CLSID 或者匹配特定的模式的检测条件，特定的注册表，比如鬼影木马感染 fips.sys 驱动程序，fips 驱动程序是通过 HKLM\SYSTEM\CurrentControlSet\Services\Fips 键加载的，从而检测到 fips.sys 被感染，同时存在\Driver\fips 对象，可以作为鬼影木马病毒存在的判断条件。等等。

当服务器接收到检测结果后，执行步骤 S314，即根据检测结果获取相应的指令，并将该指令发送给客户端。

可选地，服务器侧保存有一个指令列表或指令数据库，存储有针对不同的检测结果的处理指令。例如，当服务器根据接收到的检测结果判定该未知程序文件为恶意文件时，可以发送未知程序文件可能感染恶意程序的提醒消息给客户端，还可以发送对该未知程序文件进行查杀的指令。当服务器根据接收到的检测结果判定该未知程序文件为安全文件时，向客户端发送安全文件进行放行的命令。

客户端接收到服务器发送的指令后，执行步骤 S316，即根据获取的指令对该未知程序文件进行后续处理。

可选地，本实施例中，当客户端接收到的指令为未知程序文件可能感染恶意程序的提醒消息时，可以向用户显示该未知程序文件可能感染恶意程序的提示信息，便于用户对该程序文件进行操作。例如，用户可以根据提示消息选择对该程序文件进行查杀，此时，客户端接收到用户触发的查杀指令后，将该程序文件交由服务器侧进行查杀。减少了客户端对文件的查杀操作，增加客户端的处理速度。

当客户端接收到的指令为查杀指令时，直接根据该指令对该未知程序文件进行查杀，保证了对恶意程序进行及时地查杀。

本发明提供了一种基于云安全的文件处理方法。通过该方法，使得客户端能够

及时获取到本地的未知程序文件，并生成与该程序文件唯一对应的签名标识发送给服务器端，服务器端能够根据接收的签名标签获取对应的反馈消息并返回给客户端，客户端根据反馈消息对该未知程序文件进行相应地处理。

可见，本发明实施例提供的方法使得客户端能够实时地、动态地从服务器侧获取针对未知程序文件的处理方法，并能够及时地对恶意程序进行查杀，解决了现有技术中利用木马突破云查杀的问题。例如，解决了木马使用 DLL 劫持技术将木马 DLL 与可信任的白程序打包在一起，当用户执行白程序时，木马 DLL 会被加载的问题。

另外，与现有技术中，通过升级本地特征库和引擎程序文件才能检测并查杀新生恶意程序相比，本方法还减少了由发现恶意程序到查杀恶意程序的时间，从而加快了对新生恶意程序的打击速度，也减少了服务器的信息存储量，进而保证了客户端程序的安全。本方法可有效应用于应用层或者驱动层感染的病毒，涉及的可以处理的病毒包括计算机病毒（包括一般感染性病毒、Word 和 Excel 宏病毒、引导区病毒、脚本病毒、木马、后门程序、键盘记录器、密码盗取者等等）统称为“计算机病毒”。

实施例三

图 4 出示了本发明一个实施例的一种基于云安全的文件处理装置的结构框图。该装置执行于客户端的引擎中。该装置安全性未知的 0 包括：

生成模块 410，配置为根据本地下载的未知程序文件的签名相关信息，生成与未知程序文件唯一对应的签名标识；

查询模块 420，与上述生成模块 410 相耦合，配置为发送查询请求至服务器端，查询未知程序文件是否是恶意程序，其中，查询请求携带有未知程序文件的签名标识以及未知程序文件的部分或全部文件特征；

处理模块 430，与上述生成模块 420 相耦合，配置为接收来自服务器端的反馈消息，并根据反馈消息对未知程序文件进行后续处理，其中，服务器端根据签名标识以及文件特征生成反馈消息。

