



(12) 发明专利申请

(10) 申请公布号 CN 113259342 A

(43) 申请公布日 2021.08.13

(21) 申请号 202110511137.3

(22) 申请日 2021.05.11

(71) 申请人 鸬鹚科技(深圳)有限公司

地址 518000 广东省深圳市前海深港合作区南山街道前海青年梦工场5号楼305

(72) 发明人 陈旃

(74) 专利代理机构 深圳市世联合知识产权代理有限公司 44385

代理人 姜妍

(51) Int. Cl.

H04L 29/06 (2006.01)

H04L 29/08 (2006.01)

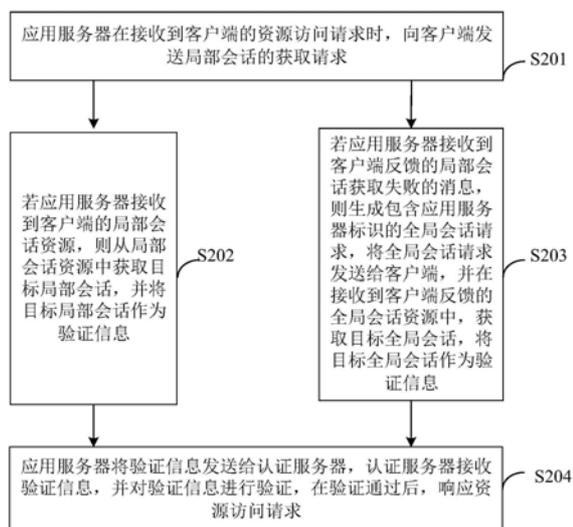
权利要求书2页 说明书8页 附图3页

(54) 发明名称

登录验证方法、装置、计算机设备及介质

(57) 摘要

本发明公开了一种登录验证方法、装置、设备及介质,包括:通过应用服务器在接收到客户端的资源访问请求时,向客户端发送局部会话的获取请求,若应用服务器接收到客户端的局部会话资源,则从局部会话资源中获取目标局部会话,并将目标局部会话作为验证信息,若应用服务器接收到客户端反馈的局部会话获取失败的消息,则生成包含应用服务器标识的全局会话请求,将全局会话请求发送给客户端,并在接收到客户端反馈的全局会话资源中,获取目标全局会话,将目标全局会话作为验证信息,应用服务器将验证信息发送给认证服务器,认证服务器接收验证信息,对验证信息进行验证,验证通过后,响应资源访问请求。采用本发明提高了多应用服务器登录验证的效率。



1. 一种登录验证方法,其特征在于,包括至少两个应用服务器和一个认证服务器,所述登录验证方法包括:

应用服务器在接收到客户端的资源访问请求时,向所述客户端发送局部会话的获取请求;

若所述应用服务器接收到所述客户端的局部会话资源,则从所述局部会话资源中获取目标局部会话,并将所述目标局部会话作为验证信息;

若所述应用服务器接收到所述客户端反馈的局部会话获取失败的消息,则生成包含应用服务器标识的全局会话请求,将所述全局会话请求发送给所述客户端,并在接收到所述客户端反馈的全局会话资源中,获取目标全局会话,将所述目标全局会话作为验证信息;

所述应用服务器将所述验证信息发送给所述认证服务器,所述认证服务器接收所述验证信息,并对所述验证信息进行验证,在验证通过后,响应所述资源访问请求。

2. 如权利要求1所述的登录验证方法,其特征在于,所述若所述应用服务器接收到所述客户端反馈的局部会话获取失败的消息,则生成包含应用服务器标识的全局会话请求,将所述全局会话请求发送给所述客户端,包括:

所述应用服务器获取所述认证服务器的初始访问地址;

结合所述初始访问地址和所述应用服务器标识,生成第一访问地址;

将所述第一访问地址发送给所述客户端,以使所述客户端采用所述第一访问地址对应的页面进行身份验证。

3. 如权利要求1所述的登录验证方法,其特征在于,在所述将所述全局会话请求发送给所述客户端之后,并且,在所述在接收到所述客户端反馈的全局会话资源中,获取目标全局会话之前,所述登录验证方法还包括:

若所述认证服务器接收到所述客户端的身份验证请求,则获取所述身份验证请求中包含的身份信息;

所述认证服务器对所述身份信息进行验证,在验证通过后,将所述身份验证结果写入到全局会话。

4. 如权利要求1至3任一项所述的登录验证方法,其特征在于,在所述应用服务器在接收到客户端的资源访问请求时,向所述客户端发送局部会话的获取请求之前,所述登录验证方法还包括:

