

小程序恶意行为检测

技术领域

[01] 本说明书一个或多个实施例涉及计算机技术领域，尤其涉及小程序恶意行为检测。

背景技术

[02] 小程序是一种不需要下载安装即可使用的应用，一般需要依托于一定的小程序平台（其它的应用软件），通过小程序平台提供的业务接口实现其业务功能。恶意小程序会造成用户隐私数据的泄露以及财产损失等问题，因此如何对小程序是否存在恶意行为进行检测，成为程序开发者关注的焦点。

[03] 现有技术通过对小程序的静态代码进行安全扫描，以检测静态代码中是否存在恶意行为。但现有技术方案存在检测准确率较低的问题。因此，需要提供一种更可靠的小程序恶意行为检测方法。

发明内容

[04] 本说明书一个或多个实施例描述了小程序恶意行为检测方法和装置，能够提高小程序恶意行为检测的准确率。

[05] 根据第一方面，提供的小程序恶意行为检测方法，包括：获取在小程序运行过程中触发产生的至少两条行为记录；提取每一条行为记录的行为特征；将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合；每一个特征组合中包括至少两个行为特征，且该至少两个行为特征在该特征组合中的先后顺序与该至少两个行为特征对应的行为记录所产生的时间顺序相同；判断是否存在一个特征组合包括预设的恶意行为记录的特征组合；如果是，则确定该小程序存在恶意行为。

[06] 在一个实施例中，所述行为记录包括如下中的至少一项：所述小程序所调用的业务接口的名称、所述小程序调用业务接口时的时间信息、所述小程序发送的调用请求中的参数信息、所述小程序所接收到的调用请求响应中的参数信息和所述小程序调用业务接口之后对应的功能页面的信息。

[07] 在一个实施例中，所述获取在小程序运行过程中触发产生的至少两条行为记录，包括：获取在小程序运行过程中由该小程序产生的至少两条行为记录；所述将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合，包括：利用该小程序产

生的至少两条行为记录的行为特征，形成一个特征组合。

[08]在一个实施例中，所述获取在小程序运行过程中触发产生的至少两条行为记录，包括：获取在小程序运行过程中由该小程序产生的至少两条行为记录；针对该至少两条行为记录中相邻的两条行为记录，判断在从产生时间更早的行为记录所对应的第一功能页面跳转到产生时间更晚的行为记录所对应的第二功能页面时，该第一功能页面是否经由至少一个第三功能页面跳转到第二功能页面，如果是，针对第三功能页面生成对应的行为记录；将由该小程序产生的至少两条行为记录以及第三功能页面对应的行为记录，作为所述在小程序运行过程中触发产生的至少两条行为记录。

[09]在一个实施例中，所述将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合，包括：利用由该小程序产生的至少两条行为记录的行为特征形成第一特征组合；利用由该小程序产生的至少两条行为记录的行为特征以及对应第三功能页面的行为记录的行为特征，形成至少一个第二特征组合。

[10]在一个实施例中，所述获取在小程序运行过程中由该小程序产生的至少两条行为记录，包括：获取在小程序运行过程中该小程序在调用至少两个业务接口时所产生的至少两条行为记录。

[11]在一个实施例中，所述提取每一条行为记录的行为特征，包括：根据该条行为记录中包括的所述小程序所调用的业务接口的名称，确定该业务接口的分类；根据预先对各分类定义的分类值，确定该业务接口的分类对应的分类值；将确定的该分类值确定为该条行为记录的行为特征；和/或，根据该条行为记录中包括的所述小程序发送的调用请求中的参数信息和所述小程序所接收到的调用请求响应中的参数信息，检测参数信息中包括的隐私数据；根据预设的数据类型与敏感权重值的对应关系，确定该隐私数据所对应的敏感权重值；将该隐私数据所对应的敏感权重值，确定为该条行为记录的行为特征。

[12]根据第二方面，提供的小程序恶意行为检测装置，包括：行为记录获取单元，被配置为获取在小程序运行过程中触发产生的至少两条行为记录；行为特征提取单元，被配置为提取每一条行为记录的行为特征；特征组合单元，被配置为将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合；每一个特征组合中包括至少两个行为特征，且该至少两个行为特征在该特征组合中的先后顺序与该至少两个行为特征对应的行为记录所产生的时间顺序相同；判断单元，被配置为判断是否存在一个特征组合包括预设的恶意行为记录的特征组合；如果是，则确定该小程序存在恶意行为。

[13]在一个实施例中，所述行为记录包括如下中的至少一项：所述小程序所调用的业务接口的名称、所述小程序调用业务接口时的时间信息、所述小程序发送的调用请求中的参数信息、所述小程序所接收到的调用请求响应中的参数信息和所述小程序调用业务接口之后对应的功能页面的信息。

[14]在一个实施例中，所述行为记录获取单元，被配置为获取在小程序运行过程中由该小程序产生的至少两条行为记录；所述特征组合单元，被配置为利用该小程序产生的至少两条行为记录的行为特征，形成一个特征组合。

