(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111177536 B
(45)授权公告日 2023.12.26

(21)申请号 201911271452.2
(22)申请日 2019.12.12
(65)同一申请的已公布的文献号
申请公布号 CN 111177536 A
(43)申请公布日 2020.05.19
(73)专利权人 上海淇玥信息技术有限公司
地址 201500 上海市崇明区横沙乡富民支路58号A2-8914室
(72)发明人 陈博 黎文杰 郑盛麟 刘禹彤
(74)专利代理机构 北京清诚知识产权代理有限公司 11691
专利代理师 何怀燕
(51)Int.Cl.
G06F 16/9535(2019.01)
G06F 21/32(2013.01)

(56)对比文件
CN 109978607 A,2019.07.05
CN 110061984 A,2019.07.26
CN 110363577 A,2019.10.22
US 2007204233 A1,2007.08.30
US 2014129942 A1,2014.05.08
US 2016164958 A1,2016.06.09
US 2017310667 A1,2017.10.26
US 2017344568 A1,2017.11.30
CN 109657434 A,2019.04.19
CN 107979521 A,2018.05.01
CN 108712435 A,2018.10.26
CN 103297404 A,2013.09.11
CN 106775742 A,2017.05.31
EP 2966586 A1,2016.01.13

审查员 郑扬银

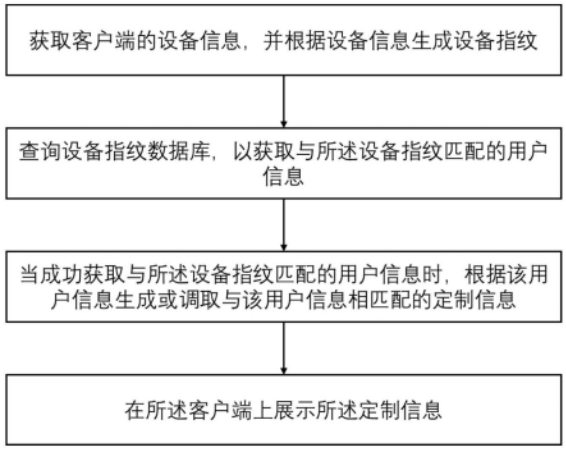
权利要求书3页 说明书9页 附图4页

(54)发明名称

基于设备指纹对未登录用户传送定制信息的方法、装置及电子设备

(57)摘要

本发明公开了一种基于设备指纹对未登录用户传送定制信息的方法、装置、电子设备及相应的计算机可读介质。所述方法包括:查询设备指纹数据库,以获取与所述设备指纹匹配的用户信息;当成功获取与所述设备指纹匹配的用户信息时,根据该用户信息生成或调取与该用户信息相匹配的定制信息;在所述客户端上展示所述定制信息。本发明能够实现在用户未登录APP的状态下,进行精准的定制信息传送和展示。



CN 111177536 B

1.一种基于设备指纹对未登录用户传送定制信息的方法,包括以下步骤:

获取客户端的设备信息,并根据设备信息通过加密算法生成唯一识别的设备指纹;当用户登录该设备时,对用户信息和根据设备信息生成的设备指纹进行绑定,形成用户和设备的一一对应关系,当用户第一次登录该

设备时,APP自动记录用户信息和设备指纹的对应关系,并记录在设备本地且上传到服务器的设备指纹数据库;在用户未登录设备情况下获取当前设备的设备指纹,或者根据当前设备的设备信息生成设备指纹;

通过查询设备指纹数据库上记录的绑定关系,以获取与所述设备指纹匹配的用户信息;

当成功获取与所述设备指纹匹配的用户信息时,根据该用户信息生成或调取与该用户信息相匹配的定制信息;当需要进行用户定制信息的扩展时,基于用户的需求建立矩阵数据模型,建立可扩矩阵数据模型与用户的对应关系,获得相匹配的定制信息;

在所述客户端上展示所述定制信息。

2.根据权利要求1所述的基于设备指纹对未登录用户传送定制信息的方法,其特征在于:

所述通过查询设备指纹数据库上记录的绑定关系,以获取与所述设备指纹匹配的用户信息包括:所述客户端向配置有设备指纹数据库的服务器发送查询指令,接收服务器返回的查询结果。

3.根据权利要求1所述的基于设备指纹对未登录用户传送定制信息的方法,其特征在于:

所述客户端预存储有多个定制信息;

当成功获取与所述设备指纹匹配的用户信息时,根据所述用户信息调取所述多个定制信息中的至少一个。

4.根据权利要求1所述的基于设备指纹对未登录用户传送定制信息的方法,其特征在于,还包括:

当未成功获取与所述设备指纹匹配的用户信息时,在所述客户端上展示默认定制信息。

5.根据权利要求1所述的基于设备指纹对未登录用户传送定制信息的方法,其特征在于,还包括:

检测客户端上的用户登录操作,当检测到客户端上的用户登录操作时,获取登录用户信息;

当成功获取与所述设备指纹匹配的用户信息时,判断所获取的与所述设备指纹匹配的用户信息与所述登录用户信息是否一致;

当所获取的与所述设备指纹匹配的用户信息与所述登录用户信息不一致时,进行安全验证。

6.根据权利要求5所述的基于设备指纹对未登录用户传送定制信息的方法,其特征在于,所述安全验证包括:

向登录用户信息中的电话号码发送告警信息,所述告警信息用于引导用户确认是否允许在该客户端上登录。

7.根据权利要求6所述的基于设备指纹对未登录用户传送定制信息的方法,其特征在于,所述安全验证还包括:

检测当前用户对于在所述客户端上登录操作的确认信息,若检测到该确认信息,则允许当前用户登录,同时,将所述设备指纹数据库中的该 客户端的设备指纹信息所对应的用户信息更新为当前用户的用户信息。

8.一种基于设备指纹对未登录用户传送定制信息的装置,包括:

获取模块,用于获取客户端的设备信息,并根据设备信息通过加密算法生成唯一识别的设备指纹;当用户登录该设备时,对用户信息和根据设备信息生成的设备指纹进行绑定,形成用户和设备的一一对应关系,当用户第一次登录该设备时,APP自动记录用户信息和设备指纹的对应关系,并记录在设备本地且上传到服务器的设备指纹数据库;在用户未登录设备情况下获取当前设备的设备指纹,或者根据当前设备的设备信息生成设备指纹;

查询模块,用于通过查询设备指纹数据库上记录的绑定关系,以获取与所述设备指纹匹配的用户信息;

匹配模块,用于当成功获取与所述设备指纹匹配的用户信息时,根据该用户信息生成或调取与该用户信息相匹配的定制信息;当需要进行用户定制信息的扩展时,基于用户的需求建立矩阵数据模型,建立可扩矩阵数据模型与用户的对应关系,获得相匹配的定制信息;

展示模块,用于在所述客户端上展示所述定制信息。

9.根据权利要求8所述的基于设备指纹对未登录用户传送定制信息的装置,其特征在于:

所述查询模块用于:向配置有设备指纹数据库的服务器发送查询指令,获取服务器返回的查询结果。

10.根据权利要求8所述的基于设备指纹对未登录用户传送定制信息的装置,其特征在于:

所述客户端预存储有多个定制信息;

所述匹配模块用于:当成功获取与所述设备指纹匹配的用户信息时,根据所述用户信息调取所述多个定制信息中的至少一个。

11.根据权利要求8所述的基于设备指纹对未登录用户传送定制信息的装置,其特征在于,所述展示模块还用于:

当未成功获取与所述设备指纹匹配的用户信息时,在所述客户端上展示默认定制信息。

12.根据权利要求8所述的基于设备指纹对未登录用户传送定制信息的装置,其特征在于,还包括:

检测模块,用于检测客户端上的用户登录操作,当检测到客户端上的用户登录操作时,获取登录用户信息;

判断模块,用于当成功获取与所述设备指纹匹配的用户信息时,判断所获取的与所述设备指纹匹配的用户信息与所述登录用户信息是否一致;

安全模块,用于当所获取的与所述设备指纹匹配的用户信息与所述登录用户信息不一致时,进行安全验证。

13.根据权利要求12所述的基于设备指纹对未登录用户传送定制信息的装置,其特征在于,所述安全模块还用于:

向登录用户信息中的电话号码发送告警信息,所述告警信息用于引导用户确认是否允许在该客户端上登录。

14.根据权利要求13所述的基于设备指纹对未登录用户传送定制信息的装置,其特征在于,所述安全模块还用于:

检测当前用户对于在所述客户端上登录操作的确认信息,若检测到该确认信息,则允许当前用户登录,同时,将所述设备指纹数据库中的该 客户端的设备指纹信息所对应的用户信息更新为当前用户的用户信息。

15.一种电子设备,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计算机程序,其特征在于,所述处理器执行所述程序时,实现如权利要求1至7中任一项所述的方法。

16.一种计算机可读存储介质,其上存储有计算机程序,该程序能够被处理器执行来实现如权利要求1-7中任一所述的方法。

基于设备指纹对未登录用户传送定制信息的方法、装置及电子设备

技术领域

[0001] 本发明涉及计算机应用领域,具体而言,涉及一种基于设备指纹对未登录用户传送定制信息的方法、装置、电子设备及计算机可读介质。

背景技术

[0002] 通常,在用户打开一个新的APP时,默认为未登录状态,此时是无法直接获取用户的基本信息,也无法对其进行精准的定制信息的传送。所述定制信息例如是营销类的信息。这样,对于APP涉足的具体产品来说,会浪费用户第一次打开APP的展示产品信息的机会。特别的,金融类APP安全性和可靠性要求高,在不使用APP时,默认为未登录状态。特别是,在用户登录新设备时,需要核验用户身份。

[0003] 因此,一种在用户未登录状态下可以对用户进行精准营销的方法有待提出。

发明内容

[0004] 本发明旨在解决现有技术中,在用户未登录时无法获取用户信息,因此无法对其传送定制信息的问题。

[0005] 为了解决上述技术问题,本发明第一方面提出一种基于设备指纹对未登录用户传送定制信息的方法,包括以下步骤:获取客户端的设备信息,并根据设备信息生成设备指纹;查询设备指纹数据库,以获取与所述设备指纹匹配的用户信息;当成功获取与所述设备指纹匹配的用户信息时,根据该用户信息生成或调取与该用户信息相匹配的定制信息;在所述客户端上展示所述定制信息。

[0006] 根据本发明的优选实施方式,所述查询设备指纹数据库,以获取与所述设备指纹匹配的用户信息包括:所述客户端向配置有设备指纹数据库的服务器发送查询指令,接收服务器返回的查询结果。

[0007] 根据本发明的优选实施方式,所述客户端预存储有多个定制信息;

[0008] 当成功获取与所述设备指纹匹配的用户信息时,根据所述用户信息调取所述多个预存储定制信息中的至少一个。

[0009] 根据本发明的优选实施方式,当未成功获取与所述设备指纹匹配的用户信息时,在所述客户端上展示默认定制信息。

[0010] 根据本发明的优选实施方式,检测客户端上的用户登录操作,当检测到客户端上的用户登录操作时,获取登录用户信息;当成功获取与所述设备指纹匹配的用户信息时,判断所获取的与所述设备指纹匹配的用户信息与所述登录用户信息是否一致;当所获取的与所述设备指纹匹配的用户信息与所述登录用户信息不一致时,进行安全验证。

[0011] 根据本发明的优选实施方式,所述安全验证包括:向登录用户信息中的电话号码发送告警信息,所述告警信息用于引导用户确认是否允许在该客户端上登录。

[0012] 根据本发明的优选实施方式,所述安全验证还包括:检测当前用户对于在所述客

户端上登录操作的确认信息,若检测到该确认信息,则允许当前用户登录,同时,将所述设备指纹数据库中的该客户端的设备指纹信息所对应的用户信息更新为当前用户的用户信息。

[0013] 为了解决上述技术问题,本发明第二方面提出一种基于设备指纹对未登录用户传送定制信息的装置,包括:获取模块,用于获取客户端的设备信息,并根据设备信息生成设备指纹;查询模块,用于查询设备指纹数据库,以获取与所述设备指纹匹配的用户信息;匹配模块,用于当成功获取与所述设备指纹匹配的用户信息时,根据该用户信息生成或调取与该用户信息相匹配的定制信息;展示模块,用于在所述客户端上展示所述定制信息。

