(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107085684 B
(45)授权公告日 2020.02.07

(21)申请号 201610088140.8

(22)申请日 2016.02.16

(65)同一申请的已公布的文献号
申请公布号 CN 107085684 A

(43)申请公布日 2017.08.22

(73)专利权人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 罗绍华

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 董文倩 李灵洁

(51)Int.Cl.
G06F 21/56(2013.01)

(56)对比文件
CN 104462968 A,2015.03.25,
CN 104462968 A,2015.03.25,
CN 101593253 A,2009.12.02,
CN 102831338 A,2012.12.19,
CN 104123493 A,2014.10.29,
CN 104715196 A,2015.06.17,
CN 104766008 A,2015.07.08,

审查员 王秋苹

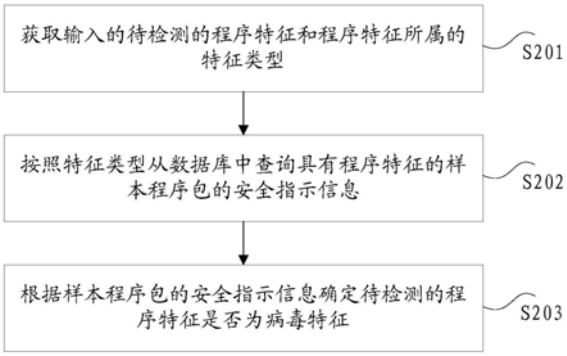
权利要求书3页 说明书14页 附图7页

(54)发明名称

程序特征的检测方法和装置

(57)摘要

本发明公开了一种程序特征的检测方法和装置。其中,该方法包括:获取输入的待检测的程序特征和程序特征所属的特征类型;按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息,其中,安全指示信息用于指示样本程序包的安全特性;根据样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征。本发明解决了相关技术中不能对安卓软件的程序特征进行准确识别的技术问题。



CN 107085684 B

1.一种程序特征的检测方法,其特征在于,包括:

获取输入的待检测的程序特征和所述程序特征所属的特征类型;

按照所述特征类型从数据库中查询具有所述程序特征的样本程序包的安全指示信息,其中,所述安全指示信息用于指示所述样本程序包的安全特性,所述按照所述特征类型从数据库中查询具有所述程序特征的样本程序包的安全指示信息包括:按照所述特征类型从所述数据库中查询具有所述程序特征的程序碎片;将查找到的程序碎片中,属于同一程序包的程序碎片进行拼接,得到所述样本程序包;读取查找到的样本程序包的安全指示信息;

根据所述样本程序包的安全指示信息确定所述待检测的程序特征是否为病毒特征。

2.根据权利要求1所述的方法,其特征在于,在所述样本程序包为一个的情况下,根据所述样本程序包的安全指示信息确定所述待检测的程序特征是否为病毒特征包括:

若所述安全指示信息指示所述样本程序包为病毒程序包,则确定所述待检测的程序特征为疑似病毒特征;

若所述安全指示信息指示所述样本程序包是安全程序包,则确定所述待检测的程序特征为安全特征。

3.根据权利要求1所述的方法,其特征在于,在所述样本程序包为多个的情况下,根据所述样本程序包的安全指示信息确定所述待检测的程序特征是否为病毒特征包括:

基于各个所述样本程序包的安全指示信息确定所述样本程序包为病毒程序包或者为安全程序包;

若确定多个所述样本程序包全部为所述安全程序包,则确定所述待检测的程序特征为安全特征;

若确定的病毒程序包的个数超过预设个数,则确定所述待检测的程序特征为所述病毒特征;

若确定的病毒程序包的个数不超过所述预设个数,则确定所述待检测的程序特征为疑似病毒特征。

4.根据权利要求3所述的方法,其特征在于,所述安全指示信息包括多个安全维度信息,其中,基于各个所述样本程序包的安全指示信息确定所述样本程序包为病毒程序包或者为安全程序包包括:

获取样本程序包的安全指示信息的每个所述安全维度信息的属性值和每个安全维度信息的权重;

判断每个所述安全维度信息的属性值和权重的乘积之和是否超过预设阈值;

若超过所述预设阈值,则确定所述样本程序包为所述安全程序包;

若未超过所述预设阈值,则确定所述样本程序包为所述病毒程序包。

5.根据权利要求1所述的方法,其特征在于,在按照所述特征类型从所述数据库中查询具有所述程序特征的程序碎片之前,所述方法还包括:

从收集到的源程序包中提取属于多个特征类型的程序碎片;

将提取到的程序碎片按照所述程序碎片所属的特征类型,保存入所述数据库,并以字典分词的方式建立所述数据库的索引。

6.根据权利要求5所述的方法,其特征在于,按照所述特征类型从所述数据库中查询具有所述程序特征的程序碎片包括:

利用所述特征类型和所述索引，查询所述数据库中具有所述程序特征的程序碎片。

7.根据权利要求5所述的方法，其特征在于，所述多个特征类型包括下述至少之二：程序包名、程序证书、程序的数据容量大小、程序的版本、程序所属的类以及程序的常量字符串。

8.一种程序特征的检测装置，其特征在于，包括：

获取单元，用于获取输入的待检测的程序特征和所述程序特征所属的特征类型；

查询单元，用于按照所述特征类型从数据库中查询具有所述程序特征的样本程序包的安全指示信息，其中，所述安全指示信息用于指示所述样本程序包的安全特性；

确定单元，用于根据所述样本程序包的安全指示信息确定所述待检测的程序特征是否为病毒特征；

其中，所述查询单元包括：查询模块，用于按照所述特征类型从所述数据库中查询具有所述程序特征的程序碎片；拼接模块，用于将查找到的程序碎片中，属于同一程序包的程序碎片进行拼接，得到所述样本程序包；读取模块，用于读取查找到的样本程序包的安全指示信息。

9.根据权利要求8所述的装置，其特征在于，在所述样本程序包为一个的情况下，所述确定单元包括：

第一确定模块，用于若所述安全指示信息指示所述样本程序包为病毒程序包，则确定所述待检测的程序特征为疑似病毒特征；

第二确定模块，用于若所述安全指示信息指示所述样本程序包是安全程序包，则确定所述待检测的程序特征为安全特征。

10.根据权利要求8所述的装置，其特征在于，在所述样本程序包为多个的情况下，所述确定单元包括：

第三确定模块，用于基于各个所述样本程序包的安全指示信息确定所述样本程序包为病毒程序包或者为安全程序包；

第四确定模块，用于若确定多个所述样本程序包全部为所述安全程序包，则确定所述待检测的程序特征为安全特征；

第五确定模块，用于若确定的病毒程序包的个数超过预设个数，则确定所述待检测的程序特征为所述病毒特征；

第六确定模块，用于若确定的病毒程序包的个数不超过所述预设个数，则确定所述待检测的程序特征为疑似病毒特征。

11.根据权利要求10所述的装置，其特征在于，所述安全指示信息包括多个安全维度信息，其中，所述第三确定模块包括：

获取子模块，用于获取样本程序包的安全指示信息的每个所述安全维度信息的属性值和每个安全维度信息的权重；

判断子模块，用于判断每个所述安全维度信息的属性值和权重的乘积之和是否超过预设阈值；

第一确定子模块，用于若超过所述预设阈值，则确定所述样本程序包为所述安全程序包；

第二确定子模块，用于若未超过所述预设阈值，则确定所述样本程序包为所述病毒程

序包。

12.根据权利要求8所述的装置,其特征在于,所述装置还包括:

提取单元,用于在按照所述特征类型从所述数据库中查询具有所述程序特征的程序碎片之前,从收集到的源程序包中提取属于多个特征类型的程序碎片;

保存单元,用于将提取到的程序碎片按照所述程序碎片所属的特征类型,保存入所述数据库,并以字典分词的方式建立所述数据库的索引。

13.根据权利要求12所述的装置,其特征在于,所述查询模块包括:

查询子模块,用于利用所述特征类型和所述索引,查询所述数据库中具有所述程序特征的程序碎片。

14.根据权利要求12所述的装置,其特征在于,所述多个特征类型包括下述至少之二:程序包名、程序证书、程序的数据容量大小、程序的版本、程序所属的类以及程序的常量字符串。

