(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113726774 B
(45)授权公告日 2023.05.02

(21)申请号 202111004304.1

(22)申请日 2021.08.30

(65)同一申请的已公布的文献号
申请公布号 CN 113726774 A

(43)申请公布日 2021.11.30

(66)本国优先权数据
202011092415.8 2020.10.13 CN

(73)专利权人 杭州涂鸦信息技术有限公司
地址 310013 浙江省杭州市西湖区浙商财富中心3幢701室

(72)发明人 钱海锋

(51)Int.Cl.
H04L 9/40(2022.01)

(56)对比文件
CN 113079134 A,2021.07.06
CN 113055371 A,2021.06.29

审查员 王莉

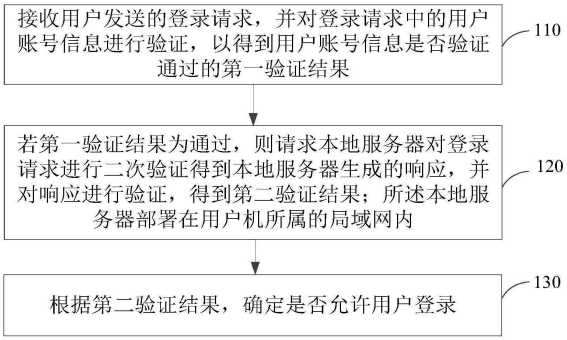
权利要求书2页 说明书8页 附图2页

(54)发明名称

客户端登录认证方法、系统和计算机设备

(57)摘要

本申请涉及一种客户端登录认证方法、系统和计算机设备，包括接收用户发送的登录请求，并对登录请求中的用户账号信息进行验证，以得到用户账号信息是否验证通过的第一验证结果；若第一验证结果为通过，则请求本地服务器对登录请求进行二次验证得到本地服务器生成的响应，并对响应进行验证，得到第二验证结果；本地服务器部署在用户机所属的局域网内；根据第二验证结果，确定是否允许用户登录。上述登录认证方法由于避免了将用户账号与登录设备或其他硬件设备绑定，也不需要将账号与IP地址绑定，只需要部署只在限制范围内能够访问的本地服务即可，从而不存在上述方案的限制，实施技术难度较小，且对操作人员和工厂无其他额外要求。



CN 113726774 B

1.一种客户端登录认证方法,其特征在于,所述方法包括:

接收用户发送的登录请求,并对所述登录请求中的用户账号信息进行验证,以得到所述用户账号信息是否验证通过的第一验证结果;

若所述第一验证结果为通过,则请求本地服务器对所述登录请求进行处理得到所述本地服务器生成的响应,并对所述响应进行验证,得到第二验证结果;所述本地服务器部署在用户机所属的局域网内;

根据所述第二验证结果,确定是否允许所述用户登录;

其中,所述若所述第一验证结果为通过,则请求本地服务器对所述登录请求进行处理得到所述本地服务器生成的响应,并对所述响应进行验证,得到第二验证结果包括:

若所述第一验证结果为通过,则与所述客户端对应的服务端生成挑战,并将所述挑战发送至所述客户端;

所述客户端在接收到所述挑战后,将所述挑战发送至所述本地服务器;

所述本地服务器根据第一预置密钥和预设加密算法对所述挑战进行加密处理,生成所述挑战对应的响应并发送至所述客户端;所述第一预置密钥与所述本地服务器所属的局域网对应;

所述服务端根据第二预置密钥和与所述预设加密算法对应的解密算法对所述响应进行二次验证,得到所述第二验证结果;所述第二预置密钥与所述客户端所属的局域网对应。

2.根据权利要求1所述的方法,其特征在于,所述客户端接收到所述挑战后,将所述挑战发送至所述本地服务器包括:

所述客户端通过Ajax或websocket方式请求所述本地服务器,将所述挑战发送给所述本地服务器;或,

通过所述客户端内安装的可以访问http服务的插件,将所述挑战发送至所述本地服务器。

3.根据权利要求1所述的方法,其特征在于,所述服务端根据第二预置密钥和与所述预设加密算法对应的解密算法对所述响应进行二次验证,得到所述第二验证结果包括:

所述服务端根据所述第二预置密钥和所述解密算法对所述响应进行解码;

若得到的解码结果与所述挑战一致,则所述第二验证结果为通过;

