(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 109583181 A
(43)申请公布日 2019.04.05

(21)申请号 201811444791.1

(22)申请日 2018.11.29

(71)申请人 新华三技术有限公司
地址 310052 浙江省杭州市滨江区长河路466号

(72)发明人 郝兆旭 刘靖靖

(74)专利代理机构 北京柏杉松知识产权代理事务所(普通合伙) 11413
代理人 丁芸 项京

(51)Int.Cl.
G06F 21/44(2013.01)
G06F 21/31(2013.01)

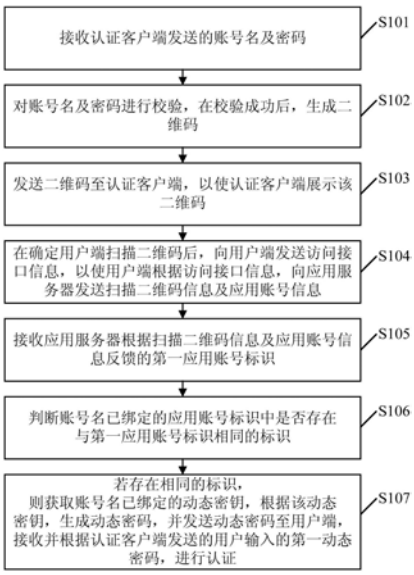
权利要求书3页 说明书11页 附图4页

(54)发明名称

一种认证方法、装置及机器可读存储介质

(57)摘要

本发明实施例提供了一种认证方法、装置及机器可读存储介质，认证服务器对认证客户端发送的账号名和密码进行校验，校验成功后，生成二维码，并将二维码发送至认证客户端，认证客户端向用户展示二维码，认证服务器在确定用户端扫描二维码后，向用户端发送访问接口信息，用户端根据访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息，认证服务器接收应用服务器反馈的第一应用账号标识，如果账号名已绑定的应用账号标识中存在与第一应用账号标识相同的标识，则获取并根据账号名已绑定的动态密钥，生成动态密码，并发送动态密码至用户端，接收并根据认证客户端发送的用户输入的第一动态密码，进行认证。通过本方案，可以提高网络安全性。



CN 109583181 A

1.一种认证方法,其特征在于,应用于认证系统中的认证服务器,所述方法包括:

接收认证客户端发送的账号名及密码;

对所述账号名及所述密码进行校验,在校验成功后,生成二维码;

发送所述二维码至所述认证客户端,以使所述认证客户端展示所述二维码;

在确定用户端扫描所述二维码后,向所述用户端发送访问接口信息,以使所述用户端根据所述访问接口信息,向应用服务器发送扫描二维码信息及应用账号信息;

接收所述应用服务器根据所述扫描二维码信息及所述应用账号信息反馈的第一应用账号标识;

判断所述账号名已绑定的应用账号标识中是否存在与所述第一应用账号标识相同的标识;

若存在相同的标识,则获取所述账号名已绑定的动态密钥;根据所述动态密钥,生成动态密码,并发送所述动态密码至所述用户端;接收并根据所述认证客户端发送的用户输入的第一动态密码,进行认证。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:

若确定所述账号名未绑定应用账号标识,则随机生成动态密钥,并将所述动态密钥、所述账号名与所述第一应用账号标识进行绑定;

根据所述动态密钥,生成动态密码;

发送所述动态密码至所述用户端;

接收并根据所述认证客户端发送的用户输入的第一动态密码,进行认证。

3.根据权利要求1或2所述的方法,其特征在于,所述根据所述动态密钥,生成动态密码,包括:

根据所述动态密钥,利用预设哈希加密算法,生成当前时刻的动态密码;

所述接收并根据所述认证客户端发送的用户输入的第一动态密码,进行认证,包括:

接收所述认证客户端发送的用户输入的账号名及第一动态密码;

根据所述账号名,获取所述账号名已绑定的动态密钥;

根据所述动态密钥,利用所述预设哈希加密算法,生成当前时刻的预设时间段内的所有动态密码;

判断生成的所有动态密码中是否存在与所述第一动态密码一致的动态密码;

若存在,则确定认证成功;

若不存在,则确定认证失败。

4.根据权利要求1所述的方法,其特征在于,在所述判断所述账号名已绑定的应用账号标识中是否存在与所述第一应用账号标识相同的标识之后,所述方法还包括:

若不存在相同的标识,则确定认证失败。

5.一种认证方法,其特征在于,应用于认证系统中的认证客户端,所述方法包括:

发送用户输入的账号名及密码至认证服务器,以使所述认证服务器对所述账号名及所述密码进行校验,在校验成功后,生成二维码;

接收所述认证服务器发送的所述二维码,并展示所述二维码,以使用户端扫描所述二维码,并根据所述认证服务器发送的访问接口信息,向应用服务器发送扫描二维码信息及应用账号信息;

接收用户输入的第一动态密码；

发送所述第一动态密码至所述认证服务器，以使所述认证服务器根据所述第一动态密码，进行认证。

6.一种认证装置，其特征在于，应用于认证系统中的认证服务器，所述装置包括：

接收模块，用于接收认证客户端发送的账号名及密码；

校验模块，用于对所述账号名及所述密码进行校验，在校验成功后，生成二维码；

发送模块，用于发送所述二维码至所述认证客户端，以使所述认证客户端展示所述二维码；在确定用户端扫描所述二维码后，向所述用户端发送访问接口信息，以使所述用户端根据所述访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息；

