(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 106295333 A
(43)申请公布日 2017.01.04

(21)申请号 201510280539.1

(22)申请日 2015.05.27

(71)申请人 安一恒通(北京)科技有限公司
地址 100091 北京市海淀区东北旺西路8号中关村软件园4号楼C座1-03

(72)发明人 邹荣新 梅银明 姚俊

(74)专利代理机构 北京英赛嘉华知识产权代理有限责任公司 11204
代理人 王达佐 马晓亚

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

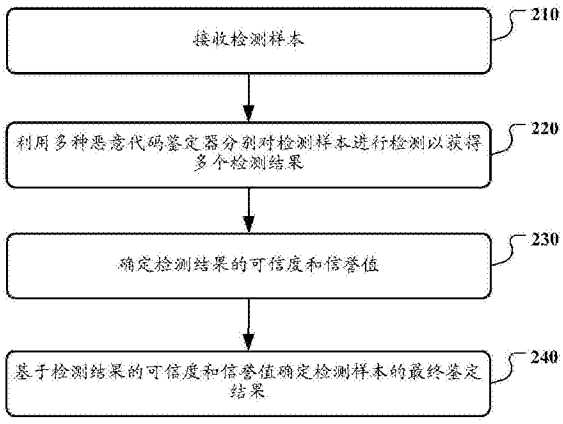
权利要求书3页 说明书9页 附图4页

(54)发明名称

用于检测恶意代码的方法和系统

(57)摘要

本申请公开了一种恶意代码检测方法和系统。该方法包括:接收检测样本;利用多种恶意代码鉴定器分别对检测样本进行检测以获得多个检测结果;确定检测结果的可信度和信誉值,其中可信度表示检测结果是否具有恶意性和/或安全性,信誉值为对应可信度的量化信任程度;以及基于检测结果的可信度和信誉值确定检测样本的最终鉴定结果。按照本申请的技术方案,合理利用各种恶意代码鉴定器的检测结果,提高了对恶意代码的检测精准率。



CN 106295333 A

1. 一种检测恶意代码的方法，包括：

接收检测样本；

利用多种恶意代码鉴定器分别对所述检测样本进行检测以获得多个检测结果；

确定检测结果的可信度和信誉值，其中所述可信度表示检测结果是否具有恶意性和/或安全性，所述信誉值为对应可信度的量化信任程度；以及

基于所述检测结果的可信度和信誉值确定所述检测样本的最终鉴定结果。

2. 根据权利要求 1 所述的方法，其中，确定检测结果的可信度和信誉值包括：

根据文件信誉评分策略，确定检测结果的可信度和信誉值；

其中，在所述文件信誉评分策略中，根据已知的各种恶意代码的信息，预先设置各类恶意代码检测结果的可信度；以及根据恶意代码鉴定器的误报率，预先设置各类恶意代码检测结果的信誉值。

3. 根据权利要求 2 所述的方法，其中，根据文件信誉评分策略，确定检测结果的可信度和信誉值包括：

确定与所述检测结果匹配的恶意代码检测结果；以及

将匹配的恶意代码检测结果的可信度和信誉值赋予所述检测结果。

4. 根据权利要求 1-3 任一所述的方法，其中，基于所述检测结果的可信度和信誉值确定所述检测样本的最终鉴定结果包括：

根据可信度和信誉值判定策略对所述检测结果的可信度和信誉值进行处理以获得对所述检测样本的最终鉴定结果。

5. 根据权利要求 4 所述的方法，其中，根据可信度和信誉值判定策略对所述检测结果的可信度和信誉值进行处理包括：

若所述检测结果的可信度之间存在冲突，则根据所述检测结果的冲突优先级和/或信誉值来确定最终鉴定结果。

6. 根据权利要求 5 所述的方法，其中，所述可信度包括以下任一：黑、白、灰、疑黑和疑白，其中黑表示检测结果具有恶意性，白表示检测结果具有安全性，灰表示不确定，疑黑表示检测结果可能具有恶意性，以及疑白表示检测结果可能具有安全性。

7. 根据权利要求 6 所述的方法，其中，所述可信度和信誉值判定策略包括以下至少一项：

若所述多个检测结果均为灰，则判定所述检测文本的最终鉴定结果为灰状态；

若所述多个检测结果均为黑，则判定所述检测文件的最终鉴定结果为黑状态；

若所述多个检测结果均为白，则判定所述检测文件的最终鉴定结果为白状态；

若所述多个检测结果存在黑白冲突并且冲突优先级不一样时，则判定所述检测文件的最终鉴定结果与具有最高优先级的检测结果一致；

若所述多个检测结果存在黑白冲突并且冲突优先级一样时，则判定所述检测文件的最终鉴定结果为灰状态；

若所述多个检测结果存在黑、疑白冲突，则判定所述检测文件的最终鉴定结果为黑状态；

若所述多个检测结果存在白、疑黑冲突，则判定所述检测文件的最终鉴定结果为白状态；

若所述多个检测结果均为疑黑，则当所述多个检测结果的累计信誉值在第一预定阈值以上时，判定所述检测文件的最终鉴定结果为黑状态，否则判定所述检测文件的最终鉴定结果为灰状态；

若所述多个检测结果均为疑白，则当所述多个检测结果的累计信誉值在第二预定阈值以上时，判定所述检测文件的最终鉴定结果为白状态，否则判定所述检测文件的最终鉴定结果为灰状态；以及

若所述多个检测结果存在疑黑疑白冲突，则当疑黑的检索结果的信誉值与疑白的检索结果的信誉值之间的差距在第三预定阈值以上时，判定所述检测文件的最终鉴定结果与信誉值高的检索结果一致，否则判定所述检测文件的最终鉴定结果为灰状态。

8. 一种检测恶意代码的系统，包括：

云检测服务器，用于接收检测样本；

多个不同类型的恶意代码鉴定器，用于从所述云检测服务器接收检测样本并对所述检测样本分别进行检测以获得多个检测结果；以及

文件信誉判定器，用于确定检测结果的可信度和信誉值，以及基于所述检测结果的可信度和信誉值确定所述检测样本的最终鉴定结果，其中所述可信度表示检测结果是否具有恶意性和/或安全性，所述信誉值为对应可信度的量化信任程度。

9. 根据权利要求 8 所述的系统，其中，所述文件信誉判定器包括：

确定单元，用于根据文件信誉评分策略，确定检测结果的可信度和信誉值；

其中，在所述文件信誉评分策略中，根据已知的各种恶意代码的信息，预先设置各类恶意代码检测结果的可信度；以及根据恶意代码鉴定器的误报率，预先设置各类恶意代码检测结果的信誉值。

