(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110856174 B
(45)授权公告日 2020.11.27

(21)申请号 201911280019.5
(22)申请日 2019.12.13
(65)同一申请的已公布的文献号
申请公布号 CN 110856174 A
(43)申请公布日 2020.02.28
(73)专利权人 上海兴容信息技术有限公司
地址 201207 上海市浦东新区中国(上海)自由贸易试验区芳春路400号1幢3层
(72)发明人 卢国鸣
(74)专利代理机构 北京专赢专利代理有限公司 11797
代理人 于刚
(51)Int.Cl.
H04W 12/06(2009.01)

(56)对比文件
CN 103746983 A,2014.04.23
CN 109040255 A,2018.12.18
CN 107612909 A,2018.01.19

审查员 童雯

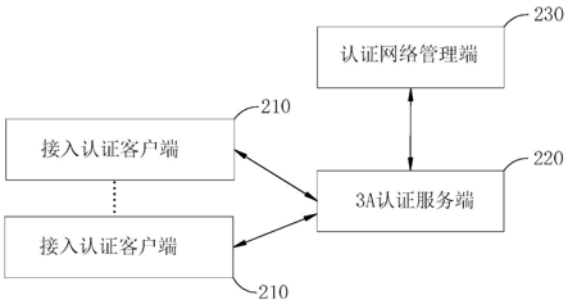
权利要求书3页 说明书12页 附图2页

(54)发明名称

一种接入认证系统、方法、装置、计算机设备和存储介质

(57)摘要

本发明适用于移动通信领域，提供了一种接入认证系统、方法、装置、计算机设备和存储介质，其中，所述接入认证系统包括：认证网络管理端以及与至少一个接入认证客户端进行通讯的3A认证服务端，3A认证服务端与认证网络管理端进行通讯。本发明实施例提供的一种接入认证系统，在实现接入认证过程中，通过3A认证服务端判断接入认证请求是否与认证网络管理端中预先储存的至少包含身份标识信息和分组密码的验证信息匹配，从而确定是否与所述接入认证客户端建立连接，在用于物联网设备的联网时，无需逐一计算后进行匹配，多个接入认证客户端可以共享分组密码，解决了现有的接入认证方式存在无法对物联网设备友好支持的技术问题。



CN 110856174 B

1.一种接入认证系统,其特征在于,所述接入认证系统包括:认证网络管理端以及与至少一个接入认证客户端进行通讯的3A认证服务端,所述3A认证服务端与所述认证网络管理端进行通讯;

所述3A认证服务端,用于获取所述接入认证客户端发送的接入认证请求,所述接入认证请求至少包含所述接入认证客户端的第一身份标识信息以及第一分组密码,所述第一分组密码用于至少一个接入认证客户端接入网络并与所述3A认证服务端进行通讯;判断所述接入认证请求是否与所述认证网络管理端中预先储存的验证信息匹配;当判断所述接入认证请求与所述认证网络管理端中预先储存的验证信息匹配时,与所述接入认证客户端建立连接,并向所述接入认证客户端返回匹配成功信息;

所述认证网络管理端,用于获取已接入所述网络的所述接入认证客户端的第二身份标识信息;根据所述第二身份标识信息和预先生成的第二分组密码生成所述预先储存的验证信息,所述第二分组密码用于至少一个所述接入认证客户端接入网络并与所述3A认证服务端进行通讯;所述第二分组密码共有多个;

其中,所述预先储存的验证信息至少包含所述已接入所述网络的所述接入认证客户端的第二身份标识信息以及所有的所述预先生成的第二分组密码;所述判断所述接入认证请求是否与所述认证网络管理端中预先储存的验证信息匹配的步骤,具体包括:判断所述接入认证请求携带的所述接入认证客户端的第一身份标识信息是否与所述已接入所述网络的所述接入认证客户端的第二身份标识信息匹配;当所述接入认证请求携带的所述接入认证客户端的第一身份标识信息与所述已接入所述网络的所述接入认证客户端的第二身份标识信息匹配时,与所述接入认证客户端建立连接,并向所述接入认证客户端返回匹配成功信息;所述判断所述接入认证请求是否与所述认证网络管理端中预先储存的验证信息匹配的步骤,还包括:判断所述接入认证请求携带的所述第一分组密码是否与所有的所述预先生成的第二分组密码中的任意一个所述第二分组密码匹配;当所述接入认证请求携带的所述第一分组密码与所有的所述预先生成的第二分组密码中的任意一个所述第二分组密码匹配时,与所述接入认证客户端建立连接,并向所述接入认证客户端返回匹配成功信息;

所述3A认证服务端还用于记录所述接入认证客户端发送的所述接入认证请求与所述认证网络管理端中预先储存的验证信息不匹配的次数,以追踪异常的接入认证请求;所述预先生成的第二分组密码是将所述网络的服务集标识信息基于PBKDF2算法计算所述网络的预共享密钥确定的;

所述认证网络管理端获取已接入所述网络的所述接入认证客户端的第二身份标识信息具体是所述认证网络管理端管理各不同的公司/部门的Wi-Fi网络第一分组密码设置,公司/部门管理员可以操作认证网络管理端来添加、禁用、删除当前公司/部门对应网络的第一分组密码,所述当前公司/部门对应网络的第一分组密码是分组Wi-Fi密码,公司管理员在进入平台操作之前需要先完成管理员身份认证,且只能管理自己管辖的公司/部门的网络对应的分组Wi-Fi密码;每个分组Wi-Fi密码的使用方是使用该网络的一个公司,或者一个部门,或者一个员工,或者一个Wi-Fi终端设备;管理员根据需求控制每个分组Wi-Fi密码使用的范围;

每个公司/部门的每个网络有其对应的独立的已绑定终端数据库,通过所述认证网络管理端,管理员可查看位于已绑定终端数据库中包含的已接入所述网络的所述接入认证客

户端的第二身份标识信息，该已绑定终端数据库包含已经绑定的Wi-Fi终端设备地址和对应的分组Wi-Fi密码，分组Wi-Fi密码对应的WPA PSK与绑定时间，对应的Wi-Fi网络的SSID以及对应的容许连接Wi-Fi网络的时间、时长、带宽；管理员可选择是否移除任意终端设备的绑定记录，以及是否回收对应的分组Wi-Fi密码绑定次数；

每个公司/部门的每个网络有其对应的独立的分组Wi-Fi密码数据库，分组Wi-Fi密码数据库包含预先生成的第二分组密码，预先生成的第二分组密码包含绑定次数使用完的分组Wi-Fi密码，以及有可剩余的可绑定次数的分组Wi-Fi密码；对于有可绑定此次数的分组Wi-Fi密码，其将被加入到可匹配分组Wi-Fi密码列表中，可匹配分组Wi-Fi密码列表中元素按照每个分组Wi-Fi密码剩余的绑定次数安装降序排列；