若得到的解码结果与所述挑战不一致或无法完成解码,则所述第二验证结果为未通过。

4.根据权利要求1所述的方法,其特征在于,所述挑战包括至少16个字节的随机数。

5.根据权利要求1所述的方法,其特征在于,所述本地服务器部署在PC机、树莓派或单片机上。

6.根据权利要求1所述的方法,其特征在于,所述方法还包括:

若所述第二验证结果为未通过,则向预留设备发出警告信息。

7.一种客户端登录认证系统,其特征在于,所述系统包括:

客户端,用于接收用户发送的登录请求;

服务端,与所述客户端对应,用于对所述登录请求中的用户账号信息进行验证,以得到所述用户账号信息是否验证通过的第一验证结果;

本地服务器,部署在用户机所属的局域网内,用于在所述第一验证结果为通过时,对所

述登录请求进行二次验证生成响应；

所述服务端还用于对所述响应进行验证，得到第二验证结果；

所述客户端还用于接收所述第二验证结果，并根据所述第二验证结果，确定是否允许所述用户登录；

其中，所述服务端还用于：若所述第一验证结果为通过，则与所述客户端对应的服务端生成挑战，并将所述挑战发送至所述客户端；

所述客户端在接收到所述挑战后，将所述挑战发送至所述本地服务器；

所述本地服务器根据第一预置密钥和预设加密算法对所述挑战进行加密处理，生成所述挑战对应的响应并发送至所述客户端；所述第一预置密钥与所述本地服务器所属的局域网对应；

所述服务端根据第二预置密钥和与所述预设加密算法对应的解密算法对所述响应进行二次验证，得到所述第二验证结果；所述第二预置密钥与所述客户端所属的局域网对应。

8.一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求1至6中任一项所述方法的步骤。

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，所述计算机程序被处理器执行时实现权利要求1至6中任一项所述的方法的步骤。

客户端登录认证方法、系统和计算机设备

技术领域

[0001] 本申请涉及数据安全技术领域，特别是涉及一种客户端登录认证方法、系统和计算机设备。

背景技术

[0002] 随着信息技术的发展，基本每一项新应用都会对应一个网页版系统，系统会要求用户进行相应的登录操作才能够使用，以确保数据的安全性。而对于有些应用系统，为了对账户进行特殊保护，需要限制系统仅可以在限制区域内登录。例如涂鸦的工厂生产需要使用PMS系统，为了方便账号登录，通常在工厂内使用账号可以是无限制的，不一定需要与人绑定。但是如果工厂的员工跳槽到别的工厂，就有可能把账号带走，从而存在安全隐患。所以，限制账号在一定区域内登录就很必要。

[0003] 传统地，限制账号在一定区域内登录的方式有：账号与登录设备绑定、账号与硬件绑定以及账号与IP地址绑定等。但是上述每种方式都有适用的场景，比如账号与登录设备绑定，由于浏览器安全限制的原因，Js无法获取到设备的硬件信息，所以要做到登录账号与设备绑定的难度相当大。其次，对于账号与硬件绑定方式，一般要求Js能与硬件直接或间接通信，现在有FIDO系列标准可以用，但是存在一个问题，需要操作人员与硬件有交互才能把流程走下去，而且每台电脑都需要接一个USB的设备，成本比较高。而对于IP地址绑定方式，限制更大，需要工厂有固定IP地址。

发明内容

[0004] 本申请提供一种基于客户端登录认证方法、系统和计算机设备，以至少解决相关技术中的限制账号登录区域方式存在较多限制以及实施难度较大的问题。

[0005] 第一方面，本申请实施例提供了一种客户端登录认证方法，所述方法包括：

[0006] 接收用户发送的登录请求，并对所述登录请求中的用户账号信息进行验证，以得到所述用户账号信息是否验证通过的第一验证结果；

[0007] 若所述第一验证结果为通过，则请求本地服务器对所述登录请求进行二次验证得到所述本地服务器生成的响应，并对所述响应进行验证，得到第二验证结果；所述本地服务器部署在用户机所属的局域网内；

[0008] 根据所述第二验证结果，确定是否允许所述用户登录。

[0009] 在其中一些实施例中，所述若所述第一验证结果为通过，则请求本地服务器对所述登录请求进行二次验证得到所述本地服务器生成的响应，并对所述响应进行验证，得到第二验证结果包括：