[0014] 根据本发明的优选实施方式,所述查询模块用于:向配置有设备指纹数据库的服务器发送查询指令,获取服务器返回的查询结果。

[0015] 根据本发明的优选实施方式,所述客户端预存储有多个定制信息;所述匹配模块用于:当成功获取与所述设备指纹匹配的用户信息时,根据所述用户信息调取所述多个预存储定制信息中的至少一个。

[0016] 根据本发明的优选实施方式,所述展示模块还用于:当未成功获取与所述设备指纹匹配的用户信息时,在所述客户端上展示默认定制信息。

[0017] 根据本发明的优选实施方式,检测模块,用于检测客户端上的用户登录操作,当检测到客户端上的用户登录操作时,获取登录用户信息;判断模块,用于当成功获取与所述设备指纹匹配的用户信息时,判断所获取的与所述设备指纹匹配的用户信息与所述登录用户信息是否一致;安全模块,用于当所获取的与所述设备指纹匹配的用户信息与所述登录用户信息不一致时,进行安全验证。

[0018] 根据本发明的优选实施方式,所述安全模块还用于:向登录用户信息中的电话号码发送告警信息,所述告警信息用于引导用户确认是否允许在该客户端上登录。

[0019] 根据本发明的优选实施方式,所述安全模块还用于:检测当前用户对于在所述客户端上登录操作的确认信息,若检测到该确认信息,则允许当前用户登录,同时,将所述设备指纹数据库中的该客户端的设备指纹信息所对应的用户信息更新为当前用户的用户信息。

[0020] 为了解决上述技术问题,本发明第三方面提出一种电子设备,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计算机程序,该处理器执行所述程序时,实现上述基于设备指纹对未登录用户传送定制信息的方法。

[0021] 为了解决上述技术问题,本发明第四方面提供一种计算机可读存储介质,其上存储有计算机程序,该程序能够被处理器执行来实现上述基于设备指纹对未登录用户传送定制信息的方法。

[0022] 本发明通过获得客户端的设备指纹,并通过匹配绑定用户从而获得未登录用户的基本信息,从而能够在用户未登录的情况下对该用户进行定制信息的传送。

[0023] 此外,本发明还能够对用户登录进行安全验证,更新设备指纹与用户信息的绑定关系,保证了安全性。

附图说明

[0024] 为了使本发明所解决的技术问题、采用的技术手段及取得的技术效果更加清楚,

下面将参照附图详细描述本发明的具体实施例。但需声明的是,下面描述的附图仅仅是本发明的示例性实施例的附图,对于本领域的技术人员来讲,在不付出创造性劳动的前提下,可以根据这些附图获得其他实施例的附图。

[0025] 图1是示出了根据本发明实施例的一种基于设备指纹对未登录用户传送定制信息的方法的流程图。

[0026] 图2是示出了根据本发明实施例的一种基于设备指纹对未登录用户传送定制信息的方法的示意图。

[0027] 图3是示出了根据本发明实施例的一种基于设备指纹对未登录用户传送定制信息的装置的模块组成图。

[0028] 图4是根据本发明的一种电子设备的示例性实施例的结构框图。

[0029] 图5是本发明的一个计算机可读介质实施例的示意图。

具体实施方式

[0030] 现在将参考附图来更加全面地描述本发明的示例性实施例,虽然各示例性实施例能够以多种具体的方式实施,但不应理解为本发明仅限于在此阐述的实施例。相反,提供这些示例性实施例是为了使本发明的内容更加完整,更加便于将发明构思全面地传达给本领域的技术人员。

[0031] 在符合本发明的技术构思的前提下,在某个特定的实施例中描述的结构、性能、效果或者其他特征可以以任何合适的方式结合到一个或更多其他的实施例中。

[0032] 在对于具体实施例的介绍过程中,对结构、性能、效果或者其他特征的细节描述是为了使本领域的技术人员对实施例能够充分理解。但是,并不排除本领域技术人员可以在特定情况下,以不含有上述结构、性能、效果或者其他特征的技术方案来实施本发明。

[0033] 附图中的流程图仅是一种示例性的流程演示,不代表本发明的方案中必须包括流程图中的所有的内容、操作和步骤,也不代表必须按照图中所显示的顺序执行。例如,流程图中有的操作/步骤可以分解,有的操作/步骤可以合并或部分合并,等等,在不脱离本发明的发明主旨的情况下,流程图中显示的执行顺序可以根据实际情况改变。

[0034] 附图中的框图一般表示的是功能实体,并不一定必然与物理上独立的实体相对应。即,可以采用软件形式来实现这些功能实体,或在一个或多个硬件模块或集成电路中实现这些功能实体,或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

[0035] 各附图中相同的附图标记表示相同或类似的元件、组件或部分,因而下文中可能省略了对相同或类似的元件、组件或部分的重复描述。还应理解,虽然本文中可能使用第一、第二、第三等表示编号的定语来描述各种器件、元件、组件或部分,但是这些器件、元件、组件或部分不应受这些定语的限制。也就是说,这些定语仅是用来将一者与另一者区分。例如,第一器件亦可称为第二器件,但不偏离本发明实质的技术方案。此外,术语“和/或”、“及/或”是指包括所列出项目中的任一个或多个的所有组合。

[0036] 图1是示出了根据本发明实施例的一种基于设备指纹对未登录用户传送定制信息的方法的流程图。

[0037] 如图1所示,本发明的方法首先获取客户端的设备信息,并根据设备信息生成设备

指纹。APP会根据用户协议,获取设备相关信息。该相关信息可以是识别设备的唯一标识信息,且每个设备的该相关信息都各不相同,例如,可以是设备IMEI,识别码,标识码等。该设备可以是智能终端,例如智能手机,IPad,智能电话手表等。APP可以是安全度较高的APP,例如金融类的APP,更具体的,银行的APP,证券交易的APP,移动支付的APP等。此类的APP如果用户要使用,大多数必须进行用户登录。

