

(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
2018 年 11 月 8 日 (08.11.2018)



(10) 国际公布号
WO 2018/201594 A1

- (51) 国际专利分类号:
G06F 11/36 (2006.01)
- (21) 国际申请号: PCT/CN2017/090308
- (22) 国际申请日: 2017 年 6 月 27 日 (27.06.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201710307282.3 2017年5月4日 (04.05.2017) CN
- (71) 申请人: 平安科技(深圳)有限公司(PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN];
中国广东省深圳市福田区八卦岭八卦三路平安大厦, Guangdong 518000 (CN)。
- (72) 发明人: 王海平(WANG, Haiping); 中国广东省深圳市福田区八卦岭八卦三路平安大厦, Guangdong 518000 (CN)。
- (74) 代理人: 深圳中一专利商标事务所(SHENZHEN ZHONGYI PATENT AND TRADEMARK OFFICE);

中国广东省深圳市福田区深南中路 1014 号老特区报社四楼 (5 号信箱), Guangdong 518028 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, 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,

(54) Title: FILE ABNORMALITY DETECTION METHOD AND DEVICE, ELECTRONIC DEVICE AND MEDIUM

(54) 发明名称: 文件异常检测方法、装置、电子设备及介质

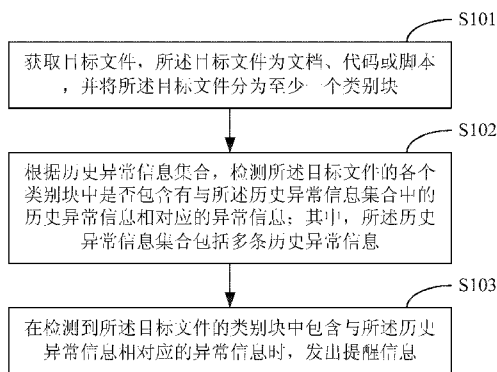


图 1

- S101 Acquire a target file, wherein the target file is a document, a code or a script, and divide the target file into at least one category block
- S102 Detect whether each category block of the target file comprises abnormal information corresponding to historical abnormal information in a historical abnormal information set according to the historical abnormal information set, wherein the historical abnormal information set comprises a plurality of historical abnormal information
- S103 When detected that the category block of the target file comprises abnormal information corresponding to the historical abnormal information, issue prompt information

(57) Abstract: The present application is applicable to the technical field of computer security, and provided thereby are a file abnormality detection method and a device, an electronic device and a medium. The file abnormality detection method comprises: acquiring a target file, wherein the target file is a document, a code or a script, and dividing the target file into at least one category block; detecting whether each category block of the target file comprises abnormal information corresponding to historical abnormal information in a historical abnormal information set according to the historical abnormal information set, wherein each category block corresponds to at least one piece of abnormal information; and when detected that the category block of the target file comprises abnormal information corresponding to the historical abnormal information, issuing prompt information. According to the present application, a target file is divided into at least one category block, so that the target file is scanned and detected by taking the category block as a unit, and different scanning and detection modes are used for different category blocks, thereby reducing unnecessary scanning and detection time, and increasing the scanning and detection efficiency.

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))。

(57) 摘要：本申请适用于计算机安全技术领域，提供了一种文件异常检测方法、装置、电子设备及介质。该文件异常检测方法包括：获取目标文件，目标文件为文档、代码或脚本，并将目标文件分为至少一个类别块；根据历史异常信息集合，检测目标文件的各个类别块中是否包含与历史异常信息集合中的历史异常信息相对应的异常信息；其中，每个类别块对应至少一个异常信息；在检测到目标文件的类别块中包含有与历史异常信息相对应的异常信息时，发出提醒信息。本申请通过将目标文件分为至少一个类别块，使得对目标文件的扫描检测以类别块为单位进行，对不同的类别块采取不同的扫描检测方式，以减少不必要的扫描检测时间，提高扫描检测的效率。

说明书

发明名称：文件异常检测方法、装置、电子设备及介质

技术领域

[0001] 本发明属于计算机安全技术领域，尤其涉及一种文件异常检测方法、装置、电子设备及介质。

背景技术

[0002] 技术人员在开发应用程序时，通常在开发完成某个功能后，需检查此功能对应的代码中是否存在在应用程序开发过程中已经发生过的问题，例如，存在代码编写错误等问题，以减少或防止再次触发相同的问题。但是上述方法需要人工检查该功能对应的代码，在该功能的代码较多时，容易导致检查效率低下的问题。

技术问题

[0003] 有鉴于此，本发明实施例提供了一种文件异常检测方法、装置、电子设备及介质，以解决现有技术中文件异常检查效率低下的问题。

问题的解决方案

技术解决方案

[0004] 本发明实施例的第一方面，提供了一种文件异常检测方法，包括：

[0005] 获取目标文件，所述目标文件为文档、代码或脚本，并将所述目标文件分为至少一个类别块；

[0006] 根据历史异常信息集合，检测所述目标文件的各个类别块中是否包含有与所述历史异常信息集合中的历史异常信息相对应的异常信息；其中，所述历史异常信息集合包括多条历史异常信息；