程序特征的检测方法和装置

技术领域

[0001] 本发明涉及程序安全领域，具体而言，涉及一种程序特征的检测方法和装置。

背景技术

[0002] 随着移动互联网的迅速发展，具有移动操作系统的智能手机和平板得到了大范围应用。由于不再局限于普通的通讯功能，智能手机等拥有独立的操作系统，因而人们可以使用智能手机随时随地进行收发邮件、购物、交易等，移动互联网市场已经显露出它巨大的价值。而在此背景下的安全风险也随之而来：恶意软件、钓鱼网站越来越多，公共wifi之类的风险应用场景也越来越多。相比于其他操作系统，随着基于linux内核的安卓智能手机操作系统的市场份额越来越多，安卓手机已经成为当前恶意软件最重要的攻击目标。

[0003] 安卓系统是一种开源的操作系统，开发人员可以将应用程序直接上传到市场供用户使用而无需经过任何审查。方便快捷的开发方式激发了各种功能的应用程序的涌现，也进一步促进了安卓操作系统的发展和普及，但也使它面临着更大的风险。移动设备存储量的增长，使其能够存储大量的个人信息和商业数据；另外，安卓智能手机可以支持支付业务，且供应商，销售商，批发商，内容提供商，移动操作者以及银行都在创建各种新的移动支付业务。这些都使移动设备等成为了攻击者们的众矢之的。越来越多的恶意程序利用移动设备来获取用户资料，进行恶意扣费和系统破坏。恶意程序利用移动设备来恶意拨打电话，发送垃圾短信，泄露用户证书，和破坏手机软硬件的事例已经屡见不鲜。

[0004] 对安卓设备上的恶意软件检测方法主要分为静态检测和动态检测两种方法。静态检测是在不运行应用程序的前提下，通过分析反编译应用程序，获取程序的源代码，或者分析程序的外部特征如文件签名等对恶意软件进行检测。而动态检测则是将应用程序运行在沙箱或者安卓系统中，在程序运行的过程中，分析程序的运行轨迹，查看程序对系统敏感资源的通信情况和使用情况，检测出程序对用户资料或者系统敏感资源的泄露来判定为恶意软件或者病毒。

[0005] 在现有的静态检测中，主要是根据安卓包提取数字签名，或运行权限做的静态分析，并得到恶意软件检测结果，以确定该apk软件是否为恶意软件。在上述方法中，由于数字签名可以被更改，因此，其并不能全面地反映恶意软件的特征，因此，仅根据数字签名进行恶意软件检测，不能够高效准确地对恶意软件进行识别。

[0006] 针对上述的问题，目前尚未提出有效的解决方案。

发明内容

[0007] 本发明实施例提供了一种程序特征的检测方法和装置，以至少解决相关技术中不能对安卓软件的程序特征进行准确识别的技术问题。

[0008] 根据本发明实施例的一个方面，提供了一种程序特征的检测方法，该方法包括：获取输入的待检测的程序特征和程序特征所属的特征类型；按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息，其中，安全指示信息用于指示样本程序包的安

全特性;根据样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征。

[0009] 根据本发明实施例的另一方面,还提供了一种程序特征的检测装置,该装置包括:获取单元,用于获取输入的待检测的程序特征和程序特征所属的特征类型;查询单元,用于按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息,其中,安全指示信息用于指示样本程序包的安全特性;确定单元,用于根据样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征。

[0010] 在本发明实施例中,在获取输入的待检测的程序特征和程序特征所属的特征类型之后,按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息(安全指示信息用于指示样本程序包的安全特性),并根据得到的样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征,与相关技术中使用程序的签名信息进行病毒检测的方法相比,本申请的方案可以将需要检测程序的各类程序特征与海量数据库(数据库中存储有实时采集到的各类应用市场的程序应用的特征,如google应用市场、安卓市场、机锋市场等)中的样本程序包进行对比,以确定待检测的程序特征是否为病毒特征,从而解决了相关技术中不能对安卓软件的程序特征进行准确识别的技术问题,实现了对安卓软件的程序特征是否为病毒特征或者安全特征的准确判断,同时还能通过对程序特征的识别判断出待检测程序是否为包括病毒或木马的恶意软件。

附图说明

[0011] 此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

[0012] 图1是根据本发明实施例的一种终端的硬件环境示意图;

[0013] 图2是根据本发明实施例的一种可选的程序特征的检测方法的流程图;

[0014] 图3是根据本发明实施例的另一种可选的程序特征的检测方法的流程图;

[0015] 图4是根据本发明实施例的第三种可选的程序特征的检测方法的流程图;

[0016] 图5是根据本发明实施例的第四种可选的程序特征的检测方法的流程图;

[0017] 图6是根据本发明实施例的第五种可选的程序特征的检测方法的流程图;

[0018] 图7是根据本发明实施例的第六种可选的程序特征的检测方法的流程图;

[0019] 图8是根据本发明实施例的一种可选的程序特征的检测装置的示意图;

[0020] 图9是根据本发明实施例的另一种可选的程序特征的检测装置的示意图;

[0021] 图10是根据本发明实施例的第三种可选的程序特征的检测装置的示意图;

[0022] 图11是根据本发明实施例的第四种可选的程序特征的检测装置的示意图;

[0023] 图12是根据本发明实施例的第五种可选的程序特征的检测装置的示意图;以及

[0024] 图13是根据本发明实施例的另一种终端的硬件环境示意图。

具体实施方式

[0025] 首先,对本发明实施例中涉及的术语解释如下:

[0026] APK:即安卓软件的安装包。

[0027] Eclipse:一种用于编译安卓软件包的编译软件。

[0028] AXMLPrinter2:一种典型的用于反编译的软件。

[0029] 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。

[0030] 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。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。

[0031] 实施例1

[0032] 根据本发明实施例，提供了一种程序特征的检测方法，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0033] 可选地，在本实施例中，上述的检测方法可以应用于如图1所示的检测终端10和服务器20所构成的硬件环境中。如图1所示，检测终端20通过网络与服务器20进行连接。上述的终端可以为移动终端或者固定终端，如笔记本电脑、台式电脑、平板电脑和PDA，以及其他的手持设备。

[0034] 上述网络包括但不限于：广域网、城域网或局域网。优选地，上述的网络为局域网。

[0035] 根据本发明实施例，提供了一种程序特征的检测方法，图2是根据本发明实施例的一种可选的程序特征的检测方法的流程图，如图2所示，该方法包括：

[0036] 步骤S201：获取输入的待检测的程序特征和程序特征所属的特征类型。

[0037] 步骤S202：按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息，其中，安全指示信息用于指示样本程序包的安全特性。

[0038] 步骤S203：根据样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征。

[0039] 采用本发明上述实施例，在获取输入的待检测的程序特征和程序特征所属的特征类型之后，按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息(安全指示信息用于指示样本程序包的安全特性)，并根据得到的样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征，与相关技术中使用程序的签名信息进行病毒检测的方法相比，本申请的方案可以将需要检测程序的各类程序特征与海量数据库(数据库中存储有实时采集到的各类应用市场的程序应用的特征，如google应用市场、安卓市场、机锋市场等)中的样本程序包进行对比，以确定待检测的程序特征是否为病毒特征，从而解决了相关技术中不能对安卓软件的程序特征进行准确识别的技术问题，实现了对安卓软件的程序特征是否为病毒特征或者安全特征的准确判断，同时还能通过对程序特征的识别判断出待检测程序是否为包括病毒或木马的恶意软件。

[0040] 其中，待检测的程序特征可以为在检测安卓包时无法确定是否为病毒特征的特

征,将这些特征提取出来,使用上述方法进行校验,可以准确验证该特征是否为病毒特征,并将确定结果用特征ID标识,如安全特征用0标识,疑似病毒特征用1标识,病毒特征用2标识。

[0041] 在检测出该特征为病毒特征的情况下,将其保存入病毒查杀应用的病毒库中,从而在使用病毒查杀应用查杀程序包的病毒时,可以更准确地检测程序包是否为病毒程序包。

[0042] 需要说明的是,在按照特征类型从数据库中查询具有程序特征的程序碎片之前,本申请的检测方法还包括如图3所示的下述步骤:

[0043] 步骤S301,从收集到的源程序包中提取属于多个特征类型的程序碎片。

[0044] 需要说明的是,多个特征类型包括下述至少之二:程序包名、程序证书、程序的数据容量大小、程序的版本、程序所属的类以及程序的常量字符串。

[0045] 步骤S302,将提取到的程序碎片按照程序碎片所属的特征类型,保存入数据库,并以字典分词的方式建立数据库的索引。

[0046] 具体地,上述方法中的步骤S301和步骤S302可以通过如图4所示的子步骤S401至S406实现。

[0047] 步骤S401,APK收集,即获取安卓APK程序包(即源程序包),如通过官方合作渠道,实时收集通过官方渠道(如google应用市场、安卓市场、机锋市场等)发布的各种安卓程序包;再如,由于安卓系统的开放性,一些用户可以自行编写和发布安卓程序包,因此,还可以通过爬虫技术实时收集各类用户在互联网发布的安卓程序包。