配置所述认证服务器和每个所述应用服务器;

配置访问策略和关联信息,以使所述认证服务器与所述应用服务器关联认证。

5. 如权利要求4所述的登录验证方法,其特征在于,所述关联信息包括全限定域名FQDN、认证统一资源标志符和跳转统一资源标志符。

6. 一种登录验证装置,其特征在于,所述登录验证装置包括:

请求获取模块,用于应用服务器在接收到客户端的资源访问请求时,向所述客户端发送局部会话的获取请求;

第一信息获取模块,用于若所述应用服务器接收到所述客户端的局部会话资源,则从所述局部会话资源中获取目标局部会话,并将所述目标局部会话作为验证信息;

第二信息获取模块,用于若所述应用服务器接收到所述客户端反馈的局部会话获取失败的消息,则生成包含应用服务器标识的全局会话请求,将所述全局会话请求发送给所述

客户端,并在接收到所述客户端反馈的全局会话资源中,获取目标全局会话,将所述目标全局会话作为验证信息;

信息验证模块,用于所述应用服务器将所述验证信息发送给所述认证服务器,所述认证服务器接收所述验证信息,并对所述验证信息进行验证,在验证通过后,响应所述资源访问请求。

7.如权利要求6所述的登录验证装置,其特征在于,所述第二信息获取模块包括:

初始地址获取单元,用于所述应用服务器获取所述认证服务器的初始访问地址;

第一地址生成单元,用于结合所述初始访问地址和所述应用服务器标识,生成第一访问地址;

第一地址发送单元,用于将所述第一访问地址发送给所述客户端,以使所述客户端采用所述第一访问地址对应的页面进行身份验证。

8.如权利要求6所述的登录验证装置,其特征在于,所述登录验证装置还包括:

身份信息获取模块,用于若所述认证服务器接收到所述客户端的身份验证请求,则获取所述身份验证请求中包含的身份信息;

全局会话生成模块,用于所述认证服务器对所述身份信息进行验证,在验证通过后,将所述身份验证结果写入到全局会话。

9.一种计算机设备,包括存储器、处理器以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,其特征在于,所述处理器执行所述计算机程序时实现如权利要求1至5任一项所述的登录验证方法。

10.一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现如权利要求1至5任一项所述的登录验证方法。

登录验证方法、装置、计算机设备及介质

技术领域

[0001] 本发明涉及数据处理领域,尤其涉及一种登录验证方法、装置、计算机设备及介质。

背景技术

[0002] 随着经济的发展与计算机技术的飞速进步,越来越多的企业涉及多个子业务,并且通过网络为不同的子业务设置相应的业务站点页面,以便更好的服务客户,考虑到数据安全,需要对用户的身份进行认证,在进行多个子业务的页面访问时,往往需要对多个子业务进行多次重复认证,这使得登录验证效率较低。

发明内容

[0003] 本发明实施例提供一种登录验证方法、装置、计算机设备和存储介质,以多应用服务器的登录验证效率。

[0004] 为了解决上述技术问题,本申请实施例提供一种登录验证方法,包括:

[0005] 应用服务器在接收到客户端的资源访问请求时,向所述客户端发送局部会话的获取请求;

[0006] 若所述应用服务器接收到所述客户端的局部会话资源,则从所述局部会话资源中获取目标局部会话,并将所述目标局部会话作为验证信息;

[0007] 若所述应用服务器接收到所述客户端反馈的局部会话获取失败的消息,则生成包含应用服务器标识的全局会话请求,将所述全局会话请求发送给所述客户端,并在接收到所述客户端反馈的全局会话资源中,获取目标全局会话,将所述目标全局会话作为验证信息;

[0008] 所述应用服务器将所述验证信息发送给所述认证服务器,所述认证服务器接收所述验证信息,并对所述验证信息进行验证,在验证通过后,响应所述资源访问请求。

[0009] 可选地,所述若所述应用服务器接收到所述客户端反馈的局部会话获取失败的消息,则生成包含应用服务器标识的全局会话请求,将所述全局会话请求发送给所述客户端,包括:

[0010] 所述应用服务器获取所述认证服务器的初始访问地址;

[0011] 结合所述初始访问地址和所述应用服务器标识,生成第一访问地址;

[0012] 将所述第一访问地址发送给所述客户端,以使所述客户端采用所述第一访问地址对应的页面进行身份验证。

[0013] 可选地,在所述将所述全局会话请求发送给所述客户端之后,并且,在所述在接收到所述客户端反馈的全局会话资源中,获取目标全局会话之前,所述登录验证方法还包括:

