(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 107277059 A
(43)申请公布日 2017.10.20

(21)申请号 201710670455.8

(22)申请日 2017.08.08

(71)申请人 沈阳东青科技有限公司
地址 110000 辽宁省沈阳市浑南区文溯街19-1号205室25号工位

(72)发明人 岳笑含 高明超

(74)专利代理机构 沈阳亚泰专利商标代理有限公司 21107
代理人 史力伏

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)

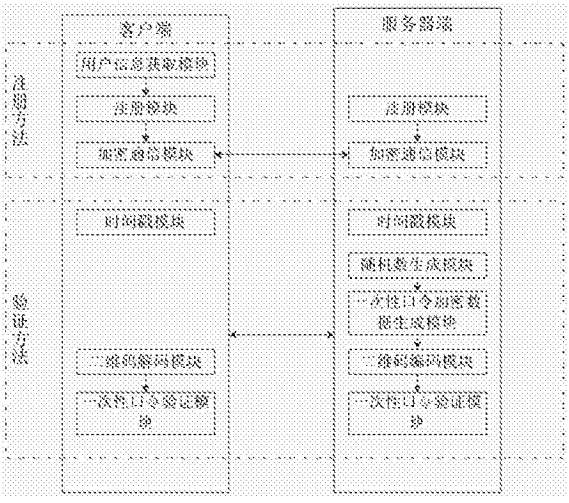
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种基于二维码的一次性口令身份认证方法及系统

(57)摘要

本发明涉及信息安全技术领域，特别是涉及一种基于二维码的一次性口令身份认证方法及系统。其在保证登陆安全性基础上能够解决用户在登陆系统时每次需要输入口令以及一次性口令认证方法难以普及的问题，为更多的用户带来更好的用户体验。基于二维码的一次性口令身份认证系统包括客户端和服务器端；基于二维码的一次性口令身份认证方法，包括注册阶段及验证阶段。



CN 107277059 A

1.一种基于二维码的一次性口令身份认证系统，其特征在于，包括客户端和服务器端；

所述客户端包括：

用户信息获取模块；用于获取客户端用户的注册信息，注册信息应包含用户的唯一ID；

加密通信模块；用于客户端与服务器端之间建立安全信道连接；

时间戳模块；用于生成时间戳，保障通信消息新鲜性；

二维码解码模块；用于将包含一次性口令加密数据的图片解码；

注册模块；在所述注册模块中客户端与服务端进行相互通信，以完成注册；

一次性口令验证模块；在一次性口令验证模块中客户端与服务器端进行交互通信，以完成一次性口令身份认证；

所述服务器端包括：

加密通信模块；用于客户端与服务器端之间建立安全信道连接；

时间戳模块；用于生成时间戳，保障通信消息新鲜性；

随机数生成模块；作为生成一次性口令的主要参数；

一次性口令加密数据生成模块；利用所述的随机数生成模块所生成的随机数参数以及服务器端主密钥参数生成一次性口令加密数据；

二维码编码模块；用于将一次性口令加密数据二进制后编码成为二维码图片；

注册模块，在该模块中服务器端与客户端进行交互通信，以完成注册；

一次性口令验证模块，在该模块中服务器端与客户端进行交互通信，以完成一次性口令身份认证。

2.一种基于二维码的一次性口令身份认证方法，其特征在于：包括注册阶段及验证阶段；所述注册阶段的注册方法包括以下步骤：

S101、客户端获取用户唯一ID信息；

S102、客户端与服务器端建立安全通信连接，将所述用户唯一ID信息发送给服务器端；

S103、服务器端通过接收到的用户唯一ID参数计算出该用户的用户长期私钥，并将所述用户长期私钥发送给客户端；

S104、客户端接收到服务器端为其颁发的所述用户长期私钥，将该私钥保存在本地设备中；

所述验证阶段的验证方法包括以下步骤：

S201、客户端发送所述用户唯一ID信息参数及时间戳参数到服务器端；

S202、服务器端接收到所述的用户唯一ID及所述的时间戳，判断时间戳有效性，如果无效则拒绝认证请求，否则获取随机数，该随机数作为一次性口令数据；

S203、服务器端利用所述一次性口令数据以及所述用户唯一ID对应的所述用户长期私钥，计算一次性口令加密数据；

S204、服务器端将一次性口令加密数据生成二维码图片数据，将二维码图片数据以及时间戳参数发送到客户端；

S205、客户端接收到所述二维码图片数据以及时间戳，判断时间戳有效性，如果无效则拒绝该验证信息，否则利用所述用户长期私钥以及二维码解码模块解密一次性口令加密数据，获得一次性口令数据；

