(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 5 月 17 日 (17.05.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/086293 A1

(51) 国际专利分类号:
G06F 21/52 (2013.01)

(21) 国际申请号: PCT/CN2017/077985

(22) 国际申请日: 2017 年 3 月 24 日 (24.03.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201611036380.X 2016年11月14日 (14.11.2016) 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: 王金锭 (WANG, Jinding); 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: 深圳市世纪恒程知识产权代理事务所 (CENFO INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市南山区南山大道3838号设计产业园金栋二层210-212（原南头城工业村11栋）, Guangdong 518052 (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, 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,

(54) **Title:** METHOD AND APPARATUS FOR DETECTING DATA LEAKAGE INTERFACE, DEVICE, AND STORAGE MEDIUM

(54) **发明名称**: 数据泄露接口检测方法、装置、设备及存储介质

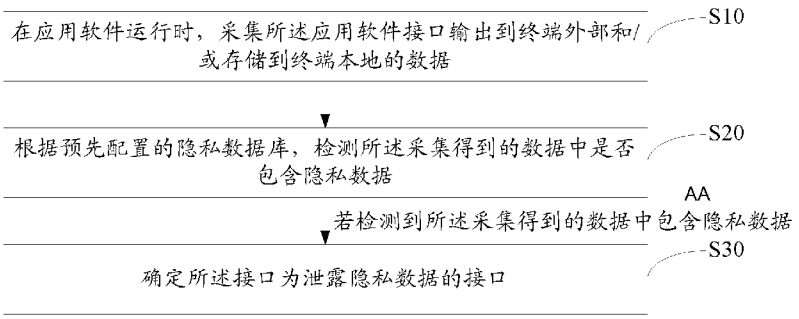

图 1

S10 ACQUIRE, WHEN APPLICATION SOFTWARE RUNS, DATA WHICH IS OUTPUT TO THE OUTSIDE OF A TERMINAL AND/OR IS STORED IN THE TERMINAL LOCALLY BY AN APPLICATION SOFTWARE INTERFACE

S20 DETECT WHETHER THE ACQUIRED DATA COMPRISE PRIVACY DATA ACCORDING TO A PRECONFIGURED PRIVACY DATABASE

S30 DETERMINE THE INTERFACE AS AN INTERFACE FOR LEAKAGE OF THE PRIVACY DATA

AA IF IT IS DETECTED THAT THE ACQUIRED DATA COMPRISE PRIVACY DATA

(57) **Abstract:** A method for detecting a data leakage interface, comprising: acquiring, when application software runs, data which is output to the outside of a terminal and/or is stored in the terminal locally by an application software interface (S10); detecting whether the acquired data comprise privacy data according to a preconfigured privacy database (S20); and if it is detected that the acquired data comprise privacy data, determining the interface as an interface for leakage of the privacy data (S30). Also disclosed are an apparatus for detecting a data leakage interface, a device, and a computer-readable storage medium. In combination with dynamic data acquisition and automatic static data analysis, the present invention ensures the integrity of data for detection and analysis, avoids false reporting and missing reporting of a privacy data leakage interface, and greatly improves the detection efficiency of the privacy leakage interface of application software and reduces labor costs.

WO 2018/086293 A1

[见续页]

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, 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：一种数据泄露接口检测方法，该方法包括：在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据（S10）；根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据（S20）；若检测到所述采集得到的数据中包含隐私数据，则确定所述接口为泄露隐私数据的接口（S30）。还公开了一种数据泄露接口检测装置、设备及计算机可读存储介质。结合动态数据采集和静态数据自动分析，保障了用于检测分析的数据的完整性，避免隐私数据泄露接口的误报、漏报，大大提高了应用软件隐私泄露接口检测的效率，降低了人工成本。

数据泄露接口检测方法、装置、设备及存储介质

[1] 技术领域

[2] 本发明涉及信息安全技术领域，尤其涉及一种数据泄露接口检测方法、装置、设备及计算机可读存储介质。

[3] 背景技术

[4] 多种多样的应用软件涉及到人们的社交、财产、办公、生活等方方面面，给人们的工作、生活带来便利，成为了智能终端必不可少的一部分。在应用过程中，应用软件能够接触、搜集大量的用户数据，包括账户密码、聊天信息等隐私信息。

[5] 为了保障用户的信息安全，目前检查应用软件隐私泄露的方法一般是人工分析，借助测试人员的经验去界定应用软件运行过程中各接口在本地存储、网络传输及日志输出等方面的数据是否涉及隐私泄露问题。一方面，人工分析的检查方式耗时较长，存在重复性的工作，浪费人力资源；另一方面，依赖测试人员的经验，可能存在遗漏或误判情况。

[6] 可见，目前的人工分析方法导致应用软件隐私泄露接口的检测效率低下。

[7] 发明内容

[8] 本发明的主要目的在于提供一种数据泄露接口检测方法、装置、设备及计算机可读存储介质，旨在解决应用软件隐私泄露接口的检测效率低下的技术问题。

[9] 为实现上述目的，本发明提供一种数据泄露接口检测方法，所述数据泄露接口检测方法包括以下步骤：

[10] 在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据；

[11] 根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据；

[12] 若检测到所述采集得到的数据中包含隐私数据，则确定所述接口为泄露隐私数据的接口。

[13] 优选地，所述采集得到的数据中包括多个数据项，所述根据预先配置的隐私数

据库，检测所述采集得到的数据中是否包含隐私数据的步骤包括：

[14] 根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据；

[15] 若检测得到至少有一个数据项包含隐私数据，则判定所述采集得到的数据中包含隐私数据。

[16] 优选地，所述确定所述接口为泄露隐私数据的接口的步骤之后，还包括：

[17] 根据所述采集得到的数据中所包含的隐私数据的安全等级，对应配置所述接口的危险等级。

[18] 优选地，所述采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据的步骤之前，还包括：

[19] 基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到所述隐私数据库；

[20] 在所述应用软件运行时，向所述应用软件输入所述隐私数据。

[21] 优选地，所述采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据的步骤包括：

[22] 抓取所述接口输出的网络信息包，得到所述接口输出到终端外部的数据；

[23] 基于预先配置的插桩，采集所述接口输出的本地广播和日志，得到所述接口存储到终端本地的数据。

[24] 此外，为实现上述目的，本发明还提供一种数据泄露接口检测装置，所述数据泄露接口检测装置包括：

[25] 采集模块，用于在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据；

[26] 检测模块，用于根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据；

[27] 确定模块，用于若检测到所述采集得到的数据中包含隐私数据，则确定所述接口为泄露隐私数据的接口。

[28] 优选地，所述采集得到的数据中包括多个数据项，所述检测模块还用于，

[29] 根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据；若检测得到至少有一个数据项包含隐私数据，则判定所述采集得到的数据中包含隐私数据

。

[30] 优选地，所述数据泄露接口检测装置还包括：

[31] 等级模块，用于根据所述采集得到的数据中所包含的隐私数据的安全等级，对应配置所述接口的危险等级。

[32] 优选地，所述数据泄露接口检测装置还包括：

[33] 配置模块，用于基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到所述隐私数据库；

[34] 输入模块，用于在所述应用软件运行时，向所述应用软件输入所述隐私数据。

[35] 优选地，所述采集模块还用于，

[36] 抓取所述接口输出的网络信息包，得到所述接口输出到终端外部的数据；基于预先配置的插桩，采集所述接口输出的本地广播和日志，得到所述接口存储到终端本地的数据。