[0048] 步骤S402,APK特征提取,即提取收集到的各安卓源程序包的不同类型的特征。

[0049] 上述步骤S402可以通过特征提取模块实现,特征提取模块实时去获取收集渠道来源的安卓程序包,利用解包技术,对各种安卓包进行逆向工程分析,提取里面的APK文件结构、classes.dex文件和mainfeset.xml文件。

[0050] 需要说明的是,安卓程序包(即APK文件)是用专业软件eclipse编译生成的文件包,上述的解包技术即利用反编译软件对APK文件的内容进行反编译的技术,具体可以通过AXMLPrinter2工具软件等反编译软件实现;通过解包技术得到classes.dex文件和mainfeset.xml文件等即上述的属于多个特征类型的程序碎片。

[0051] 可选地,该方案也可以应用于其他操作系统的程序包,如ios程序包。

[0052] 需要进一步说明的是,APK文件的实质是一个zip压缩包,APK文件结构是指解压得到的APK文件组成架构,其主要包括mainfeset.xml文件、classes.dex文件、Manifest文件、META-INF文件、RES目录、resource.arsc文件(即属于多个特征类型的程序碎片)等。

[0053] 在得到程序碎片之后,即可根据程序碎片确定其对应的包名、证书、大小、版本、类(主要指源代码的数据结构)、字符串(即常量字符串,如包括一个或多个字符的字符串)等多种维度特征(即上述实施例中的特征类型)。

[0054] 步骤S403,特征存储,即将上述得到的各个程序碎片及其包括的多种维度特征的特征数据写入特征数据库。

[0055] 步骤S404,检索服务器从特征数据库获取各个类型的程序碎片及其特征数据。

[0056] 步骤S405,检索服务器打包得到的程序碎片及其特征数据,可以将同一类型的程序碎片及其特征数据打包至同一个文件中。

[0057] 步骤S406,将得到的各个文件存储数据库中,并以字典分词的方式建立数据库的索引。该数据库可以是如图1所示的服务器集群20上的分布式数据库。

[0058] 需要说明的是,检索服务器可以实时获取特征数据库中更新的数据(即增量的特征),并对服务器集群上的文件进行及时更新和替换,在数据库中,为了标识新增的数据,可以通过时间戳来区分每天新增的数据。

[0059] 通过上述实施例,可以实时收集已发布的各类安卓源程序,即相当于提供了相关的海量数据,并提取收集到的安卓源程序的多种维度特征,包括包名、证书、大小、版本、类、字符串等多种维度,这样,在进行病毒检测时,即可基于海量数据进行特征维度搜索,从而可以提高病毒检测的准确率。

[0060] 在一个可选的实施例中,步骤S202的按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息可以通过如下子步骤实现:步骤S1,按照特征类型从数据库中查询具有程序特征的程序碎片,即利用特征类型和索引,查询数据库中具有程序特征的程序碎片;步骤S2,将查找到的程序碎片中,属于同一程序包的程序碎片进行拼接,得到样本程序包;步骤S3,读取查找到的样本程序包的安全指示信息。具体地,如图5所示:

[0061] 步骤S501,分析人员根据需要分析的不同特征类型,在浏览器上面进行元特征(即待检测程序的程序特征)提交,同时可以对元特征进行逻辑上面的与或操作。如以包名、证书、大小、版本、类、字符串、代码块为特征类型进行元特征(即具体的程序特征,如具体的证书值、版本值)的提交。

[0062] 上述的浏览器是指提供有分析人员进行特征提交功能的WEB界面,其相当于为用户提供一个操作接口。对元特征进行逻辑上面的与操作是指进行搜索时,搜索同时具有提交的多个元特征的程序碎片;对元特征进行逻辑上面的或操作是指,搜索具有提交的至少一个元特征的程序碎片。

[0063] 上述的对元特征进行逻辑操作,是指对包名、证书、大小、版本、类、字符串、代码块等查询条件进行与或操作,其是指是提供一个检索条件,如将“包名”和“证书”进行与操作时,其相当于需要查询同时满足该“包名”和“证书”条件的程序碎片;再如将“包名”和“证书”进行或操作时,其相当于需要查询满足该“包名”或“证书”条件的程序碎片。

[0064] 可选地,可以搜索一个元特征对应的程序碎片,如表1所示,在特征类型为“ConstantString”(即字符串)的情况下,搜索字符串“broadcastProcess”对应的程序碎片;也可以搜索多个元特征对应的程序碎片,如在特征类型为“ClassPrefix”(即类名前缀),搜索满足元特征“Net.youmi.android.offers.”、“net.youmi.android.appoffers.”、“com.grady.mx.”、“com.youmi.offers.”、“net.owan.android.”、“net.youmi.android.Adbrowser”、“cn.winads.studentsearn.YMPointsReceiver”、“net.slidinggmenu.tool.AdReceiver”中至少之一的程序碎片,表中的“|”符号表示或操作。

[0065] 表1:

[0066]

记录 id	特征类型	特征
53437	ConstantString	Lcom/gokgou/OReceiver
53436	ConstantString	com.liuy.oosp.inter.ExternalInterface
53435	ConstantString	broadcastProcess
53434	ConstantString	apus_en.jar
53433	ClassPrefix	Net.youmi.android.offers.|net.youmi.android.appoffers.|com.grady.mx.|com.youmi.offers.|net.owan.android.|net.youmi.android.Adbrowser|cn.winads.studentsearn.YMPointsReceiver|net.slidinggmenu.tool.AdReceiver

[0067] 步骤S502,通过WEB浏览器把进行逻辑操作过后的元特征数据通过post的方式提交至虚拟特征CGI。

[0068] 需要说明的是,post方法一种基于HTTP传输协议的向指定的目标对象提交需要被处理的数据的一种方法;CGI(即通过用网关接口,英文全称Common Gateway Interface),是外部应用程序(主要指CGI程序)与WEB服务器间的接口标准。

[0069] 步骤S503,通过CGI接口向检索服务器发起搜索请求。

[0070] CGI接口端的设备对特征类型进行适配,检查分析人员提交的检索条件是否符合检索规则。如果符合检索规则,则对检索服务器发起检索请求,否则对该请求进行丢弃并且返回不符合检索规则的提示。

[0071] 步骤S504,检索服务器向分布式数据库发起数据检索。

[0072] 具体地,检索服务器接收到CGI接口提交的请求后,会对提交上来的元数据进行解释,如对分析人员提交的检索条件进行解释,按照不同的类型和逻辑关系进行数据组合,生成满足搜索语法的语句,对存储集群发起数据检索。若分析人员提交的检索条件是需要检索满足“包名”和“证书”条件的程序碎片,则根据该检索条件生成满足搜索语法的语句,以进行查询。

[0073] 若上述分布式数据库为SQL数据库,则集群服务可以根据查询条件自动生成对应的SQL查询语句,以对SQL数据库进行查询。

[0074] 步骤S505,集群服务器根据检索服务器的请求进行搜索,即搜索满足请求中的程序特征的程序碎片。

[0075] 可选地,在进行检索服务时,根据待检测程序的程序特征从数据库中查询对应的程序碎片,即利用特征类型和索引,查询数据库中具有相同程序特征的程序碎片。

[0076] 如根据待检测程序的特征类型在数据库中确定一个需要搜索的大概范围(如包括同一类特征类型的程序碎片的文件),再以程序特征为关键字查询数据库中的各个程序碎片,并提取出具有与待检测程序具有相同程序特征的程序碎片。在这里,可以以待检测程序

的多个特征类型(如包名、证书、大小、版本、类等)来执行程序碎片的提取,以实现对待检测程序的准确检测。

[0077] 步骤S506,返回命中的程序碎片至检索服务,即将满足请求中的程序特征的程序碎片返回至检索服务器。也即存储集群服务器把存储于各节点满足检索要求的数据拼接起来,返回到检索服务。

[0078] 步骤S507,返回打包好的样本程序包至CGI接口,即检索服务器将接收到的程序碎片进行打包,得到样本程序包,并将样本程序包发送至CGI接口。

[0079] 步骤S508,CGI接口端的设备根据样本程序包从服务器端获取对应于该样本程序包的各个维度的信息(也即安全指示信息),并将各个维度的信息进行打包并发送至检测终端(即上述分析人员使用的具有WEB服务器的电脑终端)。

