(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104038503 A
(43)申请公布日 2014.09.10

(21)申请号 201410287564.8

(22)申请日 2014.06.24

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 奇智软件(北京)有限公司

(72)发明人 唐永刚

(74)专利代理机构 北京市浩天知识产权代理事务所 11276
代理人 宋菲 刘云贵

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

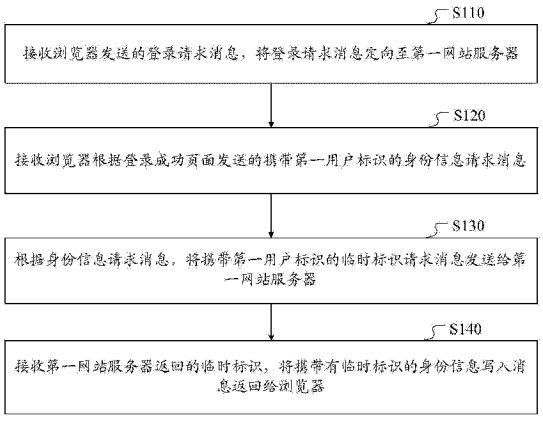
权利要求书2页 说明书11页 附图5页

(54)发明名称

跨网站登录的方法,装置和系统

(57)摘要

本发明公开了一种跨网站登录的方法,装置和系统,其中,方法包括:接收浏览器发送的登录请求消息,将登录请求消息定向至第一网站服务器,第一网站服务器接收浏览器发送的登录信息,根据登录信息获取第一用户标识,而后向浏览器返回第一用户标识和登录成功页面;浏览器根据登录成功页面发送携带第一用户标识的身份信息请求;第二网站服务器将携带第一用户标识的临时标识请求发送给第一网站服务器,之后,接收第一网站服务器根据第一用户标识生成临时标识,将临时标识返回给浏览器。根据该方案,不涉及多个临时身份信息的生成及验证接口,避免了复杂的授权过程简单,高效,并且服务器间的交互显著减少,能够降低业务故障率。



CN 104038503 A

1. 一种跨网站登录的方法，包括：

接收浏览器发送的登录请求消息，将所述登录请求消息定向至第一网站服务器，以供所述第一网站服务器接收所述浏览器发送的登录信息，根据所述登录信息获取第一用户标识，而后向所述浏览器返回所述第一用户标识和登录成功页面；

接收所述浏览器根据所述登录成功页面发送的携带所述第一用户标识的身份信息请求消息；

根据所述身份信息请求消息，将携带所述第一用户标识的临时标识请求消息发送给所述第一网站服务器，以供所述第一网站服务器根据所述第一用户标识生成临时标识；

接收所述第一网站服务器返回的所述临时标识，将携带有所述临时标识的身份信息写入消息返回给所述浏览器，以供所述浏览器将所述临时标识写入本地保存的身份信息中。

2. 根据权利要求 1 所述的方法，所述登录信息包含用户在所述第一网站服务器中已注册的登录用户名和登录密码；

所述根据登录信息获取第一用户标识进一步包括：

在所述第一网站服务器侧查找与所述登录用户名对应的第一用户标识；

若在所述第一网站服务器侧没有查找到与所述登录用户名对应的第一用户标识，则生成第一用户标识，并在所述第一网站服务器侧建立并保存所述登录用户名和所述第一用户标识的对应关系。

3. 根据权利要求 1 或 2 所述的方法，在所述接收浏览器根据所述登录成功页面发送的携带所述第一用户标识的身份信息请求消息之后还包括：

在第二网站服务器侧查找与所述第一用户标识对应的第二用户标识；

若在所述第二网站服务器侧没有查找到与所述第一用户标识对应的第二用户标识，则生成第二用户标识，并在所述第二网站服务器侧建立并保存所述第一用户标识和第二用户标识的对应关系。

4. 根据权利要求 3 所述的方法，在所述接收第一网站服务器返回的所述临时标识之后还包括：

在第二网站服务器侧建立并保存所述第二用户标识和所述临时标识的对应关系。

5. 根据权利要求 1-4 任一项所述的方法，在所述浏览器将临时标识写入本地保存的身份信息中之后还包括：

获取用户更新的第二网站服务器提供的一项或多项业务的配置信息，将所述更新的配置信息同步到云服务器中。

6. 一种跨网站登录装置，包括：

定向模块，适于接收浏览器发送的登录请求消息，将所述登录请求消息定向至第一网站服务器，以供所述第一网站服务器接收所述浏览器发送的登录信息，根据所述登录信息获取第一用户标识，而后向所述浏览器返回所述第一用户标识和登录成功页面；

请求接口模块，适于接收所述浏览器根据所述登录成功页面发送的携带所述第一用户标识的身份信息请求消息；

发送模块，适于根据所述身份信息请求消息，将携带所述第一用户标识的临时标识请求消息发送给所述第一网站服务器，以供所述第一网站服务器根据所述第一用户标识生成临时标识；

接收模块，接收所述第一网站服务器返回的所述临时标识，将携带有所述临时标识的身份信息写入消息返回给所述浏览器，以供所述浏览器将所述临时标识写入本地保存的身份信息中。

7. 根据权利要求 6 所述的装置，所述装置还包括：

查找模块，适于在第二网站服务器侧查找与所述第一用户标识对应的第二用户标识；

关联模块，适于在所述查找模块没有查找到与所述第一用户标识对应的第二用户标识时，生成第二用户标识，并在所述第二网站服务器侧建立并保存所述第一用户标识和第二用户标识的对应关系。

8. 根据权利要求 7 所述的装置，所述关联模块进一步适于：在第二网站服务器侧建立并保存所述第二用户标识和所述临时标识的对应关系。

9. 根据权利要求 6-8 任一项所述的装置，所述装置还包括：

同步模块，适于获取用户更新的第二网站服务器提供的一项或多项业务的配置信息，将所述更新的配置信息同步到云服务器中。

10. 一种跨网站登录系统，包括权利要求 6-10 任一项所述的跨网站登录装置，还包括：第一网站服务器；

所述第一网站服务器包括：

登录模块，接收所述浏览器发送的登录信息，根据所述登录信息获取第一用户标识，而后向所述浏览器返回所述第一用户标识和登录成功页面；

生成模块，接收所述发送模块发送的携带所述第一用户标识的临时标识请求消息，根据所述第一用户标识生成临时标识，返回给所述跨网站登录装置。

跨网站登录的方法，装置和系统

技术领域

[0001] 本发明涉及互联网技术领域，具体涉及一种跨网站登录的方法，装置和系统。

背景技术

[0002] 论坛，社区，社交网站等日益增多，用户在使用这些网站时通常需要注册及登录，以获取个性化服务和操作权限。各网站登录界面不同，同时，用户也需要经常变更用户名和密码，复杂的注册、登录过程可能造成用户的流失。

