(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 105429978 A
(43)申请公布日 2016.03.23

(21)申请号 201510781737.6

(22)申请日 2015.11.13

(71)申请人 中国建设银行股份有限公司
地址 100032 北京市西城区金融大街25号

(72)发明人 张舜华 王伟 赵金鑫 何小锋
包辰明 李响 梁可尊 刘威
谢潇宇 王力

(74)专利代理机构 广州三环专利代理有限公司 44202
代理人 温旭 郝传鑫

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

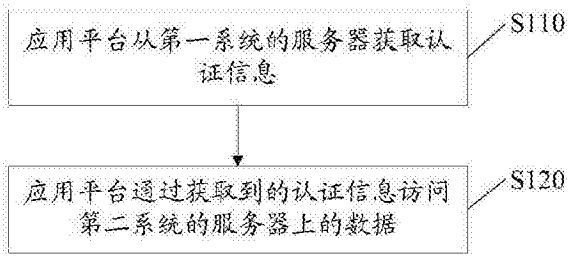
权利要求书2页 说明书6页 附图6页

(54)发明名称

数据访问方法、设备及系统

(57)摘要

本发明提供一种数据访问方法、设备及系统，所述方法包括：应用平台从第一系统的服务器获取认证信息；所述应用平台通过获取到的认证信息访问第二系统的服务器上的数据。实施本发明，可以通过使不同于开放系统的某个系统的服务器作为用于生成认证信息的授权服务器，从而实现在开放系统无需单独建立一个授权服务器的情况下保证了授权服务器与资源服务器的角色分离，降低了硬件成本。



CN 105429978 A

1. 一种数据访问方法，其特征在于，所述方法包括：

应用平台从第一系统的服务器获取认证信息；

所述应用平台通过获取到的认证信息访问第二系统的服务器上的数据。

2. 如权利要求 1 所述的方法，其特征在于，应用平台从第一系统的服务器获取认证信息包括：

所述应用平台调用所述第一系统的登录页面，以便于所述第一系统的服务器通过所述登录页面接收用户的登录信息并且根据所述登录信息判断所述应用平台的授权状态；

所述应用平台接收所述第一系统的服务器在确定所述应用平台的授权状态为已授权后生成并发送的认证信息。

3. 一种数据访问方法，其特征在于，所述方法包括：

第一系统的服务器生成认证信息和验证信息；

所述第一系统的服务器将生成的认证信息发送给应用平台并且将生成的验证信息发送给第二系统的服务器以便于所述应用平台通过所述认证信息访问所述第二系统的服务器上的数据。

4. 如权利要求 3 所述的方法，其特征在于，第一系统的服务器生成认证信息和验证信息包括：

所述第一系统的服务器接收用户的登录信息；

所述第一系统的服务器根据接收的登录信息验证所述用户是否授权所述应用平台访问所述用户在所述第二系统的服务器上的数据的至少一部分；

若已授权，则所述第一系统的服务器生成认证信息和验证信息。

5. 如权利要求 3 或 4 所述的方法，其特征在于，

所述认证信息包括：访问令牌的密文信息；

所述验证信息包括：所述访问令牌的明文信息。

6. 一种数据访问方法，其特征在于，所述方法包括：

第二系统的服务器接收第一系统的服务器发送的验证信息以及应用平台发送的访问请求；

所述第二系统的服务器从所述访问请求中解析出认证信息；

所述第二系统的服务器根据所述认证信息以及所述验证信息对所述应用平台进行验证处理；

若验证通过，则所述第二系统的服务器向所述应用平台发送与所述访问请求对应的数据。

7. 如权利要求 6 所述的方法，其特征在于，所述方法还包括：

若验证失败，则第二系统的服务器识别当前访问为虚假访问并调整所述应用平台的虚假访问次数；

所述第二系统的服务器判断调整后的虚假访问次数是否大于或者等于预定阈值；

若所述调整后的虚假访问次数大于或者等于所述预定阈值，则所述第二系统的服务器对所述应用平台进行屏蔽。

8. 一种应用平台，其特征在于，所述应用平台包括：

获取模块，用于从第一系统的服务器获取认证信息；

访问模块，用于通过所述获取模块获取到的认证信息访问第二系统的服务器上的数据。

9. 如权利要求 8 所述的应用平台，其特征在于，所述获取模块包括：

调用单元，用于调用所述第一系统的登录页面，以便于所述第一系统的服务器通过所述登录页面接收用户的登录信息并且根据所述登录信息判断所述应用平台的授权状态；

接收单元，用于接收所述第一系统的服务器在确定所述应用平台的授权状态为已授权后生成并发送的认证信息。

10. 一种数据访问系统，其特征在于，所述系统包括：

如权利要求 8 或 9 所述的应用平台，位于第一系统的服务器，和，位于第二系统的服务器；其中，

位于所述第一系统的服务器包括：

生成模块，用于生成认证信息和验证信息，

发送模块，用于将所述生成模块生成的认证信息发送给所述应用平台并且将所述生成模块生成的验证信息发送给所述第二系统的服务器以便于所述应用平台通过所述认证信息访问所述第二系统的服务器上的数据；