[37] 此外，为实现上述目的，本发明还提供一种数据泄露接口检测设备，所述数据泄露接口检测设备包括处理器及存储器，所述存储器中存储有数据泄露接口检测程序；

[38] 所述处理器用于执行所述数据泄露接口检测程序，以实现以下步骤：

[39] 在应用软件运行时，采集所述应用软件接口输出到设备外部和/或存储到设备本地的数据；

[40] 根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据；

[41] 若检测到所述采集得到的数据中包含隐私数据，则确定所述应用软件接口为泄露隐私数据的接口。

[42] 优选地，所述采集得到的数据中包括多个数据项，所述处理器还用于执行所述数据泄露接口检测程序，以实现以下步骤：

[43] 根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据；

[44] 若检测得到至少有一个数据项包含隐私数据，则判定所述采集得到的数据中包含隐私数据。

[45] 优选地，所述处理器还用于执行所述数据泄露接口检测程序，以实现以下步骤：

[46] 根据所述采集得到的数据中所包含的隐私数据的安全等级，对应配置所述应用软件接口的危险等级。

[47] 优选地，所述处理器还用于执行所述数据泄露接口检测程序，以实现以下步骤：

[48] 基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到所述隐私数据库；

[49] 在所述应用软件运行时，向所述应用软件输入所述隐私数据。

[50] 优选地，所述处理器还用于执行所述数据泄露接口检测程序，以实现以下步骤：

[51] 抓取所述应用软件接口输出的网络信息包，得到所述应用软件接口输出到设备外部的数据；

[52] 基于预先配置的插桩，采集所述应用软件接口输出的本地广播和日志，得到所述应用软件接口存储到设备本地的数据。

[53] 此外，为实现上述目的，本发明还提供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一个或者多个程序，所述一个或者多个程序可被一个或者多个处理器执行，以实现以下步骤：

[54] 在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据；

[55] 根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据；

[56] 若检测到所述采集得到的数据中包含隐私数据，则确定所述接口为泄露隐私数据的接口。

[57] 优选地，所述采集得到的数据中包括多个数据项，所述一个或者多个程序可被所述一个或者多个处理器执行，还实现以下步骤：

[58] 根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据；

[59] 若检测得到至少有一个数据项包含隐私数据，则判定所述采集得到的数据中包含隐私数据。

[60] 优选地，所述一个或者多个程序可被所述一个或者多个处理器执行，还实现以下步骤：

[61] 根据所述采集得到的数据中所包含的隐私数据的安全等级，对应配置所述接口的危险等级。

[62] 优选地，所述一个或者多个程序可被所述一个或者多个处理器执行，还实现以下步骤：

[63] 基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到所述隐私数据库；

[64] 在所述应用软件运行时，向所述应用软件输入所述隐私数据。

[65] 优选地，所述一个或者多个程序可被所述一个或者多个处理器执行，还实现以下步骤：

[66] 抓取所述接口输出的网络信息包，得到所述接口输出到终端外部的数据；

[67] 基于预先配置的插桩，采集所述接口输出的本地广播和日志，得到所述接口存储到终端本地的数据。

[68] 本发明实施例提出的一种数据泄露接口检测方法、装置、设备及计算机可读存储介质，在应用软件运行时，采集应用软件接口输出到终端外部和/或存储到终端本地的数据，由于是在应用软件动态运行过程中采集的数据，因此能够获取应用软件实际运行过程中输出的各项信息数据，使得采集的数据覆盖面更广，具有真实性、可靠性和完整性；然后，根据预先配置的隐私数据库，检测采集得到的各项数据中是否包含隐私数据，从而实现了对采集的数据中是否包含有隐私数据的自动化检测，由于是以记载了各项隐私数据的隐私数据库为依据的，因此，在对采集得到的数据进行检测时，避免了人工分析以经验为依据而导致的漏报、误报。若检测到采集得到的数据中包含隐私数据，则确定此接口为泄露隐私数据的接口，由此，可以获取应用软件中泄露隐私数据的各接口，完成对应用软件接口泄露隐私数据的检测。通过发明，结合动态数据采集和静态数据自动分析，不会遗漏应用软件接口输出的任何数据，保障了用于检测分析的数据的完整性，并且，避免隐私数据泄露接口的误报、漏报，大大提高了应用软件隐私泄露接口检测的效率，降低了人工成本。

[69] 附图说明

[70] 图1为本发明数据泄露接口检测方法第一实施例的流程示意图；

[71] 图2为图1中步骤S20的细化流程示意图；

[72] 图3为本发明数据泄露接口检测方法第二实施例的流程示意图；

[73] 图4为本发明数据泄露接口检测方法第三实施例的流程示意图；

[74] 图5为本发明数据泄露接口检测方法一实施例中采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据的步骤的细化流程示意图；

[75] 图6为本发明数据泄露接口检测装置第一实施例的功能模块示意图；

[76] 图7为本发明数据泄露接口检测装置第二实施例的功能模块示意图；

[77] 图8为本发明数据泄露接口检测装置第三实施例的功能模块示意图；

[78] 图9是本发明实施例方案涉及的硬件运行环境的设备结构示意图。

[79] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

[80] 具体实施方式

[81] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[82] 参照图1，本发明数据泄露接口检测方法第一实施例提供一种数据泄露接口检测方法，所述数据泄露接口检测方法包括：

[83] 步骤S10、在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据。

[84] 本发明通过采集应用软件运行过程中对外输出的数据，离线自动检测对外输出的数据中是否包含有隐私数据，无需人工手动检测，不依赖于人工的经验，可以全方位地自动排查应用软件的隐私泄露问题，避免漏报，提高应用软件的隐私泄露检测效率。

[85] 具体的，作为一种实施方式，启动应用软件，在应用软件运行的过程中，通过插桩、抓包等多种形式，分别采集应用软件运行过程中各接口对外输出的全部数据。

[86] 需要说明的是，应用软件运行过程中接口对外输出的全部数据包括接口以网络形式输出到终端外部的数据、存储到终端本地的数据，例如：写的日志、打印的文件、发送给终端上部署的其他应用软件的数据等。

[87] 在采集各接口输出的全部数据后，分别独立记录各接口输出的数据，以分别检

测各接口输出的数据是否涉及到隐私数据的泄露。

[88] 步骤S20、根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据。

[89] 在采集得到应用软件接口输出的全部数据后，根据预先配置的隐私数据库，检测采集得到的数据中是否包含有敏感的隐私数据。

[90] 其中，隐私数据库包括输入到应用软件的各项隐私数据以及应用软件生成的涉及用户隐私的数据，例如账户密码、聊天记录、交易记录等等。

[91] 并且，隐私数据库中记载的各项涉及用户隐私的数据，均对应有包括多种数据形式的隐私数据条目，例如账户密码对应的隐私数据条目，包括明文、哈希值、字符串等多种形式的账户密码。同一隐私数据条目中不同数据形式的隐私数据可以分节存储，从而提高了隐私数据监测的灵活性，以避免应用软件转换隐私数据的形式进行输出时，无法检测出变换数据形式后的隐私数据。

[92] 由此，在采集得到应用软件接口输出的全部数据后，在隐私数据库中查找是否有与采集的数据匹配的隐私数据条目。若在隐私数据库中找到与采集的数据匹配的隐私数据条目，则确定应用软件接口输出的数据中包含有隐私数据。

[93] 进一步地，作为一种实施方式，所述采集得到的数据中包括多个数据项，参照图2，所述步骤S20包括：

[94] 步骤S21、根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据；

[95] 步骤S22、若检测得到至少有一个数据项包含隐私数据，则判定所述采集得到的数据中包含隐私数据。

[96] 需要说明的是，采集得到的应用软件接口输出的数据中包含多个数据项，例如接口通过网络向服务器发送的每一条报文为一个数据项，接口每写出的一条日志为一个数据项。

[97] 则在采集得到各数据项后，在隐私数据库中分别查找与各数据项匹配的隐私数据条目。若一数据项与一隐私数据条目中的一节数据相同，则判断此数据项与此隐私数据条目匹配，此数据项包含有隐私数据。以此类推，分别检测各数据项，得到各数据项的检测结果。

[98] 在得到各数据项的检测结果后，若至少有一个数据项包含隐私数据，也即隐私

数据库中至少包含一条与采集的数据项匹配的隐私数据条目，则可以判定当前采集得到的数据中包含隐私数据，由此可以确定当前接口输出的数据中携带有隐私数据，可能涉及隐私数据的泄露。

[99] 由于在应用软件运行的过程中接口可能输出多个数据项，则在采集得到应用软件运行过程中接口输出的全部数据项后，分别根据隐私数据库查找对应匹配的隐私数据条目，以实现对各数据项的自动化单独校验。并且，若隐私数据库中有与数据项匹配的隐私数据条目，则可以确定当前接口输出的数据涉及到隐私信息，避免了隐私泄露的误报、漏报。