S206、客户端将所述的一次性口令数据生成的时间戳参数发送给服务器端；

S207、服务器端接收到所述一次性口令数据以及时间戳，判断时间戳有效性，如果无效则拒绝认证请求，否则比对一次性口令数据与之前发送一次性口令数据是否相同，如果不同则拒绝系统登录请求，否则准许登陆系统。

3.根据权利要求2所述的一种基于二维码的一次性口令身份认证方法，其特征在于：所述注册方法包括：

用户信息获取模块，用于获取客户端用户的注册信息，注册信息包含用户的唯一ID；

加密通信模块，用于客户端与服务器端之间建立安全信道连接；

注册模块，与所述的获取模块关联，结合所述用户信息，并基于所述的加密通信模块建立客户端与服务器端的安全连接，用于将用户的唯一ID信息发送给服务器端，服务器端接收到之后将根据用户唯一ID为客户端发送长期私钥，完成用户注册；

所述验证方法包括：

时间戳模块，用于生成时间戳，保障通信消息新鲜性；

随机数生成模块，作为生成一次性口令的主要参数；

一次性口令加密数据生成模块，利用所述的随机数生成模块所生成的随机数参数以及服务器端主密钥参数生成一次性口令加密数据；

二维码编码模块，用于将一次性口令加密数据二进制后编码成为二维码图片；

二维码解码模块，用于将包含一次性口令加密数据的图片解码；

一次性口令验证模块，客户端通过所述的二维码解码模块，获取一次性口令加密数据，利用所述的用户长期私钥解密一次性口令加密数据，获得一次性口令数据，客户端将解密后的一次性口令数据通过所述的加密通讯模块发送给服务器端；服务器端获取到一次性口令后与其所发送的一次性口令进行比对来判断口令的有效性，如果有效则身份认证通过，否则不通过。

一种基于二维码的一次性口令身份认证方法及系统

技术领域

[0001] 本发明涉及信息安全技术领域，特别是涉及一种基于二维码的一次性口令身份认证方法及系统。

背景技术

[0002] 随着互联网技术和移动设备的快速发展，越来越多的计算设备链接到网络中，并交换着大量的信息和资源，随之而来的安全问题也日益凸显。为了阻止信息数据被非法或非授权用户访问，远程用户身份认证成为了安全核心服务中的一种重要安全机制。

[0003] 在开放的网络环境下，用户身份认证安全机制用于建立客户端和服务端之间的信任关系。在众多的身份认证方法中，基于口令的认证方法是目前广泛使用的一种用于校验用户登陆信息和有效性的方法。其中，一次性口令方法，由于其具备消息新鲜性的特点，可以有效避免传统静态口令所带来的各种安全隐患，例如重放攻击、字典攻击以及仿冒攻击等，因此被一些安全等级较高的系统所采用。

[0004] 一次性口令方法虽然较传统的静态口令具备更高的安全性，然而并不能容易的被用户所记忆。因此，用户需要借助额外的技术来使用一次性口令方法实现身份认证。传统的一次性口令方法有：基于智能卡、基于时间同步令牌以及基于短信服务等技术方法。这些方法虽然可行，但很明显制约了一次性口令方法的易用性和普适性。

[0005] 由于移动电话技术的快速发展，用户通过摄像头扫描设备获取二维码信息成为了可能，因此本发明基于二维码实现一次性口令的身份认证方法及系统。

发明内容

[0006] 本发明就是针对现有技术存在的缺陷，提供一种基于二维码的一次性口令身份认证方法及系统，其主要解决了三方面问题。

[0007] 一是如何提供一种安全的一次性口令身份认证方法的问题。

[0008] 二是如何解决用户在认证时每次需要手动输入口令的问题。

[0009] 三是如何将一次性口令认证方法给用户带来更好用户体验的问题。

[0010] 其在保证登陆安全性基础上能够解决用户在登陆系统时每次需要输入口令以及一次性口令认证方法难以普及的问题，为更多的用户带来更好的用户体验。

[0011] 为实现上述目的，本发明采用如下技术方案。

[0012] 一种基于二维码的一次性口令身份认证系统，包括客户端和服务器端。

[0013] 所述客户端包括：

[0014] 用户信息获取模块；用于获取客户端用户的注册信息，注册信息应包含用户的唯一ID。

[0015] 加密通信模块；用于客户端与服务器端之间建立安全信道连接。

[0016] 时间戳模块；用于生成时间戳，保障通信消息新鲜性。

[0017] 二维码解码模块；用于将包含一次性口令加密数据的图片解码。

[0018] 注册模块;在所述注册模块中客户端与服务端进行相互通信,以完成注册;