所述接收模块，还用于接收所述应用服务器根据所述扫描二维码信息及所述应用账号信息反馈的第一应用账号标识；

判断模块，用于判断所述账号名已绑定的应用账号标识中是否存在与所述第一应用账号标识相同的标识；

获取模块，用于若所述判断模块的判断结果为存在相同的标识，则获取所述账号名已绑定的动态密钥；

生成模块，用于根据所述动态密钥，生成动态密码，并发送所述动态密码至所述用户端；

认证模块，用于接收并根据所述认证客户端发送的用户输入的第一动态密码，进行认证。

7.根据权利要求6所述的装置，其特征在于，所述装置还包括：

绑定模块，用于若确定所述账号名未绑定应用账号标识，则随机生成动态密钥，并将所述动态密钥、所述账号名与所述第一应用账号标识进行绑定。

8.根据权利要求6或7所述的装置，其特征在于，所述生成模块，具体用于：

根据所述动态密钥，利用预设哈希加密算法，生成当前时刻的动态密码；

所述认证模块，具体用于：

接收所述认证客户端发送的用户输入的账号名及第一动态密码；

根据所述账号名，获取所述账号名已绑定的动态密钥；

根据所述动态密钥，利用所述预设哈希加密算法，生成当前时刻的预设时间段内的所有动态密码；

判断生成的所有动态密码中是否存在与所述第一动态密码一致的动态密码；

若存在，则确定认证成功；

若不存在，则确定认证失败。

9.根据权利要求6所述的装置，其特征在于，所述认证模块，还用于：

若所述判断模块的判断结果为不存在相同的标识，则确定认证失败。

10.一种认证装置，其特征在于，应用于认证系统中的认证客户端，所述装置包括：

发送模块，用于发送用户输入的账号名及密码至认证服务器，以使所述认证服务器对所述账号名及所述密码进行校验，在校验成功后，生成二维码；

接收模块，用于接收所述认证服务器发送的所述二维码，并展示所述二维码，以使所述用户端扫描所述二维码，并根据所述认证服务器发送的访问接口信息，向应用服务器发送

扫描二维码信息及应用账号信息;接收用户输入的第一动态密码;

所述发送模块,还用于发送所述第一动态密码至所述认证服务器,以使所述认证服务器根据所述第一动态密码,进行认证。

11.一种机器可读存储介质,其特征在于,所述机器可读存储介质中存储有机器可执行的指令,所述指令由处理器加载并执行,以实现权利要求1-4任一项所述的方法。

一种认证方法、装置及机器可读存储介质

技术领域

[0001] 本发明涉及计算机技术领域，特别是涉及一种认证方法、装置及机器可读存储介质。

背景技术

[0002] 在个人网络或者企业网络中，为了保证网络的安全运行，要求用户需要通过登录认证，才能正常访问网络。通常的认证过程，是由用户在认证客户端上输入账号名和密码，认证服务器对账号名和密码进行校验，如果满足预先配置的匹配关系，则确定认证成功。然而，通常情况下密码是预先基于账号名静态配置的，极易被盗，网络的安全隐患较大。

[0003] 为了解决上述问题，相应的认证方法中，认证客户端向认证服务器发送认证请求，认证服务器在接收到认证请求后随机生成动态密码，认证服务器将动态密码下发至认证客户端隐藏存储，并将动态密码以短信的方式通知用户，用户可以在认证客户端输入动态密码，认证客户端将用户输入的动态密码和隐藏存储的动态密码一起发送至认证服务器，由认证服务器对两个动态密码进行比较，如果相同，则可以确定认证成功。

[0004] 由于动态密码隐藏存储在认证客户端中，如果认证客户端隐藏存储动态密码的方式被破解，则攻击者很容易通过破解隐藏的动态密码或者修改隐藏的动态密码，对应输入相同的动态密码至认证服务器进行认证，达到攻击网络的目的，网络安全性仍然较差。

发明内容

[0005] 本发明实施例的目的在于提供一种认证方法、装置及机器可读存储介质，以提高网络安全性。具体技术方案如下：

[0006] 第一方面，本发明实施例提供了一种认证方法，应用于认证系统中的认证服务器，所述方法包括：

[0007] 接收认证客户端发送的账号名及密码；

[0008] 对所述账号名及所述密码进行校验，在校验成功后，生成二维码；

[0009] 发送所述二维码至所述认证客户端，以使所述认证客户端展示所述二维码；

[0010] 在确定用户端扫描所述二维码后，向所述用户端发送访问接口信息，以使所述用户端根据所述访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息；

[0011] 接收所述应用服务器根据所述扫描二维码信息及所述应用账号信息反馈的所述第一应用账号标识；

[0012] 判断所述账号名已绑定的应用账号标识中是否存在与所述第一应用账号标识相同的标识；

[0013] 若存在相同的标识，则获取所述账号名已绑定的动态密钥；根据所述动态密钥，生成动态密码，并发送所述动态密码至所述用户端；接收并根据所述认证客户端发送的用户输入的第一动态密码，进行认证。

[0014] 第二方面，本发明实施例提供了一种认证方法，应用于认证系统中的认证客户端，

所述方法包括：

[0015] 发送用户输入的账号名及密码至认证服务器，以使所述认证服务器对所述账号名及所述密码进行校验，在校验成功后，生成二维码；

[0016] 接收所述认证服务器发送的所述二维码，并展示所述二维码，以使用户端扫描所述二维码，并根据所述认证服务器发送的访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息；

[0017] 接收用户输入的第一动态密码；

[0018] 发送所述第一动态密码至所述认证服务器，以使所述认证服务器根据所述第一动态密码，进行认证。

[0019] 第三方面，本发明实施例提供了一种认证装置，应用于认证系统中的认证服务器，所述装置包括：

[0020] 接收模块，用于接收认证客户端发送的账号名及密码；

[0021] 校验模块，用于对所述账号名及所述密码进行校验，在校验成功后，生成二维码；

[0022] 发送模块，用于发送所述二维码至所述认证客户端，以使所述认证客户端展示所述二维码；在确定用户端扫描所述二维码后，向所述用户端发送访问接口信息，以使所述用户端根据所述访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息；

[0023] 所述接收模块，还用于接收所述应用服务器根据所述扫描二维码信息及所述应用账号信息反馈的第一应用账号标识；

[0024] 判断模块，用于判断所述账号名已绑定的应用账号标识中是否存在与所述第一应用账号标识相同的标识；

[0025] 获取模块，用于若所述判断模块的判断结果为存在相同的标识，则获取所述账号名已绑定的动态密钥；

[0026] 生成模块，用于根据所述动态密钥，生成动态密码，并发送所述动态密码至所述用户端；

[0027] 认证模块，用于接收并根据所述认证客户端发送的用户输入的第一动态密码，进行认证。

[0028] 第四方面，本发明实施例提供了一种认证装置，应用于认证系统中的认证客户端，所述装置包括：

[0029] 发送模块，用于发送用户输入的账号名及密码至认证服务器，以使所述认证服务器对所述账号名及所述密码进行校验，在校验成功后，生成二维码；

[0030] 接收模块，用于接收所述认证服务器发送的所述二维码，并展示所述二维码，以使所述用户端扫描所述二维码，并根据所述认证服务器发送的访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息；接收用户输入的第一动态密码；

[0031] 所述发送模块，还用于发送所述第一动态密码至所述认证服务器，以使所述认证服务器根据所述第一动态密码，进行认证。

[0032] 第五方面，本发明实施例提供了一种认证服务器，包括处理器和机器可读存储介质，所述机器可读存储介质存储有能够被所述处理器执行的机器可执行的指令，所述指令由所述处理器加载并执行：以实现本发明实施例第一方面所述的方法步骤。