[0007] 在检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时，发出提醒信息。

[0008] 本发明实施例的第二方面，提供了一种文件异常检测装置，包括：

[0009] 获取分类模块，获取目标文件，所述目标文件为文档、代码或脚本，并将所述目标文件分为至少一个类别块；

- [0010] 检测模块，用于根据历史异常信息集合，检测所述目标文件的各个类别块中是否包含有与所述历史异常信息集合中的历史异常信息相对应的异常信息；其中，所述历史异常信息集合包括多条历史异常信息；
- [0011] 提醒模块，用于在检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时，发出提醒信息。
- [0012] 本发明实施例的第三方面，提供了一种文件异常检测电子设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的文件异常检测程序，所述处理器执行所述文件异常检测程序时实现如下步骤：
- [0013] 获取目标文件，所述目标文件为文档、代码或脚本，并将所述目标文件分为至少一个类别块；
- [0014] 根据所述历史异常信息集合，检测所述目标文件的各个类别块中是否包含与所述历史异常信息相对应的异常信息；其中，所述历史异常信息集合包括多条历史异常信息
- [0015] 在检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时，发出提醒信息。
- [0016] 本发明实施例的第四方面，提供了一种计算机可读存储介质，所述计算机可读存储介质存储有文件异常检测程序，所述文件异常检测程序被至少一个处理器执行时，实现如上述任一项所述的文件异常检测方法的步骤。

发明的有益效果

有益效果

- [0017] 本发明实施例相对于现有技术所具有的有益效果：本发明实施例，获取目标文件并将所述目标文件分为至少一个类别块；根据历史异常信息集合，检测所述目标文件的各个类别块中是否包含有与所述历史异常信息集合中的历史异常信息相对应的异常信息；其中，每个所述类别块对应至少一个所述异常信息；在检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时，发出提醒信息，通过将目标文件分为至少一个类别块，使得对目标文件的扫描检测以类别块为单位进行针对处理，对不同的类别块采取不同的扫描检测方式，以减少某些类别不必要的扫描检测时间，减少对整个目标文件的扫描检测

时间，能够提高扫描检测的效率。

对附图的简要说明

附图说明

[0018] 为了更清楚地说明本发明实施例中的技术方案，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，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0019] 图1是本发明实施例提供的文件异常检测方法的流程图；

[0020] 图2是图1中步骤S102的实现流程图；

[0021] 图3是本发明实施例提供的文件异常检测方法的具体实例流程图；

[0022] 图4是本发明实施例提供的文件异常检测程序的运行环境示意图；

[0023] 图5是本发明实施例提供的文件异常检测程序的功能模块图。

发明实施例

本发明的实施方式

[0024] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本发明实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本发明。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本发明的描述。

[0025] 为了说明本发明所述的技术方案，下面通过具体实施例来进行说明。

[0026] 图1示出了本发明实施例提供的文件异常检测方法的实现流程，详述如下：

[0027] 步骤S101，获取目标文件，所述目标文件为文档、代码或脚本，并将所述目标文件分为至少一个类别块。

[0028] 其中，可以按照系统分类、模块分类、统计分类、分析分类或应用分类等方式将所述目标文件分为至少一个类别块，以使得每个类别块代表一个系统、一个功能模块或一种应用。将目标文件分为至少一个类别块，能够使得对目标文件的扫描检测以类别块为单位进行针对处理，通过对不同的类别块采取不同的扫描检测方式，能够提高扫描检测的效率。

- [0029] 具体的，文档可以为word文档或excel文档等，代码可以为java代码、js代码、html代码、xml代码或sql脚本代码等，但并不以此为限。
- [0030] 步骤S102，根据历史异常信息集合，检测所述目标文件的各个类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息。
- [0031] 其中，所述异常信息是指目标文件中所包含的BUG（漏洞），异常信息的产生可能是由于工作人员的经验不够导致的。具体的，工作人员在处理目标文件时，由于经验不足可能导致目标文件中存在该工作人员不能预见到的异常信息（例如陷阱）。
- [0032] 所述历史异常信息集合中可以包括多条历史异常信息，每条历史异常信息均可以通过获取之前的目标文件中扫描检测出的异常信息得出。具体的，可以统计之前的目标文件中出现过的异常信息（亦称为雷点或漏洞），然后将各条异常信息按照预设规则进行分类，使得每类异常信息可以对应一个类别块。
- [0033] 然后，可以检测各个类别块中是否包含对应的历史异常信息。具体的，对于一个类别块，只需通过对应的一类历史异常信息进行扫描检测即可。
- [0034] 参见图2，一个实施例中，步骤S102可以通过以下过程实现：
- [0035] 步骤S201，获取所述目标文件的各个所述类别块和与所述类别块对应的扫描方式。
- [0036] 作为一种可实施方式，所述获取所述类别块对应的扫描方式具体为：根据各个历史目标文件中检测出的历史异常信息对各个所述类别块设置相应的扫描方式。
- [0037] 具体的，可以将获取到的各个历史异常信息按照预设规则进行分类，得到多类历史异常信息，并根据每类历史异常信息的情况，例如该类历史异常信息出现的频率、该类历史异常信息的严重程度，再结合历史异常信息与各个类别块的对应关系，对每个类别块设置相应的扫描检测方式，以减少某些类别不必要的扫描时间，减少对整个目标文件的扫描时间。历史异常信息与类别块的对应关系可以通过按照预设规则对历史目标文件进行分类，统计各类历史异常信息对应的分类块得出。
- [0038] 例如，扫描检测方式可以包括跳过扫描、部分扫描和全部扫描等。对于出现的

频率较大、严重程度较高的历史异常信息对应的分类块，可以采用全部扫描的方式进行扫描；对于出现的频率较小、严重程度较低的历史异常信息对应的分类块，可以采用部分扫描或跳过扫描的方式进行扫描。