[100] 同上，分别对采集得到的应用软件各接口输出的数据进行检测，判断各应用软件各接口输出的数据中是否包含有隐私数据。

[101] 步骤S30、若检测到所述采集得到的数据中包含隐私数据，则确定所述接口为泄露隐私数据的接口。

[102] 若检测到应用软件的一接口输出的数据中包含有隐私数据，则可以确定此接口为泄露隐私数据的接口，进一步地，可以对此接口进行标识，并记录此接口泄露的数据类型，以便对应用软件进行进一步地优化。

[103] 在本实施例中，在应用软件运行时，采集应用软件接口输出到终端外部和/或存储到终端本地的数据，由于是在应用软件动态运行过程中采集的数据，因此能够获取应用软件实际运行过程中输出的各项信息数据，使得采集的数据覆盖面更广，具有真实性、可靠性和完整性；然后，根据预先配置的隐私数据库，检测采集得到的各项数据中是否包含隐私数据，从而实现了对采集的数据中是否包含有隐私数据的自动化检测，由于是以记载了各项隐私数据的隐私数据库为依据的，因此，在对采集得到的数据进行检测时，避免了人工分析以经验为依据而导致的漏报、误报。若检测到采集得到的数据中包含隐私数据，则确定此接口为泄露隐私数据的接口，由此，可以获取应用软件中泄露隐私数据的各接口，完成对应用软件接口泄露隐私数据的检测。通过本实施例，结合动态数据采集和静态数据自动分析，不会遗漏应用软件接口输出的任何数据，保障了用于检测分析的数据的完整性，并且，避免隐私数据泄露接口的误报、漏报，大大提高了应用软件隐私泄露接口检测的效率，降低了人工成本。

[104] 进一步地，参照图3，本发明数据泄露接口检测方法第二实施例提供一种数据泄露接口检测方法，基于上述本发明数据泄露接口检测方法第一实施例，所述步骤S30之后，还包括：

[105] 步骤S40、根据所述采集得到的数据中所包含的隐私数据安全等级，对应配置所述接口的危险等级。

[106] 在分别检测各数据项是否包含隐私数据后，若仅检测到一个数据项包含隐私数据，则获取隐私数据库中与此数据项匹配的隐私数据条目，根据此匹配的隐私数据条目预设的安全等级，对应配置当前接口的危险等级。

[107] 例如，若此隐私数据条目为账户密码，对应的安全等级较高，为一级，则对应配置当前接口的危险等级为一级，亟需解决此账户泄露问题；若此隐私数据条目为聊天内容，对应的安全等级中等，为二级，则对应配置当前接口的危险等级为二级，从而使技术人员及时了解各泄露隐私的接口的危险性。

[108] 进一步地，在分别检测各数据项是否包含隐私数据后，若检测到多个数据项包含隐私数据，则分别获取隐私数据库中与此多个数据项匹配的隐私数据条目，获取各匹配的隐私数据条目预设的安全等级。

[109] 然后，根据各匹配的隐私数据条目中安全性级别最高的安全等级，对应配置当前接口的危险等级。例如，在当前采集得到数据中供检测到两个包含隐私数据的数据项：包含账户密码的数据项和包含聊天内容的数据项。其中，账户密码对应的安全等级较高，为一级，聊天内容对应的安全等级中等，为二级，则安全性级别最高的安全等级为一级，对应配置当前接口的危险等级为一级。

[110] 由此，实现了应用软件泄露隐私数据的接口的危险等级配置。

[111] 在本实施例中，若确定应用软件一接口为泄露隐私数据的接口，则根据采集得到此接口输出的数据中所包含的隐私数据的安全等级，对应配置此接口的危险等级，进一步可以形成针对此应用软件的隐私数据泄露评估报告，从而使技术人员及时了解应用软件的隐私数据泄露情况，以及泄露隐私数据的接口的危险性。

[112] 进一步地，参照图4，本发明数据泄露接口检测方法第三实施例提供一种数据泄露接口检测方法，基于上述本发明数据泄露接口检测方法第一实施例或第二

实施例（本实施例以上述本发明数据泄露接口检测方法第一实施例为例），所述步骤S10之前还包括：

[113] 步骤S50、基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到所述隐私数据库；

[114] 步骤S60、在所述应用软件运行时，向所述应用软件输入所述隐私数据。

[115] 在进行应用软件的隐私数据泄露检测时，首先需要配置用于判断应用软件接口是否泄露隐私数据的隐私数据库。

[116] 具体的，作为一种实施方式，根据预设的用于测试的各项隐私数据，配置对应的隐私数据条目。

[117] 在配置一项隐私数据对应的隐私数据条目时，需要将此项隐私数据转换为多种数据形式，不同数据形式的隐私数据可以在隐私数据条目中分节存储，便于后续数据项的匹配。

[118] 需要说明的是，在转换隐私数据的数据形式时，可以转换为明文、字符串、哈希值等多种形式，可根据实际需要灵活配置。转换的数据形式越多，更加能够减少隐私数据泄露的漏报。

[119] 在得到各项隐私数据对应的隐私数据条目后，将各隐私数据及对应的隐私数据条目配置到隐私数据库中。

[120] 在应用软件运行时，向应用软件输入预先配置的隐私数据，例如输入账户密码，模拟聊天会话输入聊天内容，模拟交易输入交易金额等等。

[121] 由此，在采集应用软件各接口输出到终端外部和/或存储到终端本地的全部数据后，可以根据隐私数据库，校验输入的隐私数据是否以各种形式被泄露。

[122] 在本实施例中，基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到隐私数据库；在应用软件运行时，向应用软件输入预设的隐私数据，从而在检测采集的数据时，可以准确地识别出经过数据形式转换的隐私数据，确定应用软件是否将隐私数据转换数据形式后输出，避免了隐私泄露接口的漏报。

[123] 进一步地，参照图5，本发明数据泄露接口检测方法第四实施例提供一种数据泄露接口检测方法，基于上述本发明数据泄露接口检测方法第一实施例、第二

实施例或第三实施例，所述步骤S10包括：

[124] 步骤S11、抓取所述接口输出的网络信息包，得到所述接口输出到终端外部的数据；

[125] 步骤S12、基于预先配置的插桩，采集所述接口输出的本地广播和日志，得到所述接口存储到终端本地的数据。

[126] 在应用软件运行时，需采集应用软件接口输出的全部数据，包括输出到终端外部和存储到终端本地的数据。

[127] 具体的，作为一种实施方式，若需要采集输出到终端外部的数据，则可以通过抓包的方式，抓取此接口通过网络发送的信息包，提取网路信息包中的数据，得到此接口输出到终端外部的数据。

[128] 当然，也可以通过插桩采集此接口通过网络发送的信息包。

[129] 作为另一种实施方式，若需要采集存储到终端本地的数据，则可以在接口上预先配置插桩，抓取接口输出的本地广播和写出的日志。

[130] 其中，由于本地广播可以被终端系统或终端中安装的其他应用软件收听，因此，存在隐私数据泄露风险，需要采集广播的数据内容进行检测；日志文件可能被终端系统或终端中安装的其他应用软件抓取、读取，因此，存在隐私数据泄露风险，需要采集广播的数据内容进行检测。

[131] 然后，提取本地广播和日志的数据内容，得到此接口存储到终端本地的数据。

[132] 当然，还可以通过插桩的方式，采集其他存储到终端本地的数据。

[133] 在本实施例中，通过抓取接口输出的网络信息包，可以得到接口输出到终端外部的数据；基于预先配置的插桩，可以采集接口输出的本地广播和日志，得到接口存储到终端本地的数据，由此，实现了对接口输出的全部数据的采集。

[134] 需要说明的是，本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[135] 进一步地，参照图6，本发明数据泄露接口检测装置第一实施例提供一种数据泄露接口检测装置，所述数据泄露接口检测装置包括：

[136] 采集模块10，用于在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据。

[137] 本发明通过采集应用软件运行过程中对外输出的数据，离线自动检测对外输出的数据中是否包含有隐私数据，无需人工手动检测，不依赖于人工的经验，可以全方位地自动排查应用软件的隐私泄露问题，避免漏报，提高应用软件的隐私泄露检测效率。