[15]在一个实施例中，所述行为记录获取单元，被配置为获取在小程序运行过程中由该小程序产生的至少两条行为记录；针对该至少两条行为记录中相邻的两条行为记录，判断在从产生时间更早的行为记录所对应的第一功能页面跳转到产生时间更晚的行为记录所对应的第二功能页面时，该第一功能页面是否经由至少一个第三功能页面跳转到第二功能页面，如果是，针对第三功能页面生成对应的行为记录；将由该小程序产生的至少两条行为记录以及第三功能页面对应的行为记录，作为所述在小程序运行过程中触发产生的至少两条行为记录。

[16]在一个实施例中，所述特征组合单元，被配置为利用由该小程序产生的至少两条行为记录的行为特征形成第一特征组合；利用由该小程序产生的至少两条行为记录的行为特征以及对应第三功能页面的行为记录的行为特征，形成至少一个第二特征组合。

[17]在一个实施例中，所述行为记录获取单元被配置为在获取在小程序运行过程中由该小程序产生的至少两条行为记录时，获取在小程序运行过程中该小程序在调用至少两个业务接口时所产生的至少两条行为记录。

[18]在一个实施例中，所述行为特征提取单元，被配置为根据该条行为记录中包括的所述小程序所调用的业务接口的名称，确定该业务接口的分类；根据预先对各分类定义的分类值，确定该业务接口的分类对应的分类值；将确定的该分类值确定为该条行为记录的行为特征；和/或，根据该条行为记录中包括的所述小程序发送的调用请求中的参数信息和所述小程序所接收到的调用请求响应中的参数信息，检测参数信息中包括的隐私数据；根据预设的数据类型与敏感权重值的对应关系，确定该隐私数据所对应的敏感权重值；将该隐私数据所对应的敏感权重值，确定为该条行为记录的行为特征。

[19]根据第三方面，提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行本说明书任一实施例所述的方法。

[20]根据第四方面，提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现本说明书任一实施例所述的方法。

[21]在本说明书实施例提供的小程序恶意行为检测方法和装置中，通过获取在小程序运行过程中触发产生的至少两条行为记录，并提取每一条行为记录的行为特征，然后将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合，如果存在一个特征组合包括预设的恶意行为记录的特征组合时，则确定该小程序存在恶意行为。本方案是针对小程序连续的多个调用行为是否存在恶意行为进行的检测，具有较高的调用行为覆盖率，因此可以提高小程序恶意行为检测的准确率。

附图说明

[22]为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本说明书的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[23]图1是本说明书一个实施例提供的系统架构示意图；

[24]图2是本说明书一个实施例提供的小程序恶意行为检测方法流程图；

[25]图3是本说明书一个实施例提供的行为记录获取的流程图；

[26]图4是本说明书一个实施例提供的行为记录的示意图；

[27]图5是本说明书另一个实施例提供的行为记录获取的流程图；

[28]图6是本说明书一个实施例提供的行为图谱示意图；

[29]图7是本说明书一个实施例提供的小程序恶意行为检测装置的结构图。

具体实施方式

[30]下面结合附图，对本说明书提供的方案进行描述。

[31]现有技术中通过对小程序的静态代码进行安全扫描，以检测静态代码中是否存在恶意行为。比如，检测静态代码中是否存在对固定特征的业务接口的调用，在调用业务接口时是否存在敏感信息的泄露等情况。现有技术都是针对单个业务接口的调用行为是否存在恶意进行的检测。然而，小程序在实际运行过程中存在连续的多个调用行为，该连

续的多个调用行为存在恶意行为。比如，小程序通过对多个不同业务接口的组合调用，将用户的敏感数据对外发送，但对单个业务接口的调用存在合理的业务需求。针对这种情况，现有技术无法检测出小程序存在的恶意行为，检测准确率较低。因此，本方案可以考虑获取小程序运行过程中的行为记录，并利用已有的恶意样本对小程序的行为记录进行检测，以确定该小程序是否存在恶意行为。

[32]下面描述以上构思的具体实现方式。

[33]为了方便对本说明书的理解，首先对本说明书所应用的系统架构进行描述。如图 1 所示，该系统架构主要包括客户端和服务端。

[34]客户端中安装有可以作为各小程序的宿主应用程序的应用程序，图 1 所示客户端中的 APP 为宿主应用程序，其中，宿主应用程序通过桥接（JavaScript Bridge）机制为各小程序提供可被调用的业务接口（JSAPI），各小程序通过调用各业务接口实现相应的业务功能。比如，宿主应用程序为“支付宝”，小程序为“菜鸟”、“交通出行”、“饿了么”等。

[35]其中，客户端可以是位于用户端的智能设备。比如，手机、平板电脑、笔记本电脑等。

[36]服务端可以是为宿主应用程序或者为客户端提供服务的服务器。

[37]图 2 示出根据一个实施例的小程序恶意行为检测方法的流程图。可以理解，该方法可以通过任何具有计算、处理能力的装置、设备、平台、设备集群来执行。参见图 2，此后，具体的实现包括：