[0038] 查询设备指纹数据库,以获取与所述设备指纹匹配的用户信息。可选地,该APP通过加密算法形成唯一识别的用户设备指纹。该用户设备指纹会存储在APP的远程服务器中。也可以将密钥放在签名文件中,应用于自身UID可以访问该文件,安全性较高。该密钥可以使非对称密钥来加密,服务端会存储对应的私钥。形成的用户设备指纹都各不相同且只有该APP可以识别。

[0039] 当成功获取与该设备指纹匹配的用户信息时,根据该用户信息生成或调取与该用户信息相匹配的定制信息。可选地,该客户端预存储有多个定制信息;当成功获取与该设备指纹匹配的用户信息时,根据该用户信息调取该多个预存储定制信息中的至少一个。特别是,用户信息可以是基于用户需求的,根据不同的用户建立对应的商业舆情定制信息。优选的,当需要进行用户定制信息的扩展时,首先基于用户的需求建立矩阵数据模型,然后建立可扩矩阵数据模型与用户的对应关系,获得相匹配的定制信息。通过建立可扩矩阵数据模型能够及时进行用户信息更新,灵活应对用户需求,提高资源利用率。当成功获取与该设备指纹匹配的用户信息时,根据该用户信息调取该多个预存储定制信息中的至少一个,也可以是多个。

[0040] 用户在设备上登录后,对用户信息和根据设备信息生成的设备指纹进行绑定。APP记录这种绑定关系,且形成了某一用户和某一设备的一一对应关系。当用户第一次登录该设备时,APP自动记录用户信息和设备指纹的对应关系,记录在设备本地且上传到服务器的设备指纹数据库。

[0041] 在用户未登录情况下(用户尚未进行第一次在设备上登录,或者已在该设备上退出登录),APP也能获取当前设备的设备指纹,或者根据当前设备的设备信息生成设备指纹。由此,APP通过查询服务器上之前记录的绑定关系,匹配出与当前设备指纹对应的用户信息,并将其作为未登录用户的用户信息,并在用户未登录的情况下对其进行精准营销。该用户信息可以包括用户ID信息,也可以包括用户使用习惯,浏览习惯,关注哪类消息等特征信息。

[0042] 由此,用户在未登录状态下,APP就可以获得曾经使用该设备用户的基本信息,并且能够推送定值消息,进行精准营销。在该客户端上展示所述定制信息。

[0043] 当未成功获取与所述设备指纹匹配的用户信息时,在该客户端上展示默认定制信息。

[0044] 同时,APP也实时检测客户端上的用户登录操作,当检测到客户端上的用户登录操作时,获取当前登录用户的用户信息;当成功获取与该设备指纹匹配的用户信息时,判断所获取的与该设备指纹匹配的用户信息与该当前登录的用户信息是否一致;当所获取的与所述设备指纹匹配的用户信息与所述登录用户信息不一致时,进行安全验证。

[0045] 一种安全验证方式是向登录用户信息中的电话号码发送告警信息,所述告警信息用于引导用户确认是否允许在该客户端上登录。具体的,该APP根据用户协议获取该设备的

信息之前,打开所述APP,默认是未登录状态。当APP安装到设备时,即可根据用户协议自动获取设备的信息。通常情况,当APP首次安装到设备时,并没有用户登录,因此,在首次打开APP时,默认是未登录的状态。

[0046] 检测当前用户对于在所述客户端上登录操作的确认信息,若检测到该确认信息,则允许当前用户登录,同时,将该设备指纹数据库中的该客户端的设备指纹信息所对应的用户信息更新为当前用户的用户信息。

[0047] 图2是示出了根据本发明实施例的一种基于设备指纹对未登录用户传送定制信息的方法的示意图。该实施例中,所述定制信息为营销信息,例如广告页、促销活动信息等。如图2所示,而当用户在新设备上登录后,则会触发新设备登录安全验证机制,通过验证后即会更新用户与设备指纹的绑定关系。判断该设备的指纹是否与用户原设备一致,如果是,不做改动。如果否,短信提醒用户在新设备上登录,然后继续判断,是否是本人操作,如果是本人操作,则无视短信,更新用户与该设备的指纹对应关系,如果非本人操作,用户可通过短信链接冻结账户并修改账号。

[0048] 可选地,判断该设备的指纹是否有对应用户,如果是,匹配对应用户信息,进行精准营销活动;如果否,显示默认页面,该默认页面是用户未登录状态。APP在之前的步骤中已经记录了设备信息,当某一用户登录过该设备时,APP也记录了绑定关系。因此,在判断该设备是否有对应用户时,APP先根据之前记录的设备信息判断用户是否为对应用户,如果是,匹配对应用户信息,进行精准营销活动。可选地,当APP要进行精准营销活动时,是APP 服务器执行营销活动到APP时,首先将这条营销消息发送到营销活动服务器,营销活动服务器首先判断此APP服务器对应的APP是否存在注册的移动终端,并返回结果给APP服务器。如果存在,对这条营销活动进行过滤、加工,然后发送给移动终端的APP。

[0049] 可选地,判断该设备的指纹是否有对应用户,如果否,展示默认页面,执行用户登录。如果APP判断不是对应用户,则展示默认页面,用户可以选择执行用户登录。

[0050] 本领域技术人员可以理解,实现上述实施例的全部或部分步骤被实现为由数据处理设备(包括计算机)执行的程序,即计算机程序。在该计算机程序被执行时,可以实现本发明提供的上述方法。而且,所述的计算机程序可以存储于计算机可读存储介质中,该存储介质可以是磁盘、光盘、ROM、RAM等可读存储介质,也可以是多个存储介质组成的存储阵列,例如磁盘或磁带存储阵列。所述的存储介质不限于集中式存储,其也可以是分布式存储,例如基于云计算的云存储。