[0014] 若所述认证服务器接收到所述客户端的身份验证请求,则获取所述身份验证请求中包含的身份信息;

[0015] 所述认证服务器对所述身份信息进行验证,在验证通过后,将所述身份验证结果

写入到全局会话。

[0016] 可选地,在所述应用服务器在接收到客户端的资源访问请求时,向所述客户端发送局部会话的获取请求之前,所述登录验证方法还包括:

[0017] 配置所述认证服务器和每个所述应用服务器;

[0018] 配置访问策略和关联信息,以使所述认证服务器与所述应用服务器关联认证。

[0019] 可选地,所述关联信息包括全限定域名FQDN、认证统一资源标志符和跳转统一资源标志符。

[0020] 为了解决上述技术问题,本申请实施例还提供一种登录验证装置,包括:

[0021] 请求获取模块,用于应用服务器在接收到客户端的资源访问请求时,向所述客户端发送局部会话的获取请求;

[0022] 第一信息获取模块,用于若所述应用服务器接收到所述客户端的局部会话资源,则从所述局部会话资源中获取目标局部会话,并将所述目标局部会话作为验证信息;

[0023] 第二信息获取模块,用于若所述应用服务器接收到所述客户端反馈的局部会话获取失败的消息,则生成包含应用服务器标识的全局会话请求,将所述全局会话请求发送给所述客户端,并在接收到所述客户端反馈的全局会话资源中,获取目标全局会话,将所述目标全局会话作为验证信息;

[0024] 信息验证模块,用于所述应用服务器将所述验证信息发送给所述认证服务器,所述认证服务器接收所述验证信息,并对所述验证信息进行验证,在验证通过后,响应所述资源访问请求。

[0025] 可选地,所述第二信息获取模块包括:

[0026] 初始地址获取单元,用于所述应用服务器获取所述认证服务器的初始访问地址;

[0027] 第一地址生成单元,用于结合所述初始访问地址和所述应用服务器标识,生成第一访问地址;

[0028] 第一地址发送单元,用于将所述第一访问地址发送给所述客户端,以使所述客户端采用所述第一访问地址对应的页面进行身份验证。

[0029] 可选地,所述登录验证装置还包括:

[0030] 身份信息获取模块,用于若所述认证服务器接收到所述客户端的身份验证请求,则获取所述身份验证请求中包含的身份信息;

[0031] 全局会话生成模块,用于所述认证服务器对所述身份信息进行验证,在验证通过后,将所述身份验证结果写入到全局会话。

[0032] 可选地,所述登录验证装置还包括:

[0033] 第一配置模块,用于配置所述认证服务器和每个所述应用服务器;

[0034] 第二配置模块,用于配置访问策略和关联信息,以使所述认证服务器与所述应用服务器关联认证。

[0035] 为了解决上述技术问题,本申请实施例还提供一种计算机设备,包括存储器、处理器以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上述登录验证方法的步骤。

[0036] 为了解决上述技术问题,本申请实施例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计算机程序,所述计算机程序被处理器执行时实现上述登录验证

方法的步骤。

[0037] 本发明实施例提供的登录验证方法、装置、计算机设备及存储介质,通过应用服务器在接收到客户端的资源访问请求时,向客户端发送局部会话的获取请求,若应用服务器接收到客户端的局部会话资源,则从局部会话资源中获取目标局部会话,并将目标局部会话作为验证信息,若应用服务器接收到客户端反馈的局部会话获取失败的消息,则生成包含应用服务器标识的全局会话请求,将全局会话请求发送给客户端,并在接收到客户端反馈的全局会话资源中,获取目标全局会话,将目标全局会话作为验证信息,应用服务器将验证信息发送给认证服务器,认证服务器接收验证信息,并对验证信息进行验证,在验证通过后,响应资源访问请求。实现在不同应用服务器需要进行身份验证时,通过全局会话和局部会话快速获取验证信息进行验证,提高了多应用服务器登录验证的效率。

附图说明

[0038] 为了更清楚地说明本发明实施例的技术方案,下面将对本发明实施例的描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动性的前提下,还可以根据这些附图获得其他的附图。

[0039] 图1是本申请可以应用于其中的示例性系统架构图;

[0040] 图2是本申请的登录验证方法的一个实施例的流程图;

[0041] 图3是根据本申请的登录验证装置的一个实施例的结构示意图;