可选地，上述装置还包括：

提取模块 440，与上述生成模块 410 相耦合，配置为扫描未知程序文件，获取文件特征；

从文件特征中提取签名相关信息。

可选地，文件特征包括下列至少之一：

MD5、SHA1、从文件中抽取部分内容计算出的特征值。

可选地，上述生成模块 410 还配置为：

获取可移植的执行体 PE 文件的可计算字段，可计算字段为 PE 文件中除去 PE 校验段、签名段以及签名内容剩余部分；

对可计算字段进行计算，将计算结果作为签名标识。

可选地，上述处理模块 430 还配置为：

签名标识在服务器端匹配成功时，接收服务器端反馈的、与签名标识相对应的查杀方法。

可选地，上述处理模块 430 还配置为：

从服务器端下载预设的、针对未知程序文件的信息参数的检测条件，判断未知程序文件是否满足检测条件；

将判断结果上传服务器端，并根据服务器端的指令执行后续处理。

可选地，上述处理模块 430 还配置为：

接收来自服务器端的未知程序文件可能感染恶意程序的提醒消息；和/或

接收来自服务器端的对未知程序文件进行查杀的查杀命令时，对未知程序文件进行查杀；和/或

在接收到用户界面触发的查杀指令时，通过服务端对未知程序文件进行查杀。

可选地，上述查杀方法包括：对未知程序文件进行扫描/判定动作和/或修复动作。

图 5 出示了本发明一个实施例的另一种基于云安全的文件处理装置的结构框图。该装置执行于上述客户端的对端服务器中。该装置 500 包括：

接收模块 510，配置为接收来自客户端的查询请求，其中，查询请求包括未知程序文件的签名标识以及未知程序文件的部分或全部文件特征；

发送模块 520，与上述接收模块 510 相耦合，配置为根据签名标识以及文件特征生成反馈消息，并将反馈消息发送至客户端，其中，客户端根据反馈消息对未知程序文件进行后续处理。

可选地，上述发送模块 520 包括：

匹配单元 521，配置为在数据库中，对签名标识进行匹配；

发送单元 522，配置为将匹配得到的查杀方法发送给客户端。

可选地，数据库包括：本地数据库和/或云端数据库。

可选地，上述接收模块 510 还配置为接收来自客户端的、未知程序文件的文件特征。

可选地，上述发送模块 520，还配置为预设的、针对未知程序文件的信息参数的检测条件发送至客户端；以及

上述接收模块 510，还配置为接收来自客户端的检测结果；

上述发送模块 520，还配置为根据检测结果发送相应指令。

可选地，上述发送模块 520 还配置为：

根据检测结果发送未知程序文件可能感染恶意程序的提醒消息至客户端；和/或

根据检测结果发送相应命令，其中，相应命令包括对未知程序文件进行查杀的

查杀命令，以及，对安全文件进行放行的命令。

本发明实施例提供了一种基于云安全的文件处理装置。通过该装置，使得客户端能够及时获取到本地的未知程序文件，并生成与该程序文件唯一对应的签名标识发送给服务器端，服务器端能够根据接收的签名标签获取对应的反馈消息并返回给客户端，客户端根据反馈消息对该未知程序文件进行相应地处理。

可见，本发明实施例提供的装置使得客户端能够实时地、动态地从服务器侧获取针对未知程序文件的处理方法，并能够及时地对恶意程序进行查杀，解决了现有技术中利用木马突破云查杀的问题。另外，与现有技术中，通过升级本地特征库和引擎程序文件才能检测并查杀新生恶意程序相比，本装置还减少了由发现恶意程序到查杀恶意程序的时间，从而加快了对新生恶意程序的打击速度，也减少了服务器的信息存储量，进而保证了客户端程序的安全。

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。

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。

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。

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。

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基于云安全的文件处理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，本发明示出了可以实现根据本发明的第一种基于云安全的文件处理方法的计算设备，例如客户端，和可以实现根据本发明的第二种基于云安全的文件处理方法的计算设备，例如常用的应用服务器。参见图 6，计算设备传统上包括处理器 610 和以存储器 620 形式的计算机程序产品或者计算机可读介质。存储器 620 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 620 具有用于执行上述方法中的任何方法步骤的程序代码 631 的存储空间 630。例如，用于程序代码的存储空间 630 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 631。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 7 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 6 的服务器中的存储器 620 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 631’，即可以由例如诸如 610 之类的处理器读取的代码，这些代码当由计算设备运行时，导致该计算设备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。