[138] 具体的，作为一种实施方式，启动应用软件，在应用软件运行的过程中，采集模块10通过插桩、抓包等多种形式，分别采集应用软件运行过程中各接口对外输出的全部数据。

[139] 需要说明的是，应用软件运行过程中接口对外输出的全部数据包括接口存储到终端本地的数据、以网络形式输出到终端外部的数据，例如：写的日志、打印的文件、发送给终端上部署的其他应用软件的数据等。

[140] 采集模块10在采集各接口输出的全部数据后，分别独立记录各接口输出的数据，以分别检测各接口输出的数据是否涉及到隐私数据的泄露。

[141] 检测模块20，用于根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据。

[142] 在采集得到应用软件接口输出的全部数据后，检测模块20根据预先配置的隐私数据库，检测采集得到的数据中是否包含有敏感的隐私数据。

[143] 其中，隐私数据库包括输入到应用软件的各项隐私数据以及应用软件生成的涉及用户隐私的数据，例如账户密码、聊天记录、交易记录等等。

[144] 并且，隐私数据库中记载的各项涉及用户隐私的数据，均对应有包括多种数据形式的隐私数据条目，例如账户密码对应的隐私数据条目，包括明文、哈希值、字符串等多种形式的账户密码。同一隐私数据条目中不同数据形式的隐私数据可以分节存储，从而提高了隐私数据监测的灵活性，以避免应用软件转换隐私数据的形式进行输出时，无法检测出变换数据形式后的隐私数据。

[145] 由此，在采集得到应用软件接口输出的全部数据后，检测模块20在隐私数据库中查找是否有与采集的数据匹配的隐私数据条目。若在隐私数据库中找到与采集的数据匹配的隐私数据条目，则确定应用软件接口输出的数据中包含有隐私

数据。

[146] 进一步地，作为一种实施方式，所述采集得到的数据中包括多个数据项，所述检测模块20还用于，

[147] 根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据；若检测得到至少有一个数据项包含隐私数据，则判定所述采集得到的数据中包含隐私数据。

[148] 需要说明的是，采集得到的应用软件接口输出的数据中包含多个数据项，例如接口通过网络向服务器发送的每一条报文为一个数据项，接口每写出的一条日志为一个数据项。

[149] 则在采集得到各数据项后，检测模块20在隐私数据库中分别查找与各数据项匹配的隐私数据条目。若一数据项与一隐私数据条目中的一节数据相同，则判断此数据项与此隐私数据条目匹配，此数据项包含有隐私数据。以此类推，检测模块20分别检测各数据项，得到各数据项的检测结果。

[150] 在得到各数据项的检测结果后，若至少有一个数据项包含隐私数据，也即隐私数据库中至少包含一条与采集的数据项匹配的隐私数据条目，则检测模块20可以判定当前采集得到的数据中包含隐私数据，由此可以确定当前接口输出的数据中携带有隐私数据，可能涉及隐私数据的泄露。

[151] 由于在应用软件运行的过程中接口可能输出多个数据项，则在采集得到应用软件运行过程中接口输出的全部数据项后，检测模块20分别根据隐私数据库查找对应匹配的隐私数据条目，以实现对各数据项的自动化单独校验。并且，若隐私数据库中有与数据项匹配的隐私数据条目，则可以确定当前接口输出的数据涉及到隐私信息，避免了隐私泄露的误报、漏报。

[152] 同上，检测模块20分别对采集得到的应用软件各接口输出的数据进行检测，判断各应用软件各接口输出的数据中是否包含有隐私数据。

[153] 确定模块30，用于若检测到所述采集得到的数据中包含隐私数据，则确定所述接口为泄露隐私数据的接口。

[154] 若检测到应用软件的一接口输出的数据中包含有隐私数据，则确定模块30可以确定此接口为泄露隐私数据的接口，进一步地，确定模块30可以对此接口进行

标识，并记录此接口泄露的数据类型，以便对应用软件进行进一步地优化。

[155] 在本实施例中，在应用软件运行时，采集模块10采集应用软件接口输出到终端外部和/或存储到终端本地的数据，由于是在应用软件动态运行过程中采集的数据，因此能够获取应用软件实际运行过程中输出的各项信息数据，使得采集的数据覆盖面更广，具有真实性、可靠性和完整性；然后，检测模块20根据预先配置的隐私数据库，检测采集得到的各项数据中是否包含隐私数据，从而实现了对采集的数据中是否包含有隐私数据的自动化检测，由于是以记载了各项隐私数据的隐私数据库为依据的，因此，在对采集得到的数据进行检测时，避免了人工分析以经验为依据而导致的漏报、误报。若检测到采集得到的数据中包含隐私数据，则确定模块30确定此接口为泄露隐私数据的接口，由此，可以获取应用软件中泄露隐私数据的各接口，完成对应用软件接口泄露隐私数据的检测。通过本实施例，结合动态数据采集和静态数据自动分析，不会遗漏应用软件接口输出的任何数据，保障了用于检测分析的数据的完整性，并且，避免隐私数据泄露接口的误报、漏报，大大提高了应用软件隐私泄露接口检测的效率，降低了人工成本。

[156] 进一步地，参照图7，本发明数据泄露接口检测装置第二实施例提供一种数据泄露接口检测装置，基于上述本发明数据泄露接口检测装置第一实施例，所述数据泄露接口检测装置还包括：

[157] 等级模块40，用于根据所述采集得到的数据中所包含的隐私数据的安全等级，对应配置所述接口的危险等级。

[158] 在分别检测各数据项是否包含隐私数据后，若仅检测到一个数据项包含隐私数据，则等级模块40获取隐私数据库中与此数据项匹配的隐私数据条目，根据此匹配的隐私数据条目预设的安全等级，对应配置当前接口的危险等级。

[159] 例如，若此隐私数据条目为账户密码，对应的安全等级较高，为一级，则等级模块40对应配置当前接口的危险等级为一级，亟需解决此账户泄露问题；若此隐私数据条目为聊天内容，对应的安全等级中等，为二级，则对应配置当前接口的危险等级为二级，从而使技术人员及时了解各泄露隐私的接口的危险性。

[160] 进一步地，在分别检测各数据项是否包含隐私数据后，若检测到多个数据项包

含隐私数据，则等级模块40分别获取隐私数据库中与此多个数据项匹配的隐私数据条目，获取各匹配的隐私数据条目预设的安全等级。

[161] 然后，等级模块40根据各匹配的隐私数据条目中安全性级别最高的安全等级，对应配置当前接口的危险等级。例如，在当前采集得到数据中供检测到两个包含隐私数据的数据项：包含账户密码的数据项和包含聊天内容的数据项。其中，账户密码对应的安全等级较高，为一级，聊天内容对应的安全等级中等，为二级，则安全性级别最高的安全等级为一级，对应配置当前接口的危险等级为一级。

[162] 由此，实现了应用软件泄露隐私数据的接口的危险等级配置。

[163] 在本实施例中，若确定应用软件一接口为泄露隐私数据的接口，则等级模块40根据采集得到此接口输出的数据中所包含的隐私数据的安全等级，对应配置此接口的危险等级，进一步可以形成针对此应用软件的隐私数据泄露评估报告，从而使技术人员及时了解应用软件的隐私数据泄露情况，以及泄露隐私数据的接口的危险性。

[164] 进一步地，参照图8，本发明数据泄露接口检测装置第三实施例提供一种数据泄露接口检测装置，基于上述本发明数据泄露接口检测装置第一实施例或第二实施例，所述数据泄露接口检测装置还包括：

[165] 配置模块50，用于基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到所述隐私数据库；

[166] 输入模块60，用于在所述应用软件运行时，向所述应用软件输入所述隐私数据。

[167] 在进行应用软件的隐私数据泄露检测时，配置模块50首先需要配置用于判断应用软件接口是否泄露隐私数据的隐私数据库。

[168] 具体的，作为一种实施方式，配置模块50根据预设的用于测试的各项隐私数据，配置对应的隐私数据条目。

[169] 在配置一项隐私数据对应的隐私数据条目时，配置模块50需要将此项隐私数据转换为多种数据形式，不同数据形式的隐私数据可以在隐私数据条目中分节存储，便于后续数据项的匹配。