[0003] 为简化登录过程，出现了用第三方合作网站账号登录业务网站的方法，例如，登录百度个人中心时，可选择采用 qq 账号或新浪微博账号登录，登录后网站自动为用户分配一个用户名或用户 ID，并且经用户授权，登录网站还可以调用第三方的部分应用。

[0004] 现有技术中，一种实现上述登录的方法是使用 Oauth 协议，根据 Oauth 协议的规定，为保护用户信息的安全性，Oauth 过程较为复杂，涉及登录网站的服务器和第三方合作网站服务器之间的多次交互，多次生成 token 或临时 token，需要复杂的接口实现，有时会过于繁琐。例如，同一互联网公司可能提供多个业务网站，并具有统一的用户中心系统网站，用户中心系统网站和其他业务网站不在同一个域名下，经常需要用户中心账号登录业务网站，这种情况下，对安全性要求较低，使用 Oauth 过程会过于复杂，效率不高。

发明内容

[0005] 鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的跨网站登录的方法，装置和系统。

[0006] 根据本发明的一个方面，提供了一种跨网站登录的方法，包括 ：接收浏览器发送的登录请求消息，将登录请求消息定向至第一网站服务器，以供第一网站服务器接收浏览器发送的登录信息，根据登录信息获取第一用户标识，而后向浏览器返回第一用户标识和登录成功页面 ；接收浏览器根据登录成功页面发送的携带第一用户标识的身份信息请求消息 ；根据身份信息请求消息，将携带第一用户标识的临时标识请求消息发送给第一网站服务器，以供第一网站服务器根据第一用户标识生成临时标识 ；接收第一网站服务器返回的所述临时标识，将携带有临时标识的身份信息写入消息返回给浏览器，以供浏览器将临时标识写入本地保存的身份信息中。

[0007] 根据本发明的另一方面，提供了一种跨网站登录装置，包括 ：定向模块，适于接收浏览器发送的登录请求消息，将登录请求消息定向至第一网站服务器，以供第一网站服务器接收浏览器发送的登录信息，根据登录信息获取第一用户标识，而后向浏览器返回第一用户标识和登录成功页面 ；请求接口模块，适于接收浏览器根据登录成功页面发送的携带第一用户标识的身份信息请求消息 ；发送模块，适于根据身份信息请求消息，将携带第一用户标识的临时标识请求消息发送给第一网站服务器，以供第一网站服务器根据第一用户标识生成临时标识 ；接收模块，接收第一网站服务器返回的临时标识，将携带有临时标识的身份信息写入消息返回给浏览器，以供浏览器将临时标识写入本地保存的身份信息中。

[0008] 根据本发明的另一个方面，提供了一种跨网站登录系统，包括上述的跨网站登录装置，还包括第一网站服务器；

[0009] 其中，第一网站服务器包括：登录模块，接收浏览器发送的登录信息，根据登录信息获取第一用户标识，而后向浏览器返回第一用户标识和登录成功页面；生成模块，接收发送模块发送的携带第一用户标识的临时标识请求消息，根据第一用户标识生成临时标识，返回给跨网站登录装置。

[0010] 根据本发明的跨网站登录方法，装置和系统，第二网站服务器的登录请求被定向至第一网站服务器，用户在第一网站服务器的登录页面输入第一网站的用户名和密码，第一网站服务器对用户名和密码进行验证，验证通过后向浏览器返回第一用户标识和登录成功页面，登录成功页面在客户端浏览器加载时，页面请求第二网站服务器根据生成 token 等临时身份信息，由于用户未使用第二网站的用户名密码，临时身份信息无法生成，第二网站服务器将第一用户标识返回第一网站服务器，第一网站服务器根据第一用户标识确定第一网站的用户名和密码，据此生成临时身份信息，传递给第二网站服务器，由第二网站服务器返回至浏览器，浏览器写入本地。之后，用户可使用该临时身份信息登录第二网站服务器。根据该方案，不涉及多个 token 等临时身份信息的生成及验证接口，避免了复杂的授权过程简单，高效，并且服务器间的交互显著减少，能够降低业务故障率。

[0011] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0012] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0013] 图 1 示出了根据本发明一个实施例的跨网站登录方法的流程图；

[0014] 图 2 示出了根据本发明另一个实施例的跨网站登录方法的流程图；

[0015] 图 3 示出了根据本发明另一个实施例的跨网站登录方法的流程图；

[0016] 图 4 示出了根据本发明一个实施例的跨网站登录装置的结构框图；

[0017] 图 5 示出了根据本发明另一个实施例的跨网站登录装置的结构框图；

[0018] 图 6 示出了根据本发明一个实施例的第一网站服务器的结构框图；

[0019] 图 7 示出了根据本发明一个实施例的跨网站登录系统的结构框图。

具体实施方式

[0020] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0021] 图 1 示出了根据本发明一个实施例的跨网站登录方法的流程图。

[0022] 用户在登录选择页面选择使用第一网站的用户名和密码登录第二网站，例如，用

户登录 360 浏览器个人中心时，选择使用人人账号登录。

[0023] 本发明中，第二网站即是用户要登录的业务网站，第一网站是授权合作网站，或同一服务商提供的不同域名网站。对于上文示例，360 浏览器个人中心为第二网站，人人网服务器为第一网站服务器。通过本发明中的方法，能够便捷地实现上述登录方式。

[0024] 本实施例描述了本发明的方法在第二网站服务器侧的执行过程，如图 1 所示，方法包括如下步骤：

[0025] 步骤 S110，接收浏览器发送的登录请求消息，将登录请求消息定向至第一网站服务器。

[0026] 第二网站服务器通过登录选择页面为用户提供登录类型选择。用户选择使用第一网站的用户名和密码登录后，浏览器向第二网站服务器发送登录请求消息，登录请求消息中包含用户选择的登录类型。

[0027] 第二网站服务器接收登录请求消息后，得知该登录请求为使用第一网站账号的登录请求，将该登录请求消息定向至第一网站服务器。

[0028] 步骤 S120，接收浏览器根据登录成功页面发送的携带第一用户标识的身份信息请求消息。

[0029] 具体地，在第二服务器执行该步骤前，浏览器与第一网站服务器间还有以下过程：

[0030] 经第二网站服务器定向后，浏览器跳转至第一网站服务器对应的登录页面。

[0031] 第一网站服务器利用该登录页面收集用户登录信息，例如，用户在页面中填写的用户名和密码等。

[0032] 第一网站服务器验证页面收集的登录信息后，根据登录信息生成第一用户标识。其中，第一用户标识包含用户名等登录信息，与用户名唯一对应。之后，将第一网站登录成功页面和第一用户标识返回给浏览器。