10. 根据权利要求 9 所述的系统，其中，所述确定单元进一步配置用于：

确定与所述检测结果匹配的恶意代码检测结果；以及

将匹配的恶意代码检测结果的可信度和信誉值赋予所述检测结果。

11. 根据权利要求 8-10 任一所述的系统，其中，所述文件信誉判定器包括：

判定单元，用于根据可信度和信誉值判定策略对所述检测结果的可信度和信誉值进行处理以获得对所述检测样本的最终鉴定结果。

12. 根据权利要求 11 所述的系统，其中，

所述确定单元进一步配置用于：为检测结果分配冲突优先级；并且

所述判定单元进一步配置用于：若所述检测结果的可信度之间存在冲突，则根据所述检测结果的冲突优先级和/或信誉值来确定最终鉴定结果。

13. 根据权利要求 12 所述的系统，其中，所述可信度包括以下任一：黑、白、灰、疑黑和疑白，其中黑表示检测结果具有恶意性，白表示检测结果具有安全性，灰表示不确定，疑黑表示检测结果可能具有恶意性，以及疑白表示检测结果可能具有安全性。

14. 根据权利要求 13 所述的系统，其中，所述可信度和信誉值判定策略包括以下至少一项：

若所述多个检测结果均为灰，则判定所述检测文本的最终鉴定结果为灰状态；

若所述多个检测结果均为黑，则判定所述检测文件的最终鉴定结果为黑状态；

若所述多个检测结果均为白，则判定所述检测文件的最终鉴定结果为白状态；

若所述多个检测结果存在黑白冲突并且冲突优先级不一样时，则判定所述检测文件的最终鉴定结果与具有最高优先级的检测结果一致；

若所述多个检测结果存在黑白冲突并且冲突优先级一样时，则判定所述检测文件的最终鉴定结果为灰状态；

若所述多个检测结果存在黑、疑白冲突，则判定所述检测文件的最终鉴定结果为黑状态；

若所述多个检测结果存在白、疑黑冲突，则判定所述检测文件的最终鉴定结果为白状态；

若所述多个检测结果均为疑黑，则当所述多个检测结果的累计信誉值在第一预定阈值以上时，判定所述检测文件的最终鉴定结果为黑状态，否则判定所述检测文件的最终鉴定结果为灰状态；

若所述多个检测结果均为疑白，则当所述多个检测结果的累计信誉值在第二预定阈值以上时，判定所述检测文件的最终鉴定结果为白状态，否则判定所述检测文件的最终鉴定结果为灰状态；以及

若所述多个检测结果存在疑黑疑白冲突，则当疑黑的检索结果的信誉值与疑白的检索结果的信誉值之间的差距在第三预定阈值以上时，判定所述检测文件的最终鉴定结果与信誉值高的检索结果一致，否则判定所述检测文件的最终鉴定结果为灰状态。

用于检测恶意代码的方法和系统

技术领域

[0001] 本公开一般涉及计算机技术领域，具体涉及网络信息安全领域，尤其涉及一种用于检测恶意代码的方法和系统。

背景技术

[0002] 随着互联网的快速发展，恶意代码的黑色利益链已经形成。恶意代码是以危害信息的安全等不良意图为目的的程序，通常都潜伏在受害计算机中实施破坏或窃取信息。由于每日新增的恶意代码样本已经数以万计，传统的客户端检测方式逐步转变为云查杀的检测方式。

[0003] 云查杀是云计算技术在反病毒中的应用。云计算是一种服务交付模型，用于对共享的可配置计算资源池进行方便、按需的网络访问。简单地说，云计算是由云计算服务提供商来搭建云计算存储和运算中心，用户通过网络来访问“云”，将“云”作为数据存储和应用服务的中心。云查杀是指反病毒厂商建立云端在线服务器集群，用于存储海量检测特征和检测规则，并使用各种鉴定器进行匹配检测。软件客户端则将要检测对象的信息通过互联网上传到云端服务器，等待服务器检测的结果。

[0004] 然而，各种鉴定器的检测方式都有自己的长处和不足，检测结果也可能存在误报的情况，这就会影响云端最终的鉴定结果。

发明内容

[0005] 鉴于现有技术中的上述缺陷或不足，期望提供一种能够有效提高恶意代码检测精准度的方案。

[0006] 第一方面，本申请实施例提供了一种检测恶意代码的方法，包括：接收检测样本；利用多种恶意代码鉴定器分别对检测样本进行检测以获得多个检测结果；确定检测结果的可信度和信誉值，其中可信度表示检测结果是否具有恶意性和/或安全性，信誉值为对应可信度的量化信任程度；以及基于检测结果的可信度和信誉值确定检测样本的最终鉴定结果。

[0007] 第二方面，本申请实施例还提供了一种检测恶意代码的系统，包括：云检测服务器，用于接收检测样本；多个不同类型的恶意代码鉴定器，用于从云检测服务器接收检测样本并对检测样本分别进行检测以获得多个检测结果；以及文件信誉判定器，用于确定检测结果的可信度和信誉值，以及基于检测结果的可信度和信誉值确定检测样本的最终鉴定结果，其中可信度表示检测结果是否具有恶意性和/或安全性，信誉值为对应可信度的量化信任程度。

[0008] 本申请实施例提供的检测恶意代码的方案，通过对多个恶意代码鉴定器的检测结果分配可信度和信誉值，能够充分利用各种恶意代码鉴定器的特性，提供恶意代码检测的精准度。在一些实施例中，检测结果的信誉值体现了恶意代码鉴定器的误报率，基于信誉值对检测结果进行判定，降低了对样本鉴定结果的误报率。在另一些实施例中，按照可信度和

信誉值判定策略，可以根据检测结果的可信度和信誉值细粒度调整鉴定结果。

附图说明

[0009] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

[0010] 图 1 示出了其中可以应用本申请实施例的示例性系统架构；

[0011] 图 2 示出了根据本申请一个实施例的用于检测恶意代码的方法的示例性流程图；

[0012] 图 3 示出了根据本申请的文件信誉评分策略的一个示例性规则表格；

[0013] 图 4 示出了根据本申请实施例的利用规则表格确定检测结果的可信度和信誉值的方法的示例性流程图；

[0014] 图 5 示出了根据本申请的可信度和信誉值判定策略的一个示例性判定逻辑的流程图；

[0015] 图 6 示出了根据本申请实施例的用于检测恶意代码的系统的示例性结构示意图；以及

[0016] 图 7 示出了适于用来实现本申请实施例的服务器的计算机系统的结构示意图。

具体实施方式

[0017] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与发明相关的部分。

[0018] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0019] 请参考图 1，其示出了可以应用本申请实施例的示例性系统架构 100。

[0020] 如图 1 所示，系统架构 100 可以包括终端设备 101、102、网络 103 和服务器 104、105、106 和 107。网络 103 用以在终端设备 101、102 和服务器 104、105、106、107 之间提供通信链路的介质。网络 103 可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

[0021] 用户 110 可以使用终端设备 101、102 通过网络 103 与服务器 104、105、106、107 交互，以访问各种服务，例如浏览网页、下载数据等。终端设备 101、102 上可以安装有各种客户端应用，例如可以接入统一资源定位符 URL 云服务的应用，包括但不限于浏览器、安全应用等。