[0039] 需要说明的是，各个历史目标文件中检测出的历史异常信息可以作为对之后的目标文件扫描检测时需要的历史异常信息。而且历史异常信息集合中的各条历史异常信息可以为当前时间之前所有时间内的异常信息，也可以为当前时间之前预设时间段内的异常信息。

[0040] 步骤S202，通过与各个所述类别块对应的扫描方式，检测所述类别块中是否包含有与所述历史异常信息集合中的历史异常信息相对应的异常信息。

[0041] 本实施例中，扫描检测方式可以包括多种扫描方式，例如跳过扫描、部分扫描和全部扫描等。例如，所述历史异常信息集合中包括三类历史异常信息，分别为第一类历史异常信息、第二类历史异常信息和第三类历史异常信息；根据预设规则将目标文件分为三个类别块，分别为第一类别块、第二类别块和第三类别块。其中，第一类别块与第一类历史异常信息对应，第二类别块与第二类历史异常信息对应，第三类别块与第三类历史异常信息对应。而第一类别块对应的扫描方式为忽略扫描，第二类别块对应的扫描方式为部分扫描，第三类别块对应的扫描方式为全部扫描。

[0042] 根据上述设置，对目标文件的第一类别块忽略扫描，对目标文件的第二类别块进行部分扫描，对目标文件的第三类别块进行全部扫描，以加快对整个目标文件的扫描速度，也能做到有的放矢，不遗漏程度较重的异常信息。

[0043] 作为一种可实施方式，所述检测所述类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息具体为：对所述各个类别块，通过关键字和预设算法进行扫描，以检测所述各个类别块中是否包含有与所述历史异常信息对应的异常信息。通过设置关键字和预设算法，能够进一步减少对目标文件的各个类别块的扫描检测时间，提高检测效率。

[0044] 步骤S103，在检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时，发出提醒信息。

[0045] 可以理解的，在检测到目标文件的类别块中包含于所述历史异常信息对应的异

常信息时，发出提醒信息，以提醒开发人员注意雷点，从而防止开发人员运行具有异常信息的目标文件。其中，提醒信息可以为声光提醒信息或文字提醒信息，对此不做限定。

[0046] 可选的，在步骤S103之后，该文件异常检测方法还可以包括：输出所述异常信息在所述目标文件中的位置信息。输出异常信息在目标文件中的位置信息，能够使得开发人员及时发现目标文件的问题以进行改正，从而提高工作效率。

[0047] 图3示出了该文件异常检测方法的具体流程示意图，详述如下：

[0048] 步骤S301，获取目标文件，所述目标文件为文档、代码或脚本，并将所述目标文件分为至少一个类别块。

[0049] 步骤S302，获取历史异常信息集合，所述历史异常信息集合包含多条历史异常信息。

[0050] 步骤S303，获取所述目标文件的各个所述类别块和与所述类别块对应的扫描方式。

[0051] 步骤S304，通过与各个类别块对应的扫描方式，通过关键字和预设算法进行扫描，以检测所述各个类别块中是否包含有与所述历史异常信息对应的异常信息。

[0052] 步骤S305，在检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时，发出提醒信息。

[0053] 步骤S306，输出所述异常信息在所述目标文件中的位置信息。

[0054] 上述文件异常检测方法，获取目标文件并将所述目标文件分为至少一个类别块；根据历史异常信息集合，检测所述目标文件的各个类别块中是否包含有与所述历史异常信息集合中的历史异常信息相对应的异常信息；其中，每个所述类别块对应至少一个所述异常信息；在检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时，发出提醒信息，通过将目标文件分为至少一个类别块，使得对目标文件的扫描检测以类别块为单位进行针对处理，对不同的类别块采取不同的扫描检测方式，以减少某些类别不必要的扫描检测时间，减少对整个目标文件的扫描检测时间，能够提高扫描检测的效率。

[0055] 应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过

程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0056] 对应于上文实施例所述的文件异常检测方法，图4示出了本发明实施例提供的文件异常检测程序的运行环境示意图。为了便于说明，仅示出了与本实施例相关的部分。

[0057] 在本实施例中，所述的文件异常检测程序400安装并运行于电子设备40中。该电子设备40可以是移动终端、掌上电脑、服务器等。该电子设备40可包括，但不限于，存储器401、处理器402及显示器403。图6仅示出了具有组件401-403的电子设备40，但是应理解的是，并不要求实施所有示出的组件，可以替代的实施更多或者更少的组件。

[0058] 所述存储器401在一些实施例中可以是所述电子设备40的内部存储单元，例如该电子设备40的硬盘或内存。所述存储器401在另一些实施例中也可以是所述电子设备40的外部存储设备，例如所述电子设备40上配备的插接式硬盘，智能存储卡（Smart Media Card，SMC），安全数字（Secure Digital，SD）卡，闪存卡（Flash Card）等。进一步地，所述存储器401还可以既包括所述电子设备40的内部存储单元也包括外部存储设备。所述存储器401用于存储安装于所述电子设备40的应用软件及各类数据，例如所述文件异常检测程序400的程序代码等。所述存储器401还可以用于暂时地存储已经输出或者将要输出的数据。

[0059] 所述处理器402在一些实施例中可以是一中央处理器（Central Processing Unit，CPU），微处理器或其他数据处理芯片，用于运行所述存储器401中存储的程序代码或处理数据，例如执行所述文件异常检测程序400等。