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、一种基于云安全的文件处理方法，包括：

根据本地下载的未知程序文件的签名相关信息，生成与所述未知程序文件唯一对应的签名标识；

发送查询请求至服务器端，查询所述未知程序文件是否是恶意程序，其中，所述查询请求携带有所述未知程序文件的签名标识以及所述未知程序文件的部分或全部文件特征；

接收来自所述服务器端的反馈消息，并根据所述反馈消息对所述未知程序文件进行后续处理，其中，所述服务器端根据所述签名标识以及所述文件特征生成所述反馈消息。

2、根据权利要求 1 所述的方法，按照如下步骤获得所述签名相关信息以及所述文件特征，包括：

扫描所述未知程序文件，获取文件特征；

从所述文件特征中提取签名相关信息。

3、根据权利要求 1 或 2 所述的方法，所述文件特征包括下列至少之一：

MD5、SHA1、从文件中抽取部分内容计算出的特征值。

4、根据权利要求 1 至 3 任一项所述的方法，根据本地下载的未知程序文件的签名相关信息，生成与所述未知程序文件唯一对应的签名标识，包括：

获取可移植的执行体 PE 文件的可计算字段，所述可计算字段为 PE 文件中除去 PE 校验段、签名段以及签名内容剩余部分；

对所述可计算字段进行计算，将计算结果作为所述签名标识。

5、根据权利要求 1 至 4 任一项所述的方法，根据所述反馈消息进行后续处理，包括：

所述签名标识在所述服务器端匹配成功时，接收所述服务器端反馈的、与所述签名标识相对应的查杀方法。

6、根据权利要求 5 所述的方法，接收所述服务器端反馈的查杀方式之后，包括：

从所述服务器端下载预设的、针对所述未知程序文件的信息参数的检测条件，判断所述未知程序文件是否满足所述检测条件；

将判断结果上传所述服务器端，并根据所述服务器端的指令执行后续处理。

7、根据权利要求 6 所述的方法，所述检测条件包括下列至少一项：

PE 加载的特定文件是否具有特定公司的有效签名；

PE 加载的特定文件的内部名称、产品名称及公司名称是否为指定的名称；

系统中是否挂有特定的钩子；

特定的进程中是否具有特定的填充数据；

系统中是否有特定驱动模块或者设备对象存在；

特定的注册表是否指向特定的文件或者特定的唯一标识 CLSID 或者匹配特定的模式；

PE 加载的进程链中是否存在安全性未知的文件。

8、根据权利要求 6 或 7 所述的方法，根据所述服务器端的指令执行后续处理，包括：

接收来自所述服务器端的所述未知程序文件可能感染恶意程序的提醒消息；和/或

接收来自所述服务器端的对所述未知程序文件进行查杀的查杀命令时，对所述未知程序文件进行查杀；和/或

在接收到用户界面触发的查杀指令时，通过服务端对所述未知程序文件进行查杀。

9、根据权利要求 5 至 8 任一项所述的方法，所述查杀方法包括：扫描/判定动作和/或修复动作。

10、一种基于云安全的文件处理方法，包括：

接收来自客户端的查询请求，其中，所述查询请求包括未知程序文件的签名标识以及所述未知程序文件的部分或全部文件特征；

根据所述签名标识以及所述文件特征生成反馈消息；

将所述反馈消息发送至所述客户端，其中，所述客户端根据所述反馈消息对所述未知程序文件进行后续处理。

11、根据权利要求 10 所述的方法，其中，将所述反馈消息发送至所述客户端，包括：

在数据库中，对所述签名标识进行匹配；

将匹配得到的查杀方法返回给所述客户端。

12、根据权利要求 11 所述的方法，其中，所述数据库包括：本地数据库和/或云端数据库。

13、根据权利要求 10 至 12 任一项所述的方法，其中，所述接收来自客户端的查询请求之前，包括：接收来自所述客户端的、所述未知程序文件的文件特征。

14、根据权利要求 11 至 13 任一项所述的方法，其中，将匹配得到的查杀方法返回给所述客户端之后，还包括：

将预设的、针对所述未知程序文件的信息参数的检测条件发送至所述客户端；以及

接收来自所述客户端的检测结果；

根据所述检测结果发送相应指令。

15、根据权利要求 14 所述的方法，其中，根据所述检测结果发送相应指令，包

括：

根据所述检测结果发送所述未知程序文件可能感染恶意程序的提醒消息至所述客户端；和/或

根据所述检测结果发送相应命令，其中，所述相应命令包括对所述未知程序文件进行查杀的查杀命令，以及，对安全文件进行放行的命令。

16、一种基于云安全的文件处理装置，包括：

生成模块，配置为根据本地下载的未知程序文件的签名相关信息，生成与所述未知程序文件唯一对应的签名标识；

查询模块，配置为发送查询请求至服务器端，查询所述未知程序文件是否是恶意程序，其中，所述查询请求携带有所述未知程序文件的签名标识以及所述未知程序文件的部分或全部文件特征；

处理模块，配置为接收来自所述服务器端的反馈消息，并根据所述反馈消息对所述未知程序文件进行后续处理，其中，所述服务器端根据所述签名标识以及所述文件特征生成所述反馈消息。