[0033] 浏览器向第二服务器请求生成身份信息，如 cookie 等。该身份信息可存入本地，用于记录、保持登录状态，。

[0034] 步骤 S130，根据身份信息请求消息，将携带第一用户标识的临时标识请求消息发送给第一网站服务器。

[0035] 第二网站服务器接收身份信息请求消息。网站服务器生成 cookie 等身份信息需要登录名和密码等登录信息。由于登录过程中未使用第二网站服务器的用户名和密码等登录信息，因此，第二网站服务器无法生成身份信息。

[0036] 第二网站服务器将带有第一用户标识的临时标识请求消息发送给第一网站服务器，第一网站服务器从第一用户标识中得到用户名等登录信息，生成临时标识，例如，生成一个 token，返回给第二网站服务器。

[0037] 步骤 S140，接收第一网站服务器返回的临时标识，将携带有临时标识的身份信息写入消息返回给浏览器。

[0038] 第二网站服务器将接收的 token 返回给浏览器后，浏览器写入本地 cookie 中，或存储在 session 中，可在后续的登录中使用。

[0039] 根据本发明上述实施例提供的方法，第二网站服务器的登录请求被定向至第一网站服务器，用户在第一网站服务器的登录页面输入第一网站的用户名和密码，验证通过后

向浏览器返回第一用户标识和登录成功页面，登录成功页面在客户端浏览器加载时，页面请求第二网站服务器根据生成 cookie 等身份信息，由于用户未使用第二网站的用户名密码，身份信息无法生成，第二网站服务器将第一用户标识返回第一网站服务器，第一网站服务器根据第一用户标识确定第一网站的用户名和密码，据此生成临时身份信息，传递给第二网站服务器，由第二网站服务器返回至浏览器，浏览器写入本地。之后，用户可使用该临时身份信息登录第二网站服务器。根据该方案，跨站登录不涉及多个 token 的生成及验证接口，避免了复杂的授权过程简单，高效，并且服务器间的交互显著减少，能够降低业务故障率。

[0040] 图 2 示出了根据本发明另一个实施例的跨网站登录方法的流程图，如图 2 所示，方法包括如下步骤：

[0041] 步骤 S210，接收用户的跨站登录请求，通过浏览器将该登录请求发送至第二网站服务器。

[0042] 第二网站服务器提供登录选择页面，用户选择使用第一网站的用户名和密码登录后，浏览器向第二网站服务器发送登录请求消息，登录请求中包含用户选择的登录类型，第二网站服务器根据登录类型，选择处理方式。

[0043] 步骤 S220，第二网站服务器接收登录请求后，将浏览器定向至第一网站服务器登录页面。

[0044] 第二网站服务器利用服务器端的重定向方法，例如，通过 HttpServletResponse 接口的 sendRedirect() 方法，将浏览器定向至第一网站服务器登录页面。

[0045] 定向后，浏览器跳转到第一网站的登录页面。

[0046] 步骤 S230，浏览器将第一网站登录页面接收的登录信息发送给第一网站服务器。

[0047] 登录信息包括用户名和密码，用户在第一网站登录页面中输入用户名和密码，由浏览器提交至第一网站服务器。

[0048] 步骤 S240，第一网站服务器验证登录信息，验证成功，执行步骤 S260，否则，执行步骤 S250。

[0049] 具体地，进行用户名和密码的验证。

[0050] 步骤 S250，第一网站服务器向浏览器返回登录失败页面。

[0051] 验证失败，返回登录失败界面，流程结束。

[0052] 步骤 S260，第一网站服务器侧查找与登录用户名对应的第一用户标识，若查找成功，执行步骤 S280，否则，执行步骤 S270。

[0053] 可选地，第一网站服务器为每个已注册用户分配一个用户标识，并与用户名等关联，保存在第一网站服务器侧。例如，分配一个 UID(User Identification)。第一用户标识与用户名等登录信息对应，可用于同步第一网站配置信息。

[0054] 该步骤为可选步骤。

[0055] 步骤 S270，生成第一用户标识并在第一网站服务器建立并保存登录用户名和第一用户标识的关系。

[0056] 若验证后的登录用户名没有第一用户标识，为登录用户名分配一个第一用户标识。

[0057] 第一用户标识中可以是与用户名唯一对应的 UID，或者根据自定义方式生成，例

如，可以使用用户名或用户名的编码作为第一用户标识，还可以在其中添加时间戳等信息，则每次使用第一网站账号登录，从第一网站服务器获得不同的第一用户标识，但从每个第一用户标识中都能够反向地获取用户名信息。

[0058] 步骤 S280，向浏览器返回登录成功页面以及第一用户标识。

[0059] 步骤 S290，浏览器向第二网站服务器发送身份信息请求消息，身份信息请求消息中带有第一用户标识。

[0060] 登录成功后，页面通过浏览器向第二网站服务器请求生成 cookie 等身份信息。

[0061] 具体地，浏览器请求第二网站服务器上的 cookie 生成接口，例如，该接口为第二网站服务器上的 php 脚本，浏览器将第一用户标识添加在 http 请求头中。

[0062] 请求 cookie 等身份信息的目的是在客户端保持登录状态，浏览器在 cookie 有效期内向第二网站服务器请求 URL 时，将 cookie 加入到 http 请求头中，服务器验证 cookie，在页面刷新等操作之后，仍然能够保持登录状态。

[0063] 第二服务器生成 cookie 需要获取本次登录的 token。

[0064] cookie 中还包括域、路径等信息，表明 cookie 的作用范围，由于上述的限制，第二网站的 cookie 只能由第二网站的服务器发送给浏览器。

[0065] 步骤 S2100，第二网站服务器查找与第一用户标识对应的第二用户标识，若查找成功，执行步骤 S2120，否则，执行步骤 S2110。

[0066] 使用第一网站账号登录第二网站后，第二网站服务将第一用户标识和第二用户标识绑定，第二用户标识可为用户在第二网站的用户 ID，与用户在第二网站的用户名唯一对应。

[0067] 具体地，可通过绑定用户名的方式建立第一用户标识和第二用户标识的关系。例如，在用户首次使用第一网站账号登录第二网站成功后，提示用户将将第一网站的用户名与用户在第二网站已有的用户名绑定。如果用户此时尚未在第二网站注册用户名，则执行步骤 S2100，自动为第二用户标识分配一个第二网站的用户 ID，之后，用户可选择为该 ID 设置一个用户名，完成绑定。

[0068] 步骤 S2110，第二网站服务器生成第二用户标识并在第二网站服务器侧建立并保存第一用户标识和第二用户标识的对应关系。

[0069] 通过步骤 S2100-S2110 查找或建立的用户标识间的关系可用于同步用户配置信息，详见步骤 S2170。

[0070] 步骤 S2120，第二网站服务器根据请求消息，将携带第一用户标识的临时标识请求消息发送给第一网站服务器。

[0071] 第二服务器生成 cookie 需要获取本次登录的 token，token 由服务器程序根据用户名等登录信息生成，由于登录过程中未使用第二网站服务器登录信息，因此，第二网站服务器无法生成 token。