其中，接入认证客户端首先关联到Wi-Fi网络提供设备，Wi-Fi网络提供设备发送接入点随机值ANonce到接入认证客户端，接入认证客户端根据输入的密码和Wi-Fi网络的SSID信息计算PSK，使用PSK作为认证所需要的PMK，接入认证客户端生成终端随机值SNonce，然后根据Wi-Fi网络提供设备广播的Wi-Fi认证算法配置来计算PTK，并使用PTK来计算要发送的数据帧的消息完整性校验码MIC，然后发送包含有SNonce和MIC的数据帧到Wi-Fi网络提供设备；当Wi-Fi网络提供设备接收到该数据帧时，Wi-Fi网络提供设备检查该接入认证客户端的地址是否在认证缓存区存在，如果存在则使用缓存中认证数据计算是否符合，如果不符合，且3A认证服务端状态健康，删除缓存中该接入认证客户端的认证数据，继续从3A认证服务端发起认证，如果认证成功，3A认证服务端返回匹配成功信息，匹配成功信息内包含PMK、网络访问策略、认证缓存策略；Wi-Fi网络提供设备根据缓存策略缓存该接入认证客户端的认证信息以便进行候选的验证；如果本地认证缓存没有包含该接入认证客户端的认证信息，则直接提交到3A认证服务端进行候选流程；

根据所述接入认证请求中包含所述接入认证客户端的第一身份标识信息以及第一分组密码，来匹配到对应的公司/部门以及具体Wi-Fi网络，3A认证服务端选择对应的已绑定终端数据库和分组Wi-Fi密码数据库来进行匹配所述接入认证请求；如果3A认证服务端检查所述接入认证客户端地址在黑名单，则返回失败并终止后续流程，如果不在，3A认证服务端在对应的已绑定终端数据库查找该接入认证客户端对应的绑定信息来验证所述第一身份标识信息，如果已绑定终端数据库内存在该接入认证客户端对应的绑定信息，则使用该接入认证客户端对应的绑定信息中的PSK和Wi-Fi网络提供设备发送的认证算法来计算出PTK，然后计算认证请求帧的MIC，如果匹配MIC，则认证通过，返回包含PMK的成功结果并终止流程，如果匹配失败，则对Wi-Fi终端设定的单位时间失败次数加一，如果超过了容许的单位时间内失败次数，那么接入认证客户端地址进入黑名单，并返回失败，终止后续流程。

2.一种接入认证方法，其特征在于，运用于权利要求1所述的接入认证系统的3A认证服务端上，所述接入认证方法包括：

获取所述接入认证客户端发送的接入认证请求，所述接入认证请求至少包含所述接入认证客户端的第一身份标识信息以及第一分组密码，所述第一分组密码用于至少一个接入认证客户端接入网络并与所述3A认证服务端进行通讯；

判断所述接入认证请求是否与所述认证网络管理端中预先储存的验证信息匹配；当判断所述接入认证请求与所述认证网络管理端中预先储存的验证信息匹配时，与所述接入认证客户端建立连接，并向所述接入认证客户端返回匹配成功信息。

3.一种接入认证装置,其特征在于,设置于权利要求1所述的接入认证系统的3A认证服务端上,所述接入认证装置包括:

获取单元,用于获取所述接入认证客户端发送的接入认证请求,所述接入认证请求至少包含所述接入认证客户端的第一身份标识信息以及第一分组密码,所述第一分组密码用于至少一个接入认证客户端接入网络并与所述3A认证服务端进行通讯;

判断单元,用于判断所述接入认证请求是否与所述认证网络管理端中预先储存的验证信息匹配;当判断所述接入认证请求与所述认证网络管理端中预先储存的验证信息匹配时,与所述接入认证客户端建立连接,并向所述接入认证客户端返回匹配成功信息。

4.一种计算机设备,其特征在于,包括存储器和处理器,所述存储器中存储有计算机程序,所述计算机程序被所述处理器执行时,使得所述处理器执行权利要求2所述接入认证方法的步骤。

5.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质上存储有计算机程序,所述计算机程序被处理器执行时,使得所述处理器执行权利要求2所述接入认证方法的步骤。

一种接入认证系统、方法、装置、计算机设备和存储介质

技术领域

[0001] 本发明属于移动通信领域，尤其涉及一种接入认证系统、方法、装置、计算机设备和存储介质。

背景技术

[0002] 随着移动通信技术的发展，无线网络技术也得到了快速发展。在无线网络中，对于需要接入的终端设备，大多需要进行接入认证，以保证网络传输过程的安全。例如，在网络接入时需要使用Wi-Fi网络设备配置的唯一接入密码，即PSK(Pre-Shared Key，预共享密钥)，网络中所有终端设备使用这个PSK接入网络。

[0003] 目前，基于动态PSK的认证方式具有良好的安全性，但是每个用户设备都绑定一个全局唯一的私有密码，其要求每一个Wi-Fi密码绑定到唯一一个Wi-Fi设备接口。但是目前市面上很多物联网设备需要分享终端设备正在使用的Wi-Fi网络信息和密码信息发送到物联网设备，以便物联网设备接入Wi-Fi网络，这种认证方式对于物联网设备不友好。

[0004] 因此，现有的接入认证方式对于物联网设备的联网需要同时保证密码和物联网设备对应，操作起来较复杂，存在无法对物联网设备友好支持的问题。

发明内容

[0005] 本发明实施例的目的在于提供一种接入认证系统、方法、装置、计算机设备和存储介质，旨在解决现有的接入认证方式存在无法对物联网设备友好支持的技术问题。

[0006] 本发明实施例是这样实现的：一种接入认证系统，所述接入认证系统包括：认证网络管理端以及与至少一个接入认证客户端进行通讯的3A认证服务端，所述3A认证服务端与所述认证网络管理端进行通讯；

[0007] 所述3A认证服务端，用于获取所述接入认证客户端发送的接入认证请求，所述接入认证请求至少包含所述接入认证客户端的第一身份标识信息以及第一分组密码，所述第一分组密码用于至少一个接入认证客户端接入网络并与所述3A认证服务端进行通讯；判断所述接入认证请求是否与所述认证网络管理端中预先储存的验证信息匹配；当判断所述接入认证请求与所述认证网络管理端中预先储存的验证信息匹配时，与所述接入认证客户端建立连接，并向所述接入认证客户端返回匹配成功信息；

[0008] 所述认证网络管理端，用于获取已接入所述网络的所述接入认证客户端的第二身份标识信息；根据所述第二身份标识信息和预先生成的第二分组密码生成所述预先储存的验证信息，所述第二分组密码用于至少一个所述接入认证客户端接入网络并与所述3A认证服务端进行通讯；所述第二分组密码共有多个。

[0009] 本发明实施例的另一目的在于提供一种接入认证方法，运用于所述的接入认证系统的3A认证服务端上，所述接入认证方法包括：

[0010] 获取所述接入认证客户端发送的接入认证请求，所述接入认证请求至少包含所述接入认证客户端的第一身份标识信息以及第一分组密码，所述第一分组密码用于至少一个

接入认证客户端接入网络并与所述3A认证服务端进行通讯；

[0011] 判断所述接入认证请求是否与所述认证网络管理端中预先储存的验证信息匹配；当判断所述接入认证请求与所述认证网络管理端中预先储存的验证信息匹配时，与所述接入认证客户端建立连接，并向所述接入认证客户端返回匹配成功信息。