[0042] 图4是根据本申请的计算机设备的一个实施例的结构示意图。

具体实施方式

[0043] 除非另有定义,本文所使用的所有的技术和科学术语与属于本申请的技术领域的技术人员通常理解的含义相同;本文中在申请的说明书中所使用的术语只是为了描述具体的实施例的目的,不是旨在于限制本申请;本申请的说明书和权利要求书及上述附图说明中的术语“包括”和“具有”以及它们的任何变形,意图在于覆盖不排他的包含。本申请的说明书和权利要求书或上述附图中的术语“第一”、“第二”等是用于区别不同对象,而不是用于描述特定顺序。

[0044] 在本文中提及“实施例”意味着,结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例,也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是,本文所描述的实施例可以与其它实施例相结合。

[0045] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例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,本领域普通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。

[0046] 请参阅图1,如图1所示,系统架构100可以包括终端设备101、102、103,网络104和服务器105。网络104用以在终端设备101、102、103和服务器105之间提供通信链路的介质。网络104可以包括各种连接类型,例如有线、无线通信链路或者光纤电缆等等。

[0047] 用户可以使用终端设备101、102、103通过网络104与服务器105交互,以接收或发送消息等。

[0048] 终端设备101、102、103可以是具有显示屏并且支持网页浏览的各种电子设备,包括但不限于智能手机、平板电脑、电子书阅读器、MP3播放器(Moving Picture E界面显示perts Group Audio Layer III,动态影像专家压缩标准音频层面3)、MP4(Moving Picture E界面显示perts Group Audio Layer IV,动态影像专家压缩标准音频层面4)播放器、膝上型便携计算机和台式计算机等等。

[0049] 服务器105可以是提供各种服务的服务器,例如对终端设备101、102、103上显示的页面提供支持的后台服务器。

[0050] 需要说明的是,本申请实施例所提供的登录验证方法由服务器执行,所述服务器包括应用服务器和验证服务器,相应地,登录验证装置设置于服务器中。

[0051] 应该理解,图1中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要,可以具有任意数目的终端设备、网络和服务器,本申请实施例中的终端设备101、102、103具体可以对应的是实际生产中的应用系统。

[0052] 请参阅图2,图2示出本发明实施例提供一种登录验证方法,以该方法应用在图1中的服务端为例进行说明,详述如下:

[0053] S201:应用服务器在接收到客户端的资源访问请求时,向客户端发送局部会话的获取请求。

[0054] 具体地,在用户需要访问某个应用服务器中的资源时,通过客户端访问该应用服务器的资源对应的网址链接,生成关于该资源的资源访问请求,应用服务器在接收到客户端的资源访问请求时,向客户端发送局部会话的获取请求。

[0055] 其中,局部会话是指客户端与应用服务器之间建立的,并保持了客户端与应用服务器对应的服务的登录状态的会话,在每次登录应用服务器成功后,会生成一个局部会话,在后续判断登录权限时,只需在后台通过获取局部会话进行验证即可,而无需用户每次都进行登录操作。会话是指一个终端用户与交互系统进行通讯的过程。

[0056] 例如,在一具体实施方式中,用户使用客户端登录应用服务器A成功后,建立局部会话,由于http协议是非连接的,也即,浏览器读取完应用服务器A的一个页面信息的内容就中断了,在访问应用服务器A对应的另外一个页面信息时,通过验证局部会话即可实现用户的登录权限的验证,避免每次打开同一应用服务器的不同页面均需要进行登录的情况。

[0057] 应理解,应用服务器向客户端发送的局部会话请求中,包含有应用服务器的标识,因而,客户端在接收到该局部会话请求后,只会在缓存中查询带有该应用服务器标识的局部会话。

[0058] S202:若应用服务器接收到客户端的局部会话资源,则从局部会话资源中获取目标局部会话,并将目标局部会话作为验证信息。

[0059] 具体地,局部会话有效时,客户端基于应用服务器发送的局部会话的获取请求,将对应的局部会话资源发送给应用服务器,应用服务器接收到客户端的局部会话资源后,从局部会话资源中获取目标局部会话,并将目标局部会话作为验证信息。

[0060] 其中,目标局部会话是指与待访问的资源相关联的会话,应用服务器与客户端之间的局部会话,可以是一个,也可以是多个,在应用服务器与客户端之间的局部会话为多个

时,从多个局部会话中,选取待访问的资源相关的局部会话作为目标局部会话,用于后续的验证。

[0061] S203:若应用服务器接收到客户端反馈的局部会话获取失败的消息,则生成包含应用服务器标识的全局会话请求,将全局会话请求发送给客户端,并在接收到客户端反馈的全局会话资源中,获取目标全局会话,将目标全局会话作为验证信息。