[0051] 下面描述本发明的装置实施例,该装置可以用于执行本发明的方法实施例。对于本发明装置实施例中描述的细节,应视为对于上述方法实施例的补充;对于在本发明装置实施例中未披露的细节,可以参照上述方法实施例来实现。

[0052] 图3是本发明的基于设备指纹对未登录用户传送定制信息的装置的模块示意图,如图3所示,装置包括获取模块、查询模块、匹配模块和展示模块。

[0053] 其中,获取模块用于获取客户端的设备信息,并根据设备信息生成设备指纹。具体的,获取模块获取客户端的设备信息,并根据设备信息生成设备指纹。APP会根据用户协议,获取设备相关信息。该相关信息可以是识别设备的唯一标识信息,且每个设备的该相关信息都各不相同,例如设备IMEI,识别码,标识码等。该设备可以是智能终端,例如智能手机,IPad等。APP可以是安全度较高的APP,例如金融类的APP,更具体的,银行的APP,证券交易的

APP,移动支付的APP等。此类的APP如果用户要使用,大多数必须进行用户登录。

[0054] 查询模块,用于查询设备指纹数据库,以获取与该设备指纹匹配的用户信息。具体的,查询设备指纹数据库,以获取与所述设备指纹匹配的用户信息。可选地,该APP通过加密算法形成唯一识别的用户设备指纹。该用户设备指纹会存储在APP的远程服务器中。也可以将密钥放在签名文件中,应用于自身UID可以访问该文件,安全性较高。该密钥可以使非对称密钥来加密,服务端会存储对应的私钥。形成的用户设备指纹都各不相同且只有该APP可以识别。

[0055] 优选的,该查询模块向配置有设备指纹数据库的服务器发送查询指令,获取服务器返回的查询结果。

[0056] 匹配模块,用于当成功获取与所述设备指纹匹配的用户信息时,根据该用户信息生成或调取与该用户信息相匹配的定制信息。优选的,该客户端预存储有多个定制信息;所述匹配模块在成功获取与所述设备指纹匹配的用户信息时,根据该用户信息调取所述多个预存储定制信息中的至少一个。也就是说,当成功获取与该设备指纹匹配的用户信息时,根据该用户信息生成或调取与该用户信息相匹配的定制信息。可选地,该客户端预存储有多个定制信息;当成功获取与该设备指纹匹配的用户信息时,根据该用户信息调取该多个预存储定制信息中的至少一个。特别是,用户信息可以是基于用户需求的,根据不同的用户建立对应的商业舆情定制信息。优选的,当需要进行用户定制信息的扩展时,首先基于用户的需求建立矩阵数据模型,然后建立可扩矩阵数据模型与用户的对应关系,获得相匹配的定制信息。通过建立可扩矩阵数据模型能够及时进行用户信息更新,灵活应对用户需求,提高资源利用率。当成功获取与该设备指纹匹配的用户信息时,根据该用户信息调取该多个预存储定制信息中的至少一个,也可以是多个。

[0057] 用户在设备上登录后,对用户信息和根据设备信息生成的设备指纹进行绑定。APP记录这种绑定关系,且形成了某一用户和某一设备的一一对应关系。当用户第一次登录该设备时,APP自动记录用户信息和设备指纹的对应关系,记录在设备本地且上传到服务器的设备指纹数据库。

[0058] 在用户未登录情况下(用户第一次在设备上登录,或者已在该设备上退出登录),APP也能获取当前设备的设备指纹,或者根据当前设备的设备信息生成设备指纹。由此,APP通过查询服务器上之前记录的绑定关系,匹配出与当前设备指纹对应的用户信息,并将其作为未登录用户的用户信息,并在用户未登录的情况下对其进行精准营销。该用户信息可以包括用户ID信息,也可以包括用户使用习惯,浏览习惯,关注哪类消息等特征信息。

[0059] 展示模块,用于在该客户端上展示所述定制信息。当未成功获取与该设备指纹匹配的用户信息时,在该客户端上展示默认定制信息。

[0060] 作为优选的实施方式,本发明的装置还包括检测模块、判断模块和安全模块。

[0061] 检测模块,用于检测客户端上的用户登录操作,当检测到客户端上的用户登录操作时,获取登录用户信息。具体的检测模块实时检测客户端上的用户登录操作,当检测到客户端上的用户登录操作时,获取当前登录用户的用户信息。

[0062] 判断模块用于当成功获取与该设备指纹匹配的用户信息时,判断所获取的与所述设备指纹匹配的用户信息与该登录用户信息是否一致。具体的,当成功获取与该设备指纹匹配的用户信息时,判断所获取的与该设备指纹匹配的用户信息与该当前登录的用户信息

是否一致;当所获取的与所述设备指纹匹配的用户信息与所述登录用户信息不一致时,进行安全验证。

[0063] 安全模块,用于当所获取的与该设备指纹匹配的用户信息与该登录用户信息不一致时,进行安全验证。

[0064] 优选的,安全模块向登录用户信息中的电话号码发送告警信息,该告警信息用于引导用户确认是否允许在该客户端上登录。。具体的,该APP根据用户协议获取该设备的信息之前,打开所述APP,默认是未登录状态。当APP安装到设备时,即可根据用户协议自动获取设备的信息。通常情况,当APP首次安装到设备时,并没有用户登录,因此,在首次打开APP时,默认是未登录的状态。

[0065] 优选的,安全模块还检测当前用户对于在该客户端上登录操作的确认信息,若检测到该确认信息,则允许当前用户登录,同时,将该设备指纹数据库中的该客户端的设备指纹信息所对应的用户信息更新为当前用户的用户信息。

[0066] 本领域技术人员可以理解,上述装置实施例中的各模块可以按照描述分布于装置中,也可以进行相应变化,分布于不同于上述实施例的一个或多个装置中。上述实施例的模块可以合并为一个模块,也可以进一步拆分成多个子模块。

[0067] 下面描述本发明的电子设备实施例,该电子设备可以视为对于上述本发明的方法和装置实施例的实体形式的实施方式。对于本发明电子设备实施例中描述的细节,应视为对于上述方法或装置实施例的补充;对于在本发明电子设备实施例中未披露的细节,可以参照上述方法或装置实施例来实现。