[0060] 所述显示器403在一些实施例中可以是LED显示器、液晶显示器、触控式液晶显示器以及OLED（Organic Light-Emitting Diode，有机发光二极管）触摸器等。所述显示器403用于显示在所述电子设备40中处理的信息以及用于显示可视化的用户界面，例如应用菜单界面、应用图标界面等。所述电子设备40的部件401-403通过系统总线相互通信。

[0061] 请参阅图5，是本发明实施例提供的文件异常检测程序400的功能模块图。在本实施例中，所述的文件异常检测程序400可以被分割成一个或多个模块，所述一

个或者多个模块被存储于所述存储器401中，并由一个或多个处理器（本实施例为所述处理器402）所执行，以完成本发明。例如，在图5中，所述的文件异常检测程序400可以被分割成获取分类模块501、存储模块502、检测模块503和提醒模块504。本发明所称的模块是指能够完成特定功能的一系列计算机程序指令段，比程序更适合于描述所述文件异常检测程序400在所述电子设备40中的执行过程。以下描述将具体介绍所述模块501-504的功能。

[0062] 其中，获取分类模块501，用于获取目标文件，所述目标文件为文档、代码或脚本，并将所述目标文件分为至少一个类别块。存储模块502，用于存储历史异常信息集合，所述历史异常信息集合中包括多条历史异常信息。检测模块503，用于根据所述存储模块502中存储的所述历史异常信息集合，检测所述目标文件的各个类别块中是否包含与所述历史异常信息相对应的异常信息。其中，每个所述类别块对应至少一个所述异常信息。提醒模块504，用于在所述检测模块检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时，发出提醒信息。

[0063] 参见图5，一个实施例中，所述检测模块503包括获取单元601和检测单元602。其中，获取单元601，用于获取所述目标文件的各个所述类别块和与所述类别块对应的扫描方式。检测单元602，用于通过与各个所述类别块对应的扫描方式，检测所述类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息。

[0064] 可选的，所述获取单元601具体用于：获取预设时间段内各个所述目标文件中的各个异常信息，然后根据获取的各个异常信息对各个所述类别块设置相应的扫描方式。

[0065] 可选的，所述检测单元602具体用于：对所述各个类别块，通过关键字和预设算法进行扫描，以检测所述各个类别块中是否包含有与所述历史异常信息对应的异常信息。

[0066] 可选的，该文件异常检测程序还可以包括显示模块505。显示模块505，用于输出所述异常信息在所述目标文件中的位置信息。

[0067] 综上所述，安装并运行于电子设备40中的文件异常检测程序400，获取目标文

件并将所述目标文件分为至少一个类别块；根据历史异常信息集合，检测所述目标文件的各个类别块中是否包含有与所述历史异常信息集合中的历史异常信息相对应的异常信息；其中，每个所述类别块对应至少一个所述异常信息；在检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时，发出提醒信息，通过将目标文件分为至少一个类别块，使得对目标文件的扫描检测以类别块为单位进行针对处理，对不同的类别块采取不同的扫描检测方式，以减少某些类别不必要的扫描检测时间，减少对整个目标文件的扫描检测时间，能够提高扫描检测的效率。

[0068] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块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。另外，各功能单元、模块的具体名称也只是为了便于相互区分，并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0069] 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0070] 在本发明所提供的实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，以上所描述的系统实施例仅仅是示意性的，例如，所述模块或单元的划分，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

通讯连接可以通过一些接口，装置或单元的间接耦合或通讯连接，可以是电性，机械或其它的形式。

[0071] 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。

[0072] 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。

[0073] 所述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，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实施例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一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本发明实施例各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

[0074] 以上所述实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围，均应包含在本发明的保护范围之内。

权利要求书

- [权利要求 1] 一种文件异常检测方法，其特征在于，包括：
- 获取目标文件，所述目标文件为文档、代码或脚本，并将所述目标文件分为至少一个类别块；
- 根据历史异常信息集合，检测所述目标文件的各个类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息；其中，所述历史异常信息集合包括多条历史异常信息；
- 在检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时，发出提醒信息。
- [权利要求 2] 根据权利要求1所述的文件异常检测方法，其特征在于，所述检测所述目标文件的各个类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息包括：
- 获取所述目标文件的各个所述类别块和与所述类别块对应的扫描方式；
- 通过与各个所述类别块对应的扫描方式，检测所述类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息。
- [权利要求 3] 根据权利要求2所述的文件异常检测方法，其特征在于，所述获取所述类别块对应的扫描方式具体为：
- 获取预设时间段内各个所述目标文件中检测出的异常信息，然后根据获取的各个异常信息对各个所述类别块设置相应的扫描方式。
- [权利要求 4] 根据权利要求2所述的文件异常检测方法，其特征在于，所述检测所述类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息具体为：
- 对所述各个类别块，通过关键字和预设算法进行扫描，以检测所述各个类别块中是否包含与所述历史异常信息对应的异常信息。
- [权利要求 5] 根据权利要求1至4中任一项所述的文件异常检测方法，其特征在于，还包括：
- 输出所述异常信息在所述目标文件中的位置信息。