[0072] 第二网站服务器将携带第一用户标识的 token 请求发送给第一网站服务器，由第一网站服务器生成 token。

[0073] 步骤 S2130，第一网站服务器根据临时标识请求消息中携带的第一用户标识，查询对应的登录用户名。

[0074] 根据保存的用户名和标识关系进行查询。

[0075] 步骤 S2140，第一网站服务器根据用户名和密码生成临时标识，并将临时标识返回给第二网站服务器。

[0076] 进一步地，为提高安全性，还可以在 token 中加入其他信息，例如，客户端 IP，有效时间等，例如，可以设置 token 在一个 session 有效，则每次按上述流程登录后，产生的 token 不同，并且导致之前的 token 失效。

[0077] 第二网站服务器从第一网站服务器获取 token，从自身获取其他信息，如域，路径等，生成 cookie。

[0078] token 还可以用于向第二网站服务器授权，例如，允许第二网站在第一网站发布分享信息等。

[0079] 步骤 S2150，第二网站服务器将临时标识返回给浏览器。

[0080] 步骤 S2160，浏览器将临时标识写在本地身份信息中。

[0081] 通过在 http 响应头中添加 set-cookie 将带有 token 的 cookie 返回给浏览器并通知浏览器写入本地 cookie。

[0082] 步骤 S2170，将用户在第二网站的配置信息更新到云服务器。

[0083] 通过步骤 S2100-S2110 中建立的第一用户标识和第二用户标识的关系，能够实现下述功能。

[0084] 记录用户使用第一网站账号登录第二网站后更新的第二网站服务器提供的一项或多项业务的配置信息，将配置信息同第二用户标识关联，同步到云服务器中；从云服务器获取与第二用户标识关联的配置信息，根据配置信息对业务进行设置后，返回给浏览器。

[0085] 用户使用第一网站账号登录第二网站后进行的设置信息，例如，导航，皮肤，消息状态等，可以同步给对应的第二网站账号。

[0086] 进一步地，还可以将用户在第一网站的配置信息通过云服务器同步给第二网站。

[0087] 例如，第一网站服务器为世界之窗浏览器用户中心，第二网站服务器为 360 安全浏览器用户中心，用户在世界之窗浏览器中进行了收藏夹，标签页等设置，用户使用该账号登录第二网站，或使用对应的第二网站账号登录第二网站时，将世界之窗浏览器中的收藏夹同步给 360 安全浏览器。

[0088] 根据本发明上述实施例提供的方法，跨站登录不涉及多个 token 的生成及验证接口，避免了复杂的授权过程简单，高效，并且服务器间的交互显著减少，能够降低业务故障率。通过第一用户标识和第二用户标识的绑定，实现了第一网站账号和第二网站账号之间的配置信息共享，为用户提供了便利。

[0089] 图 3 示出了根据本发明另一个实施例的跨网站登录方法的流程图，如图 3 所示，方法包括如下步骤：

[0090] 步骤 S310，根据第二网站服务器的登录请求定向，向浏览器返回第一网站服务器的登录页面。

[0091] 步骤 S320，接收浏览器发送的第三方登录页面中输入的登录信息并验证登录信息。

[0092] 步骤 S330，生成包含登录信息的第一用户标识，并向浏览器返回第一用户标识和第一网站登录成功页面。

[0093] 步骤 S340，接收第二网站服务器的携带第一用户标识的临时标识请求。

[0094] 步骤 S350，根据第一用户标识中的登录信息生成临时标识。

[0095] 步骤 S360，将生成的临时标识返回给第二网站服务器。

[0096] 步骤 S310-S360 在第一网站服务器侧执行，具体实施方式可参照上一实施例，此处不再赘述

[0097] 步骤 S370，第二网站服务器存储临时标识，通知浏览器将临时标识写入本地身份信息。

[0098] 将 token 存储在第二网站服务器的数据库中。

[0099] 该步骤还包括：在第二网站服务器侧建立并保存第二用户标识和临时标识的对应关系。

[0100] 步骤 S380，第二网站服务器接收携带临时标识的第二网站登录请求，利用保存的临时标识进行验证。

[0101] 浏览器将 token 写入本地身份信息 cookie 后，再次请求第二网站服务时，在请求中携带包含临时标识的身份信息，供第二网站验证。

[0102] 步骤 S390，验证通过后，返回第二网站登录后页面。

[0103] 根据上述方式，在临时标识有效期内，浏览器能够保持登录状态。

[0104] 图 4 示出了根据本发明一个实施例的一种跨网站登录装置的结构框图，如图 4 所示，装置包括：

[0105] 定向模块 410，适于接收浏览器发送的登录请求消息，将登录请求消息定向至第一网站服务器，以供第一网站服务器接收浏览器发送的登录信息，根据登录信息获取第一用户标识，而后向浏览器返回所述第一用户标识和登录成功页面。

[0106] 请求接口模块 420，适于接收浏览器根据登录成功页面发送的携带第一用户标识的身份信息请求消息。

[0107] 发送模块 430，适于根据身份信息请求消息，将携带第一用户标识的临时标识请求消息发送给第一网站服务器，以供第一网站服务器根据第一用户标识生成临时标识。

[0108] 接收模块 440，接收第一网站服务器返回的临时标识，将携带有临时标识的身份信息写入消息返回给浏览器，以供浏览器将临时标识写入本地保存的身份信息中。

[0109] 图 5 示出了根据本发明另一个实施例的跨网站登录装置的结构框图，如图 5 所示，装置包括：

[0110] 定向模块 510，适于接收浏览器发送的登录请求消息，将登录请求消息定向至第一网站服务器，以供第一网站服务器接收浏览器发送的登录信息，根据登录信息获取第一用户标识，而后向浏览器返回所述第一用户标识和登录成功页面。

[0111] 请求接口模块 520，适于接收浏览器根据登录成功页面发送的携带第一用户标识的身份信息请求消息。

[0112] 发送模块 530，适于根据身份信息请求消息，将携带第一用户标识的临时标识请求消息发送给第一网站服务器，以供第一网站服务器根据第一用户标识生成临时标识。

[0113] 接收模块 540，接收第一网站服务器返回的临时标识，将携带有临时标识的身份信息写入消息返回给浏览器，以供浏览器将临时标识写入本地保存的身份信息中。

[0114] 查找模块 550，适于在第二网站服务器侧查找与第一用户标识对应的第二用户标识；

[0115] 关联模块 560，适于在查找模块 550 没有查找到与第一用户标识对应的第二用户标识时，生成第二用户标识，并在第二网站服务器侧建立并保存所述第一用户标识和第二用户标识的对应关系。