[38]步骤 200：获取在小程序运行过程中触发产生的至少两条行为记录；

[39]步骤 202：提取每一条行为记录的行为特征；

[40]步骤 204：将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合；每一个特征组合中包括至少两个行为特征，且该至少两个行为特征在该特征组合中的先后顺序与该至少两个行为特征对应的行为记录所产生的时间顺序相同；

[41]步骤 206：判断是否存在一个特征组合包括预设的恶意行为记录的特征组合；如果是，则确定该小程序存在恶意行为。

[42]在图 2 所示的小程序恶意行为检测方法中，通过获取在小程序运行过程中触发产生的至少两条行为记录，并提取每一条行为记录的行为特征，然后将连续产生的至少两条

行为记录的至少两个行为特征形成至少一个特征组合，如果存在一个特征组合包括预设的恶意行为记录的特征组合时，则确定该小程序存在恶意行为。本方案是针对小程序连续的多个调用行为是否存在恶意行为进行的检测，具有较高的调用行为覆盖率，因此可以提高小程序恶意行为检测的准确率。

[43]下面描述图 2 所示的各个步骤的执行方式。

[44]针对步骤 200，获取在小程序运行过程中触发产生的至少两条行为记录。

[45]在本说明书实施例中，本步骤 200 中，小程序运行过程中会触发产生行为记录，而触发产生的该至少两条行为记录至少对应如下两种情形。

[46]情形一：该至少两条行为记录包括：在小程序运行过程中由该小程序产生的至少两条行为记录。

[47]情形二：该至少两条行为记录包括：在小程序运行过程中由该小程序产生的至少两条行为记录，以及，根据该由小程序产生的至少两条行为记录生成的行为记录。

[48]下面针对上述两种情形分别对本说明书实施例的行为记录获取方法进行说明。

[49]针对情形一：

[50]在该情形一时，图 3 示出了本说明书一个实施例提供的一种行为记录获取的流程图，请参考图 3，本步骤 200 具体可以包括：步骤 300：获取在小程序运行过程中由该小程序产生的至少两条行为记录。

[51]在本步骤 300 中，获取在小程序运行过程中由该小程序产生的至少两条行为记录时，可以是获取在小程序运行过程中该小程序在调用至少两个业务接口时所产生的至少两条行为记录。比如，小程序在调用上传文件功能的业务接口时会产生一条行为记录，小程序在调用下载文件功能的业务接口时会产生一条行为记录。

[52]可以理解，该行为记录除了是小程序在运行过程中调用业务接口产生的以外，还可以是小程序在运行过程中按小程序对应的静态代码执行相应逻辑时产生的。

[53]在本说明书实施例中，该行为记录可以包括如下中的至少一项：该小程序所调用的业务接口的名称、该小程序调用业务接口时的时间信息、该小程序发送的调用请求中的参数信息、该小程序所接收到的调用请求响应中的参数信息和该小程序调用业务接口之后对应的功能页面的信息。

[54]请参考图 4，为服务端获取到的在小程序运行过程中由该小程序产生的多条行为记

录的示意图。以第一条行为记录为例，对该行为记录中包括的内容进行说明。在第一条行为记录中，该小程序所调用的业务接口的名称为：GetUserInfo；该小程序调用该业务接口时的时间为：15:00:00；该小程序发送的调用请求中的参数信息为：参数 1；该小程序所接收到的调用请求响应中的参数信息为：返回结果 1；该小程序调用该业务接口之后对应的功能页面为：功能页面 1。

[55]针对情形二：

[56]在该情形二时，图 5 示出了本说明书一个实施例提供的另一种行为记录获取的流程图，请参考图 5，本步骤 200 具体可以包括：步骤 500：获取在小程序运行过程中由该小程序产生的至少两条行为记录。

[57]本步骤 500 与步骤 300 的执行过程相同，对本步骤 500 的描述请参考步骤 300 的描述，在此不再赘述。

[58]步骤 502：针对该至少两条行为记录中相邻的两条行为记录，判断在从产生时间更早的行为记录所对应的第一功能页面跳转到产生时间更晚的行为记录所对应的第二功能页面时，该第一功能页面是否经由至少一个第三功能页面跳转到第二功能页面，如果是，针对第三功能页面生成对应的行为记录。

[59]其中，本步骤所述相邻的两条行为记录是指，对步骤 500 中获取的至少两条行为记录按照行为记录产生时间的先后顺序进行排序后，处于相邻位置的两条行为记录。

[60]每一条行为记录都对应一个功能页面。比如，小程序在调用业务接口 1 之后会进入功能页面 1，在功能页面 1 上小程序调用了业务接口 2，那么在调用了业务接口 2 之后会进入功能页面 2。另外，根据行为记录包括的内容可知，该小程序调用业务接口之后对应的功能页面的信息可以位于行为记录中。