[0012] 本发明实施例的另一目的在于提供一种接入认证装置，设置于所述的接入认证系统的3A认证服务端上，所述接入认证装置包括：

[0013] 获取单元，用于获取所述接入认证客户端发送的接入认证请求，所述接入认证请求至少包含所述接入认证客户端的第一身份标识信息以及第一分组密码，所述第一分组密码用于至少一个接入认证客户端接入网络并与所述3A认证服务端进行通讯；

[0014] 判断单元，用于判断所述接入认证请求是否与所述认证网络管理端中预先储存的验证信息匹配；当判断所述接入认证请求与所述认证网络管理端中预先储存的验证信息匹配时，与所述接入认证客户端建立连接，并向所述接入认证客户端返回匹配成功信息。

[0015] 本发明实施例的另一目的在于提供一种计算机设备，所述计算机设备包括存储器和处理器，所述存储器中存储有计算机程序，所述计算机程序被所述处理器执行时，使得所述处理器执行上述接入认证方法的步骤。

[0016] 本发明实施例的另一目的在于提供一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时，使得所述处理器执行上述接入认证方法的步骤。

[0017] 本发明实施例提供的接入认证系统包括：认证网络管理端以及与至少一个接入认证客户端进行通讯的3A认证服务端，所述3A认证服务端与所述认证网络管理端进行通讯。本发明实施例提供的接入认证系统，在实现接入认证过程中，通过3A认证服务端判断接入认证请求是否与所述认证网络管理端中预先储存的至少包含身份标识信息和分组密码的验证信息匹配，可以确定是否与所述接入认证客户端建立连接，在用于物联网设备的联网时，无需逐一计算后进行匹配，多个接入认证客户端可以共享分组密码，因此计算量会相应降低，可以对物联网设备友好支持，解决了现有的接入认证方式存在无法对物联网设备友好支持的技术问题。

附图说明

[0018] 图1为本发明实施例提供的一种接入认证系统的应用环境图；

[0019] 图2为本发明实施例提供的一种接入认证系统的架构图；

[0020] 图3为本发明实施例提供的一种接入认证系统中3A认证服务端执行的步骤流程图；

[0021] 图4为本发明实施例提供的一种接入认证装置的结构示意图；

[0022] 图5为一个实施例中计算机设备的内部结构框图。

具体实施方式

[0023] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0024] 可以理解，本申请所使用的术语“第一”、“第二”等可在本文中用于描述各种元件，但除非特别说明，这些元件不受这些术语限制。这些术语仅用于将第一个元件与另一个元件区分。举例来说，在不脱离本申请的范围的情况下，可以将第一xx脚本称为第二xx脚本，且类似地，可将第二xx脚本称为第一xx脚本。

[0025] 图1为本发明实施例提供的一种接入认证系统的应用环境图，如图1所示，在该应用环境中，包括终端110、第一服务器120以及第二服务器130。

[0026] 所述第一服务器120、第二服务器130均可以是独立的物理服务器或终端，也可以是多个物理服务器构成的服务器集群，可以是提供云服务器、云数据库、云存储和CDN(Content Delivery Network，内容分发网络)等基础云计算服务的云服务器，但并不局限于此，可用于数据的传输和数据的处理。

[0027] 所述终端110可以是智能终端，如台式计算机、笔记本电脑等计算机设备，也可以是便于携带的智能终端，如平板电脑、智能手机、掌上电脑、智能眼镜、智能手表、智能手环、智能音箱等，但并不局限于此，所述终端110的数量可以是一个，也可以是多个，这里并不加限制。

[0028] 所述终端110与所述第一服务器120可以通过有线网络或者无线网络进行连接，本发明在此不做限制。所述第二服务器130与所述第一服务器120可以通过有线网络或者无线网络进行连接，本发明在此不做限制。

[0029] 如图2所示，提出了一种接入认证系统的架构图。在本发明实施例提供的接入认证系统中，包括认证网络管理端230以及与至少一个接入认证客户端210进行通讯的3A认证服务端220，所述3A认证服务端220与所述认证网络管理端230进行通讯。

[0030] 作为本发明的一个优选实施例，所述3A认证服务端220，运行于所述第一服务器120上，用于获取所述接入认证客户端210发送的接入认证请求，所述接入认证请求至少包含所述接入认证客户端210的第一身份标识信息以及第一分组密码，所述第一分组密码用于至少一个接入认证客户端210接入网络并与所述3A认证服务端220进行通讯；判断所述接入认证请求是否与所述认证网络管理端230中预先储存的验证信息匹配；当判断所述接入认证请求与所述认证网络管理端230中预先储存的验证信息匹配时，与所述接入认证客户端210建立连接，并向所述接入认证客户端210返回匹配成功信息。

[0031] 在本发明实施例中，所述3A认证服务端220与图1示出的所述第一服务器120相关联，运行于所述第一服务器120上，可以是运行于所述第一服务器120上的一个程序，也可以所述第一服务器120的一个功能模块。

[0032] 在本发明实施例中，所述3A认证服务端220负责对接入认证客户端210进行身份认证，以鉴别其是否有权限访问所保护的网络资源；3A认证服务端可以是AAA(Authentication Authorization Accounting，认证、授权与计费)服务器，全程使用网络连接服务接入认证客户端210；所述第一服务器120可以是独立的物理服务器或终端，也可以是多个物理服务器构成的服务器集群，可以是提供云服务器、云数据库、云存储和CDN等基础云计算服务的云服务器；所述3A认证服务端220和接入认证客户端210之间全程使用合法的网络连接。

[0033] 作为本发明又一种实施例，所述3A认证服务端220负责管理已接入的接入认证客户端210的用户凭据，以及用户对应的策略，认证网络管理端230通过RADIUS协议访问3A认

证服务端220来查询凭据是否有效，以决定是否开放该终端用户对受保护的网络资源访问。

[0034] 作为本发明又一种实施例，所述3A认证服务端220在接收到认证的时候，先检查认证的来源Wi-Fi网络提供设备信息，以及对应的3A认证服务端220的密码，如果密码验证错误，或者Wi-Fi提供设备或者网络未知，则返回失败并终止后续流程。

[0035] 作为本发明又一种实施例，对于部分物联网设备通过分享接入认证客户端210的Wi-Fi信息和密码的情况，如果策略容许物联网设备都是用同样的密码，那么只需要使用同一个接入认证客户端210设置这些物联网设备。如果策略要求多个物联网设备使用独立的密码，或者分组使用不同的分组Wi-Fi密码，那么设置一个终端设备，例如智能手机作为接入认证客户端210，系统记录该设置智能手机的Wi-Fi设备地址，当该终端设备的认证进入3A认证服务端220的时候，3A认证服务端220在绑定该终端设备的时候不减少待绑定的分组Wi-Fi密码使用次数，也不要求Wi-Fi网络提供设备缓存该Wi-Fi终端的认证信息，因此该智能手机可以使用目标物联网设备的将要使用的分组Wi-Fi密码接入Wi-Fi网络，然后设置对应的物联网设备。

