

(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
2024 年 12 月 19 日 (19.12.2024)



(10) 国际公布号
WO 2024/255583 A1

- (51) 国际专利分类号:
G06F 21/60 (2013.01)
- (21) 国际申请号: PCT/CN2024/095704
- (22) 国际申请日: 2024 年 5 月 28 日 (28.05.2024)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202310707303.6 2023年6月14日 (14.06.2023) CN
- (71) 申请人: 深圳 **TCL** 新技术有限公司
(**SHENZHEN TCL NEW TECHNOLOGY CO., LTD.**)
[CN/CN]; 中国广东省深圳市南山区西丽街道中山园路 1001 号国际 E 城 D4 栋 9 楼,
Guangdong 518052 (CN)。
- (72) 发明人: 罗康(**LUO, Kang**); 中国广东省深圳市南山区西丽街道中山园路 1001 号国际 E 城 D4 栋 9 楼,
Guangdong 518052 (CN)。黎明德(**LI, Mingde**); 中国广东省深圳市南山区西丽街道中山园路 1001 号
国际 E 城 D4 栋 9 楼, Guangdong 518052 (CN)。

- (74) 代理人: 深圳紫藤知识产权代理有限公司 (**PURPLEVINE INTELLECTUAL PROPERTY (SHENZHEN) CO., LTD.**); 中国广东省深圳市前海深港合作区南山街道听海大道 5059 号前海鸿荣源中心 A 座 2401, Guangdong 518000 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, MK, MT, NL, NO,

(54) **Title:** DEVICE PRIVACY MANAGEMENT METHOD AND APPARATUS, ELECTRONIC DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 设备隐私管理方法、装置、电子设备及存储介质

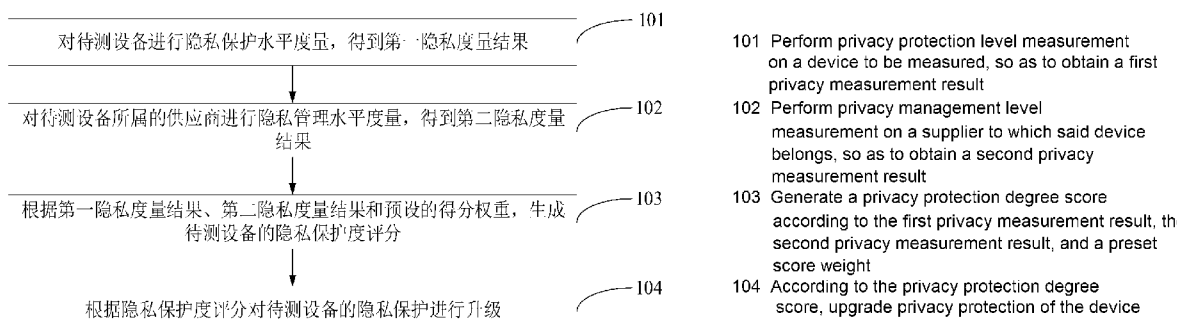


图 2

(57) **Abstract:** Embodiments of the present application disclose a device privacy management method. The method comprises: performing privacy protection level measurement on a device to be measured, so as to obtain a first privacy measurement result; performing privacy management level measurement on a supplier to which said device belongs, so as to obtain a second privacy measurement result; generating a privacy protection degree score according to the first privacy measurement result, the second privacy measurement result, and a preset score weight; and upgrading privacy protection of the device. Thus, privacy security and protection management is implemented.

(57) **摘要:** 本申请实施例公开了一种设备隐私管理方法, 包括: 对待测设备进行隐私保护水平度量, 得到第一隐私度量结果; 对待测设备所属的供应商进行隐私管理水平度量, 得到第二隐私度量结果; 根据第一隐私度量结果、第二隐私度量结果和预设的得分权重, 生成隐私保护度评分; 对待测设备的隐私保护进行升级。实现隐私安全保护管理。

[见续页]

WO 2024/255583 A1

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))。

设备隐私管理方法、装置、电子设备及存储介质

本申请要求申请日为 2023 年 06 月 14 日、申请号为 202310707303.6、申请名称为“设备隐私管理方法、装置、电子设备及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请实施例涉及计算机技术领域，具体涉及一种设备隐私管理方法、装置、电子设备及存储介质，其中，存储介质包括计算机可读存储介质。

背景技术

随着全球隐私保护立法越来越多和执法越来越严格，企业面临着越来越大的隐私保护方面的压力。智能家居发展速度加快，大量智能家电进入千家万户，它的安全与隐私保护得到了广泛关注。

技术问题

目前，很多产品的用户数据隐私保护还主要仅针对在产品本身，使得难以准确衡量产品的隐私保护情况，无法对产品进行隐私安全保护管理。

技术方案

本申请实施例提供一种设备隐私管理方法、装置、电子设备及存储介质，可以提升产品隐私保护衡量结果的准确性。

第一方面，本申请实施例提供了一种设备隐私管理方法，包括：

对待测设备进行隐私保护水平度量，得到第一隐私度量结果；

对所述待测设备所属的供应商进行隐私管理水平度量，得到第二隐私度量结果；

根据所述第一隐私度量结果、所述第二隐私度量结果和预设的得分权重，生成所述待测设备的隐私保护度评分；

根据所述隐私保护度评分对所述待测设备的隐私保护进行升级。

第二方面，本申请实施例还提供了一种设备隐私管理装置，包括：

第一度量模块，用于对待测设备进行隐私保护水平度量，得到第一隐私度量结果；

第二度量模块，用于对所述待测设备所属的供应商进行隐私管理水平度量，得到第二隐私度量结果；

评分生成模块，用于根据所述第一隐私度量结果、所述第二隐私度量结果和预设的得分权重，生成所述待测设备的隐私保护度评分；

隐私管理模块，用于根据所述隐私保护度评分对所述待测设备的隐私保护进行升级。

其中，在本申请的一些实施例中，第一度量模块包括：

获取单元，用于获取待测设备在隐私保护项的隐私安全得分；

第一生成单元，用于根据所述隐私保护项对应的得分权重以及所述隐私保护项对应的所述隐私安全得分生成第一隐私度量结果；

所述隐私保护项包括产品合规风险测试项、产品隐私安全保护技术测试项、产品适配法律测试项或产品隐私保护要求度测试项中的至少一种。

其中，在本申请的一些实施例中，若所述隐私保护项为产品合规风险测试项，获取单元包括：

配置子单元，用于配置合规风险测试用例；

测试子单元，用于根据所述合规风险测试用例对待测设备进行测试，得到合规风险测试结果，所述合规风险测试结果对应一风险等级得分；

第一计算子单元,用于计算各个合规风险测试用例对应的风险等级得分的平均值,得到平均风险等级得分;

第一生成子单元,用于将所述平均风险等级得分作为所述待测设备在所述产品合规风险测试项的隐私安全得分。

其中,在本申请的一些实施例中,若所述隐私保护项为产品隐私安全保护技术测试项,获取单元包括:

第一确定子单元,用于确定待测设备支持的隐私安全保护技术项;

第二确定子单元,用于针对每个隐私安全保护技术项,确定所述隐私安全保护技术项所应用的隐私安全保护技术的类型、强度以及数量;

获取子单元,用于获取预设映射关系集合,所述预设映射关系集合包括预设的隐私安全保护技术的类型、强度以及数量和安全评分的映射关系;

第三确定子单元,用于根据所述预设映射关系集合,根据所述隐私安全保护技术项应用的隐私安全保护技术的类型、强度或者数量确定安全评分;

第二计算子单元,用于计算各个隐私安全保护技术项的安全评分的平均值,得到平均安全评分;

第二生成子单元,用于将所述平均安全评分作为所述待测设备在所述产品隐私安全保护技术测试项的隐私安全得分。

其中,在本申请的一些实施例中,若所述隐私保护项为产品适配法律测试项,获取单元包括:

区域确定子单元,用于确定待测设备待上线的目标区域;

基线确定子单元,用于确定所述目标区域所需满足的目标法律基线;

得分确定子单元,用于根据所述待测设备当前满足的实际法律基线和所述目标法律基线,确定所述待测设备的隐私安全得分。

其中,在本申请的一些实施例中,第二度量模块包括:

供应商确定单元,用于确定所述待测设备所属的供应商;

管理水平确定单元,用于根据参考隐私信息管理体系和隐私成熟度模型对所述供应商的隐私管理水平进行度量,得到隐私管理水平得分;

第一匹配单元,用于将参考软件安全开发生命周期与所述待测设备的实际软件安全开发生命周期进行匹配,得到第一匹配结果;

第二匹配单元,用于将参考研发隐私保护设计流程与所述待测设备的实际研发隐私保护设计流程进行匹配,得到第二匹配结果;

研发水平确定单元,用于根据所述第一匹配结果和所述第二匹配结果得到研发设计隐私管控得分;

第二生成单元,用于根据所述隐私管理水平得分和所研发设计隐私管控得分,生成第二隐私度量结果。

其中,在本申请的一些实施例中,隐私管理模块包括:

保护技术确定单元,用于若所述隐私保护度评分不满足评分阈值,则确定待测设备的隐私保护项对应的当前隐私保护技术;

保护技术变更单元,用于变更所述当前隐私保护技术,得到目标隐私保护技术;

度量结果更新单元,用于基于所述目标隐私保护技术重新度量得到更新后第一隐私度量结果;

评分更新单元,用于将更新后第一隐私度量结果与第一得分权重相乘得到第一保护度得分,将第二隐私度量结果与第二得分权重相乘得到第二保护度得分,将第一保护度得分和第二保护度得分相加,得到更新后隐私保护度评分;

隐私管理单元,用于根据所述更新后隐私保护度评分对所述待测设备的隐私保护进行升级。

第三方面,本申请实施例还提供了一种电子设备,电子设备包括存储器、处理器及存储在存

存储器中并可在处理器上运行的计算机程序,处理器执行计算机程序时实现上述第一方面中的设备隐私管理方法中的步骤或者实现上述第三方面中的设备隐私管理方法中的步骤。

第四方面,本申请实施例还提供了一种存储介质,该存储介质包括计算机可读存储介质,计算机可读存储介质上存储有计算机程序,计算机程序被处理器执行时实现上述的设备隐私管理方法中的步骤。

第五方面,本申请实施例还提供了一种计算机程序产品或计算机程序,该计算机程序产品或计算机程序包括计算机指令,该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令,处理器执行该计算机指令,使得该计算机设备执行本申请实施例所述的各种可选实现方式中提供的方法。

有益效果

本申请实施例对待测设备进行隐私保护水平度量,得到第一隐私度量结果,对所述待测设备所属的供应商进行隐私管理水平度量,得到第二隐私度量结果,根据所述第一隐私度量结果和所述第二隐私度量结果,生成所述待测设备的隐私保护度评分,根据所述隐私保护度评分对所述待测设备的隐私保护进行升级。其中,通过对供应商的隐私管理水平进行度量得到第二隐私度量结果,并根据该第二隐私度量结果以及针对产品本身的隐私的第一隐私度量结果生成待测设备的隐私保护度评分,相较于传统的仅针对产品本身的隐私水平的评估方案,本申请实施例丰富了产品隐私保护的衡量维度,提升产品隐私保护衡量结果的准确性,便于实现对产品的隐私安全保护管理。

附图说明

为了更清楚地说明本申请中的技术方案,下面将对实施例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。

图1是本申请实施例提供的设备隐私管理方法的场景示意图;

图2是本申请实施例提供的设备隐私管理方法的流程示意图;

图3是本申请实施例提供的各个隐私安全保护技术项及其对应的安全评分的结果示意图;

图4是本申请实施例提供的设备隐私管理的架构示意图;

图5是本申请实施例提供的设备隐私管理方法的另一示意图;

图6是本申请实施例提供的设备隐私管理装置的结构示意图;

图7是本申请实施例提供的电子设备的结构示意图。

本发明的实施方式

下面将结合本申请中的附图,对本申请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,本领域技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

本申请实施例提供一种设备隐私管理方法、装置、电子设备及存储介质。具体地,本申请实施例提供适用于电子设备的设备隐私管理装置,其中,电子设备包括终端,其中,终端包括但不限于手机、平板电脑、计算机或者电视等设备。

请参阅图1,以终端设备执行设备隐私管理方法为例,其中,设备隐私管理方法的具体执行过程如下:

服务器10获取待测设备11的配置参数信息,根据该配置参数信息对该待测设备11进行隐私保护水平度量,得到第一隐私度量结果;

随后,服务器 10 获取该待测设备的供应商信息,以并对该供应商的隐私管理水平进行度量,得到第二隐私度量结果;

然后,根据第一隐私度量结果和第二隐私度量结果生成隐私保护度评分,根据该隐私保护度评分对待测设备的隐私保护进行升级。

可以理解的是,通过对供应商的隐私管理水平进行度量得到第二隐私度量结果,并根据该第二隐私度量结果以及针对产品本身的隐私的第一隐私度量结果生成待测设备的隐私保护度评分,相较于传统的仅针对产品本身的隐私水平的评估方案,本申请实施例丰富了产品隐私保护的衡量维度,提升产品隐私保护衡量结果的准确性,便于实现对产品的隐私安全保护管理。

以下分别进行详细说明。需说明的是,以下实施例的描述顺序不作为对实施例优先顺序的限定。

请参阅图 2,图 2 是本申请实施例提供的设备隐私管理方法的流程示意图。该设备隐私管理方法的具体流程可以如下:

101、对待测设备进行隐私保护水平度量,得到第一隐私度量结果。

需要说明的是,设备的隐私保护水平指该设备在应用时对用户数据的隐私保护水平,由设备在应用时设备的相关配置参数决定,即,第一隐私度量结果是针对设备本身而言得到的评估结果。

其中,待测设备指需要进行隐私保护评估的设备,例如,生产后出厂的设备、研发测试所用的设备或者应用过程中存在隐私安全问题而需要进行测试的设备等。

102、对所述待测设备所属的供应商进行隐私管理水平度量,得到第二隐私度量结果。

需要说明的是,供应商的隐私管理水平指该供应商隐私保护的控制水平,其中,该供应商为开发或者生产该设备的企业。

可以理解的是,通过对生产该设备的企业针对隐私管理水平的度量,可以从更多维度分析设备的隐私保护水平,例如,该企业的隐私保护的控制水平越高,则相应的产品的隐私保护水平也通常较高。

103、根据所述第一隐私度量结果、所述第二隐私度量结果和预设的得分权重,生成所述待测设备的隐私保护度评分。

可以理解的是,隐私保护度评分是针对设备在用户数据隐私保护方面的评分,该评分越高,则说明该设备或者该产品的隐私保护越好,反之,评分越低,则说明该设备或者该产品的隐私保护越差。

可以理解的是,通过从多个维度的度量结果生成隐私保护度评分,实现从多个维度对设备隐私保护情况进行度量、以及评分,提升隐私保护度评分的准确性。

其中,得分权重反映每个隐私度量结果对应的得分的占比情况,例如,在本申请实施例中,第一隐私度量结果和第二隐私度量结果的得分权重各占 50%。其中,在本申请实施例中,得分权重可以根据实际需要进行灵活调整,在此对得分权重的具体数值不做限定。

104、根据所述隐私保护度评分对所述待测设备的隐私保护进行升级。

其中,通过得到设备的隐私保护度评分,则可以根据该隐私保护度评分对设备进行隐私保护升级,例如,若设备的隐私保护度评分较低,则需要通过调整设备在隐私保护方面的技术、强度等方式来提升设备的隐私保护度评分。

相应的,根据该隐私保护度评分也可以判断是否允许相应的设备引入,例如,当设备的隐私保护度评分较低时,则拒绝该设备的引入,当设备的隐私保护度评分达到标准时,才允许该设备引入,其中,设备引入也称设备引进,指设备购入或者进口设备等。

可以理解的是,通过对供应商的隐私管理水平进行度量得到第二隐私度量结果,并根据该第二隐私度量结果以及针对产品本身的隐私的第一隐私度量结果生成待测设备的隐私保护度

评分,相较于传统的仅针对产品本身的隐私水平的评估方案,本申请实施例丰富了产品隐私保护的衡量维度,提升产品隐私保护衡量结果的准确性,便于实现对产品的隐私安全保护管理。

可选的,在本申请实施例中,第一隐私度量结果是针对设备在应用过程中隐私评分情况,因此,通过得到待测设备在各个隐私保护项的隐私安全得分,便可以得到该待测设备的第一隐私度量结果,即,可选的,在本申请的一些实施例中,步骤“对待测设备进行隐私保护水平度量,得到第一隐私度量结果”,包括:

获取待测设备在隐私保护项的隐私安全得分;

根据所述隐私保护项对应的得分权重以及所述隐私保护项对应的所述隐私安全得分生成第一隐私度量结果;

所述隐私保护项包括产品合规风险测试项、产品隐私安全保护技术测试项、产品适配法律测试项或产品隐私保护要求度测试项中的至少一种。

需要说明的是,隐私保护项是待测设备主要针对的几个检测项,该几个检测项从不同的维度实现对设备隐私安全的检测。

其中,通过各个检测项的隐私安全得分综合得到设备在应用过程中的动态的第一隐私度量结果。

相应的,得分权重反映每个隐私保护项的得分占比情况,例如,当隐私保护项为四个时,则各个隐私保护项的得分权重可以分别为 25%。其中,该得分权重的具体数值也可以根据实际需要进行灵活调整。

需要说明的是,产品合规风险测试项是针对设备是否合规风险的检测,在该过程中,可以构建测试用例,基于测试用例对设备进行测试,以获取到针对合规风险的测试结果,即,可选的,在本申请的一些实施例中,若所述隐私保护项为产品合规风险测试项,步骤“获取待测设备在隐私保护项的隐私安全得分”,包括:

配置合规风险测试用例;

根据所述合规风险测试用例对待测设备进行测试,得到合规风险测试结果,所述合规风险测试结果对应一风险等级得分;

计算各个合规风险测试用例对应的风险等级得分的平均值,得到平均风险等级得分;

将所述平均风险等级得分作为所述待测设备在所述产品合规风险测试项的隐私安全得分。

可以理解的是,合规风险测试用例是针对待测设备在产品合规风险测试方面建立的测试用例,基于该测试用例的执行,获取待测设备在产品合规方面的风险情况。其中,合规风险测试用例中包括所针对的待测试项目以及相关的测试文件及测试输入数据等。

合规风险测试用例可以包括多条,每条测试用例分别对应一个测试结果,测试结果可以用得分表示,得分 0-5 之间,不同的得分对应不同的风险等级,例如,严重: 0 分;高危: 1 分;

中危: 2 分;低危: 4 分;无风险(通过): 5 分。

相应的,针对设备的产品合规风险测试项的隐私安全得分,可以由多个测试用例的合规风险

测试结果来综合得到,例如,合规风险检测的隐私安全得分 = $\frac{\sum_{i=1}^N L_i}{N}$ (L_i 表示第 i 条测试用例的测试结果得分),其中, N 为测试用例的数量或者条数,即以多个合规风险测试用例的测试结果得分的均值来表示该产品合规风险测试项的隐私安全得分。

需要说明的是,产品隐私安全保护技术测试项是针对设备配置的隐私安全保护技术的测试,可以从应用的隐私安全保护技术的类型、强度或者数量多少等角度来对设备的产品隐私安全保护技术进行评分,即,可选的,在本申请的一些实施例中,若所述隐私保护项为产品隐私安全保护技术测试项,步骤“获取待测设备在隐私保护项的隐私安全得分”,包括:

确定待测设备支持的隐私安全保护技术项；

针对每个隐私安全保护技术项，确定所述隐私安全保护技术项所应用的隐私安全保护技术的类型、强度以及数量；

获取预设映射关系集合，所述预设映射关系集合包括预设的隐私安全保护技术的类型、强度以及数量和安全评分的映射关系；

根据所述预设映射关系集合，根据所述隐私安全保护技术项应用的隐私安全保护技术的类型、强度或者数量确定安全评分；

计算各个隐私安全保护技术项的安全评分的平均值，得到平均安全评分；

将所述平均安全评分作为所述待测设备在所述产品隐私安全保护技术测试项的隐私安全得分。

需要说明的是，隐私安全保护技术项是设备为达到隐私安全的目的而采用的保护技术项目，例如，请参阅图 3，图 3 是本申请实施例提供的各个隐私安全保护技术项及其对应的安全评分的结果示意图，其中，隐私安全保护技术项包括数据加密、数据备份和回复、安全套接层协议传输数据、云端采用的安全产品、接口认证授权、数据脱敏、匿名算法、差分隐私等技术项，相应的，针对每个隐私安全保护技术项，根据该隐私安全保护技术项所应用到的保护技术的类型、强度或者数量等确定相应的隐私安全保护技术项的安全评分。

例如，保护技术的类型越安全，保护强度越高，以及保护技术的数量越多，对应的安全评分越高。具体的，在本申请实施例中，可以根据隐私安全保护技术的类型、强度、数量和安全评分之间预先建立的映射关系，来得到当前的各个隐私安全保护技术项的安全评分，进而根据各个安全评分的均值，得到待测设备针对该产品隐私安全保护技术测试项的隐私安全得分。相应的，针对产品隐私安全保护技术测试项的隐私安全得分，也可以由该产品隐私安全保护技术测试项对应的多个隐私安全保护技术项的安全评分来综合得到，例如，产品隐私安全保

护技术评分 = $\frac{\sum_{i=1}^N L_i}{N}$ (L_i 表示第 i 条隐私安全保护技术项的安全得分)。

需要说明的是，产品适配法律测试项是针对设备是否满足相应国家或者区域的法律需求，针对该法律需求进行的隐私安全测试，例如，产品所使用的法律是否满足相应地区的隐私安全法律基线等，即，可选的，在本申请的一些实施例中，若所述隐私保护项为产品适配法律测试项，步骤“获取待测设备在隐私保护项的隐私安全得分”，包括：

确定待测设备待上线的目标区域；

确定所述目标区域所需满足的目标法律基线；

根据所述待测设备当前满足的实际法律基线和所述目标法律基线，确定所述待测设备的隐私安全得分。

可以理解的，法律基线是法律对应的基准，即设备所满足的法律要求，如，本申请实施例中，法律基线主要指设备在隐私法方面所对应的隐私法律要求。根据设备当前适用的实际法律基线与上线区域的目标法律基线的比较，可以得到该设备在产品适配法律测试项的隐私安全得分。例如，如 A 国的隐私法要求比较低或者没有隐私法，但是产品采取的隐私保护措施已超出了 A 国法律要求，则评分为 5 分；B 国的隐私法要求特别高，但是产品未采取的隐私保护措施，则评分为 0 分。

可选的，在本申请实施例中，还可以根据产品的类型来确定该设备需要满足的隐私保护要求度，即，每种产品类型对应的隐私保护要求度不同，相应的，若隐私保护项为产品隐私保护要求度测试项，则“获取待测设备在隐私保护项的隐私安全得分”包括：

确定待测设备的产品类型；

根据该产品类型和映射关系，确定该待测设备对应的产品隐私保护要求度；

将所述产品隐私保护要求度作为所述待测设备针对所述产品类型方面的隐私安全得分。

其中，该映射关系包括预设的产品类型与预设的产品隐私保护要求度之间的映射关系。

可以理解的是，该映射关系可以根据不同产品的数据隐私要求保护程度进行预定义，例如，智能灯光控制、智能窗帘、智能抽油烟机、蓝牙温湿度传感器对应的产品隐私保护要求度为 1，智能空调、智能冰箱（不带屏幕）、智能洗衣机、智能空气净化器、智能新风系统和蓝牙体脂称的产品隐私保护要求度为 2，智能扫地机器人（不带摄像头）和智能冰箱（带屏幕）的产品隐私保护要求度为 3，智能电视和智能网关的产品隐私保护要求度为 4，智能门锁、智能摄像头、智能门铃、智能猫眼、智能扫地机器人（带摄像头）、智能手表和智能手机的产品隐私保护要求度为 5 等。

需要说明的是，第二隐私度量结果是针对研发或者设计该设备的企业的隐私管理水平以及该企业研发设计流程进行的评分结果，而企业的隐私管理水平以及该企业研发设计流程的评分结果在一定程度上反映研发出的设备的隐私保护情况，例如，若企业的隐私管理水平较高，且研发设计流程的评分结果为设计流程较规范，则对应研发出的设备的隐私保护和规范也相应会更高，因此，可以将该企业的评估结果作为相应设备隐私保护的参考，即，可选的，在本申请的一些实施例中，步骤“对所述待测设备所属的供应商进行隐私管理水平度量，得到第二隐私度量结果”，包括：

确定所述待测设备所属的供应商；

根据参考隐私信息管理体系和隐私成熟度模型对所述供应商的隐私管理水平进行度量，得到隐私管理水平得分；

将参考软件安全开发生命周期与所述待测设备的实际软件安全开发生命周期进行匹配，得到第一匹配结果；

将参考研发隐私保护设计流程与所述待测设备的实际研发隐私保护设计流程进行匹配，得到第二匹配结果；

根据所述第一匹配结果和所述第二匹配结果得到研发设计隐私管控得分；

根据所述隐私管理水平得分和所研发设计隐私管控得分，生成第二隐私度量结果。

其中，匹配结果反映匹配程度，可以用百分比或者 0-1 之间的小数进行表示，例如，第一匹配结果的百分比较高则说明两个生命周期较为接近或者一致，第一匹配结果的百分比较低则说明两个生命周期相似性较低；又例如，第二匹配结果的百分比比较高则说明隐私保护设计流程较为接近或者一致，反之，第二匹配结果的百分比比较低则说明两个隐私保护设计流程基本不同或者重合性较低。其中，用百分比的方式反映两个比较对象之间的匹配程度。

相应的，第一匹配结果和第二匹配结果也可以通过权重占比的方式计算得到研发设计隐私管控得分，例如，将两个匹配结果对应的百分比分别与权重占比相乘后相加得到最终的研发设计隐私管控得分。

可以理解的是，隐私管理水平得分反映的是企业针对隐私管理的水平，研发设计隐私管控得分反映的是企业针对设备在研发时的隐私管控得分。

其中，软件安全开发生命周期：（SSDLC，Software security development life cycle）和隐私保护设计流程（PbD，Privacy by Design）具有相应的参考标准，通过判断该企业是否满足相应的标准，来判断该企业的研发设计隐私管控得分。