[0062] 具体地,在客户端未缓存与应用服务器之间的局部会话,或者,缓存的局部会话失效时,应用服务器不能接收到客户端反馈的局部会话,此时,应用服务器将接收到获取失败的消息,此时,通过全局会话进行验证,具体为:应用服务器生成包含应用服务器标识的全局会话请求,将全局会话请求发送给客户端,并在接收到客户端反馈的全局会话资源中,获取目标全局会话,将目标全局会话作为验证信息。

[0063] 需要说明的是,步骤S202和步骤S203之间,没有必然的先后关系,其具体也可以是并列执行。

[0064] S204:应用服务器将验证信息发送给认证服务器,认证服务器接收验证信息,并对验证信息进行验证,在验证通过后,响应资源访问请求。

[0065] 本实施例中,通过应用服务器在接收到客户端的资源访问请求时,向客户端发送局部会话的获取请求,若应用服务器接收到客户端的局部会话资源,则从局部会话资源中获取目标局部会话,并将目标局部会话作为验证信息,若应用服务器接收到客户端反馈的局部会话获取失败的消息,则生成包含应用服务器标识的全局会话请求,将全局会话请求发送给客户端,并在接收到客户端反馈的全局会话资源中,获取目标全局会话,将目标全局会话作为验证信息,应用服务器将验证信息发送给认证服务器,认证服务器接收验证信息,并对验证信息进行验证,在验证通过后,响应资源访问请求。实现在不同应用服务器需要进行身份验证时,通过全局会话和局部会话快速获取验证信息进行验证,提高了多应用服务器登录验证的效率。

[0066] 在本实施例的一些可选的实现方式中,步骤S202中,若应用服务器接收到客户端反馈的局部会话获取失败的消息,则生成包含应用服务器标识的全局会话请求,将全局会话请求发送给客户端,包括:

[0067] 应用服务器获取认证服务器的初始访问地址;

[0068] 结合初始访问地址和应用服务器标识,生成第一访问地址;

[0069] 将第一访问地址发送给客户端,以使客户端采用第一访问地址对应的页面进行身份验证。

[0070] 在本实施例的一些可选的实现方式中,该登录验证方法还包括:

[0071] 若认证服务器接收到客户端的身份验证请求,则获取身份验证请求中包含的身份信息;

[0072] 认证服务器对身份信息进行验证,在验证通过后,将身份验证结果写入到全局会话。

[0073] 在本实施例的一些可选的实现方式中,步骤S201之前,该登录验证方法还包括:

[0074] 配置认证服务器和每个应用服务器;

[0075] 配置访问策略和关联信息,以使认证服务器与应用服务器关联认证。

[0076] 进一步地,所述关联信息包括全限定域名FQDN、认证统一资源标志符和跳转统一

资源标志符。

[0077] 需要说明的是,在配置过程中,对应用服务器设置虚拟服务,并使用域名访问虚拟服务,否则会出现访问拒绝的页面。

[0078] 本实施例中,通过预先对每个应用服务器和认证服务器进行配置,确定各种不同的访问策略,有利于提高登录验证的兼容性和稳健性。

[0079] 应理解,上述实施例中各步骤的序号的大小并不意味着执行顺序的先后,各过程的执行顺序应以其功能和内在逻辑确定,而不对本发明实施例的实施过程构成任何限定。

[0080] 图3示出与上述实施例登录验证方法一一对应的登录验证装置的原理框图。如图3所示,该登录验证装置包括请求获取模块31、第一信息获取模块32、第二信息获取模块33和信息验证模块34。各功能模块详细说明如下:

[0081] 请求获取模块31,用于应用服务器在接收到客户端的资源访问请求时,向客户端发送局部会话的获取请求;

[0082] 第一信息获取模块32,用于若应用服务器接收到客户端的局部会话资源,则从局部会话资源中获取目标局部会话,并将目标局部会话作为验证信息;

[0083] 第二信息获取模块33,用于若应用服务器接收到客户端反馈的局部会话获取失败的消息,则生成包含应用服务器标识的全局会话请求,将全局会话请求发送给客户端,并在接收到客户端反馈的全局会话资源中,获取目标全局会话,将目标全局会话作为验证信息;

[0084] 信息验证模块34,用于应用服务器将验证信息发送给认证服务器,认证服务器接收验证信息,并对验证信息进行验证,在验证通过后,响应资源访问请求。

[0085] 可选地,第二信息获取模块33包括:

[0086] 初始地址获取单元,用于应用服务器获取认证服务器的初始访问地址;

[0087] 第一地址生成单元,用于结合初始访问地址和应用服务器标识,生成第一访问地址;

[0088] 第一地址发送单元,用于将第一访问地址发送给客户端,以使客户端采用第一访问地址对应的页面进行身份验证。

[0089] 可选地,登录验证装置还包括:

[0090] 身份信息获取模块,用于若认证服务器接收到客户端的身份验证请求,则获取身份验证请求中包含的身份信息;

[0091] 全局会话生成模块,用于认证服务器对身份信息进行验证,在验证通过后,将身份验证结果写入到全局会话。

[0092] 可选地,登录验证装置还包括:

[0093] 第一配置模块,用于配置认证服务器和每个应用服务器;

[0094] 第二配置模块,用于配置访问策略和关联信息,以使认证服务器与应用服务器关联认证。

[0095] 关于登录验证装置的具体限定可以参见上文中对于登录验证方法的限定,在此不再赘述。上述登录验证装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中,也可以以软件形式存储于计算机设备中的存储器中,以便于处理器调用执行以上各个模块对应的操作。

[0096] 为解决上述技术问题,本申请实施例还提供计算机设备。具体请参阅图4,图4为本实施例计算机设备基本结构框图。

[0097] 所述计算机设备4包括通过系统总线相互通信连接存储器41、处理器42、网络接口43。需要指出的是,图中仅示出了具有组件连接存储器41、处理器42、网络接口43的计算机设备4,但是应理解的是,并不要求实施所有示出的组件,可以替代的实施更多或者更少的组件。其中,本技术领域技术人员可以理解,这里的计算机设备是一种能够按照事先设定或存储的指令,自动进行数值计算和/或信息处理的设备,其硬件包括但不限于微处理器、专用集成电路(Application Specific Integrated Circuit,ASIC)、可编程门阵列(Field-Programmable Gate Array,FPGA)、数字处理器(Digital Signal Processor,DSP)、嵌入式设备等。

[0098] 所述计算机设备可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。所述计算机设备可以与用户通过键盘、鼠标、遥控器、触摸板或声控设备等方式进行人机交互。

[0099] 所述存储器41至少包括一种类型的可读存储介质,所述可读存储介质包括闪存、硬盘、多媒体卡、卡型存储器(例如,SD或D界面显示存储器等)、随机访问存储器(RAM)、静态随机访问存储器(SRAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、可编程只读存储器(PROM)、磁性存储器、磁盘、光盘等。在一些实施例中,所述存储器41可以是所述计算机设备4的内部存储单元,例如该计算机设备4的硬盘或内存。在另一些实施例中,所述存储器41也可以是所述计算机设备4的外部存储设备,例如该计算机设备4上配备的插接式硬盘,智能存储卡(Smart Media Card,SMC),安全数字(Secure Digital,SD)卡,闪存卡(Flash Card)等。当然,所述存储器41还可以既包括所述计算机设备4的内部存储单元也包括其外部存储设备。本实施例中,所述存储器41通常用于存储安装于所述计算机设备4的操作系统和各类应用软件,例如电子文件的控制的程序代码等。此外,所述存储器41还可以用于暂时地存储已经输出或者将要输出的各类数据。

[0100] 所述处理器42在一些实施例中可以是中央处理器(Central Processing Unit,CPU)、控制器、微控制器、微处理器、或其他数据处理芯片。该处理器42通常用于控制所述计算机设备4的总体操作。本实施例中,所述处理器42用于运行所述存储器41中存储的程序代码或者处理数据,例如运行电子文件的控制的程序代码。

[0101] 所述网络接口43可包括无线网络接口或有线网络接口,该网络接口43通常用于在所述计算机设备4与其他电子设备之间建立通信连接。

[0102] 本申请还提供了另一种实施方式,即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界面显示程序,所述界面显示程序可被至少一个处理器执行,以使所述至少一个处理器执行如上述的登录验证方法的步骤。

[0103] 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,本申请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,空调器,或者网络设备等)执行本申请各个实施例所述的方法。

[0104] 显然,以上所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例,附图中给出了本申请的较佳实施例,但并不限制本申请的专利范围。本申请可以以许多不同的形式来实现,相反地,提供这些实施例的目的是使对本申请的公开内容的理解更加透彻全面。尽管参照前述实施例对本申请进行了详细的说明,对于本领域的技术人员来而言,其依然可以对前述各具体实施方式所记载的技术方案进行修改,或者对其中部分技术特征进行等效替换。凡是利用本申请说明书及附图内容所做的等效结构,直接或间接运用在其他相关的技术领域,均同理在本申请专利保护范围之内。