[0010] 若所述第一验证结果为通过，则与所述客户端对应的服务端生成挑战，并将所述挑战发送至所述客户端；

[0011] 所述客户端在接收到所述挑战后，将所述挑战发送至所述本地服务器，以请求所述本地服务器对所述登录请求进行二次验证；

[0012] 所述本地服务器根据第一预置密钥和预设加密算法对所述挑战进行加密处理，生成所述挑战对应的响应并发送至所述客户端；所述第一预置密钥与所述本地服务器所属的局域网对应；

[0013] 所述服务端根据第二预置密钥和与所述预设加密算法对应的解密算法对所述响应进行二次验证，得到所述第二验证结果；所述第二预置密钥与所述客户端所属的局域网对应。

[0014] 在其中一些实施例中，所述客户端接收到所述挑战后，将所述挑战发送至所述本地服务器包括：

[0015] 所述客户端通过Ajax或websocket方式请求本地服务器，将所述挑战发送给所述本地服务器；或，

[0016] 通过所述客户端内安装的可以访问http服务的插件，将所述挑战发送至所述本地服务器。

[0017] 在其中一些实施例中，所述服务端根据第二预置密钥和与所述预设加密算法对应的解密算法对所述响应进行二次验证，得到所述第二验证结果包括：

[0018] 所述服务端根据所述第二预置密钥和所述解密算法对所述响应进行解码；

[0019] 若得到的解码结果与所述挑战一致，则所述第二验证结果为通过；

[0020] 若得到的解码结果与所述挑战不一致或无法完成解码，则所述第二验证结果为未通过。

[0021] 在其中一些实施例中，所述挑战包括至少16个字节的随机数。

[0022] 在其中一些实施例中，所述本地服务器部署在PC机、树莓派或单片机上。

[0023] 在其中一些实施例中，所述方法还包括：若所述第二验证结果为未通过，则向预留设备发出警告信息。

[0024] 第二方面，本申请实施例提供了一种客户端登录认证系统，所述系统包括：

[0025] 客户端，用于接收用户发送的登录请求；

[0026] 服务端，与所述客户端对应，用于对所述登录请求中的用户账号信息进行验证，以得到所述用户账号信息是否验证通过的第一验证结果；

[0027] 本地服务器，部署在用户机所属的局域网内，用于在所述第一验证结果为通过时，对所述登录请求进行二次验证生成响应；

[0028] 所述服务端还用于对所述响应进行验证，得到第二验证结果；

[0029] 所述客户端还用于接收所述第二验证结果，并根据所述第二验证结果，确定是否允许所述用户登录。

[0030] 第三方面，本申请实施例提供了一种计算机设备，包括存储器、处理器以及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现如上述第一方面所述的客户端登录认证方法。

[0031] 第四方面，本申请实施例提供了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第一方面所述的客户端登录认证方法。

[0032] 相比于相关技术，本申请实施例提供的客户端登录认证方法包括：接收用户发送的登录请求，并对所述登录请求中的用户账号信息进行验证，以得到所述用户账号信息是否验证通过的第一验证结果；若所述第一验证结果为通过，则请求本地服务器对所述登录

请求进行二次验证得到所述本地服务器生成的响应，并对所述响应进行验证，得到第二验证结果；所述本地服务器部署在用户机所属的局域网内；根据所述第二验证结果，确定是否允许所述用户登录，解决了相关技术中的限制账号登录区域方式存在较多限制以及实施难度较大的问题。

[0033] 本申请的一个或多个实施例的细节在以下附图和描述中提出，以使本申请的其他特征、目的和优点更加简明易懂。

附图说明

[0034] 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：

[0035] 图1为一个实施例中提供的客户端登录认证方法的流程图；

[0036] 图2为一个实施例中提供的客户端登录认证系统的结构框图；

[0037] 图3为一个实施例中计算机设备的内部结构图。

具体实施方式

[0038] 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做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。

[0039] 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做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。

[0040] 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。

[0041] 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“多个”是指两个或两个以上。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。

[0042] 本申请所描述的各种技术可应用于登录客户端时使用，客户端包括了如万维网使

用的网页浏览器,收寄电子邮件时的电子邮件客户端,以及即时通讯的客户端软件等,本申请均以客户端为网页浏览器为例进行说明。

[0043] 图1为一个实施例提供的客户端登录认证方法的流程图,如图1所示,客户端登录认证方法包括步骤110至步骤130;其中:

[0044] 步骤110,接收用户发送的登录请求,并对登录请求中的用户账号信息进行验证,以得到用户账号信息是否验证通过的第一验证结果。

[0045] 用户账号信息可以包括用户注册使用的用户名和密码。客户端接收到用户的登录请求,与客户端对应的服务器对登录请求中的用户账号密码进行验证。具体地,用户账号信息可由服务器管理员统一进行配置,并将所分配的用户账户与其所对应的权限进行绑定。当用户登录客户端时,需要输入先前已经进行注册成功的用户账号以及对应的密码,服务器通过验证该账号以及密码来确认用户的合法性,只有已在客户端中进行合法注册的用户才可进行后续操作。

[0046] 步骤120,若第一验证结果为通过,则请求本地服务器对登录请求进行二次验证得到本地服务器生成的响应,并对响应进行验证,得到第二验证结果;本地服务器部署在用户所属的局域网内。

[0047] 若用户的账号密码输入正确,则对该用户的登录请求进行二次验证,已验证该用户是否是在允许登录区域内的登录操作。本实施例通过在用户机所属的局域网内部署本地服务器,用户只有在该局域网内登录才能访问该本地服务器。例如,有两个工厂,分别为A工厂和B工厂。在A工厂所属的局域网中部署第一本地服务器,在B工厂所属的局域网中部署第二本地服务器。当用户在A工厂里面登录时,只能访问到A工厂里面部署的第一本地服务,通过本地服务来判断账号的登录区域。

[0048] 可以理解的是,对于任何一个工厂,如果需要保证只有在工厂内部可以登录系统,那么只需要在自己工厂内部署一个本地服务,保证只有工厂内部能够访问这个本地服务即可以有效限制工厂外部人员登录系统。

[0049] 本地服务一般部署在独立的机器上,可以是普通的PC机,也可以是树莓派等小型SOC单板电脑,甚至可以是单片机。

[0050] 步骤130,根据第二验证结果,确定是否允许用户登录。

[0051] 由于服务端本身就预先设置了账号可以登录的区域,因此,比对本地服务器和服务端的数据,数据一致用户才可以成功登录。

[0052] 与现有技术相比,本申请提供的客户端登录认证方法包括接收用户发送的登录请求,并对登录请求中的用户账号信息进行验证,以得到用户账号信息是否验证通过的第一验证结果。若第一验证结果为通过,则请求本地服务器对登录请求进行二次验证得到本地服务器生成的响应,并对响应进行验证,得到第二验证结果;本地服务器部署在用户端所属的局域网内。根据第二验证结果,确定是否允许用户登录。上述登录认证方法在用户所属的局域网内部署只能在限制范围内访问的本地服务,在用户账户信息验证通过后,通过本地服务对用户的登录请求进行二次验证,以验证该用户是否在客户端所属的局域网内登录,二次验证通过,则允许用户登录,否则拒绝用户登录,从而可以有效限制客户端只能在一定区域内登录。由于该方法不需要将用户账号与登录设备或其他硬件设备绑定,也不需要将账号与IP地址绑定,只需要部署只在限制范围内能够访问的本地服务即可,从而不存在上

述方案的限制,实施技术难度较小,且对操作人员和工厂无其他额外要求。

[0053] 在其中一些实施例中,若第一验证结果为通过,则请求本地服务器对登录请求进行二次验证得到本地服务器生成的响应,并对响应进行验证,得到第二验证结果包括:

[0054] 若第一验证结果为通过,则与客户端对应的服务端生成挑战,并将挑战发送至客户端;

[0055] 客户端在接收到挑战后,将挑战发送至本地服务器,以请求本地服务器对登录请求进行二次验证;

[0056] 本地服务器根据第一预置密钥和预设加密算法对挑战进行加密处理,生成挑战对应的响应并发送至客户端;第一预置密钥与本地服务器所属的局域网对应;

[0057] 服务端根据第二预置密钥和与预设加密算法对应的解密算法对响应进行二次验证,得到第二验证结果;第二预置密钥与客户端所属的局域网对应。

[0058] 在其中一些实施例中,挑战包括至少16个字节的随机数。将随机数作为待机密的数据,也就是明文P。本地服务器根据第一预置密钥和预设加密算法对随机数进行加密得到第一密文,将第一密文作为响应发送至客户端。预设加密算法可以是对称加密算法,也可以是非对称加密算法,本实施例不对加密算法的类型作具体限定。