[0033] 第六方面，本发明实施例提供了一种机器可读存储介质，所述机器可读存储介质

内存储有机器可执行的指令，所述指令由处理器加载并执行，以实现本发明实施例第一方面所述的方法步骤。

[0034] 第七方面，本发明实施例提供了一种认证客户端，包括处理器和机器可读存储介质，所述机器可读存储介质存储有能够被所述处理器执行的机器可执行的指令，所述指令由所述处理器加载并执行：以实现本发明实施例第二方面所述的方法步骤。

[0035] 第八方面，本发明实施例提供了一种机器可读存储介质，所述机器可读存储介质内存储有机器可执行的指令，所述指令由处理器加载并执行，以实现本发明实施例第二方面所述的方法步骤。

[0036] 本发明实施例提供的一种认证方法、装置及机器可读存储介质，认证服务器通过对认证客户端发送的账号名和密码进行校验，在校验成功后，生成二维码，并将二维码发送至认证客户端，认证客户端可以向用户展示二维码，认证服务器在确定用户端扫描二维码后，向用户端发送访问接口信息，使得用户端可以根据该访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息，应用服务器根据扫描二维码信息及应用账号信息向认证服务器反馈第一应用账号标识，如果账号名已绑定的应用账号标识中存在与第一应用账号标识相同的标识，则获取并根据账号名已绑定的动态密钥，生成动态密码，并发送动态密码至用户端，接收并根据认证客户端发送的用户输入的第一动态密码，进行认证。利用账号名与应用账号标识之间的绑定关系，在用户端的第一应用账号标识与账号名绑定的应用账号标识相同时，认证服务器才生成动态密码并下发，攻击者在攻击时，需要同时破解账号名、密码，还需要破解账号名绑定的应用账号标识和动态密码，破解难度较高，因此，提高了网络安全性。

附图说明

[0037] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术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的前提下，还可以根据这些附图获得其他的附图。

[0038] 图1为本发明实施例的应用于认证服务器的认证方法的流程示意图；

[0039] 图2为本发明实施例的应用于认证客户端的认证方法的流程示意图；

[0040] 图3为本发明实施例的认证方法的交互流程示意图；

[0041] 图4为本发明实施例的应用于认证服务器的认证装置的结构示意图；

[0042] 图5为本发明实施例的应用于认证客户端的认证装置的结构示意图；

[0043] 图6为本发明实施例的认证服务器的结构示意图；

[0044] 图7为本发明实施例的认证客户端的结构示意图。

具体实施方式

[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，所描述的实施例仅仅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做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] 为了提高网络安全性，本发明实施例提供了一种认证方法、装置、认证服务器、认证客户端及机器可读存储介质。下面首先对本发明实施例所提供的认证方法进行介绍。

[0047] 本发明实施例所提供的认证方法可以应用于认证系统，认证系统可以包括用户端、认证客户端、认证服务器和应用服务器，用户端可以为可扫描二维码的软件客户端，认证客户端可以为安装有浏览器等应用软件的硬件电子设备(例如个人计算机、手机等)，当然认证客户端也可以为认证服务器的软件客户端，在本实施例中，以认证客户端为硬件设备为例进行说明。认证服务器可以为网络管理服务器(即网管服务器)等提供认证服务的服务器，应用服务器可以为可扫描二维码应用软件的后台管理服务器。本实施例中的认证服务器与应用服务器不归属于同一厂商。

[0048] 如图1所示，本发明实施例所提供的一种认证方法，应用于认证服务器，该认证方法可以包括如下步骤：

[0049] S101，接收认证客户端发送的账号名及密码。

[0050] S102，对账号名及密码进行校验，在校验成功后，生成二维码。

[0051] S103，发送二维码至认证客户端，以使认证客户端展示该二维码。

[0052] S104，在确定用户端扫描二维码后，向用户端发送访问接口信息，以使用户端根据访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息。

[0053] S105，接收应用服务器根据扫描二维码信息及应用账号信息反馈的第一应用账号标识。

[0054] S106，判断账号名已绑定的应用账号标识中是否存在与第一应用账号标识相同的标识。

[0055] S107，若存在相同的标识，则获取账号名已绑定的动态密钥，根据该动态密钥，生成动态密码，并发送动态密码至用户端，接收并根据认证客户端发送的用户输入的第一动态密码，进行认证。

[0056] 如图2所示，本发明实施例所提供的一种认证方法，应用于认证客户端，该认证方法可以包括如下步骤：

[0057] S201，发送用户端输入的账号名及密码至认证服务器，以使认证服务器对账号名及密码进行校验，在校验成功后，生成二维码。

[0058] S202，接收认证服务器发送的二维码，并展示该二维码，以使用户端扫描该二维码，并根据认证服务器发送的访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息。

[0059] S203，接收用户输入的第一动态密码。

[0060] S204，发送第一动态密码至认证服务器，以使认证服务器根据第一动态密码，进行认证。

[0061] 用户可以在认证客户端上输入账号名和密码，由认证客户端将账号名和密码发送至认证服务器进行校验，如果校验成功，则生成二维码，认证服务器将生成的二维码发送给认证客户端，认证客户端上可以展示该二维码，以便用户利用用户端可以对该二维码进行扫描，认证服务器在确定用户端扫描二维码后，可以向用户端发送访问接口信息，用户端根据该访问接口信息向应用服务器发送扫描二维码信息和应用账号信息，应用服务器可以根据应用账号信息查找到对应的第一应用账号标识，并且根据扫描二维码信息向认证服务器

发送该第一应用账号标识，认证服务器可以在确定账号名已绑定的应用账号标识中存在与第一应用账号标识相同的标识时，获取动态密钥、生成动态密码，并将该动态密码下发给用户端，用户在得到动态密码后，可以在认证客户端上输入动态密码，认证服务器对输入的动态密码进行认证。通过本方案，利用账号名与应用账号标识之间的绑定关系，在用户端的第一应用账号标识存在于与账号名绑定的应用账号标识中时，认证服务器才生成动态密码并下发，攻击者在攻击时，需要同时破解账号名、密码，还需要破解账号名绑定的应用账号标识和动态密码，破解难度较高，提高了网络安全性。

[0062] 为了便于理解，下面从用户端、认证客户端、认证服务器和应用服务器的交互过程，对本发明实施例所提供的认证方法进行介绍，如图3所示，该认证方法可以包括如下步骤：

