

身份认证方法、系统及计算设备

本申请要求 2017 年 12 月 18 日递交的申请号为 201711366337.4、发明名称为“身份认证方法、系统及计算设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本申请涉及物联网领域，具体而言，涉及一种身份认证方法、系统及计算设备。

背景技术

10 随着信息技术的发展，物联网逐渐发展成集信息采集、传输、处理于一体的系统，被广泛运用于各行各业，可以缩短很多业务环节，减少机械劳动。在物联网系统中，由物联网边缘设备采集数据，发送给服务器进行运算处理分析，然后由服务器下发操作指令，由边缘设备执行。由于大量的原始数据，都需要传输到服务器进行分析和处理，对网络带宽和存储容量要求很高。同时给服务器带来了很大的处理负荷，容易出现延迟、
15 网络不稳定的现象。因而，将所有的物联网设备都接入互联网与服务器进行通信，是不现实的。边缘计算是在此基础上发展起来的一项技术，对于物联网而言，边缘计算将许多对设备的控制通过本地设备来实现，大大提升了处理效率，减轻了服务器的处理负荷。

目前，在物联网边缘计算中，有很多设备是无法和服务端通信，因而，无法通过服务端来操作这些设备，只能通过建立局域网环境来操作。例如，通过安装的客户端终端
20 与设备组件局域网来操作设备，这边需要对能操作设备的各个应用程序进行身份认证，才能保证物联网设备的安全以及功能的正常使用。当用户购买回某个物联网设备后，只需要下载相关的客户端程序，就控制该设备，例如，用户在家中安装用于监控家中情况的摄像头后，可以通过手机下载该摄像头的控制应用程序，即可看家中的情况。但是，这种方式，容易被非法者通过破解得到的 IP 地址连接上用户家中的摄像头，便可查看
25 用户家中的情况。由此，为了保证物联网设备的安全，并不是每个能连上该设备的客户端都具有对该设备进行操作的权限的。而由于物联网边缘的设备，不具有联网条件，在没有上网能力的情况下，无法实现对用于操作该设备的客户端进行认证，存在安全隐患。

针对上述现有技术中，在联网设备对非联网设备进行操作的过程中，由于非联网设备无法连接认证服务器，导致接入该非联网设备的联网设备无法完成身份认证的问题，
30 目前尚未提出有效的解决方案。

发明内容

本发明实施例提供了一种身份认证方法、系统及计算设备，以至少解决现有技术中，在联网设备对非联网设备进行操作的过程中，由于非联网设备无法连接认证服务器，导致接入该非联网设备的联网设备无法完成身份认证的技术问题。

根据本发明实施例的一个方面，提供了一种身份认证方法，包括：第一设备与第二设备建立通信连接，并通过互联网获取加密信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备；第一设备使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备；第一设备接收第二设备返回的验证结果，其中，第二设备基于验证信息来验证加密后的身份信息。

根据本发明实施例的另一方面，还提供了一种身份认证方法，包括：第二设备与第一设备建立通信连接，并接收第一设备传输的待验证的身份信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备；第二设备基于验证信息来验证第一设备传输的待验证的身份信息，得到验证结果；其中，待验证的身份信息为使用加密信息加密后的数据。

根据本发明实施例的另一方面，还提供了一种身份认证方法，包括：第二设备接收来自第一设备传输的待验证的身份信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备；第二设备根据验证信息验证待验证的身份信息，得到验证结果；在验证结果为身份信息可信的情况下，生成用于加解密数据的共享密钥，其中，共享密钥用于保证第一设备和第二设备之间进行安全数据传输；其中，待验证的身份信息为使用加密信息加密后的数据。

根据本发明实施例的另一方面，还提供了一种身份认证系统，包括：第一设备，用于通过互联网获取加密信息，使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备；第二设备，与第一设备建立通信连接，用于基于验证信息来验证加密后的身份信息，得到验证结果，并将验证结果返回至第一设备；其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备。

根据本发明实施例的另一方面，还提供了计算设备，包括：通信装置，与控制设备建立通信连接，用于接收来自控制设备传输的待验证的身份信息，其中，控制设备为允许访问互联网的设备；处理器，与通信装置连接，用于根据验证信息，验证控制设备传输的待验证的身份信息，得到验证结果，并在验证结果为身份信息可信的情况下，生成

用于加解密数据的共享密钥，其中，共享密钥用于保证通信装置和控制设备之间进行安全数据传输。

根据本发明实施例的另一方面，还提供了一种存储介质，存储介质包括存储的程序，其中，在程序运行时控制存储介质所在设备执行上述任意一项的身份认证方法。

5 根据本发明实施例的另一方面，还提供了一种计算终端，包括：处理器，处理器用于运行程序，其中，程序运行时执行上述任意一项的身份认证方法。

根据本发明实施例的另一方面，还提供了一种身份认证系统，包括：处理器；以及存储器，与处理器连接，用于为处理器提供处理以下处理步骤的指令：第一设备与第二设备建立通信连接，并通过互联网获取加密信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备；第一设备使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备；第一设备接收第二设备返回的验证结果，其中，第二设备基于验证信息来验证加密后的身份信息。

10

在本发明实施例中，通过第一设备与第二设备建立通信连接，并通过互联网获取加密信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备；第一设备使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备；第一设备接收第二设备返回的验证结果，其中，第二设备基于验证信息来验证加密后的身份信息，达到了根据非联网设备中内置的验证信息对用于操作该非联网设备的对象的身份信息进行验证的目的，从而实现了在通过客户端操作非联网设备的时候，非联网设备对客户端身份进行认证以提高客户端与非联网设备之间数据传输的安全性的技术效果，进而解决了现有技术中，在联网设备对非联网设备进行操作的