[0059] 由于本地服务器中存储的第一预置密钥与该本地服务器所属的局域网一一对应,第二预置密钥与客户端所属的局域网一一对应,因此,只有用户在客户端所属的局域网中登录时,其能访问的本地服务器属于客户端所属的局域网中,因此,第一预置密钥和第二预置密钥才能匹配,服务端才可以根据第二预置密钥和与预设加密算法对应的解密算法对第一密文进行解码得到服务端生成的挑战,从而通过第二验证,允许该用户登录。

[0060] 在其中一些实施例中,服务端根据第二预置密钥和与预设加密算法对应的解密算法对响应进行二次验证,得到第二验证结果包括:

[0061] 服务端根据第二预置密钥和解密算法对响应进行解码;

[0062] 若得到的解码结果与挑战一致,则第二验证结果为通过;

[0063] 若得到的解码结果与挑战不一致或无法完成解码,则第二验证结果为未通过。

[0064] 在其中一些实施例中,客户端接收到挑战后,将挑战发送至本地服务器包括:

[0065] 客户端通过Ajax或websocket方式请求本地服务器,将挑战发送给本地服务器;或,

[0066] 通过客户端内安装的可以访问http服务的插件,将挑战发送至本地服务器。

[0067] 通常,浏览器可以通过Ajax或websocket方式请求本地服务器。但是有的浏览器,例如Chrome可能会为了提升数据访问安全进行更新,更新后若禁止混合模式的访问。通常线上服务是https服务,而本地服务大多是http服务,这样就构成了一个混合模式页面,就有可能会被禁止访问本地的http服务。本实施例通过在客户端内安装可以访问http服务的插件,通过浏览器插件来代理这个局域网访问。

[0068] 在其中一些实施例中,方法还包括:若第二验证结果为未通过,则向预留设备发出警告信息。

[0069] 该警告信息可以为手机短信,或是发送到预设报警终端的报警信息。

[0070] 应该理解的是,虽然图1的流程图中的各个步骤按照箭头的指示依次显示,但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明,这些步骤的

执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，图1中的至少一部分步骤可以包括多个子步骤或者多个阶段，这些子步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些子步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

[0071] 本实施例还提供了一种客户端登录认证系统，该系统用于实现上述实施例及优选实施方式，上述已经对此进行过说明的在此不再赘述。

[0072] 在一个实施例中，如图2所示，提供了一种客户端登录认证系统，系统包括：

[0073] 客户端，用于接收用户发送的登录请求；

[0074] 服务端，与客户端对应，用于对登录请求中的用户账号信息进行验证，以得到用户账号信息是否验证通过的第一验证结果；

[0075] 本地服务器，部署在用户所属的局域网内，用于在第一验证结果为通过时，对登录请求进行二次验证生成响应；

[0076] 服务端还用于对响应进行验证，得到第二验证结果；

[0077] 客户端还用于接收第二验证结果，并根据第二验证结果，确定是否允许用户登录。

[0078] 具体登录认证流程如下：

[0079] 1.用户使用用户名与密码登录系统；

[0080] 2.用户名与密码验证成功后，服务端生成一个挑战；

[0081] 3.服务端返回挑战以要求客户端进行额外的认证，即二次认证；

[0082] 4.客户端通过Ajax、websocket方式或通过插件请求本地服务，把挑战发送给本地服务器；

[0083] 5.本地服务器通过密码学算法，把挑战与内置密钥计算后生成响应；

[0084] 6.本地服务器把响应返回给客户端；

[0085] 7.客户端把响应提交给服务端进行验证；

[0086] 8.服务端使用与本地服务器中匹配的算法和内置密钥验证响应是否正确；

[0087] 9.把验证结果返回给客户端，如果验证正确，则登录成功，否则登录失败。

[0088] 上述系统通过在用户所属的局域网内部署只能在限制范围内访问的本地服务，在用户账户信息验证通过后，通过本地服务对用户的登录请求进行二次验证，以验证该用户是否在客户端所属的局域网内登录，二次验证通过，则允许用户登录，否则拒绝用户登录，从而可以有效限制客户端只能在一定区域内登录。由于该方法不需要将用户账号与登录设备或其他硬件设备绑定，也不需要将账号与IP地址绑定，只需要部署只在限制范围内能够访问的本地服务即可，从而不存在上述方案的限制，实施技术难度较小，且对操作人员和工厂无其他额外要求。