[0063] S301，认证客户端将用户输入的账号名和密码发送至认证服务器。

[0064] 认证客户端可以为安装有浏览器、网络管理软件、第三方应用等应用软件的电子设备，是一个登录认证的硬件电子设备，用户在认证客户端上输入账号名和密码，用户输入的账号名和密码是预先为该用户分配的，该密码为针对账号名分配的静态密码。这里的账号名和密码是用于登录认证服务器使用的。

[0065] S302，认证服务器对账号名和密码进行校验，在校验成功后，生成二维码。

[0066] 认证服务器在接收到账号名和密码后，由于认证服务器记录有账号名和密码的匹配关系，可以对账号名和密码进行校验，校验是否满足预设的匹配关系，如果不满足，则可以直接向认证客户端反馈校验失败的结果，由认证客户端提示用户账号名或密码错误。如果校验结果满足匹配关系，则说明校验成功，可以生成相应的二维码。具体生成二维码的方式，可以是在确定校验成功之后，随机生成一个32位的动态密钥，该动态密钥与账号名具有对应关系，根据该动态密钥，生成一个包含有动态密钥的信息的二维码。

[0067] S303，认证服务器发送二维码至认证客户端。

[0068] S304，认证客户端展示二维码。

[0069] S305，用户端扫描二维码。

[0070] 认证服务器在生成二维码后，将该二维码发送至认证客户端，由认证客户端展示该二维码。用户在观察到认证客户端上展示的二维码后，可以利用用户端对该二维码进行扫描。

[0071] 需要说明的是，在本实施例中，用户端可以为微信、支付宝等可扫描二维码的第三方应用软件的软件客户端，用户端可以安装在认证客户端上，当然也可以安装在于不同于认证客户端的其他移动设备上。

[0072] S306，认证服务器在确定用户端扫描二维码后，向用户端发送访问接口信息。

[0073] 用户端扫描二维码时，可以访问到认证服务器的页面，认证服务器在确定有用户端扫描二维码，即识别到用户端访问页面的事件之后，会向用户端发送一个访问接口信息，该访问接口信息中包含有应用服务器的访问地址。

[0074] S307，用户端根据访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息。

[0075] 访问接口信息中包含有应用服务器的访问地址，例如网页地址，则用户端可以向应用服务器进行访问，发送扫描二维码信息及应用账号信息至应用服务器。其中，扫描二维

码信息包括账号名及动态密钥，由于二维码中可以隐藏有账号名和动态密钥，用户端在扫描二维码之后，可以提取到账号名和动态密钥，将其发送给应用服务器，使得应用服务器可以识别出应该向哪一个认证服务器反馈信息；应用账号信息可以包括应用账号的账号名、国家、性别等信息。

[0076] S308，应用服务器根据扫描二维码信息及应用账号信息反馈第一应用账号标识至认证服务器。

[0077] 应用服务器在接收到应用账号信息后，针对同一个应用账号，可以查找到唯一的应用账号标识，基于扫描二维码信息，可以确定向哪一个认证服务器反馈查找到的第一应用账号标识。

[0078] S309，认证服务器在确定账号名已绑定的应用账号标识中存在与第一应用账号标识相同的标识时，获取并根据账号名已绑定的动态密钥，生成动态密码。

[0079] 若认证服务器中绑定了账号名、应用账号标识和对应的动态密钥，在接收到应用服务器反馈的第一应用账号标识之后，认证服务器需要判断账号名已绑定的应用账号标识中是否存在与第一应用账号标识相同的标识，如果存在相同的标识，则根据已绑定的动态密钥生成动态密码，并基于动态密码进行认证。

[0080] 可选的，若账号名已绑定的应用账号标识不存在与第一应用账号标识相同的标识，则认证服务器可以确定认证失败。

[0081] 如果账号名已绑定的应用账号标识与第一应用账号标识不同，则说明当前扫描二维码的应用账号标识并不是之前已与账号名绑定的应用账号标识，该应用账号标识的用户即可能为非法用户，则可以确定认证失败，此时，认证服务器可以向用户端反馈一个错误信息，例如，提示用户端使用绑定的应用账号获取动态密码。

[0082] 如果用户是第一次登陆认证，认证服务器上并没有记录过账号名、应用账号标识和动态密钥的绑定关系，因此，在账号名未绑定应用账号标识时，需要对账号名、应用账号标识和动态密钥进行绑定。

[0083] 由此，认证服务器还可以执行如下步骤：

[0084] A1、若账号名未绑定应用账号标识，则随机生成动态密钥，并将动态密钥、账号名与第一应用账号标识进行绑定；

[0085] A2、根据动态密钥，生成动态密码；

[0086] A3、发送动态密码至用户端；

[0087] A4、接收并根据认证客户端发送的用户输入的第一动态密码，进行认证。

[0088] 如果账号名没有绑定过应用账号标识，则可以随机的生成一个动态密钥，并将动态密钥、账号名和第一应用账号标识进行绑定。

[0089] 为了保证动态密钥的安全性，往往将动态密钥设置的位数较多，例如32位，但是为了方便用户使用，需要给用户展示一个位数较少的动态密码，因此，可以根据动态密钥生成动态密码。根据动态密钥生成动态密码的方式，可以采用双因素认证方式。

[0090] 可选的，根据动态密钥生成动态密码的方式，具体可以为：

[0091] 根据动态密钥，利用预设哈希加密算法，生成当前时刻的动态密码。

[0092] 预设哈希加密算法可以为HmacSHA1(键控哈希)加密算法。

[0093] 双因素认证是指采用基于时间、时间、密钥等多个变量而生成的一次性密码来代

替传统的静态密码，每次认证时的随机参数不同，所以每次产生的动态密码也不同，由于每次生成动态密码时参数的随机性，保证了每次动态密码的不可预测性，从而在最基本的密码认证环节保证了网络的安全性。使用动态密码和HmacSHA1加密算法可以创建生成SecretKeySpec(KeySpec接口的实现类)，构建密钥规范，生成动态密码。

[0094] S310，认证服务器发送动态密码至用户端。

[0095] 认证服务器在生成动态密码后，即可将动态密码发送至用户端，只需要消耗少量的用户端的网络流量，不再需要消耗用户的短信费用，节约了用户的成本。

[0096] S311，认证客户端将用户输入的第一动态密码发送至认证服务器。

[0097] 用户在接收到认证服务器下发的动态密码之后，可以在认证客户端上输入自己在用户端上接收到的动态密码，认证客户端将用户输入的第一动态密码发送至认证服务器，由认证服务器进行认证。

[0098] S312，认证服务器根据第一动态密码，进行认证。

[0099] 认证服务器在接收到第一动态密码后，可以根据第一动态密码进行认证，如上述，第一动态密码可以为基于双因素认证生成的动态密码，则可选的，认证服务器具体可以执行如下步骤：

