(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114915439 A
(43)申请公布日 2022.08.16

(21)申请号 202111588597.2

(22)申请日 2021.12.23

(66)本国优先权数据
202111254534.3 2021.10.27 CN

(71)申请人 杭州拼便宜网络科技有限公司
地址 311215 浙江省杭州市萧山区萧山经济开发区金一路79号A座301室

(72)发明人 吴志刚 诸葛可环 张朋信

(74)专利代理机构 南京乐羽知行专利代理事务所(普通合伙) 32326
专利代理师 孙承尧

(51)Int.Cl.
H04L 9/40(2022.01)
G06Q 30/06(2012.01)
G06F 21/32(2013.01)
G06F 21/31(2013.01)

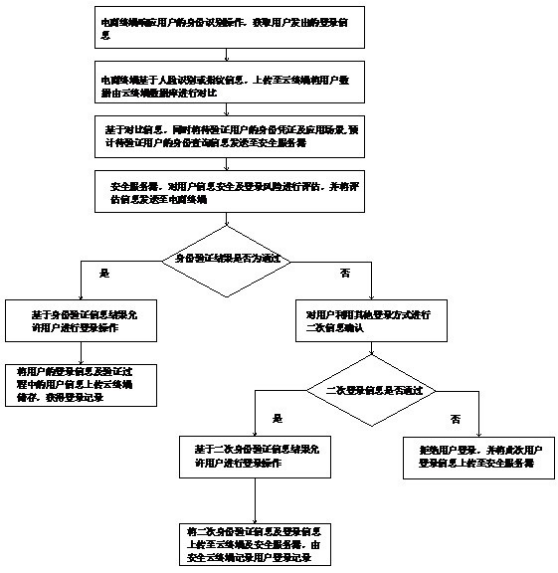
权利要求书2页 说明书8页 附图5页

(54)发明名称

电商平台身份验证的方法、装置、电子设备及存储介质

(57)摘要

本申请公开了一种电商平台身份验证的方法、装置、电子设备及存储介质。本申请的有益之处在于电商终端相应用户的身份识别操作,进而获取用户发出的登录信息,用户可通过不同的用户终端进行登录操作,可使用手机、电脑等获取用户的人像或指纹进行登录,适用范围更广泛;电商终端接收用户数据并传输至云终端,与云终端内部的数据进行对比,安全性更高,对比完成后获得对比结果,由电商客户端将对比数据用户的身份凭证,应用场景待验证的身份查询信息发送至安全服务器中,由安全服务器进行验证,对用户的登录风险进行评估,电商终端接收身份验证信息,防止他人进行登录,多重验证保护,安全性更高,更值得使用。



CN 114915439 A

1.一种电商平台身份验证的方法,包括:

电商终端响应用户的身份识别操作获取用户发出的信息;

其中,用户可通过用户终端进行登录操作,连接所述电商终端,通过所述用户终端进行面部或指纹识别,上传用户的登录数据;

所述电商终端接收所述用户数据,将所述用户数据上传至云终端,读取所述云终端的数据,由所述云终端的数据库与所述用户数据进行对比;

使用所述云终端储存数据,节省数据的储存陈本。

2.如权利要求1所述的一种电商平台身份验证的方法,其特征在于:

基于所述用户数据与所述云终端数据的对比,同时将待验证用户的身份凭证及应用场景,预计待验证所述用户的身份查询信息发送至安全服务器;

所述用户数据包括用户的登录信息、登录地点及登录时连接的网络;

所述安全服务器检测所述用户信息安全及登录风险进行评估,并将评估信息发送至所述电商终端;

所述安全服务器,检测用户信息与所述云终端数据的对比结果,评估所述用户登录地点和连接的网络,防止通过同一网络对所述用户发生盗号等行;

所述电商终端接收评估结果进行身份验证。

3.如权利要求2所述的一种电商平台身份验证的方法,其特征在于:

所述身份验证通过时,基于所述身份验证信息结果允许用户进行登录操作;

同时将用户的登录信息及验证过程中的用户数据上传至所述云终端,获得登录记录;

其中,所述电商终端使用户登入,所述用户数据上传至所述云终端后,增加所述云终端中的数据,便于所述用户下次登录时进行数据对比,提高用户的登录速度,减少用户的等待时间。

4.如权利要求2所述的一种电商平台身份验证的方法,其特征在于:

所述身份验证未通过后,用户利用其他登录防止进行二次信息确认;

所述安全服务器接收二次身份验证指令;

增加二次登入机会,防止所述用户对比数据发生错误,造成用户无法登录;

由所述安全服务器进行二次身份验证安全性更高。

5.如权利要求1所述的一种电商平台身份验证的方法,其特征在于:

所述安全服务器发送短信验证码或语音验证码至用户终端上,所述用户终端接收所述安全服务器发送的所述短信验证码或语音验证码,并将收到的所述短信验证码或语音验证码输入至所述电商终端中;

所述电商终端将接收的用户验证数据发送至所述安全服务器,由所述安全服务器进行验证,提高验证效率;

其中,所述语音验证利用智能外呼系统向所述用户发起语音通话;

当所述用户接通所述语音通话后,向所述电商终端播报所述身份验证结果。

6.如权利要求1所述的一种电商平台身份验证的方法,其特征在于:

所述二次登录信息通过时,基于所述二次身份验证信息结构允许所述用户进行登录操作;