[61]以步骤 500 中获取的至少两条行为记录中相邻的行为记录 1 和行为记录 2 为例对本步骤进行说明。其中，行为记录 1 对应功能页面 1，行为记录 2 对应功能页面 2，行为记录 1 的产生时间早于行为记录 2 的产生时间。

[62]可以理解，服务端可以预先存储有小程序的各个功能页面之间的关系。根据功能页面 1 与功能页面 2 之间的关系可以确定，该小程序从功能页面 1 跳转到功能页面 2 时除了从功能页面 1 直接跳转到功能页面 2 之外，还可以经由一个功能页面 1A1、功能页面 1A2 之后跳转到功能页面 2，以及还可以经由一个功能页面 1B1 之后跳转到功能页面 2，即从功能页面 1 跳转到功能页面 2 存在如下三条路径：

[63] 路径 1: 功能页面 1→功能页面 2;

[64] 路径 2: 功能页面 1→功能页面 1A1→功能页面 1A2→功能页面 2;

[65] 路径 3: 功能页面 1→功能页面 1B1→功能页面 2。

[66] 那么需要针对功能页面 1A1、功能页面 1A2 和功能页面 1B1 分别生成对应的行为记录。

[67] 在针对第三功能页面生成对应的行为记录时, 可以根据预先存储的功能页面与业务接口的对应关系, 以及在调用该业务接口和返回调用请求响应时对应的参数信息, 生成对应的行为记录。需要说明的是, 第三功能页面对应行为记录的产生时间需要位于第一功能页面和第二功能页面之间。以路径 2 为例, 该路径 2 中包括的各功能页面所对应的行为记录的产生时间按照先后顺序依次为: 各功能页面 1、功能页面 1A1、功能页面 1A2、功能页面 2。

[68] 步骤 504: 将由该小程序产生的至少两条行为记录以及第三功能页面对应的行为记录, 作为所述在小程序运行过程中触发产生的至少两条行为记录。

[69] 通过确定相邻的两条行为记录分别对应的第一功能页面和第二功能页面之间是否存在经由的第三功能页面, 以及针对经由的第三功能页面生成对应的行为记录, 并将第三功能页面生成的行为记录与由该小程序产生的至少两条行为记录的一起, 作为在小程序运行过程中触发产生的至少两条行为记录。使得用于检测小程序是否存在恶意行为的行为记录更加丰富, 进而在利用更丰富的行为记录分析小程序是否存在恶意行为时, 检测准确率更高。

[70] 无论是情形一还是情形二, 在本说明书实施例中, 小程序运行过程中触发产生的行为记录可以是由客户端获取并发来的。

[71] 根据前述对本说明书所应用的系统架构进行的描述可知, 宿主应用程序通过桥接机制为各小程序提供可被调用的业务接口。在小程序调用一个业务接口时, 会按照约定的协议向 JavaScript Bridge 发送调用请求, 其中调用请求中包括携带的参数信息和所需调用的业务接口的信息。然后, 由宿主应用程序根据该业务接口的信息调用该业务接口, 从而向该小程序返回调用请求响应。因此, 客户端可以获取到小程序在运行过程中调用至少两个业务接口时所产生的至少两条行为记录。

[72] 在本说明书一个实施例中, 客户端在获取行为记录时, 可以通过一个安全切面模块来实现。具体地, 可以利用 Hook (钩子函数) 方式或静态代码替换方式, 对 JavaScript

Bridge 进行切面,使得当小程序在向 JavaScript Bridge 发送调用请求时先将执行逻辑路由到一个安全切面模块上,由该安全切面模块接收调用请求,并转发给 JavaScript Bridge,以及 JavaScript Bridge 在将调用请求响应发送给安全切面模块,由安全切面模块将调用请求响应发送给小程序。如此,安全切面模块就可以获取到小程序调用业务接口时的行为记录了。

[73]其中,切面,即面向切面编程(AOP, Aspect-oriented Programming),它是通过预编译、运行时动态代理或注入的方式,实现在不修改源代码的情况下给程序动态添加功能的编程范式。因此,通过安全切面模块来获取调用请求和调用请求响应,可以对小程序对业务接口的调用行为进行监控,在不影响小程序实现其业务功能的情况下,实现对该调用行为的记录。

[74]针对步骤 202,提取每一条行为记录的行为特征。

[75]在本说明书实施例中,在提取行为特征时,至少可以针对如下两个维度分别进行提取。

[76]维度一:行为记录所对应业务接口的功能。

[77]维度二:行为记录所对应数据的敏感程度。

[78]下面针对上述两个维度分别对该行为特征的提取进行说明。

[79]在维度一上,本步骤 202 可以包括:根据该条行为记录中包括的所述小程序所调用的业务接口的名称,确定该业务接口的分类;根据预先对各分类定义的分类值,确定该业务接口的分类对应的分类值;将确定的该分类值确定为该条行为记录的行为特征。

[80]在本说明书实施例中,可以预先针对宿主应用程序可以提供的全量业务接口,根据各业务接口实现的业务功能,对全量业务接口进行分类。比如,该分类可以包括:文件操作类、网络操作类、设备信息类等。并针对每一个分类定义分类值,比如,文件操作类对应分类值为 1,网络操作类对应的分类值为 2,设备信息类对应的分类值为 3。

