(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 112738024 A
(43)申请公布日 2021.04.30

(21)申请号 202011428813.2

(22)申请日 2020.12.09

(71)申请人 杭州安恒信息技术股份有限公司
地址 310051 浙江省杭州市滨江区西兴街道联慧街188号

(72)发明人 吴新杰 范渊 刘博

(74)专利代理机构 杭州华进联浙知识产权代理有限公司 33250
代理人 龙伟

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

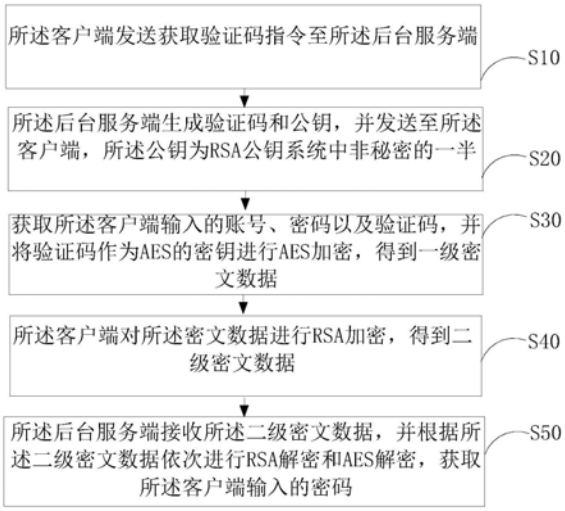
权利要求书2页 说明书8页 附图3页

(54)发明名称

加密认证方法、系统、存储介质及设备

(57)摘要

本申请涉及一种加密认证方法，应用于登录平台中，其中，该加密认证方法包括：接受客户端发送的获取验证码指令；根据接收到的获取验证码指令生成验证码和公钥，并发送至客户端，公钥为RSA公钥系统中非秘密的一半；获取客户端输入的账号、密码以及验证码，并将验证码作为AES的密钥进行AES加密，得到一级密文数据，发送至客户端；接收到客户端发送的二级密文数据后，对二级密文数据依次进行RSA解密和AES解密，以获取客户端输入的密码；二级密文数据为对一级密文数据进行RSA加密得到。通过本申请，对验证码和密码在数据传输过程中的安全性进行优化，有效的保证了数据的安全性。



CN 112738024 A

1.一种加密认证方法,其特征在于,应用于登录平台中,所述方法包括:

接受客户端发送的获取验证码指令;

根据接收到的所述获取验证码指令生成验证码和公钥,并发送至所述客户端;

获取所述客户端输入的账号、密码以及验证码,并将验证码作为AES的密钥进行AES加密,得到一级密文数据,发送至所述客户端;

接收到所述客户端发送的二级密文数据后,对所述二级密文数据依次进行RSA解密和AES解密,以获取所述客户端输入的密码;所述二级密文数据为对所述一级密文数据进行RSA加密得到。

2.根据权利要求1所述的加密认证方法,其特征在于,对所述二级密文数据依次进行RSA解密和AES解密步骤之前还包括:

比对所述客户端输入的验证码是否正确;

若否,则返回执行接受所述客户端发送的获取验证码指令步骤。

3.根据权利要求1所述的加密认证方法,其特征在于,所述获取所述客户端输入的密码的步骤之后还包括:

比对所述客户端输入的密码是否正确;

若否,则统计预设时间内输入密码错误的次数;

当输入密码错误的次数达到阈值时,周期时间内限制当前账户的登录。

4.根据权利要求1所述的加密认证方法,其特征在于,所述验证码为字符类验证码或智力测试验证码中的一种。

5.根据权利要求3所述的加密认证方法,其特征在于,所述统计预设时间内输入密码错误的次数的步骤之后还包括:

当输入密码错误的次数达到阈值时,向所述客户端对应绑定的接收端发送预警信息,所述预警信息包含登入端对应的IP地址、登入时间以及所述客户端的类别。

6.一种加密认证系统,应用于登录平台中,所述登录平台包括客户端和后台服务端,其特征在于,所述加密认证系统包括:

验证码指令模块:用于接受客户端发送的获取验证码指令;

反馈模块:用于接受客户端发送的获取验证码指令;根据接收到的所述获取验证码指令生成验证码和公钥,并发送至所述客户端;

一级加密模块:用于获取所述客户端输入的账号、密码以及验证码,并将验证码作为AES的密钥进行AES加密,得到一级密文数据,发送至所述客户端;

二级加密模块:用于对所述一级密文数据进行RSA加密,得到二级密文数据;

解密模块:用于接收到所述客户端发送的二级密文数据后,对所述二级密文数据依次进行RSA解密和AES解密,以获取所述客户端输入的密码。

7.根据权利要求6所述的加密认证系统,其特征在于,所述系统还包括:

所述验证码为字符类验证码或智力测试验证码中的一种。

8.根据权利要求6所述的加密认证系统,其特征在于,所述系统还包括:

比对模块:用于比对所述客户端输入的验证码是否正确;

若否,则返回执行接受所述客户端发送的获取验证码指令步骤;

校验统计模块:用于比对所述客户端输入的密码是否正确;

若否,则统计预设时间内输入密码错误的次数;

时钟模块:用于当输入密码错误的次数达到阈值时,周期时间内限制当前账户的登录

预警模块:当输入密码错误的次数达到阈值时,向所述客户端对应绑定的接收端发送预警信息,所述预警信息包含登入端对应的IP地址、登入时间以及所述客户端的类别。

9.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现如权利要求1－5任一所述的加密认证方法。

10.一种加密认证设备,其特征在于,包括存储器、处理器以及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时实现如权利要求1－5任一所述的加密认证方法。

加密认证方法、系统、存储介质及设备

技术领域

[0001] 本发明涉及信息安全技术领域，特别涉及一种加密认证方法、系统、存储介质及设备。

背景技术

[0002] 在当今的数据安全技术领域中的多数场景下，前端在登录时，会向后端传输用户名和密码用于身份鉴定，但是用户的密码是非常敏感的数据，一旦泄漏会造成无法估量的损失。

[0003] 所以，现在基本上的传输都不会是使用密码的明文传输，或多或少的做一些加密处理，现阶段通常采用的加密手段是使用对称加密，也就是说前端会存有一个加密使用的密钥。

[0004] 然而，这个密钥一般是固定(固定的生成方式)或者后端传输给前端的，所以非常容易被破获，从而使加密功能失效，造成密码泄漏。

发明内容

[0005] 基于此，本发明的目的是提供一种加密认证方法、系统、存储介质及设备，对验证码和密码在数据传输过程中的安全性进行优化，有效的保证了数据的安全性。

[0006] 本发明提供一种加密认证方法，应用于登录平台中，所述登录平台包括客户端和后台服务端，其中，所述方法包括：

[0007] 所述客户端发送获取验证码指令至所述后台服务端；

[0008] 所述后台服务端生成验证码和公钥，并发送至所述客户端，所述公钥为RSA公钥系统中非秘密的一半；

[0009] 获取所述客户端输入的账号、密码以及验证码，并将验证码作为AES的密钥进行AES加密，得到一级密文数据；

[0010] 所述客户端对所述密文数据进行RSA加密，得到二级密文数据；

[0011] 所述后台服务端接收所述二级密文数据，并根据所述二级密文数据依次进行RSA解密和AES解密，获取所述客户端输入的密码。

[0012] 本发明提供的加密认证方法，在使用客户端用户输入的验证码作为AES的密钥对密码进行AES加密，然后对AES加密后的密文进行RSA加密，传输到后台服务端，后台服务端先验证验证码是否正确，再进行RSA解密、AES解密。通过上述加密认证方法，通过使用动态随机生成的AES密钥，并用RSA加密AES加密后的密文，解决AES密钥泄露导致中间人劫持破解出密码的问题。

[0013] 进一步的，对所述二级密文数据依次进行RSA解密和AES解密步骤之前还包括：

[0014] 比对所述客户端输入的验证码是否正确；

[0015] 若否，则返回执行接受客户端发送的获取验证码指令步骤。

[0016] 进一步的，所述获取所述客户端输入的密码的步骤之后还包括：

[0017] 比对所述客户端输入的密码是否正确；

[0018] 若否，则统计预设时间内输入密码错误的次数；

[0019] 当输入密码错误的次数达到阈值时，周期时间内限制当前账户的登录。

[0020] 进一步的，所述验证码为字符类验证码或智力测试验证码中的一种。

[0021] 进一步的，所述统计预设时间内输入密码错误的次数的步骤之后还包括：

[0022] 当输入密码错误的次数达到阈值时，向所述客户端对应绑定的接收端发送预警信息，所述预警信息包含登入端对应的IP地址、登入时间以及所述客户端的类别。

[0023] 本发明提供一种加密认证系统，应用于登录平台中，所述加密认证系统包括：

[0024] 验证码指令模块：用于接受客户端发送的获取验证码指令；

[0025] 反馈模块：用于根据接收到的所述获取验证码指令生成验证码和公钥，并发送至所述客户端，所述公钥为RSA公钥系统中非秘密的一半；

[0026] 一级加密模块：用于获取所述客户端输入的账号、密码以及验证码，并将验证码作为AES的密钥进行AES加密，得到一级密文数据，发送至所述客户端；

[0027] 二级加密模块：用于对所述一级密文数据进行RSA加密，得到二级密文数据；

[0028] 解密模块：用于接收到所述客户端发送的二级密文数据后，对所述二级密文数据依次进行RSA解密和AES解密，以获取所述客户端输入的密码。

[0029] 进一步的，所述系统还包括：

[0030] 比对模块：用于比对所述客户端输入的验证码是否正确；

[0031] 若否，则返回执行接受客户端发送的获取验证码指令步骤。

[0032] 进一步的，所述系统还包括：

[0033] 校验统计模块：用于比对所述客户端输入的密码是否正确；

[0034] 若否，则统计预设时间内输入密码错误的次数；

[0035] 时钟模块：用于当输入密码错误的次数达到阈值时，周期时间内限制当前账户的登录。

[0036] 进一步的，所述验证码为字符类验证码或智力测试验证码中的一种。

[0037] 进一步的，所述系统还包括：

[0038] 预警模块：当输入密码错误的次数达到阈值时，向所述客户端对应绑定的接收端发送预警信息，所述预警信息包含登入端对应的IP地址、登入时间以及所述客户端的类别。