[0100] 接收认证客户端发送的用户输入的账号名及第一动态密码；

[0101] 根据账号名，获取账号名已绑定的动态密钥；

[0102] 根据动态密钥，利用预设哈希加密算法，生成当前时刻的预设时间段内的所有动态密码；

[0103] 判断生成的所有动态密码中是否存在与第一动态密码一致的动态密码；

[0104] 若存在，则确定认证成功；

[0105] 若不存在，则确定认证失败。

[0106] 认证服务器可以获取到认证客户端上用户输入的第一动态密码和账户名，根据账户名可以获取到该账户名已绑定的动态密码，通过该动态密钥和当前时刻对第一动态密码进行校验，可以设置动态密码的有效时间，即可以根据动态密钥，利用与生成向用户端下发的动态密码的相同哈希加密算法，生成当前时刻的预设时间段内的所有动态密码，例如当前时刻为13:00:00，则可以生成12:59:30-13:00:00之间所有的动态密码，也就是说，设置了动态密码30秒的有效时间，在这30秒认证服务器基于同一个动态密钥所生成的动态密码中一定有某一些动态密码一致。则可以判断生成的所有动态密码中是否存在与第一动态密码一致的动态密码，如果存在，则说明下发的动态密码可用，认证可以通过。如果不存在，则说明下发动态密码到用户输入第一动态密码的间隔时间过长，为防止是非法用户恶意盗取动态密码，可以确定认证失败，提示用户重新获取动态密码。

[0107] 应用本实施例，认证服务器通过对认证客户端发送的账号名和密码进行校验，在校验成功后，生成二维码，并将二维码发送至认证客户端，认证客户端可以向用户展示二维码，认证服务器在确定用户端扫描二维码后，向用户端发送访问接口信息，使得用户端可以根据该访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息，应用服务器根据扫描二维码信息及应用账号信息向认证服务器反馈第一应用账号标识，如果账号名已绑定的应用账号标识中存在与第一应用账号标识相同的标识，则获取并根据账号名已绑定的动态密钥，生成动态密码，并发送动态密码至用户端，接收并根据认证客户端发送的用户输

入的第一动态密码，进行认证。利用账号名与应用账号标识之间的绑定关系，在用户端的第一应用账号标识与账号名绑定的应用账号标识相同时，认证服务器才生成动态密码并下发，攻击者在攻击时，需要同时破解账号名、密码，还需要破解账号名绑定的应用账号标识和动态密码，破解难度较高，因此，提高了网络安全性。

[0108] 相应于上述方法实施例，本发明实施例提供了一种认证装置，应用于认证系统中的认证服务器，如图4所示，该认证装置可以包括：

[0109] 接收模块410，用于接收认证客户端发送的账号名及密码；

[0110] 校验模块420，用于对所述账号名及所述密码进行校验，在校验成功后，生成二维码；

[0111] 发送模块430，用于发送所述二维码至所述认证客户端，以使所述认证客户端展示所述二维码；在确定用户端扫描所述二维码后，向所述用户端发送访问接口信息，以使所述用户端根据所述访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息；

[0112] 所述接收模块410，还用于接收所述应用服务器根据所述扫描二维码信息及所述应用账号信息反馈的第一应用账号标识；

[0113] 判断模块440，用于判断所述账号名已绑定的应用账号标识中是否存在与所述第一应用账号标识相同的标识；

[0114] 获取模块450，用于若所述判断模块的判断结果为存在相同的标识，则获取所述账号名已绑定的动态密钥；

[0115] 生成模块460，用于根据所述动态密钥，生成动态密码，并发送所述动态密码至所述用户端；

[0116] 认证模块470，用于接收并根据所述认证客户端发送的用户输入的第一动态密码，进行认证。

[0117] 可选的，所述装置还可以包括：

[0118] 绑定模块，用于若确定所述账号名未绑定应用账号标识，则随机生成动态密钥，并将所述动态密钥、所述账号名与所述第一应用账号标识进行绑定。

[0119] 可选的，所述生成模块460，具体可以用于：

[0120] 根据所述动态密钥，利用预设哈希加密算法，生成当前时刻的动态密码；

[0121] 所述认证模块470，具体可以用于：

[0122] 接收所述认证客户端发送的用户输入的账号名及第一动态密码；

[0123] 根据所述账号名，获取所述账号名已绑定的动态密钥；

[0124] 根据所述动态密钥，利用所述预设哈希加密算法，生成当前时刻的预设时间段内的所有动态密码；

[0125] 判断生成的所有动态密码中是否存在与所述第一动态密码一致的动态密码；

[0126] 若存在，则确定认证成功；

[0127] 若不存在，则确定认证失败。

[0128] 可选的，所述认证模块470，还可以用于：

[0129] 若所述判断模块的判断结果为不存在相同的标识，则确定认证失败。

[0130] 相应于上述方法实施例，本发明实施例还提供了一种认证装置，应用于认证系统中的认证客户端，如图5所示，该认证装置可以包括：

[0131] 发送模块510，用于发送用户输入的账号名及密码至认证服务器，以使所述认证服务器对所述账号名及所述密码进行校验，在校验成功后，生成二维码；

[0132] 接收模块520，用于接收所述认证服务器发送的所述二维码，并展示所述二维码，以使所述用户端扫描所述二维码，并根据所述认证服务器发送的访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息；接收用户输入的第一动态密码；

[0133] 所述发送模块510，还用于发送所述第一动态密码至所述认证服务器，以使所述认证服务器根据所述第一动态密码，进行认证。

[0134] 应用本实施例，认证服务器通过对认证客户端发送的账号名和密码进行校验，在校验成功后，生成二维码，并将二维码发送至认证客户端，认证客户端可以向用户展示二维码，认证服务器在确定用户端扫描二维码后，向用户端发送访问接口信息，使得用户端可以根据该访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息，应用服务器根据扫描二维码信息及应用账号信息向认证服务器反馈第一应用账号标识，如果账号名已绑定的应用账号标识中存在与第一应用账号标识相同的标识，则获取并根据账号名已绑定的动态密钥，生成动态密码，并发送动态密码至用户端，接收并根据认证客户端发送的用户输入的第一动态密码，进行认证。利用账号名与应用账号标识之间的绑定关系，在用户端的第一应用账号标识与账号名绑定的应用账号标识相同时，认证服务器才生成动态密码并下发，攻击者在攻击时，需要同时破解账号名、密码，还需要破解账号名绑定的应用账号标识和动态密码，破解难度较高，因此，提高了网络安全性。