17、根据权利要求 16 所述的装置，其中，还包括：

提取模块，配置为扫描所述未知程序文件，获取文件特征；从所述文件特征中提取签名相关信息。

18、根据权利要求 16 或 17 所述的装置，其中，所述文件特征包括下列至少之一：

MD5、SHA1、从文件中抽取部分内容计算出的特征值。

19、根据权利要求 16 至 18 任一项所述的装置，其中，所述生成模块还配置为：

获取可移植的执行体 PE 文件的可计算字段，所述可计算字段为 PE 文件中除去 PE 校验段、签名段以及签名内容剩余部分；

对所述可计算字段进行计算，将计算结果作为所述签名标识。

20、根据权利要求 16 至 19 任一项所述的装置，其中，所述处理模块还配置为：

所述签名标识在所述服务器端匹配成功时，接收所述服务器端反馈的、与所述签名标识相对应的查杀方法。

21、根据权利要求 20 所述的装置，其中，所述处理模块还配置为：

从所述服务器端下载预设的、针对所述未知程序文件的信息参数的检测条件，判断所述未知程序文件是否满足所述检测条件；

将判断结果上传所述服务器端，并根据所述服务器端的指令执行后续处理。

22、根据权利要求 21 所述的装置，其中，所述处理模块还配置为：

接收来自所述服务器端的所述未知程序文件可能感染恶意程序的提醒消息；和/或

接收来自所述服务器端的对所述未知程序文件进行查杀的查杀命令时，对所述

未知程序文件进行查杀；和/或

在接收到用户界面触发的查杀指令时，通过服务端对所述未知程序文件进行查杀。

23、根据权利要求 20 至 22 任一项所述的装置，其中，所述查杀方法包括：对所述未知程序文件进行扫描/判定动作和/或修复动作。

24、一种基于云安全的文件处理装置，包括：

接收模块，配置为接收来自客户端的查询请求，其中，所述查询请求包括未知程序文件的签名标识以及所述未知程序文件的部分或全部文件特征；

发送模块，配置为根据所述签名标识以及所述文件特征生成反馈消息，并将所述反馈消息发送至所述客户端，其中，所述客户端根据所述反馈消息对所述未知程序文件进行后续处理。

25、根据权利要求 24 所述的装置，其中，所述发送模块包括：

匹配单元，配置为在数据库中，对所述签名标识进行匹配；

发送单元，配置为将匹配得到的查杀方法发送给所述客户端。

26、根据权利要求 25 所述的装置，其中，所述数据库包括：本地数据库和/或云端数据库。

27、根据权利要求 24 至 26 任一项所述的装置，其中，所述接收模块还配置为接收来自所述客户端的、所述未知程序文件的文件特征。

28、根据权利要求 24 至 27 任一项所述的装置，其中，

所述发送模块，还配置为预设的、针对所述未知程序文件的信息参数的检测条件发送至所述客户端；以及

所述接收模块，还配置为接收来自所述客户端的检测结果；

所述发送模块，还配置为根据所述检测结果发送相应指令。

29、根据权利要求 28 所述的装置，其中，所述发送模块还配置为：

根据所述检测结果发送所述未知程序文件可能感染恶意程序的提醒消息至所述客户端；和/或

根据所述检测结果发送相应命令，其中，所述相应命令包括对所述未知程序文件进行查杀的查杀命令，以及，对安全文件进行放行的命令。

30、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计算设备上运行时，导致所述计算设备执行根据权利要求 1-9 中的任一个所述的基于云安全的文件处理方法，和/或，根据权利要求 10-15 任一个所述的基于云安全的文件处理方法。

31、一种计算机可读介质，其中存储了如权利要求 30 所述的计算机程序。

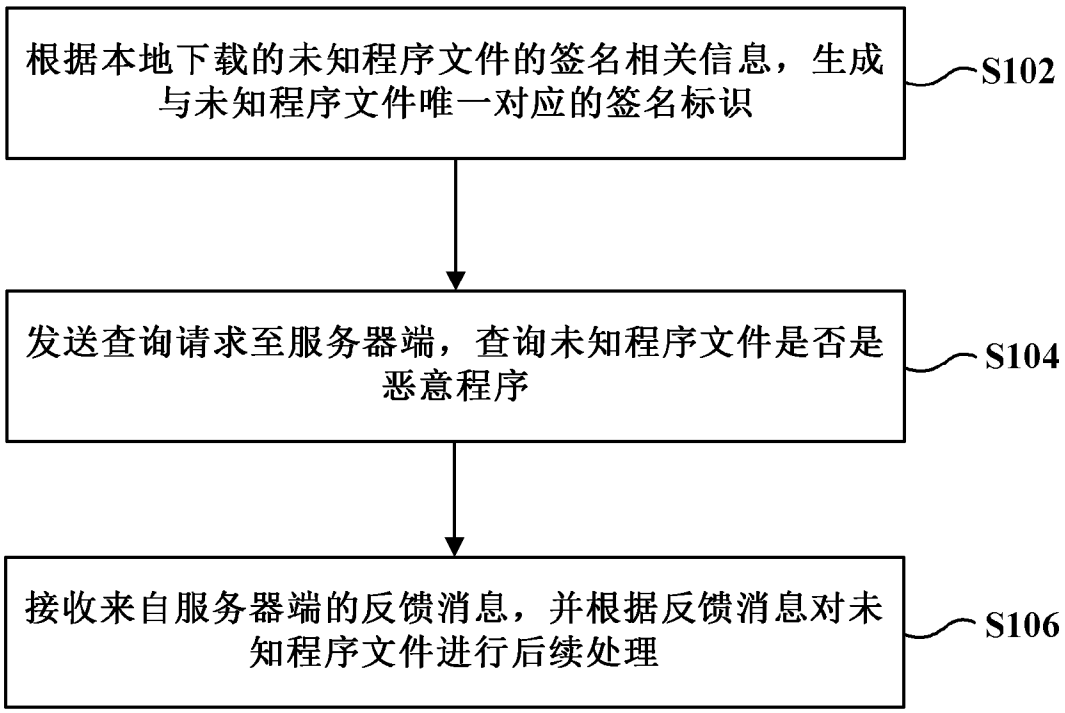
根据本地下载的未知程序文件的签名相关信息，生成与未知程序文件唯一对应的签名标识
S102
发送查询请求至服务器端，查询未知程序文件是否是恶意程序
S104
接收来自服务器端的反馈消息，并根据反馈消息对未知程序文件进行后续处理
S106