所述用户登录完成后,所述电商终端将所述二次身份验证信息及登录信息上传子所述

云终端与安全服务器中，由所述云终端记录用户登记记录，下次所述用户登录时，提高所述云终端对比效率。

7.如权利要求1所述的一种电商平台身份验证的方法，其特征在于：

所述二次登录信息未通过时，拒绝用户登录，并将此次用户登录信息上传至安全服务器；

其中，所述安全服务器将此次登录标记为危险登录信息，与下次登录进行对比，提高危险登录的分辨效率。

8.一种电商平台身份验证的装置，包括：

第一接收模块，接收所述用户终端中的登录数据，可接收手机终端及计算机终端多种终端的数据，适用范围更广泛；

云终端，用以储存用户的数据，在所述云终端内搜索所述用户数据的对比数据；

第一验证模块，验证所述用户数据及对比数据，同时证验证用户的身份凭证及应用场景，预计待验证用户的身份查询信息，对所述用户信息安全及登录风险进行评估，判断所述用户是否登录；

数据收集模块，收集用户的登录数据，积累所述用户数据，提高用以下次登录的对比时间；

发送模块，发送短信验证码至所述用户终端，通过智能外呼系统向所述用户发起语音通话；

第二接收模块，接收用户所述短信验证码，同时接收用户的语音播报；

第二验证模块，验证所述短信验证码及所述语音播报验证码，判断用户数据的准确性，多种验证方式，便于所述用户登录。

9.一种电子设备，包括：

一个或多个处理器；

存储装置，其上存储有一个或多个程序；

当所述一个或多个程序被所述一个或多个处理器执行，使得所述处理器实现如权利要求1至7任意一项所述的方法。

10.一种计算机存储介质，其上存储有计算机程序，其中，所述计算机程序被处理器执行时实现如权利要求1至7任意一项所述的方法。

电商平台身份验证的方法、装置、电子设备及存储介质

技术领域

[0001] 本申请涉及计算机技术领域，具体而言，涉及一种电商平台身份验证的方法、装置、设备及存储介质。

背景技术

[0002] 在目前的电商技术领域中，电商平台需对用户的身份进行验证便于用户进行登录。

[0003] 如图1所示，在相关技术中，通过互联网平台的方式进行电子上午运作，现今的用户通过多种用户端登录电商终端然后进行商务活动，这一过程中，用户登录电商终端，易发生盗号或验证信息错误等请况，需提高用户使用用户终端登录电商终端的安全性，及用户登录的便利性。

发明内容

[0004] 本申请的内容部分用于以简要的形式介绍构思，这些构思将在后面的具体实施方式部分被详细描述。本申请的内容部分并不旨在标识要求保护的技术方案的关键特征或必要特征，也不旨在用于限制所要求的保护的技术方案的范围。

[0005] 本申请的一些实施例提出了电商平台身份验证方法、装置、电子设备和计算机存储介质，来解决以上背景技术部分提到的技术问题。

[0006] 作为本申请的第一方面，本申请的一些实施例提供了一种电商平台身份验证方法，包括：电商终端响应用户的身份识别操作获取用户发出的信息。

[0007] 其中，用户可通过用户终端进行登录操作，连接所述电商终端，通过所述用户终端进行面部或指纹识别，上传用户的登录数据。

[0008] 所述电商终端接收所述用户数据，将所述用户数据上传至云终端，读取所述云终端的数据，由所述云终端的数据库与所述用户数据进行对比。

[0009] 使用所述云终端储存数据，节省数据的储存陈本。

[0010] 基于所述用户数据与所述云终端数据的对比，同时将待验证用户的身份凭证及应用场景，预计待验证所述用户的身份查询信息发送至安全服务器。

[0011] 所述用户数据包括用户的登录信息、登录地点及登录时连接的网络。

[0012] 所述安全服务器检测所述用户信息安全及登录风险进行评估，并将评估信息发送至所述电商终端。

[0013] 所述安全服务器，检测用户信息与所述云终端数据的对比结果，评估所述用户登录地点和连接的网络，防止通过同一网络对所述用户发生盗号等行。

[0014] 所述电商终端接收评估结果进行身份验证。

[0015] 所述身份验证通过时，基于所述身份验证信息结果允许用户进行登录操作。

[0016] 同时将用户的登录信息及验证过程中的用户数据上传至所述云终端，获得登录记录。

[0017] 其中，所述电商终端使用户登入，所述用户数据上传至所述云终端后，增加所述云终端中的数据，便于所述用户下次登录时进行数据对比，提高用户的登录速度，减少用户的等待时间。

[0018] 所述身份验证未通过后，用户利用其他登录防止进行二次信息确认。

[0019] 所述安全服务器接收二次身份验证指令。

[0020] 增加二次登入机会，防止所述用户对比数据发生错误，造成用户无法登录。

[0021] 由所述安全服务器进行二次身份验证安全性更高。

[0022] 所述安全服务器发送短信验证码或语音验证码至用户终端上，所述用户终端接收所述安全服务器发送的所述短信验证码或语音验证码，并将收到的所述短信验证码或语音验证码输入至所述电商终端中。

[0023] 所述电商终端将接收的用户验证数据发送至所述安全服务器，由所述安全服务器进行验证，提高验证效率。

[0024] 其中，所述语音验证利用智能外呼系统向所述用户发起语音通话。

[0025] 当所述用户接通所述语音通话后，向所述电商终端播报所述身份验证结果。

[0026] 所述二次登录信息通过时，基于所述二次身份验证信息结构允许所述用户进行登录操作。

[0027] 所述用户登录完成后，所述电商终端将所述二次身份验证信息及登录信息上传子所述云终端与安全服务器中，由所述云终端记录用户登记记录，下次所述用户登录时，提高所述云终端对比效率。