15

20

过程中，由于非联网设备无法连接认证服务器，导致接入该非联网设备的联网设备无法完成身份认证的技术问题。

附图说明

25 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：

图 1 是根据本申请实施例 1 的一种可选的身份认证系统示意图；

图 2 是根据本申请实施例 1 的一种可选的身份认证系统交互示意图；

图 3 是根据本申请实施例 2 的一种身份认证方法流程图；

30 图 4 是根据本申请实施例 2 的一种可选的身份认证方法流程图；

图 5 是根据本申请实施例 2 的一种可选的身份认证方法流程图；

图 6 是根据本申请实施例 2 的一种可选的身份认证方法流程图；

图 7 是根据本申请实施例 2 的一种可选的身份认证方法流程图；

图 8 是根据本申请实施例 3 的一种身份认证方法流程图；

5 图 9 是根据本申请实施例 4 的一种身份认证方法流程图；

图 10 是根据本申请实施例 5 的一种计算设备示意图；

图 11 是根据本申请实施例 6 的一种身份认证装置示意图；以及

图 12 是根据本申请实施例 7 的一种计算机终端的硬件结构框图。

10 具体实施方式

为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请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申请一部分的实施例，而不是全部的实施例。基于本申请中的实施例，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，都应当属于本申请保
15 护的范围。

需要说明的是，本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变
20 形，意图在于覆盖不排除他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

首先，在对本申请实施例进行描述的过程中出现的部分名词或术语适用于如下解释：

25 物联网，是指通过各种信息传感设备，实时采集任何需要监控、连接、互动的物体或过程等各种需要的信息，与互联网那个结合形成的一个巨大的网络。

边缘计算，是指在靠近物或数据源头的一侧，采用网络、计算、存储、应用核心能力为一体的开放平台，提供最近端服务。其应用程序在边缘侧发起，产生更快的网络服务响应，满足实时业务、应用智能、安全与隐私保护等方面的基本要求。物联网边缘计
30 算实现了将许多对物联网设备的控制通过本地设备实现，从而减轻了服务端的处理负

荷、提升了处理效率。

第一设备，可以是与互联网连接的设备，可以访问互联网，包括但不限于物联网边缘计算中，安装有用于对各种物联网基础设备进行控制或操作的应用程序的设备。

第二设备，可以是非联网设备，即没有连接互联网的设备，作为一种可选的实施例，
5 可以是物联网边缘计算中的没有连接互联网的各种物联网基础设备。

实施例 1

根据本申请实施例，提供了一种身份认证系统实施例，可以应用于对任何一种非联网设备的操作对象的身份认证。

作为一种可选的实施例，本实施例可以应用于物联网边缘计算中对物联网边缘设备进行操作的客户端或基于 Web 的应用中，其中，客户端或基于 Web 的应用安装于联网设备（包括但不限于手机、笔记本电脑、平板电脑、计算机等）上，联网设备可以与服务端进行通信。
10

由于在物联网边缘计算中，很多物联网基础设备（例如，智能灯、智能空调等）是无法和服务端进行通信的，而是通过联网设备（例如，手机）上安装的客户端应用程序或者通过基于 Web 的物联网应用来对物联网基础设备进行操作。
15

在通过联网设备上安装的客户端应用或基于 Web 的应用访问物联网基础设备并对物联网基础设备进行操作的时候，现有技术中，第一种方式是通过这些客户应用或基于 Web 的应用直接登录来对物联网基础设备进行操作，物联网基础设备不对访问或操作该物联网基础设备的应用进行身份认证，且传输的数据为明文传输，安全性很低；第二种方式
20 是由这些物联网基础设备直接访问服务端，由服务端下发可信任列表，当客户应用或基于 Web 的应用连接到物联网基础设备上，由设备判断当前的应用是否在可信任列表中，进而确定提供服务还是拒绝服务。

由上可以看出，上述第一种方式，在不对应用进行身份认证的情况下，直接通过应用对物联网基础设备进行操作，存在安全隐患；上述第二种方式，由设备与服务端通信，大量的设备容易导致服务端处理负荷增大。
25

在上述背景下，发明人经研究发现，如果可以提供一种身份认证方案，应用于没有连接互联网（即无法与服务端通信）的设备，对操作该设备的对象的身份进行认证，不仅实现了对操作非联网设备的应用进行身份认证以提高安全性，而且还不会增加服务端的处理负荷。

30 作为一种可选的实施例，图 1 是根据本申请实施例的一种可选的身份认证系统示意

图，如图 1 所示，该系统包括：第一设备 101 和第二设备 103。其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备。也就是说，第一设备可以与服务端通信，第二设备不可以与服务端通信。需要说明的是，第二设备不可以与服务端通信包括但不限于如下两种情形：（1）第二设备本身没有联网功能（例如，物联网边缘计算中的各种物联网基础设备），无法与服务端通信；（2）第二设备具有联网功能，但是没有访问服务端的权限（例如，为了防止大量设备访问服务端造成服务处理负荷过大的问题，而限制某些设备不允许访问服务端）。

其中，第一设备 101，用于通过互联网获取加密信息，使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备。

具体地，第一设备可以是任意一种能够访问互联网的终端设备，包括但不限于手机、笔记本电脑、平板电脑、计算机等；第二设备可以是能够上网的设备，也可以是不能够上网设备，本申请实施例提供的身份认证方法主要应用于没有与互联网连接或者无法与服务端通信第二设备，包括但不限于任意一种物联网边缘设备（或称基础设备）。加密信息可以是用于对第一设备向第二设备传输的身份信息进行加密的密钥信息。容易注意的是，采用的加密算法不同，获取到的加密信息也不同。

例如，在采用对称加密算法的情况下，上述加密信息可以是对身份信息进行加密的密钥，发送方（第一设备 101）利用该加密信息对身份信息加密，接收方（第二设备 103）利用该密钥对身份信息进行解密。在采用非对称加密算法的情况下，上述加密信息可以包括：对身份信息进行加密的私钥以及对加密后的身份信息进行解密的公钥，发送方（第一设备 101）利用该私钥对身份信息加密，接收方（第二设备 103）利用该私钥对应的公钥对身份信息进行解密。

需要说明的是，上述第一设备上安装的应用包括但不限于如下任意一种操作系统的上应用：Windows、iOS、Android 等。第一设备上安装的应用可以是客户端应用程序，也可是需要通过第一设备上安装的浏览器来访问的一些基于 Web 的应用。用户可以通过第一设备安装的这些应用操作第二设备。