图 1

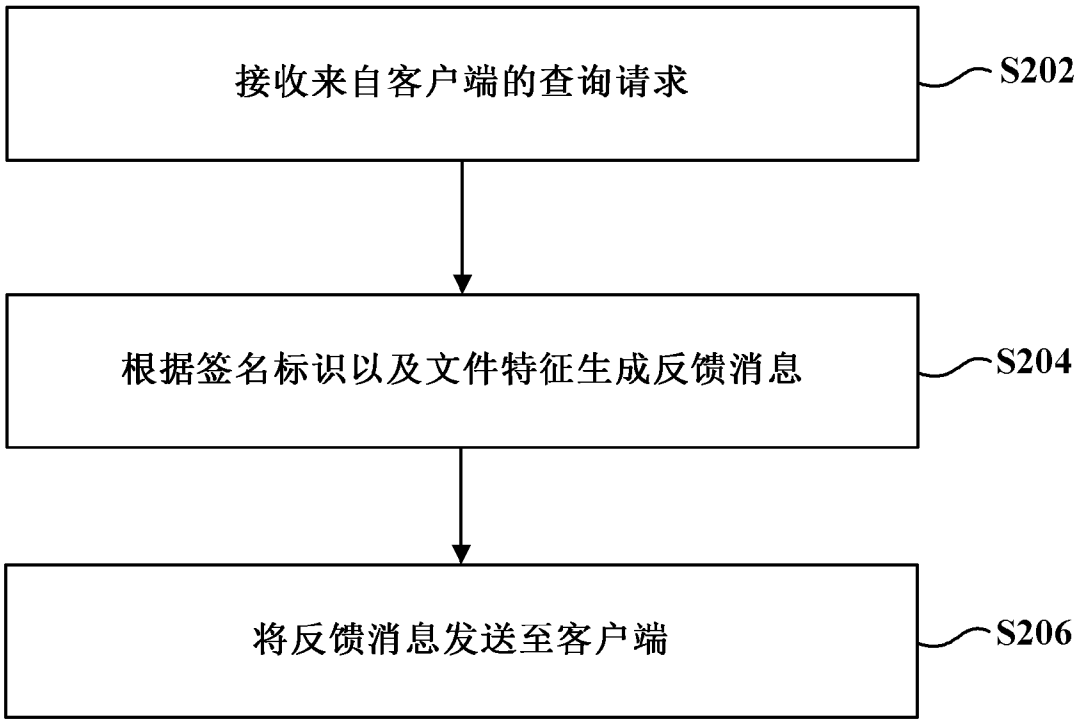
接收来自客户端的查询请求
S202
根据签名标识以及文件特征生成反馈消息
S204
将反馈消息发送至客户端
S206