[0028] 所述二次登录信息未通过时，拒绝用户登录，并将此次用户登录信息上传至安全服务器。

[0029] 其中，所述安全服务器将此次登录标记为危险登录信息，与下次登录进行对比，提高危险登录的分辨效率。

[0030] 作为本申请的第二方面，本申请的一些实施例提供了一种电商平台身份验证装置，包括：第一接收模块，接收所述用户终端中的登录数据，可接收手机终端及计算机终端多种终端的数据，适用范围更广泛。

[0031] 云终端，用以储存用户的数据，在所述云终端内搜索所述用户数据的对比数据。

[0032] 第一验证模块，验证所述用户数据及对比数据，同时证验证用户的身份凭证及应用场景，预计待验证用户的身份查询信息，对所述用户信息安全及登录风险进行评估，判断所述用户是否登录。

[0033] 数据收集模块，收集用户的登录数据，积累所述用户数据，提高用以下次登录的对比时间。

[0034] 发送模块，发送短信验证码至所述用户终端，通过智能外呼系统向所述用户发起语音通话。

[0035] 第二接收模块，接收用户所述短信验证码，同时接收用户的语音播报。

[0036] 第二验证模块，验证所述短信验证码及所述语音播报验证码，判断用户数据的准确性，多种验证方式，便于所述用户登录。

[0037] 作为本申请的第三方面，本申请的一些实施例提供了一种电子设备，包括：一个或多个处理器；存储装置，其上存储有一个或多个程序，当一个或多个程序被一个或多个处理

器执行，使得一个或多个处理器实现上述第一方面任一实现方式所描述的方法。

[0038] 作为本申请的第四方面，本申请的一些实施例提供了一种计算机存储介质，其上存储有计算机程序，其中，程序被处理器执行时实现上述第一方面任一实现方式所描述的方法。

[0039] 本申请的有益效果在于：一种电商平台身份验证的方法、装置、设备和存储介质，电商终端相应用户的身份识别操作，进而获取用户发出的登录信息，用户可通过不同的用户终端进行登录操作，可使用手机、电脑等获取用户的人像或指纹进行登录，适用范围更广泛；电商终端接收用户数据并传输至云终端，与云终端内部的数据进行对比，对比完成后获得对比结果，由电商客户端将对比数据用户的身份凭证，应用场景待验证的身份查询信息发送至安全服务器中，由安全服务器进行验证，对用户的登录风险进行评估，电商终端接收身份验证信息，防止他人进行登录，多重验证保护，安全性更高；身份验证结果通过，基于身份验证允许用户进行登录操作，同时将用户登录信息上传至云终端，记录用户的登录历史，身份验证结果不通过时，利用其他防止进行二次信息确认，二次信息确认可通过短信验证码或语音验证码发送至用户终端中，由安全服务器接收并验证短信验证码或语音，二次登录信息通过后，允许用户登录操作由安全服务器记录此次用户登录记录，并进行重点标注，二次登录信息未通过后，拒绝用户登录，并将此次登录信息上传至安全服务器，标记为危险登录，进而提高用户登录的安全性。

[0040] 更具体而言，本申请一些实施例可能产生如下的具体有益效果：

1.用户可通过多种用户终端进行登录，包括手机或电脑等，使用更便利，操作更简单；

2.用户通过面部识别或指纹识别进行登录，上传登录数据，面部或指纹识别操作较为简单，登录效率更高。

[0041] 3.电商终端将用户数据传输至云终端进行匹配，云终端储存数据使用成本数据较低。

[0042] 4.安全服务器结合对比数据，登录环境对用户登录风险进行评估，进而控制用户是否进行登录，可控制环境风险，防止发生盗号等。

[0043] 5.身份验证结果为通过时可进行二次登录，通过短信验证码或语音验证码进行身份验证，二次验证为通过后将此次用户登录信息上传至安全服务器，并标记为危险登录，可为下次提供登录对比数据，提高用户帐号的安全性。

附图说明

[0044] 构成本申请的一部分的附图用来提供对本申请的进一步理解，使得本申请的其它特征、目的和优点变得更明显。本申请的示意性实施例附图及其说明用于解释本申请，并不构成对本申请的不当限定。

[0045] 另外，贯穿附图中，相同或相似的附图标记表示相同或相似的元素。应当理解附图是示意性的，元件和元素不一定按照比例绘制。

[0046] 在附图中：

图1是本申请的一些实施例的电商平台身份验证方法的应用场景的示意图；

图2是根据本申请一种实施例的电商平台身份验证方法的流程图；

图3是根据本申请一种实施例的电商平台身份验证方法的一部分步骤的流程图；

图4是根据本申请一种实施例的电商平台身份验证装置的结构图；

图5是根据本申请一种实施例的电商平台身份验证装置的结构图；

图6是根据本申请一种实施例的电子设备的结构示意图。

[0047] 图中附图标记的含义：

100、电商系统；101、用户终端；102、电商终端；103、云终端；104、安全服务器；

200、检测装置；201、第一接收模块；202、云终端；203、第一验证模块；204、数据手机模块；205、发送模块；206、第二接收模块；207、第二验证模块；