第二设备 103，与第一设备建立通信连接，用于基于验证信息来验证加密后的身份信息，得到验证结果，并将验证结果返回至第一设备。

具体地，由于第二设备是没有连接互联网的，或者说是无法与对应的服务端进行通信的，为了实现对操作第二设备的对象的身份进行认证，因而，作为一种可选的实施例，可以在第二设备出厂时可以内置一些用于对操作对象的身份进行验证的信息，以便当第

一设备与第二设备建立通信连接后，第二设备可以通过内置的验证信息对操作第二设备的第一设备的身份信息进行验证。

一种可选的实施例中，上述验证信息可以是服务端证书签证的平台的根证书，该证书签证平台可以是用于服务端向第一设备签发数字证书的平台。

5 可选地，第一设备 101 可以通过如下任意一种通信方式与第二设备 103 建立通信连接：传输控制协议 TCP、用户数据报协议 UDP、蓝牙、Zigbee、WiFi。

作为一种可选的实施例，如图 1 所示，上述系统还可以包括：服务器 105，与第一设备 101 通信，该服务器 105 接收第一设备 101 发起的登录请求，并根据登录请求生成加密信息，其中，加密信息包括如下至少之一：密钥对和数字证书。其中，密钥对包括：
10 私钥和公钥，用于对第一设备向第二设备传输的身份信息进行非对称加密，即第一设备利用私钥对传输至第一设备的身份信息进行加密，第二设备利用与该私钥对应的公钥对接收到的加密后的身份信息进行解密。可选地，上述数字证书可以用于对公钥进行传输。

图 2 是根据本申请实施例的一种可选的身份认证系统交互示意图，如图 2 所示，第一设备 101、第二设备 103 和服务器 105 之间的交互过程如下：

15 （1）第一设备 101 获取登录账号，通过该登录账号向服务器 105 发出登录请求。
 （2）服务器 105 根据第一设备的登录请求生成对应的加密信息，其中，加密信息包括如下至少之一：密钥对和数字证书。

需要说明的是，服务器 105 至少可以根据登录请求中第一设备的登录账号生成对应的加密信息，作为一种可选的实施例，服务器 105 还可以根据登录请求中第一设备的登录账号生成一个与该登录账号对应的使用者账号（也称使用账号，作为第一设备使用第
20 二设备的账号），以及对应的加密信息。可选地，服务器 105 还可以针对不同的使用者账号授予不同的使用权限。

容易注意的是，由于使用者账号与登录账号是一一对应的，因而，可以直接采用第一设备的登录账号作为操作或使用第二设备的账号，也可以生成一个专门的使用者账号，本申请对此不作限定，只要可以用于标识第一设备的身份信息，均属于本申请保护的
25 范围。

 （3）第一设备 101 接收到服务器 105 返回的加密信息后，根据登录账号和加密信息，生成加密后的身份信息。

具体地，第一设备 101 可以使用密钥对中的私钥对登录账号和/或随机数进行加密，
30 得到加密结果，并基于登录账号，以及如下至少之一的信息生成加密后的身份信息：加

密结果和数字证书。包括但不限于如下三种实施方式：

第一种可选的实施方式，第一设备 101 使用服务器 105 返回的密钥对中的私钥对登录账号进行加密，得到加密结果，并基于加密结果和数字证书生成加密后的身份信息。其中，数字证书可以用于传输该私钥对应的公钥。

5 第二种可选的实施方式，第一设备 101 使用服务器 105 返回的密钥对中的私钥对登录账号和随机数（假设为第一随机数）进行加密，得到加密结果，并基于加密结果和数字证书生成加密后的身份信息。其中，数字证书可以用于传输该私钥对应的公钥。

第三种可选的实施方式，第一设备 101 使用服务器 105 返回的密钥对中的私钥对随机数（假设为第一随机数）进行加密，得到加密结果，并基于第一设备的登录账号、加密结果和数字证书生成加密后的身份信息。其中，数字证书可以用于传输该私钥对应的公钥。

（4）第一设备 101 将加密后的身份信息发送至第二设备 103。

可选地，在通过（3）中任意一种可选的实施方式，生成加密后的身份信息后，还可以将生成的加密后的身份信息添加第一设备的数字签名，并将添加数字签名后的身份信息发送至第二设备 103。

（5）第一设备 101 接收到来自第一设备 101 发送的加密后的身份信息后，对加密的身份信息进行解密。

具体地，在第一设备 101 对加密的身份信息进行解密的时候，首先可以基于预先安装的根证书，判断待验证的身份信息中包含的数字证书是否可信，并在数字证书不可信的情况下，向第一设备 101 返回的身份验证失败的结果。

进一步地，在数字证书可信的情况下，第二设备 103 提取数字证书中包含的公钥，并通过数字签名验证接收到的数据是否被篡改，在接收到的数据被篡改的情况下，第一设备接收第二设备返回的身份验证失败的结果。

进一步地，在接收到的数据未被篡改的情况下，第二设备 103 利用从数字证书中提取到的公钥对加密结果进行解密，得到登录账号和/或随机数（即第一随机数），并判断登录账号是否存在于可信任列表中，其中，可信任列表包含允许登录第二设备的至少一个账户，在登录账号不存在于可信任列表的情况下，向第一设备返回身份验证失败的结果。

其中，在第二设备 103 判断登录账号是否存在于可信任列表中之前，还可以判断可信任列表中是否存在登录账号，并在可信任列表中不存在登录账号的情况下，第二设备

将解密得到的登录账号作为管理账号，并添加到可信任列表中，其中，管理账号用于管理可信任列表中的至少一个登录账号。

可选地，在登录账号存在于可信任列表的情况下，第二设备 103 生成随机数（即第二随机数据），并根据第一随机数和第二随机数，生成共享密钥，共享密钥用于保证后续第一设备和第二设备之间进行安全数据传输。

（6）第一设备 101 根据第一随机数和服务器返回的第二随机数，生成用于保证后续第一设备和第二设备之间进行安全数据传输共享密钥。

实施例 2

根据本申请实施例，还提供了一种身份认证方法实施例，本实施例可以应用于实施例 1 中的身份认证系统中，包括但不限于实施例 1 中场景。需要说明的是，在附图的流程图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。