[170] 需要说明的是，在转换隐私数据的数据形式时，可以转换为明文、字符串、哈希值等多种形式，可根据实际需要灵活配置。转换的数据形式越多，更加能够减少隐私数据泄露的漏报。

[171] 配置模块50在得到各项隐私数据对应的隐私数据条目后，将各隐私数据及对应的隐私数据条目配置到隐私数据库中。

[172] 在应用软件运行时，输入模块60向应用软件输入预先配置的隐私数据，例如输入账户密码，模拟聊天会话输入聊天内容，模拟交易输入交易金额等等。

[173] 由此，在采集应用软件各接口输出到终端外部和/或存储到终端本地的全部数据后，检测模块20可以根据隐私数据库，校验输入的隐私数据是否以各种形式被泄露。

[174] 在本实施例中，配置模块50基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到隐私数据库；在应用软件运行时，输入模块60向应用软件输入预设的隐私数据，从而在检测采集的数据时，可以准确地识别出经过数据形式转换的隐私数据，确定应用软件是否将隐私数据转换数据形式后输出，避免了隐私泄露接口的漏报。

[175] 进一步地，本发明数据泄露接口检测装置第四实施例提供一种数据泄露接口检测装置，基于上述本发明数据泄露接口检测装置第一实施例、第二实施例或第三实施例，所述采集模块10还用于，

[176] 抓取所述接口输出的网络信息包，得到所述接口输出到终端外部的数据；基于预先配置的插桩，采集所述接口输出的本地广播和日志，得到所述接口存储到终端本地的数据。

[177] 在应用软件运行时，采集模块10需采集应用软件接口输出的全部数据，包括输出到终端外部和存储到终端本地的数据。

[178] 具体的，作为一种实施方式，若需要采集输出到终端外部的数据，则采集模块10可以通过抓包的方式，抓取此接口通过网络发送的信息包，提取网路信息包中的数据，得到此接口输出到终端外部的数据。

[179] 当然，采集模块10也可以通过插桩采集此接口通过网络发送的信息包。

[180] 作为另一种实施方式，若需要采集存储到终端本地的数据，则采集模块10可以

在接口上预先配置插桩，抓取接口输出的本地广播和写出的日志。

[181] 其中，由于本地广播可以被终端系统或终端中安装的其他应用软件收听，因此，存在隐私数据泄露风险，需要采集广播的数据内容进行检测；日志文件可能被终端系统或终端中安装的其他应用软件抓取、读取，因此，存在隐私数据泄露风险，需要采集广播的数据内容进行检测。

[182] 然后，采集模块10提取本地广播和日志的数据内容，得到此接口存储到终端本地的数据。

[183] 当然，采集模块10还可以通过插桩的方式，采集其他存储到终端本地的数据。

[184] 在本实施例中，采集模块10通过抓取接口输出的网络信息包，可以得到接口输出到终端外部的数据；基于预先配置的插桩，可以采集接口输出的本地广播和日志，得到接口存储到终端本地的数据，由此，实现了对接口输出的全部数据的采集。

[185] 需要说明的是，在硬件实现上，以上采集模块10、检测模块20、确定模块30、等级模块40、配置模块50以及输入模块60等可以以硬件形式内嵌于或独立于数据泄露接口检测装置中，也可以以软件形式存储于数据泄露接口检测装置的存储器中，以便于处理器调用执行以上各个模块对应的操作。该处理器可以为中央处理单元（CPU)、微处理器、单片机等。

[186] 如图9所示，图9是本发明实施例方案涉及的硬件运行环境的设备结构示意图。

[187] 本发明实施例数据泄露接口检测设备可以是PC，也可以是智能手机、平板电脑、电子书阅读器、便携计算机等终端设备。

[188] 如图9所示，数据泄露接口检测设备可以包括：处理器1001，例如CPU，以及存储器1002。这些组件之间的连接通信可以通过通信总线实现。存储器1002可以是高速RAM存储器，也可以是稳定的存储器（non-volatile memory），例如磁盘存储器。存储器1002可选的还可以是独立于前述处理器1001的存储装置。

[189] 可选地，数据泄露接口检测设备还可以包括用户接口、网络接口、摄像头、RF（Radio Frequency，射频）电路，传感器、音频电路、WiFi模块等等。用户接口可以包括显示屏（Display）、输入单元比如键盘（Keyboard），可选用户接口还可以包括标准的有线接口、无线接口。网络接口可选的可以包括标准的有线

接口、无线接口（如WI-FI接口）。

[190] 本领域技术人员可以理解，图9中示出的数据泄露接口检测设备结构并不构成对数据泄露接口检测设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[191] 如图9所示，作为一种计算机存储介质的存储器1002中可以包括操作系统以及数据泄露接口检测程序。其中，操作系统是管理和控制数据泄露接口检测设备硬件与软件资源的程序，支持数据泄露接口检测程序以及其他程序或软件的运行。

[192] 在图9所示的数据泄露接口检测设备中，处理器1001可以用于执行存储器1002中存储的数据泄露接口检测程序，以实现以下步骤：

[193] 在应用软件运行时，采集所述应用软件接口输出到设备外部和/或存储到设备本地的数据；

[194] 根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据；

[195] 若检测到所述采集得到的数据中包含隐私数据，则确定所述应用软件接口为泄露隐私数据的接口。

[196] 进一步地，所述采集得到的数据中包括多个数据项，处理器1001还可以执行存储器1002中存储的数据泄露接口检测程序，以实现以下步骤：

[197] 根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据；

[198] 若检测得到至少有一个数据项包含隐私数据，则判定所述采集得到的数据中包含隐私数据。

[199] 进一步地，处理器1001还可以执行存储器1002中存储的数据泄露接口检测程序，以实现以下步骤：

[200] 根据所述采集得到的数据中所包含的隐私数据的安全等级，对应配置所述应用软件接口的危险等级。

[201] 进一步地，处理器1001还可以执行存储器1002中存储的数据泄露接口检测程序，以实现以下步骤：

[202] 基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到所述隐私数据库；

[203] 在所述应用软件运行时，向所述应用软件输入所述隐私数据。

[204] 进一步地，处理器1001还可以执行存储器1002中存储的数据泄露接口检测程序，以实现以下步骤：

[205] 抓取所述应用软件接口输出的网络信息包，得到所述应用软件接口输出到设备外部的数据；

[206] 基于预先配置的插桩，采集所述应用软件接口输出的本地广播和日志，得到所述应用软件接口存储到设备本地的数据。

[207] 本发明数据泄露接口检测设备的具体实施例与上述数据泄露接口检测方法和装置各实施例基本相同，在此不作赘述。

[208] 本发明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一个或者多个程序，所述一个或者多个程序可被一个或者多个处理器执行，以实现以下步骤：

[209] 在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据；

[210] 根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据；

[211] 若检测到所述采集得到的数据中包含隐私数据，则确定所述接口为泄露隐私数据的接口。

[212] 进一步地，所述采集得到的数据中包括多个数据项，所述一个或者多个程序可被所述一个或者多个处理器执行，还实现以下步骤：

[213] 根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据；

[214] 若检测得到至少有一个数据项包含隐私数据，则判定所述采集得到的数据中包含隐私数据。

[215] 进一步地，所述一个或者多个程序可被所述一个或者多个处理器执行，还实现以下步骤：

[216] 根据所述采集得到的数据中所包含的隐私数据的安全等级，对应配置所述接口的危险等级。

[217] 进一步地，所述一个或者多个程序可被所述一个或者多个处理器执行，还实现以下步骤：

[218] 基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到所述隐私数据库；

[219] 在所述应用软件运行时，向所述应用软件输入所述隐私数据。

[220] 进一步地，所述一个或者多个程序可被所述一个或者多个处理器执行，还实现以下步骤：

[221] 抓取所述接口输出的网络信息包，得到所述接口输出到终端外部的数据；

[222] 基于预先配置的插桩，采集所述接口输出的本地广播和日志，得到所述接口存储到终端本地的数据。

[223] 本发明计算机可读存储介质的具体实施例与上述数据泄露接口检测方法和装置各实施例基本相同，在此不作赘述。

[224] 还需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[225] 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。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上述实施例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。