[0116] 可选地，关联模块 560 进一步适于：在第二网站服务器侧建立并保存所述第二用户标识和所述临时标识的对应关系。

[0117] 可选地，装置还包括：同步模块 570，适于获取用户更新的第二网站服务器提供的一项或多项业务的配置信息，将更新的配置信息同步到云服务器中。

[0118] 图 6 示出了根据本发明一个实施例的第一网站服务器的结构框图，如图 6 所示，包括：

[0119] 登录模块 610，接收浏览器发送的登录信息，根据登录信息获取第一用户标识，而后向浏览器返回所述第一用户标识和登录成功页面。

[0120] 其中，登录信息包含用户在第一网站服务器中已注册的登录用户名和登录密码；登录模块 610 具体适于：在第一网站服务器侧查找与登录用户名对应的第一用户标识；若在第一网站服务器侧没有查找到与登录用户名对应的第一用户标识，则生成第一用户标识，并在第一网站服务器侧建立并保存所述登录用户名和第一用户标识的对应关系。

[0121] 生成模块 620，接收发送模块发送的携带第一用户标识的临时标识请求消息，根据第一用户标识生成临时标识，返回给跨网站登录装置。

[0122] 图 7 示出了根据本发明一个实施例的跨网站登录系统的结构框图，如图 7 所示，系统包括：

[0123] 上述的跨网站登录装置，以及第一网站服务器。

[0124] 根据本发明上述实施例提供的跨网站登录装置和系统，登录请求被定向至第一网站服务器，用户在第一网站服务器的登录页面输入第一网站的用户名和密码，第一网站服务器对用户名和密码进行验证，验证通过后向浏览器返回第一用户标识和登录成功页面，登录成功页面在客户端浏览器加载时，页面请求第二网站服务器生成 token 等临时身份信息，由于用户未使用第二网站的用户名密码，临时身份信息无法生成，第二网站服务器将第一用户标识返回第一网站服务器，第一网站服务器根据第一用户标识确定第一网站的用户名和密码，据此生成临时身份信息，传递给第二网站服务器，由第二网站服务器返回至浏览器，浏览器写入本地。之后，用户可使用该临时身份信息登录第二网站服务器。根据该方案，不涉及多个 token 等临时身份信息的生成及验证接口，避免了复杂的授权过程简单，高效，并且服务器间的交互显著减少，能够降低业务故障率。通过第一用户标识和第二用户标识的绑定，以及与云服务器的同步，实现了第一网站账号和第二网站账号之间的配置信息共享，为用户提供了便利。并且，在临时标识有效期内，浏览器能够保持登录状态。

[0125] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0126] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构

和技术，以便不模糊对本说明书的理解。

[0127] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0128] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和／或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0129] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0130] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的跨网站登录装置和系统中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0131] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0132] 本发明公开了：

[0133] A1、一种跨网站登录的方法，包括：

[0134] 接收浏览器发送的登录请求消息，将所述登录请求消息定向至第一网站服务器，

以供所述第一网站服务器接收所述浏览器发送的登录信息，根据所述登录信息获取第一用户标识，而后向所述浏览器返回所述第一用户标识和登录成功页面；

[0135] 接收所述浏览器根据所述登录成功页面发送的携带所述第一用户标识的身份信息请求消息；

[0136] 根据所述身份信息请求消息，将携带所述第一用户标识的临时标识请求消息发送给所述第一网站服务器，以供所述第一网站服务器根据所述第一用户标识生成临时标识；

[0137] 接收所述第一网站服务器返回的所述临时标识，将携带有所述临时标识的身份信息写入消息返回给所述浏览器，以供所述浏览器将所述临时标识写入本地保存的身份信息中。

[0138] A2、根据 A1 所述的方法，所述登录信息包含用户在所述第一网站服务器中已注册的登录用户名和登录密码；

[0139] 所述根据登录信息获取第一用户标识进一步包括：

[0140] 在所述第一网站服务器侧查找与所述登录用户名对应的第一用户标识；

[0141] 若在所述第一网站服务器侧没有查找到与所述登录用户名对应的第一用户标识，则生成第一用户标识，并在所述第一网站服务器侧建立并保存所述登录用户名和所述第一用户标识的对应关系。

[0142] A3、根据 A1 或 A2 所述的方法，在所述接收浏览器根据所述登录成功页面发送的携带所述第一用户标识的身份信息请求消息之后还包括：

[0143] 在第二网站服务器侧查找与所述第一用户标识对应的第二用户标识；

[0144] 若在所述第二网站服务器侧没有查找到与所述第一用户标识对应的第二用户标识，则生成第二用户标识，并在所述第二网站服务器侧建立并保存所述第一用户标识和第二用户标识的对应关系。

[0145] A4、根据 A3 所述的方法，在所述接收第一网站服务器返回的所述临时标识之后还包括：

[0146] 在第二网站服务器侧建立并保存所述第二用户标识和所述临时标识的对应关系。

[0147] A5、根据 A1-A4 任一项所述的方法，在所述浏览器将临时标识写入本地保存的身份信息中之后还包括：

[0148] 获取用户更新的第二网站服务器提供的一项或多项业务的配置信息，将所述更新的配置信息同步到云服务器中。

[0149] B6、一种跨网站登录装置，包括：

[0150] 定向模块，适于接收浏览器发送的登录请求消息，将所述登录请求消息定向至第一网站服务器，以供所述第一网站服务器接收所述浏览器发送的登录信息，根据所述登录信息获取第一用户标识，而后向所述浏览器返回所述第一用户标识和登录成功页面；

[0151] 请求接口模块，适于接收所述浏览器根据所述登录成功页面发送的携带所述第一用户标识的身份信息请求消息；

[0152] 发送模块，适于根据所述身份信息请求消息，将携带所述第一用户标识的临时标识请求消息发送给所述第一网站服务器，以供所述第一网站服务器根据所述第一用户标识生成临时标识；

[0153] 接收模块，接收所述第一网站服务器返回的所述临时标识，将携带有所述临时标

识的身份信息写入消息返回给所述浏览器，以供所述浏览器将所述临时标识写入本地保存的身份信息中。

[0154] B7、根据 B6 所述的装置，所述装置还包括：

[0155] 查找模块，适于在第二网站服务器侧查找与所述第一用户标识对应的第二用户标识；

[0156] 关联模块，适于在所述查找模块没有查找到与所述第一用户标识对应的第二用户标识时，生成第二用户标识，并在所述第二网站服务器侧建立并保存所述第一用户标识和第二用户标识的对应关系。