[81]可以理解,服务端中存储有业务接口名称、分类及分类值的对应关系。那么针对一条行为记录提取行为特征时,可以直接根据行为记录中包括的该小程序所调用的业务接口的名称以及存储的对应关系,确定出分类值,将确定出的该分类值确定为该条行为记录的行为特征。

[82]需要说明的是,在该维度一上,除上述针对分类定义分类值以外,还可以有其他形

式的定义。比如，进一步细化分类粒度。以文件操作类包括的业务接口的功能为：上传文件、下载文件、获取文件路径等为例，可以针对文件操作类中的上传文件、下载文件、获取文件路径分别定义一个对应的分类值，以该分类值作为提取的行为特征之后，在利用该行为特征检测小程序是否存在恶意行为时，使得检测准确率进一步提高。

[83]在维度二上，本步骤 202 可以包括：根据该条行为记录中包括的所述小程序发送的调用请求中的参数信息和所述小程序所接收到的调用请求响应中的参数信息，检测参数信息中包括的隐私数据；根据预设的数据类型与敏感权重值的对应关系，确定该隐私数据所对应的敏感权重值；将该隐私数据所对应的敏感权重值，确定为该条行为记录的行为特征。

[84]在本说明书实施例中，由于小程序在调用业务接口时可能会涉及到隐私数据，而小程序存在恶意行为与隐私数据存在一定的关系。因此，可以将行为记录中所对应数据的敏感程度作为一个维度，来提取行为特征。

[85]在本说明书实施例中，服务端可以预先对隐私数据的数据类型进行定义，以及定义每一个数据类型的敏感权重值。该数据类型可以包括位置信息、用户 ID、身份信息、文件名等。在对每一个数据类型定义敏感权重值时，可以依据该数据类型所对应数据的敏感程度来定义。比如，身份信息的敏感权重值高于位置信息的敏感权重值。

[86]可以理解，服务端中存储有各数据类型与敏感权重值的对应关系。那么针对一条行为记录提取行为特征时，可以直接根据行为记录中包括的参数信息（该小程序发送的调用请求中的参数信息和该小程序所接收到的调用请求响应中的参数信息），检测该参数信息是否包括隐私数据，并确定该隐私数据的数据类型。然后，根据服务端中存储的各数据类型与敏感权重值的对应关系，确定出该隐私数据对应的敏感权重值。

[87]需要说明的是，在该维度二上，如果行为记录中的参数信息中包括多个隐私数据，那么可以利用每一个隐私数据的敏感权重值计算出该行为记录的综合敏感权重值，将该综合敏感权重值确定为该条行为记录的行为特征。

[88]其中，该综合敏感权重值的计算方式可以有多种，比如，将各隐私数据的敏感权重值相加，再比如，将各隐私数据的敏感权重值相加之和处于隐私数据的个数等。

[89]作为本说明书一个优选实施例，将上述两个维度上分别确定的分类值和敏感权重值，均作为该条行为记录的行为特征，在利用该优选实施例的行为特征进行后续特征组合的比较判断时，需要分类值和敏感权重值均相同，才能确定该行为特征相同，如此，分析

粒度更细化，进一步提高了检测准确度。

[90] 本说明书实施例中，通过将行为特征量化为数值形式，在利用数值形式的行为特征进行后续特征组合的比较判断时，可以直接比较数值是否相等来确定行为特征是否相同，判断比较过程更加便捷，提高了小程序恶意行为的检测速度。

[91] 针对步骤 204，将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合；每一个特征组合中包括至少两个行为特征，且该至少两个行为特征在该特征组合中的先后顺序与该至少两个行为特征对应的行为记录所产生的时间顺序相同。

[92] 在本说明书实施例中，在步骤 200 中小程序运行过程中触发产生的至少两条行为记录对应不同的情形时，本步骤 204 形成的特征组合会不同。下面对两种情形分别进行说明。

[93] 在步骤 200 中小程序运行过程中触发产生的至少两条行为记录对应情形一时，该步骤 204 可以包括：利用该小程序产生的至少两条行为记录的行为特征，形成一个特征组合。

[94] 举例来说，根据步骤 200 可以得到：按行为记录的产生时间的先后顺序依次为，行为记录 1、行为记录 2、行为记录 3……行为记录 n，n 为不小于 2 的整数。根据步骤 202 可以提取依次提取出行为特征 1、行为特征 2、行为特征 3……行为特征 n。那么本步骤 204 中形成的一个特征组合为：行为特征 1、行为特征 2、行为特征 3……行为特征 n。

[95] 在步骤 200 中小程序运行过程中触发产生的至少两条行为记录对应情形二时，该步骤 204 可以包括：利用由该小程序产生的至少两条行为记录的行为特征形成第一特征组合；利用由该小程序产生的至少两条行为记录的行为特征以及对应第三功能页面的行为记录的行为特征，形成至少一个第二特征组合。