[226] 以上仅为本发明的可选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

权利要求书

[权利要求 1] 一种数据泄露接口检测方法，其特征在于，所述数据泄露接口检测方法包括以下步骤：

在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据；

根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据；

若检测到所述采集得到的数据中包含隐私数据，则确定所述接口为泄露隐私数据的接口。

[权利要求 2] 如权利要求1所述的数据泄露接口检测方法，其特征在于，所述采集得到的数据中包括多个数据项，所述根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据的步骤包括：

根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据；

若检测得到至少有一个数据项包含隐私数据，则判定所述采集得到的数据中包含隐私数据。

[权利要求 3] 如权利要求1所述的数据泄露接口检测方法，其特征在于，所述确定所述接口为泄露隐私数据的接口的步骤之后，还包括：

根据所述采集得到的数据中所包含的隐私数据的安全等级，对应配置所述接口的危险等级。

[权利要求 4] 如权利要求1所述的数据泄露接口检测方法，其特征在于，所述采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据的步骤之前，还包括：

基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到所述隐私数据库；

在所述应用软件运行时，向所述应用软件输入所述隐私数据。

[权利要求 5] 如权利要求1所述的数据泄露接口检测方法，其特征在于，所述采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据的步骤包括：

抓取所述接口输出的网络信息包，得到所述接口输出到终端外部的数据；

基于预先配置的插桩，采集所述接口输出的本地广播和日志，得到所述接口存储到终端本地的数据。

[权利要求 6] 一种数据泄露接口检测装置，其特征在于，所述数据泄露接口检测装置包括：

采集模块，用于在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据；

检测模块，用于根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据；

确定模块，用于若检测到所述采集得到的数据中包含隐私数据，则确定所述接口为泄露隐私数据的接口。

[权利要求 7] 如权利要求6所述的数据泄露接口检测装置，其特征在于，所述采集得到的数据中包括多个数据项，所述检测模块还用于，

根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据；若检测得到至少有一个数据项包含隐私数据，则判定所述采集得到的数据中包含隐私数据。

[权利要求 8] 如权利要求6所述的数据泄露接口检测装置，其特征在于，所述数据泄露接口检测装置还包括：

等级模块，用于根据所述采集得到的数据中所包含的隐私数据的安全等级，对应配置所述接口的危险等级。

[权利要求 9] 如权利要求6所述的数据泄露接口检测装置，其特征在于，所述数据泄露接口检测装置还包括：

配置模块，用于基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到所述隐私数据库；

输入模块，用于在所述应用软件运行时，向所述应用软件输入所述隐私数据。

[权利要求 10] 如权利要求6所述的数据泄露接口检测装置，其特征在于，所述采集

模块还用于，

抓取所述接口输出的网络信息包，得到所述接口输出到终端外部的数据；基于预先配置的插桩，采集所述接口输出的本地广播和日志，得到所述接口存储到终端本地的数据。

[权利要求 11] 一种数据泄露接口检测设备，其特征在于，所述数据泄露接口检测设备包括处理器及存储器，所述存储器存储有数据泄露接口检测程序；所述处理器用于执行所述数据泄露接口检测程序，以实现以下步骤：

在应用软件运行时，采集所述应用软件接口输出到设备外部和/或存储到设备本地的数据；

根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据；

若检测到所述采集得到的数据中包含隐私数据，则确定所述应用软件接口为泄露隐私数据的接口。

[权利要求 12] 如权利要求11所述的数据泄露接口检测设备，其特征在于，所述采集得到的数据中包括多个数据项，所述处理器还用于执行所述数据泄露接口检测程序，以实现以下步骤：

根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据；

若检测得到至少有一个数据项包含隐私数据，则判定所述采集得到的数据中包含隐私数据。

[权利要求 13] 如权利要求11所述的数据泄露接口检测设备，其特征在于，所述处理器还用于执行所述数据泄露接口检测程序，以实现以下步骤：

根据所述采集得到的数据中所包含的隐私数据的安全等级，对应配置所述应用软件接口的危险等级。

[权利要求 14] 如权利要求11所述的数据泄露接口检测设备，其特征在于，所述处理器还用于执行所述数据泄露接口检测程序，以实现以下步骤：

基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到所述隐私数据库；

在所述应用软件运行时，向所述应用软件输入所述隐私数据。

[权利要求 15] 如权利要求11所述的数据泄露接口检测设备，其特征在于，所述处理器还用于执行所述数据泄露接口检测程序，以实现以下步骤：

抓取所述应用软件接口输出的网络信息包，得到所述应用软件接口输出到设备外部的数据；

基于预先配置的插桩，采集所述应用软件接口输出的本地广播和日志，得到所述应用软件接口存储到设备本地的数据。

[权利要求 16] 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有一个或者多个程序，所述一个或者多个程序可被一个或者多个处理器执行，以实现以下步骤：

在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据；

根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据；

若检测到所述采集得到的数据中包含隐私数据，则确定所述接口为泄露隐私数据的接口。

[权利要求 17] 如权利要求16所述的计算机可读存储介质，其特征在于，所述采集得到的数据中包括多个数据项，所述一个或者多个程序可被所述一个或者多个处理器执行，还实现以下步骤：

根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据；

若检测得到至少有一个数据项包含隐私数据，则判定所述采集得到的数据中包含隐私数据。

[权利要求 18] 如权利要求16所述的计算机可读存储介质，其特征在于，所述一个或者多个程序可被所述一个或者多个处理器执行，还实现以下步骤：

根据所述采集得到的数据中所包含的隐私数据的安全等级，对应配置所述接口的危险等级。

[权利要求 19] 如权利要求16所述的计算机可读存储介质，其特征在于，所述一个或者多个程序可被所述一个或者多个处理器执行，还实现以下步骤：

基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得

到所述隐私数据库；

在所述应用软件运行时，向所述应用软件输入所述隐私数据。

[权利要求 20] 如权利要求16所述的计算机可读存储介质，其特征在于，所述一个或者多个程序可被所述一个或者多个处理器执行，还实现以下步骤：

抓取所述接口输出的网络信息包，得到所述接口输出到终端外部的数据；

基于预先配置的插桩，采集所述接口输出的本地广播和日志，得到所述接口存储到终端本地的数据。

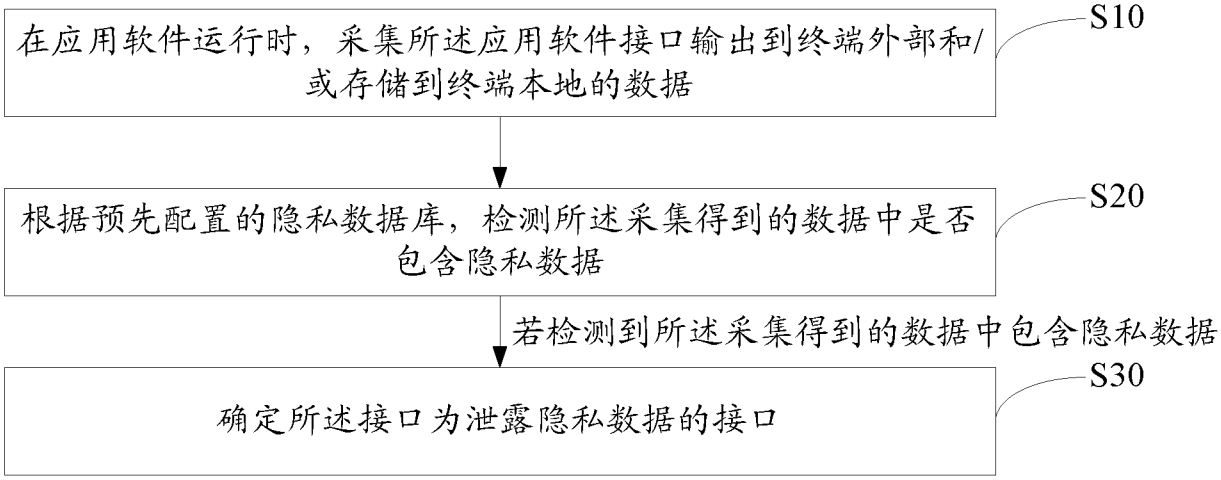
在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据
S10
根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据
S20
若检测到所述采集得到的数据中包含隐私数据
确定所述接口为泄露隐私数据的接口
S30