[0157] B8、根据 B7 所述的装置，所述关联模块进一步适于：在第二网站服务器侧建立并保存所述第二用户标识和所述临时标识的对应关系。

[0158] B9、根据 B6-B8 任一项所述的装置，所述装置还包括：

[0159] 同步模块，适于获取用户更新的第二网站服务器提供的一项或多项业务的配置信息，将所述更新的配置信息同步到云服务器中。

[0160] C10、一种跨网站登录系统，包括权利要求 6-10 任一项所述的跨网站登录装置，还包括：第一网站服务器；

[0161] 所述第一网站服务器包括：

[0162] 登录模块，接收所述浏览器发送的登录信息，根据所述登录信息获取第一用户标识，而后向所述浏览器返回所述第一用户标识和登录成功页面；

[0163] 生成模块，接收所述发送模块发送的携带所述第一用户标识的临时标识请求消息，根据所述第一用户标识生成临时标识，返回给所述跨网站登录装置。

[0164] C11、根据 C10 所述的系统，所述登录信息包含用户在所述第一网站服务器中已注册的登录用户名和登录密码；

[0165] 所述登录模块具体适于：在所述第一网站服务器侧查找与所述登录用户名对应的第一用户标识；

[0166] 若在所述第一网站服务器侧没有查找到与所述登录用户名对应的第一用户标识，则生成第一用户标识，并在所述第一网站服务器侧建立并保存所述登录用户名和所述第一用户标识的对应关系。

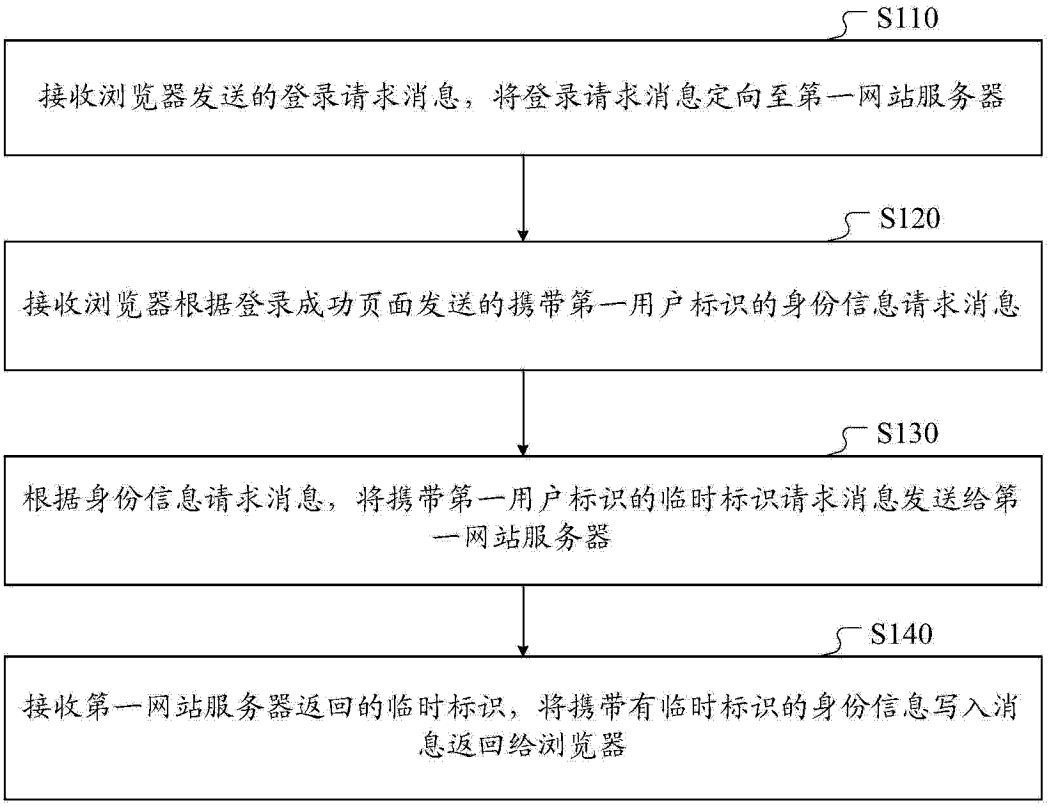

S110
接收浏览器发送的登录请求消息，将登录请求消息定向至第一网站服务器
S120
接收浏览器根据登录成功页面发送的携带第一用户标识的身份信息请求消息
S130
根据身份信息请求消息，将携带第一用户标识的临时标识请求消息发送给第一网站服务器
S140
接收第一网站服务器返回的临时标识，将携带有临时标识的身份信息写入消息返回给浏览器