- [权利要求 6] 一种文件异常检测装置，其特征在于，包括：
获取分类模块，获取目标文件，所述目标文件为文档、代码或脚本，并将所述目标文件分为至少一个类别块；
检测模块，用于根据历史异常信息集合，检测所述目标文件的各个类别块中是否包含有与所述历史异常信息集合中的历史异常信息相对应的异常信息；其中，所述历史异常信息集合包括多条历史异常信息；
提醒模块，用于在检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时，发出提醒信息。
- [权利要求 7] 根据权利要求6所述的文件异常检测装置，其特征在于，所述检测模块包括：
获取单元，用于获取所述目标文件的各个所述类别块和与所述类别块对应的扫描方式；
检测单元，用于通过与各个所述类别块对应的扫描方式，检测所述类别块中是否包含有与所述历史异常信息集合中的历史异常信息相对应的异常信息。
- [权利要求 8] 根据权利要求7所述的文件异常检测装置，其特征在于，所述获取单元具体用于：获取预设时间段内各个所述目标文件中检测出的异常信息，然后根据获取的各个异常信息对各个所述类别块设置相应的扫描方式。
- [权利要求 9] 根据权利要求7所述的文件异常检测装置，其特征在于，所述检测单元具体用于：对所述各个类别块，通过关键字和预设算法进行扫描，以检测所述各个类别块中是否包含有与所述历史异常信息对应的异常信息。
- [权利要求 10] 根据权利要求6至9中任一项所述的文件异常检测装置，其特征在于，还包括：
输出模块，用于输出所述异常信息在所述目标文件中的位置信息。
- [权利要求 11] 一种文件异常检测电子设备，其特征在于，包括存储器、处理器及存储在该存储器上并可在该处理器上运行的文件异常检测程序，所

述处理器执行所述文件异常检测程序时实现如下步骤:

获取目标文件, 所述目标文件为文档、代码或脚本, 并将所述目标文件分为至少一个类别块;

根据历史异常信息集合, 检测所述目标文件的各个类别块中是否包含与所述历史异常信息相对应的异常信息; 其中, 所述历史异常信息集合包括多条历史异常信息

在检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时, 发出提醒信息。

[权利要求 12] 根据权利要求11所述的文件异常检测电子设备, 其特征在于, 所述根据历史异常信息集合, 检测所述目标文件的各个类别块中是否包含与所述历史异常信息相对应的异常信息具体包括:
获取所述目标文件的各个所述类别块和与所述类别块对应的扫描方式;

通过与各个所述类别块对应的扫描方式, 检测所述类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息。

[权利要求 13] 根据权利要求12所述的文件异常检测电子设备, 其特征在于, 所述获取所述目标文件的各个所述类别块和与所述类别块对应的扫描方式具体为: 获取预设时间段内各个所述目标文件中检测出的异常信息, 然后根据获取的各个异常信息对各个所述类别块设置相应的扫描方式。

[权利要求 14] 根据权利要求12所述的文件异常检测电子设备, 其特征在于, 所述通过与各个所述类别块对应的扫描方式, 检测所述类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息具体为:
对所述各个类别块, 通过关键字和预设算法进行扫描, 以检测所述各个类别块中是否包含有与所述历史异常信息对应的异常信息。

[权利要求 15] 根据权利要求11至14中任一项所述的文件异常检测电子设备, 其特征在于, 所述处理器执行所述文件异常检测程序时, 还实现如下步骤:
输出所述异常信息在所述目标文件中的位置信息。

[权利要求 16] 一种计算机可读存储介质, 所述计算机可读存储介质存储有文件异常

检测程序，其特征在于，所述文件异常检测程序被至少一个处理器执行时实现如下步骤：

获取目标文件，所述目标文件为文档、代码或脚本，并将所述目标文件分为至少一个类别块；

根据历史异常信息集合，检测所述目标文件的各个类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息；其中，所述历史异常信息集合包括多条历史异常信息；

在检测到所述目标文件的类别块中包含与所述历史异常信息相对应的异常信息时，发出提醒信息。

[权利要求 17] 根据权利要求16所述的计算机可读存储介质，其特征在于，所述检测所述目标文件的各个类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息包括：

获取所述目标文件的各个所述类别块和与所述类别块对应的扫描方式；

通过与各个所述类别块对应的扫描方式，检测所述类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息。

[权利要求 18] 根据权利要求17所述的计算机可读存储介质，其特征在于，所述获取所述类别块对应的扫描方式具体为：

获取预设时间段内各个所述目标文件中检测出的异常信息，然后根据获取的各个异常信息对各个所述类别块设置相应的扫描方式。

[权利要求 19] 根据权利要求17所述的计算机可读存储介质，其特征在于，所述检测所述类别块中是否包含与所述历史异常信息集合中的历史异常信息相对应的异常信息具体为：