相应的，针对隐私管理水平得分，可以通过企业是否满足相关的隐私信息管理体系，以及还可以通过隐私成熟度模型来分析企业的隐私管理水平，例如，根据 ISO27701 隐私管理体系对公司整体隐私管理水平进行评估后得出管理体系评估分数；根据经典隐私成熟度模型如 ISC2、NIST、GAPP、CNIL 对公司整体隐私管理水平进行模型评估分数。

相应的，针对研发设计隐私管控得分，可以通过设备研发的生命周期以及隐私保护设计流程等方面来分析设备的隐私保护得分，例如，对公司研发软件安全开发生命周期（SSDLC）水

平进行评估，得出研发周期评估分数；对公司研发隐私保护设计流程（PbD）水平进行评估，得出隐私设计流程评估分数。

相应的，在得到各个检测项的评分后，可以通过各个检测项的权重将各个评分进行融合，得到隐私保护度评分，例如，请参阅图 4，图 4 是本申请实施例提供的设备隐私管理的架构示意图，其中，该设备隐私管理的架构包括静态度量模块 A、动态度量模块 B 和结果可视化模块 C，其中，静态度量模块 A 用于对研发或者设计该待测设备的企业的隐私管理水平的评估，动态度量模块 B 用于对待测设备在应用过程中的动态隐私数据进行评估，结果可视化模块 C 用于将静态度量模块 A 和动态度量模块 B 融合得到的隐私保护度评分进行可视化展示。其中，在本申请实施例中，静态度量模块 A 和动态度量模块 B 的融合权重各占 50%；

相应的，针对静态度量模块 A，静态度量模块 A 又包括公司内控度量部分 a1 和研发管控度量部分 a2，各占 50%，公司内控度量部分 a1 包括隐私信息管理体系测试部分 a11 和隐私成熟度模型测试部分 a12，其中，隐私信息管理体系测试部分 a11 的管理体系评估分数占公司内控度量部分 a1 的 80%，隐私成熟度模型测试部分 a12 的模型评估分数占公司内控度量部分 a1 的 20%。

例如，静态度量模块 A 的第二隐私度量结果 St 为： $(\text{管理体系评估分数} \times 0.8 + \text{模型评估分数} \times 0.2) \times 0.5 + \text{研发管控度量得分} \times 0.5$ 。

相应的，针对动态度量模块 B，该动态度量模块 B 包括产品合规风险测试项 b1、产品隐私安全保护技术测试项 b2、产品适配法律测试项 b3 或产品隐私保护要求度测试项 b4，其中，各个测试项的融合权重分别占动态度量模块 B 的 40%、40%、10% 和 10%。

例如，动态度量模块 B 的第一隐私度量结果 Dy 为： $\text{合规风险检测评分} \times 0.4 + \text{产品隐私安全保护技术评分} \times 0.4 + \text{法律适配度} \times 0.1 + 1/\text{选择产品类型隐私保护要求强度} \times 0.1$ 。

可选的，在根据隐私保护度评分对待测设备的隐私保护进行升级时，则可以通过调整待测设备的隐私保护数据，来得到新的隐私保护度评分，根据新的隐私保护度评分的变化情况，来确定适合该待测设备的隐私保护数据，即，可选的，在本申请的一些实施例中，步骤“根据所述隐私保护度评分对所述待测设备的隐私保护进行升级”，包括：

确定待测设备的隐私保护项对应的当前隐私保护技术；

变更所述当前隐私保护技术，得到目标隐私保护技术；

根据所述目标隐私保护技术更新所述第一隐私度量结果，得到更新后第一隐私度量结果；

根据所述更新后第一隐私度量结果和所述第二隐私度量结果，得到更新后隐私保护度评分；

根据所述更新后隐私保护度评分对所述待测设备的隐私保护进行升级。

其中，通过选择或添加其他隐私保护技术，查看不同的隐私保护技术对应产品隐私保护分数的影响，看看是否达到了上线国家的隐私保护要求。

可以理解的是，本申请实施例通过静态度量、动态度量以及结果可视化的形式实现对设备隐私安全保护评估流程的工程化配置，基于该流程可以实现对各个设备的隐私安全保护评估。基于该评估流程对设备进行隐私安全评估，可降低对操作人员的专业技能要求，降低应用成本，从企业和设备本身等多个维度实现对设备的隐私安全评估，能更加全面了解产品隐私缺陷，在动态度量部分，还可以通过调整各个隐私保护项所应用的隐私保护技术来得到不同的隐私保护度评分，实现根据成本采取不同的措施，来判断隐私保护的程度以及是否满足当地法律法规要求。

相应的，在对设备进行隐私安全评估后，可以通过对设备进行相应的隐私安全改进，进而得到隐私保护效果较好的设备，当用户使用该设备进行通信或者应用时，则可以较好的保护用户的数据，提升隐私安全性。

请参阅图 5，图 5 是本申请实施例提供的设备隐私管理的另一方法流程图，其中，该设备隐私管理的具体流程包括：

201、启动隐私保护管理系统；

先启动静态度量部分：

202、是否更新公司内控度量，若选择，则执行步骤 203；

其中，该公司内控度量通常每年更新，不需要每次都更新。且每年中该公司内控度量值基本不变，因此，若未选择更新，则延用历史的公司内控度量结果即可。

203、根据 ISO27701 隐私管理体系对公司整体隐私管理水平进行评估，得出管理体系评估分数；

204、根据经典隐私成熟度模型对公司整体隐私管理水平进行评估分数，得到模型评估分数；其中，隐私成熟度模型包括 ISC2、NIST、GAPP、CNIL。

205、是否更新研发管控制度量，若是，则执行步骤 206；

其中，该研发管控制度量通常每年更新，不需要每次都更新；且每年中该研发管控制度量值基本不变，因此，若未选择更新，则延用历史的研发管控制度量结果即可。

206、对公司研发软件安全开发生命周期（SSDLC）水平进行评估，得出研发周期评估分数；

207、对公司研发隐私保护设计流程（PbD）水平进行评估，得出隐私设计流程评估分数；

启动动态度量部分：

208、选择智能家居产品上线国家的法律，确定针对法律适配的法律隐私安全得分；

209、选择待评估的智能家居产品类型，得到产品隐私保护要求程度得分；

其中，根据产品类型与产品隐私保护要求度之间的对应关系确定当前产品类型对应的产品隐私保护要求程度得分。

210、选择待评估的智能家居产品类型目前采用的隐私安全保护技术或待采用的隐私安全保护技术，得到隐私安全技术安全评分；

其中，根据预先建立的隐私安全保护技术的类型、强度、数量和安全评分之间的映射关系，得到当前的智能家居的隐私安全技术安全评分。

211、对智能家居产品进行合规风险检测，得到合规风险隐私安全得分；

其中，可以通过自动检测的方式检测智能产品存在的风险，并得出分数；例如，配置并执行合规风险测试用例，将各个合规风险测试用例的得分进行平均处理，得到智能家居在合规风险检测方面的隐私安全得分。

212、将管理体系评估分数、模型评估分数、研发周期评估分数和隐私设计流程评估分数、法律隐私安全得分、产品隐私保护要求程度得分、隐私安全技术安全评分和合规风险隐私安全得分，进行加权、计算最终分数，得到隐私保护度评分；

例如，隐私保护度评分=[（管理体系评估分数*0.8+模型评估分数*0.2）*0.5+（研发周期评估分数*0.5+隐私设计流程评估分数*0.5）*0.5]*0.5+[合规风险隐私安全得分*0.4+隐私安全技术安全评分*0.4+法律隐私安全得分*0.1+产品隐私保护要求程度得分*0.1]*0.5。

213、显示智能家居隐私保护度评分，以及各维度评分、可提升的隐私保护项；

其中，可提升的隐私保护项指评分较低的隐私保护项。

214、根据可提升的隐私保护项，选择是否重新计算当前评估分数，重复步骤 208-213，直至没有可提升的隐私保护项。

可以理解的是，本申请实施例结合了多种隐私保护评估方法和安全开发流程，能更加全面了解产品隐私缺陷。可根据成本采取不同的措施，来判断隐私保护的程度以及是否满足当地法律法规要求。

为便于更好的实施本申请的设备隐私管理方法，本申请还提供一种基于上述设备隐私管理方法的设备隐私管理装置。其中第三目标词语的含义与上述设备隐私管理方法中相同，具体实现细节可以参考方法实施例中的说明。

请参阅图 6，图 6 是本申请实施例提供的设备隐私管理装置的结构示意图，其中，该设备隐

私管理装置可以包括：

第一度量模块 301，用于对待测设备进行隐私保护水平度量，得到第一隐私度量结果；
第二度量模块 302，用于对所述待测设备所属的供应商进行隐私管理水平度量，得到第二隐私度量结果；