位于所述第二系统的服务器包括：

接收模块，用于接收所述第一系统的服务器发送的验证信息以及所述应用平台发送的访问请求，

解析模块，用于从所述接收模块接收的访问请求中解析出认证信息，

验证模块，用于根据所述解析模块所解析出的认证信息以及所述接收模块所接收的验证信息对所述应用平台进行验证处理，

发送模块，用于当所述验证模块确定为验证通过时，向所述应用平台发送与所述访问请求对应的数据。

数据访问方法、设备及系统

技术领域

[0001] 本发明涉及通信领域，更为具体而言，涉及数据访问方法、设备及系统。

背景技术

[0002] 随着互联网的发展，互联网系统越来越庞大，数据量也快速增加，为了能让第三方应用参与到系统的建设中，丰富系统应用，例如微信、新浪微博等各大互联网系统都支持OAuth2.0（开放授权）协议以建立自己的生态链系统。该OAuth2.0协议是一个开放标准（允许第三方应用在用户授权的前提下访问用户在服务商那里存储的各种信息）。

[0003] 然而，在现有技术中，支持OAuth2.0的开放互联网系统需要建立两个服务器，即用于生成认证信息的授权服务器和用于存储资源的资源服务器，因此，对于支持OAuth2.0的互联网系统的前期开发来讲需要较高的软硬件成本。

发明内容

[0004] 为解决上述技术问题，本发明提供一种数据访问方法、设备及系统。

[0005] 一方面，本发明的实施方式提供了一种数据访问方法，所述方法包括：

[0006] 应用平台从第一系统的服务器获取认证信息；

[0007] 所述应用平台通过获取到的认证信息访问第二系统的服务器上的数据。

[0008] 相应地，本发明实施方式提供了一种应用平台，所述应用平台包括：

[0009] 获取模块，用于从第一系统的服务器获取认证信息；

[0010] 访问模块，用于通过所述获取模块获取到的认证信息访问第二系统的服务器上的数据。

[0011] 另一方面，本发明实施方式提供一种数据访问方法，所述方法包括：

[0012] 第一系统的服务器生成认证信息和验证信息；

[0013] 所述第一系统的服务器将生成的认证信息发送给应用平台并且将生成的验证信息发送给第二系统的服务器以便于所述应用平台通过所述认证信息访问所述第二系统的服务器上的数据。

[0014] 又一方面，本发明实施方式提供一种数据访问方法，所述方法包括：

[0015] 第二系统的服务器接收第一系统的服务器发送的验证信息以及应用平台发送的访问请求；

[0016] 所述第二系统的服务器从所述访问请求中解析出认证信息；

[0017] 所述第二系统的服务器根据所述认证信息以及所述验证信息对所述应用平台进行验证处理；

[0018] 若验证通过，则所述第二系统的服务器向所述应用平台发送与所述访问请求对应的数据。

[0019] 再一方面，本发明实施方式提供一种数据访问系统，所述系统包括：如上所述的应用平台，位于第一系统的服务器，和，位于第二系统的服务器；其中，

[0020] 所述第一系统的服务器包括：

[0021] 生成模块，用于生成认证信息和验证信息，

[0022] 发送模块，用于将所述生成模块生成的认证信息发送给所述应用平台并且将所述生成模块生成的验证信息发送给所述第二系统的服务器以便于所述应用平台通过所述认证信息访问所述第二系统的服务器上的数据；

[0023] 所述第二系统的服务器包括：

[0024] 接收模块，用于接收所述第一系统的服务器发送的验证信息以及所述应用平台发送的访问请求，

[0025] 解析模块，用于从所述接收模块接收的访问请求中解析出认证信息，

[0026] 验证模块，用于根据所述解析模块所解析出的认证信息以及所述接收模块所接收的验证信息对所述应用平台进行验证处理，

[0027] 发送模块，用于当所述验证模块确定为验证通过时，向所述应用平台发送与所述访问请求对应的数据。

[0028] 实施本发明提供的数据访问方法、设备及系统，可以通过使不同于开放系统的某个系统的服务器作为用于生成认证信息的授权服务器，从而实现在开放系统无需单独建立一个授权服务器的情况下保证了授权服务器与资源服务器的角色分离，降低了硬件成本。

附图说明

[0029] 图 1 是根据本发明实施方式的一种数据访问方法的流程图；

[0030] 图 2 示出了图 1 所示的处理 S110 的一种实施方式；

[0031] 图 3 是根据本发明实施方式的另一种数据访问方法的流程图；

[0032] 图 4 示出了图 3 所示的处理 S210 的一种实施方式；

[0033] 图 5 是根据本发明实施方式的又一种数据访问方法的流程图；

[0034] 图 6 是根据本发明实施方式的再一种数据访问方法的流程图；

[0035] 图 7 是根据本发明实施方式的数据访问系统的架构图；

[0036] 图 8 示出了图 7 所示的应用平台 100 的结构示意图；

[0037] 图 9 示出了图 8 所示的获取模块 110 的结构示意图；

[0038] 图 10 示出了图 7 所示的服务器 200 的结构示意图；

[0039] 图 11 示出了图 10 所示的生成模块 210 的结构示意图；

[0040] 图 12 示出了图 7 所示的服务器 300 的结构示意图。

具体实施方式

[0041] 为使本发明的实施例的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述。

[0042] 图 1 是根据本发明实施方式的一种数据访问方法的流程图，参见图 1，该方法包括：

[0043] S110：应用平台从第一系统的服务器获取认证信息。其中，优选地，所述第二系统可以是一种现有的系统。

[0044] S120：应用平台通过获取到的认证信息访问第二系统（一种开放系统）的服务器

上的数据。

[0045] 其中，在本发明的实施方式中，所述认证信息例如可以是访问令牌或者是访问令牌的密文信息。

[0046] 如图 2 所示，在本发明的实施方式中，上述处理 S110 可以通过以下方式实现：

[0047] S111：所述应用平台调用所述第一系统的登录页面，以便于所述第一系统的服务器通过所述登录页面接收用户的登录信息并且根据所述登录信息判断所述应用平台的授权状态。