[0068] 图4是根据本发明的一种电子设备的示例性实施例的结构框图。图4显示的电子设备仅仅是一个示例,不应对本发明实施例的功能和使用范围带来任何限制。

[0069] 如图4所示,该示例性实施例的电子设备310以通用数据处理设备的形式表现。电子设备310的组件可以包括但不限于:至少一个处理单元311、至少一个存储单元312、连接不同系统组件(包括存储单元312和处理单元311)的总线316、显示单元313等。

[0070] 其中,所述存储单元312存储有计算机可读程序,其可以是源程序或都只读程序的代码。所述程序可以被处理单元311执行,使得所述处理单元210执行本发明各种实施方式的步骤。例如,所述处理单元311可以执行如图1所示的步骤。

[0071] 所述存储单元312可以包括易失性存储单元形式的可读介质,例如随机存取存储单元(RAM)3121和/或高速缓存存储单元3122,还可以进一步包括只读存储单元(ROM)3123。所述存储单元312还可以包括具有一组(至少一个)程序模块3125的程序/实用工具3124,这样的程序模块3125包括但不限于:操作系统、一个或者多个应用程序、其它程序模块以及程序数据,这些示例中的每一个或某种组合中可能包括网络环境的实现。

[0072] 总线316可以为表示几类总线结构中的一种或多种,包括存储单元总线或者存储单元控制器、外围总线、图形加速端口、处理单元或者使用多种总线结构中的任意总线结构的局域总线。

[0073] 电子设备310也可以与一个或多个外部设备320(例如键盘、显示器、网络设备、蓝牙设备等)通信,使得用户能经由这些外部设备320与该电子设备310交互,和/或使得该电子设备310能与一个或多个其它数据处理设备(例如路由器、调制解调器等等)进行通信。这种通信可以通过输入/输出(I/O)接口314进行,还可以通过网络适配器315与一个或者多个

网络(例如局域网(LAN),广域网(WAN)和/或公共网络,例如因特网)进行。网络适配器315可以通过总线316与电子设备310的其它模块通信。应当明白,尽管图中未示出,电子设备310中可使用其它硬件和/或软件模块,包括但不限于:微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0074] 图5是本发明的一个计算机可读介质实施例的示意图。如图5所示,所述计算机程序可以存储于一个或多个计算机可读介质上。计算机可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以为但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。可读存储介质的更具体的例子(非穷举的列表)包括:具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0075] 当所述计算机程序被一个或多个数据处理设备执行时,使得该计算机可读介质能够实现本发明的上述方法,即:一种基于设备指纹对未登录用户传送定制信息的方法、装置、电子设备及相应的计算机可读介质。所述方法包括:查询设备指纹数据库,以获取与所述设备指纹匹配的用户信息;当成功获取与所述设备指纹匹配的用户信息时,根据该用户信息生成或调取与该用户信息相匹配的定制信息;在所述客户端上展示所述定制信息。因此本发明能够实现,在用户未登录APP的状态下,APP通过设备指纹判断用户信息,进行传送定值消息,对用户进行精准营销。免去了用户登录APP,APP才可以识别用户信息这一过程。特别是金融领域的APP,只有当用户登录APP后,APP才被激活运行。并且当用户登录新设备时,可以判断是否是本人操作,保证了安全性,解决了提高精准营销率,提高用户存留率的问题。通过以上的实施方式的描述,本领域的技术人员易于理解,本发明描述的示例性实施例可以通过软件实现,也可以通过软件结合必要的硬件的方式来实现。因此,根据本发明实施方式的技术方案可以以软件产品的形式体现出来,该软件产品可以存储在一个计算机可读的存储介质(可以是CD-ROM,U盘,移动硬盘等)中或网络上,包括若干指令以使得一台数据处理设备(可以是个人计算机、服务器、或者网络设备等)执行根据本发明的上述方法。

[0076] 所述计算机可读存储介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了可读程序代码。这种传播的数据信号可以采用多种形式,包括但不限于电磁信号、光信号或上述的任意合适的组合。可读存储介质还可以是可读存储介质以外的任何可读介质,该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。可读存储介质上包含的程序代码可以用任何适当的介质传输,包括但不限于无线、有线、光缆、RF等等,或者上述的任意合适的组合。

[0077] 可以以一种或多种程序设计语言的任意组合来编写用于执行本发明操作的程序代码,所述程序设计语言包括面向对象的程序设计语言—诸如Java、C++等,还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中,远程计算设备可以通过任意种类的网络,包括局域网(LAN)或广域网(WAN),连接到用户计算设备,或者,可以连接到外部计算设备(例如利用因特网服务提供商来通过因特网连接)。

[0078] 综上所述,本发明可以执行计算机程序的方法、装置、电子设备或计算机可读介质来实现。可以在实践中使用微处理器或者数字信号处理器(DSP)等通用数据处理设备来实现本发明的一些或者全部功能。

[0079] 以上所述的具体实施例,对本发明的目的、技术方案和有益效果进行了进一步详细说明,应理解的是,本发明不与任何特定计算机、虚拟装置或者电子设备固有相关,各种通用装置也可以实现本发明。以上所述仅为本发明的具体实施例而已,并不用于限制本发明,凡在本发明的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