100

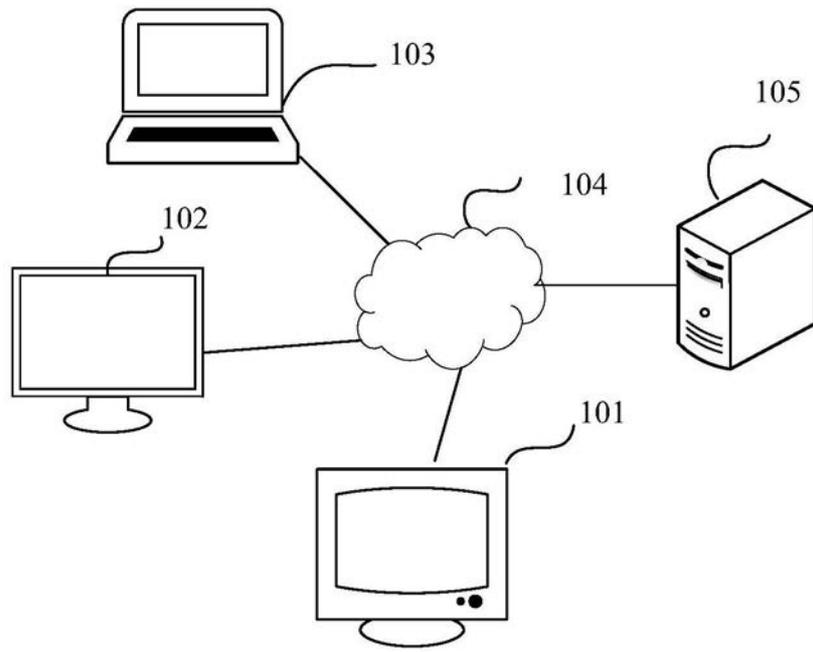


图1

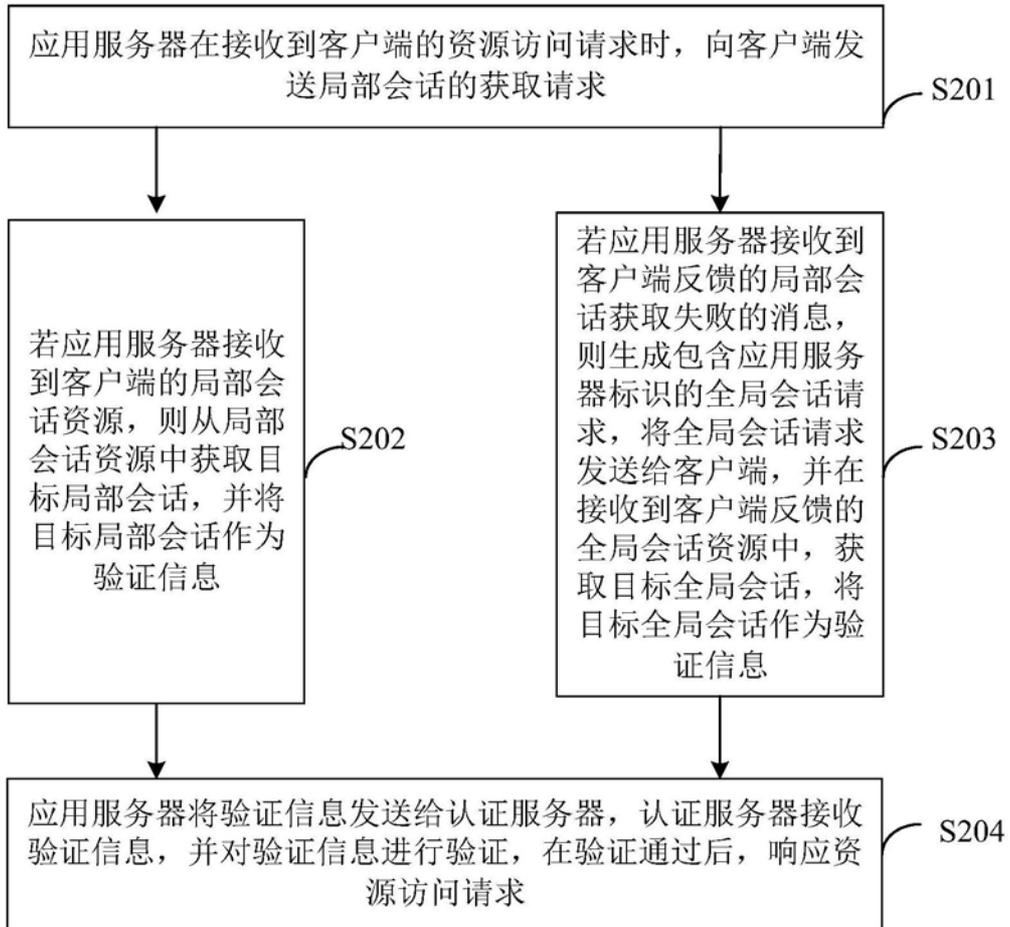