[0036] 本发明实施例通过判断所述接入认证请求是否与所述认证网络管理端230中预先储存的验证信息匹配；当判断所述接入认证请求与所述认证网络管理端230中预先储存的验证信息匹配时，与所述接入认证客户端210建立连接，并向所述接入认证客户端210返回匹配成功信息，无需逐一计算后进行匹配，通过多个Wi-Fi终端可以共享分组Wi-Fi密码，候选的可绑定Wi-Fi密码数目减少，因此计算量会相应降低，提升了认证性能，在对于物联网设备的联网时，无需逐个同时保证密码和物联网设备对应，可以对物联网设备友好支持。

[0037] 作为本发明的一个优选实施例，所述认证网络服务端230，运行于所述第二服务器130上，用于获取已接入所述网络的所述接入认证客户端210的第二身份标识信息；根据所述第二身份标识信息和预先生成的第二分组密码生成所述预先储存的验证信息，所述第二分组密码用于至少一个所述接入认证客户端210接入网络并与所述3A认证服务端220进行通讯；所述第二分组密码共有多个。

[0038] 在本发明实施例中，所述认证网络服务端230与图1示出的所述第二服务器130相关联，运行于所述第二服务器130上，可以是运行于所述第二服务器130上的一个程序，也可以所述第二服务器130的一个功能模块。

[0039] 在本发明实施例中，所述认证网络服务端230生成所述预先储存的验证信息是通过服务器实现的，所述服务器可以是独立的物理服务器或终端，也可以是多个物理服务器构成的服务器集群，可以是提供云服务器、云数据库、云存储和CDN等基础云计算服务的云服务器。

[0040] 作为本发明一种实施例，所述认证网络服务端230获取已接入所述网络的所述接入认证客户端210的第二身份标识信息，具体的，所述认证网络管理端230管理各不同的公司/部门的Wi-Fi网络第一分组密码设置，公司/部门管理员可以操作认证网络管理端230来添加、禁用、删除当前公司/部门对应网络的第一分组密码，即分组Wi-Fi密码，公司管理员在进入平台操作之前需要先完成管理员身份认证，且只能管理自己管辖的公司/部门的网络对应的分组Wi-Fi密码。每个分组Wi-Fi密码的使用方可以是使用该网络的一个公司，或者一个部门，或者一个员工，甚至一个Wi-Fi终端设备；其他公司、部门、员工或Wi-Fi终端设备不能使用该分组Wi-Fi密码。管理员根据实际需求灵活的控制每个分组Wi-Fi密码使用的

范围,并通过邮件等方式告知相关人员。

[0041] 作为本发明又一种实施例,每个公司/部门的每个网络有其对应的独立的已绑定终端设备数据库,通过所述认证网络管理端230,管理员也可以查看位于已绑定终端设备数据库中包含的已接入所述网络的所述接入认证客户端210的第二身份标识信息,该数据库包含已经绑定的Wi-Fi终端设备地址和对应的分组Wi-Fi密码,分组Wi-Fi密码对应的WPA(Wi-Fi Protected Access,保护无线电脑网络安全系统)PSK、绑定时间等信息,对应的Wi-Fi网络的SSID(Service Set Identifier,服务集标识)以及对应的容许连接Wi-Fi网络的时间、时长、带宽等策略信息。管理员可以选择是否移除任意终端设备的绑定记录,以及是否回收对应的分组Wi-Fi密码绑定次数,如果选择回收绑定次数,那么对应的分组Wi-Fi密码可绑定设备数目增加一个,如果对应分组Wi-Fi密码从可绑定的分组Wi-Fi密码列表中移除,并将被重新加入到可绑定分组Wi-Fi密码列表中。

[0042] 作为本发明又一种实施例,每个公司/部门的每个网络有其对应的独立的分组Wi-Fi密码数据库,分组Wi-Fi密码数据库包含预先生成的第二分组密码,预先生成的第二分组密码包含绑定次数使用完的分组Wi-Fi密码,以及有可剩余的可绑定次数的分组Wi-Fi密码。对于有可绑定此次数的分组Wi-Fi密码,其将被加入到可匹配分组Wi-Fi密码列表中,可匹配分组Wi-Fi密码列表中元素按照每个分组Wi-Fi密码剩余的绑定次数安装降序排列,即更大几率的匹配成功的分组Wi-Fi密码将会被优先尝试。

[0043] 作为本发明又一种实施例,接入认证客户端210首先关联到Wi-Fi网络提供设备,Wi-Fi网络提供设备发送接入点随机值ANonce(Authenticator Nonce,Wi-Fi产生的接入点随机值)到接入认证客户端210,接入认证客户端210根据输入的密码和Wi-Fi网络的SSID信息计算PSK,使用PSK作为认证所需要的PMK(Pairwise Master Key),接入认证客户端210生成终端随机值SNonce(Supplicant Nonce,Wi-Fi终端产生的接入点随机值),然后根据Wi-Fi网络提供设备广播的Wi-Fi认证算法配置来计算PTK(Pairwise Transient Key),并使用PTK来计算要发送的数据帧的消息完整性校验和MIC(Message Integrity Code),然后发送包含有SNonce和MIC的数据帧到Wi-Fi网络提供设备。当Wi-Fi网络提供设备接收到该数据帧时,Wi-Fi网络提供设备检查该接入认证客户端210的地址是否在认证缓存区存在,如果存在则使用缓存中认证数据计算是否符合,如果不符合,且3A认证服务端220状态健康,删除缓存中该接入认证客户端210的认证数据,继续从3A认证服务端220发起认证,如果认证成功,3A认证服务端220返回匹配成功信息,匹配成功信息内包含PMK、网络访问策略、认证缓存策略等。Wi-Fi网络提供设备根据缓存策略缓存该接入认证客户端210的认证信息以便进行候选的验证。如果本地认证缓存没有包含该接入认证客户端210的认证信息,则直接提交到3A认证服务端220进行候选流程。

[0044] 作为本发明又一种实施例,根据所述接入认证请求中包含所述接入认证客户端210的第一身份标识信息以及第一分组密码,来匹配到对应的公司/部门以及具体Wi-Fi网络,3A认证服务端220选择对应的已绑定终端数据库和分组Wi-Fi密码数据库来进行匹配所述接入认证请求。首先,3A认证服务端220检查所述接入认证客户端210地址是否在黑名单,如果在,则返回失败并终止后续流程,如果不在,3A认证服务端220在对应的终端绑定数据库查找该接入认证客户端210对应的绑定信息来验证所述第一身份标识信息,如果数据库内存在该条目,则使用该条目中的PSK和Wi-Fi网络提供设备发送的认证算法来计算出PTK,

然后计算认证请求帧的MIC，如果匹配MIC，则认证通过，返回包含PMK的成功结果并终止流程，如果匹配失败，则对Wi-Fi终端设定的单位时间失败次数加一，如果超过了容许的单位时间内失败次数，那么接入认证客户端210地址进入黑名单，并返回失败，终止后续流程。