[0039] 本发明还提出一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现上述的加密认证方法。

[0040] 本发明还提出一种加密认证设备，包括存储器、处理器以及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述的加密认证方法。

[0041] 本发明的附加方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实施例了解到。

附图说明

[0042] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0043] 图1为本发明第一实施例提出的加密认证方法流程图；

[0044] 图2为本发明第一实施中对二级密文数据依次进行RSA解密和AES解密步骤之前的流程图；

[0045] 图3为本发明第一实施中获取客户端输入的密码步骤后的流程图；

[0046] 图4为本发明第一实施中统计预设时间内输入密码错误次数步骤后的流程图；

[0047] 图5为本发明第二实施例的加密认证系统结构示意图；

[0048] 图6为本发明第三实施例当中的加密认证设备。

具体实施方式

[0049] 为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行描述和说明。应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。基于本申请提供的实施例，本领域普通技术人员在没有作出创造性劳动的前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0050] 显而易见地，下面描述中的附图仅仅是本申请的一些示例或实施例，对于本领域的普通技术人员而言，在不付出创造性劳动的前提下，还可以根据这些附图将本申请应用于其他类似情景。此外，还可以理解的是，虽然这种开发过程中所作出的努力可能是复杂并且冗长的，然而对于与本申请公开的内容相关的本领域的普通技术人员而言，在本申请揭露的技术内容的基础上进行的一些设计，制造或者生产等变更只是常规的技术手段，不应当理解为本申请公开的内容不充分。

[0051] 在本申请中提及“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。本领域普通技术人员显式地和隐式地理解的是，本申请所描述的实施例在不冲突的情况下，可以与其它实施例相结合。

[0052] 除非另作定义，本申请所涉及的技术术语或者科学术语应当为本申请所属技术领域内具有一般技能的人士所理解的通常意义。本申请所涉及的“一”、“一个”、“一种”、“该”等类似词语并不表示数量限制，可表示单数或复数。本申请所涉及的术语“包括”、“包含”、“具有”以及它们任何变形，意图在于覆盖不排他的包含；例如包含了一系列步骤或模块(单元)的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可以还包括没有列出的步骤或单元，或可以还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。本申请所涉及的“连接”、“相连”、“耦接”等类似的词语并非限定于物理的或者机械的连接，而是可以包括电气的连接，不管是直接的还是间接的。本申请所涉及的“多个”是指两个或两个以上。“和/或”描述关联对象的关联关系，表示可以存在三种关系，例如，“A和/或B”可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。字符“/”一般表示前后关联对象是一种“或”的关系。本申请所涉及的术语“第一”、“第二”、“第三”等仅仅是区别类似的对象，不代表针对对象的特定排序。

[0053] 本实施例还提供了一种加密认证方法。应用于登录平台中，所述登录平台包括客户端和后台服务端，图1是根据本申请第一实施例提出的加密认证方法的流程图，如图1所示，该流程包括如下步骤：

[0054] 步骤S10，所述客户端发送获取验证码指令至所述后台服务端。

[0055] 在本发明实施例中，所述客户端在进行登录时，在登录页面需要输入账号信息、密码信息以及验证码信息，其验证码的获取途径可以是登录界面随机分配的一个字符类验证码或智力测试验证码，还可以是通过账号所对应绑定的接收端反馈的验证码，接收端可以是手机号码、微信、QQ、MSN等通讯应用工具以及APP等。

[0056] 步骤S20，所述后台服务端生成验证码和公钥，并发送至所述客户端，所述公钥为RSA公钥系统中非秘密的一半。

[0057] 其中，后台服务端接收到客户端的获取验证码指令后，生成验证码的同时还生成一RSA公钥，并将生成的验证码信息反馈至客户端。

[0058] 步骤S30，获取所述客户端输入的账号、密码以及验证码，并将验证码作为AES的密钥进行AES加密，得到一级密文数据。

[0059] 本发明实施例中，通过获取客户端输的的账号、密码以及验证码信息，且以验证码作为AES的密钥进行AES加密，由于验证码的生成逻辑每次都是随机的，因此通过动态验证码生成的AES密钥也是随机的，极大程度解决了固定密钥的泄露问题，使用动态AES密钥对用户输入的密码进行加密，生成一级密文数据。