[96] 举例来说，根据步骤 200 可以得到：按行为记录的产生时间的先后顺序依次为，行为记录 1、行为记录 2、行为记录 3……行为记录 n，n 为不小于 2 的整数。且从行为记录 1 对应的功能页面 1 跳转到行为记录 2 对应的功能页面 2 时还可以经由一个功能页面 1A1，以及从行为记录 2 对应的功能页面 2 跳转到行为记录 3 对应的功能页面 3 时还可以经由一个功能页面 2A1。那么针对功能页面 1A1 和功能页面 2A1 生成有行为记录 1A1 和行为记录 2A1。根据步骤 202 可以提取依次提取出行为特征 1、行为特征 1A1、行为特征 2、行为特征 2A1、行为特征 3……行为特征 n。

[97] 在形成特征组合时，为了便于确定可以形成的特征组合的个数，可以先还原出小程

序的行为图谱。图6为本说明书实施例公开的一个行为图谱示意图,该行为图谱由各行为节点及行为节点间的边关系组成,行为节点与行为记录相对应。根据该行为图谱,可以得出四条行为链路:行为节点1→行为节点2→行为节点3.....行为节点n;行为节点1→行为节点2→行为节点2A1→行为节点3.....行为节点n;行为节点1→行为节点1A1→行为节点2→行为节点3.....行为节点n;行为节点1→行为节点1A1→行为节点2→行为节点2A1→行为节点3.....行为节点n。

[98]那么得到的上述四条行为链路,本步骤204可以形成四个特征组合。

[99]首先,根据第一条行为链路,可以利用行为记录1、行为记录2、行为记录3.....行为记录n的行为特征形成一个特征组合:行为特征1、行为特征2、行为特征3.....行为特征n。

[100]然后,根据第二至四条行为链路,可以利用行为记录1、行为记录1A1、行为记录2、行为记录2A1、行为记录3.....行为记录n,形成三个特征组合,分别为:

[101]特征组合1:行为特征1、行为特征2、行为特征2A1、行为特征3.....行为特征n。

[102]特征组合2:行为特征1、行为特征1A1、行为特征2、行为特征3.....行为特征n。

[103]特征组合3:行为特征1、行为特征1A1、行为特征2、行为特征2A1、行为特征3.....行为特征n。

[104]针对步骤206,判断是否存在一个特征组合包括预设的恶意行为记录的特征组合,如果是,则确定该小程序存在恶意行为。

[105]在本说明书实施例中,该恶意行为记录的特征组合是针对已经发现的具有恶意行为的恶意行为记录按照步骤202至步骤204所形成的特征组合。

[106]例如,该恶意行为为如下连续的三个行为:调用用户摄像头进行拍照→文件保存到本地→上传图片到服务器。

[107]再如,该恶意行为为如下连续的五個行为:设置小程序标题(XXX棋牌游戏)→打开支付接口→输入固定的收款账号→获取支付状态。

[108]在本说明书实施例中,以特征组合为行为特征1、行为特征2、行为特征3、行为特征4、行为特征5.....行为特征n为例,以及将步骤202中两个维度上的确定的分类值和敏感权重值,均作为该条行为记录的行为特征,那么该特征组合为:(X1, Y1)、(X2, Y2)、(X3, Y3)、(X4, Y4)、(X5, Y5).....(Xn, Yn),其中, Xn 用于表征行为特征 n

的分类值， Y_n 用于表征行为特征 n 的敏感权重值。

[109] 假设一个已知的恶意行为记录的特征组合为：(X2, Y2)、(X3, Y3)、(X4, Y4)。那么在判断针对小程序形成的特征组合是否包括该恶意行为记录的特征组合时，需要按顺序比较一一对应位置上的行为特征是否相同。比如，首先，比较小程序形成的特征组合中的(X1, Y1)、(X2, Y2)、(X3, Y3)三个行为特征，与该恶意行为记录的特征组合是否相同，比较结果为不相同。然后，比较小程序形成的特征组合中的(X2, Y2)、(X3, Y3)、(X4, Y4)三个行为特征，与该恶意行为记录的特征组合是否相同，比较结果为相同。那么就可以确定该小程序形成的特征组合包括该恶意行为记录的特征组合。

[110] 以上实现了对小程序恶意行为的检测。

[111] 另一方面的实施例，还提供了一种小程序恶意行为检测装置，如图 7 示出一个实施例的小程序恶意行为检测装置。可以理解，该装置可以通过任何具有计算、处理能力的装置、设备、平台和设备集群来实现。如图 7 所示，该装置 70 包括：行为记录获取单元 71，被配置为获取在小程序运行过程中触发产生的至少两条行为记录；行为特征提取单元 72，被配置为提取每一条行为记录的行为特征；特征组合单元 73，被配置为将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合；每一个特征组合中包括至少两个行为特征，且该至少两个行为特征在该特征组合中的先后顺序与该至少两个行为特征对应的行为记录所产生的时间顺序相同；判断单元 74，被配置为判断是否存在一个特征组合包括预设的恶意行为记录的特征组合；如果是，则确定该小程序存在恶意行为。