[0045] 作为本发明又一种实施例，对于不在已绑定终端数据库内的所述接入认证客户端210，3A认证服务端220尝试从对应的分组Wi-Fi密码数据库进行匹配，根据上一步相同的逻辑计算MIC，如果匹配，则减少对应分组Wi-Fi密码的可匹配数目，并根据可匹配数据调整其在分组Wi-Fi密码数据库中的位置，在数目为零的情况下，将该分组Wi-Fi密码移出分组Wi-Fi密码数据库，将该接入认证客户端210和分组Wi-Fi密码的匹配记录加入到已绑定在已绑定终端数据库，返回包含PMK的成功结果并终止流程。

[0046] 作为本发明又一种实施例，如果当前待绑定的分组Wi-Fi密码验证匹配失败，则继续查找下一个待绑定的分组Wi-Fi密码，如果有一个分组Wi-Fi密码匹配，那么与所述接入认证客户端210建立连接，并向所述接入认证客户端210返回匹配成功信息。如果所有的分组Wi-Fi密码都无法完成匹配，则对所述接入认证客户端210设定的单位时间失败次数加一，如果超过了容许的单位时间内失败次数，那么该接入认证客户端210地址进入黑名单，并返回失败，终止后续流程。

[0047] 本发明实施例通过3A认证服务端220来实现Wi-F网络的认证接入，同时提供中心云平台实现企业或者部门自己的内部认证以及分组Wi-Fi密码生成，分发和管理，不同的企业或者部门，或者其它分类实体对应的分组Wi-Fi密码数据库都是分开存取，分组Wi-Fi密码数据库和对应的企业或者部分或者其它场所实体的Wi-Fi网络提供设备信息和Wi-Fi网络配置信息关联，根据接入认证请求的来源对应的Wi-Fi网络提供设备信息，以及Wi-Fi网络配置信息来动态区分使用的组密码数据库，通过切分到不同的密码数据库能够有效减少数据存取，提高查询性能，对于计算量大的分组Wi-Fi密码的动态匹配，能够有效的缩短穷举比对时间。

[0048] 本发明实施例通过判断所述接入认证请求是否与所述认证网络管理端230中预先储存的验证信息匹配，所述接入认证请求至少包含所述接入认证客户端210的第一身份标识信息以及第一分组密码，所述预先储存的验证信息是根据所述第二身份标识信息和预先生成的第二分组密码生成的；当判断所述接入认证请求与所述认证网络管理端230中预先储存的验证信息匹配时，与所述接入认证客户端210建立连接，并向所述接入认证客户端210返回匹配成功信息，无需逐一计算后进行匹配，通过多个Wi-Fi终端可以共享分组Wi-Fi密码，候选的可绑定Wi-Fi密码数目减少，因此计算量会相应降低，提升了认证性能，在对于物联网设备的联网时，无需逐个同时保证密码和物联网设备对应，可以对物联网设备友好支持，同时，根据接入认证请求的来源对应的Wi-Fi网络提供设备信息，以及Wi-Fi网络配置信息来动态区分使用的组密码数据库，通过切分到不同的密码数据库能够有效减少数据存取，提高查询性能，对于计算量大的分组Wi-Fi密码的动态匹配，能够有效的缩短穷举比对时间。

[0049] 本发明实施例提供的一种接入认证系统，所述预先储存的验证信息至少包含所述已接入所述网络的所述接入认证客户端210的第二身份标识信息以及所有的所述预先生成的第二分组密码。

[0050] 在本发明实施例中，对于部分物联网设备通过分享接入认证客户端210的Wi-Fi信

息和密码的情况，如果策略容许物联网设备都是用同样的密码，那么只需要使用同一个接入认证客户端210设置这些物联网设备。如果策略要求多个物联网设备使用独立的密码，或者分组使用不同的分组Wi-Fi密码，那么设置一个终端设备，例如智能手机作为接入认证客户端210，系统记录该设置智能手机的Wi-Fi设备地址，当该终端设备的认证进入3A认证服务端220的时候，3A认证服务端220在绑定该终端设备的时候不减少待绑定的分组Wi-Fi密码使用次数，也不要求Wi-Fi网络提供设备缓存该Wi-Fi终端的认证信息，因此该智能手机可以使用目标物联网设备的将要使用的分组Wi-Fi密码接入Wi-Fi网络，然后设置对应的物联网设备。

[0051] 本发明实施例通过设置至少包含所述已接入所述网络的所述接入认证客户端210的第二身份标识信息以及所有的所述预先生成的第二分组密码的所述预先储存的验证信息，当判断所述接入认证请求与所述认证网络管理端230中预先储存的验证信息匹配时，与所述接入认证客户端210建立连接，并向所述接入认证客户端210返回匹配成功信息，无需逐一计算后进行匹配，通过多个Wi-Fi终端可以共享分组Wi-Fi密码，候选的可绑定Wi-Fi密码数目减少，因此计算量会相应降低，提升了认证性能，在对于物联网设备的联网时，无需逐个同时保证密码和物联网设备对应，可以对物联网设备友好支持，降低了信息泄露的风险，提供了足够安全的Wi-Fi认证和数据保护。

[0052] 本发明实施例提供的一种接入认证系统，所述判断所述接入认证请求是否与所述认证网络管理端230中预先储存的验证信息匹配的步骤，具体包括：

[0053] 判断所述接入认证请求携带的所述接入认证客户端210的第一身份标识信息是否与所述已接入所述网络的所述接入认证客户端210的第二身份标识信息匹配；

[0054] 当所述接入认证请求携带的所述接入认证客户端210的第一身份标识信息与所述已接入所述网络的所述接入认证客户端210的第二身份标识信息匹配时，与所述接入认证客户端210建立连接，并向所述接入认证客户端210返回匹配成功信息。

[0055] 在本发明实施例中，对于通过接入认证请求的接入认证客户端210，3A认证服务端220会返回用户的认证密码相关信息以及认证缓存时间等其它认证凭据到Wi-Fi网络提供设备，如Wi-Fi接入点或者Wi-Fi控制器，Wi-Fi网络设备在本地存储进行Wi-Fi认证所需要的用户密码或者其它凭据信息Wi-Fi网络信息，并记录对应的Wi-Fi终端设备地址，在凭据的有效时间内，后续该接入认证客户端210主动或者被动等情况断开Wi-Fi网络再重新认证时，Wi-Fi提供设备使用本地存储的认证数据来对Wi-Fi终端设备进行认证。

[0056] 本发明实施例提供的一种接入认证系统，所述判断所述接入认证请求是否与所述认证网络管理端230中预先储存的验证信息匹配的步骤，还包括：

[0057] 判断所述接入认证请求携带的所述第一分组密码是否与所有的所述预先生成的第二分组密码中的任意一个所述第二分组密码匹配；

[0058] 当所述接入认证请求携带的所述第一分组密码与所有的所述预先生成的第二分组密码中的任意一个所述第二分组密码匹配时，与所述接入认证客户端210建立连接，并向所述接入认证客户端210返回匹配成功信息。

[0059] 在本发明实施例中，所述判断所述接入认证请求是否与所述认证网络管理端230中预先储存的验证信息匹配的步骤可以通过服务器实现，所述服务器可以是独立的物理服务器或终端，也可以是多个物理服务器构成的服务器集群，可以是提供云服务器、云数据