图 1

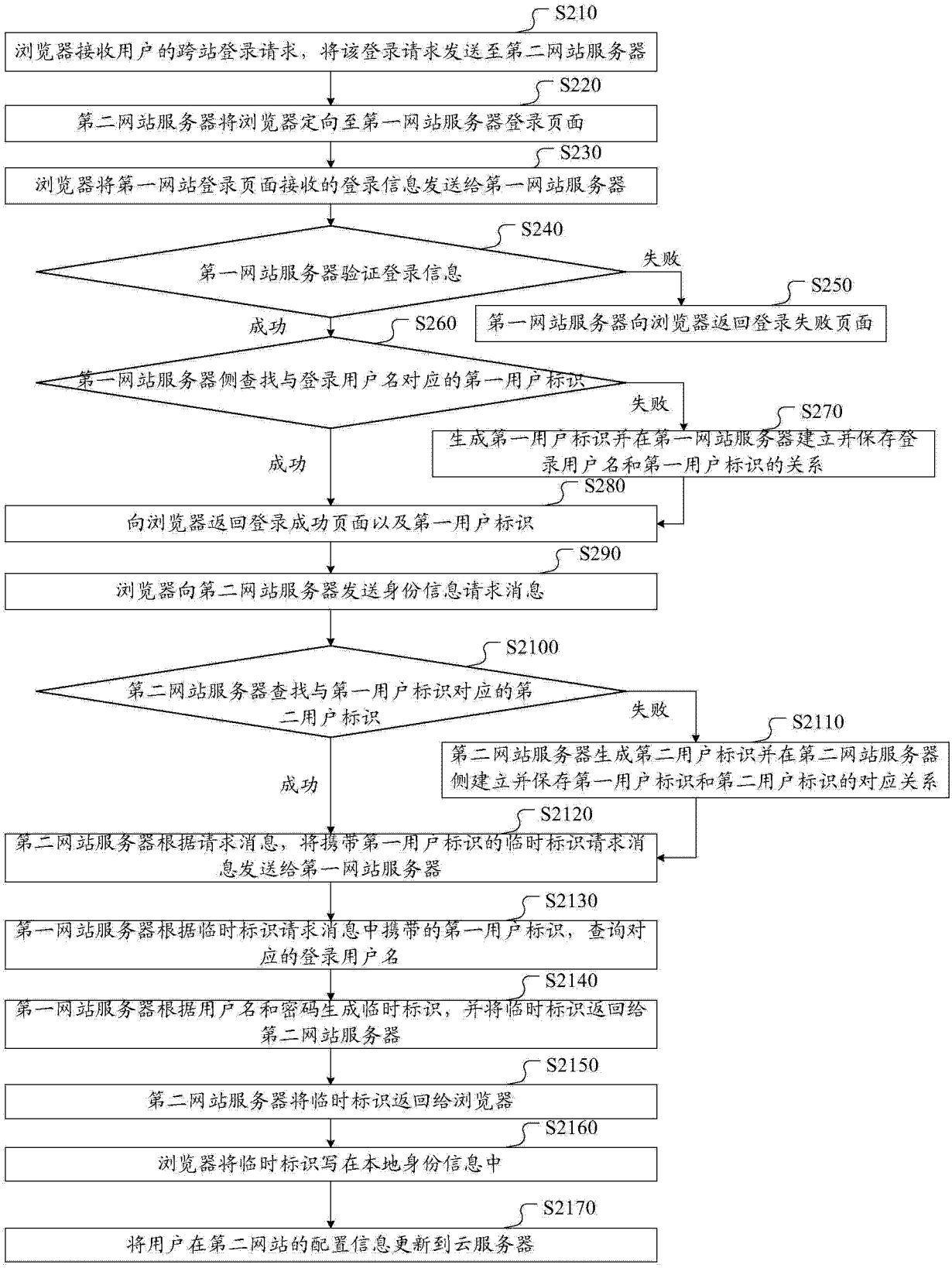

S210
浏览器接收用户的跨站登录请求，将该登录请求发送至第二网站服务器
S220
第二网站服务器将浏览器定向至第一网站服务器登录页面
S230
浏览器将第一网站登录页面接收的登录信息发送给第一网站服务器
S240
第一网站服务器验证登录信息
失败
S250
第一网站服务器向浏览器返回登录失败页面
成功
S260
第一网站服务器侧查找与登录用户名对应的第一用户标识
失败
S270
生成第一用户标识并在第一网站服务器建立并保存登录用户名和第一用户标识的关系
成功
S280
向浏览器返回登录成功页面以及第一用户标识
S290
浏览器向第二网站服务器发送身份信息请求消息
S2100
第二网站服务器查找与第一用户标识对应的第二用户标识
失败
S2110
第二网站服务器生成第二用户标识并在第二网站服务器侧建立并保存第一用户标识和第二用户标识的对应关系
成功
S2120
第二网站服务器根据请求消息，将携带第一用户标识的临时标识请求消息发送给第一网站服务器
S2130
第一网站服务器根据临时标识请求消息中携带的第一用户标识，查询对应的登录用户名
S2140
第一网站服务器根据用户名和密码生成临时标识，并将临时标识返回给第二网站服务器
S2150
第二网站服务器将临时标识返回给浏览器
S2160
浏览器将临时标识写在本地身份信息中
S2170
将用户在第二网站的配置信息更新到云服务器

图 2

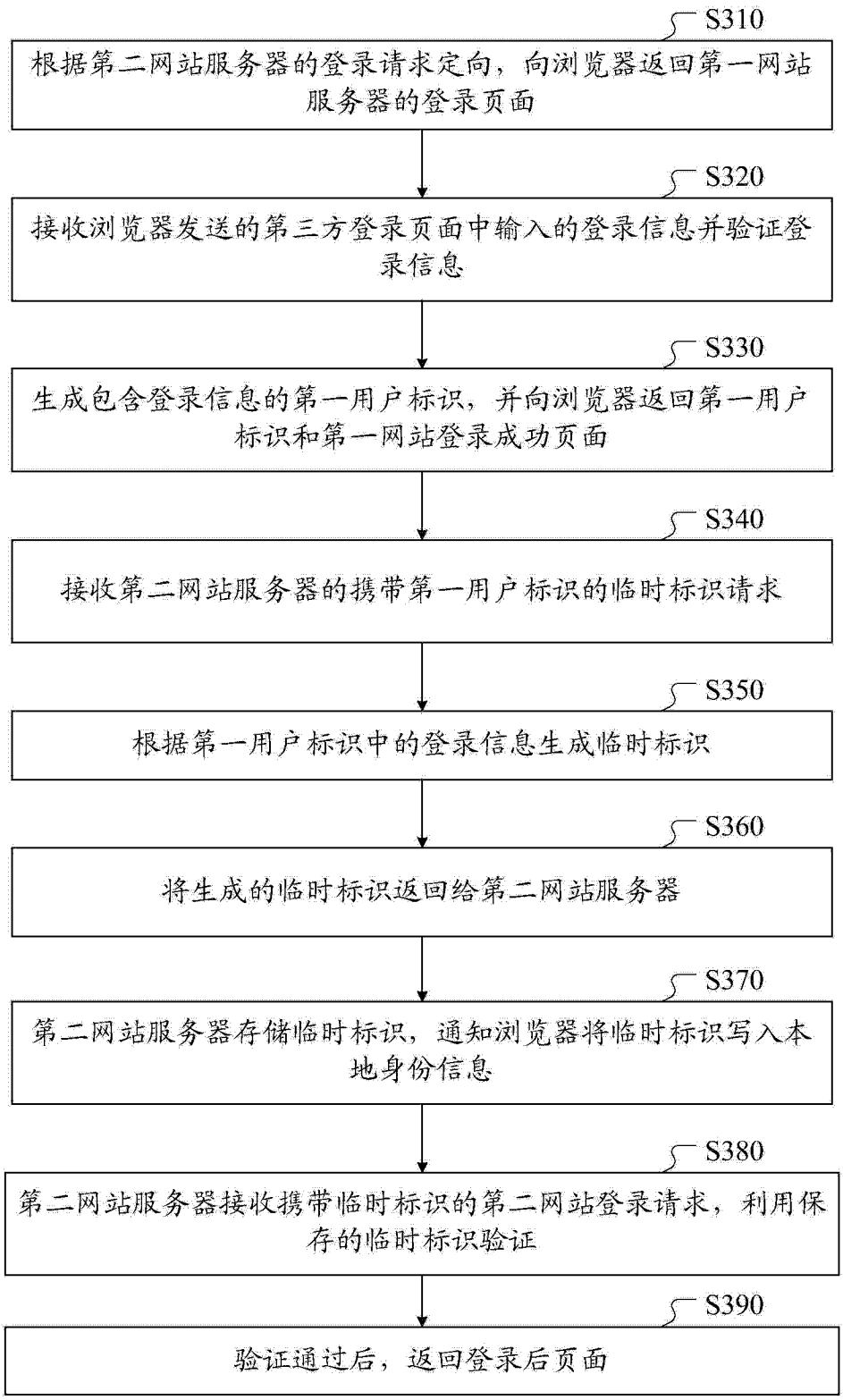

S310
根据第二网站服务器的登录请求定向，向浏览器返回第一网站服务器的登录页面
S320
接收浏览器发送的第三方登录页面中输入的登录信息并验证登录信息
S330
生成包含登录信息的第一用户标识，并向浏览器返回第一用户标识和第一网站登录成功页面
S340
接收第二网站服务器的携带第一用户标识的临时标识请求
S350
根据第一用户标识中的登录信息生成临时标识
S360
将生成的临时标识返回给第二网站服务器
S370
第二网站服务器存储临时标识，通知浏览器将临时标识写入本地身份信息
S380
第二网站服务器接收携带临时标识的第二网站登录请求，利用保存的临时标识验证
S390
验证通过后，返回登录后页面