[0135] 本发明实施例还提供了一种认证服务器，如图6所示，包括处理器601和机器可读存储介质602，所述机器可读存储介质602存储有能够被所述处理器601执行的机器可执行的指令，所述指令由所述处理器601加载并执行：以实现本发明实施例所提供的应用于认证服务器的认证方法的步骤。

[0136] 本发明实施例还提供了一种认证客户端，如图7所示，包括处理器701和机器可读存储介质702，所述机器可读存储介质702存储有能够被所述处理器701执行的机器可执行的指令，所述指令由所述处理器701加载并执行：以实现本发明实施例所提供的应用于认证客户端的认证方法的步骤。

[0137] 上述机器可读存储介质可以包括RAM(Random Access Memory，随机存取存储器)，也可以包括NVM(Non-volatile Memory，非易失性存储器)，例如至少一个磁盘存储器。可选的，机器可读存储介质还可以是至少一个位于远离前述处理器的存储装置。

[0138] 上述处理器可以是通用处理器，包括CPU(Central Processing Unit，中央处理器)、NP(Network Processor，网络处理器)等；还可以是DSP(Digital Signal Processor，数字信号处理器)、ASIC(Application Specific Integrated Circuit，专用集成电路)、FPGA(Field-Programmable Gate Array，现场可编程门阵列)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。

[0139] 机器可读存储介质602与处理器601之间、机器可读存储介质702与处理器701之间可以通过有线连接或者无线连接的方式进行数据传输，并且认证服务器与认证客户端之间以及认证服务器、认证客户端与其他的设备之间可以通过有线通信接口或者无线通信接口进行通信。图6和图7所示的仅为通过总线进行数据传输的示例，不作为具体连接方式的限定。

[0140] 本实施例中，处理器601通过读取机器可读存储介质602中存储的机器可执行的指令，处理器701通过读取机器可读存储介质702中存储的机器可执行的指令，通过加载并执行指令，能够实现：认证服务器通过对认证客户端发送的账号名和密码进行校验，在校验成功后，生成二维码，并将二维码发送至认证客户端，认证客户端可以向用户展示二维码，认证服务器在确定用户端扫描二维码后，向用户端发送访问接口信息，使得用户端可以根据该访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息，应用服务器根据扫描二维码信息及应用账号信息向认证服务器反馈第一应用账号标识，如果账号名已绑定的应用账号标识中存在与第一应用账号标识相同的标识，则获取并根据账号名已绑定的动态密钥，生成动态密码，并发送动态密码至用户端，接收并根据认证客户端发送的用户输入的第一动态密码，进行认证。利用账号名与应用账号标识之间的绑定关系，在用户端的第一应用账号标识与账号名绑定的应用账号标识相同时，认证服务器才生成动态密码并下发，攻击者在攻击时，需要同时破解账号名、密码，还需要破解账号名绑定的应用账号标识和动态密码，破解难度较高，因此，提高了网络安全性。

[0141] 另外，本发明实施例还提供了一种机器可读存储介质，所述机器可读存储介质内存储有机器可执行的指令，所述指令被处理器加载并执行，以实现本发明实施例所提供的应用于认证服务器的认证方法的步骤。

[0142] 本发明实施例还提供了一种机器可读存储介质，所述机器可读存储介质内存储有机器可执行的指令，所述指令被处理器加载并执行，以实现本发明实施例所提供的应用于认证客户端的认证方法的步骤。

[0143] 本实施例中，机器可读存储介质存储有处理器在运行时执行本发明实施例所提供的应用于认证服务器和认证客户端的认证方法的机器可执行的指令，因此能够实现：认证服务器通过对认证客户端发送的账号名和密码进行校验，在校验成功后，生成二维码，并将二维码发送至认证客户端，认证客户端可以向用户展示二维码，认证服务器在确定用户端扫描二维码后，向用户端发送访问接口信息，使得用户端可以根据该访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息，应用服务器根据扫描二维码信息及应用账号信息向认证服务器反馈第一应用账号标识，如果账号名已绑定的应用账号标识中存在与第一应用账号标识相同的标识，则获取并根据账号名已绑定的动态密钥，生成动态密码，并发送动态密码至用户端，接收并根据认证客户端发送的用户输入的第一动态密码，进行认证。利用账号名与应用账号标识之间的绑定关系，在用户端的第一应用账号标识与账号名绑定的应用账号标识相同时，认证服务器才生成动态密码并下发，攻击者在攻击时，需要同时破解账号名、密码，还需要破解账号名绑定的应用账号标识和动态密码，破解难度较高，因此，提高了网络安全性。

[0144] 对于认证服务器、认证客户端及机器可读存储介质实施例而言，由于其涉及的方法内容基本相似于前述的方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0145] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要

素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0146] 本说明书中的各个实施例均采用相关的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置、认证服务器、认证客户端以及机器可读存储介质实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0147] 以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内所作的任何修改、等同替换、改进等，均包含在本发明的保护范围内。