对所述各个类别块，通过关键字和预设算法进行扫描，以检测所述各个类别块中是否包含与所述历史异常信息对应的异常信息。

[权利要求 20] 根据权利要求16至19中任一项所述的计算机可读存储介质，其特征在于，所述文件异常检测程序被至少一个处理器执行时，还实现如下步骤：

输出所述异常信息在所述目标文件中的位置信息。

说明书附图

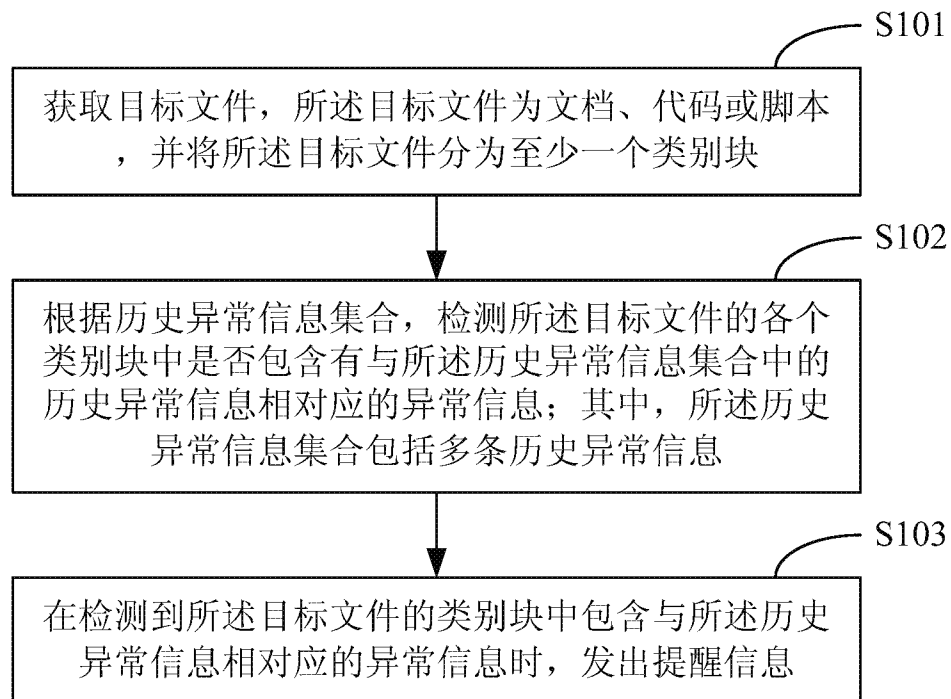


图 1

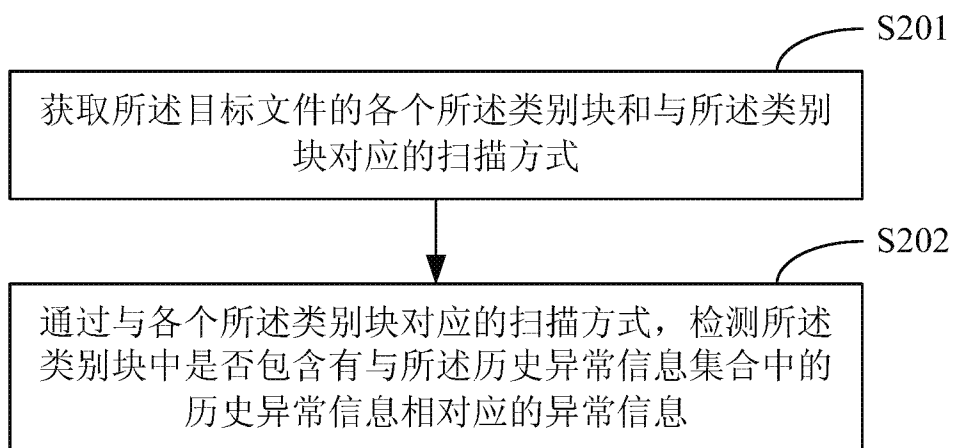


图 2

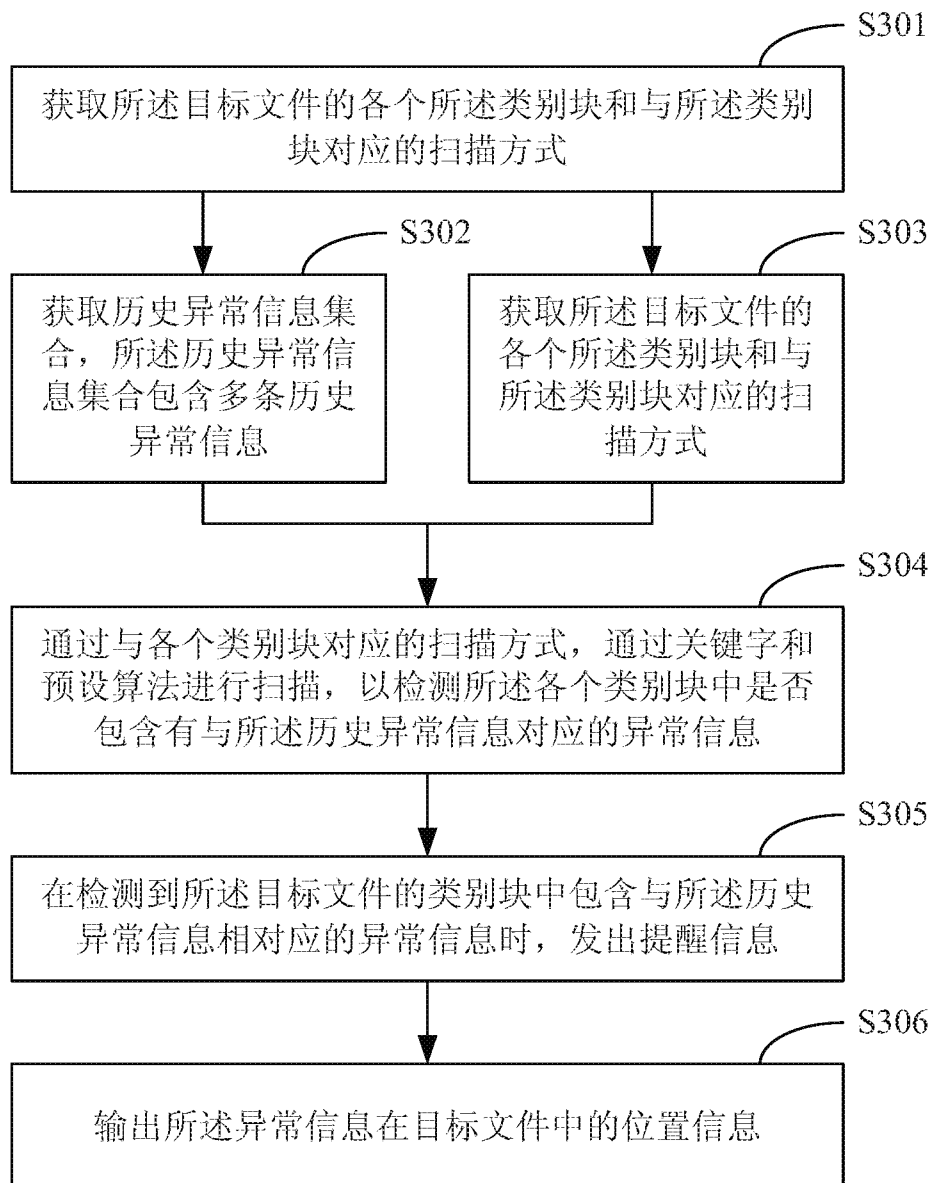


图 3

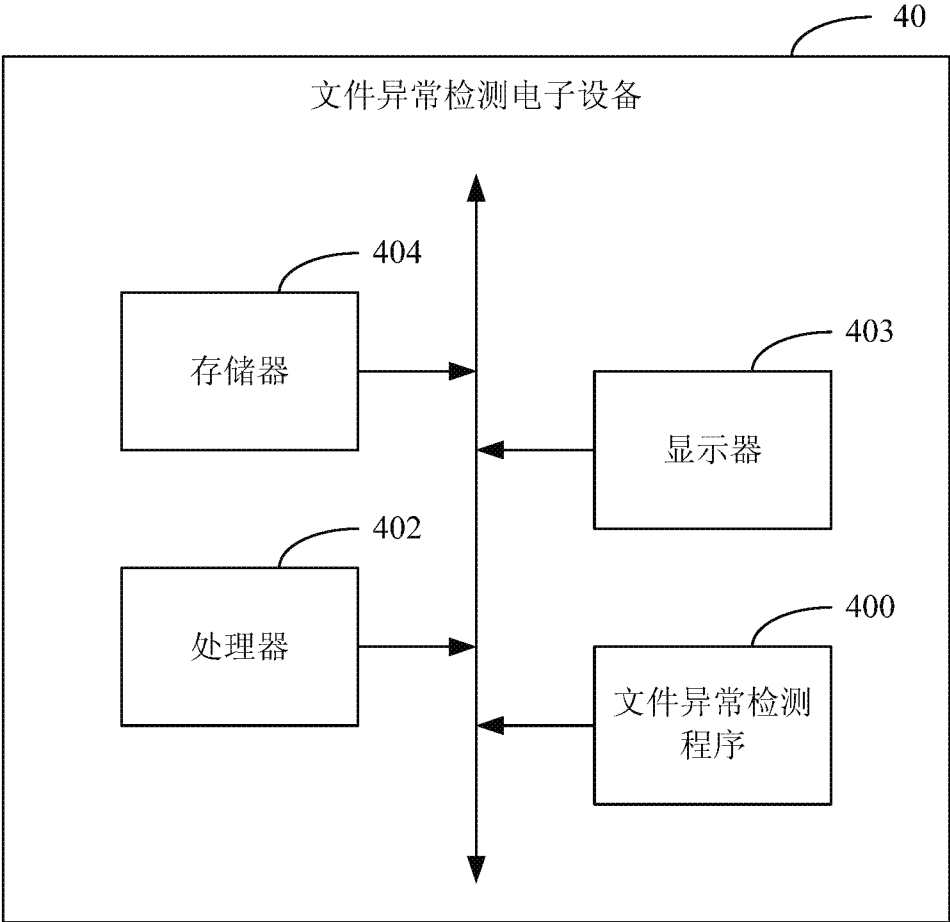


图 4

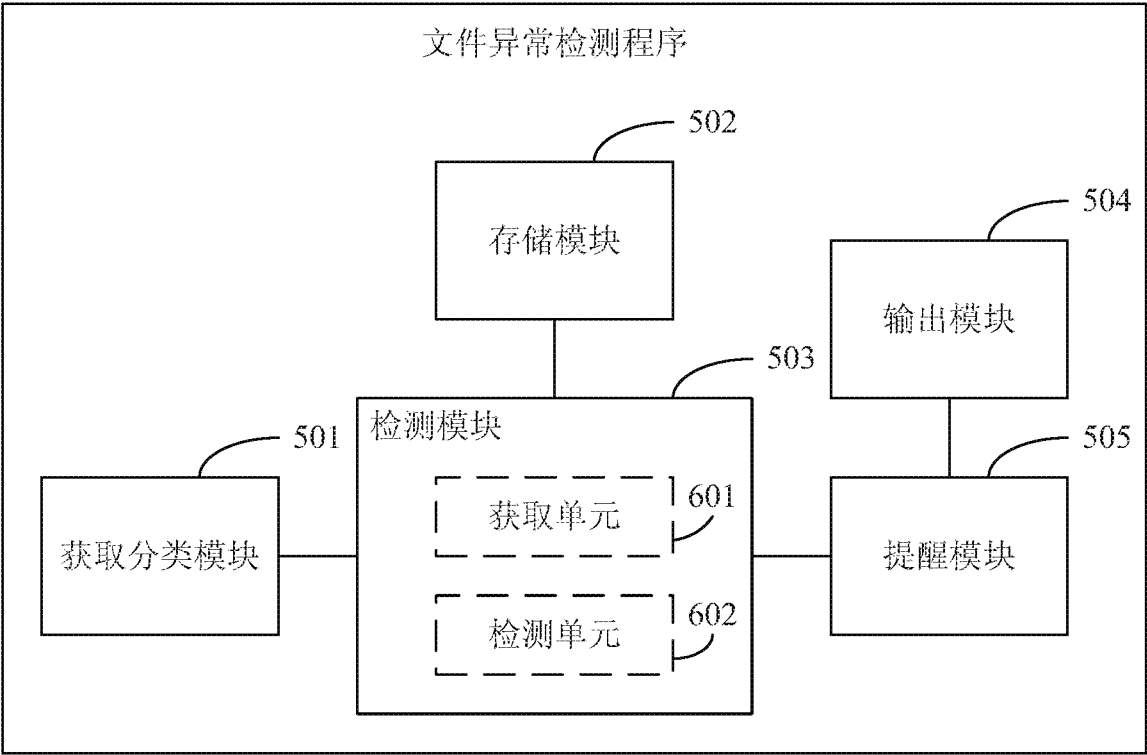


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2017/090308

A. CLASSIFICATION OF SUBJECT MATTER

G06F 11/36(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)

G06F

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)

CNKI, CNABS, SIPOABS, DWPI: 异常, 信息, 漏洞, 错误, 消息, 提醒, 历史, 比对, exception, message, information, error, history, message, compare

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 106371983 A (BEIJING 58 INFORMATION TECHNOLOGY CO., LTD.) 01 February 2017 (2017-02-01) description, paragraphs 0005-0045, and figures 1-2	1-20
Y	CN 106201757 A (NETEASE (HANGZHOU) NETWORK CO., LTD.) 07 December 2016 (2016-12-07) abstract	1-20
A	CN 106021358 A (SHENZHEN YUNZHIJIA NETWORK CO., LTD.) 12 October 2016 (2016-10-12) entire document	1-20
A	US 7729270 B2 (INTERNATIONAL BUSINESS MACHINES CORPORATION ET AL.) 01 June 2010 (2010-06-01) entire document	1-20

☐ 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