[0080] 步骤S509,接收打包好的数据包,并通过解包获取样本程序包的各个维度的信息(也即安全指示信息)。

[0081] 步骤S510,根据样本程序包(样本程序包的数量可以为1个,也可以为多个)的各个维度的信息(也即安全指示信息)确定待检测程序的安全性。如分析人员通过浏览器上面的安全指示信息进行对应的分析,判断出待检测程序的程序特征是否为病毒特征或者安全特征,以确定待检测程序是否为病毒或木马。

[0082] 通过上述实施例,突破了以往的单数据杀包可能导致的误杀漏杀;结合系统服务的多维度数据,对安卓包中各个维度的特征类型,进行快速检索和分析,依赖后台存储的海量数据,多安卓包数据、多维度数据去分析该安卓包的安全特性。同时提高了分析的效率,有效做到对安卓程序包病毒性特征的更精确的检测。

[0083] 在一个可选地实施例中,在样本程序包为一个的情况下,上述的步骤S203的根据样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征可以包括如图6所示的如下步骤:

[0084] 步骤S601,若安全指示信息指示样本程序包为病毒程序包,则确定待检测的程序特征为疑似病毒特征。

[0085] 上述安全指示信息包括多个安全维度信息,具体可以包括“安全级别”、“老白名单”、“新白名单”、“病毒id”等信息。如其安全级别为“风险”,则可以确定待检测的程序特征为疑似病毒特征。

[0086] 步骤S602,若安全指示信息指示样本程序包是安全程序包,则确定待检测的程序特征为安全特征。即在各个安全维度信息的信息均正常的情况下,则确定待检测的程序特征为安全特征。

[0087] 在另一个可选地实施例中,在样本程序包为多个的情况下,上述的步骤S203的根据样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征可以包括如图7所示的如下步骤:

[0088] 步骤S701,基于各个样本程序包的安全指示信息确定样本程序包为病毒程序包或者为安全程序包。

[0089] 可选地,步骤S701的基于各个样本程序包的安全指示信息确定样本程序包为病毒程序包或者为安全程序包可以包括:步骤S7011,获取样本程序包的安全指示信息的每个安全维度信息的属性值和每个安全维度信息的权重;步骤S7012,判断每个安全维度信息的属

性值和权重的乘积之和是否超过预设阈值;步骤S7013,若超过预设阈值,则确定样本程序包为安全程序包;若未超过预设阈值,则确定样本程序包为病毒程序包。

[0090] 具体地,可以根据历史信息为每一个安全维度信息设置一个权重比,在得到每个安全维度信息的属性值之后,将其与对应的权重值相乘得到其权重,再将每个安全维度信息的权重相加,即可根据得到的和值和预设阈值判断样本程序包是否为病毒程序包。

[0091] 步骤S702,若确定多个样本程序包全部为安全程序包,则确定待检测的程序特征为安全特征。

[0092] 步骤S703,若确定的病毒程序包的个数超过预设个数,则确定待检测的程序特征为病毒特征。该预设个数可以为5,在得到的多个样本程序包中,若为病毒程序包的数量超过5个,则确定待检测的程序特征为病毒特征,即待检测程序为带病毒的程序。

[0093] 步骤S704,若确定的病毒程序包的个数不超过预设个数,则确定待检测的程序特征为疑似病毒特征。

[0094] 例如,在得到的多个样本程序包中,若为病毒程序包的数量大于0且不大于5个,则确定待检测的程序特征为疑似病毒特征,即待检测程序可能为带病毒的程序。

[0095] 通过上述实施例,结合根据待检测程序的各个程序特征得到的样本程序包,并判断样本程序包的程序特征是否为病毒特征或者疑似病毒特征,从而可以实现对程序特征的准确识别。

[0096] 需要说明的是,对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本发明并不受所描述的动作顺序的限制,因为依据本发明,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本发明所必须的。

[0097] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中,包括若干指令用以使得一台终端设备(可以是手机,计算机,服务器,或者网络设备等)执行本发明各个实施例所述的方法。

[0098] 实施例2

[0099] 根据本发明实施例,还提供了一种用于实施上述程序特征的检测方法的程序特征的检测装置,如图8所示,该装置包括:获取单元30、查询单元40以及确定单元50。

[0100] 获取单元30用于获取输入的待检测的程序特征和程序特征所属的特征类型。

[0101] 查询单元40用于按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息,其中,安全指示信息用于指示样本程序包的安全特性。

[0102] 确定单元50用于根据样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征。

[0103] 采用本发明上述实施例,在获取单元获取输入的待检测的程序特征和程序特征所属的特征类型之后,查询单元按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息(安全指示信息用于指示样本程序包的安全特性),确定单元根据得到的样本

程序包的安全指示信息确定待检测的程序特征是否为病毒特征，与相关技术中使用程序的签名信息进行病毒检测的方法相比，本申请的方案可以将需要检测程序的各类程序特征与海量数据库(数据库中存储有实时采集到的各类应用市场的程序应用的特征，如google应用市场、安卓市场、机锋市场等)中的样本程序包进行对比，以确定待检测的程序特征是否为病毒特征，从而解决了相关技术中不能对安卓软件的程序特征进行准确识别的技术问题，实现了对安卓软件的程序特征是否为病毒特征或者安全特征的准确判断，同时还能通过对程序特征的识别判断出待检测程序是否为包括病毒或木马的恶意软件。

[0104] 其中，待检测的程序特征可以为在检测安卓包时无法确定是否为病毒特征的特征，将这些特征提取出来，使用上述方法进行校验，可以准确验证该特征是否为病毒特征，并将确定结果用特征ID标识，如安全特征用0标识，疑似病毒特征用1标识，病毒特征用2标识。

[0105] 在检测出该特征为病毒特征的情况下，将其保存入病毒查杀应用的病毒库中，从而在使用病毒查杀应用查杀程序包的病毒时，可以更准确地检测程序包是否为病毒程序包。

[0106] 需要说明的是，为了提高检测的全面性和准确性，本申请的检测装置还包括如图9所示的提取单元60，用于在按照特征类型从数据库中查询具有程序特征的程序碎片之前，从收集到的源程序包中提取属于多个特征类型的程序碎片；保存单元70，用于将提取到的程序碎片按照程序碎片所属的特征类型，保存入数据库，并以字典分词的方式建立数据库的索引。

[0107] 图9中还示出了获取单元30、查询单元40以及确定单元50，上述的多个特征类型包括下述至少之二：程序包名、程序证书、程序的数据容量大小、程序的版本、程序所属的类以及程序的常量字符串。

[0108] 具体地，可以通过官方合作渠道，实时收集通过官方渠道(如google应用市场、安卓市场、机锋市场等)发布的各种安卓程序包；由于安卓系统的开放性，一些用户可以自行编写和发布安卓程序包，因此，还可以通过爬虫技术实时收集各类用户在互联网发布的安卓程序包。然后利用解包技术，对各种安卓包进行逆向工程分析，提取里面的APK文件结构、classes.dex文件和mainfeset.xml文件。

[0109] 需要说明的是，安卓程序包(即APK文件)是用专业软件eclipse编译生成的文件包，上述的解包技术即利用反编译软件对APK文件的内容进行反编译的技术，具体可以通过AXMLPrinter2工具软件等反编译软件实现；通过解包技术得到classes.dex文件和mainfeset.xml文件等即上述的属于多个特征类型的程序碎片。

[0110] 可选地，该方案也可以应用于其他操作系统的程序包，如ios程序包。

[0111] 需要进一步说明的是，APK文件的实质是一个zip压缩包，APK文件结构是指解压得到的APK文件组成架构，其主要包括mainfeset.xml文件、classes.dex文件、Manifest文件、META-INF文件、RES目录、resource.arsc文件(即属于多个特征类型的程序碎片)等。

[0112] 在得到程序碎片之后，即可根据程序碎片确定其对应的包名、证书、大小、版本、类(主要指源代码的数据结构)、字符串(即常量字符串，如包括一个或多个字符的字符串)等多种维度特征(即上述实施例中的特征类型)。并将上述得到的各个程序碎片及其包括的多种维度特征的特征数据写入特征数据库。这样，检索服务器即可从特征数据库获取各个类

型的程序碎片及其特征数据，并将同一类型的程序碎片及其特征数据打包至同一个文件中。然后将得到的各个文件存储数据库中，并以字典分词的方式建立数据库的索引。该数据库可以是如图1所示的服务器集群20上的分布式数据库。