800、电子设备；801、处理装置；802、ROM；803、RAM；804、总线；805、I/O接口；806、输入装置；807、输出装置；808、存储装置；809、通信装置。

具体实施方式

[0048] 下面将参照附图更详细地描述本公开的实施例。虽然附图中显示了本公开的某些实施例，然而应当理解的是，本公开可以通过各种形式来实现，而且不应该被解释为限于这里阐述的实施例。相反，提供这些实施例是为了更加透彻和完整地理解本公开。应当理解的是，本公开的附图及实施例仅用于示例性作用，并非用于限制本公开的保护范围。

[0049] 另外还需要说明的是，为了便于描述，附图中仅示出了与有关发明相关的部分。在不冲突的情况下，本公开中的实施例及实施例中的特征可以相互组合。

[0050] 需要注意，本公开中提及的“第一”、“第二”等概念仅用于对不同的装置、模块或单元进行区分，并非用于限定这些装置、模块或单元所执行的功能的顺序或者相互依存关系。

[0051] 需要注意，本公开中提及的“一个”、“多个”的修饰是示意性而非限制性的，本领域技术人员应当理解，除非在上下文另有明确指出，否则应该理解为“一个或多个”。

[0052] 本公开实施方式中的多个装置之间所交互的消息或者信息的名称仅用于说明性的目的，而并不是用于对这些消息或信息的范围进行限制。

[0053] 下面将参考附图并结合实施例来详细说明本公开。

[0054] 一种实施例的电商平台身份验证方法

参照图1所示，本申请的电商平台身份验证方法由图1中100电商系统所执行，该电商系统100包括多个用户终端101、电商终端102、云终端103和安全服务器104，其中用户终端101、电商终端102、云终端103和安全服务器104可以构成基于有线通讯或无线通讯的数据交互。

[0055] 其中，电商终端可以被构造为一台PC终端，也可以被构造为诸如平板电脑、手机等其他智能终端设备。

[0056] 参照图2-3所示，本申请的一个实施例的电商平台身份验证方法方法，包括如下步骤：

优选的，电商终端响应用户的身份识别操作获取用户发出的信息，电商终端接收用户数据，将用户数据上传至云终端，读取云终端的数据，由云终端的数据库与用户数据进行对比。

[0057] 其中，响应用户点击身份验证选项的操作，在一些实施例中，用户可通过用户终端进行登录操作，连接电商终端，通过用户终端进行面部或指纹识别，上传用户的登录数据，

使用云终端储存数据，节省数据的储存陈本。

[0058] 优选的，基于用户数据与云终端数据的对比，同时将待验证用户的身份凭证及应用场景，预计待验证用户的身份查询信息发送至安全服务器，用户数据包括用户的登录信息、登录地点及登录时连接的网络，安全服务器检测用户信息安全及登录风险进行评估，并将评估信息发送至电商终端。

[0059] 在本实施方式中，上传将待验证用户的身份凭证，可以是待验证用户的人脸图像数据或指纹数据，对待验证用户的人脸图像数据或指纹数据进行比对，复合预先设置的对应特征后，对用户数据包括用户的登录信息、登录地点及登录时连接的网络，对用户的登入网路进行监测，防止危险程序或危险网络接用户的登录网络，并对用户登陆地点进行风险评估，检测是否发生过网络侵入的案例，进而对登录风险进行评估，在同时输送用户信息与云终端数据的对比结果。

[0060] 优选的，电商终端接收评估结果进行身份验证，身份验证通过时，基于身份验证信息结果允许用户进行登录操作，同时将用户的登录信息及验证过程中的用户数据上传至云终端，获得登录记录。

[0061] 其中，用户登入电商终端完成后，此时收集用户的登录信息，如：登录时间、登录地点、及登录时的风险评估，对用户的登录数据进行分类打包，上传至云终端，便于下次登录时进行下载对比，其中分类打包便于下次对比时选取数据，进而提高对比速度。

[0062] 电商终端使用户登入，用户数据上传至云终端后，增加云终端中的数据，便于用户下次登录时进行数据对比，提高用户的登录速度，减少用户的等待时间。

[0063] 优选的，身份验证未通过后，根据联系信息将身份验证结果发送给用户，用户利用其他登录防止进行二次信息确认，向用户终端输送二次身份验证信息，同时安全服务器接收二次身份验证指令。

[0064] 进一步，提示用户时候利用二次登入机会，若用户选择重新发起身份验证，则可执行用二次登入操作。若用户选择不重新发起身份验证，则不进行验证，可执行操作防止用户对比数据发生错误，造成用户无法登录，由安全服务器进行二次身份验证安全性更高，

优选的，安全服务器发送短信验证码或语音验证码至用户终端上，用户终端接收安全服务器发送的短信验证码或语音验证码，并将收到的短信验证码或语音验证码输入至电商终端中。

[0065] 其中，用于响应用户的身份验证操作，获取用户的联系信息，以及用户的人脸图像，电商终端将接收的用户验证数据发送至安全服务器，由安全服务器进行验证，提高验证效率，语音验证利用智能外呼系统向用户发起语音通话。当用户接通语音通话后，向电商终端播报身份验证结果。