[0019] 一次性口令验证模块;在一次性口令验证模块中客户端与服务器端进行交互通信,以完成一次性口令身份认证。

[0020] 所述服务器端包括。

[0021] 加密通信模块;用于客户端与服务器端之间建立安全信道连接。

[0022] 时间戳模块;用于生成时间戳,保障通信消息新鲜性。

[0023] 随机数生成模块;作为生成一次性口令的主要参数。

[0024] 一次性口令加密数据生成模块;利用所述的随机数生成模块所生成的随机数参数以及服务器端主密钥参数生成一次性口令加密数据。

[0025] 二维码编码模块;用于将一次性口令加密数据二进制后编码成为二维码图片。

[0026] 注册模块,在该模块中服务器端与客户端进行交互通信,以完成注册。

[0027] 一次性口令验证模块,在该模块中服务器端与客户端进行交互通信,以完成一次性口令身份认证。

[0028] 一种基于二维码的一次性口令身份认证方法,包括注册阶段及验证阶段;所述注册阶段的注册方法包括以下步骤:

[0029] S101、客户端获取用户唯一ID信息。

[0030] S102、客户端与服务器端建立安全通信连接,将所述用户唯一ID信息发送给服务器端。

[0031] S103、服务器端通过接收到的用户唯一ID参数计算出该用户的用户长期私钥,并将所述用户长期私钥发送给客户端。

[0032] S104、客户端接收到服务器端为其颁发的所述用户长期私钥,将该私钥保存在本地设备中。

[0033] 所述验证阶段的验证方法包括以下步骤:

[0034] S201、客户端发送所述用户唯一ID信息参数及时间戳参数到服务器端。

[0035] S202、服务器端接收到所述的用户唯一ID及所述的时间戳,判断时间戳有效性,如果无效则拒绝认证请求,否则获取随机数,该随机数作为一次性口令数据。

[0036] S203、服务器端利用所述一次性口令数据以及所述用户唯一ID对应的所述用户长期私钥,计算一次性口令加密数据。

[0037] S204、服务器端将一次性口令加密数据生成二维码图片数据,将二维码图片数据以及时间戳参数发送到客户端。

[0038] S205、客户端接收到所述二维码图片数据以及时间戳,判断时间戳有效性,如果无效则拒绝该验证信息,否则利用所述用户长期私钥以及二维码解码模块解密一次性口令加密数据,获得一次性口令数据。

[0039] S206、客户端将所述的一次性口令数据生成的时间戳参数发送给服务器端;

[0040] S207、服务器端接收到所述一次性口令数据以及时间戳,判断时间戳有效性,如果无效则拒绝认证请求,否则比对一次性口令数据与之前发送一次性口令数据是否相同,如果不同则拒绝系统登录请求,否则准许登陆系统。

[0041] 具体地,所述注册方法包括:

[0042] 用户信息获取模块,用于获取客户端用户的注册信息,注册信息包含用户的唯一

ID。

[0043] 加密通信模块，用于客户端与服务器端之间建立安全信道连接。

[0044] 注册模块，与所述的获取模块关联，结合所述用户信息，并基于所述的加密通信模块建立客户端与服务器端的安全连接，用于将用户的唯一ID信息发送给服务器端，服务器端接收到之后将根据用户唯一ID为客户端发送长期私钥，完成用户注册。

[0045] 所述验证方法包括：

[0046] 时间戳模块，用于生成时间戳，保障通信消息新鲜性。

[0047] 随机数生成模块，作为生成一次性口令的主要参数。

[0048] 一次性口令加密数据生成模块，利用所述的随机数生成模块所生成的随机数参数以及服务器端主密钥参数生成一次性口令加密数据；

[0049] 二维码编码模块，用于将一次性口令加密数据二进制后编码成为二维码图片。

[0050] 二维码解码模块，用于将包含一次性口令加密数据的图片解码。

[0051] 一次性口令验证模块，客户端通过所述的二维码解码模块，获取一次性口令加密数据，利用所述的用户长期私钥解密一次性口令加密数据，获得一次性口令数据，客户端将解密后的一次性口令数据通过所述的加密通讯模块发送给服务器端；服务器端获取到一次性口令后与其所发送的一次性口令进行比对来判断口令的有效性，如果有效则身份认证通过，否则不通过。