[0060] 步骤S40，所述客户端对所述密文数据进行RSA加密，得到二级密文数据。

[0061] 本发明实施例中，在通过动态AES密钥对用户输入的密码进行加密，生成一级密文数据之后，对一级密文数据使用RSA加密算法进行二次加密。RSA公钥由后台服务端传输过来，使用RSA公钥对一级密文数据进行二次加密，由于RSA是属于非对称加密，需要使用指定的私钥进行解密，私钥并没有传输给客户端，因此使用RSA加密生成的二级密文数据再次增强了劫持破解难度。

[0062] 步骤S50，所述后台服务端接收所述二级密文数据，并根据所述二级密文数据依次进行RSA解密和AES解密，获取所述客户端输入的密码。

[0063] 通过上述步骤，解决了现有的加密手段只是对密码进行对称的加密，而密钥在前端也有存储，只要能拿到密钥，那么密文就会被快速的破解的技术问题。本申请通过动态非对称加密技术对动态验证码加密过的密文进行加密，所以每次对密码加密的密钥都是不同，而且不是以明文的方式进行传输，有效的保证了数据的安全性。

[0064] 请参阅图2，为本发明对所述二级密文数据依次进行RSA解密和AES解密步骤之前的流程图。其具体步骤包括：

[0065] 步骤S41，比对所述客户端输入的验证码是否正确。

[0066] 步骤S42，若是，则执行步骤S50。

[0067] 步骤S43，若否，则返回执行接受客户端发送的获取验证码指令步骤。

[0068] 本发明实施例中，关于验证码的识别类型为字符类验证码，具体的，验证码可以是图片验证码、短信验证码、简单的计算式验证码，还可以是图片类的验证码。通过设置不同类型的验证码，以提升了非人工操作过程中破译验证码的操作难度。

[0069] 本发明实施例通过比对客户端输入的验证码是否与后台服务端预设的验证码一致，来确保在数据传输过程中对账号和密码的安全性保护，且验证码的设置类型为上述多种验证码中的其中一种，极大的降低了计算机设备验证码被破译的可能性。提升了该加密认证方法的安全性。

[0070] 请参阅图3，为本发明获取客户端输入的密码步骤后的流程图。其具体步骤包括：

[0071] 步骤S51,比对所述客户端输入的密码是否正确。

[0072] 其中,后台服务端接收到的密码与当前账号预设的密码进行比对,以实现最后的校验步骤,完成登录。

[0073] 步骤S52,若否,则统计预设时间内输入密码错误的次数;

[0074] 本发明实施例中,上述关于验证码的比对登录验证过程是为了防止其他通过设备程序通过穷举法去获取对应账号的密码信息,验证码作为一种人机识别手段,其终极目的,就是区分正常人和机器的操作,验证码的作用在于区分人和机器,防止被暴力破解,提高破解密码的难度。当通过验证码的识别后,后台服务端校验比对密码信息,当密码比对不一致时,可以理解的可能存在以下几种情形:一、输入失误;二、非本人操作试探登录;三、密码记错导致输入错误。为了防止上述第二种异常登录情况发生的同时,满足由于第一种和第三种情况的输入错误的再次登录应允。本发明实施例设置异常登录次数限制。通过统计错误密码登录次数来实现。

[0075] 步骤S53,当输入密码错误的次数达到阈值时,周期时间内限制当前账户的登录。

[0076] 本发明实施例中,阈值的设置次数为3次,周期时间的设置时间为每日的凌晨6点。实际效果是:在异常登录过程中,超过3次存在错误密码尝试登录的情况下,限制该账号的登录,具体限制时间直到次日的凌晨6点。

[0077] 可以理解的,为了适应对应登录端对于信息安全和登录体验感,在本发明其他实施例中,阈值的设置次数还可以是其他更多或者更少的设置次数,周期时间的设置也可以随具体的环境条件设置。以达到信息安全性考量以及操作登录体验感提升的目的效果。

[0078] 请参阅图4,为本发明第一实施中统计预设时间内输入密码错误次数步骤后的流程图。具体步骤如下:

[0079] 步骤S54,当输入密码错误的次数达到阈值时,向所述客户端对应绑定的接收端发送预警信息。

[0080] 本发明实施例中,所述预警信息包含登入端对应的IP地址、登入时间以及所述客户端的类别。通过向预设的客户端发送登录端的预警信息,以便于使用人员确定当前的异常登录当不是本人操作时,有效的提供关于异常登录人员对应的登录信息,以便于去侦察获取异常登录人员的地理位置和非法操作证据。进一步的提升了关于异常登录的非法性打击效果,在另一种方式上提升了账号登录的安全性。

[0081] 需要说明的是,在上述流程中或者附图的流程图中示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行,并且,虽然在流程图中示出了逻辑顺序,但是在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤。

[0082] 本实施例还提供了一种加密认证系统,该系统用于实现上述实施例及优选实施方式,已经进行过说明的不再赘述。如以下所使用的,术语“模块”、“单元”、“子单元”等可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的系统较佳地以软件来实现,但是硬件,或者软件和硬件的组合的实现也是可能并被构想的。