[0022] 终端设备 101、102 可以是各种电子设备，包括但不限于个人电脑、智能手机、智能电视、平板电脑、个人数字助理、电子书阅读器等等。

[0023] 服务器 104、105、106、107 可以是提供各种服务的服务器。服务器可以响应于用户的服务请求而提供服务。可以理解，一个服务器可以提供一种或多种服务，同一种服务也可以由多个服务器来提供。在本申请的实施例中，所涉及的服务器可以位于云端，这些服务器可以包括但不限于，云检测服务器、各种恶意代码鉴定服务器、文件信誉判定服务器等。

[0024] 应该理解，图 1 中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器。

[0025] 如背景技术中所提到的，目前的各种恶意代码鉴定器的检测方式具有各自的优点和缺点，检测结果也存在误报的情况，这会影响云端最终的鉴定结果。

[0026] 鉴于现有技术的上述缺陷，本申请实施例提供了一种基于文件信誉值的恶意代码检测方案。具体的，针对各个恶意代码鉴定器对检测样本的检测结果分配可信度和信誉值。可信度表示检测结果是否具有恶意性和 / 或安全性，信誉值则为对应可信度的量化信任程度。然后，基于一个或多个检测结果的可信度和信誉值确定检测样本的最终鉴定结果。

[0027] 参考图 2，其示出了根据本申请一个实施例的用于检测恶意代码的方法的示例性流程图。图 2 所示的方法由服务器侧的系统完成，该系统可以位于云端。

[0028] 如图 2 所示，在步骤 210 中，接收检测样本。

[0029] 服务器可以从客户端接收检测样本。客户端可以在需要进行恶意代码检测或病毒查杀时，向服务器提出请求，请求的同时可以将需要检测的样本上传给服务器。

[0030] 接着，在步骤 220 中，利用多种恶意代码鉴定器分别对检测样本进行检测以获得多个检测结果。

[0031] 服务器接收到检测样本后，可以将该检测样本分发给多个恶意代码鉴定器，以在各个恶意代码鉴定器处分别进行恶意代码检测。

[0032] 在一些实施例中，服务器也可以在对检测样本进行预处理之后再分发给恶意代码鉴定器。预处理例如可以包括针对不同类型的检测样本，预先进行不同的处理。例如，对于压缩包，可以先对压缩包进行解压。

[0033] 在一些实施例中，服务器可以选择向部分或全部恶意代码鉴定器分发检测样本。例如，服务器可以根据检测样本的特性，排除那些明显不适合该类检测样本的恶意代码鉴定器，从而提高检测结果的准确定。

[0034] 一般而言，根据鉴定方法所基于的特征不同，恶意代码鉴定器可以分为基于静态特征的鉴定器，基于动态行为的鉴定器，以及基于静态特征和动态行为的鉴定器。静态特征例如可以包括以下方面 :文件名称、程序形态、API（应用编程接口）数量特性、文件的版本信息、文件长度信息、PE（可移植可执行）结构特性、文件加壳信息等。动态行为例如可以包括以下方面 :自启动行为，进程隐藏行为，通信隐藏行为等。本申请对于恶意代码鉴定器的类型没有限制，可以使用现有技术中已知的或者未来开发的各种类型的恶意代码鉴定器。

[0035] 恶意代码鉴定器的检测结果例如可以包括所检测出的恶意代码的类别。计算机反病毒研究组织 (CARO) 提出了一种恶意代码的分类命名方法，其命名规则如下 :

[0036] [<malware_type>://][<platform>]/<family_name>[.<group_name>]\[.<infective_length>][.<variant>[<devolution]][<modifiers>]

[0037] 其中，<malware_type> 指明了恶意代码的类型（常见如 virus（病毒）、backdoor（后门），Trojan（木马），Adware（广告软件）等）。<platform> 字段定义了恶意代码执行所需要的操作系统环境，例如“W32”或“Win32”是指 32 位 Windows 操作系统，“Linux”指 Linux 系统，“OSX”指 Mac OSX。<family_name> 同 <group_name> 字段通常代表恶意代码的家族信息。<infective_length> 字段定义了文件感染型病毒的感染长度。<variant>（通常是一个字母）字段用来区分具有相同恶意代码家族的变种。剩余的字段根据具体环境定义。

[0038] 下面是几个常见的恶意代码名称定义例子 :

[0039] Net-Worm://Win32.Welchia 一种 Windows 平台网络蠕虫；

[0040] Backdoor://Win32.ciadoor.121 一种 Windows 平台后门型木马，属于 ciadoor 家族；

[0041] Virus://Win32.Parite.B 一种 windows 内存驻留型文件感染病毒，属于 Parite 家族。

[0042] 由于上述命名规则不是强制执行的，因此不同反恶意代码服务提供商对恶意代码的类别可能有不同的命名方式。换言之，不同恶意代码鉴定器对同一检测样本检测出的恶意代码可能有不同的命名方式。

[0043] 然后，在步骤 230 中，确定检测结果的可信度和信誉值。

[0044] 在本文中，可信度表示检测结果是否具有恶意性和 / 或安全性，换言之，检测出的恶意代码类别是否具有威胁性，或者是否具有安全性。信誉值为对应可信度的量化信任程度。

[0045] 在一些实施例中，可信度可以包括以下任一 ：黑、白、灰、疑黑和疑白，其中黑表示检测结果具有恶意性，白表示检测结果具有安全性，灰表示不确定，疑黑表示检测结果可能具有恶意性，以及疑白表示检测结果可能具有安全性。

[0046] 信誉值可以采用各种数值特征来表示，例如采用正整数来表示。针对检测结果的可信度，可以有对应的信誉值。例如，假设某一检测结果的可信度为黑，其对应的信誉值为 100。这表示该检测出的结果具有恶意性的概率极高。又例如，假设某一检测结果的可信度为灰，其对应的信誉值为 1。这表示该检测出的结果是否具有恶意性不确定，并且这种不确定的概率很低。

[0047] 在一些实施例中，检测结果的可信度和信誉值的确定是根据文件信誉评分策略来进行的。在文件信誉评分策略中，可以根据已知的各种恶意代码的信息，预先设置各类恶意代码检测结果的可信度 ；以及根据恶意代码鉴定器的误报率，预先设置各类恶意代码检测结果的信誉值。例如，目前已知多种恶意代码以及这些恶意代码所属的家族，因此可以根据这些已知信息预先设置各类恶意代码检测结果的可信度。另外，根据恶意代码鉴定器的历史判定结果，可以统计鉴定器的误报率，从而基于误报率来预先设置各类恶意代码检测结果的信誉值。可选的或附加的，还可以由病毒分析人员根据积累的经验人工调整可信度和 / 或信誉值。

[0048] 图 3 示出了根据本申请的文件信誉评分策略的一个示例性规则表格。在图 2 的步骤 230 中，可以根据该规则表格来确定检测结果的可信度和信誉值。

[0049] 如图 3 所示，第一列为规则 ID，用于标识不同的规则 ；第二列为任务类型，鉴定器引擎所执行的任务类型，任务类型例如可以根据文件处理的紧急程度和重要性进行区分 ；第三列为鉴定器引擎，也即各种恶意代码鉴定器，第四列为冲突优先级，用于标识不同规则在发生冲突时的优先级（在后文将描述到）；第五列为鉴定规则，也即鉴定器引擎所检测出的各种检测结果，其可以标识所检测出的恶意代码的类型 ；第六列为可信度，也即各个规则或恶意代码检测结果所对应的可信度 ；第七列为信誉值，也即各个规则对应于相应的可信度的量化信任程度。可以理解，规则表格还可以包含一些其他内容。为了不必要地模糊本申请的实施例，图 3 中未示出那些附加内容。