库、云存储和CDN等基础云计算服务的云服务器。

[0060] 作为本发明一种实施例，通过给位于同一个公司，或者同一个部门，或者单独一个人分配一个对应Wi-Fi网络的分组Wi-Fi密码，并限制该密码可以绑定的设备数目来简化用户的在设备上配置Wi-Fi网络，即对应的所述第二分组密码匹配，分组Wi-Fi密码可以和多个接入认证客户端210自动匹配绑定。在部门增加新员工，或者员工要接入自己的新的接入认证客户端210，或者新增智能物联网设备的时候，不需要获取新密码，也不需要进行复杂的绑定流程，该分组Wi-Fi密码只能供有限的Wi-Fi设备使用。当新的接入认证客户端210在相应的Wi-Fi网络中使用该分组Wi-Fi密码完成绑定时，该分组Wi-Fi密码可以绑定的设备数据减一，新绑定的接入认证客户端210会进入到绑定设备列表，后续可以直接通过该密码接入对应的Wi-Fi网络，无需重新执行进行绑定流程。当该分组Wi-Fi密码可绑定的Wi-Fi设备数目为零的时候，未绑定分组Wi-Fi密码的接入认证客户端210将无法通过该密码完成绑定，只能使用其它可用分组Wi-Fi密码，否则不能接入Wi-Fi网络。

[0061] 本发明实施例通过判断所述接入认证请求携带的所述第一分组密码是否与所有的所述预先生成的第二分组密码中的任意一个所述第二分组密码匹配，当所述接入认证请求携带的所述第一分组密码与所有的所述预先生成的第二分组密码中的任意一个所述第二分组密码匹配时，与所述接入认证客户端210建立连接，并向所述接入认证客户端210返回匹配成功信息，无需逐一计算后进行匹配，通过多个Wi-Fi终端可以共享分组Wi-Fi密码，候选的可绑定Wi-Fi密码数目减少，因此计算量会相应降低，提升了认证性能，在对于物联网设备的联网时，无需逐个同时保证密码和物联网设备对应，可以对物联网设备友好支持。

[0062] 本发明实施例提供的一种接入认证系统，所述3A认证服务端220，还用于记录所述接入认证客户端210发送的所述接入认证请求与所述认证网络管理端230中预先储存的验证信息不匹配的次数，以追踪异常的接入认证请求。

[0063] 作为本发明一种实施例，所述3A认证服务端220追踪记录认证失败的次数，同时Wi-Fi网络提供设备周期性检查3A认证服务端220认证失败次数，如果该周期内没有认证发生，那么Wi-Fi网络设备主动发起认证请求来检测3A认证服务端220的健康状态。该认证请求可以是居于预配置账户的认证请求，也可以是如服务器状态查询这样的状态请求。如果3A认证服务端220在配置的多个周期内连续失败，那么Wi-Fi网络提供设备设置该3A认证服务端220为失败状态，同时开始周期性检测该3A认证服务端220是否重新存活。在存在备用3A认证服务端220的情况下，切换发送接入认证请求到备用3A认证服务端220，如果没有备用3A认证服务端220，Wi-Fi网络提供设备将不对已经缓存的终端和其对应的密码信息进行超时处理，直到有一个以上的3A认证服务端220状态恢复到健康可服务的状态。

[0064] 作为本发明又一种实施例，当3A认证服务端220接收到接入认证客户端210的接入认证请求时，且该接入认证客户端210的认证凭据信息已经在预先储存的验证信息中缓存，则使用已经缓存的信息对接入认证客户端210进行认证。若认证成功，则开通接入认证客户端210的网络访问权限。如果认证失败，则执行如下操作：当有至少一个健康可用的3A认证服务端220存在时，Wi-Fi网络提供设备删除对应该接入认证客户端210的缓存认证凭据信息，然后发送认证请求到3A认证服务端220完成认证；如果认证依然失败，则返回失败信息到接入认证客户端210；如果没有健康可用的3A认证服务端220存在，Wi-Fi网络提供设备保留缓存的该终端认证凭据信息，直接返回失败信息到接入认证客户端210。

[0065] 本发明实施例通过3A认证服务端220记录一段时间内接入认证客户端210认证失败的次数来追踪异常和恶意的密码绑定请求。对于异常或者恶意的接入认证客户端210,3A认证服务端220将这些3A认证服务端220的地址存入黑名单一段时间。对于黑名单内的接入认证客户端210,AAA认证服务器跳过接入认证请求直接返回认证错误,减轻计算负担,同时避免恶意穷举Wi-Fi网络密码。

[0066] 本发明实施例提供的一种接入认证系统所述预先生成的第二分组密码是将所述网络的服务集标识信息基于PBKDF2算法计算所述网络的预共享密钥确定的。

[0067] 在本发明实施例中,所述预先生成的第二分组密码是对于每个新产生同一网络内的不重复分组Wi-Fi密码,根据该Wi-Fi网络的SSID信息使用PBKDF2(Password-Based Key Derivation Function,导出密钥函数)算法计算出预共享密钥PSK,且PSK=PBKDF2(HMAC-SHA1,分组Wi-Fi密码,SSID,4096,256),计算结果存储在分组Wi-Fi密码数据库,其中HMAC-SHA1是基于SHA1(Secure Hash Algorithm 1,安全散列算法1)的哈希运算消息认证码。

[0068] 作为本发明一种实施例,提出了图2所示出的一种接入认证系统实现接入认证的流程,详述如下。

[0069] 企业或者部门管理员通过认证网络管理端230来生成新的分组Wi-Fi密码,并将分组Wi-Fi密码分配给需要连接的接入认证客户端210,即Wi-Fi终端设备。已绑定终端设备数据库维护已经绑定的Wi-Fi终端设备的地址信息、使用的分组Wi-Fi密码信息和使用时长、带宽、限制策略等信息。分组Wi-Fi密码数据库记录所有的分组Wi-Fi密码、密码对应的公司/部门等网络信息、分组Wi-Fi密码可绑定的Wi-Fi终端设备数目以及已经绑定的Wi-Fi终端设备数目等。3A认证服务端220负责对从网络接收到的接入认证请求进行验证,对已经存在于已绑定终端设备数据库的Wi-Fi终端设备通过与数据库中对应的条目进行验证,如果验证通过就对Wi-Fi终端设备返回成功结果,否则返回失败结果,对不存在已绑定终端设备数据库的Wi-Fi终端设备,将所述接入认证请求携带的所述第一分组密码和可绑定的分组Wi-Fi密码逐一进行验证,若有一个分组Wi-Fi密码可以匹配验证通过,则返回成功结果,并加入该Wi-Fi终端设备到已绑定终端设备数据库,否则返回错误。Wi-Fi网络提供设备对Wi-Fi终端提供Wi-Fi网络服务,根据Wi-Fi终端设备输入的Wi-Fi密码凭据发送验证请求到3A认证服务端220对Wi-Fi终端设备进行验证。

[0070] 如图3所示,提出了一种接入认证系统中3A认证服务端220执行的接入认证方法的步骤流程图,具体包括以下步骤:

[0071] 在步骤S302中,获取所述接入认证客户端210发送的接入认证请求,所述接入认证请求至少包含所述接入认证客户端210的第一身份标识信息以及第一分组密码,所述第一分组密码用于至少一个接入认证客户端210接入网络并与所述3A认证服务端220进行通讯。

[0072] 在本发明实施例中,所述3A认证服务端与图1示出的所述第一服务器120相关联,运行于所述第一服务器120上,可以是运行于所述第一服务器120上的一个程序,也可以所述第一服务器120的一个功能模块,所述服务器可以是独立的物理服务器或终端,也可以是多个物理服务器构成的服务器集群,可以是提供云服务器、云数据库、云存储和CDN等基础云计算服务的云服务器。

[0073] 在步骤S304中,判断所述接入认证请求是否与所述认证网络管理端230中预先储存的验证信息匹配;当判断所述接入认证请求与所述认证网络管理端230中预先储存的验

证信息匹配时，与所述接入认证客户端210建立连接，并向所述接入认证客户端210返回匹配成功信息。

[0074] 在本发明实施例中，通过提供一个基于分组Wi-Fi密码动态绑定以及认证缓存的高性能、高容错且容易扩展、实施和维护的接入认证系统，分组Wi-Fi密码在同一个公司/部门的同一个网络内不重复，每个分组Wi-Fi密码可以被配置容许数目的Wi-Fi设备所使用，数目达到配置容许的上限时，其他Wi-Fi设备无法和该分组Wi-Fi密码尝试绑定，从而可以在BYOD(Bring Your Own Device，携带自己的设备办公)模式下实现单用户多设备，可维护性高，具有良好的经济性和可靠性，密码动态绑定时可选密码数目更少，有效提高了匹配性能，从而友好安全的访客网络。

[0075] 如图4所示，在一个实施例中，提供了一种接入认证装置，所述接入认证装置可以集成于上述的3A认证服务端220中，具体可以包括：获取单元410与判断单元420。

[0076] 获取单元410，用于获取所述接入认证客户端210发送的接入认证请求，所述接入认证请求至少包含所述接入认证客户端210的第一身份标识信息以及第一分组密码，所述第一分组密码用于至少一个接入认证客户端210接入网络并与所述3A认证服务端220进行通讯。

[0077] 判断单元420，用于判断所述接入认证请求是否与所述认证网络管理端230中预先储存的验证信息匹配；当判断所述接入认证请求与所述认证网络管理端230中预先储存的验证信息匹配时，与所述接入认证客户端210建立连接，并向所述接入认证客户端210返回匹配成功信息。

[0078] 在本发明实施例中，所述接入认证装置可以是数据电路端接设备，如调制解调器、集线器、桥接器或交换机；也可以是一个数据终端设备，如数字手机，打印机或主机，所述主机可以是路由器、工作站、服务器或无线传感器；还可以是智能终端，如笔记本电脑等计算机设备，也可以是便于携带的智能终端，如平板电脑、掌上电脑、智能眼镜、智能手表、智能手环、智能音箱等，但并不局限于此，可用于数据的转换、管理、处理和传输，所述获取单元410与判断单元420均存储有操作系统，用于处理各种基本方法服务和用于执行硬件相关任务的程序；还存储有应用软件，用于实现本发明实施例中的接入认证方法的步骤。

[0079] 所述接入认证装置可执行如上述任一实施例中提供的接入认证方法的步骤，其中，本发明实施例提供了一种接入认证方法，所述方法包括如下步骤，如图3所示：

[0080] 在步骤S302中，获取所述接入认证客户端210发送的接入认证请求，所述接入认证请求至少包含所述接入认证客户端210的第一身份标识信息以及第一分组密码，所述第一分组密码用于至少一个接入认证客户端210接入网络并与所述3A认证服务端220进行通讯。

[0081] 在本发明实施例中，所述3A认证服务端与图1示出的所述第一服务器120相关联，运行于所述第一服务器120上，可以是运行于所述第一服务器120上的一个程序，也可以所述第一服务器120的一个功能模块，所述服务器可以是独立的物理服务器或终端，也可以是多个物理服务器构成的服务器集群，可以是提供云服务器、云数据库、云存储和CDN等基础云计算服务的云服务器。

[0082] 在步骤S304中，判断所述接入认证请求是否与所述认证网络管理端230中预先储存的验证信息匹配；当判断所述接入认证请求与所述认证网络管理端230中预先储存的验证信息匹配时，与所述接入认证客户端210建立连接，并向所述接入认证客户端210返回匹

配成功信息。

[0083] 在一个实施例中，提出了一种计算机设备，所述计算机设备包括存储器、处理器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本发明实施例中的接入认证方法的步骤。

[0084] 图5示出了一个实施例中计算机设备的内部结构图。如图5所示，该计算机设备包括通过系统总线连接的处理器、存储器、网络接口和输入装置。其中，该计算机设备的存储器存储有操作系统，还可存储有计算机程序，该计算机程序被处理器执行时，可使得处理器实现所述接入认证方法。计算机设备的输入装置可以是计算机设备外壳上设置的按键、轨迹球或触控板，还可以是外接的键盘、触控板或鼠标等。

[0085] 在本发明实施例中，存储器可以是高速随机存取存储器，诸如DRAM、SRAM、DDR、RAM、或者其他随机存取固态存储设备，或者非易失性存储器，诸如一个或多个硬盘存储设备、光盘存储设备、内存设备等。

[0086] 本领域技术人员可以理解，图5中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

[0087] 在一个实施例中，本申请提供的接入认证装置可以实现为一种计算机程序的形式，计算机程序可在如图5所示的计算机设备上运行。计算机设备的存储器中可存储组成该接入认证装置的各个程序模块，比如，图4所示的获取单元410与判断单元420。各个程序模块构成的计算机程序使得处理器执行本说明书中描述的本申请各个实施例的接入认证方法中的步骤。

[0088] 例如，图5所示的计算机设备可以通过如图4所示的接入认证装置中的获取单元410执行步骤S302，获取所述接入认证客户端210发送的接入认证请求，所述接入认证请求至少包含所述接入认证客户端210的第一身份标识信息以及第一分组密码，所述第一分组密码用于至少一个接入认证客户端210接入网络并与所述3A认证服务端220进行通讯。计算机设备可通过判断单元420执行步骤S304，判断所述接入认证请求是否与所述认证网络管理端230中预先储存的验证信息匹配；当判断所述接入认证请求与所述认证网络管理端230中预先储存的验证信息匹配时，与所述接入认证客户端210建立连接，并向所述接入认证客户端210返回匹配成功信息。

[0089] 另外，本发明实施例还提供了一种计算机可读存储介质，计算机可读存储介质上存储有计算机程序，计算机程序被处理器执行时，使得处理器执行上述接入认证方法的步骤。

[0090] 在本发明所提供的几个实施例中，应该理解到，所描述的实施例仅仅是示意性的，例如，所述模块的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个模块可以结合或者可以集成到一起，或一些模块可以忽略，可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。