由于在通过客户终端对设备进行操作的过程中，在设备没有联网（即无法与服务端进行通信）的情况下，存在已经联网的客户终端无法在设备上完成身份认证的技术问题。

为了解决上述问题，本申请提供了一种身份认证方法实施例，图 3 是根据本申请实施例的一种身份认证方法流程图，如图 3 所示，包括如下步骤：

步骤 S302，第一设备与第二设备建立通信连接，并通过互联网获取加密信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备。

具体地，上述加密信息可以是用于对第一设备向第二设备传输的身份信息进行加密的密钥信息。其中，第一设备可以是任意一种能够访问互联网的终端设备，包括但不限于手机、笔记本电脑、平板电脑、计算机等；第二设备可以是能够上网的设备，也可以是不能够上网设备，本申请实施例提供的身份认证方法主要应用于没有与互联网连接或者无法与服务端通信第二设备，包括但不限于任意一种物联网边缘设备（或称基础设备）。

可选地，上述第一设备上安装的应用包括但不限于如下任意一种操作系统的上应用：Windows、iOS、Android 等。第一设备上安装的应用可以是客户端应用程序，也可能是需要通过第一设备上安装的浏览器来访问的一些基于 Web 的应用。用户可以通过第一设备安装的这些应用操作第二设备。

一种可选的实施例中，第一设备可以通过如下任意一种通信方式与第二设备建立通

信连接：传输控制协议 TCP、用户数据报协议 UDP、蓝牙、Zigbee、WiFi。

容易注意的是，采用的加密算法不同，获取到的加密信息也不同。

作为第一种可选的实施方案，在采用对称加密算法的情况下，上述加密信息可以是对身份信息进行加密的密钥，第一设备利用该加密信息对身份信息加密，第二设备利用该密钥对身份信息进行解密。

作为第二种可选的实施方案，在采用非对称加密算法的情况下，上述加密信息可以包括：对身份信息进行加密的私钥以及对加密后的身份信息进行解密的公钥，第一设备利用该私钥对身份信息加密，第二设备利用该私钥对应的公钥对身份信息进行解密。

步骤 S304，第一设备使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备。

具体地，在第一设备与第二设备建立通信连接，并从互联网上获取到对应的加密信息，可以使用该加密信息对第一设备登录第二设备的账户的身份信息进行加密，加密方式包括但不限于如下三种：①第一设备使用加密信息对第一设备的身份信息进行加密，得到加密后的身份信息；②第一设备使用加密信息对第一设备的身份信息和第一设备生成的随机数进行加密，得到加密后的身份信息；③第一设备基于第一设备的身份信息，并使用加密信息对和第一设备生成的随机数进行加密，得到加密后的身份信息。

步骤 S306，第一设备接收第二设备返回的验证结果，其中，第二设备基于验证信息来验证加密后的身份信息。

具体地，由于第二设备是没有连接互联网的，或者说是无法与对应的服务端进行通信的，为了实现对操作第二设备的对象的身份进行认证，因而，作为一种可选的实施例，可以在第二设备出厂时可以内置一些用于对操作对象的身份进行验证的信息，以便当第一设备与第二设备建立通信连接后，第二设备根据内置的验证信息对接收到的来自第一设备发送的身份信息进行验证，并将验证结果返回到第一设备。

作为一种可选的实施例，上述验证信息可以是服务端证书签平台的根证书，该证书签平台可以是用于服务端向第一设备签发数字证书的平台。

由上可知，在本申请上述实施例中，通过允许访问互联网的第一设备从互联网上获取加密信息，并使用该加密信息加密第一设备登录第二设备的账户的身份信息，以便第二设备可以通过验证信息，对接收到的身份信息进行验证，以便在确定第一设备的身份信息为可信的情况下，才与第一设备进行通信。

容易注意的是，第二设备中验证信息可以对第一设备获取到的加密信息进行验证，

以根据验证结果，来确定第一设备的身份是否可信。因而，通过本申请上述实施例公开的方案，达到了根据非联网设备中内置的验证信息对用于操作该非联网设备的对象的身份信息进行验证的目的，从而实现了在通过客户端操作非联网设备的时候，非联网设备对客户端身份进行认证以提高客户端与非联网设备之间数据传输的安全性的技术效果。

- 5 由此，本申请提供的上述实施例 2 的方案解决了现有技术中，在联网设备对非联网设备进行操作的过程中，由于非联网设备无法连接认证服务器，导致接入该非联网设备的联网设备无法完成身份认证的技术问题。

在一种可选的实施例中，如图 4 所示，上述步骤 S304，第一设备使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备，包括：

- 10 步骤 S402，第一设备获取登录账号，并接收认证服务器返回的加密信息，其中，加密信息包括如下至少之一：密钥对和数字证书。

- 具体地，认证服务器可以是用于认证对第二设备进行操作的对象的服务器，例如，当第二设备为物联网基础设备（例如，智能灯、智能空调等）的情况下，该认证服务器可以是提供应用服务的服务器，第一设备可以通过安装对应的应用程序来操作第二设备。由于第二设备无法与认证服务器进行通信，为了验证操作第二设备的第一设备的身份信息是否为可信的，能够与服务端（即认证服务器）通信的第一设备可以根据当前注册或已注册该应用的一个账号登录认证服务器，以便认证服务器生成对应的加密信息，用于第一设备加密第一设备向第二设备发送的身份信息。
- 15

- 需要说明的是，加密信息中的密钥对包括：私钥和公钥，用于对第一设备向第二设备传输的身份信息进行非对称加密，即第一设备利用私钥对传输至第一设备的身份信息进行加密，第二设备利用与该私钥对应的公钥对接收到的加密后的身份信息进行解密。可选地，上述数字证书可以用于对公钥进行传输。
- 20

- 容易注意的是，上述登录账号用于表征第一设备登录第二设备的账户的身份信息，可以是第一设备登录认证服务器的账号，也可以是认证服务器根据第一设备登录认证服务器的账号生成的一个对应的使用者账号（也称使用账号，作为第一设备使用第二设备的账号）。
- 25