[0050] 图 4 示出了根据本申请实施例的利用规则表格确定检测结果的可信度和信誉值

的方法的示例性流程图，也即示出了图 2 中的步骤 230 的一种示例性实现方式。

[0051] 如图 4 所示，在步骤 410 中，确定与检测结果匹配的恶意代码检测结果。在该步骤中，可以通过查找规则表格，来确定与检测结果匹配的规则。

[0052] 例如，如果样本 72AAC543B9CBBF597852E254325772BF 经过多种恶意代码鉴定器查杀后检测出的结果为：

[0053] GScan:Adware.Win32.MultiPlug.susp

[0054] PScan:Win32/Ramnit.A virus

[0055] DScan:0.2

[0056] 以图 3 中所示的规则表格为例，此时可以确定，GScan 鉴定器引擎的检测结果与规则 405 匹配，PScan 鉴定器引擎的检测结果未找到匹配规则，DScan 鉴定器引擎的检测结果也未找到匹配规则。

[0057] 接着，在步骤 420 中，将匹配的恶意代码检测结果的可信度和信誉值赋予对应的检测结果。

[0058] 继续上述示例，根据图 3 的规则表格，规则 405 的可信度为疑黑，分值为 50，所以 GScan 鉴定器引擎的检测结果的可信度为疑黑，分值为 50。其余鉴定器引擎的检测结果未匹配上规则，因此舍弃这些检测结果。

[0059] 返回图 2，在确定了检测结果的可信度和信誉值之后，继而在步骤 240 中，基于检测结果的可信度和信誉值确定检测样本的最终鉴定结果。

[0060] 在一些实施例中，根据可信度和信誉值判定策略对检测结果的可信度和信誉值进行处理以获得对检测样本的最终鉴定结果。

[0061] 当多个检测结果的可信度一致时，可以比较容易地确定最终鉴定结果。当多个检测结果的可信度不一致，存在冲突时，可信度和信誉值判定策略还可以考虑检测结果的冲突优先级和 / 或信誉值。因此，在前述的步骤 230 中，根据文件信誉分配策略同时为检测结果分配冲突优先级（例如根据图 3 中的表格第四列冲突优先级进行分配）。可以设计多种可信度和信誉值判定策略，以确定最终鉴定结果。

[0062] 图 5 示出了根据本申请的可信度和信誉值判定策略的一个示例性判定逻辑的流程图。

[0063] 如图 5 所示，在步骤 501 中，将确定了可信度和信誉值的检测结果汇集成文件可信分值表。接着在步骤 502 中，判断这些检测结果的可信度是否全部为黑。如果是，则跳至步骤 520，判定最终鉴定结果为黑状态；否则，前进到步骤 503。

[0064] 在步骤 503 中，判断这些检测结果的可信度是否全部为灰。如果是，则跳至步骤 530，判定最终鉴定结果为灰状态；否则，前进到步骤 504。

[0065] 在步骤 504 中，判断这些检测结果的可信度是否全部为白。如果是，则跳至步骤 540，判断最终鉴定结果为白状态；否则，前进到步骤 505。

[0066] 在步骤 505 中，判断这些检测结果的可信度是否全部为疑黑。如果是，则在步骤 506 中，对检测结果的信誉值进行累加。接着，在步骤 507 中，判断累加的信誉值是否大于等于第一预定阈值，如果是，则跳至步骤 520，判定最终鉴定结果为黑状态；否则，跳至步骤 530，判断最终鉴定结果为灰状态。第一预定阈值例如可以是 100。如果步骤 505 中判断为否，则前进到步骤 508。

[0067] 在步骤 508 中，判断这些检测结果的可信度是否全部为疑白。如果是，则在步骤 509 中，对检测结果的信誉值进行累加。接着，在步骤 510 中，判断累加的信誉值是否大于等于第二预定阈值，如果是，则跳至步骤 540，判定最终鉴定结果为白状态；否则，跳至步骤 530，判断最终鉴定结果为灰状态。第二预定阈值例如可以是 100。如果步骤 508 中判断为否，则前进到步骤 511。

[0068] 在步骤 511 中，判断这些检测结果的可信度是否存在黑白冲突。如果是，则在步骤 512 中，对检测结果的冲突优先级进行比较。响应于可信度为黑的检测结果的冲突优先级最高，跳至步骤 520，判定最终鉴定结果为黑状态。响应于可信度为白的检测结果的冲突优先级最高否则，跳至步骤 540，判断最终鉴定结果为白状态。换言之，最终鉴定结果与具有最高冲突优先级的检测结果一致。响应于可信度分别为黑和白的检测结果的冲突优先级相同，跳至步骤 530，判定最终鉴定结果为灰状态。如果步骤 511 中判断为否，则前进到步骤 513。

[0069] 在步骤 513 中，判断这些检测结果的可信度是否存在黑疑白冲突。如果是，则跳至步骤 520，直接判定最终鉴定结果为黑状态；否则，前进到步骤 514。

[0070] 在步骤 514 中，判断这些检测结果的可信度是否存在白疑黑冲突。如果是，则跳至步骤 540，直接判定最终鉴定结果为白状态；否则，前进到步骤 515。

[0071] 在步骤 515 中，判断这些检测结果的可信度是否存在疑黑疑白冲突。如果是，则在步骤 516 中，确定疑黑的检索结果的信誉值与疑白的检索结果的信誉值之间的差距。例如，可以通过将疑黑信誉值减去疑白信誉值。反过来也可以。响应于疑黑信誉值与疑白信誉值的差值大于等于第一阈值，也即疑黑信誉值比疑白信誉值足够高，则跳至步骤 520，判定最终鉴定结果为黑状态。响应于疑黑信誉值与疑白信誉值的差值小于等于第二阈值，也即疑黑信誉值比疑白信誉值足够低，则跳至步骤 540，判断最终鉴定结果为白状态。响应于疑黑信誉值与疑白信誉值的差值介于第一阈值与第二阈值之间，也即疑黑信誉值与疑白信誉值相差不够大，则跳至步骤 530，判定最终鉴定结果为灰状态。在一些实施例中，第一阈值与第二阈值的绝对值可以相同，例如第一阈值为 100，第二阈值为 -100。因此，上述判断逻辑也可以表述为：若多个检测结果存在疑黑疑白冲突，则当疑黑的检索结果的信誉值与疑白的检索结果的信誉值之间的差距在第三预定阈值以上时，判定最终鉴定结果与信誉值高的检索结果一致，否则判定最终鉴定结果为灰状态。这里，第三预定阈值为第一阈值和第二阈值的绝对值，例如 100。