[0083] 图5是根据本申请第二实施例的加密认证系统的结构框图,应用于登录平台中,所述登录平台包括客户端和后台服务端,如图5所示,该加密认证系统包括:

[0084] 验证码指令模块51:用于接受客户端发送的获取验证码指令。

[0085] 反馈模块52:用于根据接收到的所述获取验证码指令生成验证码和公钥,并发送

至所述客户端，所述公钥为RSA公钥系统中非秘密的一半。

[0086] 一级加密模块53：用于获取所述客户端输入的账号、密码以及验证码，并将验证码作为AES的密钥进行AES加密，得到一级密文数据，发送至所述客户端。

[0087] 二级加密模块54：用于对所述一级密文数据进行RSA加密，得到二级密文数据。

[0088] 解密模块55：用于接收到所述客户端发送的二级密文数据后，对所述二级密文数据依次进行RSA解密和AES解密，以获取所述客户端输入的密码。

[0089] 此外，该加密认证系统还包括：

[0090] 比对模块56：用于比对所述客户端输入的验证码是否正确；

[0091] 若否，则返回执行接受客户端发送的获取验证码指令步骤。

[0092] 校验统计模块57：用于比对所述客户端输入的密码是否正确；

[0093] 若否，则统计预设时间内输入密码错误的次数；

[0094] 时钟模块58：用于当输入密码错误的次数达到阈值时，周期时间内限制当前账户的登录。

[0095] 预警模块59：当输入密码错误的次数达到阈值时，向所述客户端对应绑定的接收端发送预警信息，所述预警信息包含登入端对应的IP地址、登入时间以及所述客户端的类别。

[0096] 综上，本发明上述实施例当中的加密认证系统，通过动态AES密钥对用户输入的密码进行加密，生成一级密文数据之后，对一级密文数据使用RSA加密算法进行二次加密。RSA公钥由后台服务端传输过来，使用RSA公钥对一级密文数据进行二次加密，由于RSA是属于非对称加密，需要使用指定的私钥进行解密，私钥并没有传输给客户端，因此使用RSA加密生成的二级密文数据再次增强了劫持破解难度，解决的现有的加密手段只是对密码进行对称的加密，而密钥在前端也有存储，只要能拿到密钥，那么密文就会被快速的破解的技术问题。此外，通过动态非对称加密技术对动态验证码加密过的密文进行加密，所以每次对密码加密的密钥都是不同，而且不是以明文的方式进行传输，有效的保证了数据的安全性。此外，通过设置不同类型的验证码，以提升了非人工操作过程中破译验证码的操作难度。此外，为了防止非本人操作试探登录的异常登录情况发生的，并满足由于输入失误和码记错导致输入错误的再次登录应允。本发明实施例设置异常登录次数限制。通过统计错误密码登录次数来实现。

[0097] 需要说明的是，上述各个模块可以是功能模块也可以是程序模块，既可以通过软件来实现，也可以通过硬件来实现。对于通过硬件来实现的模块而言，上述各个模块可以位于同一处理器中；或者上述各个模块还可以按照任意组合的形式分别位于不同的处理器中。

[0098] 本发明另一方面还提出一种加密认证设备，请参阅图6，所示为本发明实施例三当中的加密认证设备，包括存储器20、处理器10以及存储在存储器上并可在处理器上运行的计算机程序30，所述处理器10执行所述程序30时实现如上述的加密认证方法。

[0099] 其中，所述加密认证设备具体可以为带有数据库的计算机设备，例如服务器等，处理器10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、微处理器或其他加密认证芯片，用于运行存储器20中存储的程序代码或处理数据，例如执行访问限制程序等。

[0100] 其中，存储器20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DX存储器等)、磁性存储器、磁盘、光盘等。存储器20在一些实施例中可以是加密认证设备的内部存储单元，例如该加密认证设备的硬盘。存储器20在另一些实施例中也可以是加密认证设备的外部存储装置，例如加密认证设备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。进一步地，存储器20还可以既包括加密认证设备的内部存储单元也包括外部存储装置。存储器20不仅可以用于存储安装于加密认证设备的应用软件及各类数据，还可以用于暂时地存储已经输出或者将要输出的数据。

[0101] 需要指出的是，图6示出的结构并不构成对加密认证设备的限定，在其它实施例当中，该加密认证设备可以包括比图示更少或者更多的部件，或者组合某些部件，或者不同的部件布置。