[112] 一种可能的实施方式中，所述行为记录包括如下中的至少一项：所述小程序所调用的业务接口的名称、所述小程序调用业务接口时的时间信息、所述小程序发送的调用请求中的参数信息、所述小程序所接收到的调用请求响应中的参数信息和所述小程序调用业务接口之后对应的功能页面的信息。

[113] 一种可能的实施方式中，所述行为记录获取单元 71，被配置为获取在小程序运行过程中由该小程序产生的至少两条行为记录；所述特征组合单元 73，被配置为利用该小程序产生的至少两条行为记录的行为特征，形成一个特征组合。

[114] 一种可能的实施方式中，所述行为记录获取单元 71，被配置为获取在小程序运行过程中由该小程序产生的至少两条行为记录；针对该至少两条行为记录中相邻的两条行为记录，判断在从产生时间更早的行为记录所对应的第一功能页面跳转到产生时间更晚

的行为记录所对应的第二功能页面时,该第一功能页面是否经由至少一个第三功能页面跳转到第二功能页面,如果是,针对第三功能页面生成对应的行为记录;将由该小程序产生的至少两条行为记录以及第三功能页面对应的行为记录,作为所述在小程序运行过程中触发产生的至少两条行为记录。

[115]一种可能的实施方式中,所述特征组合单元 73,被配置为利用由该小程序产生的至少两条行为记录的行为特征形成第一特征组合;利用由该小程序产生的至少两条行为记录的行为特征以及对应第三功能页面的行为记录的行为特征,形成至少一个第二特征组合。

[116]一种可能的实施方式中,所述行为记录获取单元 71 被配置为在获取在小程序运行过程中由该小程序产生的至少两条行为记录时,获取在小程序运行过程中该小程序在调用至少两个业务接口时所产生的至少两条行为记录。

[117]一种可能的实施方式中,所述行为特征提取单元 73,被配置为根据该条行为记录中包括的所述小程序所调用的业务接口的名称,确定该业务接口的分类;根据预先对各分类定义的分类值,确定该业务接口的分类对应的分类值;将确定的该分类值确定为该条行为记录的行为特征;和/或,根据该条行为记录中包括的所述小程序发送的调用请求中的参数信息和所述小程序所接收到的调用请求响应中的参数信息,检测参数信息中包括的隐私数据;根据预设的数据类型与敏感权重值的对应关系,确定该隐私数据所对应的敏感权重值;将该隐私数据所对应的敏感权重值,确定为该条行为记录的行为特征。

[118]本说明书一个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,当所述计算机程序在计算机中执行时,令计算机执行说明书中任一个实施例中的方法。

[119]本说明书一个实施例提供了一种计算设备,包括存储器和处理器,所述存储器中存储有可执行代码,所述处理器执行所述可执行代码时,实现执行说明书中任一个实施例中的方法。

[120]可以理解的是,本说明书实施例示意的结构并不构成对小程序恶意行为检测装置的具体限定。在说明书的另一些实施例中,小程序恶意行为检测装置可以包括比图示更多或者更少的部件,或者组合某些部件,或者拆分某些部件,或者不同的部件布置。图示的部件可以以硬件、软件或者软件和硬件的组合来实现。

[121]上述装置、系统内的各模块之间的信息交互、执行过程等内容,由于与本说明书方法实施例基于同一构思,具体内容可参见本说明书方法实施例中的叙述,此处不再赘

述。

[122] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[123] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、挂件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

[124] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

权利要求书

1、小程序恶意行为检测方法，包括：

获取在小程序运行过程中触发产生的至少两条行为记录；

提取每一条行为记录的行为特征；

将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合；每一个特征组合中包括至少两个行为特征，且该至少两个行为特征在该特征组合中的先后顺序与该至少两个行为特征对应的行为记录所产生的时间顺序相同；

判断是否存在一个特征组合包括预设的恶意行为记录的特征组合；

如果是，则确定该小程序存在恶意行为。

2、根据权利要求1所述的方法，其中，所述行为记录包括如下中的至少一项：所述小程序所调用的业务接口的名称、所述小程序调用业务接口时的时间信息、所述小程序发送的调用请求中的参数信息、所述小程序所接收到的调用请求响应中的参数信息和所述小程序调用业务接口之后对应的功能页面的信息。

3、根据权利要求1所述的方法，其中，

所述获取在小程序运行过程中触发产生的至少两条行为记录，包括：获取在小程序运行过程中由该小程序产生的至少两条行为记录；

所述将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合，包括：利用该小程序产生的至少两条行为记录的行为特征，形成一个特征组合。

4、根据权利要求1所述的方法，其中，所述获取在小程序运行过程中触发产生的至少两条行为记录，包括：

获取在小程序运行过程中由该小程序产生的至少两条行为记录；

针对该至少两条行为记录中相邻的两条行为记录，判断在从产生时间更早的行为记录所对应的第一功能页面跳转到产生时间更晚的行为记录所对应的第二功能页面时，该第一功能页面是否经由至少一个第三功能页面跳转到第二功能页面，如果是，针对第三功能页面生成对应的行为记录；