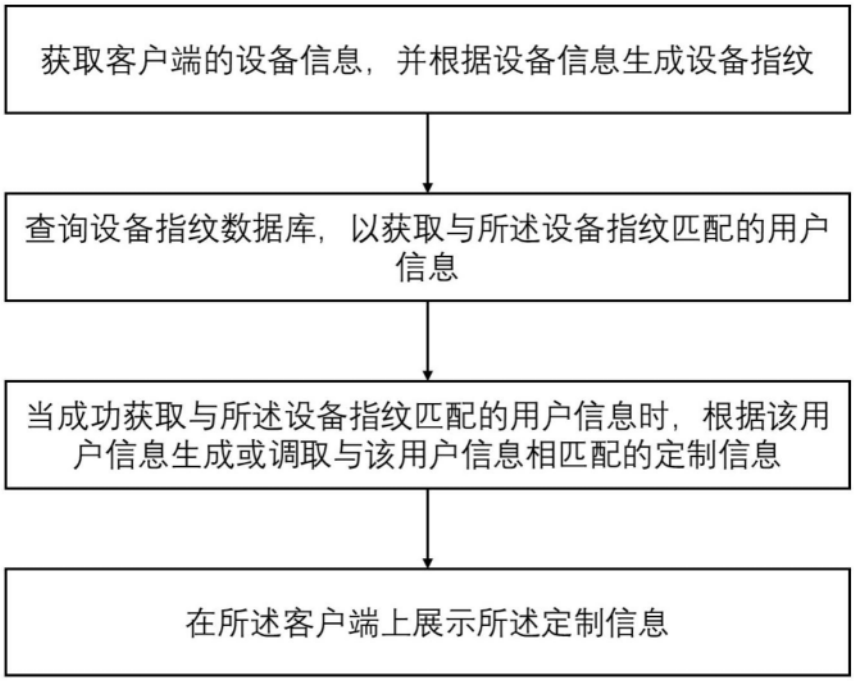

获取客户端的设备信息，并根据设备信息生成设备指纹
查询设备指纹数据库，以获取与所述设备指纹匹配的用户信息
当成功获取与所述设备指纹匹配的用户信息时，根据该用户信息生成或调取与该用户信息相匹配的定制信息
在所述客户端上展示所述定制信息

图1

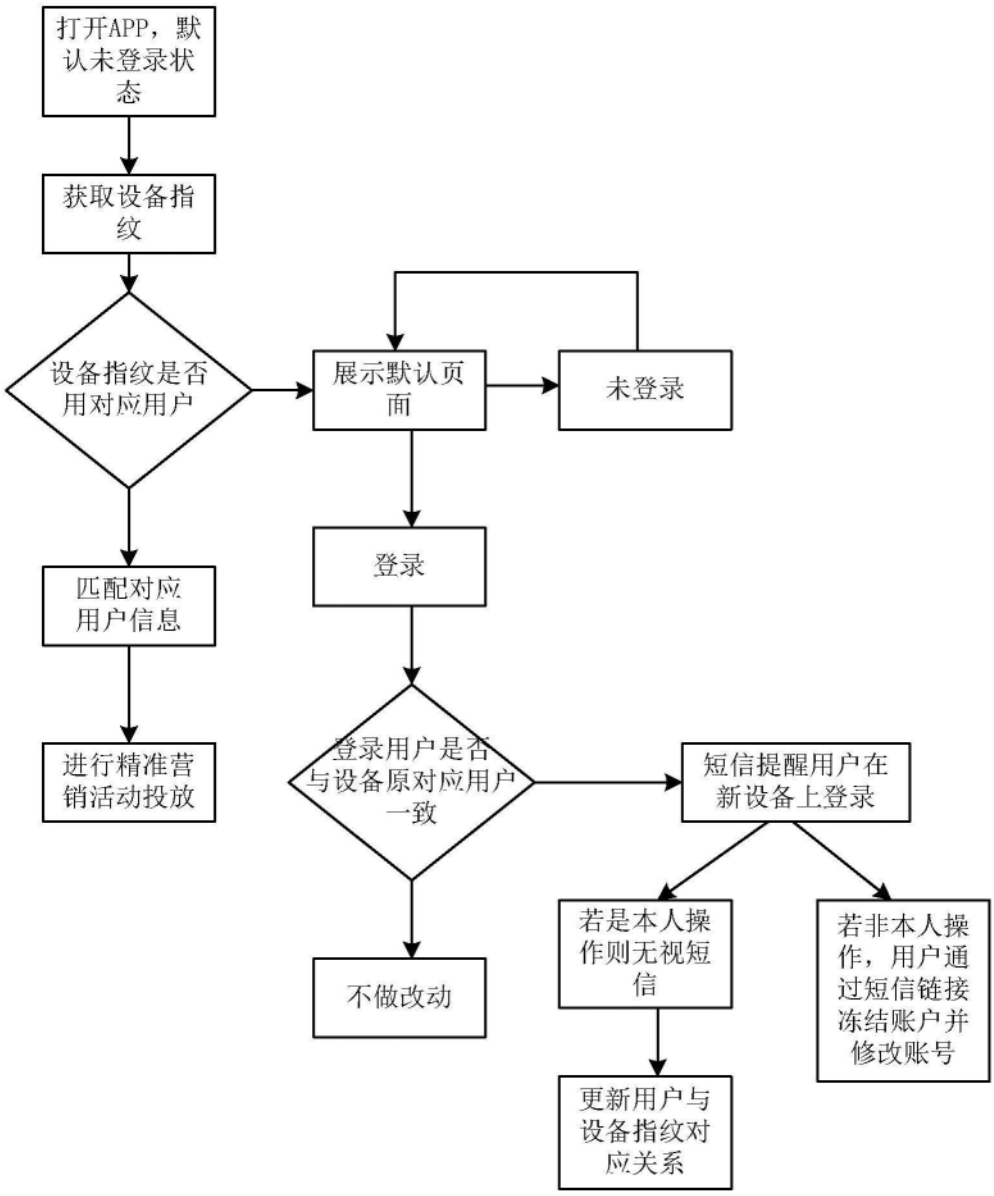

打开APP，默认未登录状态
获取设备指纹
设备指纹是否用对应用户
展示默认页面
未登录
匹配对应用户信息
进行精准营销活动投放
登录
登录用户是否与设备原对应用户一致
短信提醒用户在新设备上登录
不做改动
若是本人操作则无视短信
若非本人操作，用户通过短信链接冻结账户并修改账号
更新用户与设备指纹对应关系