图 1

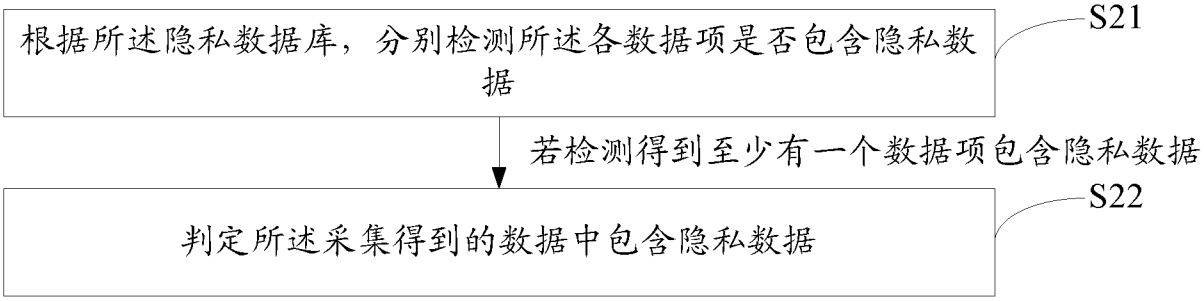
根据所述隐私数据库，分别检测所述各数据项是否包含隐私数据
S21
若检测得到至少有一个数据项包含隐私数据
判定所述采集得到的数据中包含隐私数据
S22

图 2

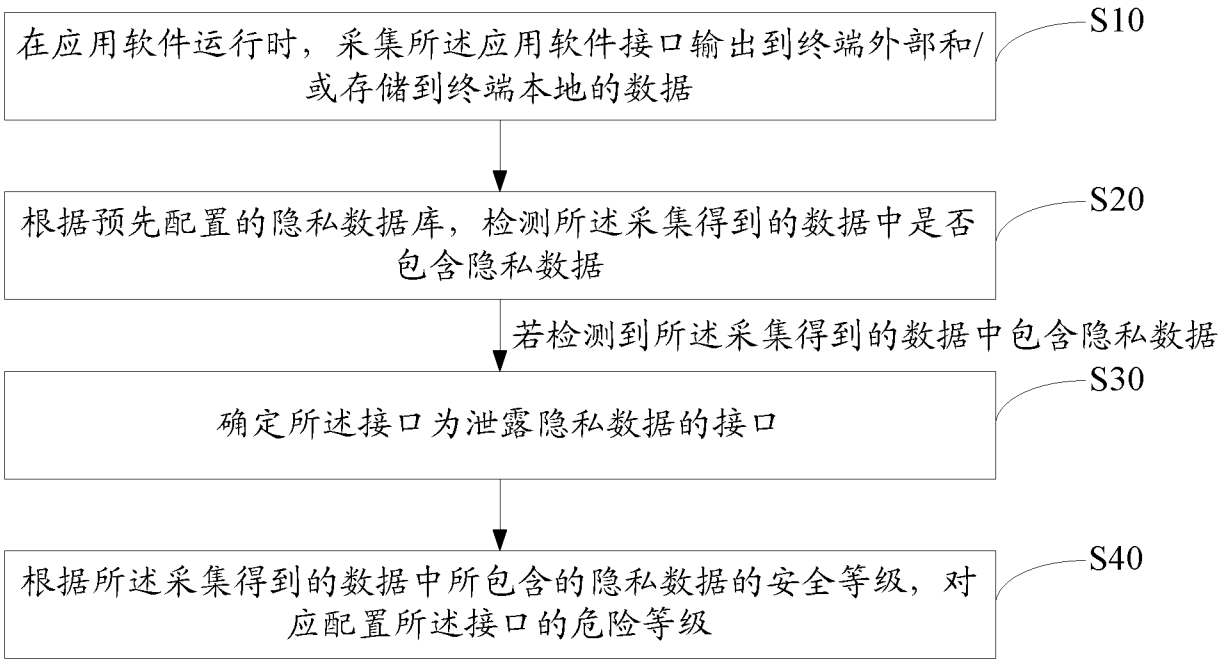
在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据
S10
根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据
S20
若检测到所述采集得到的数据中包含隐私数据
确定所述接口为泄露隐私数据的接口
S30
根据所述采集得到的数据中所包含的隐私数据的安全等级，对应配置所述接口的危险等级
S40

图 3

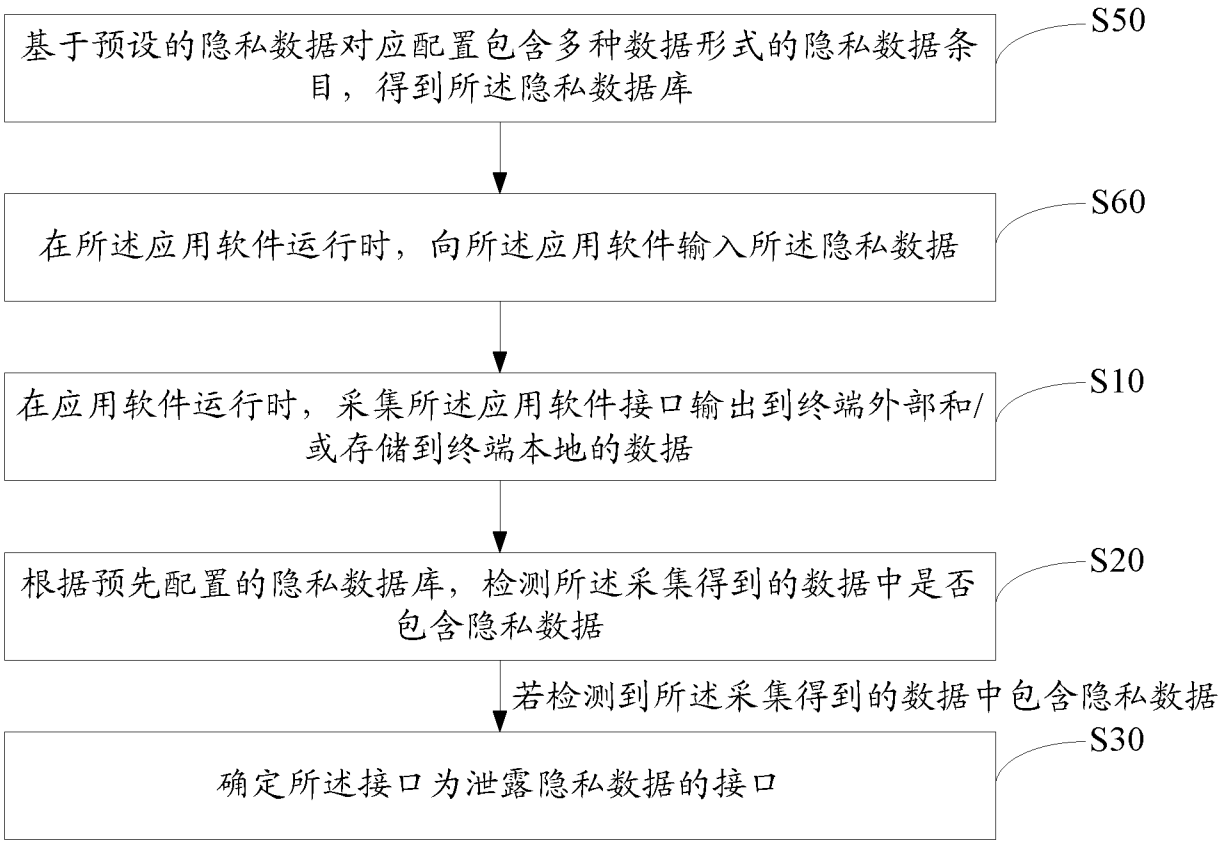
基于预设的隐私数据对应配置包含多种数据形式的隐私数据条目，得到所述隐私数据库
S50
在所述应用软件运行时，向所述应用软件输入所述隐私数据
S60
在应用软件运行时，采集所述应用软件接口输出到终端外部和/或存储到终端本地的数据
S10
根据预先配置的隐私数据库，检测所述采集得到的数据中是否包含隐私数据
S20
若检测到所述采集得到的数据中包含隐私数据
确定所述接口为泄露隐私数据的接口
S30