[0089] 在其中一些实施例中，若所述第一验证结果为通过，则与所述客户端对应的服务端生成挑战，并将所述挑战发送至所述客户端；所述客户端在接收到所述挑战后，将所述挑战发送至所述本地服务器，以请求所述本地服务器对所述登录请求进行二次验证；所述本地服务器根据第一预置密钥和预设加密算法对所述挑战进行加密处理，生成所述挑战对应的响应并发送至所述客户端；所述第一预置密钥与所述本地服务器所属的局域网对应；所述服务端根据第二预置密钥和与所述预设加密算法对应的解密算法对所述响应进行二次验证，得到所述第二验证结果；所述第二预置密钥与所述客户端所属的局域网对应。

[0090] 在其中一些实施例中,所述客户端通过Ajax或websocket方式请求本地服务器,将所述挑战发送给所述本地服务器;或,通过所述客户端内安装的可以访问http服务的插件,将所述挑战发送至所述本地服务器。

[0091] 在其中一些实施例中,所述服务端还用于根据所述第二预置密钥和所述解密算法对所述响应进行解码;若得到的解码结果与所述挑战一致,则所述第二验证结果为通过;若得到的解码结果与所述挑战不一致或无法完成解码,则所述第二验证结果为未通过。

[0092] 在其中一些实施例中,所述挑战包括至少16个字节的随机数。

[0093] 在其中一些实施例中,所述本地服务器部署在PC机、树莓派或单片机上。

[0094] 在其中一些实施例中,上述系统还包括报警模块,用于若所述第二验证结果为未通过,则向预留设备发出警告信息。

[0095] 关于客户端登录认证系统的具体限定可以参见上文中对于客户端登录认证方法的限定,在此不再赘述。

[0096] 另外,结合图1描述的本申请实施例提供的客户端登录认证方法可以由计算机设备来实现。图3为根据本申请实施例的计算机设备的硬件结构示意图。

[0097] 计算机设备可以包括处理器31以及存储有计算机程序指令的存储器32。

[0098] 具体地,上述处理器31可以包括中央处理器(CPU),或者特定集成电路(Application Specific Integrated Circuit,简称为ASIC),或者可以被配置成实施本申请实施例的一个或多个集成电路。

[0099] 其中,存储器32可以包括用于数据或指令的大容量存储器。举例来说而非限制,存储器32可包括硬盘驱动器(Hard Disk Drive,简称为HDD)、软盘驱动器、固态驱动器(Solid State Drive,简称为SSD)、闪存、光盘、磁光盘、磁带或通用串行总线(Universal Serial Bus,简称为USB)驱动器或者两个或更多个以上这些的组合。在合适的情况下,存储器32可包括可移除或不可移除(或固定)的介质。在合适的情况下,存储器32可在数据处理装置的内部或外部。在特定实施例中,存储器32是非易失性(Non-Volatile)存储器。在特定实施例中,存储器32包括只读存储器(Read-Only Memory,简称为ROM)和随机存取存储器(Random Access Memory,简称为RAM)。在合适的情况下,该ROM可以是掩模编程的ROM、可编程ROM(Programmable Read-Only Memory,简称为PROM)、可擦除PROM(Erasable Programmable Read-Only Memory,简称为EPROM)、电可擦除PROM(Electrically Erasable Programmable Read-Only Memory,简称为EEPROM)、电可改写ROM(Electrically Alterable Read-Only Memory,简称为EAROM)或闪存(FLASH)或者两个或更多个以上这些的组合。在合适的情况下,该RAM可以是静态随机存取存储器(Static Random-Access Memory,简称为SRAM)或动态随机存取存储器(Dynamic Random Access Memory,简称为DRAM),其中,DRAM可以是快速页模式动态随机存取存储器(Fast Page Mode Dynamic Random Access Memory,简称为FPMDRAM)、扩展数据输出动态随机存取存储器(Extended Date Out Dynamic Random Access Memory,简称为EDODRAM)、同步动态随机存取内存(Synchronous Dynamic Random-Access Memory,简称SDRAM)等。