评分生成模块 303，用于根据所述第一隐私度量结果、所述第二隐私度量结果和预设的得分权重，生成所述待测设备的隐私保护度评分；

隐私管理模块 304，用于根据所述隐私保护度评分对所述待测设备的隐私保护进行升级。

其中，在本申请的一些实施例中，第一度量模块 301 包括：

获取单元，用于获取待测设备在隐私保护项的隐私安全得分；

第一生成单元，用于根据所述隐私保护项对应的得分分子权重以及所述隐私保护项对应的所述隐私安全得分生成第一隐私度量结果；

所述隐私保护项包括产品合规风险测试项、产品隐私安全保护技术测试项、产品适配法律测试项或产品隐私保护要求度测试项中的至少一种。

其中，在本申请的一些实施例中，若所述隐私保护项为产品合规风险测试项，获取单元包括：

配置子单元，用于配置合规风险测试用例；

测试子单元，用于根据所述合规风险测试用例对待测设备进行测试，得到合规风险测试结果，所述合规风险测试结果对应一风险等级得分；

第一计算子单元，用于计算各个合规风险测试用例对应的风险等级得分的平均值，得到平均风险等级得分；

第一生成子单元，用于将所述平均风险等级得分作为所述待测设备在所述产品合规风险测试项的隐私安全得分。

其中，在本申请的一些实施例中，若所述隐私保护项为产品隐私安全保护技术测试项，获取单元包括：

第一确定子单元，用于确定待测设备支持的隐私安全保护技术项；

第二确定子单元，用于针对每个隐私安全保护技术项，确定所述隐私安全保护技术项所应用的隐私安全保护技术的类型、强度以及数量；

获取子单元，用于获取预设映射关系集合，所述预设映射关系集合包括预设的隐私安全保护技术的类型、强度以及数量和安全评分的映射关系；

第三确定子单元，用于根据所述预设映射关系集合，根据所述隐私安全保护技术项应用的隐私安全保护技术的类型、强度或者数量确定安全评分；

第二计算子单元，用于计算各个隐私安全保护技术项的安全评分的平均值，得到平均安全评分；

第二生成子单元，用于将所述平均安全评分作为所述待测设备在所述产品隐私安全保护技术测试项的隐私安全得分。

其中，在本申请的一些实施例中，若所述隐私保护项为产品适配法律测试项，获取单元包括：

区域确定子单元，用于确定待测设备待上线的目标区域；

基线确定子单元，用于确定所述目标区域所需满足的目标法律基线；

得分确定子单元，用于根据所述待测设备当前满足的实际法律基线和所述目标法律基线，确定所述待测设备的隐私安全得分。

其中，在本申请的一些实施例中，第二度量模块 302 包括：

供应商确定单元，用于确定所述待测设备所属的供应商；

管理水平确定单元，用于根据参考隐私信息管理体系和隐私成熟度模型对所述供应商的隐私管理水平进行度量，得到隐私管理水平得分；

第一匹配单元，用于将参考软件安全开发生命周期与所述待测设备的实际软件安全开发生命

周期进行匹配,得到第一匹配结果;

第二匹配单元,用于将参考研发隐私保护设计流程与所述待测设备的实际研发隐私保护设计流程进行匹配,得到第二匹配结果;

研发水平确定单元,用于根据所述第一匹配结果和所述第二匹配结果得到研发设计隐私管控得分;

第二生成单元,用于根据所述隐私管理水平得分和所研发设计隐私管控得分,生成第二隐私度量结果。

其中,在本申请的一些实施例中,隐私管理模块 304 包括:

保护技术确定单元,用于若所述隐私保护度评分不满足评分阈值,则确定待测设备的隐私保护项对应的当前隐私保护技术;

保护技术变更单元,用于变更所述当前隐私保护技术,得到目标隐私保护技术;

度量结果更新单元,用于基于所述目标隐私保护技术重新度量得到更新后第一隐私度量结果;

评分更新单元,用于将更新后第一隐私度量结果与第一得分权重相乘得到第一保护度得分,将第二隐私度量结果与第二得分权重相乘得到第二保护度得分,将第一保护度得分和第二保护度得分相加,得到更新后隐私保护度评分;

隐私管理单元,用于根据所述更新后隐私保护度评分对所述待测设备的隐私保护进行升级。

其中,在本申请实施例首先由第一度量模块 301 对待测设备进行隐私保护水平度量,得到第一隐私度量结果,接着,由第二度量模块 302 对所述待测设备所属的供应商进行隐私管理水平度量,得到第二隐私度量结果,随后,由评分生成模块 303 根据所述第一隐私度量结果、所述第二隐私度量结果和预设的得分权重,生成所述待测设备的隐私保护度评分,然后,由隐私管理模块 304 根据所述隐私保护度评分对所述待测设备的隐私保护进行升级。

其中,本申请实施例通过对供应商的隐私管理水平进行度量得到第二隐私度量结果,并根据该第二隐私度量结果以及针对产品本身的隐私的第一隐私度量结果生成待测设备的隐私保护度评分,相较于传统的仅针对产品本身的隐私水平的评估方案,本申请实施例丰富了产品隐私保护的衡量维度,提升产品隐私保护衡量结果的准确性,便于实现对产品的隐私安全保护管理。

此外,本申请还提供一种电子设备,如图 7 所示,其示出了本申请所涉及的电子设备的结构示意图,具体来讲:

该电子设备可以包括一个或者一个以上处理核心的处理器 401、一个或一个以上计算机可读存储介质的存储器 402、电源 403 和输入单元 404 等部件。本领域技术人员可以理解,图 7 中示出的电子设备结构并不构成对电子设备的限定,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。其中:

处理器 401 是该电子设备的控制中心,利用各种接口和线路连接整个电子设备的各个部分,通过运行或执行存储在存储器 402 内的软件程序和/或模块,以及调用存储在存储器 402 内的数据,执行电子设备的各种功能和处理数据。可选的,处理器 401 可包括一个或多个处理核心;优选的,处理器 401 可集成应用处理器和调制解调处理器,其中,应用处理器主要处理操作系统、对象界面和应用程序等,调制解调处理器主要处理无线通信。可以理解的是,上述调制解调处理器也可以不集成到处理器 401 中。

存储器 402 可用于存储软件程序以及模块,处理器 401 通过运行存储在存储器 402 的软件程序以及模块,从而执行各种功能应用以及设备隐私管理。存储器 402 可主要包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能等)等;存储数据区可存储根据电子设备的使用所创建的数据等。此外,存储器 402 可以包括高速随机存取存储器,还可以包括非易失性存储器,例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地,存储器 402 还可以

包括存储器控制器，以提供处理器 401 对存储器 402 的访问。

电子设备还包括给各个部件供电的电源 403，优选的，电源 403 可以通过电源管理系统与处理器 401 逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源 403 还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。

该电子设备还可包括输入单元 404，该输入单元 404 可用于接收输入的数字或字符信息，以及产生与对象设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。

尽管未示出，电子设备还可以包括显示单元等，在此不再赘述。具体在本实施例中，电子设备中的处理器 401 会按照如下的指令，将一个或一个以上的应用程序的进程对应的可执行文件加载到存储器 402 中，并由处理器 401 来运行存储在存储器 402 中的应用程序，从而实现本申请所提供的任一种设备隐私管理方法中的步骤。

对待测设备进行隐私保护水平度量，得到第一隐私度量结果，对所述待测设备所属的供应商进行隐私管理水平度量，得到第二隐私度量结果，根据所述第一隐私度量结果、所述第二隐私度量结果和预设的得分权重，生成所述待测设备的隐私保护度评分，根据所述隐私保护度评分对所述待测设备的隐私保护进行升级。其中，通过对供应商的隐私管理水平进行度量得到第二隐私度量结果，并根据该第二隐私度量结果以及针对产品本身的隐私的第一隐私度量结果生成待测设备的隐私保护度评分，相较于传统的仅针对产品本身的隐私水平的评估方案，本申请实施例丰富了产品隐私保护的衡量维度，提升产品隐私保护衡量结果的准确性，便于实现对产品的隐私安全保护管理。

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可以通过指令来完成，或通过指令控制相关的硬件来完成，该指令可以存储于一计算机可读存储介质中，并由处理器进行加载和执行。

为此，本申请提供一种存储介质，该存储介质包括计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序能够被处理器进行加载，以执行本申请所提供的任一种设备隐私管理方法中的步骤。

其中，该计算机可读存储介质可以包括：只读存储器（ROM，Read Only Memory）、随机存取记忆体（RAM，Random Access Memory）、磁盘或光盘等。

由于该计算机可读存储介质中所存储的指令，可以执行本申请所提供的任一种设备隐私管理方法中的步骤，因此，可以实现本申请所提供的任一种设备隐私管理方法所能实现的有益效果，详见前面的实施例，在此不再赘述。

以上对本申请所提供的一种设备隐私管理方法、装置、电子设备以及存储介质进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上，本说明书内容不应理解为对本发明的限制。