[0072] 如果步骤 515 中判断为否，则前进到步骤 517，判断其他可能的冲突。这些冲突不是非常激烈，可以利用一些简单的判定逻辑进行判断。例如，当存在黑和疑黑冲突时，判定最终结果为黑状态；当存在白和疑白冲突时，判定最终结果为白状态；当存在疑黑和灰冲突或疑白和灰冲突时，判定最终结果为灰状态。为了简单清晰起见，图 5 中没有对这些冲突判断进行描绘。另外，为了连线清晰起见，图 5 中示出了重复的最终结果框图：黑状态 520、灰状态 530 和白状态 540，这种图示方式不影响图 5 的判定逻辑。

[0073] 可以理解，图 5 所示的判定逻辑仅是示例性的。本领域技术人员也可以设定其他的判定逻辑。例如，图 5 中的黑白冲突根据冲突优先级来判定，也可以根据信誉值来判定，类似于疑黑疑白冲突。又例如，图 5 中的疑黑疑白冲突根据信誉值来判定，其也可以根据冲突优先级来判定。再例如，黑白冲突和疑黑疑白冲突可以同时考虑冲突优先级和信誉值。例如，首先根据冲突优先级进行判定，当冲突优先级相同时，再根据信誉值来判定。

[0074] 回顾前面的示例，也即针对样本 72AAC543B9CBBF597852E254325772BF 经过多种恶意代码鉴定器查杀后检测出的结果为：

[0075] GScan:Adware.Win32.MultiPlug.susp

[0076] PScan:Win32/Ramnit.A virus

[0077] DScan:0.2

[0078] 以图 3 中所示的规则表格为例，GScan 鉴定器引擎的检测结果与规则 405 匹配，可信度为疑黑，分值为 50。其余鉴定器引擎的检测结果未匹配上任何规则，丢弃这些检测结果。

[0079] 按照图 5 所示的判定逻辑，此时检测结果的可信度为疑黑，分值为 50，低于第一预定阈值（例如 100），因此，判定最终鉴定结果为灰状态。

[0080] 又例如，假设针对样本 EF1766F750C01D741F8D980DC345DD2F，经过多种恶意代码鉴定器查杀后检测出的结果分别为：

[0081] GScan:Adware.Win32.Downloader.Gex

[0082] PScan:Win32/Wapomi.AX virus

[0083] DScan:0.3

[0084] 以图 3 中所示的规则表格为例，GScan 鉴定器引擎的检测结果与规则 404 匹配，可信度为黑，分值为 100。其余鉴定器引擎的检测结果未匹配上任何规则，丢弃这些检测结果。

[0085] 按照图 5 所示的判定逻辑，此时检测结果的可信度全为黑，因此，判定最终鉴定结果为黑状态。

[0086] 应当注意，尽管在附图中以特定顺序描述了本发明方法的操作，但是，这并非要求或者暗示必须按照该特定顺序来执行这些操作，或是必须执行全部所示的操作才能实现期望的结果。相反，流程图中描绘的步骤可以改变执行顺序。例如，图 5 中的各种判定逻辑可以按任意顺序执行或者并发进行。附加地或备选地，可以省略某些步骤，将多个步骤合并为一个步骤执行，和 / 或将一个步骤分解为多个步骤执行。

[0087] 参考图 6，其示出了根据本申请一个实施例的用于检测恶意代码的系统的示例性结构图。图 6 所示的系统位于服务器侧，尤其是位于云端。该系统泛指多个不同功能的服务器相互连接组成的服务器集群，对外表现为一个整体，相互配合共同完成检测恶意代码的功能。

[0088] 如图 6 所示，用于检测恶意网址的系统 600 可以包括云检测服务器 610，一个或多个不同类型的恶意代码鉴定器 620-1，620-2，…，620-N，以及文件信誉判定器 630。

[0089] 云检测服务器 610 用于接收客户端上传的检测样本。云检测服务器 610 还将检测样本分发给各个恶意代码鉴定器 620-1，620-2，…，620-N。

[0090] 每个恶意代码鉴定器 620-1，620-2，…，620-N 根据自己的鉴定方法，对云检测服务器 610 分发的检测样本进行检测。这些恶意代码鉴定器可以位于与云检测服务器相同或不同的云端服务器上。

[0091] 文件信誉判定器 630 用于汇集恶意代码鉴定器 620-1，620-2，…，620-N 的检测结果，对这些检测结果进行分析处理，以确定检测样本的最终鉴定结果。在一些实施例中，对检测结果的分析处理可以包括：确定检测结果的可信度和信誉值，以及基于检测结果的可信度和信誉值确定检测样本的最终鉴定结果。

[0092] 为了执行上述分析处理，文件信誉判定器630可以包括确定单元631和判定单元632。确定单元631用于根据来自块640的文件信誉评分策略，确定检测结果的可信度和信誉值。判定单元632用于根据来自块640的可信度和信誉值判定策略对检测结果的可信度和信誉值进行处理以获得对检测样本的最终鉴定结果。

[0093] 当确定单元631确定检测结果的可信度和信誉值时，可以首先寻找与检测结果匹配的恶意代码检测结果；然后将匹配的恶意代码检测结果的可信度和信誉值赋予该检测结果。

[0094] 在一些实施例中，可信度和信誉值判定策略还考虑了检测结果的冲突优先级。在这些实施例中，确定单元631进一步配置用于为检测结果分配冲突优先级。具体而言，根据文件信誉评分策略，确定检测结果的冲突优先级。判定单元632进一步配置用于：若检测结果的可信度之间存在冲突，则根据检测结果的冲突优先级和/或信誉值来确定最终鉴定结果。

[0095] 在一些实施例中，可信度和信誉值判定策略的示例性判断逻辑例如可以包括以下至少一项：

[0096] 若多个检测结果均为灰，则判定检测文本的最终鉴定结果为灰状态；

[0097] 若多个检测结果均为黑，则判定检测文件的最终鉴定结果为黑状态；

[0098] 若多个检测结果均为白，则判定检测文件的最终鉴定结果为白状态；

[0099] 若多个检测结果存在黑白冲突并且冲突优先级不一样时，则判定检测文件的最终鉴定结果与具有最高优先级的检测结果一致；

[0100] 若多个检测结果存在黑白冲突并且冲突优先级一样时，则判定检测文件的最终鉴定结果为灰状态；

[0101] 若多个检测结果存在黑、疑白冲突，则检测文件的最终鉴定结果为黑状态；

[0102] 若多个检测结果存在白、疑黑冲突，则判定检测文件的最终鉴定结果为白状态；

[0103] 若多个检测结果均为疑黑，则当多个检测结果的累计信誉值在第一预定阈值以上时，判定检测文件的最终鉴定结果为黑状态，否则判定检测文件的最终鉴定结果为灰状态；

[0104] 若多个检测结果均为疑白，则当多个检测结果的累计信誉值在第二预定阈值以上时，判定检测文件的最终鉴定结果为白状态，否则判定检测文件的最终鉴定结果为灰状态；以及