图 4

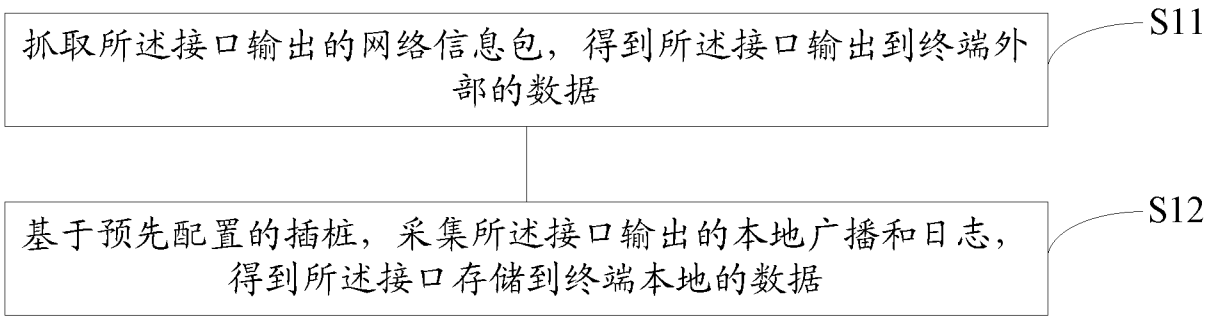
抓取所述接口输出的网络信息包，得到所述接口输出到终端外部的数据
S11
基于预先配置的插桩，采集所述接口输出的本地广播和日志，得到所述接口存储到终端本地的数据
S12

图 5

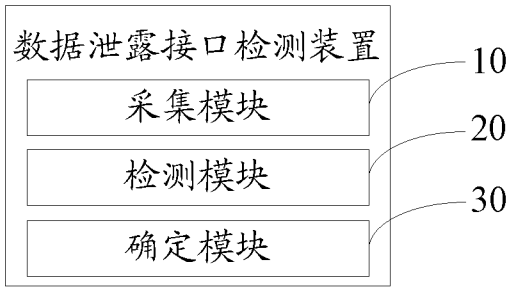
数据泄露接口检测装置
采集模块
检测模块
确定模块
10
20
30

图 6

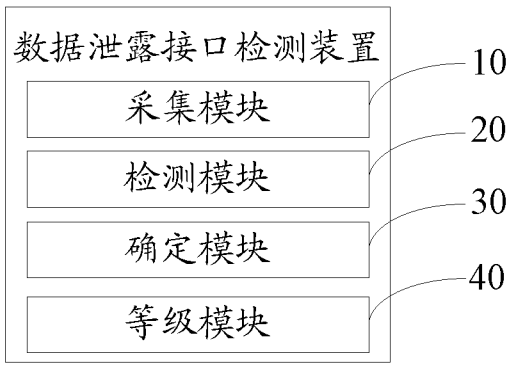
数据泄露接口检测装置
采集模块
检测模块
确定模块
等级模块
10
20
30
40

图 7

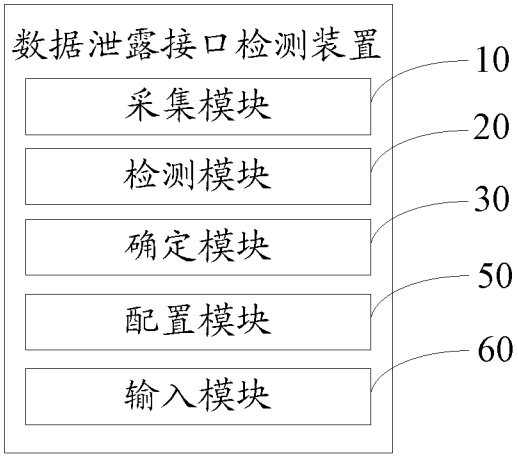
数据泄露接口检测装置
采集模块
检测模块
确定模块
配置模块
输入模块
10
20
30
50
60

图 8

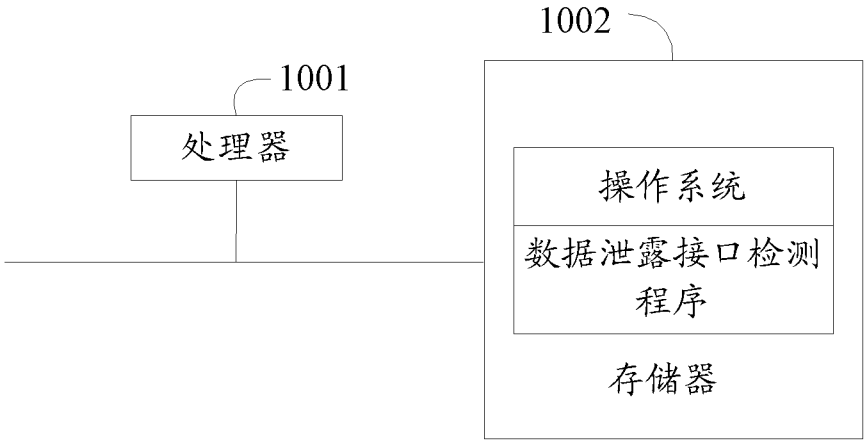
1002
1001
处理器
操作系统
数据泄露接口检测程序
存储器

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/077985

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/52 (2013.01) 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)

CNPAT, CNKI, WPI, EPODOC, IEEE: detect, leak, intimacy, privacy, 探测, 检测, 泄露, 接口, 数据, 隐私

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103729595 A (SOUTHEAST UNIVERSITY), 16 April 2014 (16.04.2014), claims 1-5	1-20
A	CN 103984900 A (NANJING CYBERPEACE TECHNOLOGY CO., LTD. et al.), 13 August 2014 (13.08.2014), entire document	1-20
A	CN 103309808 A (INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES et al.), 18 September 2013 (18.09.2013), entire document	1-20
A	CN 103327183 A (INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES), 25 September 2013 (25.09.2013), entire document	1-20
A	US 2015227746 A1 (NORTHWESTERN UNIVERSITY), 13 August 2015 (13.08.2015), 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	Date of mailing of the international search report
13 June 2017	30 June 2017
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 LI, Dong Telephone No. (86-10) 62414436

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/077985

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103729595 A	16 April 2014	None	
CN 103984900 A	13 August 2014	None	
CN 103309808 A	18 September 2013	WO 2014198171 A1	18 December 2014
CN 103327183 A	25 September 2013	None	
US 2015227746 A1	13 August 2015	None	

国际检索报告

国际申请号
PCT/CN2017/077985

A. 主题的分类

G06F 21/52(2013.01)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））

CNPAT,CNKI,WPI,EPODOC,IEEE:detect，leak，intimacy，privacy，探测，检测，泄露，接口，数据，隐私

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
X	CN 103729595 A (东南大学) 2014年 4月 16日 (2014-04-16) 权利要求1-5	1-20
A	CN 103984900 A (南京赛宁信息技术有限公司 等) 2014年 8月 13日 (2014-08-13) 全文	1-20
A	CN 103309808 A (中国科学院信息工程研究所 等) 2013年 9月 18日 (2013-09-18) 全文	1-20
A	CN 103327183 A (中国科学院信息工程研究所) 2013年 9月 25日 (2013-09-25) 全文	1-20
A	US 2015227746 A1 (NORTHWESTERN UNIVERSITY) 2015年 8月 13日 (2015-08-13) 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	国际检索报告邮寄日期
2017年 6月 13日	2017年 6月 30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	受权官员 李东 电话号码 (86-10)62414436

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/077985

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 103729595 A	2014年 4月 16日	无	
CN 103984900 A	2014年 8月 13日	无	
CN 103309808 A	2013年 9月 18日	WO 2014198171 A1	2014年 12月 18日
CN 103327183 A	2013年 9月 25日	无	
US 2015227746 A1	2015年 8月 13日	无	