其中，可以理解的是，在本申请的具体实施方式中，涉及到待测设备的配置数据（合规风险数据、适配法律数据、隐私安全保护技术、产品类型等），以及该待测设备对应的企业的相关信息（企业的名称、企业的隐私管理水平，包括管理隐私的水平和研发该设备的生命周期和相应的隐私设计流程）等相关的数据，当本申请以上实施例运用到具体产品或技术中时，需要获得用户许可或者同意，且相关数据的收集、使用和处理需要遵守相关国家和地区的相关法律法规和标准。

权利要求书

1、一种设备隐私管理方法，其中，包括：

对待测设备进行隐私保护水平度量，得到第一隐私度量结果；

对所述待测设备所属的供应商进行隐私管理水平度量，得到第二隐私度量结果；

根据所述第一隐私度量结果、所述第二隐私度量结果和预设的得分权重，生成所述待测设备的隐私保护度评分；

根据所述隐私保护度评分对所述待测设备的隐私保护进行升级。

2、根据权利要求 1 所述的方法，其中，所述对待测设备进行隐私保护水平度量，得到第一隐私度量结果，包括：

获取待测设备在隐私保护项的隐私安全得分；

根据所述隐私保护项对应的得分权重以及所述隐私保护项对应的所述隐私安全得分生成第一隐私度量结果；

所述隐私保护项包括产品合规风险测试项、产品隐私安全保护技术测试项、产品适配法律测试项或产品隐私保护要求度测试项中的至少一种。

3、根据权利要求 2 所述的方法，其中，若所述隐私保护项为产品合规风险测试项，所述获取待测设备在隐私保护项的隐私安全得分，包括：

配置合规风险测试用例；

根据所述合规风险测试用例对待测设备进行测试，得到合规风险测试结果，所述合规风险测试结果对应一风险等级得分；

计算各个合规风险测试用例对应的风险等级得分的平均值，得到平均风险等级得分；

将所述平均风险等级得分作为所述待测设备在所述产品合规风险测试项的隐私安全得分。

4、根据权利要求 2 所述的方法，其中，若所述隐私保护项为产品隐私安全保护技术测试项，所述获取待测设备在隐私保护项的隐私安全得分，包括：

确定待测设备支持的隐私安全保护技术项；

针对每个隐私安全保护技术项，确定所述隐私安全保护技术项所应用的隐私安全保护技术的类型、强度以及数量；

获取预设映射关系集合，所述预设映射关系集合包括预设的隐私安全保护技术的类型、强度以及数量和安全评分的映射关系；

根据所述预设映射关系集合，根据所述隐私安全保护技术项应用的隐私安全保护技术的类型、强度或者数量确定安全评分；

计算各个隐私安全保护技术项的安全评分的平均值，得到平均安全评分；

将所述平均安全评分作为所述待测设备在所述产品隐私安全保护技术测试项的隐私安全得分。

5、根据权利要求 2 所述的方法，其中，若所述隐私保护项为产品适配法律测试项，所述获取待测设备在隐私保护项的隐私安全得分，包括：

确定待测设备待上线的目标区域；

确定所述目标区域所需满足的目标法律基线；

根据所述待测设备当前满足的实际法律基线和所述目标法律基线，确定所述待测设备的隐私安全得分。

6、根据权利要求 1 所述的方法，其中，所述对所述待测设备所属的供应商进行隐私管理水平度量，得到第二隐私度量结果，包括：

确定所述待测设备所属的供应商；

根据参考隐私信息管理体系和隐私成熟度模型对所述供应商的隐私管理水平进行度量，得到隐私管理水平得分；

将参考软件安全开发生命周期与所述待测设备的实际软件安全开发生命周期进行匹配，得到第一匹配结果；

将参考研发隐私保护设计流程与所述待测设备的实际研发隐私保护设计流程进行匹配，得到第二匹配结果；

根据所述第一匹配结果和所述第二匹配结果得到研发设计隐私管控得分；

根据所述隐私管理水平得分和所研发设计隐私管控得分，生成第二隐私度量结果。

7、根据权利要求 2 所述的方法，其中，所述根据所述隐私保护度评分对所述待测设备的隐私保护进行升级，包括：

若所述隐私保护度评分不满足评分阈值，则确定待测设备的隐私保护项对应的当前隐私保护技术；

变更所述当前隐私保护技术，得到目标隐私保护技术；

基于所述目标隐私保护技术重新度量得到更新后第一隐私度量结果；

根据所述更新后第一隐私度量结果和所述第二隐私度量结果，得到更新后隐私保护度评分；

根据所述更新后隐私保护度评分对所述待测设备的隐私保护进行升级。

8、根据权利要求 7 所述的方法，其中，所述根据所述更新后第一隐私度量结果和所述第二隐私度量结果，得到更新后隐私保护度评分，包括：

将更新后第一隐私度量结果与第一得分权重相乘得到第一保护度得分；

将第二隐私度量结果与第二得分权重相乘得到第二保护度得分；

将第一保护度得分和第二保护度得分相加，得到更新后隐私保护度评分。

9、根据权利要求 2 所述的方法，其中，所述获取待测设备在隐私保护项的隐私安全得分，包括：

确定待测设备的产品类型；

根据该产品类型和映射关系，确定该待测设备对应的产品隐私保护要求度；

将所述产品隐私保护要求度作为所述待测设备针对所述产品类型方面的隐私安全得分。

10、根据权利要求 1 所述的方法，其中，所述隐私保护水平是所述设备在使用时对用户数据的隐私保护水平，由所述设备在使用时所述设备的相关配置参数决定；

所述隐私管理水平指所述供应商隐私保护的控制水平，其中，所述供应商为开发或者生产所述设备的企业。

11、根据权利要求 1 所述的方法，其中，所述预设的得分权重包括针对第一隐私度量结果的第一得分权重和针对所述第二隐私度量结果的第二得分权重，所述第一得分权重和所述第二得分权重分别包括 50%。

12、根据权利要求 4 所述的方法，其中，所述隐私安全保护技术项包括数据加密、数据备份和回复、安全套接层协议传输数据、云端采用的安全产品、接口认证授权、数据脱敏、匿名算法、差分隐私中的至少一种。

13、根据权利要求 6 所述的方法，其中，所述根据所述第一匹配结果和所述第二匹配结果得到研发设计隐私管控得分，包括：

将所述第一匹配结果对应的第一百分比和所述第二匹配结果对应的第二百分比，按照权重数据运算后得到研发设计隐私管控得分。

14、根据权利要求 6 所述的方法，其中，所述参考隐私信息管理体系包括 ISO27701，所述隐私成熟度模型包括 ISC2、NIST、GAPP、CNIL 中的至少一种。

15、一种设备隐私管理装置，其中，包括：

第一度量模块，用于对待测设备进行隐私保护水平度量，得到第一隐私度量结果；

第二度量模块，用于对所述待测设备所属的供应商进行隐私管理水平度量，得到第二隐私度量结果；

评分生成模块，用于根据所述第一隐私度量结果、所述第二隐私度量结果和预设的得分权重，生成所述待测设备的隐私保护度评分；

隐私管理模块，用于根据所述隐私保护度评分对所述待测设备的隐私保护进行升级。

16、根据权利要求 15 所述的装置，其中，所述第一度量模块包括：

获取单元，用于获取待测设备在隐私保护项的隐私安全得分；

第一生成单元，用于根据所述隐私保护项对应的得分权重以及所述隐私保护项对应的所述隐私安全得分生成第一隐私度量结果；

所述隐私保护项包括产品合规风险测试项、产品隐私安全保护技术测试项、产品适配法律测试项或产品隐私保护要求度测试项中的至少一种。

17、根据权利要求 16 所述的装置，其中，所述隐私保护项为产品合规风险测试项，所述获取单元包括：

配置子单元，用于配置合规风险测试用例；

测试子单元，用于根据所述合规风险测试用例对待测设备进行测试，得到合规风险测试结果，所述合规风险测试结果对应一风险等级得分；

第一计算子单元，用于计算各个合规风险测试用例对应的风险等级得分的平均值，得到平均风险等级得分；

第一生成子单元，用于将所述平均风险等级得分作为所述待测设备在所述产品合规风险测试项的隐私安全得分。

18、根据权利要求 16 所述的装置，其中，所述隐私保护项为产品隐私安全保护技术测试项，所述获取单元包括：

第一确定子单元，用于确定待测设备支持的隐私安全保护技术项；

第二确定子单元，用于针对每个隐私安全保护技术项，确定所述隐私安全保护技术项所应用的隐私安全保护技术的类型、强度以及数量；

获取子单元，用于获取预设映射关系集合，所述预设映射关系集合包括预设的隐私安全保护技术的类型、强度以及数量和安全评分的映射关系；

第三确定子单元，用于根据所述预设映射关系集合，根据所述隐私安全保护技术项应用的隐私安全保护技术的类型、强度或者数量确定安全评分；

第二计算子单元，用于计算各个隐私安全保护技术项的安全评分的平均值，得到平均安全评分；

第二生成子单元，用于将所述平均安全评分作为所述待测设备在所述产品隐私安全保护技术测试项的隐私安全得分。

19、一种电子设备，其中，所述电子设备包括存储器、处理器及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现如权利要求 1-14 任一项所述设备隐私管理方法的步骤。