[0105] 若多个检测结果存在疑黑疑白冲突，则当疑黑的检索结果的信誉值与疑白的检索结果的信誉值之间的差距在第三预定阈值以上时，判定检测文件的最终鉴定结果与信誉值高的检索结果一致，否则判定检测文件的最终鉴定结果为灰状态。

[0106] 应当理解，系统600中记载的诸子系统或单元与参考图2-图5描述的方法中的各个步骤相对应。由此，上文针对方法描述的操作和特征同样适用于系统600及其中包含的单元，在此不再赘述。

[0107] 下面参考图7，其示出了适于用来实现本申请实施例的服务器的计算机系统700的结构示意图。

[0108] 如图7所示，计算机系统700包括中央处理单元(CPU)701，其可以根据存储在只读存储器(ROM)702中的程序或者从存储部分708加载到随机访问存储器(RAM)703中的程

序而执行各种适当的动作和处理。在 RAM 703 中，还存储有系统 700 操作所需的各种程序和数据。CPU 701、ROM 702 以及 RAM 703 通过总线 704 彼此相连。输入 / 输出 (I/O) 接口 705 也连接至总线 704。

[0109] 以下部件连接至 I/O 接口 705 ：包括键盘、鼠标等的输入部分 706 ；包括诸如阴极射线管 (CRT)、液晶显示器 (LCD) 等以及扬声器等的输出部分 707 ；包括硬盘等的存储部分 708 ；以及包括诸如 LAN 卡、调制解调器等的网络接口卡的通信部分 709。通信部分 709 经由诸如因特网的网络执行通信处理。驱动器 710 也根据需要连接至 I/O 接口 705。可拆卸介质 711，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器 710 上，以便于从其上读出的计算机程序根据需要被安装入存储部分 708。

[0110] 特别地，根据本公开的实施例，上文参考图 2- 图 7 描述的过程可以被实现为计算机软件程序。例如，本公开的实施例包括一种计算机程序产品，其包括有形地包含在机器可读介质上的计算机程序，所述计算机程序包含用于执行图 2- 图 5 的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分 709 从网络上被下载和安装，和 / 或从可拆卸介质 711 被安装。

[0111] 附图中的流程图和框图，图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，所述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和 / 或流程图中的每个方框、以及框图和 / 或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0112] 描述于本申请实施例中所涉及到的单元或模块可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的单元或模块也可以设置在处理器中。这些单元或模块的名称在某种情况下并不构成对该单元或模块本身的限定。

[0113] 作为另一方面，本申请还提供了一种计算机可读存储介质，该计算机可读存储介质可以是上述实施例中所述装置中所包含的计算机可读存储介质 ；也可以是单独存在，未装配入设备中的计算机可读存储介质。计算机可读存储介质存储有一个或者一个以上程序，所述程序被一个或者一个以上的处理器用来执行描述于本申请的公式输入方法。

[0114] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本申请中所涉及的发明范围，并不限于上述技术特征的特定组合而成的技术方案，同时也应涵盖在不脱离所述发明构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的（但不限于）具有类似功能的技术特征进行互相替换而形成的技术方案。