图 2

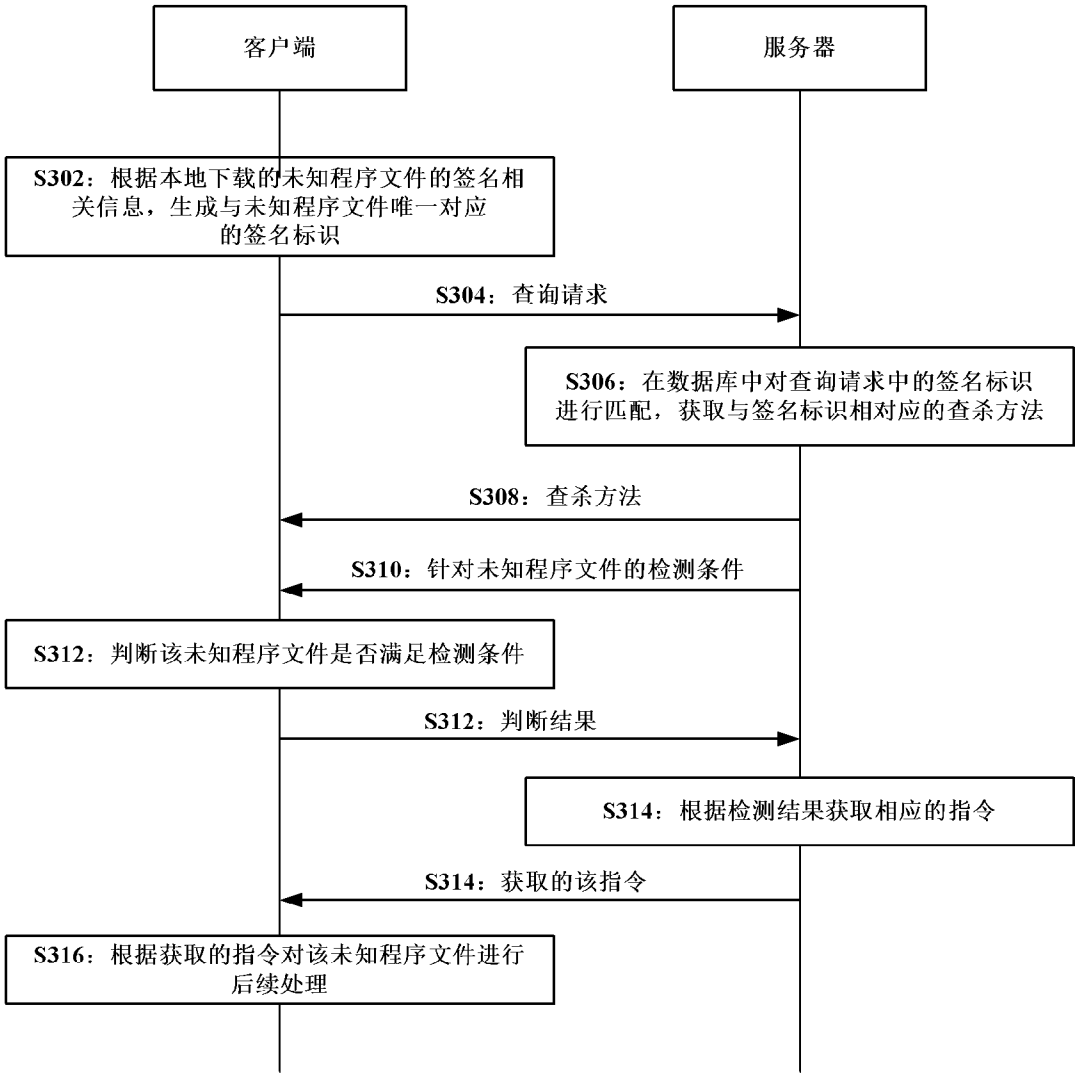
客户端
服务器
S302：根据本地下载的未知程序文件的签名相关信息，生成与未知程序文件唯一对应的签名标识
S304：查询请求
S306：在数据库中对查询请求中的签名标识进行匹配，获取与签名标识相对应的查杀方法
S308：查杀方法
S310：针对未知程序文件的检测条件
S312：判断该未知程序文件是否满足检测条件
S312：判断结果
S314：根据检测结果获取相应的指令
S314：获取的该指令
S316：根据获取的指令对该未知程序文件进行后续处理

图 3

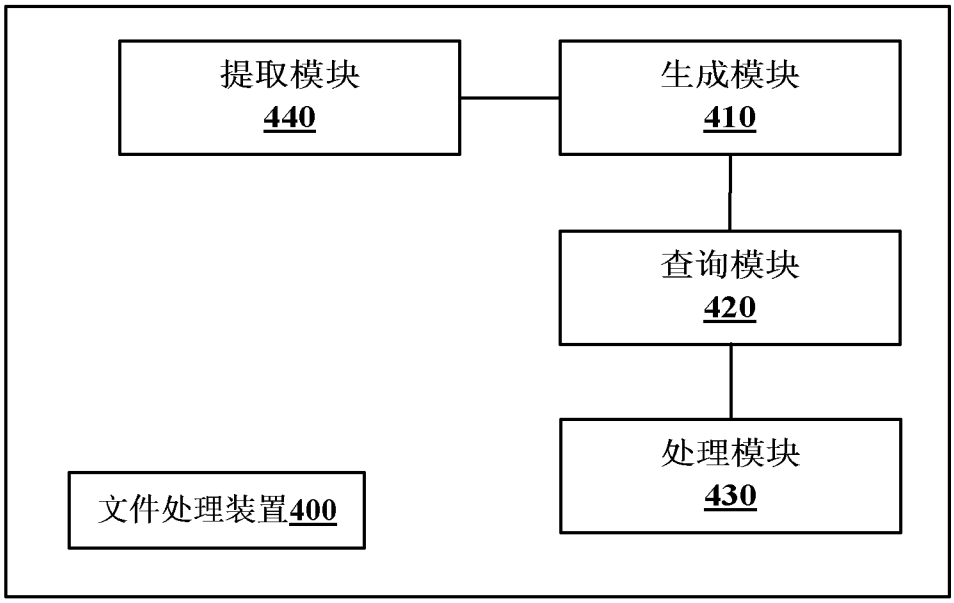
提取模块
440
生成模块
410
查询模块
420
处理模块
430
文件处理装置400