[0066] 优选的，二次登录信息通过时，基于二次身份验证信息结构允许用户进行登录操作。

[0067] 进一步，用户登录完成后，电商终端将二次身份验证信息及登录信息上传子云终端与安全服务器中，由云终端记录用户登记记录，身份验证结果与身份验证过程中的人员信息相关联地存储，以获得身份验证记录，其中，人员信息包括用户的个人信息和业务人员的个人信息，下次用户登录时，提高云终端对比效率。

[0068] 优选的，二次登录信息未通过时，拒绝用户登录，并将此次用户登录信息上传至安

全服务器。

[0069] 进一步，其中，安全服务器将此次登录标记为危险登录信息，与下次登录进行对比，进行身份验证时，其身份验证结果为未通过。此时可以将被验证的业务人员的图像、用户的个人信息、身份验证结果、地点以及时间等信息相关联地存储，从而形成异常信息记录。若有用户仍然遭受损失，可以在必要时向有关部门提供材料，提高危险登录的分辨效率。

[0070] 参照图4-5所示，本申请的一个实施例的电商平台身份验证装置，包括：第一接收模块、云终端、第一验证模块、数据收集模块、发送模块、第二接收模块和第二验证模块，第一接收模块接收用户终端中的登录数据，可接收手机终端及计算机终端多种终端的数据，适用范围更广泛，云终端，用以储存用户的数据，在云终端内搜索用户数据的对比数据，以基于搜索结果获得身份验证结果。其中，当搜索到业务人员的注册人脸图像时，身份验证结果为通过，第一验证模块，验证用户数据及对比数据，同时证验证用户的身份凭证及应用场景，预计待验证用户的身份查询信息，对用户信息安全及登录风险进行评估，判断用户是否登录，数据收集模块，收集用户的登录数据，积累用户数据，提高用以下次登录的对比时间，发送模块，发送短信验证码至用户终端，通过智能外呼系统向用户发起语音通话，第二接收模块，接收用户短信验证码，通过语音通知的方式，将身份验证结果发送给用户包括：利用智能外呼系统向用户发起语音通话，第二验证模块，验证短信验证码及语音播报验证码，当用户接通语音通话后，播报身份验证结果。判断用户数据的准确性，多种验证方式，便于用户登录，基于身份验证结果获得业务人员的个人信息。将身份验证结果与身份验证过程中的人员信息相关联地存储，以获得身份验证记录，其中，人员信息包括用户的个人信息和业务人员的个人信息。

[0071] 参照图6所示，电子设备800可以包括处理装置(例如中央处理器、图形处理器等)801，其可以根据存储在只读存储器(ROM)802中的程序或者从存储装置808加载到随机访问存储器(RAM)803中的程序而执行各种适当的动作和处理。在RAM803中，还存储有电子设备800操作所需的各种程序和数据。处理装置801、ROM802以及RAM803通过总线804彼此相连。输入/输出(I/O)接口805也连接至总线804。

[0072] 通常，以下装置可以连接至I/O接口805：包括例如触摸屏、触摸板、键盘、鼠标、摄像头、麦克风、加速度计、陀螺仪等的输入装置806：包括例如液晶显示器(LCD)、扬声器、振动器等的输出装置807；包括例如磁带、硬盘等的存储装置808：以及通信装置809。通信装置809可以允许电子设备800与其他设备进行无线或有线通信以交换数据。

[0073] 虽然图6示出了具有各种装置的电子设备800，但是应理解的是，并不要求实施或具备所有示出的装置。可以替代地实施或具备更多或更少的装置。

[0074] 图6中示出的每个方框可以代表一个装置，也可以根据需要代表多个装置。

[0075] 特别地，根据本公开的一些实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本公开的一些实施例包括一种计算机程序产品，其包括承载在计算机存储介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的一些实施例中，该计算机程序可以通过通信装置809从网络上被下载和安装，或者从存储装置808被安装，或者从ROM802被安装。在该计算机程序被处理装置801执行时，执行本公开的一些实施例的方法中限定的上述功能。

[0076] 需要说明的是,本公开的一些实施例上述的计算机存储介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——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。计算机可读存储介质的更具体的例子可以包括但不限于:具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0077] 在本公开的一些实施例中,计算机可读存储介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本公开的一些实施例中,计算机可读信号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,其中承载了计算机可读的程序代码。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。计算机可读信号介质还可以是计算机可读存储介质以外的任何计算机存储介质,该计算机可读信号介质可以发送、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。计算机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:电线、光缆、RF(射频)等等,或者上述的任意合适的组合。

[0078] 在一些实施方式中,客户端、服务器可以利用诸如HTTP(HyperTextTransferProtocol,超文本传输协议)之类的任何当前已知或未来研发的网络协议进行通信,并且可以与任意形式或介质的数字数据通信(例如,通信网络)互连。通信网络的示例包括局域网(“LAN”),广域网(“WAN”),网际网(例如,互联网)以及端对端网络(例如,adhoc端对端网络),以及任何当前已知或未来研发的网络。

[0079] 上述计算机存储介质可以是上述电子设备中所包含的:也可以是单独存在,而未装配入该电子设备中。上述计算机存储介质承载有一个或者多个程序,当上述一个或者多个程序被该电子设备执行时,使得该电子设备:接收用户终端中的登录数据,可接收手机终端及计算机终端多种终端的数据,适用范围更广泛,云终端用以储存用户的数据,在云终端内搜索用户数据的对比数据,第一验证模块验证用户数据及对比数据,于响应用户的身份验证操作,获取用户的联系信息,以及业务人员的人脸图像,同时证验证用户的身份凭证及应用场景,预计待验证用户的身份查询信息,对用户信息安全及登录风险进行评估,判断用户是否登录,当搜索到业务人员的注册人脸图像时,身份验证结果为通过。用于根据联系信息将身份验证结果发送给用户,提高验证效率,数据收集模块收集用户的登录数据,积累用户数据,提高用以下次登录的对比时间,发送模块发送短信验证码至用户终端,通过智能外呼系统向用户发起语音通话,第二接收模块接收用户短信验证码,同时接收用户的语音播报,第二验证模块验证短信验证码及语音播报验证码,判断用户数据的准确性,多种验证方式,便于用户登录。