[0100] 存储器32可以用来存储或者缓存需要处理和/或通信使用的各种数据文件,以及处理器32所执行的可能的计算机程序指令。

[0101] 处理器31通过读取并执行存储器32中存储的计算机程序指令,以实现上述实施例

中的任意一种客户端登录认证方法。

[0102] 在其中一些实施例中，计算机设备还可包括通信接口33和总线30。其中，如图3所示，处理器31、存储器32、通信接口33通过总线30连接并完成相互间的通信。

[0103] 通信接口33用于实现本申请实施例中各模块、装置、单元和/或设备之间的通信。通信端口33还可以实现与其他部件例如：外接设备、图像/数据采集设备、数据库、外部存储以及图像/数据处理工作站等之间进行数据通信。

[0104] 总线30包括硬件、软件或两者，将计算机设备的部件彼此耦接在一起。总线30包括但不限于以下至少之一：数据总线(Data Bus)、地址总线(Address Bus)、控制总线(Control Bus)、扩展总线(Expansion Bus)、局部总线(Local Bus)。举例来说而非限制，总线30可包括图形加速接口(Accelerated Graphics Port，简称为AGP)或其他图形总线、增强工业标准架构(Extended Industry Standard Architecture，简称为EISA)总线、前端总线(Front Side Bus，简称为FSB)、超传输(Hyper Transport，简称为HT)互连、工业标准架构(Industry Standard Architecture，简称为ISA)总线、无线带宽(InfiniBand)互连、低引脚数(Low Pin Count，简称为LPC)总线、存储器总线、微信道架构(Micro Channel Architecture，简称为MCA)总线、外围组件互连(Peripheral Component Interconnect，简称为PCI)总线、PCI-Express(PCI-X)总线、串行高级技术附件(Serial Advanced Technology Attachment，简称为SATA)总线、视频电子标准协会局部(Video Electronics Standards Association Local Bus，简称为VLB)总线或其他合适的总线或者两个或更多个以上这些的组合。在合适的情况下，总线30可包括一个或多个总线。尽管本申请实施例描述和示出了特定的总线，但本申请考虑任何合适的总线或互连。

[0105] 该计算机设备可以基于获取到的程序指令，执行本申请实施例中的客户端登录认证方法，从而实现结合图1描述的客户端登录认证方法。

[0106] 另外，结合上述实施例中的客户端登录认证方法，本申请实施例可提供一种计算机可读存储介质来实现。该计算机可读存储介质上存储有计算机程序指令；该计算机程序指令被处理器执行时实现上述实施例中的任意一种客户端登录认证方法。

[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申请专利范围的限制。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。

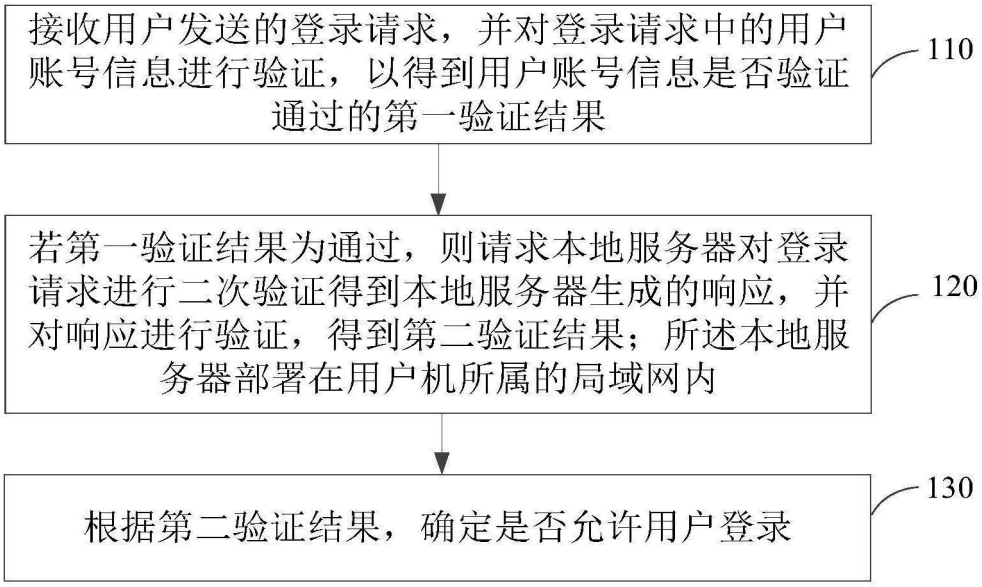

接收用户发送的登录请求，并对登录请求中的用户账号信息进行验证，以得到用户账号信息是否验证通过的第一验证结果
110
若第一验证结果为通过，则请求本地服务器对登录请求进行二次验证得到本地服务器生成的响应，并对响应进行验证，得到第二验证结果；所述本地服务器部署在用户机所属的局域网内
120
根据第二验证结果，确定是否允许用户登录
130