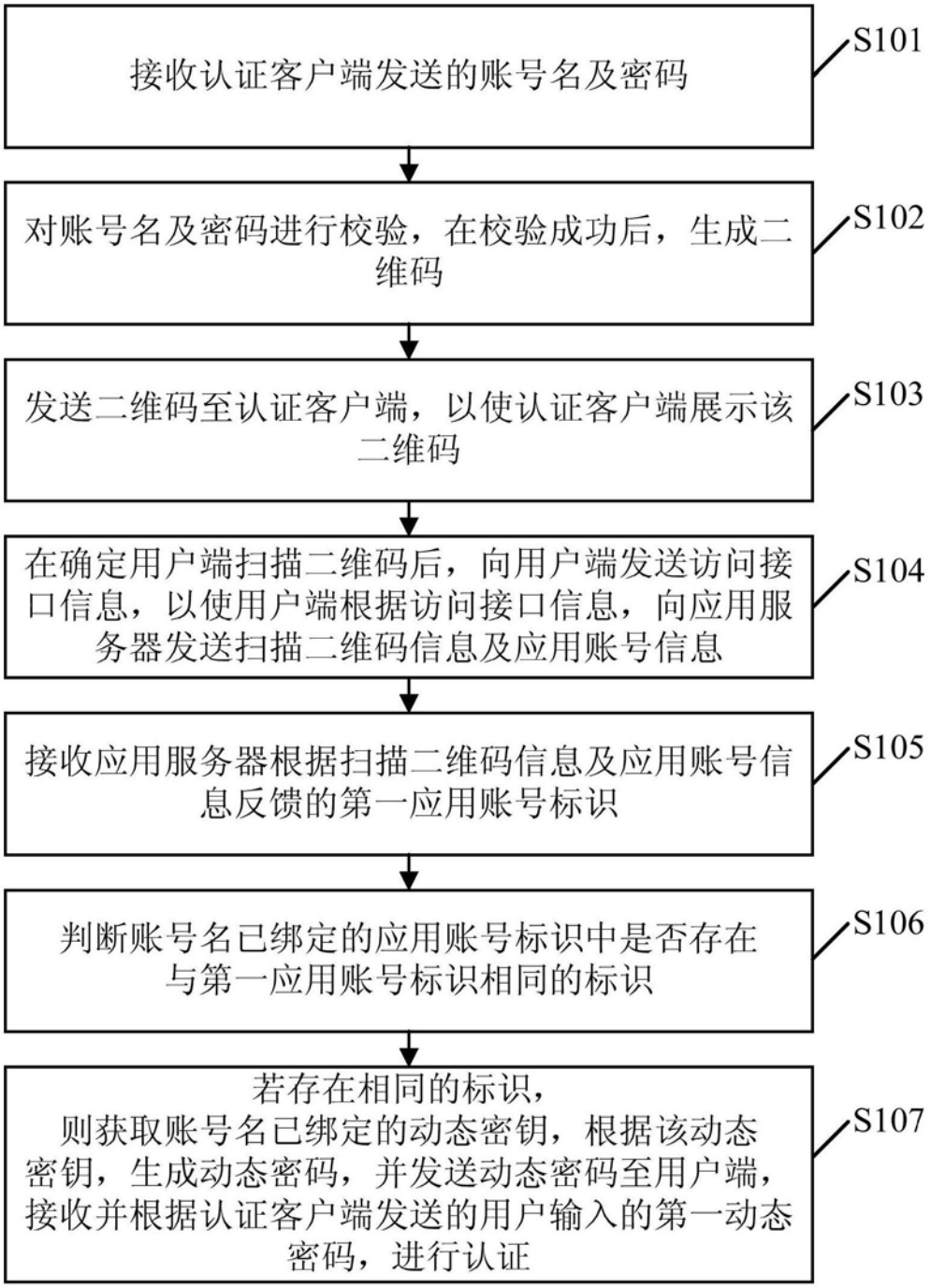

接收认证客户端发送的账号名及密码
S101
对账号名及密码进行校验，在校验成功后，生成二维码
S102
发送二维码至认证客户端，以使认证客户端展示该二维码
S103
在确定用户端扫描二维码后，向用户端发送访问接口信息，以使用户端根据访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息
S104
接收应用服务器根据扫描二维码信息及应用账号信息反馈的第一应用账号标识
S105
判断账号名已绑定的应用账号标识中是否存在与第一应用账号标识相同的标识
S106
若存在相同的标识，
则获取账号名已绑定的动态密钥，根据该动态密钥，生成动态密码，并发送动态密码至用户端，接收并根据认证客户端发送的用户输入的第一动态密码，进行认证
S107

图1

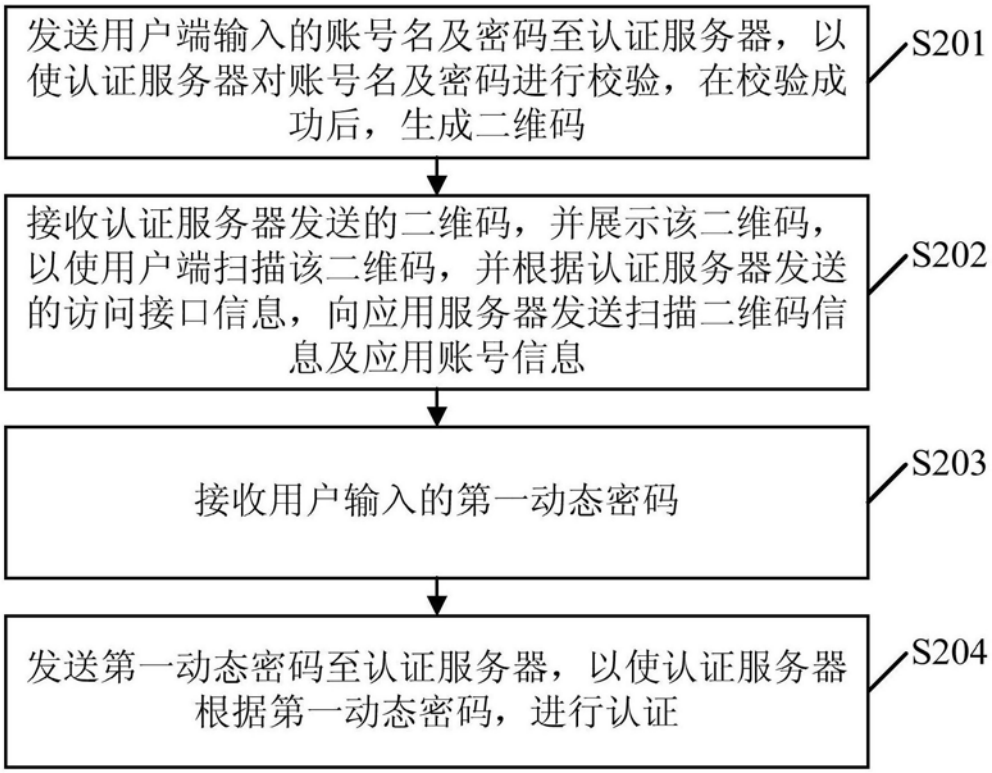

发送用户端输入的账号名及密码至认证服务器，以使认证服务器对账号名及密码进行校验，在校验成功后，生成二维码
S201
接收认证服务器发送的二维码，并展示该二维码，以使用户端扫描该二维码，并根据认证服务器发送的访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息
S202
接收用户输入的第一动态密码
S203
发送第一动态密码至认证服务器，以使认证服务器根据第一动态密码，进行认证
S204