[0048] S112：所述应用平台接收所述第一系统的服务器在确定所述应用平台的授权状态为已授权后生成并发送的认证信息。

[0049] 图 3 是根据本发明实施方式的另一种数据访问方法的流程图。参见图 3，该方法包括：

[0050] S210：第一系统的服务器生成认证信息和验证信息。其中，优选地，所述第二系统可以是一种现有的系统。

[0051] S220：所述第一系统的服务器将生成的认证信息发送给应用平台并且将生成的验证信息发送给第二系统的服务器以便于所述应用平台通过所述认证信息访问所述第二系统的服务器上的数据。

[0052] 如图 4 所示，在本发明的实施方式中，上述处理 S210 可以通过以下方式实现：

[0053] S211：所述第一系统的服务器接收用户的登录信息。

[0054] S212：所述第一系统的服务器根据接收的登录信息验证所述用户是否授权所述应用平台访问所述用户在所述第三系统的服务器上的数据的至少一部分，若是，则执行 S213，否则，返回处理 S211。

[0055] S213：所述第一系统的服务器生成认证信息和验证信息。

[0056] 在本发明的实施方式中，所述第一系统的服务器可以生成访问令牌，将所述访问令牌作为所述认证信息以及所述验证信息；或者，通过所述应用平台的密钥对所述访问令牌进行加密处理，将所述访问令牌的密文信息作为所述认证信息，将所述访问令牌的明文信息作为所述验证信息，并将所述密钥发送给所述第二系统的服务器。

[0057] 图 5 是根据本发明实施方式的又一种数据访问方法的流程图。参见图 5，该方法包括：

[0058] S310：第二系统的服务器接收第一系统的服务器发送的验证信息以及应用平台发送的访问请求。其中，优选地，所述第二系统可以是一种现有的系统。

[0059] S320：所述第二系统的服务器从所述访问请求中解析出认证信息。

[0060] S330：所述第二系统的服务器根据所述认证信息以及所述验证信息对所述应用平台进行验证处理，若验证通过，则执行 S340，若验证失败，则执行 S350。

[0061] S340：所述第二系统的服务器向所述应用平台发送与所述访问请求对应的数据，返回处理 S310。

[0062] S350：第二系统的服务器识别当前访问为虚假访问并调整所述应用平台的虚假访问次数。

[0063] S360：所述第二系统的服务器判断调整后的虚假访问次数是否大于或者等于预定阈值，若是，则执行 S370，若否，则返回处理 S310。

[0064] S370：所述第二系统的服务器对所述应用平台进行屏蔽，返回处理 S310。

[0065] 当然，本发明的实施方式不限于此，当上述处理 S330 的验证结果为验证失败时，还可以直接拒绝所述应用平台的访问并提示相应信息然后返回处理 S310。

[0066] 下面以所述第一系统为购买所述应用平台的应用市场为例对本发明的数据访问方法的处理流程进行具体说明。如图 6 所示，该方法包括：

[0067] S410：应用平台（一种第三方应用）在用户发起登录操作后调用第一系统（例如可以是用于购买所述应用平台的应用市场）的登录页面。

[0068] S420：第一系统的服务器通过该登录页面接收用户的登录信息（包括用户名以及密码等信息），根据用户的登录信息判断所述用户是否购买所述应用平台（在本发明的实施方式中，只要用户购买了某一系统即默认为该用户授权该系统访问其在服务提供方上存储的数据），若是，则执行 S430，否则，返回 S410。

[0069] 在本发明的实施方式中，第一系统的服务器可以直接根据用户的登录信息判断是否已授权而无需在每次生成认证信息前都需要用户进行授权操作。

[0070] S430：所述第一系统的服务器生成访问令牌，通过应用平台的密钥对该访问令牌进行加密，将访问令牌的密文信息作为认证信息，将访问令牌的明文信息作为验证信息。

[0071] 其中，在本发明的实施方式中，所述第一系统的服务器例如可以将用户进行登录的会话的标识符作为访问令牌。

[0072] S440：所述第一系统的服务器将认证信息发送给应用平台，将验证信息以及所述密钥发送给第二系统（一种开放系统）的服务器。

[0073] S450：所述应用平台向所述第二系统的服务器发送带有所述认证信息的访问请求。

[0074] 其中，在本发明的实施方式中，所述应用平台例如可以将所述认证信息作为 cookie（储存在用户本地终端上的数据）进行存放，并且在访问所述第二系统的服务器时可以携带该 cookie，对此，需要保证所述应用平台、第一系统以及第二系统拥有相同的二级域名空间以克服不能跨域名发送 cookie 的问题。

[0075] S460：所述第二系统的服务器从所述访问请求中解析出认证信息，根据所述认证信息以及验证信息对所述应用平台进行验证处理，若验证通过，则执行 S470，若验证失败，则执行 S480。