[0091] 应该理解的是，虽然本发明各实施例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，各实施例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。

[0092] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一非易失性计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限，RAM以多种形式可得，诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(S6nchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0093] 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。

[0094] 以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本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，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

[0095] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

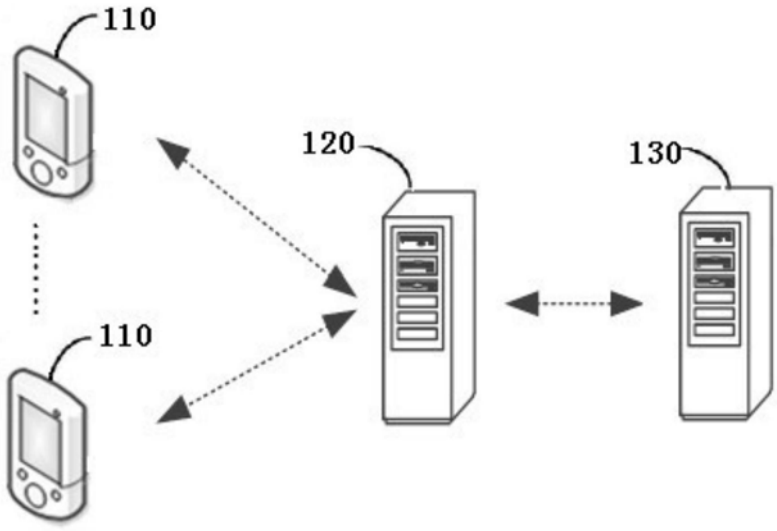

110
120
130
110

图1

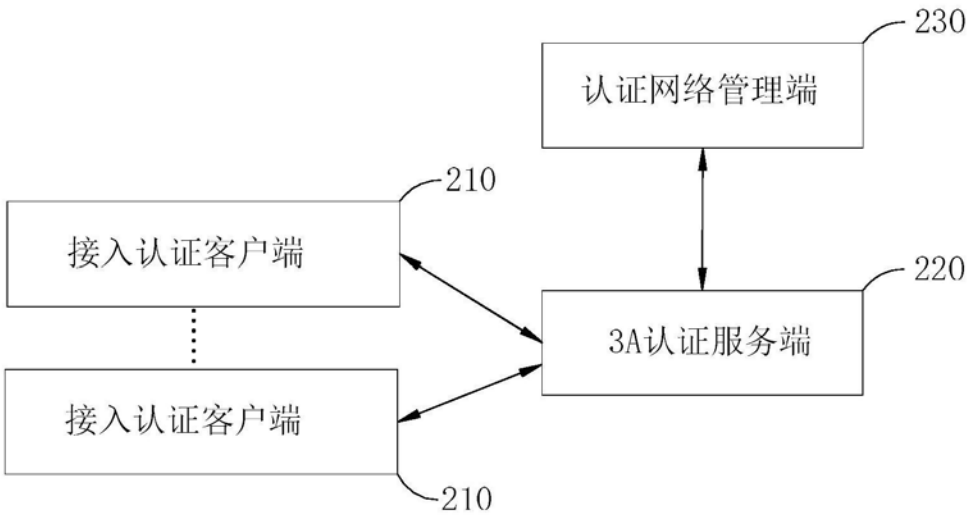

230
认证网络管理端
210
接入认证客户端
220
3A认证服务端
接入认证客户端
210

图2

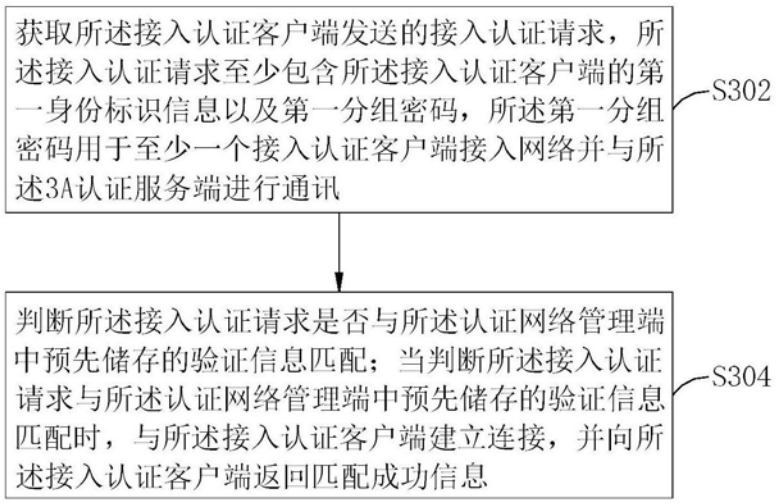

获取所述接入认证客户端发送的接入认证请求，所述接入认证请求至少包含所述接入认证客户端的第一身份标识信息以及第一分组密码，所述第一分组密码用于至少一个接入认证客户端接入网络并与所述3A认证服务端进行通讯
S302
判断所述接入认证请求是否与所述认证网络管理端中预先储存的验证信息匹配；当判断所述接入认证请求与所述认证网络管理端中预先储存的验证信息匹配时，与所述接入认证客户端建立连接，并向所述接入认证客户端返回匹配成功信息
S304

图3

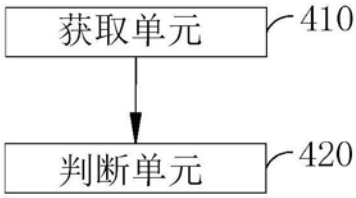

获取单元
410
判断单元
420

图4

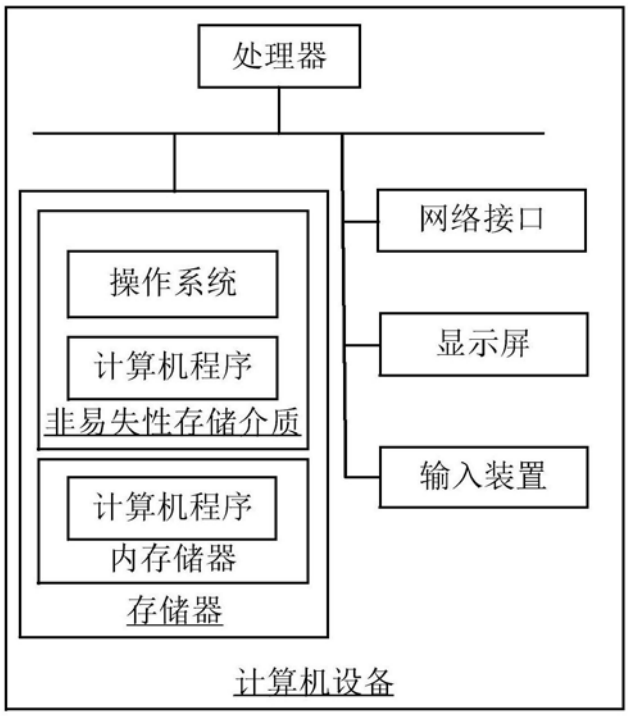

处理器
网络接口
操作系统
计算机程序
非易失性存储介质
显示屏
输入装置
计算机程序
内存储器
存储器
计算机设备

图5