图2

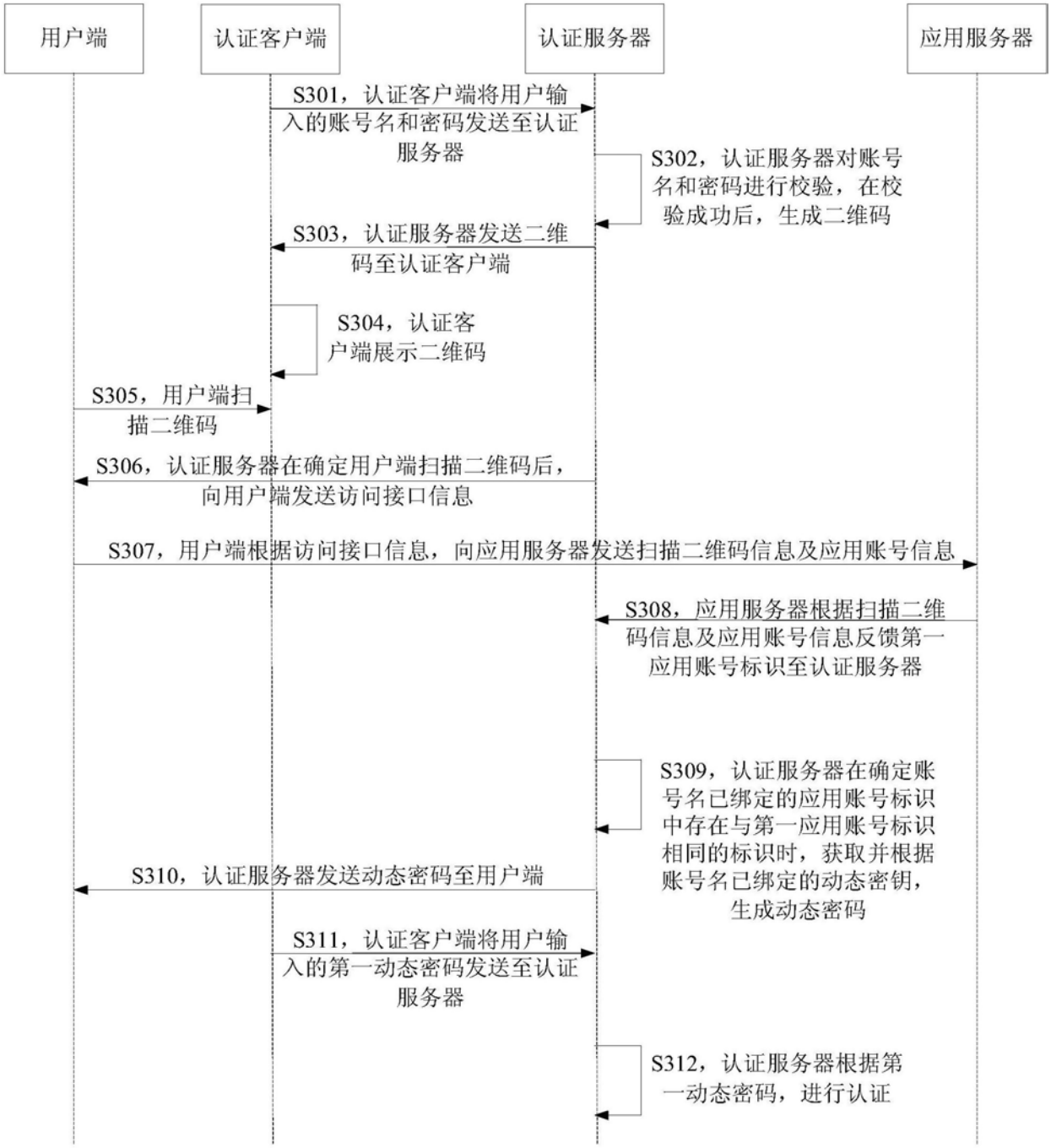

用户端
认证客户端
认证服务器
应用服务器
S301，认证客户端将用户输入的账号名和密码发送至认证服务器
S302，认证服务器对账号名和密码进行校验，在校验成功后，生成二维码
S303，认证服务器发送二维码至认证客户端
S304，认证客户端展示二维码
S305，用户端扫描二维码
S306，认证服务器在确定用户端扫描二维码后，向用户端发送访问接口信息
S307，用户端根据访问接口信息，向应用服务器发送扫描二维码信息及应用账号信息
S308，应用服务器根据扫描二维码信息及应用账号信息反馈第一应用账号标识至认证服务器
S309，认证服务器在确定账号名已绑定的应用账号标识中存在与第一应用账号标识相同的标识时，获取并根据账号名已绑定的动态密钥，生成动态密码
S310，认证服务器发送动态密码至用户端
S311，认证客户端将用户输入的第一动态密码发送至认证服务器
S312，认证服务器根据第一动态密码，进行认证

图3

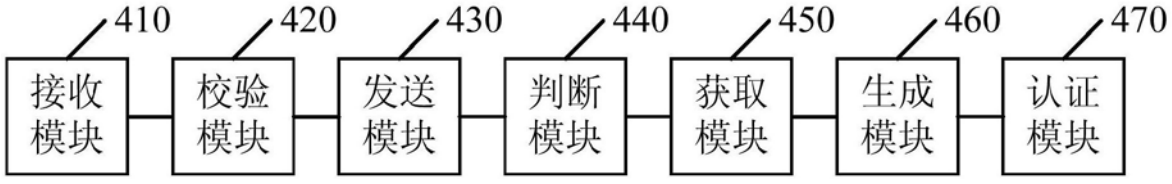

410
420
430
440
450
460
470
接收模块
校验模块
发送模块
判断模块
获取模块
生成模块
认证模块

图4

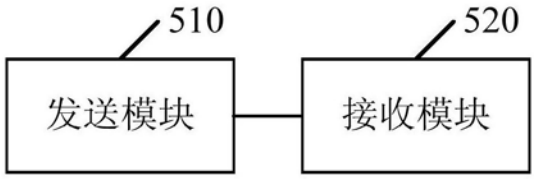


图5

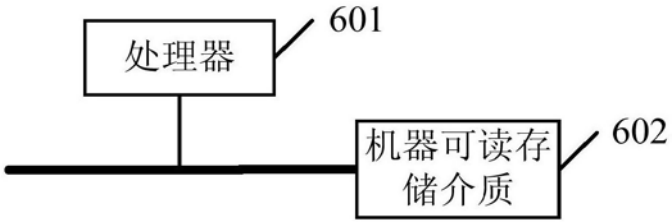


图6

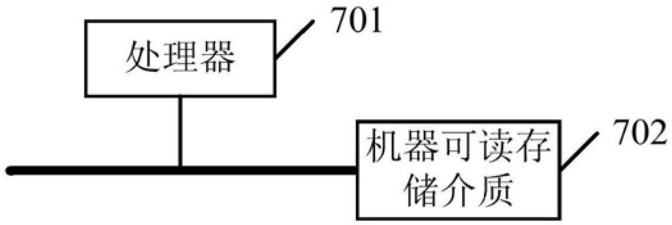


图7