[0076] 其中，所述验证处理具体可以通过以下方式实现：所述第二系统的服务器利用所述密钥对认证信息进行解密，将解密后的认证信息与验证信息进行匹配，若匹配成功，则验证通过，若匹配失败，则验证失败。

[0077] S470：所述第二系统的服务器向所述应用平台发送与所述访问请求对应的数据，返回 S410。

[0078] S480：第二系统的服务器识别当前访问为虚假访问并调整所述应用平台的虚假访问次数。

[0079] S490：第二系统的服务器判断调整后的虚假访问次数是否大于或等于预定阈值，若是，则执行 S500，否则，返回 S410。

[0080] S500：所述第二系统的服务器对所述应用平台进行屏蔽，返回 S410。

[0081] 图 7 是根据本发明实施方式的数据访问系统的架构图。参见图 7，所述系统包括：

应用平台（一种第三方应用）100，位于第一系统的服务器200，以及位于第二系统的服务器300，其中，所述第二系统是一种支持开放标准的开放系统，优选地，所述第一系统可以是一种现有系统，具体地：

[0082] 应用平台100，用于执行下述操作：从服务器200获取认证信息；通过获取到的认证信息访问服务器300上的数据。

[0083] 在本发明的实施方式中，上述应用平台100所要执行的操作例如在应用平台100的客户端侧执行。

[0084] 服务器200，用于执行下述操作：生成认证信息和验证信息；将生成的认证信息发送给应用平台100并且将生成的验证信息发送给300以便于所述应用平台100通过所述认证信息访问所述服务器300上的数据。

[0085] 服务器300，用于执行下述操作：接收服务器200发送的验证信息以及应用平台100发送的访问请求；从所述访问请求中解析出认证信息；根据所述认证信息以及所述验证信息对所述应用平台100进行验证处理；若验证通过，则向所述应用平台100发送与所述访问请求对应的数据。

[0086] 图8示出了图7所示的应用平台100的结构示意图，参见图8，应用平台100包括：获取模块110以及访问模块120，具体地：

[0087] 获取模块110，用于从所述服务器200获取认证信息。

[0088] 访问模块120，用于通过所述获取模块110获取到的认证信息访问所述服务器300上的数据。

[0089] 在本发明的实施方式中，上述获取模块110以及访问模块120例如可以全部配置于客户端侧。

[0090] 如图9所示，在本发明的实施方式中，获取模块110可以包括：调用单元111以及接收单元112，具体地：

[0091] 调用单元111，用于调用所述第一系统的登录页面，以便于所述服务器200通过所述登录页面接收用户的登录信息并且根据所述登录信息判断所述应用平台100的授权状态；

[0092] 接收单元112，用于接收所述服务器200在确定所述应用平台100的授权状态为已授权后生成并发送的认证信息。

[0093] 图10示出了图7所示的服务器200的结构示意图。参见图10，所述服务器200包括：生成模块210以及发送模块220，具体地：

[0094] 生成模块210，用于生成认证信息和验证信息。

[0095] 发送模块220，用于将所述生成模块210生成的认证信息发送给应用平台100并且将所述生成模块210生成的验证信息发送给服务器300以便于所述应用平台100通过所述认证信息访问所述服务器300上的数据。

[0096] 如图11所示，在本发明的实施方式中，所述生成模块210可以包括：接收单元211、验证单元212以及生成单元213，具体地：

[0097] 接收单元211，用于接收用户的登录信息。

[0098] 验证单元212，用于根据所述接收单元211接收的登录信息验证所述用户是否授权所述应用平台100访问所述用户在所述服务器300上的数据的至少一部分。

[0099] 生成单元213，用于当所述验证单元212验证为已授权时，生成认证信息和验证信息。

[0100] 在本发明的实施方式中，所述服务器200可以生成访问令牌；将所述访问令牌作为所述认证信息以及所述验证信息，或者，通过应用平台的密钥对所述访问令牌进行加密处理，将所述访问令牌的密文信息作为所述认证信息，将所述访问令牌的明文信息作为所述验证信息，并将所述密钥发送给所述服务器300。

[0101] 图12示出了图7所示的服务器300的结构示意图。参见图12，所述服务器300包括：接收模块310、解析模块320、验证模块330、发送模块340、识别及调整模块350、判断模块360以及屏蔽模块370，具体地：

[0102] 接收模块310，用于接收所述服务器200发送的验证信息以及应用平台100发送的访问请求。

[0103] 解析模块320，用于从所述接收模块310接收的访问请求中解析出认证信息。

[0104] 验证模块330，用于根据所述解析模块320所解析出的认证信息以及所述接收模块310所接收的验证信息对所述应用平台100进行验证处理。

[0105] 发送模块340，用于当所述验证模块330确定为验证通过时，向所述应用平台100发送与所述访问请求对应的数据。

[0106] 识别及调整模块350，用于当所述验证模块330确定为验证失败时，识别当前访问为虚假访问并调整所述应用平台100的虚假访问次数。

[0107] 判断模块360，用于判断所述识别及调整模块350调整后的虚假访问次数是否大于或者等于预定阈值。

[0108] 屏蔽模块370，用于当所述判断模块360的判断结果为所述调整后的虚假访问次数大于或者等于所述预定阈值时，对所述应用平台100进行屏蔽。

[0109] 当然，本发明的实施方式不限于此，例如可以通过用于当所述验证模块330确定为验证失败时，拒绝所述应用平台100的访问并提示相应信息的拒绝及提示模块来代替所述识别及调整模块350、比较模块360以及屏蔽模块370。