[0113] 需要说明的是，检索服务器可以实时获取特征数据库中更新的数据(即增量的特征)，并对服务器集群上的文件进行及时更新和替换，在数据库中，为了标识新增的数据，可以通过时间戳来区分每天新增的数据。

[0114] 通过上述实施例，可以实时收集已发布的各类安卓源程序，即相当于提供了相关的海量数据，并提取收集到的安卓源程序的多种维度特征，包括包名、证书、大小、版本、类、字符串等多种维度，这样，在进行病毒检测时，即可基于海量数据进行特征维度搜索，从而可以提高病毒检测的准确率。

[0115] 如图10所示，上述实施例中的查询单元40可以包括：查询模块401，用于按照特征类型从数据库中查询具有程序特征的程序碎片；拼接模块402，用于将查找到的程序碎片中，属于同一程序包的程序碎片进行拼接，得到样本程序包；读取模块403，用于读取查找到的样本程序包的安全指示信息。查询模块401包括：查询子模块4011，用于利用特征类型和索引，查询数据库中具有程序特征的程序碎片。

[0116] 分析人员根据需要分析的不同特征类型，在浏览器上面进行元特征(即待检测程序的程序特征)提交，同时可以对元特征进行逻辑上面的与或操作。如以包名、证书、大小、版本、类、字符串、代码块为特征类型进行元特征(即具体的程序特征，如具体的证书值、版本值)的提交。在通过WEB浏览器把进行逻辑操作过后的元特征数据通过post的方式提交至虚拟特征CGI之后，CGI接口端的设备对特征类型进行适配，检查分析人员提交的检索条件是否符合检索规则。如果符合检索规则，则对检索服务器发起检索请求，否则对该请求进行丢弃并且返回不符合检索规则的提示。

[0117] 检索服务器接收到CGI接口提交的请求后，会对提交上来的元数据进行解释，如对分析人员提交的检索条件进行解释，按照不同的类型和逻辑关系进行数据组合，生成满足搜索语法的语句，对存储集群发起数据检索。若分析人员提交的检索条件是需要检索满足“包名”和“证书”条件的程序碎片，则根据该检索条件生成满足搜索语法的语句，以进行查询。如根据待检测程序的程序特征从数据库中查询对应的程序碎片，即利用特征类型和索引，查询数据库中具有相同程序特征的程序碎片，并返回查询到的程序碎片。

[0118] CGI接口端的设备根据样本程序包从服务器端获取对应于该样本程序包的各个维度的信息(也即安全指示信息)，并将各个维度的信息进行打包并发送至检测终端(即上述分析人员使用的具有WEB服务器的电脑终端)。从而可以根据样本程序包(样本程序包的数量可以为1个，也可以为多个)的各个维度的信息(也即安全指示信息)确定待检测程序的安全性。如分析人员通过浏览器上面的安全指示信息进行对应的分析，判断出待检测程序的程序特征是否为病毒特征或者安全特征，以确定待检测程序是否为病毒或木马。

[0119] 通过上述实施例，突破了以往的单数据杀包可能导致的误杀漏杀；结合系统服务的多维度数据，对安卓包中各个维度的特征类型，进行快速检索和分析，依赖后台存储的海量数据，多安卓包数据、多维度数据去分析该安卓包的安全特性。同时提高了分析的效率，有效做到对安卓程序包病毒性特征更精确的检测。

[0120] 在一个可选的实施例中，在样本程序包为一个的情况下，如图11所示，确定单元50

可以包括:第一确定模块501,用于若安全指示信息指示样本程序包为病毒程序包,则确定待检测的程序特征为疑似病毒特征;第二确定模块502,用于若安全指示信息指示样本程序包是安全程序包,则确定待检测的程序特征为安全特征。

[0121] 在另一个可选的实施例中,在样本程序包为多个的情况下,如图12所示,确定单元50可以包括:第三确定模块503,用于基于各个样本程序包的安全指示信息确定样本程序包为病毒程序包或者为安全程序包;第四确定模块504,用于若确定多个样本程序包全部为安全程序包,则确定待检测的程序特征为安全特征;第五确定模块505,用于若确定的病毒程序包的个数超过预设个数,则确定待检测的程序特征为病毒特征,该预设个数可以为5,在得到的多个样本程序包中,若为病毒程序包的数量超过5个,则确定待检测的程序特征为病毒特征,即待检测程序为带病毒的程序;第六确定模块506,用于若确定的病毒程序包的个数不超过预设个数,则确定待检测的程序特征为疑似病毒特征,例如,在得到的多个样本程序包中,若为病毒程序包的数量大于0且不大于5个,则确定待检测的程序特征为疑似病毒特征,即待检测程序可能为带病毒的程序。

[0122] 可选地,上述的安全指示信息包括多个安全维度信息(如“安全级别”、“老白名单”、“新白名单”、“病毒id”等信息),其中,第三确定模块包括:获取子模块,用于获取样本程序包的安全指示信息的每个安全维度信息的属性值和每个安全维度信息的权重;判断子模块,用于判断每个安全维度信息的属性值和权重的乘积之和是否超过预设阈值;第一确定子模块,用于若超过预设阈值,则确定样本程序包为安全程序包;第二确定子模块,用于若未超过预设阈值,则确定样本程序包为病毒程序包。

[0123] 具体地,可以根据历史信息为每一个安全维度信息设置一个权重比,在得到每个安全维度信息的属性值之后,将其与对应的权重值相乘得到其权重,再将每个安全维度信息的权重相加,即可根据得到的和值和预设阈值判断样本程序包是否为病毒程序包。

[0124] 通过上述实施例,结合根据待检测程序的各个程序特征得到的样本程序包,并判断样本程序包的程序特征是否为病毒特征或者疑似病毒特征,从而可以实现对程序特征的准确识别。

[0125] 本实施例中所提供的各个模块与方法实施例对应步骤所提供的使用方法相同、应用场景也可以相同。当然,需要注意的是,上述模块涉及的方案可以不限于上述实施例中的内容和场景,且上述模块可以运行在计算机终端或移动终端,可以通过软件或硬件实现。

[0126] 实施例3

[0127] 根据本发明实施例,还提供了一种用于实施上述程序特征的检测方法的终端,上述实施例中的程序特征的检测装置可以设置在该终端上。

[0128] 如图13所示,该终端包括:一个或多个(图中仅示出一个)处理器901、存储器902、以及传输装置903,如图13所示,该终端还可以包括输入输出设备904。

[0129] 其中,存储器902可用于存储软件程序以及模块,如本发明实施例中的程序特征的检测方法和装置对应的程序指令/模块,处理器901通过运行存储在存储器902内的软件程序以及模块,从而执行各种功能应用以及数据处理,即实现上述的程序特征的检测方法。存储器902可包括高速随机存储器,还可以包括非易失性存储器,如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中,存储器902可进一步包括相对于处理器901远程设置的存储器,这些远程存储器可以通过网络连接至终端。上述网络的实例包

括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0130] 上述的传输装置903用于经由一个网络接收或者发送数据，还可以用于处理器与存储器之间的数据传输。上述的网络具体实例可包括有线网络及无线网络。在一个实例中，传输装置903包括一个网络适配器(Network Interface Controller，NIC)，其可通过网线与其他网络设备与路由器相连从而可与互联网或局域网进行通讯。在一个实例中，传输装置903为射频(Radio Frequency，RF)模块，其用于通过无线方式与互联网进行通讯。

[0131] 其中，具体地，存储器902用于存储应用程序。

[0132] 处理器901可以通过传输装置903调用存储器902存储的应用程序，以执行下述步骤：获取输入的待检测的程序特征和程序特征所属的特征类型；按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息，其中，安全指示信息用于指示样本程序包的安全特性；根据样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征。

[0133] 采用本发明上述实施例，在获取输入的待检测的程序特征和程序特征所属的特征类型之后，按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息(安全指示信息用于指示样本程序包的安全特性)，并根据得到的样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征，与相关技术中使用程序的签名信息进行病毒检测的方法相比，本申请的方案可以将需要检测程序的各类程序特征与海量数据库(数据库中存储有实时采集到的各类应用市场的程序应用的特征，如google应用市场、安卓市场、机锋市场等)中的样本程序包进行对比，以确定待检测的程序特征是否为病毒特征，从而解决了相关技术中不能对安卓软件的程序特征进行准确识别的技术问题，实现了对安卓软件的程序特征是否为病毒特征或者安全特征的准确判断，同时还能通过对程序特征的识别判断出待检测程序是否为包括病毒或木马的恶意软件。