[0052] 与现有技术相比本发明有益效果。

[0053] 本发明实施例由客户端根据用户自身唯一ID通过服务器端为其颁发用户长期私钥，在用户登陆系统时可向服务器端请求一次性口令二维码，通过该二维码客户端可实现一次性口令的身份认证进而获得系统登陆访问权限。该方法不但提高了身份认证方式的安全性，而且为用户提供了更好的用户体验。

附图说明

[0054] 下面结合附图和具体实施方式对本发明做进一步说明。本发明保护范围不仅局限于以下内容的表述。

[0055] 图1是本发明基于二维码的一次性口令身份认证方法的一个实施例的结构示意图。

[0056] 图2是本发明基于二维码的一次性口令身份认证方法的一个实施例的注册方法流程示意图。

[0057] 图3是本发明基于二维码的一次性口令身份认证方法的一个实施例的验证方法流程示意图。

具体实施方式

[0058] 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。以下对至少一个示例性实施例的描述实际上仅仅是说明性的，决不作为对本发明及其应用或使用的任何限制。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。

[0059] 除非另外具体说明，否则在这些实施例中阐述的部件和步骤的相对布置、数字表达式和数值不限制本发明的范围。

[0060] 同时，应当明白，为了便于描述，附图中所示出的各个部分的尺寸并不是按照实际的比例关系绘制的。

[0061] 对于相关领域普通技术人员已知的技术、方法和设备可能不作详细讨论，但在适当情况下，所述技术、方法和设备应当被视为授权说明书的一部分。

[0062] 在这里示出和讨论的所有示例中，任何具体值应被解释为仅仅是示例性的，而不是作为限制。因此，示例性实施例的其它示例可以具有不同的值。

[0063] 应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步讨论。

[0064] 由于传统基于静态口令的身份认证方式存在例如重放攻击、字典攻击以及仿冒攻击等各种安全隐患，且用户在登陆系统进行身份认证时每次需要手动输入，因此存在安全性和便捷性等问题；此外，传统的一次性口令技术虽然可以增强身份认证的安全性，但由于技术门槛较高无法有效普及大众。针对上述问题，本发明提出基于二维码的一次性口令身份认证方法，下面详细说明。

[0065] 请参阅图1，图1为本发明的一个实施例结构示意图。

[0066] 如图1所示，本发明包括客户端和服务器端，以及注册方法和验证方法，其中客户端在注册方法中至少包括：用户信息获取模块，用于获取用户信息，包含用户唯一ID信息，在这里，用户唯一ID信息可以是硬件设备唯一标识码、手机号、邮箱地址、身份证等具有唯一性的信息，在身份认证过程中，用户可在客户端的输入界面输入用户唯一ID信息。加密通信模块，运行在客户端与服务器端，用于建立安全连接，可利用SSL(Secure Sockets Layer安全套接层)协议建立该安全连接，保障通信的机密性、完整性和认证性，确保交互的信息不被泄漏、篡改和冒充。注册模块，与用户信息获取模块连接，利用其获取的用户信息，具体地，在身份认证之前，用户在客户端中的输入界面输入用户信息进行注册，通过加密通信模块将用户唯一ID信息发送给服务器端，并保存服务器端发送的长期密钥。

[0067] 服务器端在注册方法中至少包括：加密通讯模块和注册模块，其中注册模块通过加密通讯模块接收到用户唯一ID信息后，利用其主密钥为该用户生成唯一长期密钥，并通过加密通讯模块将该长期密钥发送给客户端。

[0068] 客户端在验证方法中至少包括：时间戳模块，为每次交互通信提供时间戳用于确保通信消息新鲜性，从而防止重放攻击。进一步，在客户端发起身份认证请求时，用户填写其用户唯一ID参数，客户端利用时间戳模块生成时间戳参数，将上述两个参数发送给服务器端。二维码解码模块，当客户端接收到服务器端发送的二维码图片后，通过该模块可以将图片进行解码，解码后的数据为一次性口令加密数据。一次性口令验证模块，利用用户长期密钥对解码后的一次性口令加密数据进行解密操作，对解密后的一次性口令加上时间戳进行加密，结果值作为认证信息发送给服务器端。

[0069] 服务器端在验证方法中至少包括：时间戳模块，如前所述。随机数生成模块，在接收到客户端发起的身份认证请求信息后，包括用户唯一ID和时间戳，如请求信息有效则该模块生成一个随机数作为一次性口令数据。一次性口令加密数据生成模块，将随机数生成模块生成的一次性口令数据利用与用户唯一ID对应的长期私钥进行加密，生成一次性口令