20、一种计算机可读存储介质，其中，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求 1-14 任一项所述设备隐私管理方法的步骤。

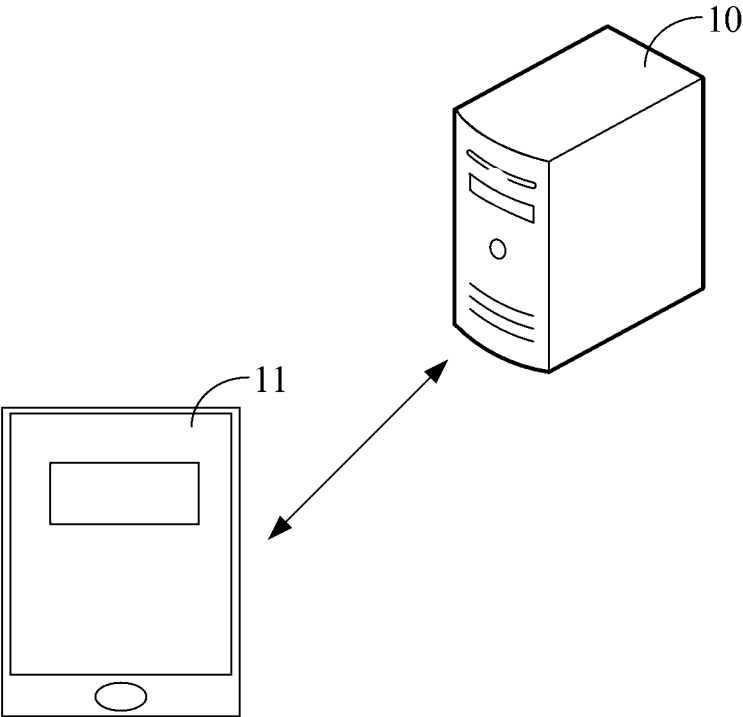


图 1

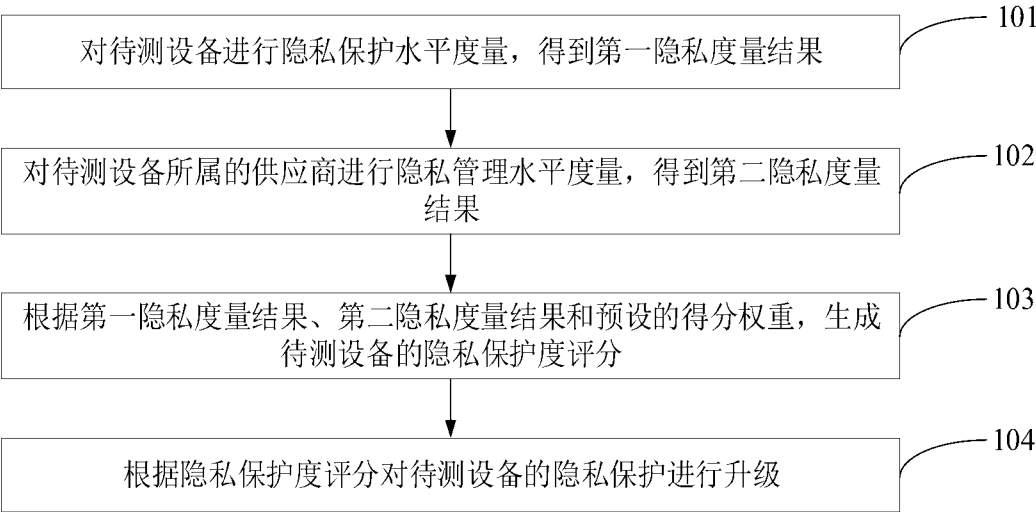


图 2

隐私安全保护技术项	安全评分
数据加密	1-5
数据备份和回复	4
安全套接层协议传输数据	2
云端采用的安全产品	1-5
接口认证授权	2
数据脱敏	1
匿名算法	5
差分隐私	5