由于使用者账号与登录账号是一一对应的，因而，可以直接采用第一设备的登录账号作为操作或使用第二设备的账号，也可以生成一个专门的使用者账号，本申请对此不作限定，只要可以用于标识第一设备的身份信息，均属于本申请保护的范围。

- 30 步骤 S404，第一设备根据登录账号和加密信息，生成加密后的身份信息。

具体地，在第一设备根据登录账号和加密信息，生成加密后的身份信息的过程中，可以通过如下任意一种方式来生成加密后的身份信息：①第一设备使用加密信息对登录账号进行加密，得到加密后的身份信息；②第一设备使用加密信息对登录账号和第一设备生成的随机数进行加密，得到加密后的身份信息；③第一设备基于登录账号，并使用加密信息对和第一设备生成的随机数进行加密，得到加密后的身份信息。

作为一种可选的实施方案，在采用非对称加密算法对身份信息进行加密的情况下，获取到的密钥对的中私钥来进行加密，则上述步骤 S404 可以包括：步骤 S4041，第一设备使用密钥对中的私钥对登录账号和/或随机数进行加密，得到加密结果；步骤 S4043，第一设备基于登录账号，以及如下至少之一的信息生成加密后的身份信息：加密结果和数字证书。

以上述第二种方式为例，上述步骤 S4041，第一设备使用密钥对中的私钥对登录账号和/或随机数进行加密，得到加密结果，可以包括如下步骤：步骤 S4041a，第一设备获取第一随机数；步骤 S4041b，第一设备使用密钥对中的私钥对登录账号和第一随机数进行加密，得到加密结果。

容易注意的是，本申请中根据第一设备的登录账号来获取特定的密钥对和数字证书，具体实施可以没有账号，以别的介质来获取密钥对的证书，均属于本申请保护范围。

步骤 S406，第一设备发送加密后的身份信息至第二设备。

具体地，第一设备在根据获取到的据登录账号和加密信息，生成加密后的身份信息后，可以将生成的加密后的身份信息添加第一设备的数字签名，并将添加数字签名后的身份信息发送至第二设备。

通过上述步骤 S402 至 S406 公开的方案，实现对待验证的身份信息进行加密传输的目的。

在一种可选的实施例，在第一设备使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备之前，上述方法还可以包括：步骤 S303，第一设备向认证服务器发起登录请求，其中，认证服务器根据登录请求生成加密信息，其中，加密信息包括如下至少之一：密钥对和数字证书。其中，密钥对包括：私钥和公钥，用于对第一设备向第二设备传输的身份信息进行非对称加密，即第一设备利用私钥对传输至第一设备的身份信息进行加密，第二设备利用与该私钥对应的公钥对接收到的加密后的身份信息进行解密。可选地，上述数字证书可以用于对公钥进行传输。

需要说明的是，为了确保第二设备接收到来自第一设备的数据没有被篡改，第一设

备在向第二设备发送加密后的身份信息时，可以添加第一设备的数字签名，并将添加数字签名后的身份信息发送至第二设备。因而，作为一种可选的实施例，如图 5 所示，第一设备发送加密后的身份信息至第二设备，可以包括如下步骤：

步骤 S502，第一设备将加密后的身份信息添加第一设备的数字签名；

5 步骤 S504，第一设备将添加数字签名后的身份信息发送至第二设备。

通过上述步骤 S502 至 S504 公开的方案，可以使得第二设备在接收到第一设备发送的身份信息后，根据数字签名协议验证内容是否被篡改。

基于上述实施例，作为一种可选的实施方式，如图 6 所示，在第一设备将添加数字签名后的身份信息发送至第二设备之后，上述方法还可以包括如下步骤：

10 步骤 S602，第二设备基于预先安装的根证书，判断待验证的身份信息中包含的数字证书是否可信。

具体地，第二设备中的根证书可以是服务端证书签发平台的根证书，该证书签发平台可以是用于服务端向第一设备签发数字证书的平台。通过证书签发平台的根证书可以验证该证书签发平台（即认证服务器）向第一设备返回的数字证书是否可信。

15 步骤 S604，在数字证书不可信的情况下，第一设备接收第二设备返回的身份验证失败的结果。

具体地，在根据第二设备中预先安装的根证书，确定第一设备发送的待验证的身份信息不可信的情况下，第二设备可以返回身份验证失败的结果。

可选地，在数字证书可信的情况下，上述方法还可以包括如下步骤：

20 步骤 S606，第二设备提取数字证书中包含的公钥，并通过数字签名验证接收到的数据是否被篡改；

步骤 S608，在接收到的数据被篡改的情况下，第一设备接收第二设备返回的身份验证失败的结果。

25 由于第二设备接收到来自第一设备发送的待验证的身份信息是采用密钥对的中私钥进行加密的，因而，在根据第二设备中安装的根证书确定接收到的数字证书可信的情况下，可以通过接收到的数字证书中包含的公钥对待验证的身份信息进行解密，为了避免不必要的操作，可以首先根据接收到的数据中包含的第一设备的数字签名来验证接收到数据内容是否被篡改，在篡改的情况下，返回身份验证失败的结果。

可选地，在接收到的数据未被篡改的情况下，上述方法还可以包括如下步骤：

30 步骤 S610，第二设备利用公钥对加密结果进行解密，得到登录账号和/或第一随机

数。

在根据接收到的数字签名根据数字签名协议验证第二设备接收到身份信息内容没有被篡改的情况下，可以根据从数字证书中提取到的公钥对采用私钥加密的身份信息进行解密，得到第一设备的身份信息（例如，登录账号），以及第一设备生产的随机数（即第一随机数）。

步骤 S612，第二设备判断登录账号是否存在于可信任列表中，其中，可信任列表包含允许登录第二设备的至少一个账户。

具体地，上述可信任列表中存储了至少一个可信的账户的身份信息（例如，登录账号，或者，根据登录账号生产的使用者账号）。

10 可选地，在判断登录账号是否存在于可信任列表中之前，上述方法还可以包括如下步骤：步骤 S611a，第二设备判断可信任列表中是否存在登录账号；步骤 S611b，在可信任列表中不存在登录账号的情况下，第二设备将解密得到的登录账号作为管理账号，并添加到可信任列表中，其中，管理账号用于管理可信任列表中的至少一个登录账号。