图 3

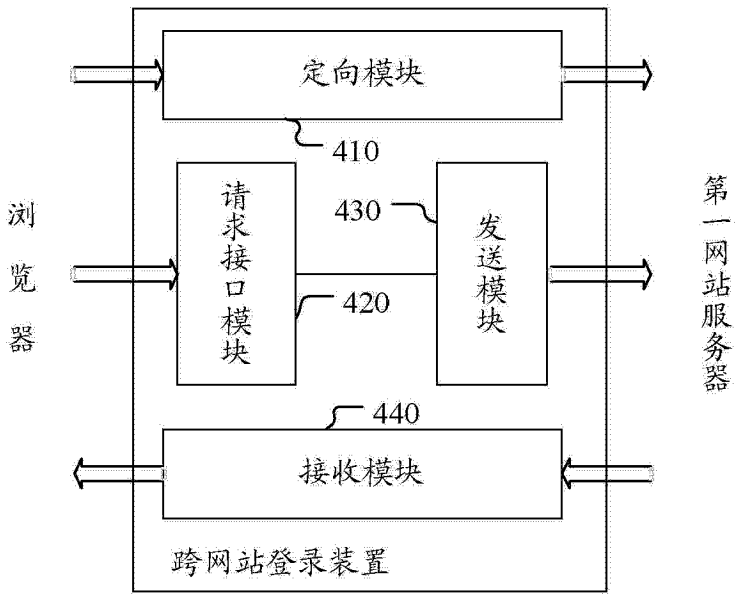

定向模块
410
请求接口模块
430
发送模块
420
440
接收模块
跨网站登录装置
浏览器
第一网站服务器

图 4

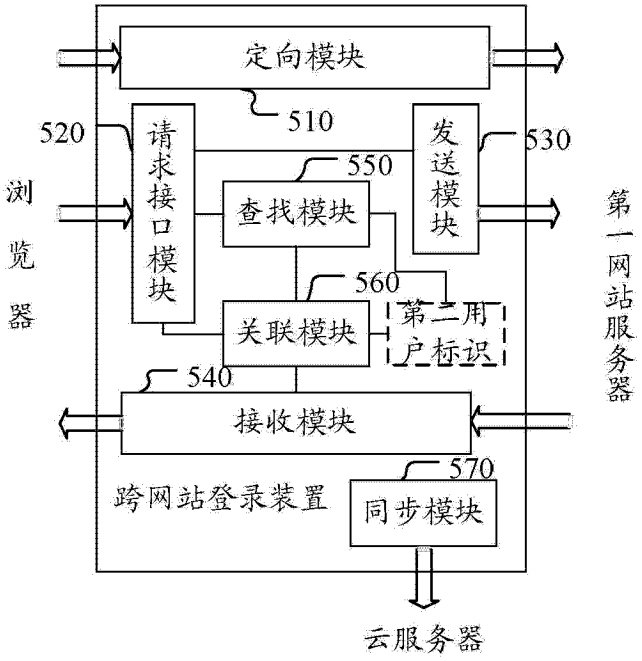

定向模块
510
520
请求接口模块
发送模块
530
550
查找模块
560
关联模块
第二用户标识
540
接收模块
570
同步模块
跨网站登录装置
浏览器
第一网站服务器
云服务器

图 5

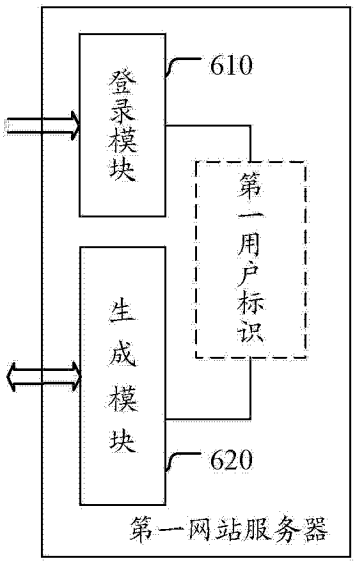

610
登录模块
第一用户标识
生成模块
620
第一网站服务器

图 6

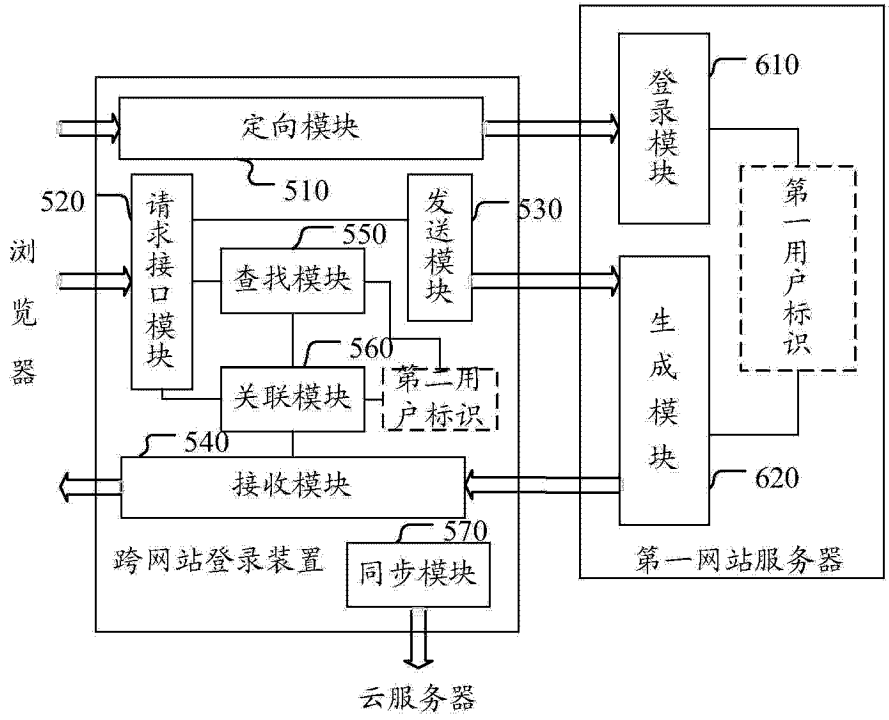

浏览器
520
定向模块
510
请求接口模块
查找模块
550
发送模块
530
关联模块
560
第二用户标识
540
接收模块
570
同步模块
跨网站登录装置
登录模块
610
第一用户标识
生成模块
620
第一网站服务器
云服务器

图 7