[0110] 实施本发明提供的数据访问方法、设备及系统，可以通过使不同于开放系统的某个系统的服务器作为用于生成认证信息的授权服务器，从而实现在开放系统无需单独建立一个授权服务器的情况下保证了授权服务器与资源服务器的角色分离，降低了硬件成本。

[0111] 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本发明可借助软件结合硬件平台的方式来实现。基于这样的理解，本发明的技术方案对背景技术做出贡献的全部或者部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，智能手机或者网络设备等）执行本发明各个实施例或者实施例的某些部分所述的方法。

[0112] 本发明说明书中使用的术语和措辞仅仅为了举例说明，并不意味构成限定。本领域技术人员应当理解，在不脱离所公开的实施方式的基本原理的前提下，对上述实施方式中的各细节可进行各种变化。因此，本发明的范围只由权利要求确定，在权利要求中，除非另有说明，所有的术语应按最宽泛合理的意思进行理解。

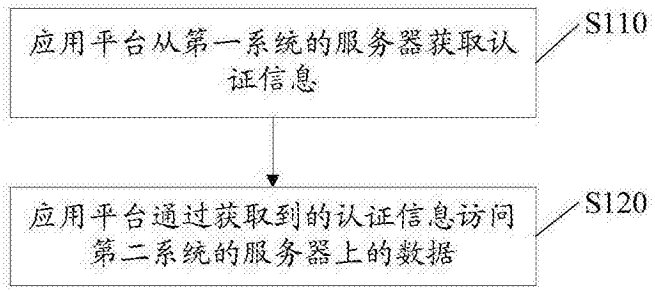

应用平台从第一系统的服务器获取认证信息
S110
应用平台通过获取到的认证信息访问第二系统的服务器上的数据
S120

图 1

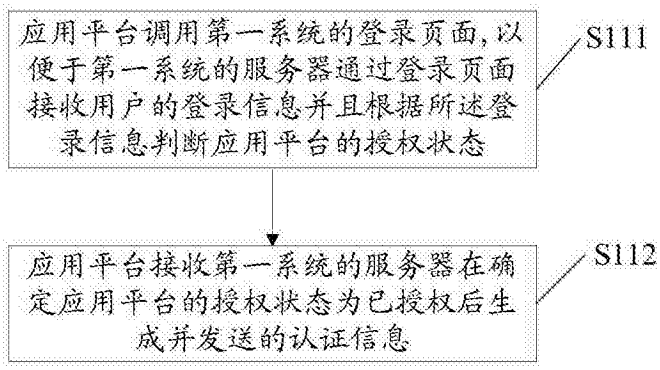

应用平台调用第一系统的登录页面,以便于第一系统的服务器通过登录页面接收用户的登录信息并且根据所述登录信息判断应用平台的授权状态
S111
应用平台接收第一系统的服务器在确定应用平台的授权状态为已授权后生成并发送的认证信息
S112

图 2

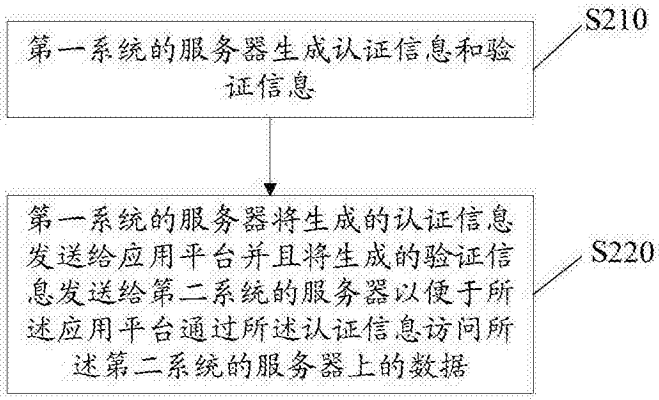

第一系统的服务器生成认证信息和验证信息
S210
第一系统的服务器将生成的认证信息发送给应用平台并且将生成的验证信息发送给第二系统的服务器以便于所述应用平台通过所述认证信息访问所述第二系统的服务器上的数据
S220