图 4

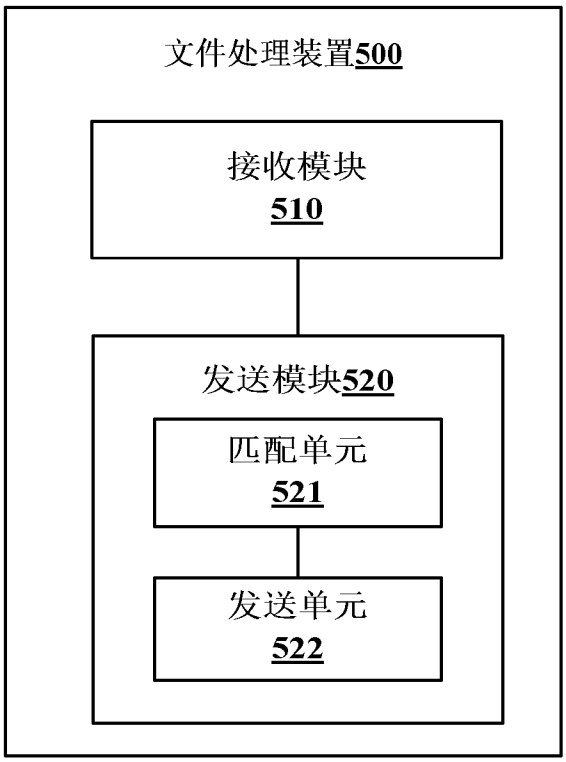
文件处理装置500
接收模块
510
发送模块520
匹配单元
521
发送单元
522

图 5

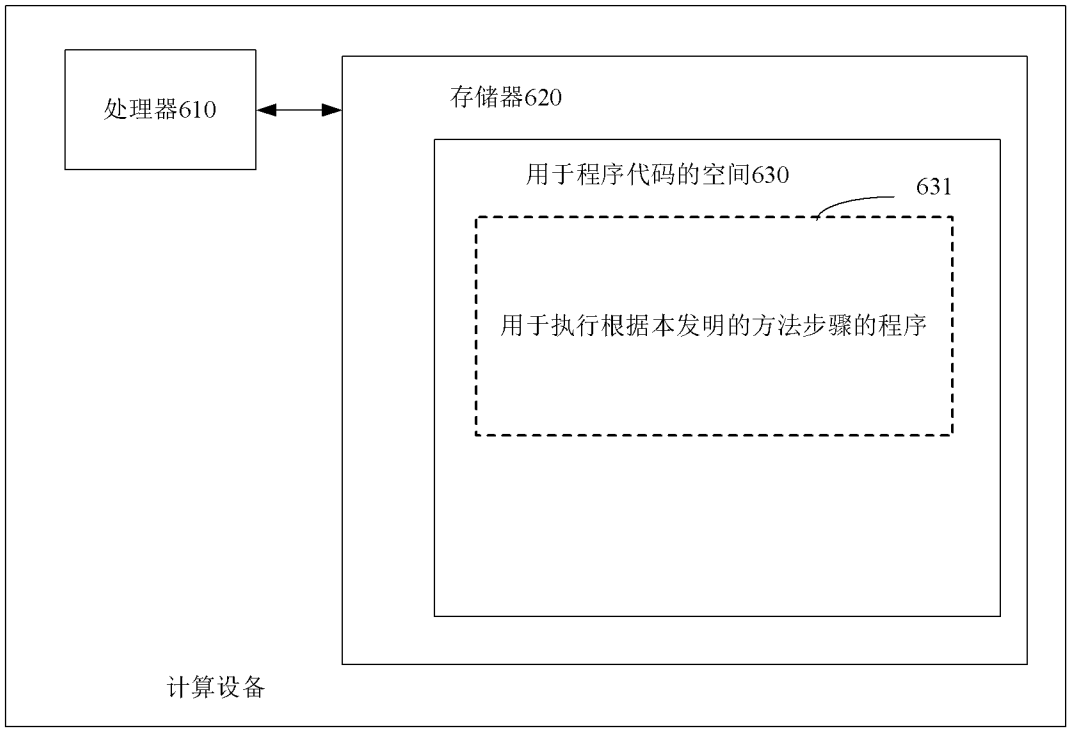
处理器610
存储器620
用于程序代码的空间630
631
用于执行根据本发明的方法步骤的程序
计算设备