加密数据。二维码编码模块，将一次性口令加密数据二进制处理后编码为二维码图片，可通过Code One、Maxi Code、QRCode、Data Matrix或者CODE49、CODE16K、PDF417等技术实现编码，将编码后的二维码图片发送到客户端。一次性口令验证模块，服务器端接收到客户端的认证信息后，利用该认证信息比对一次性口令数据是否符合，如果符合则通过身份认证。

[0070] 为进一步解释本发明在客户端与服务器端的认证交互过程，以及更具体的实施方式，以下通过流程图方式对本发明的注册方法和验证方法分别进行阐述，相关主要符号说明参见表1。表1为主要符号说明表。

[0071]

符号	说明
$Hash(\cdot)$	密码学哈希函数，例如 MD5，SHA1 等。
$Enc_{QR}(\cdot)$	二维码编码函数，生成二维码图片。
$Dec_{QR}(\cdot)$	二维码解码函数，将扫描设备获取的二维码图片转换成数据。
MK	服务器端的主密钥，用于为用户生成唯一长期私钥。
t_1，t_2，t_3	时间戳，用于确保消息新鲜性。

[0072] 如图2所示，本发明提供的注册方法，至少包含以下步骤：

[0073] S101客户端通过所述用户信息获取模块获取所述用户唯一ID信息，即id。

[0074] S102客户端与服务器端通过加密通信模块建立SSL安全通信连接，将用户唯一ID信息id发送给服务器端。

[0075] S103服务器端通过接收到的用户唯一ID参数id利用如下公式计算出该用户的用户长期私钥sk_{id}，并将所述用户长期私钥sk_{id}发送给客户端。

[0076] $sk_{id}=Hash(id,MK)$；

[0077] 上述公式中的哈希函数Hash可选择MD5、SHA-1或SHA-256等，因此长期私钥sk_{id}的长度，可为分别为128bit，160bit，256bit等。

[0078] S104客户端接收到服务器端为其颁发的所述用户长期私钥sk_{id}，将该私钥sk_{id}保存在个人本地设备中，例如保存在移动电话、平板电脑、个人计算机等，作为其长期私钥。

[0079] 如图3所示，本发明提供的验证方法，至少包含以下步骤：

[0080] S201客户端发起身份认证请求，发送所述用户唯一ID信息参数id及通过所述时间戳模块生成的时间戳参数t_1到服务器端。

[0081] S202服务器端接收到id及t_1后，验证时间戳t_1的有效性，如果与当前系统的差值超过一定时间，则判断时间戳无效，如果无效则拒绝认证请求，否则通过所述随机数生成模块获取随机数rand，该随机数rand作为一次性口令数据，其中要求随机数的大小应不大于与

所选择的哈希函数输出结果值的大小。

[0082] S203服务器端利用所述一次性口令数据rand以及所述用户唯一ID对应的所述用户长期私钥sk_{id}，通过如下公式计算一次性口令加密数据c_{psw}。

[0083] $$c_{psw} = rand \oplus sk_{id};$$

[0084] 上式中，$\oplus$为异或运算，在此实施例中，本发明所采用的加解密算法是计算效率较高的异或运算，因此在系统性能上可以减轻服务器的计算压力以满足大规模认证请求的需求。

[0085] S204服务器端将一次性口令加密数据c_{psw}通过(二维码编码模块)二维码编码算法$img_{QR}=Enc_{QR}(c_{psw})$生成二维码图片数据$img_{QR}$，并利用时间戳模块获取时间戳$t_2$，计算哈希值$h_1=Hash(rand,t_1,t_2)$以确保消息完整性，将二维码图片数据$img_{QR}$、$h_1$以及$t_2$发送到客户端。

[0086] S205客户端接收到维码图片数据img_{QR}、h_1以及t_2，判断时间戳t_2有效性，如果无效则拒绝该验证信息，否则利用用户长期私钥sk_{id}及如下公式计算一次性口令值(否则利用所述用户长期私钥以及所述二维码解码模块解密一次性口令加密数据，获得一次性口令数据)。