图2

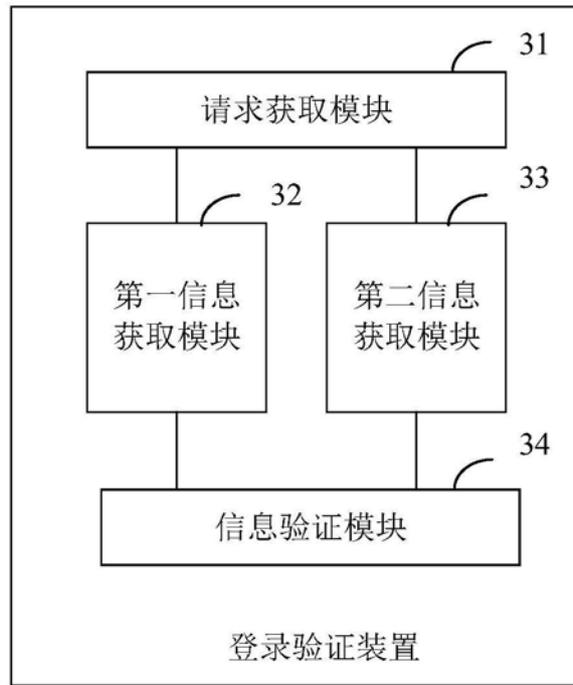


图3

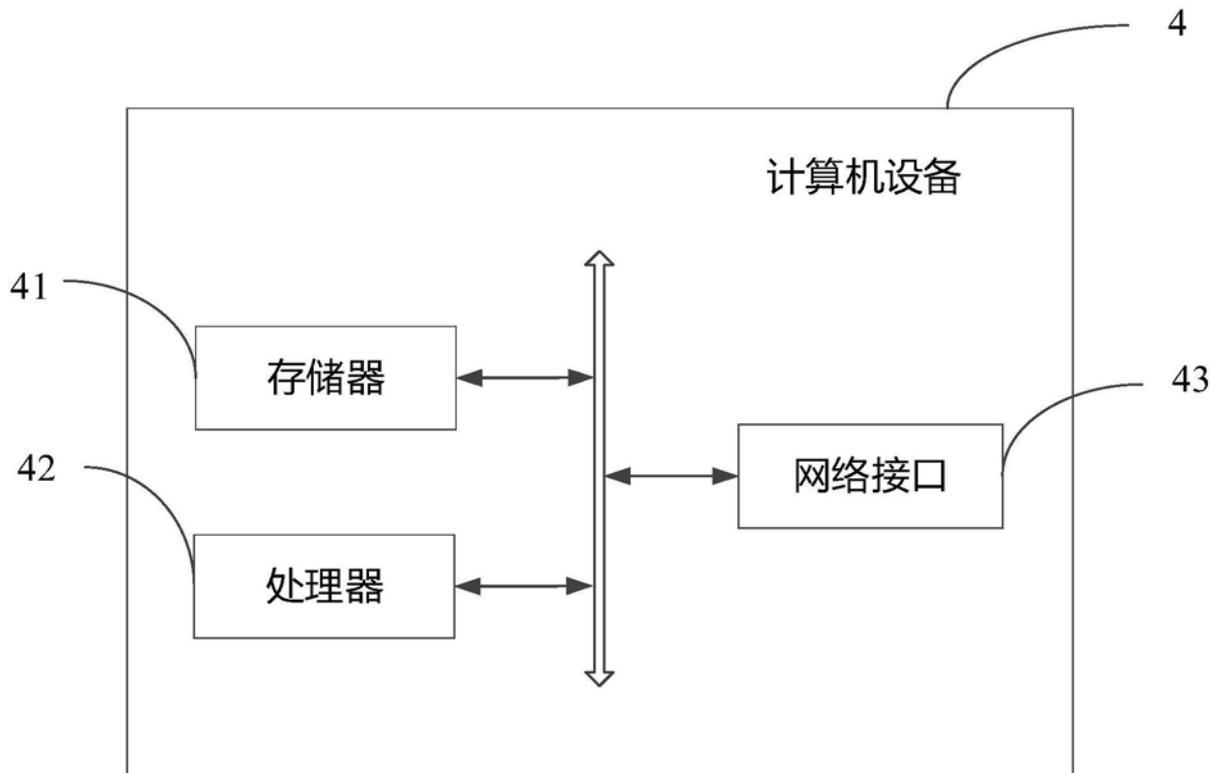


图4