将由该小程序产生的至少两条行为记录以及第三功能页面对应的行为记录，作为所述在小程序运行过程中触发产生的至少两条行为记录。

5、根据权利要求4所述的方法，其中，所述将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合，包括：

利用由该小程序产生的至少两条行为记录的行为特征形成第一特征组合；

利用由该小程序产生的至少两条行为记录的行为特征以及对应第三功能页面的行

为记录的行为特征，形成至少一个第二特征组合。

6、根据权利要求 3 或 4 所述的方法，其中，所述获取在小程序运行过程中由该小程序产生的至少两条行为记录，包括：

获取在小程序运行过程中该小程序在调用至少两个业务接口时所产生的至少两条行为记录。

7、根据权利要求 1 所述的方法，其中，所述提取每一条行为记录的行为特征，包括：

根据该条行为记录中包括的所述小程序所调用的业务接口的名称，确定该业务接口的分类；根据预先对各分类定义的分类值，确定该业务接口的分类对应的分类值；将确定的该分类值确定为该条行为记录的行为特征；

和/或，

根据该条行为记录中包括的所述小程序发送的调用请求中的参数信息和所述小程序所接收到的调用请求响应中的参数信息，检测参数信息中包括的隐私数据；根据预设的数据类型与敏感权重值的对应关系，确定该隐私数据所对应的敏感权重值；将该隐私数据所对应的敏感权重值，确定为该条行为记录的行为特征。

8、小程序恶意行为检测装置，包括：

行为记录获取单元，被配置为获取在小程序运行过程中触发产生的至少两条行为记录；

行为特征提取单元，被配置为提取每一条行为记录的行为特征；

特征组合单元，被配置为将连续产生的至少两条行为记录的至少两个行为特征形成至少一个特征组合；每一个特征组合中包括至少两个行为特征，且该至少两个行为特征在该特征组合中的先后顺序与该至少两个行为特征对应的行为记录所产生的时间顺序相同；

判断单元，被配置为判断是否存在一个特征组合包括预设的恶意行为记录的特征组合；如果是，则确定该小程序存在恶意行为。

9、根据权利要求 8 所述的装置，其中，所述行为记录包括如下中的至少一项：所述小程序所调用的业务接口的名称、所述小程序调用业务接口时的时间信息、所述小程序发送的调用请求中的参数信息、所述小程序所接收到的调用请求响应中的参数信息和所述小程序调用业务接口之后对应的功能页面的信息。

10、根据权利要求 8 所述的装置，其中，

所述行为记录获取单元，被配置为获取在小程序运行过程中由该小程序产生的至少

两条行为记录；

所述特征组合单元，被配置为利用该小程序产生的至少两条行为记录的行为特征，形成一个特征组合。

11、根据权利要求 8 所述的装置，其中，所述行为记录获取单元，被配置为获取在小程序运行过程中由该小程序产生的至少两条行为记录；针对该至少两条行为记录中相邻的两条行为记录，判断在从产生时间更早的行为记录所对应的第一功能页面跳转到产生时间更晚的行为记录所对应的第二功能页面时，该第一功能页面是否经由至少一个第三功能页面跳转到第二功能页面，如果是，针对第三功能页面生成对应的行为记录；将由该小程序产生的至少两条行为记录以及第三功能页面对应的行为记录，作为所述在小程序运行过程中触发产生的至少两条行为记录。

12、根据权利要求 11 所述的装置，其中，所述特征组合单元，被配置为利用由该小程序产生的至少两条行为记录的行为特征形成第一特征组合；利用由该小程序产生的至少两条行为记录的行为特征以及对应第三功能页面的行为记录的行为特征，形成至少一个第二特征组合。

13、根据权利要求 10 或 11 所述的装置，其中，所述行为记录获取单元被配置为在获取在小程序运行过程中由该小程序产生的至少两条行为记录时，获取在小程序运行过程中该小程序在调用至少两个业务接口时所产生的至少两条行为记录。

14、根据权利要求 8 所述的装置，其中，所述行为特征提取单元，被配置为根据该条行为记录中包括的所述小程序所调用的业务接口的名称，确定该业务接口的分类；根据预先对各分类定义的分类值，确定该业务接口的分类对应的分类值；将确定的该分类值确定为该条行为记录的行为特征；和/或，根据该条行为记录中包括的所述小程序发送的调用请求中的参数信息和所述小程序所接收到的调用请求响应中的参数信息，检测参数信息中包括的隐私数据；根据预设的数据类型与敏感权重值的对应关系，确定该隐私数据所对应的敏感权重值；将该隐私数据所对应的敏感权重值，确定为该条行为记录的行为特征。

15、一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行权利要求 1-7 中任一项所述的方法。

16、一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-7 中任一项所述的方法。