图2

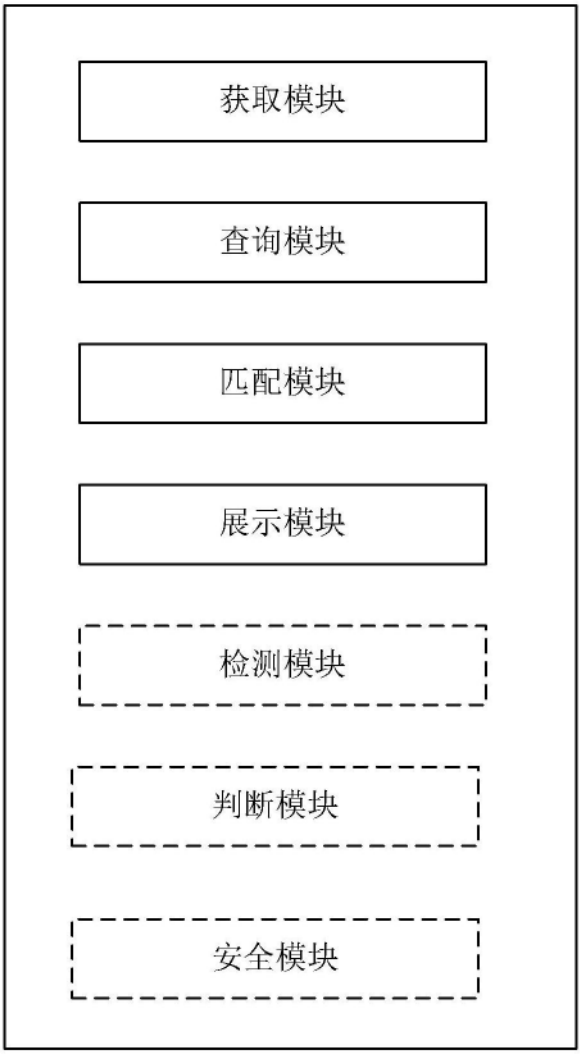


图3

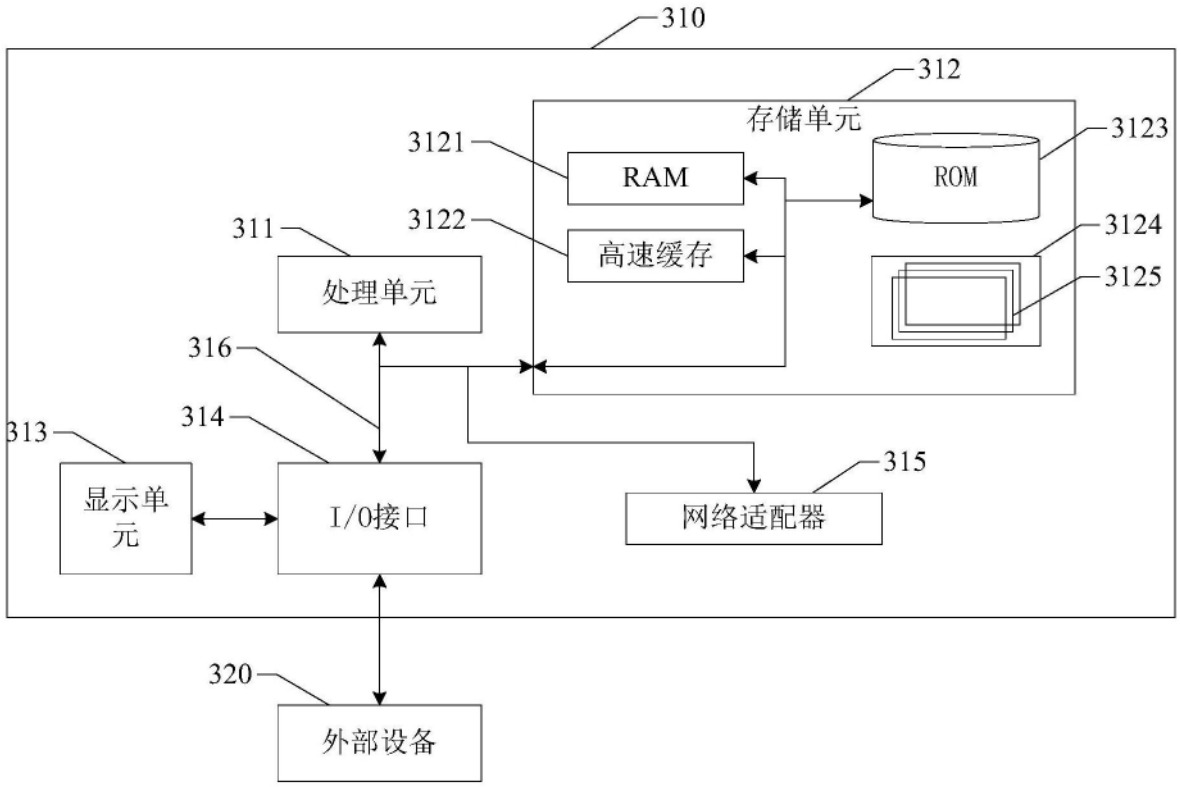

310
312
存储单元
3121
RAM
3123
ROM
3122
高速缓存
3124
3125
311
处理单元
316
314
313
显示单元
I/O接口
315
网络适配器
320
外部设备

图4

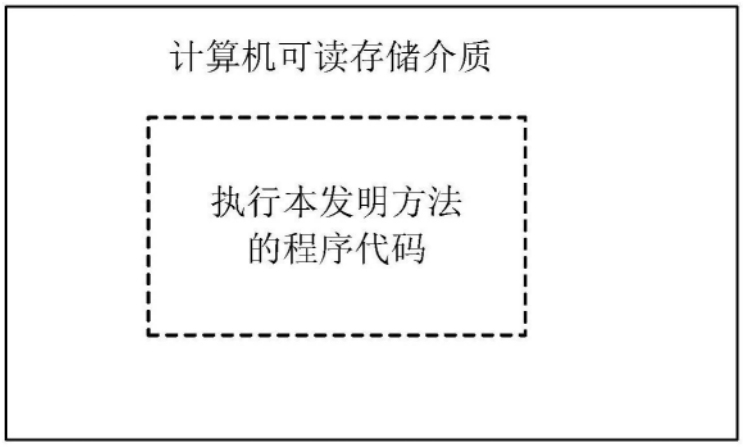

计算机可读存储介质
执行本发明方法
的程序代码

图5