[0134] 其中，待检测的程序特征可以为在检测安卓包时无法确定是否为病毒特征的特征，将这些特征提取出来，使用上述方法进行校验，可以准确验证该特征是否为病毒特征，并将确定结果用特征ID标识，如安全特征用0标识，疑似病毒特征用1标识，病毒特征用2标识。

[0135] 需要说明的是，为了提高检测的全面性和准确性，还可以在按照特征类型从数据库中查询具有程序特征的程序碎片之前，从收集到的源程序包中提取属于多个特征类型的程序碎片；将提取到的程序碎片按照程序碎片所属的特征类型，保存入数据库，并以字典分词的方式建立数据库的索引。从而通过数据库进行检测。

[0136] 上述实施例中的终端可以为台式计算机或移动终端，通过移动终端的屏幕输入的显示指令，可以为用户操作终端的屏幕输入的触摸指令，如长按指令、滑动指令等，本申请对显示指令的形式不作限定。

[0137] 可选地，本实施例中的具体示例可以参考上述实施例中所描述的示例，本实施例在此不再赘述。

[0138] 需要进一步说明的是，寄存区域为系统的内存和系统处理器中的寄存器。

[0139] 本领域普通技术人员可以理解，图13所示的结构仅为示意，终端可以是台式机、笔记本、平板电脑、掌上电脑以及移动互联网设备(Mobile Internet Devices，MID)、PAD等终端设备。图13其并不对上述电子装置的结构造成限定。例如，终端还可包括比图13中所示更多或者更少的组件(如网络接口、显示装置等)，或者具有与图13所示不同的配置。

[0140] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令终端设备相关的硬件来完成,该程序可以存储于一计算机可读存储介质中,存储介质可以包括:闪存盘、只读存储器(Read-Only Memory,ROM)、随机存取器(Random Access Memory,RAM)、磁盘或光盘等。

[0141] 实施例4

[0142] 本发明的实施例还提供了一种存储介质。可选地,在本实施例中,上述存储介质可以用于执行程序特征的检测方法。

[0143] 可选地,在本实施例中,上述存储介质可以位于上述实施例所示的网络中的多个网络设备中的至少一个网络设备上。

[0144] 可选地,在本实施例中,存储介质被设置为存储用于执行以下步骤的程序代码:获取输入的待检测的程序特征和程序特征所属的特征类型;按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息,其中,安全指示信息用于指示样本程序包的安全特性;根据样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征。

[0145] 采用本发明上述实施例,在获取输入的待检测的程序特征和程序特征所属的特征类型之后,按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息(安全指示信息用于指示样本程序包的安全特性),并根据得到的样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征,与相关技术中使用程序的签名信息进行病毒检测的方法相比,本申请的方案可以将需要检测程序的各类程序特征与海量数据库(数据库中存储有实时采集到的各类应用市场的程序应用的特征,如google应用市场、安卓市场、机锋市场等)中的样本程序包进行对比,以确定待检测的程序特征是否为病毒特征,从而解决了相关技术中不能对安卓软件的程序特征进行准确识别的技术问题,实现了对安卓软件的程序特征是否为病毒特征或者安全特征的准确判断,同时还能通过对程序特征的识别判断出待检测程序是否为包括病毒或木马的恶意软件。

[0146] 其中,待检测的程序特征可以为在检测安卓包时无法确定是否为病毒特征的特征,将这些特征提取出来,使用上述方法进行校验,可以准确验证该特征是否为病毒特征,并将确定结果用特征ID标识,如安全特征用0标识,疑似病毒特征用1标识,病毒特征用2标识。

[0147] 需要说明的是,为了提高检测的全面性和准确性,还可以在按照特征类型从数据库中查询具有程序特征的程序碎片之前,从收集到的源程序包中提取属于多个特征类型的程序碎片;将提取到的程序碎片按照程序碎片所属的特征类型,保存入数据库,并以字典分词的方式建立数据库的索引。从而通过数据库进行检测。

[0148] 上述实施例中的终端可以为台式计算机或移动终端,通过移动终端的屏幕输入的显示指令,可以为用户操作终端的屏幕输入的触摸指令,如长按指令、滑动指令等,本申请对显示指令的形式不作限定。

[0149] 可选地,本实施例中的具体示例可以参考上述实施例中所描述的示例,本实施例在此不再赘述。

[0150] 需要进一步说明的是,寄存区域为系统的内存和系统处理器中的寄存器。

[0151] 上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

[0152] 上述实施例中的集成的单元如果以软件功能单元的形式实现并作为独立的产品

销售或使用时，可以存储在上述计算机可读取的存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在存储介质中，包括若干指令用以使得一台或多台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。

[0153] 在本发明的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0154] 在本申请所提供的几个实施例中，应该理解到，所揭露的客户端，可通过其它的方式实现。其中，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

[0155] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0156] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0157] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

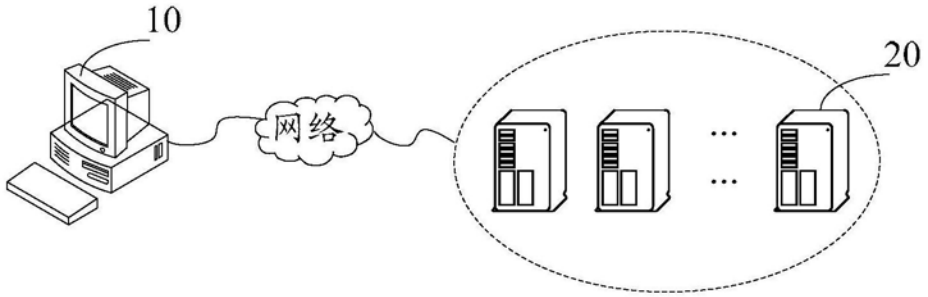

10
网络
20

图1

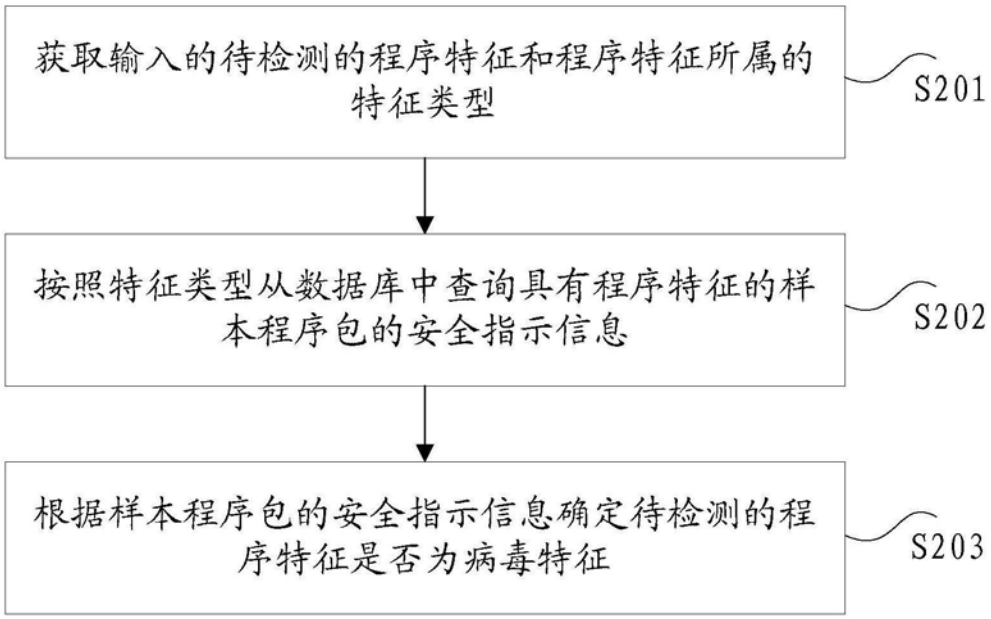

获取输入的待检测的程序特征和程序特征所属的特征类型
S201
按照特征类型从数据库中查询具有程序特征的样本程序包的安全指示信息
S202
根据样本程序包的安全指示信息确定待检测的程序特征是否为病毒特征
S203