通过上述步骤 S611a 和 S611b，将第一设备首次传输到第二设备的身份信息（例如，15 登录账号，或者，根据登录账号生产的使用者账号）作为管理员账号，并添加到可信任账号列表中，其中，管理员账号对应的账户可以删除或增加可信任列表中的其他账号，从而解决了需要将第二设备连接到服务器来获取可信任列表，从而到至服务器处理负荷过高的问题。

步骤 S614，在登录账号不存在于可信任列表的情况下，第一设备接收第二设备返回20 的身份验证失败的结果。如果解密得到的登录账号不在可信任列表中，说明该登录账号不可信，因而，可以向第一设备返回身份验证失败的结果，并终止第一设备向第二设备的操作。

可选地，在登录账号存在于可信任列表的情况下，上述方法还可以包括如下步骤：

25 步骤 S616，第一设备根据第一随机数和认证服务器返回的第二随机数，生成共享密钥，其中，第二随机数为第二设备在登录账号存在于可信任列表的情况下，第二设备生成的随机数；其中，第二设备根据第一随机数和第二随机数，生成共享密钥。

在第二设备确定第一设备的身份为可信的情况下，根据生成第二随机数和第一设备生成的第一随机数，生成第一设备与第二设备之间传输数据的共享密钥，可以用于第一设备与第二设备后续进行安全数据传输。

30 作为一种可选的实施例，图 7 是根据本申请实施例的一种可选的身份认证方法流程

图，如图 7 所示，包括如下步骤：

(1) 客户端（即上述第一设备）登录账号。即用户通过客户端设备安装的客户端程序或基于 Web 的应用登录。

(2) 服务端返回登录账号对应的使用者账号、密钥对、数字证书。

5 具体地，服务端根据登录的账号生成使用者账号，密钥对，并对这个密钥通过授权平台签发一个数字证书。可选地，服务端可以将这些信息保存在数据中，以便下次该登录账号登录时，可以直接读取。

(3) 客户端与非联网设备（即上述第二设备）建立通信连接。可选地，客户端通过 TCP 或 UDP 连接非联网设备。

10 (4) 客户端将使用者账号、随机数（即第一随机数）利用私钥加密，发送给非联网设备，协议中包含数字证书和数字签名。

(5) 非联网设备根据根证书验证数字证书和签名。

具体地，非联网设备在接收到客户端传输来的数据后，解析出数字证书，并通过根证书验证收到的数字证书是否可信，如果数字证书不可信，则返回认证失败错误。如果
15 数字证书可信，则从数字证书中提取出公钥，通过数字签名协议验证协议内容是否被篡改过，如果内容被篡改过，则返回认证失败错误。

(6) 生成共享密钥。

如果内容未被篡改，非联网设备通过公钥解密出使用者账号和第一随机数，判断可信任列表是否空，如果可信任列表为空，则将该使用者账号作为管理员账号，并生成第
20 二随机数，与客户端的第一随机数据生成用于客户端与非联网设备之间安全数据传输的共享密钥。其中，客户端根据自己生成的第一随机数和服务端返回的第二随机数，生成用于客户端与非联网设备之间安全数据传输的共享密钥。

通过本申请上述实施例公开的方案，在第一设备与第二设备建立通信连接后，通过私钥加密传输的数据，数字证书传输公钥，非联网设备验证数字证书为可信后，通过从
25 数字证书中提取到的公钥解密数据，得到第一设备的身份信息，从而解决了非联网设备需要连接服务端来添加可信任账号的问题，一次通信便完成身份确认和共享密钥生成的目的。

实施例 3

根据本申请实施例，还提供了一种身份认证方法实施例，本实施例可以应用于实施
30 例 1 中的身份认证系统中，包括但不限于实施例 1 中场景。需要说明的是，在附图的流

程图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。

图 8 是根据本申请实施例的一种身份认证方法流程图，如图 8 所示，包括如下步骤：

- 5 步骤 S802，第二设备与第一设备建立通信连接，并接收第一设备传输的待验证的身份信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备。

需要说明的是，上述第二设备可以是能够上网的设备，也可以是不能够上网设备，本申请实施例提供的身份认证方法主要应用于没有与互联网连接或者无法与服务端通信第二设备，包括但不限于任意一种物联网边缘设备（或称基础设备）；上述待验证的身份信息为使用加密信息加密后的数据；第一设备可以是任意一种能够访问互联网的终端设备，包括但不限于手机、笔记本电脑、平板电脑、计算机等。

第二设备可以通过如下任意一种通信方式与第一设备建立通信连接：传输控制协议 TCP、用户数据报协议 UDP、蓝牙、Zigbee、WiFi。

- 15 步骤 S804，第二设备基于验证信息来验证第一设备传输的待验证的身份信息，得到验证结果。

具体地，上述验证信息可以是在第二设备出厂时可以内置一些用于对操作对象的身份进行验证的信息；由于第二设备是没有连接互联网的，或者说是无法与对应的服务端进行通信的，为了实现对操作第二设备的对象的身份进行认证，在第二设备出厂时可以
20 内置一些用于对操作对象的身份进行验证的信息，以便当第一设备与第二设备建立通信连接后，第二设备根据内置的验证信息对接收到的来自第一设备发送的身份信息进行验证，并将验证结果返回到第一设备。

一种可选的实施例中，上述验证信息可以是服务端证书签证平台的根证书，该证书签证平台可以是用于服务端向第一设备签发数字证书的平台。

- 25 由上可知，在本申请上述实施例中，不允许访问互联网的第二设备与允许访问互联网的第一设备建立通信连接，并接收第一设备发送的待验证的身份信息，第二设备通过验证信息来第一设备的身份信息，以便在确定第一设备的身份信息为可信的情况下，才与第一设备进行通信。