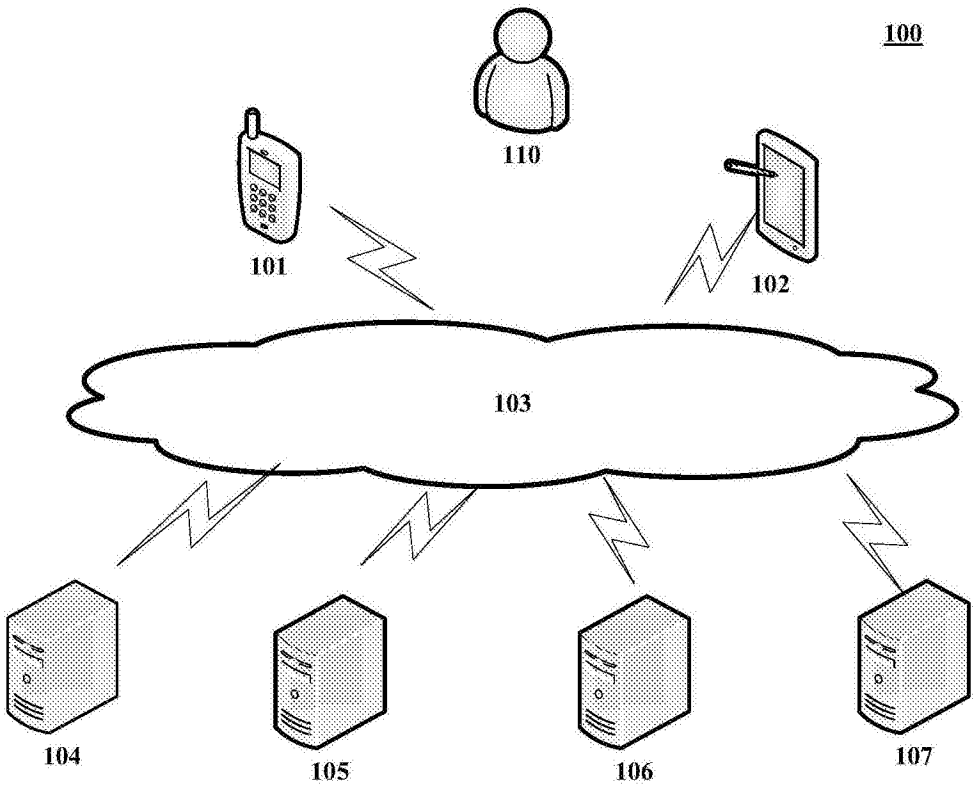

100
110
101
102
103
104
105
106
107

图 1

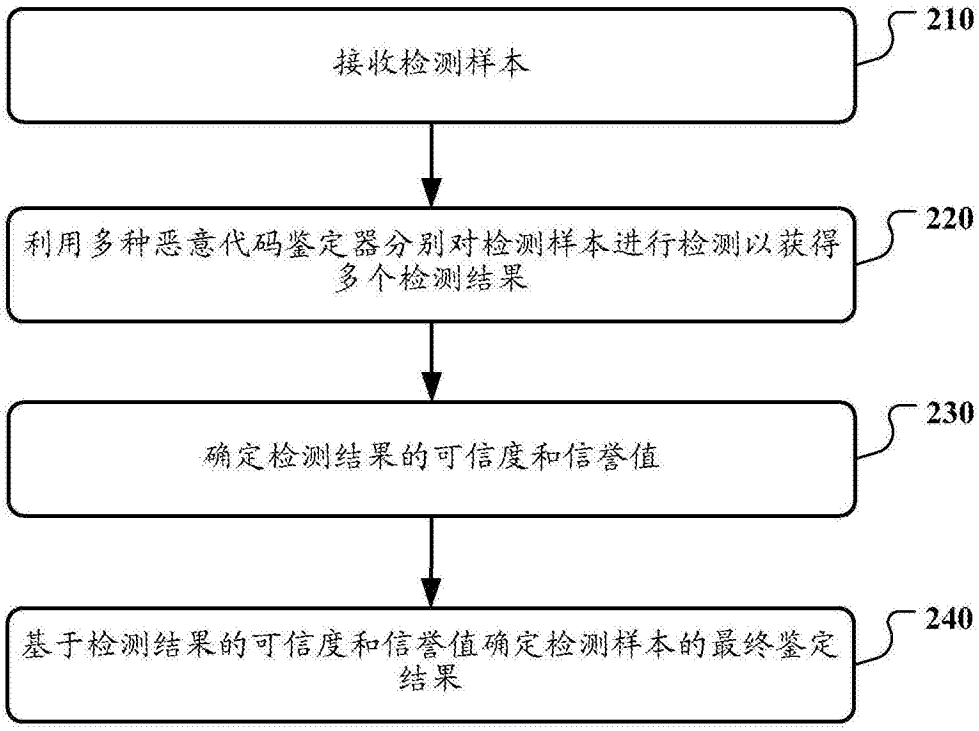

接收检测样本
210
利用多种恶意代码鉴定器分别对检测样本进行检测以获得多个检测结果
220
确定检测结果的可信度和信誉值
230
基于检测结果的可信度和信誉值确定检测样本的最终鉴定结果
240

图 2

规则ID	任务类型	鉴定器引擎	冲突优先级	鉴定规则	可信度	信誉值	其他
413	0	GScan	10	PUA.Win32.Softcnapp.susp	灰	50	
412	0	GScan	10	PUA.Win32.InstallMonstr.LLCS	疑黑	59	
411	0	AScan	10	Trojan.Win32.Patched.*	灰	1	
410	119	DScan	1	0.1	灰	1	
409	0	PScan	10	Adare/BBar*	灰	1	
408	609	DScan	1	0.1	灰	1	
407	608	DScan	1	0.1	灰	1	
406	601	DScan	1	0.1	灰	1	
405	0	GScan	10	Adware.Win32.MultiPlug.susp	疑黑	50	
404	0	GScan	8	Adware.Win32.Downloader.Gex	黑	100	
403	0	GScan	10	Adware.Win32.Solimba.susp	灰	50	
402	0	GScan	10	PUA.Win32.Montiera.cras	灰	50	

图 3

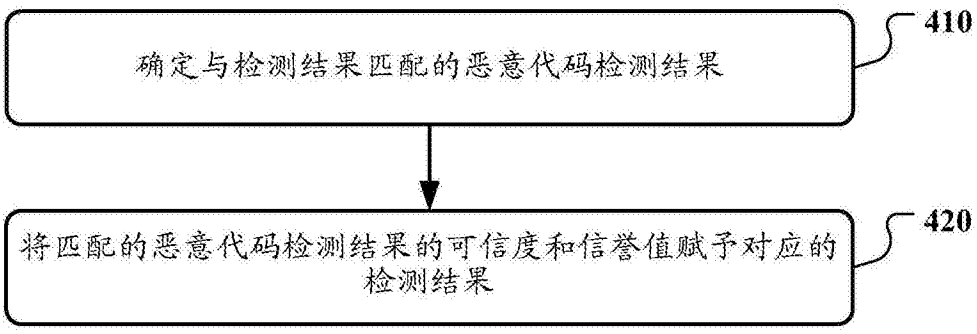


图 4

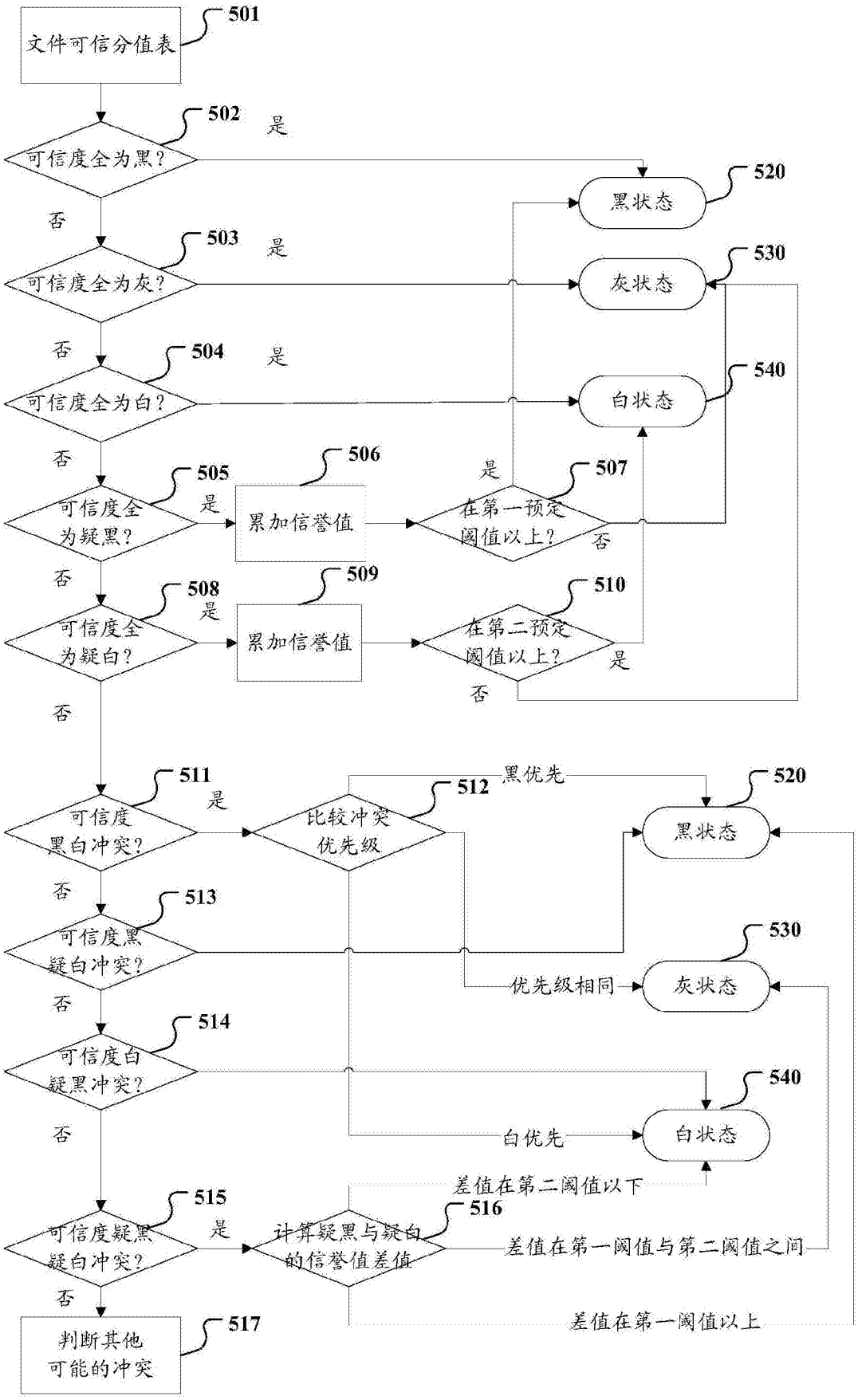

文件可信分值表
501
可信度全为黑?
502
是
黑状态
520
否
可信度全为灰?
503
是
灰状态
530
否
可信度全为白?
504
是
白状态
540
否
可信度全为疑黑?
505
是
累加信誉值
506
在第一预定阈值以上?
507
是
否
否
可信度全为疑白?
508
是
累加信誉值
509
在第二预定阈值以上?
510
是
否
否
可信度黑白冲突?
511
是
比较冲突优先级
512
黑优先
否
可信度黑疑白冲突?
513
优先级相同
否
可信度白疑黑冲突?
514
白优先
否
可信度疑黑疑白冲突?
515
是
计算疑黑与疑白的信誉值差值
516
差值在第二阈值以下
差值在第一阈值与第二阈值之间
差值在第一阈值以上
否
判断其他可能的冲突
517