图2

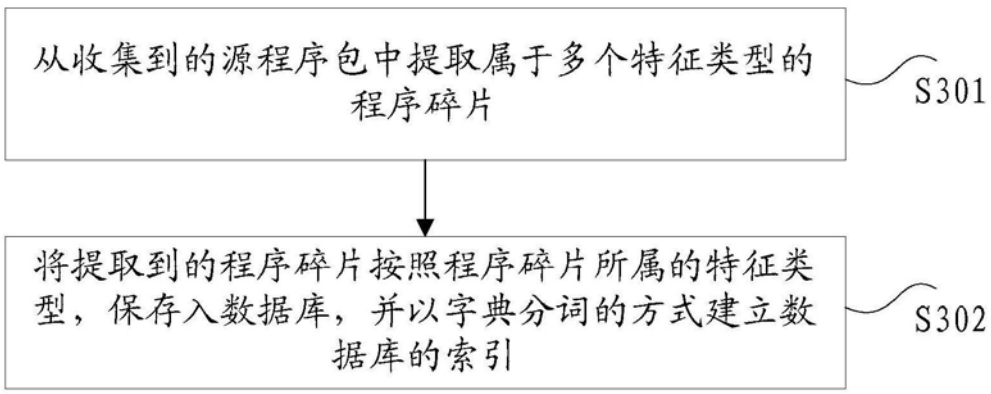

从收集到的源程序包中提取属于多个特征类型的程序碎片
S301
将提取到的程序碎片按照程序碎片所属的特征类型，保存入数据库，并以字典分词的方式建立数据库的索引
S302

图3

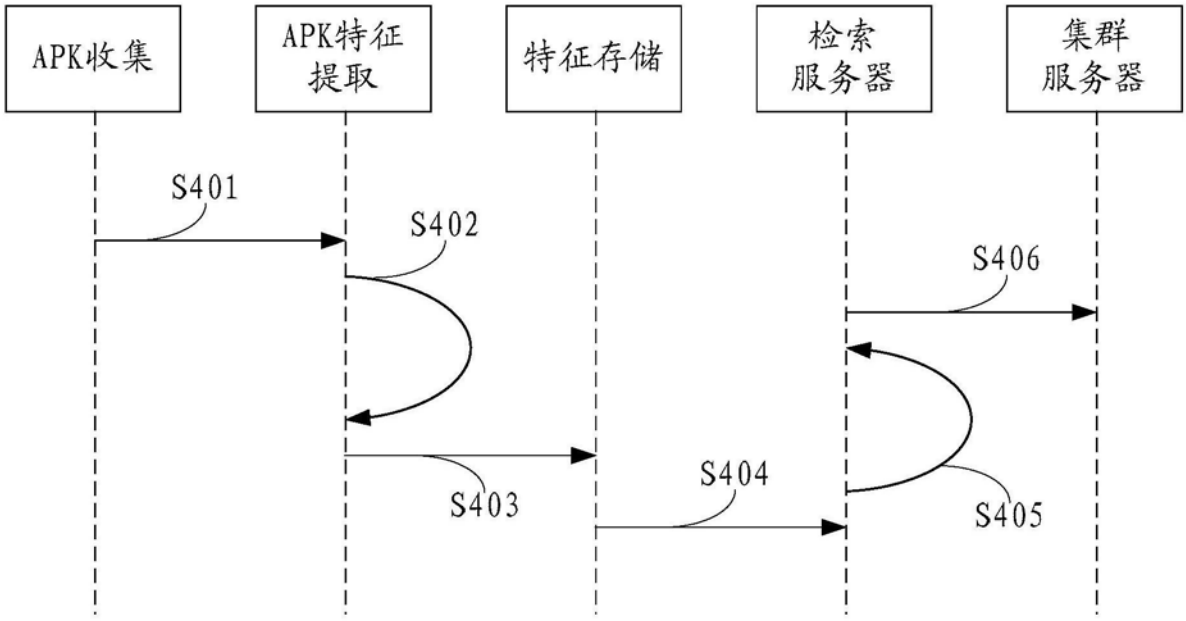

APK收集
APK特征提取
特征存储
检索服务器
集群服务器
S401
S402
S406
S403
S404
S405

图4

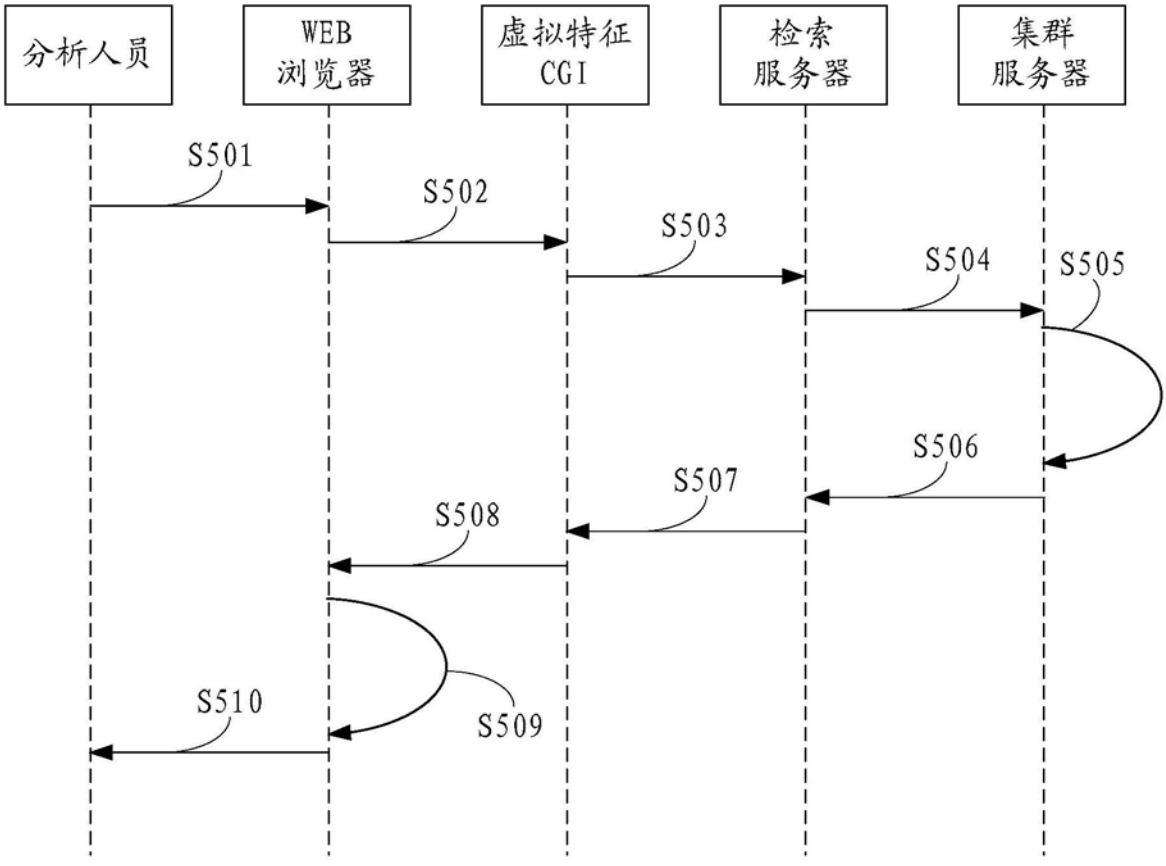

分析人员
WEB浏览器
虚拟特征CGI
检索服务器
集群服务器
S501
S502
S503
S504
S505
S506
S507
S508
S509
S510

图5

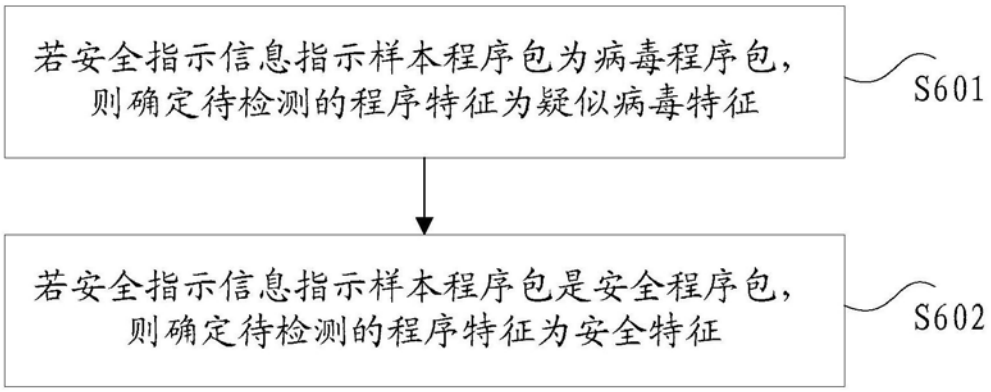

若安全指示信息指示样本程序包为病毒程序包，则确定待检测的程序特征为疑似病毒特征
S601
若安全指示信息指示样本程序包是安全程序包，则确定待检测的程序特征为安全特征
S602