图 3

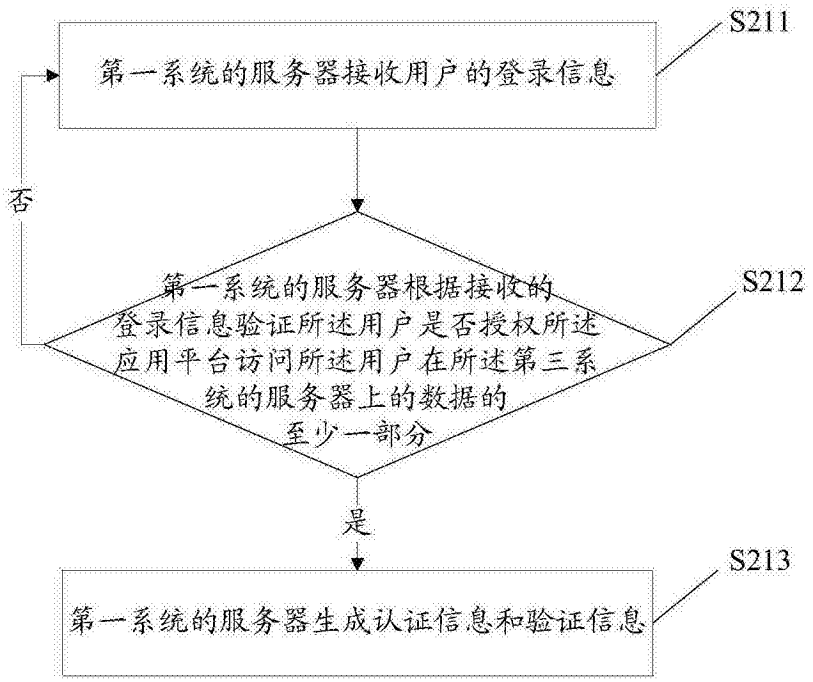

S211
第一系统的服务器接收用户的登录信息
否
第一系统的服务器根据接收的登录信息验证所述用户是否授权所述应用平台访问所述用户在所述第三系统的服务器上的数据的至少一部分
S212
是
S213
第一系统的服务器生成认证信息和验证信息

图 4

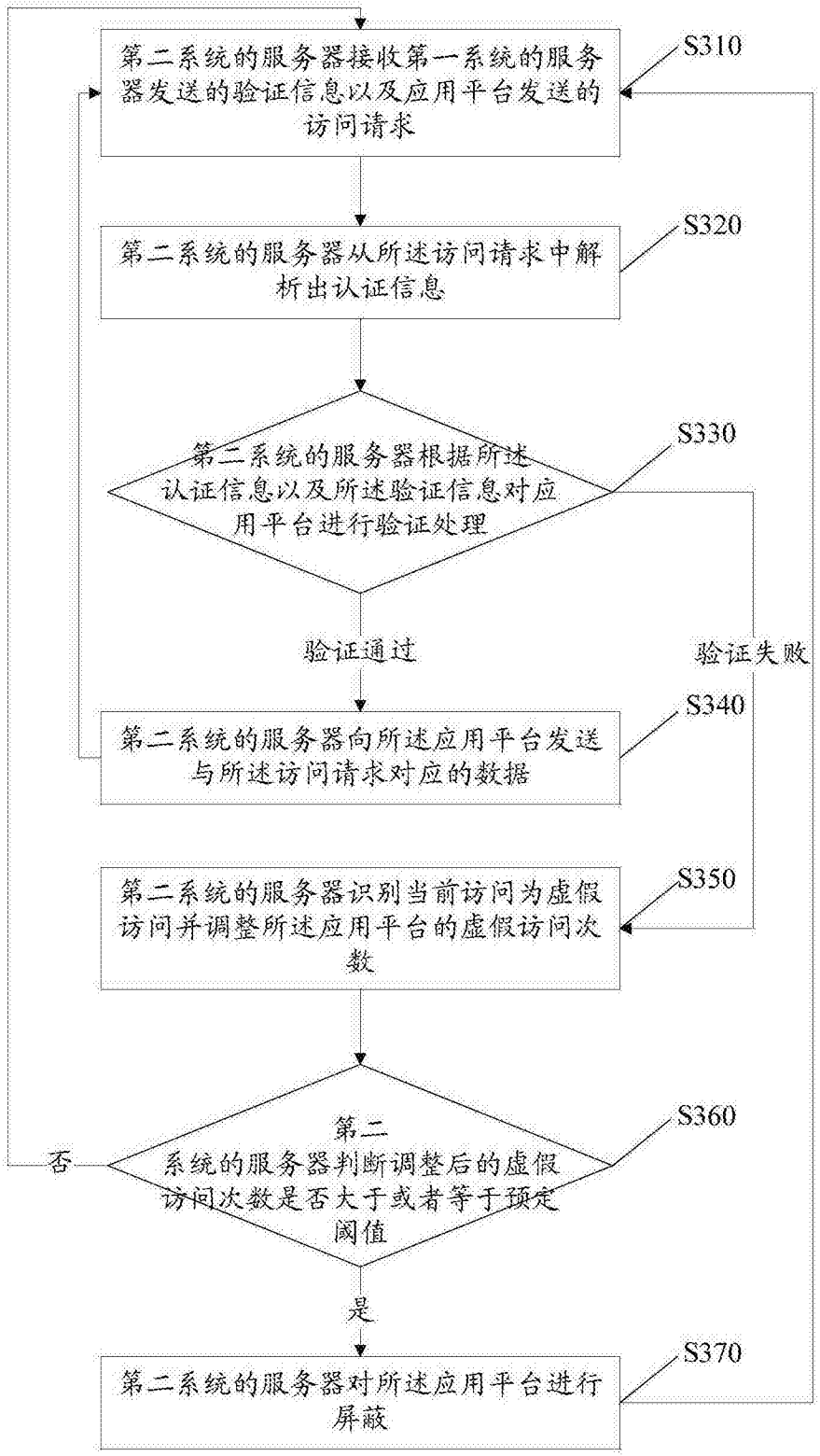

第二系统的服务器接收第一系统的服务器发送的验证信息以及应用平台发送的访问请求
S310
第二系统的服务器从所述访问请求中解析出认证信息
S320
第二系统的服务器根据所述认证信息以及所述验证信息对应用平台进行验证处理
S330
验证通过
验证失败
第二系统的服务器向所述应用平台发送与所述访问请求对应的数据
S340
第二系统的服务器识别当前访问为虚假访问并调整所述应用平台的虚假访问次数
S350
第二系统的服务器判断调整后的虚假访问次数是否大于或者等于预定阈值
S360
否
是
第二系统的服务器对所述应用平台进行屏蔽
S370