图 5

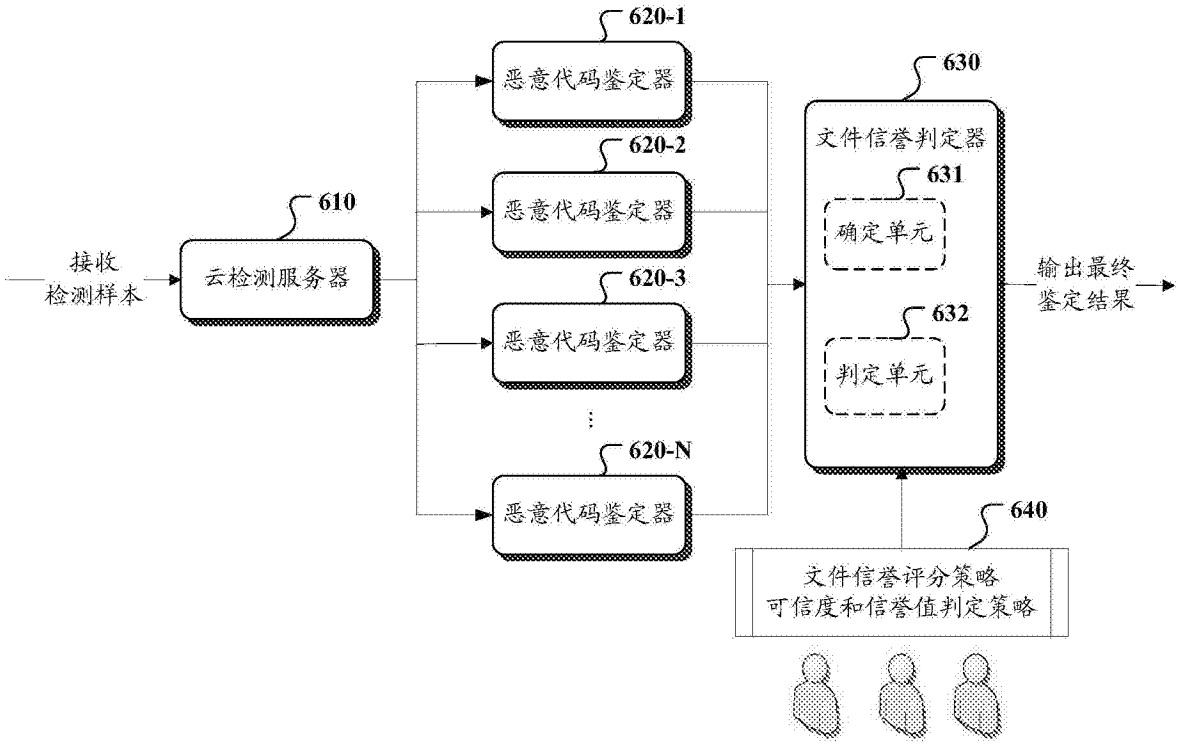

620-1
恶意代码鉴定器
630
文件信誉判定器
620-2
恶意代码鉴定器
631
确定单元
610
接收
检测样本
云检测服务器
620-3
恶意代码鉴定器
输出最终
鉴定结果
632
判定单元
620-N
恶意代码鉴定器
640
文件信誉评分策略
可信度和信誉值判定策略

图 6

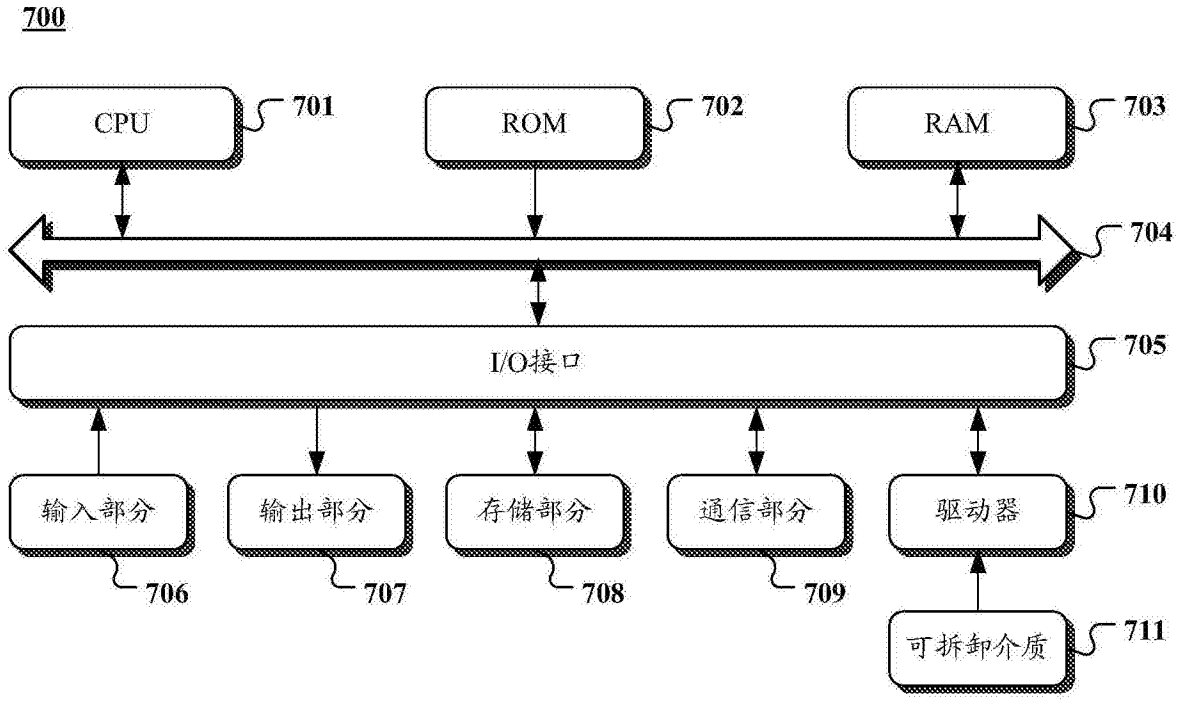

700
CPU
701
ROM
702
RAM
703
704
I/O接口
705
输入部分
706
输出部分
707
存储部分
708
通信部分
709
驱动器
710
可拆卸介质
711

图 7