图6

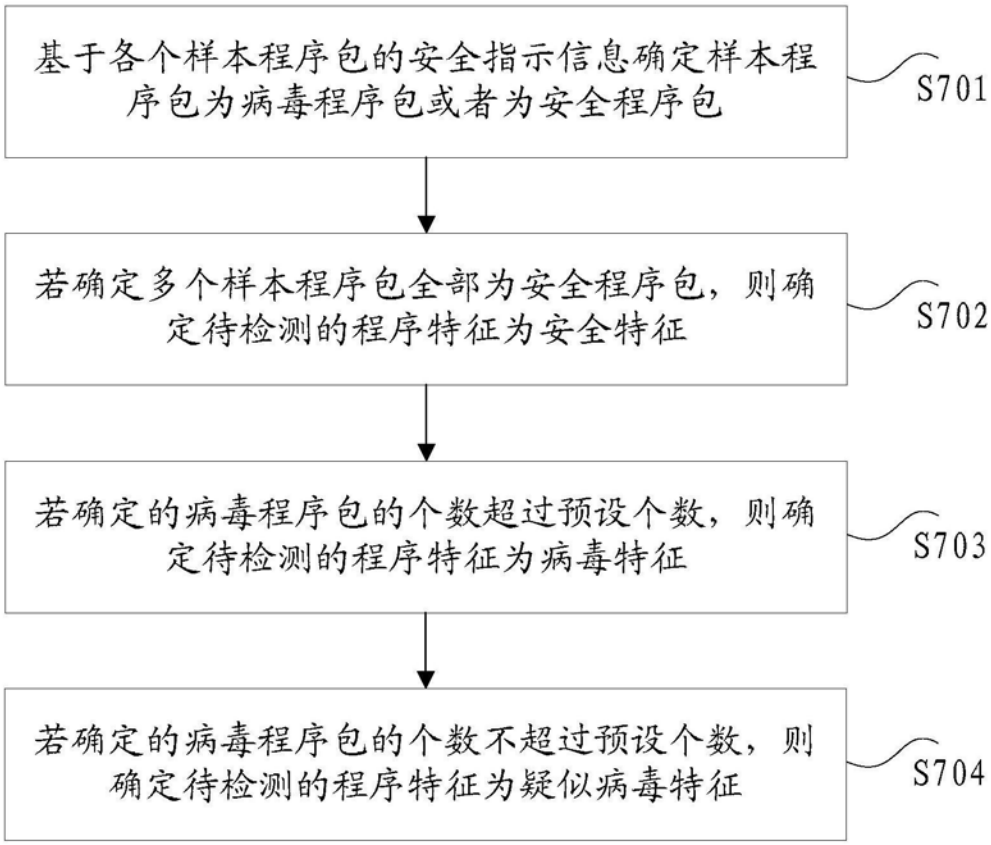

基于各个样本程序包的安全指示信息确定样本程序包为病毒程序包或者为安全程序包
S701
若确定多个样本程序包全部为安全程序包，则确定待检测的程序特征为安全特征
S702
若确定的病毒程序包的个数超过预设个数，则确定待检测的程序特征为病毒特征
S703
若确定的病毒程序包的个数不超过预设个数，则确定待检测的程序特征为疑似病毒特征
S704

图7

图8

图9

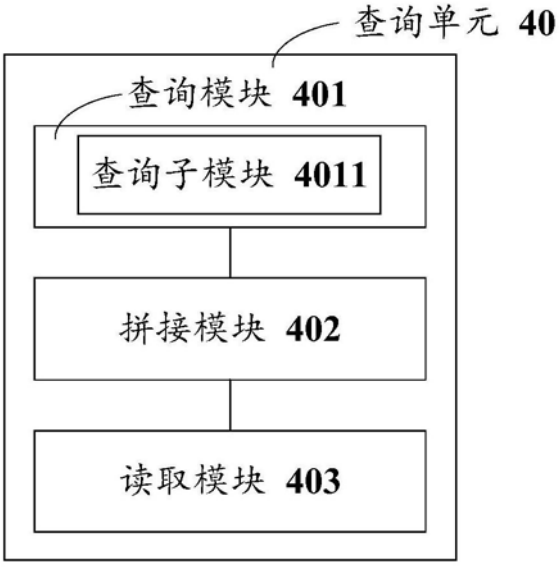

查询单元 40
查询模块 401
查询子模块 4011
拼接模块 402
读取模块 403

图10

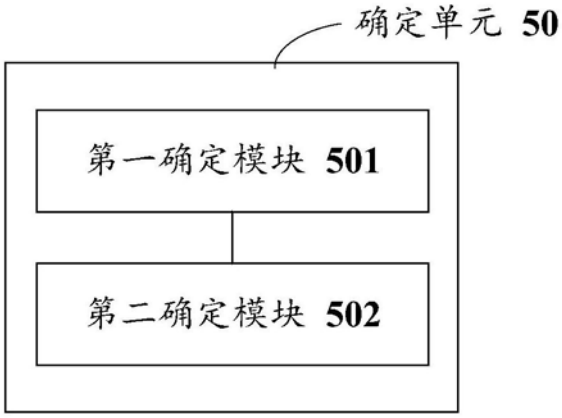

确定单元 50
第一确定模块 501
第二确定模块 502

图11

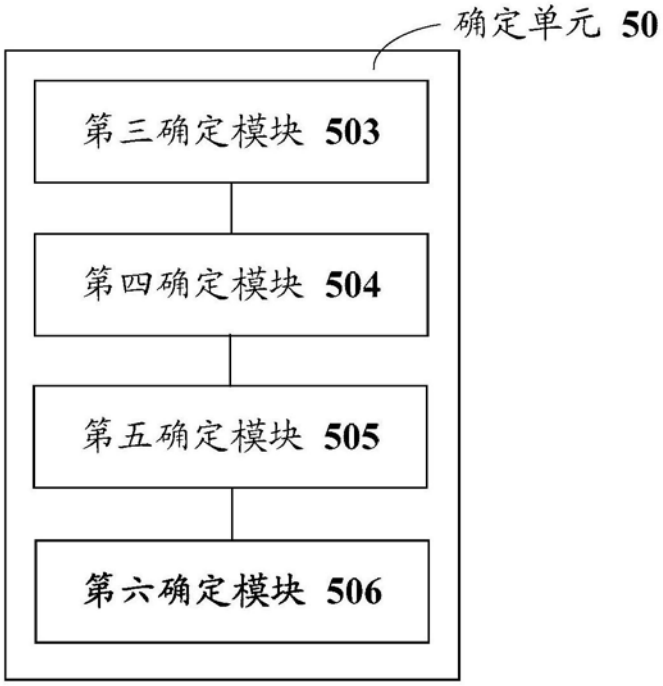


图12

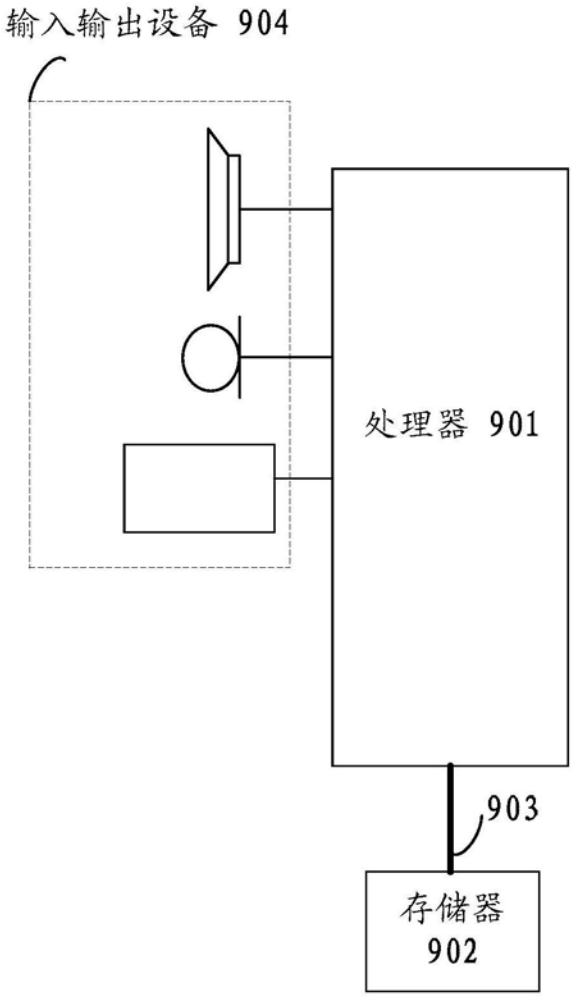


图13