图 6

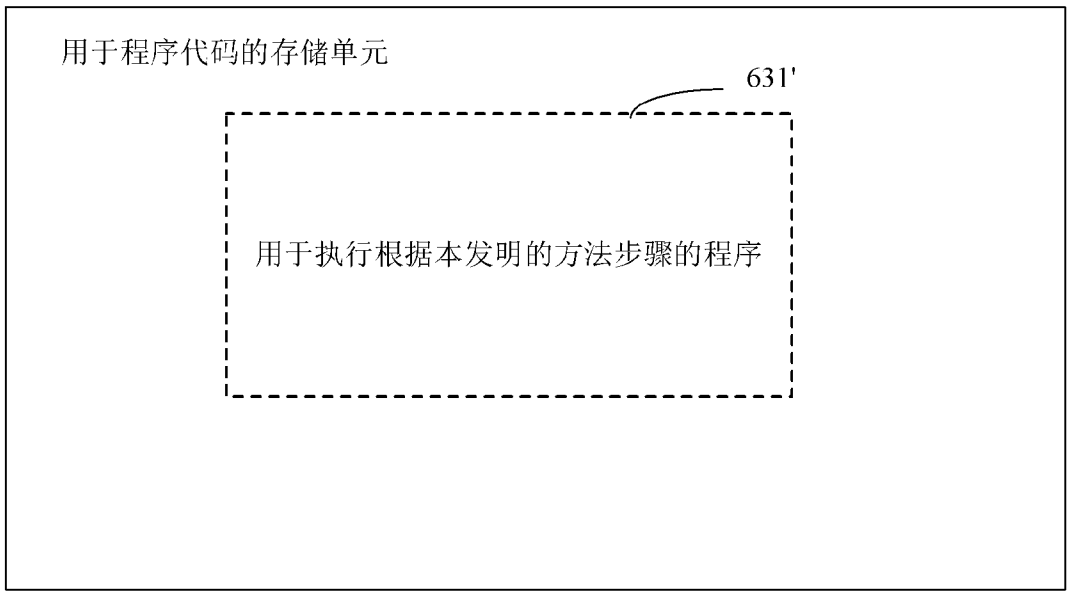
用于程序代码的存储单元
631'
用于执行根据本发明的方法步骤的程序

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/079076

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

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)

H04L 29

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, GOOGLE: security, virus, baleful, file feature, enquiry, server, feedback

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103281325 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 04 September 2013 (04.09.2013) description, paragraphs [0097]-[0237], and figures 1-5	1-31
X	CN 101719846 A (CHINA MOBILE GROUP TIANJIN BRANCH CO., LTD.) 02 June 2010 (02.06.2010) description, paragraphs [0046]-[0130], and figures 1-7	1-6, 8-31
Y	CN 101719846 A (CHINA MOBILE GROUP TIANJIN BRANCH CO., LTD.) 02 June 2010 (02.06.2010) description, paragraphs [0046]-[0130], and figures 1-7	7
Y	CN 102663288 A (QIZHI SOFTWARE (BEIJING) CO., LTD.) 12 September 2012 (12.09.2012) description, paragraphs [0061]-[0094], and figures 1-3	7
X	CN 101594248 A (QIHOO SOFTWARE TECHNOLOGY (BEIJING) CO., LTD.) 02 December 2009 (02.12.2009) description, page 5, the last paragraph to page 13, the fifth paragraph, and figures 1-5	1-6, 8-31
X	CN 102693388 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.) 26 September 2012 (26.09.2012) description, paragraphs [0005]-[0019], and figure 1	1-6, 8-31

☐ 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
22 July 2014	02 September 2014
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 ZHANG, Xia Telephone No. (86-10) 61648105

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/079076

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103281325 A	04 September 2013	None	
CN 101719846 A	02 June 2010	None	
CN 102663288 A	12 September 2012	None	
CN 101594248 A	02 December 2009	None	
CN 102693388 A	26 September 2012	None	

国际检索报告

国际申请号
PCT/CN2014/079076

A. 主题的分类

H04L 29/06(2006.01)i

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)

H04L 29

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, GOOGLE，安全，病毒，恶意，文件特征，查询，服务器，反馈，security,virus, baleful,file feature,enquiry,server,feedback

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
PX	CN 103281325 A (北京奇虎科技有限公司等) 2013年 9月 04日 (2013-09-04) 说明书第[0097]-[0237]段，图1-5	1-31
X	CN 101719846 A (中国移动通信集团天津有限公司) 2010年 6月 02日 (2010-06-02) 说明书第[0046]-[0130]段，图1-7	1-6， 8-31
Y	CN 101719846 A (中国移动通信集团天津有限公司) 2010年 6月 02日 (2010-06-02) 说明书第[0046]-[0130]段，图1-7	7
Y	CN 102663288 A (奇智软件北京有限公司) 2012年 9月 12日 (2012-09-12) 说明书第[0061]-[0094]段，图1-3	7
X	CN 101594248 A (奇智软件技术北京有限公司) 2009年 12月 02日 (2009-12-02) 说明书第5页倒数第1段至第13页第5段，图1-5	1-6， 8-31
X	CN 102693388 A (腾讯科技深圳有限公司) 2012年 9月 26日 (2012-09-26) 说明书第[0005]-[0019]段，图1	1-6， 8-31

☐ 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" 在国际申请日的当天或之后公布的在先申请或专利

"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
2014年 7月 22日	2014年 9月 02日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国	张霞
传真号 (86-10)62019451	电话号码 (86-10)61648105

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/079076

检索报告引用的专利文件	公布日（年/月/日）	同族专利	公布日（年/月/日）
CN 103281325 A	2013年 9月 04日	无	
CN 101719846 A	2010年 6月 02日	无	
CN 102663288 A	2012年 9月 12日	无	
CN 101594248 A	2009年 12月 02日	无	
CN 102693388 A	2012年 9月 26日	无	