[0087] $$rand' = Dec_{QR}(img_{QR}) \oplus sk_{id};$$

[0088] 为区别服务器端一次性口令值rand，此处用rand′表示客户端计算出的一次性口令值。

[0089] 进一步，客户端判断h_1是否等于$Hash(rand',t_1,t_2)$，如果不相等则表示消息被篡改，则拒绝该验证信息，否则进行下一步。

[0090] S206客户端将所述的一次性口令数据rand′以及通过所述时间戳模块生成的时间戳参数t_3，计算哈希值$h_2=Hash(rand',t_2,t_3)$，将h_2和t_3发送给服务器端。

[0091] S207服务器端接收到h_2和t_3，判断时间戳t_3有效性，如果无效则拒绝认证请求，否则计算哈希值比对，即验证h_2是否等于$Hash(rand,t_2,t_3)$，如果不同则拒绝系统登录请求，否则表明客户端的一次性口令正确，身份验证通过。

[0092] 以上所述仅为本发明的实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

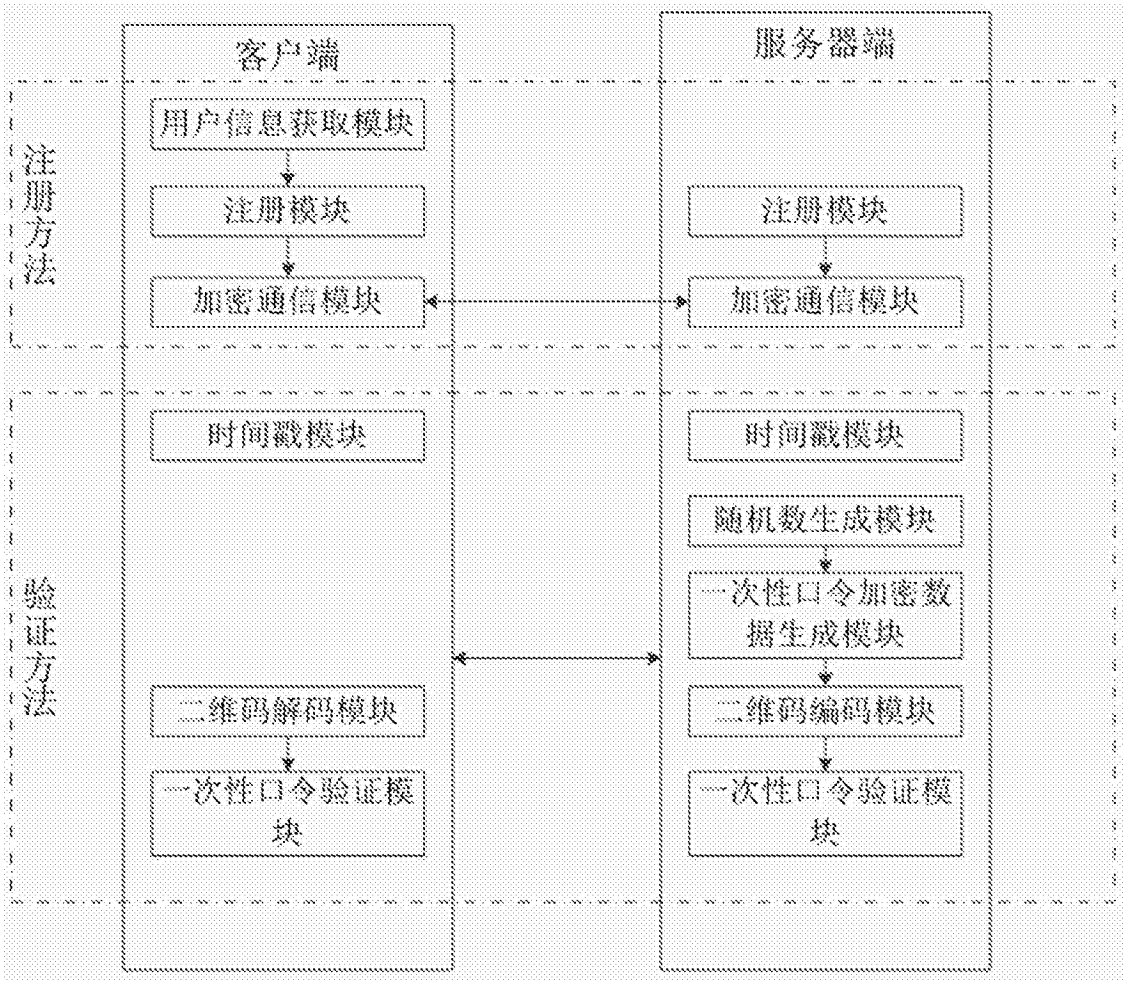

客户端
服务器端
注册方法
用户信息获取模块
注册模块
加密通信模块
注册模块
加密通信模块
验证方法
时间戳模块
时间戳模块
随机数生成模块
一次性口令加密数据生成模块
二维码解码模块
二维码编码模块
一次性口令验证模块
一次性口令验证模块