容易注意的是，第一设备发送的待验证的身份信息是使用加密信息加密后的数据，
30 而第二设备中验证信息可以对第一设备获取到的加密信息进行验证，以根据验证结果，

来确定第一设备的身份是否可信。因而，通过本申请上述实施例公开的方案，达到了根据非联网设备中内置的验证信息对用于操作该非联网设备的对象的身份信息进行验证的目的，从而实现了在通过客户端操作非联网设备的时候，非联网设备对客户端身份进行认证以提高客户端与非联网设备之间数据传输的安全性的技术效果。

- 5 由此，本申请提供的上述实施例 3 的方案解决了现有技术中，在联网设备对非联网设备进行操作的过程中，由于非联网设备无法连接认证服务器，导致接入该非联网设备的联网设备无法完成身份认证的技术问题。

实施例 4

- 10 根据本申请实施例，还提供了一种身份认证方法实施例，本实施例可以应用于实施例 1 中的身份认证系统中，包括但不限于实施例 1 中场景。需要说明的是，在附图的流程图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。

图 9 是根据本申请实施例的一种身份认证方法流程图，如图 9 所示，包括如下步骤：

- 15 步骤 S902，第二设备接收来自第一设备传输的待验证的身份信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备。

- 具体地，上述第二设备可以是能够上网的设备，也可以是不能够上网设备，本申请实施例提供的身份认证方法主要应用于没有与互联网连接或者无法与服务端通信第二设备，包括但不限于任意一种物联网边缘设备（或称基础设备）；上述待验证的身份信息为使用加密信息加密后的数据；第一设备可以是任意一种能够访问互联网的终端设备，包括但不限于手机、笔记本电脑、平板电脑、计算机等。
- 20

步骤 S904，第二设备根据验证信息验证待验证的身份信息，得到验证结果。

- 其中，验证信息可以是在第二设备出厂时可以内置一些用于对操作对象的身份进行验证的信息；一种可选的实施例中，该验证信息可以是服务端证书签证平台的根证书，该证书签证平台可以是用于服务端向第一设备签发数字证书的平台。
- 25

步骤 S906，在验证结果为身份信息可信的情况下，生成用于加解密数据的共享密钥，其中，共享密钥用于保证第一设备和第二设备之间进行安全数据传输。

具体地，共享密钥可以用于第一设备与第二设备后续进行安全数据传输的密钥信息。

- 30 由上可知，在本申请上述实施例中，不允许访问互联网的第二设备与允许访问互联

网的第一设备建立通信连接，并接收第一设备发送的待验证的身份信息，第二设备通过验证信息来第一设备的身份信息是否可信，并在确定第一设备的身份信息为可信的情况下，生成用于第一设备与第二设备之间进行通信的共享密钥。

容易注意的是，第一设备发送的待验证的身份信息是使用加密信息加密后的数据，而第二设备中验证信息可以对第一设备获取到的加密信息进行验证，以根据验证结果，来确定第一设备的身份是否可信。因而，通过本申请上述实施例公开的方案，达到了根据非联网设备中内置的验证信息对用于操作该非联网设备的对象的身份信息进行验证，并在身份可信的情况下，生成用于安全数据传输的共享密钥的目的，从而实现了在通过客户端操作非联网设备的时候，非联网设备对客户端身份进行认证以提高客户端与非联网设备之间数据传输的安全性的技术效果。

由此，本申请提供的上述实施例 4 的方案解决了现有技术中，在联网设备对非联网设备进行操作的过程中，由于非联网设备无法连接认证服务器，导致接入该非联网设备的联网设备无法完成身份认证的技术问题。

在一种可选的实施例中，在第二设备接收来自第一设备传输的待验证的身份信息之前，上述方法还包括：第一设备获取登录账号，并接收认证服务器返回的加密信息，其中，加密信息包括如下至少之一：密钥对和数字证书；第一设备根据登录账号和加密信息，生成待验证的身份信息；第一设备发送待验证的身份信息至第二设备。

在一种可选的实施例中，第二设备通过如下任意一种通信方式接收第一设备发送的待验证的身份信息：传输控制协议 TCP、用户数据报协议 UDP、蓝牙、Zigbee、WiFi。

在一种可选的实施例中，在第一设备获取登录账号，并接收服务器返回的认证服务器返回的加密信息之前，上述方法还包括：第一设备向认证服务器发起登录请求，其中，认证服务器根据登录请求生成加密信息。

在一种可选的实施例中，第一设备根据登录账号和加密信息，生成待验证的身份信息，包括：第一设备使用密钥对中的私钥对登录账号和/或随机数进行加密，得到加密结果；第一设备基于登录账号，以及如下至少之一的信息生成待验证的身份信息：加密结果和数字证书。

在一种可选的实施例中，第一设备使用密钥对中的私钥对登录账号和/或随机数进行加密，得到加密结果，包括：第一设备获取第一随机数；第一设备使用密钥对中的私钥对登录账号和第一随机数进行加密，得到加密结果。

在一种可选的实施例中，第一设备发送待验证的身份信息至第二设备，可以包括：

第一设备将待验证的身份信息添加第一设备的数字签名；第一设备将添加数字签名后的身份信息发送至第二设备。

在一种可选的实施例中，第二设备根据验证信息验证第一设备传输的待验证的身份信息，得到验证结果，可以包括：第二设备基于预先安装的根证书，判断待验证的身份信息中包含的数字证书是否可信；在数字证书不可信的情况下，第二设备向第一设备返回身份验证失败的结果。

可选地，在数字证书可信的情况下，上述方法还包括：在数字证书可信的情况下，第二设备提取数字证书中包含的公钥，并通过数字签名验证接收到的数据是否被篡改；在接收到的数据被篡改的情况下，第二设备向第一设备返回身份验证失败的结果。

可选地，在接收到的数据未被篡改的情况下，上述方法还包括：第二设备利用公钥对加密结果进行解密，得到登录账号和/或第一随机数；第二设备判断登录账号是否存在于可信任列表中，其中，可信任列表包含允许登录第二设备的至少一个账户；在登录账号不存在于可信任列表的情况下，第二设备向第一设备返回身份验证失败的结果。

可选地，在登录账号存在于可信任列表的情况下，第二设备确定第一设备传输的身份信息为可信的验证结果。

可选地，在登录账号存在于可信任列表的情况下，第二设备确定第一设备传输的身份信息为可信的验证结果之后，上述方法还包括：第二设备获取第二随机数，并根据第一随机数和第二随机数生成共享密钥；其中，第一设备根据第一随机数和认证服务器返回的第二随机数，生成共享密钥。