[0102] 综上，本发明上述实施例当中的加密认证设备，通过动态AES密钥对用户输入的密码进行加密，生成一级密文数据之后，对一级密文数据使用RSA加密算法进行二次加密。RSA公钥由后台服务端传输过来，使用RSA公钥对一级密文数据进行二次加密，由于RSA是属于非对称加密，需要使用指定的私钥进行解密，私钥并没有传输给客户端，因此使用RSA加密生成的二级密文数据再次增强了劫持破解难度，解决的现有的加密手段只是对密码进行对称的加密，而密钥在前端也有存储，只要能拿到密钥，那么密文就会被快速的破解的技术问题。此外，通过动态非对称加密技术对动态验证码加密过的密文进行加密，所以每次对密码加密的密钥都是不同，而且不是以明文的方式进行传输，有效的保证了数据的安全性。通过设置不同类型的验证码，以提升了非人工操作过程中破译验证码的操作难度。为了防止非本人操作试探登录的异常登录情况发生的，并满足由于输入失误和码记错导致输入错误的再次登录应允。本发明实施例设置异常登录次数限制。通过统计错误密码登录次数来实现。

[0103] 本发明实施例还提出一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现如上述的加密认证方法。

[0104] 本领域技术人员可以理解，在流程图中表示或在此以其他方式描述的逻辑和/或步骤，例如，可以被认为是用于实现逻辑功能的可执行指令的定序列表，可以具体实现在任何计算机可读介质中，以供指令执行系统、装置或设备(如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统)使用，或结合这些指令执行系统、装置或设备而使用。就本说明书而言，“计算机可读介质”可以是任何可以包含、存储、通信、传播或传输程序以供指令执行系统、装置或设备或结合这些指令执行系统、装置或设备而使用的装置。

[0105] 计算机可读介质的更具体的示例(非穷尽性列表)包括以下：具有一个或多个布线的电连接部(电子装置)，便携式计算机盘盒(磁装置)，随机存取存储器(RAM)，只读存储器(ROM)，可擦除可编辑只读存储器(EPROM或闪速存储器)，光纤装置，以及便携式光盘只读存储器(CDROM)。另外，计算机可读介质甚至可以是可在其上打印所述程序的纸或其他合适的介质，因为可以例如通过对纸或其他介质进行光学扫描，接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得所述程序，然后将其存储在计算机存储器中。

[0106] 应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件

或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或它们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列(PGA)，现场可编程门阵列(FPGA)等。

[0107] 以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

[0108] 以上所述实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。

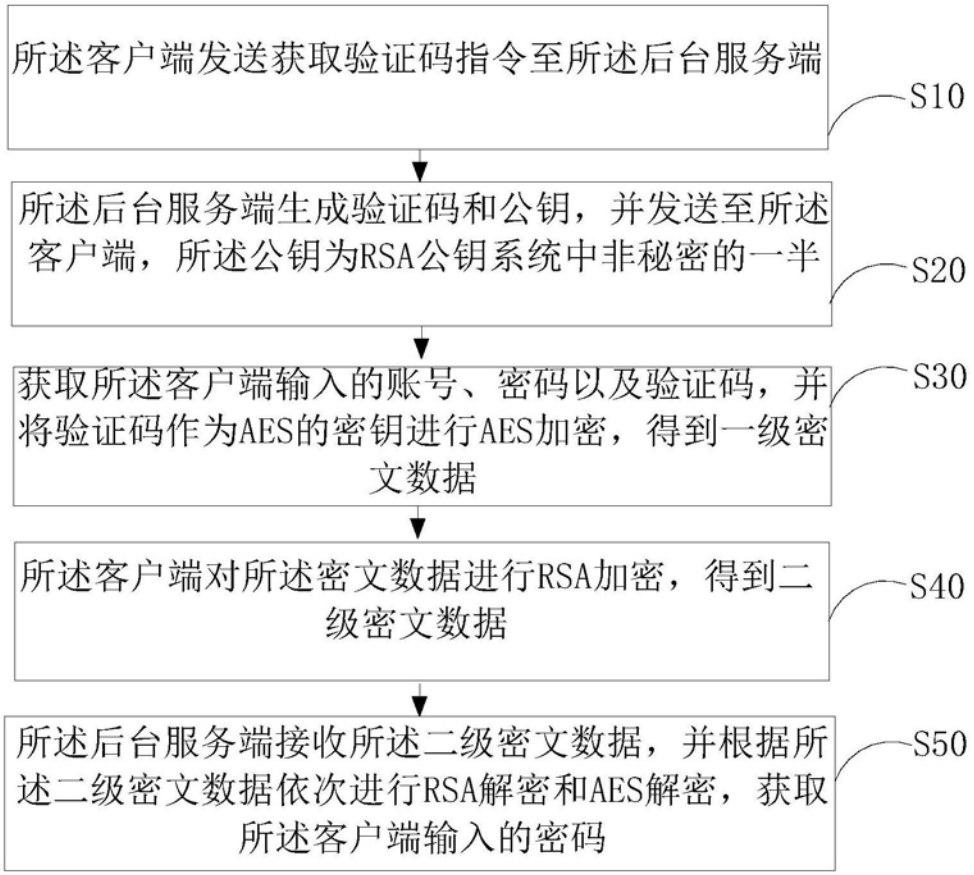

所述客户端发送获取验证码指令至所述后台服务端
S10
所述后台服务端生成验证码和公钥，并发送至所述客户端，所述公钥为RSA公钥系统中非秘密的一半
S20
获取所述客户端输入的账号、密码以及验证码，并将验证码作为AES的密钥进行AES加密，得到一级密文数据
S30
所述客户端对所述密文数据进行RSA加密，得到二级密文数据
S40
所述后台服务端接收所述二级密文数据，并根据所述二级密文数据依次进行RSA解密和AES解密，获取所述客户端输入的密码
S50