图 5

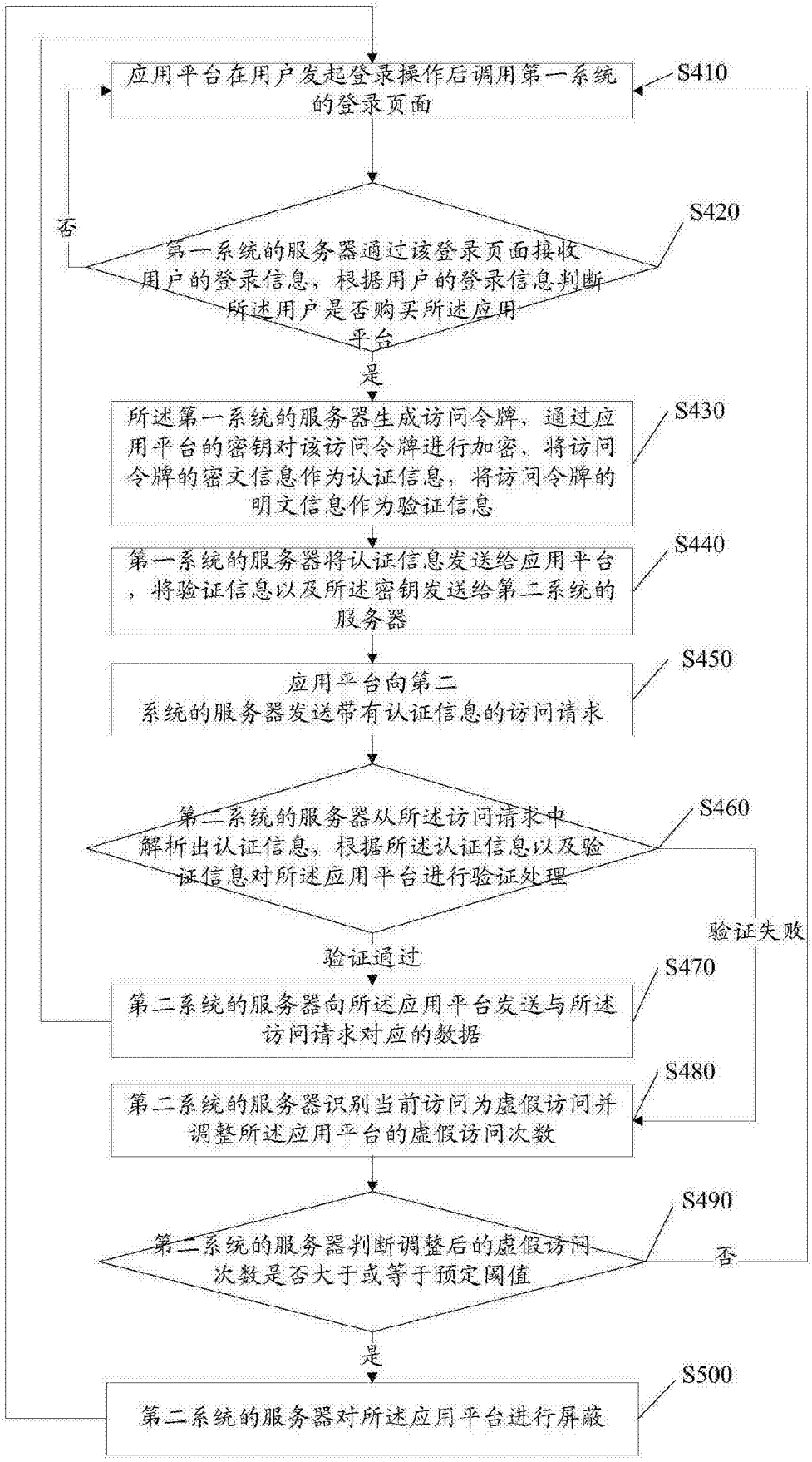

应用平台在用户发起登录操作后调用第一系统的登录页面
S410
第一系统的服务器通过该登录页面接收用户的登录信息，根据用户的登录信息判断所述用户是否购买所述应用平台
S420
否
是
所述第一系统的服务器生成访问令牌，通过应用平台的密钥对该访问令牌进行加密，将访问令牌的密文信息作为认证信息，将访问令牌的明文信息作为验证信息
S430
第一系统的服务器将认证信息发送给应用平台，将验证信息以及所述密钥发送给第二系统的服务器
S440
应用平台向第二系统的服务器发送带有认证信息的访问请求
S450
第二系统的服务器从所述访问请求中解析出认证信息，根据所述认证信息以及验证信息对所述应用平台进行验证处理
S460
验证失败
验证通过
第二系统的服务器向所述应用平台发送与所述访问请求对应的数据
S470
第二系统的服务器识别当前访问为虚假访问并调整所述应用平台的虚假访问次数
S480
第二系统的服务器判断调整后的虚假访问次数是否大于或等于预定阈值
S490
否
是
第二系统的服务器对所述应用平台进行屏蔽
S500