30 January 2018

Date of mailing of the international search report

09 February 2018

Name and mailing address of the ISA/CN

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

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2017/090308

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	106371983	A	01 February 2017	None			
CN	106201757	A	07 December 2016	None			
CN	106021358	A	12 October 2016	None			
US	7729270	B2	01 June 2010	US	2006153090	A1	13 July 2006

国际检索报告

国际申请号

PCT/CN2017/090308

A. 主题的分类 G06F 11/36 (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) G06F 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)) CNKI, CNABS, SIPOABS, DWPI: 异常, 信息, 漏洞, 错误, 消息, 提醒, 历史, 比对, exception, message, information, error, history, message, compare																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>Y</td> <td>CN 106371983 A (五八同城信息技术有限公司) 2017年 2月 1日 (2017 - 02 - 01) 说明书0005-0045段, 附图1-2</td> <td>1-20</td> </tr> <tr> <td>Y</td> <td>CN 106201757 A (网易杭州网络有限公司) 2016年 12月 7日 (2016 - 12 - 07) 摘要</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 106021358 A (深圳云之家网络有限公司) 2016年 10月 12日 (2016 - 10 - 12) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>US 7729270 B2 (INTERNATIONAL BUSINESS MACHINES CORPORATION 等) 2010年 6月 1日 (2010 - 06 - 01) 全文</td> <td>1-20</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	Y	CN 106371983 A (五八同城信息技术有限公司) 2017年 2月 1日 (2017 - 02 - 01) 说明书0005-0045段, 附图1-2	1-20	Y	CN 106201757 A (网易杭州网络有限公司) 2016年 12月 7日 (2016 - 12 - 07) 摘要	1-20	A	CN 106021358 A (深圳云之家网络有限公司) 2016年 10月 12日 (2016 - 10 - 12) 全文	1-20	A	US 7729270 B2 (INTERNATIONAL BUSINESS MACHINES CORPORATION 等) 2010年 6月 1日 (2010 - 06 - 01) 全文	1-20
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
Y	CN 106371983 A (五八同城信息技术有限公司) 2017年 2月 1日 (2017 - 02 - 01) 说明书0005-0045段, 附图1-2	1-20															
Y	CN 106201757 A (网易杭州网络有限公司) 2016年 12月 7日 (2016 - 12 - 07) 摘要	1-20															
A	CN 106021358 A (深圳云之家网络有限公司) 2016年 10月 12日 (2016 - 10 - 12) 全文	1-20															
A	US 7729270 B2 (INTERNATIONAL BUSINESS MACHINES CORPORATION 等) 2010年 6月 1日 (2010 - 06 - 01) 全文	1-20															
☐ 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 2018年 1月 30日		国际检索报告邮寄日期 2018年 2月 9日															
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		授权官员 马雅凡 电话号码 (86-10) 62089420															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/090308

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	106371983	A	2017年 2月 1日	无	
CN	106201757	A	2016年 12月 7日	无	
CN	106021358	A	2016年 10月 12日	无	
US	7729270	B2	2010年 6月 1日	US 2006153090 A1	2006年 7月 13日