图1

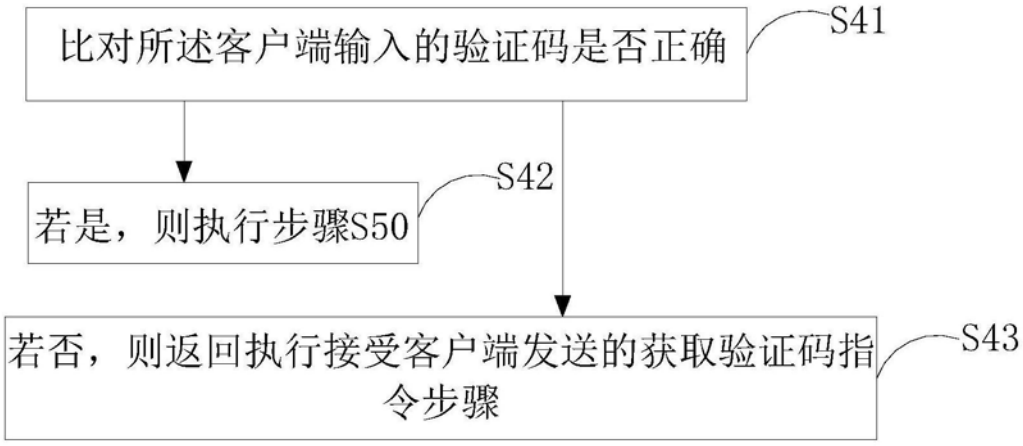

比对所述客户端输入的验证码是否正确
S41
若是，则执行步骤S50
S42
若否，则返回执行接受客户端发送的获取验证码指令步骤
S43

图2

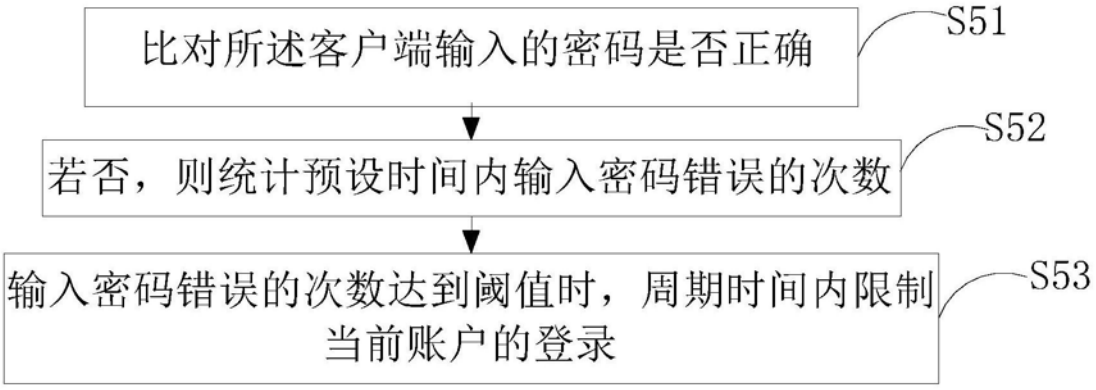

比对所述客户端输入的密码是否正确
S51
若否，则统计预设时间内输入密码错误的次数
S52
输入密码错误的次数达到阈值时，周期时间内限制当前账户的登录
S53

图3

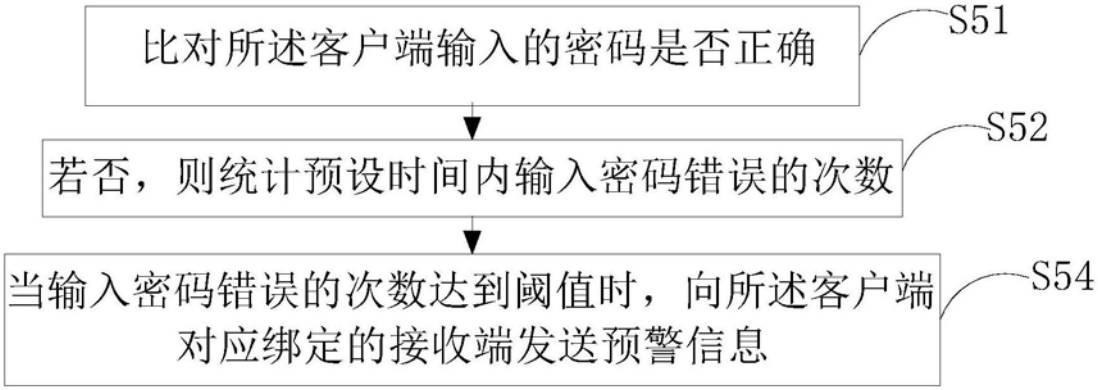

比对所述客户端输入的密码是否正确
S51
若否，则统计预设时间内输入密码错误的次数
S52
当输入密码错误的次数达到阈值时，向所述客户端对应绑定的接收端发送预警信息
S54