[0080] 可以以一种或多种程序设计语言或其组合来编写用于执行本公开的一些实施例的操作的计算机程序代码,上述程序设计语言包括面向对象的程序设计语言—诸如Java、Smalltalk、C++,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机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服

务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)——连接到用户计算机，或者，可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0081] 附图中的流程图和框图，图示了按照本公开各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，该模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。

[0082] 也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。

[0083] 例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0084] 描述于本公开的一些实施例中的单元可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的单元也可以设置在处理器中，这些单元的名称在某种情况下并不构成对该单元本身的限定。

[0085] 本文中以上描述的功能可以至少部分地由一个或多个硬件逻辑部件来执行。例如，非限制性地，可以使用的示范类型的硬件逻辑部件包括：现场可编程门阵列(FPGA)、专用集成电路(ASIC)、专用标准产品(ASSP)、片上系统(SOC)、复杂可编程逻辑设备(CPLD)等等。

[0086] 以上描述仅为本公开的一些较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本公开的实施例中所涉及的发明范围，并不限于上述技术特征的特定组合而成的技术方案，同时也应涵盖在不脱离上述发明构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本公开的实施例中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

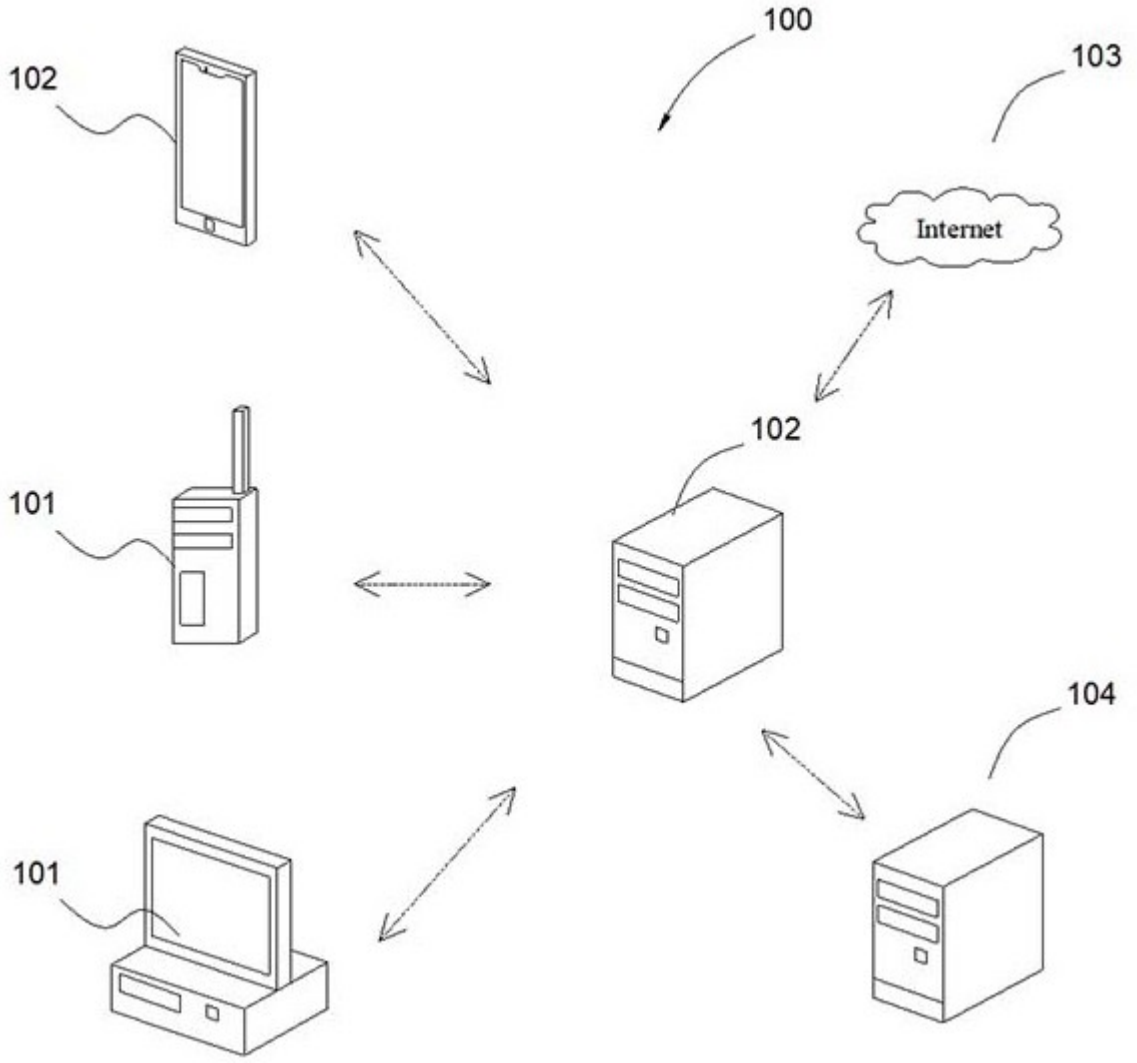


图1

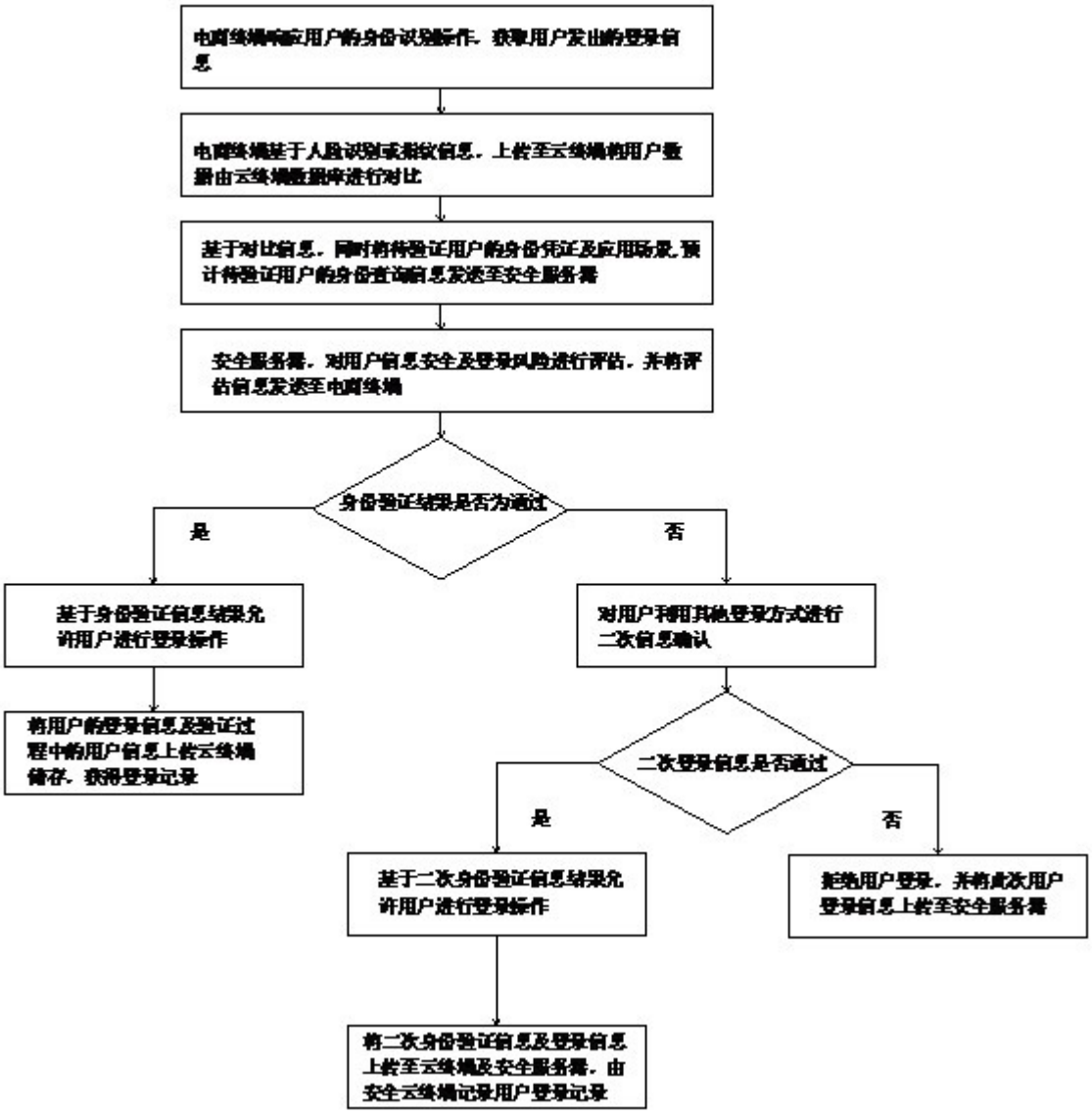

电商终端响应用户的身份识别操作，获取用户发出的登录信息
电商终端基于人脸识别或指纹信息，上传至云终端将用户数据由云终端数据库进行对比
基于对比信息，同时将待验证用户的身份凭证及应用场景，预计待验证用户的身份查询信息发送至安全服务器
安全服务器，对用户信息安全及登录风险进行评估，并将评估信息发送至电商终端
身份验证结果是否为通过
是
否
基于身份验证信息结果允许用户进行登录操作
将用户的登录信息及验证过程中的用户信息上传云终端储存，获得登录记录
对用户利用其他登录方式进行二次信息确认
二次登录信息是否通过
是
否
基于二次身份验证信息结果允许用户进行登录操作
拒绝用户登录，并将此次用户登录信息上传至安全服务器
将二次身份验证信息及登录信息上传至云终端及安全服务器，由安全云终端记录用户登录记录