图1

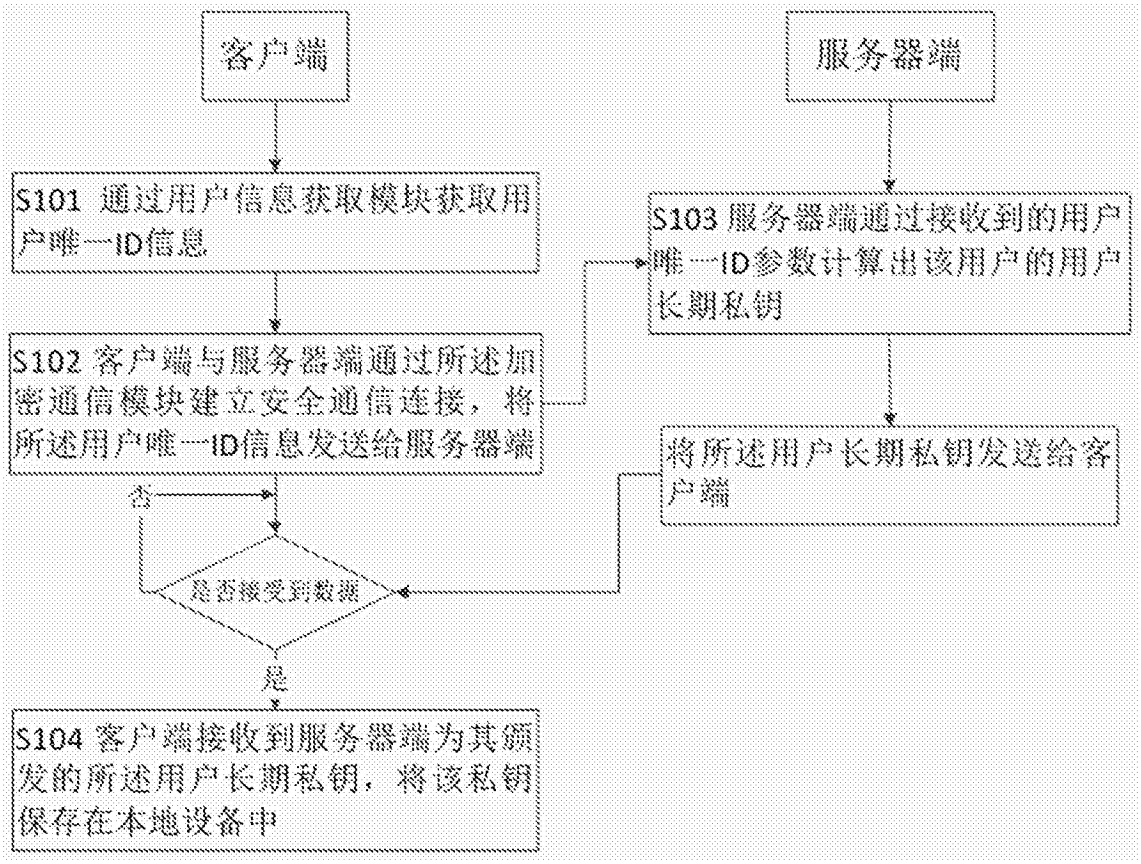

客户端
服务器端
S101 通过用户信息获取模块获取用户唯一ID信息
S102 客户端与服务器端通过所述加密通信模块建立安全通信连接，将所述用户唯一ID信息发送给服务器端
S103 服务器端通过接收到的用户唯一ID参数计算出该用户的用户长期私钥
将所述用户长期私钥发送给客户端
否
是否接受到数据
是
S104 客户端接收到服务器端为其颁发的所述用户长期私钥，将该私钥保存在本地设备中