图 3

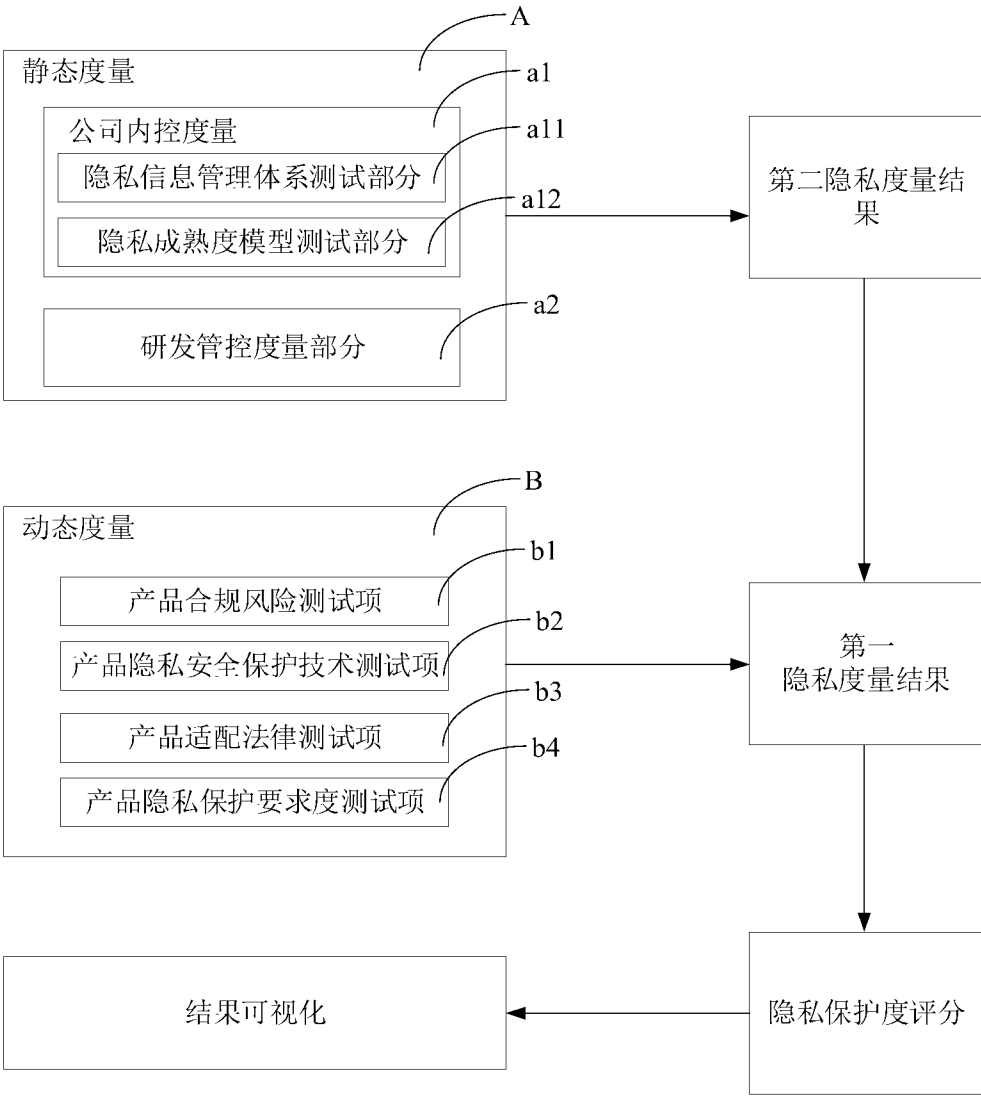


图 4

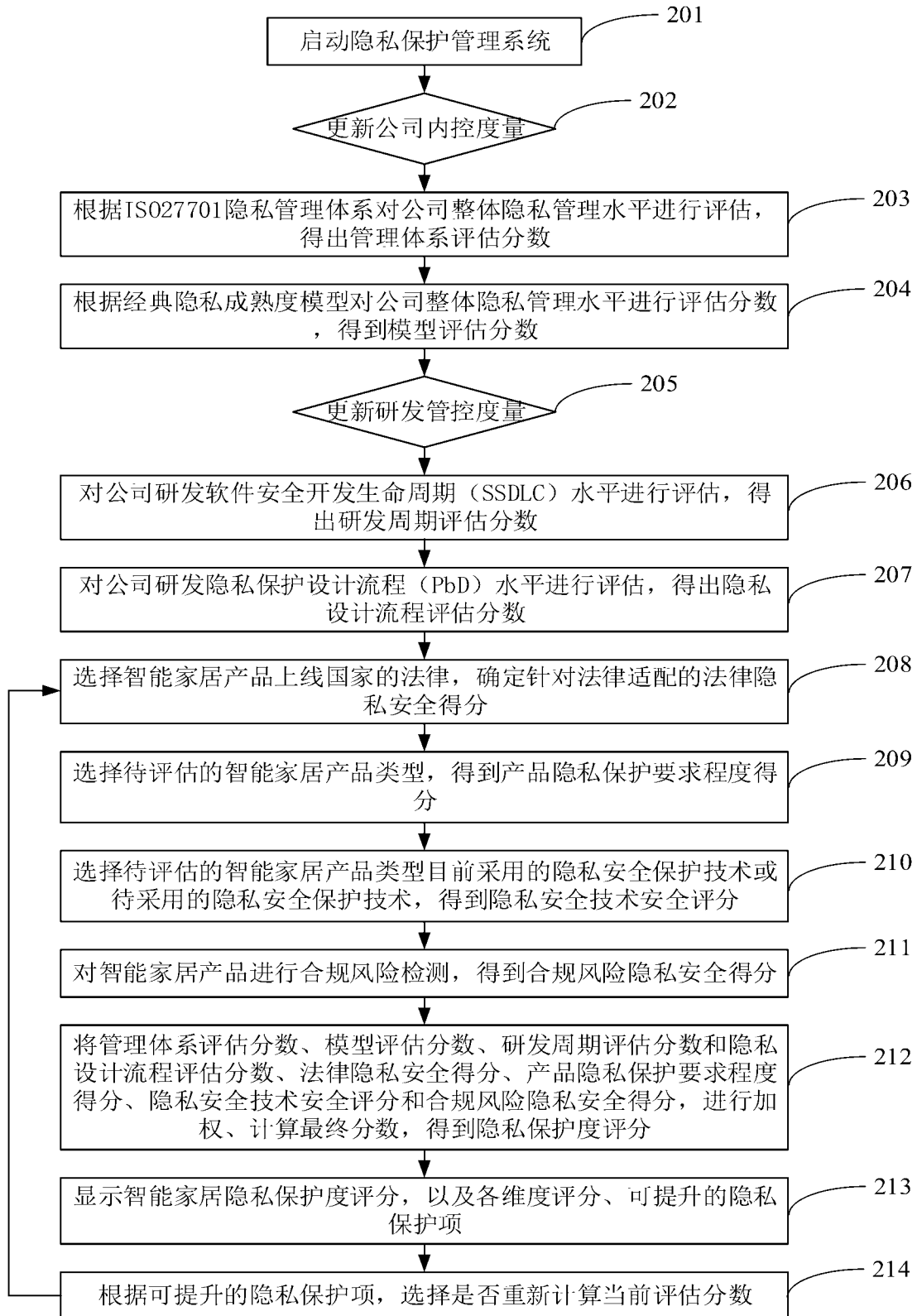


图 5

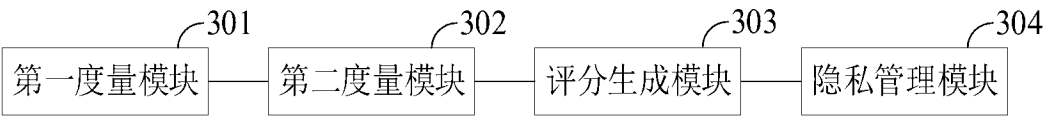


图 6

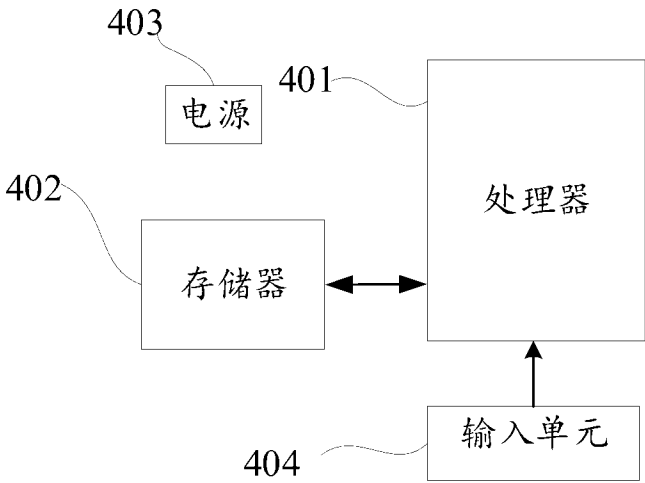


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/095704

A. CLASSIFICATION OF SUBJECT MATTER G06F 21/60(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) IPC: 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, CNTXT, USTXT, EPTXT, WOTXT, VEN, CNABS, IEEE, BING: 隐私保护, 设备, 得分, 第二, 供应商, 加权, 权重, privacy protection, device, score, second, provider, weight		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 117407892 A (SHENZHEN TCL NEW TECHNOLOGY CO., LTD.) 16 January 2024 (2024-01-16) description, paragraphs [0005]-[0051] and [0061]-[0222], and figures 1-7	1-20
Y	CN 113221161 A (ZHU HONGDONG) 06 August 2021 (2021-08-06) description, paragraphs [0026], [0044], and [0065]-[0069], figures 1-4, and claim 10	1-20
Y	HUAWEI TECHNOLOGIES CO., LTD. "华为隐私保护治理白皮书 (Huawei Privacy Protection Whitepaper)" https://www.huawei.com/cn/news/2022/11/huawei-privacy-protection-whitepaper , 09 November 2022 (2022-11-09), page 10, section 3.3	1-20
A	CN 114357509 A (SHENZHEN TCL NEW TECHNOLOGY CO., LTD.) 15 April 2022 (2022-04-15) entire document	1-20
A	CN 109716345 A (PRIVITAR LTD.) 03 May 2019 (2019-05-03) 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 "D" document cited by the applicant in the international application "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 15 August 2024		Date of mailing of the international search report 20 August 2024
Name and mailing address of the ISA/CN China National Intellectual Property Administration (ISA/CN) China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088		Authorized officer Telephone No.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 111400747 A (XI'AN JIAOTONG UNIVERSITY) 10 July 2020 (2020-07-10) entire document	1-20
A	US 2014173684 A1 (NYMITY, INC.) 19 June 2014 (2014-06-19) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/095704

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	117407892	A	16 January 2024	None			
CN	113221161	A	06 August 2021	None			
CN	114357509	A	15 April 2022	None			
CN	109716345	A	03 May 2019	SG	11201809476	VA	29 November 2018
				US	2020327252	A1	15 October 2020
				US	11698990	B2	11 July 2023
				EP	3449414	A1	06 March 2019
				EP	3449414	B1	08 December 2021
				WO	2017187207	A1	02 November 2017
				US	2023359770	A1	09 November 2023
CN	111400747	A	10 July 2020	None			
US	2014173684	A1	19 June 2014	US	8966575	B2	24 February 2015

A. 主题的分类

G06F 21/60(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)

IPC: 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, CNTXT, USTXT, EPTXT, WOTXT, VEN, CNABS, IEEE, BING: 隐私保护, 设备, 得分, 第二, 供应商, 加
权, 权重, privacy protection, device, score, second, provider, weight

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
PX	CN 117407892 A (深圳TCL新技术有限公司) 2024年1月16日 (2024 - 01 - 16) 说明书第[0005]-[0051], [0061]-[0222]段、附图1-7	1-20
Y	CN 113221161 A (朱洪东) 2021年8月6日 (2021 - 08 - 06) 说明书第[0026], [0044], [0065]-[0069]段、附图1-4、权利要求10	1-20
Y	华为技术有限公司. "华为隐私保护治理白皮书" https://www.huawei.com/cn/news/2022/11/huawei-privacy-protection-whitepaper , 2022年11月9日 (2022 - 11 - 09), 第10页第3.3节	1-20
A	CN 114357509 A (深圳TCL新技术有限公司) 2022年4月15日 (2022 - 04 - 15) 全文	1-20
A	CN 109716345 A (普威达有限公司) 2019年5月3日 (2019 - 05 - 03) 全文	1-20
A	CN 111400747 A (西安交通大学) 2020年7月10日 (2020 - 07 - 10) 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

"D" 申请人在国际申请中引证的文件

"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

2024年8月15日

国际检索报告邮寄日期

2024年8月20日

ISA/CN的名称和邮寄地址

中国国家知识产权局
中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

张建

电话号码 (+86) 010-53961432

PCT/ISA/210 表(第2页) (2022年7月)

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
A	US 2014173684 A1 (NYMITY, INC.) 2014年6月19日 (2014 - 06 - 19) 全文	1-20

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/095704

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	117407892	A	2024年1月16日	无			
CN	113221161	A	2021年8月6日	无			
CN	114357509	A	2022年4月15日	无			
CN	109716345	A	2019年5月3日	SG	11201809476	VA	2018年11月29日
				US	2020327252	A1	2020年10月15日
				US	11698990	B2	2023年7月11日
				EP	3449414	A1	2019年3月6日
				EP	3449414	B1	2021年12月8日
				WO	2017187207	A1	2017年11月2日
				US	2023359770	A1	2023年11月9日
CN	111400747	A	2020年7月10日	无			
US	2014173684	A1	2014年6月19日	US	8966575	B2	2015年2月24日