图 6

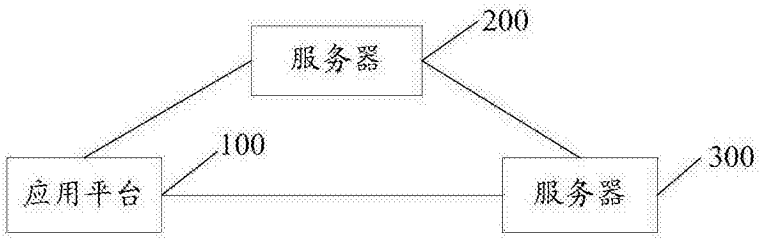


图 7

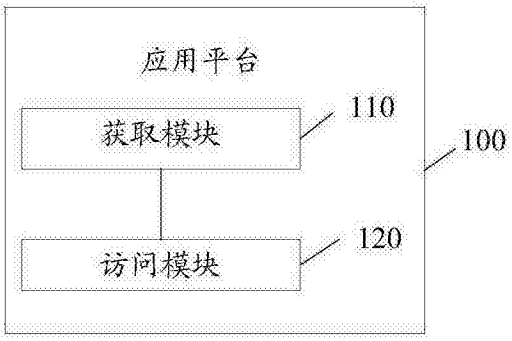


图 8

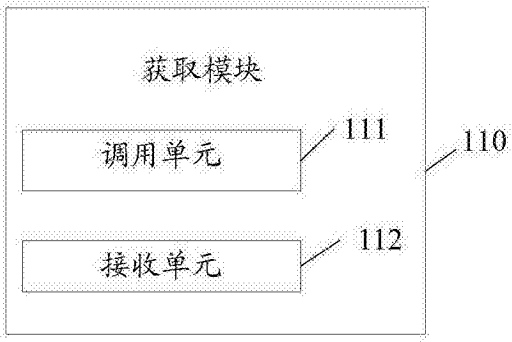


图 9

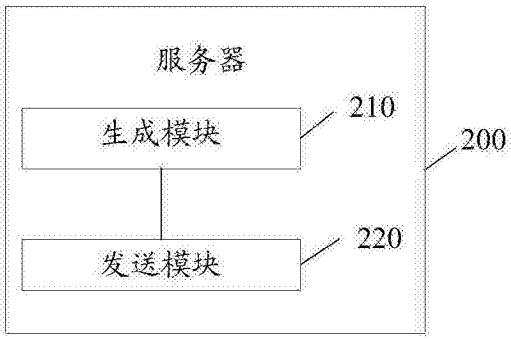


图 10

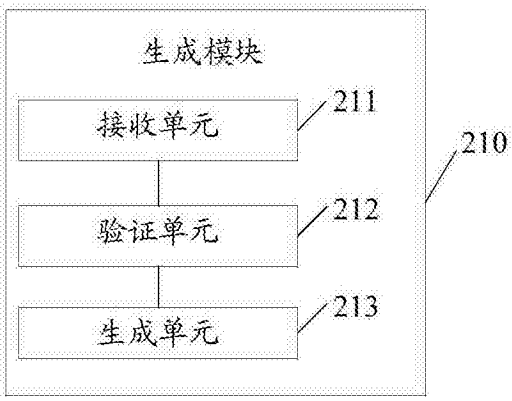


图 11

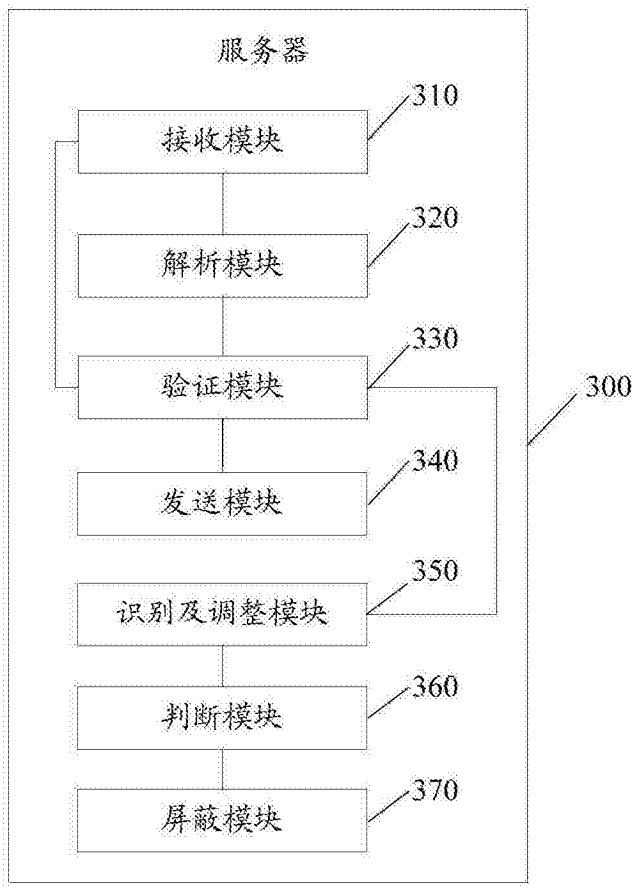

服务器
310
接收模块
320
解析模块
330
验证模块
300
340
发送模块
350
识别及调整模块
360
判断模块
370
屏蔽模块

图 12