图2

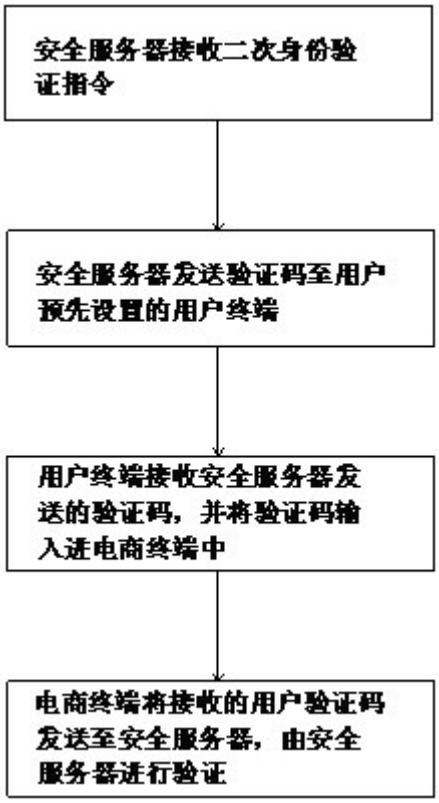

安全服务器接收二次身份验证指令
安全服务器发送验证码至用户预先设置的用户终端
用户终端接收安全服务器发送的验证码，并将验证码输入进电商终端中
电商终端将接收的用户验证码发送至安全服务器，由安全服务器进行验证

图3

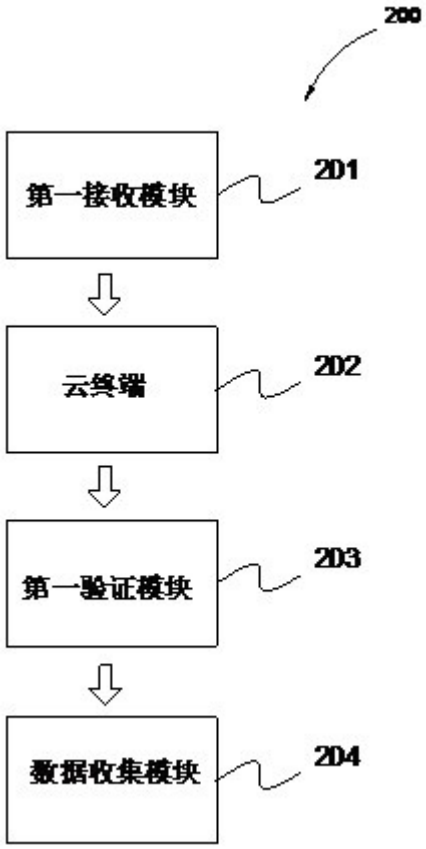

200
第一接收模块
201
云终端
202
第一验证模块
203
数据收集模块
204

图4

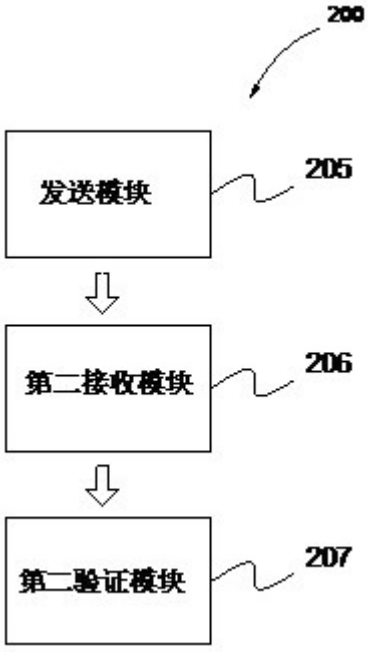

200
发送模块
205
第二接收模块
206
第二验证模块
207

图5

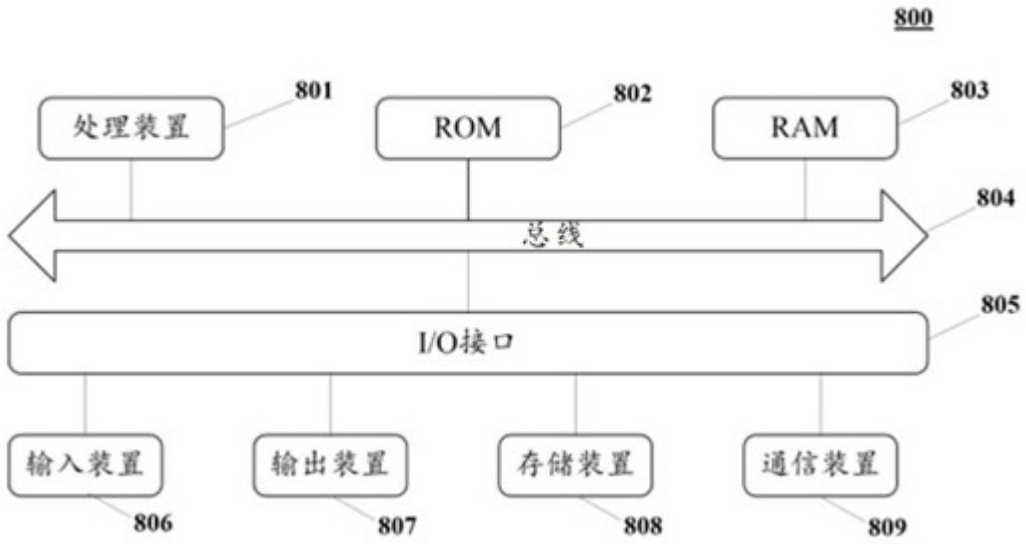

800
处理装置
801
ROM
802
RAM
803
804
总线
805
I/O接口
输入装置
806
输出装置
807
存储装置
808
通信装置
809

图6