图1

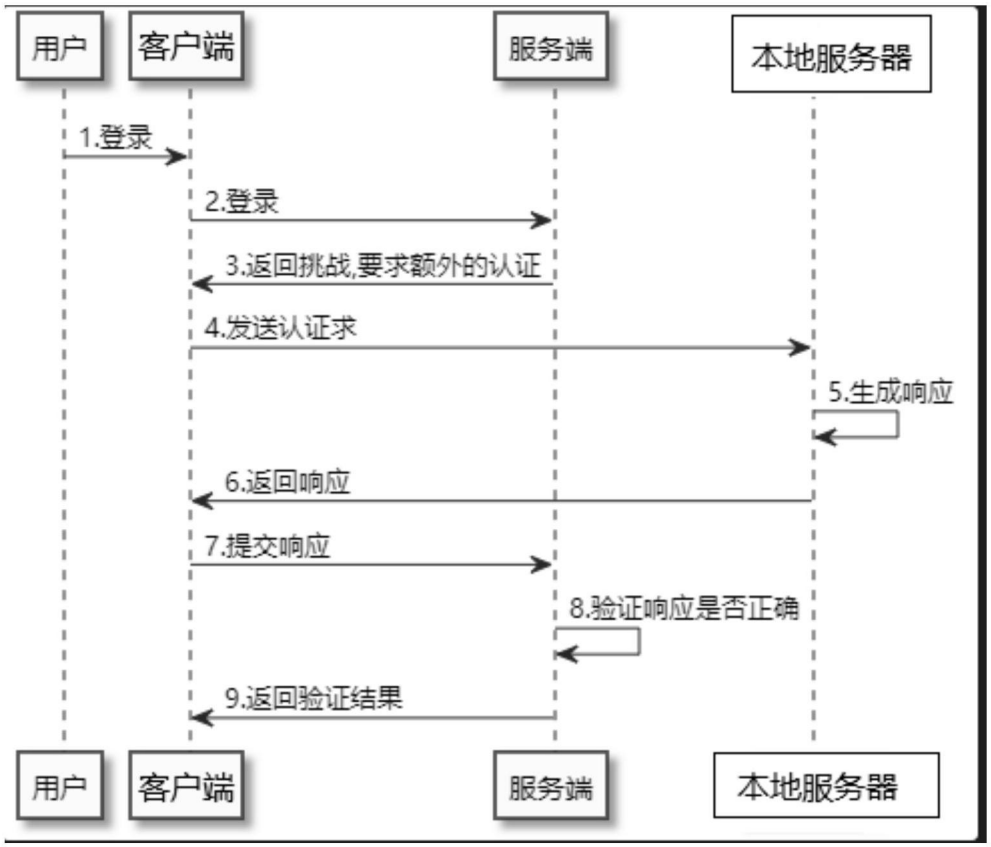

用户
客户端
服务端
本地服务器
1.登录
2.登录
3.返回挑战,要求额外的认证
4.发送认证求
5.生成响应
6.返回响应
7.提交响应
8.验证响应是否正确
9.返回验证结果
用户
客户端
服务端
本地服务器

图2

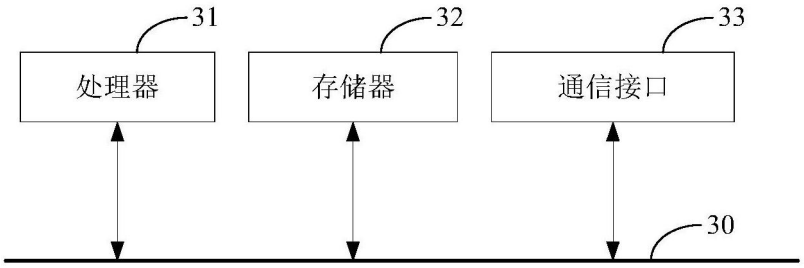


图3