图2

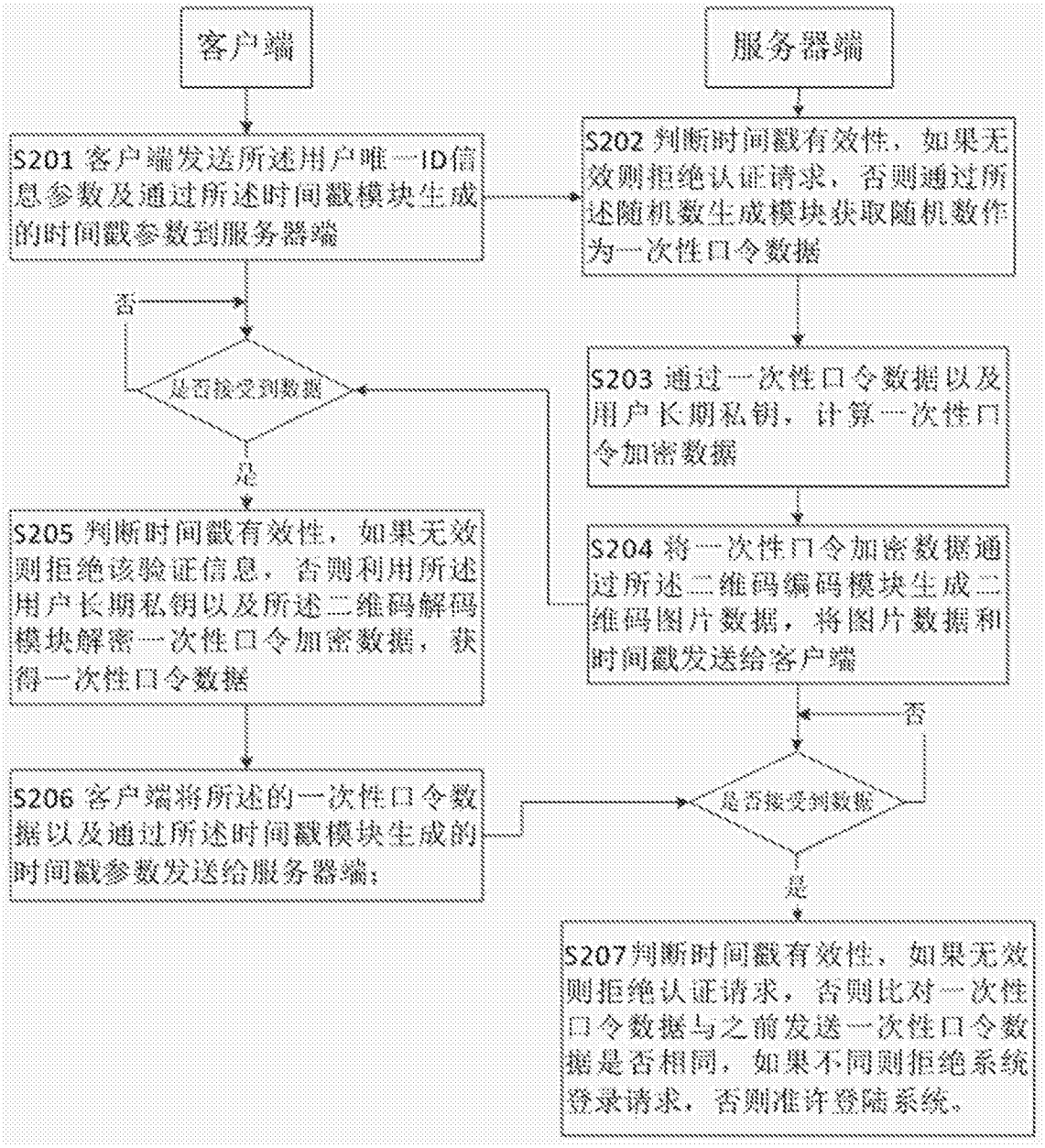

客户端
服务器端
S201 客户端发送所述用户唯一ID信息参数及通过所述时间戳模块生成的时间戳参数到服务器端
S202 判断时间戳有效性，如果无效则拒绝认证请求，否则通过所述随机数生成模块获取随机数作为一次性口令数据
否
是否接受到数据
是
S203 通过一次性口令数据以及用户长期私钥，计算一次性口令加密数据
S204 将一次性口令加密数据通过所述二维码编码模块生成二维码图片数据，将图片数据和时间戳发送给客户端
S205 判断时间戳有效性，如果无效则拒绝该验证信息，否则利用所述用户长期私钥以及所述二维码解码模块解密一次性口令加密数据，获得一次性口令数据
否
是否接受到数据
是
S206 客户端将所述的一次性口令数据以及通过所述时间戳模块生成的时间戳参数发送给服务器端；
S207判断时间戳有效性，如果无效则拒绝认证请求，否则比对一次性口令数据与之前发送一次性口令数据是否相同，如果不同则拒绝系统登录请求，否则准许登陆系统。

图3