图4

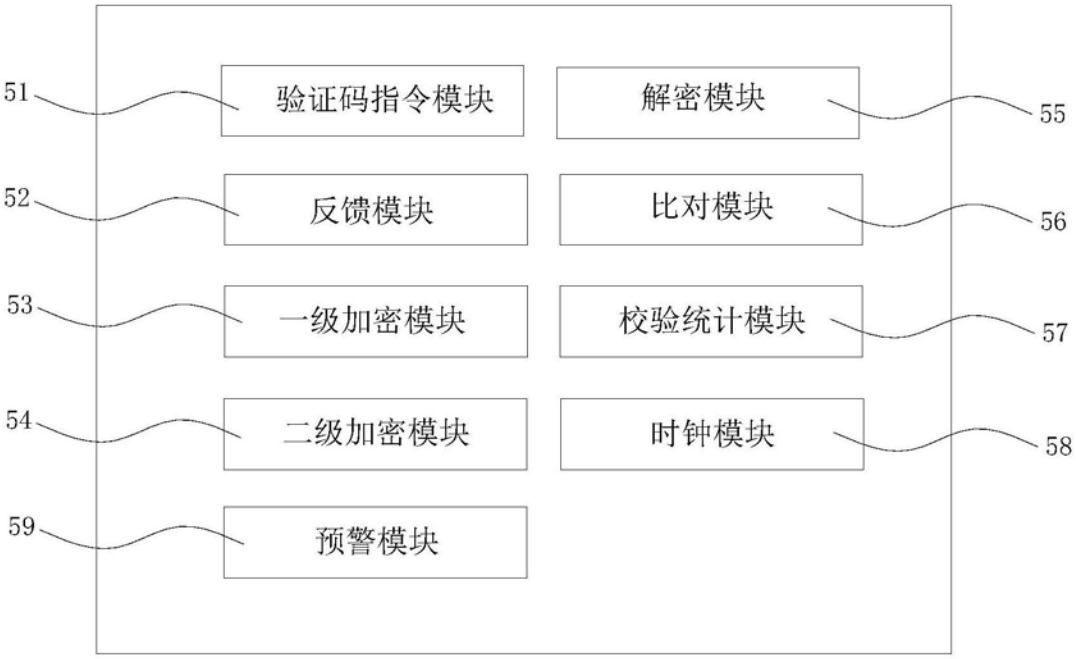

51
验证码指令模块
52
反馈模块
53
一级加密模块
54
二级加密模块
59
预警模块
解密模块
55
比对模块
56
校验统计模块
57
时钟模块
58

图5

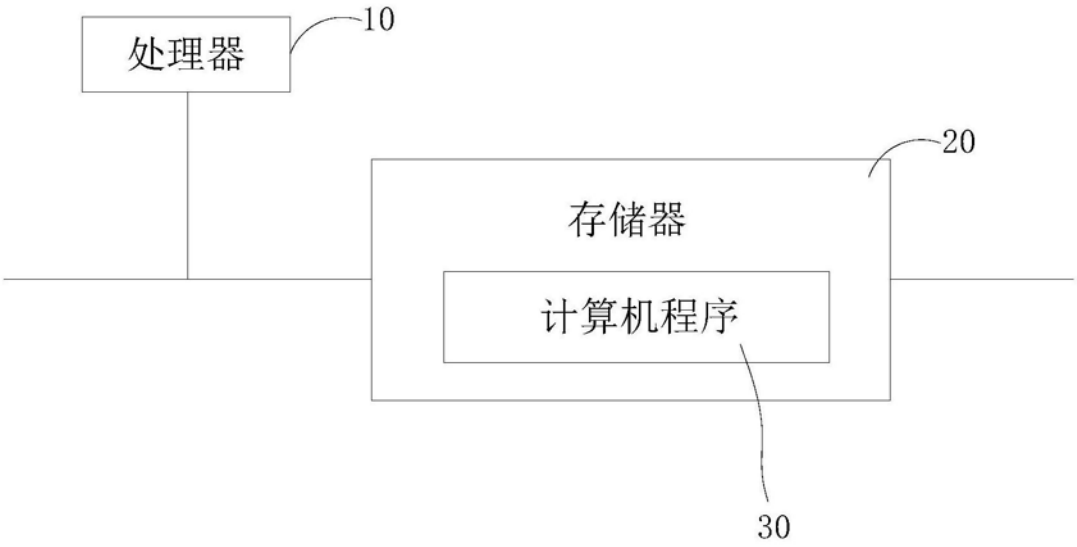

处理器
10
20
存储器
计算机程序
30

图6