作为一种可选的实施例，在第二设备利用公钥对加密结果进行解密，得到登录账号和/或第一随机数之后，上述方法还包括：第二设备判断可信任列表中是否存在登录账号；在可信任列表中不存在登录账号的情况下，第二设备将解密得到的登录账号作为管理账号，并添加到可信任列表中，其中，管理账号用于管理可信任列表中的至少一个登录账号。

需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请并不受所描述的动作顺序的限制，因为依据本申请，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本申请所必须的。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例

的身份认证方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端

5 设备（可以是手机，计算机，服务器，或者网络设备等）执行本申请各个实施例所述的方法。

实施例 5

根据本申请实施例，还提供了一种用于实现上述身份认证方法的计算设备实施例，图 10 是根据本申请实施例的一种计算设备示意图，如图 10 所示，该计算设备 10 包括：

10 通信装置 1001 和处理器 1003。

其中，通信装置 1001，与控制设备建立通信连接，用于接收来自控制设备传输的待验证的身份信息，其中，控制设备为允许访问互联网的设备；

处理器 1003，与通信装置连接，用于根据验证信息，验证控制设备传输的待验证的身份信息，得到验证结果，并在验证结果为身份信息可信的情况下，生成用于加解密数据的共享密钥，其中，共享密钥用于保证通信装置和控制设备之间进行安全数据传输。

15 数据的共享密钥，其中，共享密钥用于保证通信装置和控制设备之间进行安全数据传输。

作为一种可选的实施例，上述计算设备可以是物联网边缘计算中的物联网基础设备（例如，智能灯、智能空调等），该计算设备无法和服务端进行通信的，而是通过联网设备（例如，手机）上安装的客户端应用程序或者通过基于 Web 的物联网应用来对物联网基础设备进行操作。上述控制设备可以是用于控制或操作计算设备的联网设备，控制

20 设备可以与服务端通信，并且控制设备通过安装的客户端应用或基于 Web 的应用操作上述计算设备，包括但不限于手机、笔记本电脑、平板电脑、计算机等。

计算设备 10 通过通信装置 1001 与控制设备通信，其通讯协议包括但不限于如下任意一种：传输控制协议 TCP、用户数据报协议 UDP、蓝牙、Zigbee、WiFi。

由上可知，在本申请上述实施例中，通过允许访问互联网的第一设备从互联网上获取加密信息，并使用该加密信息加密第一设备登录第二设备的账户的身份信息，以便第二设备可以通过验证信息，对接收到的身份信息进行验证，以便在确定第一设备的身份信息为可信的情况下，才与第一设备进行通信。

25 取加密信息，并使用该加密信息加密第一设备登录第二设备的账户的身份信息，以便第二设备可以通过验证信息，对接收到的身份信息进行验证，以便在确定第一设备的身份信息为可信的情况下，才与第一设备进行通信。

容易注意的是，第二设备中验证信息可以对第一设备获取到的加密信息进行验证，以根据验证结果，来确定第一设备的身份。因而，通过本申请上述实施例公开的方案，

30 达到了根据非联网设备中内置的验证信息对用于操作该非联网设备的对象的身份信息

进行验证的目的，从而实现了在通过客户端操作非联网设备的时候，非联网设备对客户端身份进行认证以提高客户端与非联网设备之间数据传输的安全性的技术效果。

由此，本申请提供的上述实施例 2 的方案解决了现有技术中，在联网设备对非联网设备进行操作的过程中，由于非联网设备无法连接认证服务器，导致接入该非联网设备的联网设备无法完成身份认证的技术问题。

实施例 6

根据本申请实施例，还提供了一种用于实现上述身份认证方法的装置实施例，图 11 是根据本申请实施例的一种身份认证装置示意图，如图 11 所示，该装置包括：获取单元 111、加密单元 113 和接收单元 115。

其中，获取单元 111，用于通过第一设备与第二设备建立通信连接，并通过互联网获取加密信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备；

加密单元 113，用于第一设备使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备；

接收单元 115，用于第一设备接收第二设备返回的验证结果，其中，第二设备基于验证信息来验证加密后的身份信息。

此处需要说明的是，上述获取单元 111、加密单元 113 和接收单元 115 对应于实施例 2 中的步骤 S302 至 S306，上述模块与对应的步骤所实现的示例和应用场景相同，但不限于上述实施例 2 所公开的内容。需要说明的是，上述模块作为装置的一部分可以在诸如一组计算机可执行指令的计算机系统中执行。

由上可知，在本申请上述实施例中，通过允许访问互联网的第一设备从互联网上获取加密信息，并使用该加密信息加密第一设备登录第二设备的账户的身份信息，以便第二设备可以通过验证信息，对接收到的身份信息进行验证，以便在确定第一设备的身份信息为可信的情况下，才与第一设备进行通信。

容易注意的是，第二设备中验证信息可以对第一设备获取到的加密信息进行验证，以根据验证结果，来确定第一设备的身份是否可信。因而，通过本申请上述实施例公开的方案，达到了根据非联网设备中内置的验证信息对用于操作该非联网设备的对象的身份信息进行验证的目的，从而实现了在通过客户端操作非联网设备的时候，非联网设备对客户端身份进行认证以提高客户端与非联网设备之间数据传输的安全性的技术效果。

由此，本申请提供的上述实施例 5 的方案解决了现有技术中，在联网设备对非联网

设备进行操作的过程中，由于非联网设备无法连接认证服务器，导致接入该非联网设备的联网设备无法完成身份认证的技术问题。

在一种可选的实施例中，加密单元包括：获取模块，用于通过第一设备获取登录账号，并接收认证服务器返回的加密信息，其中，加密信息包括如下至少之一：密钥对和数字证书；生成模块，用于通过第一设备根据登录账号和加密信息，生成加密后的身份信息；发送模块，用于通过第一设备发送加密后的身份信息至第二设备。

在一种可选的实施例中，生成模块包括：第一加密模块，用于通过第一设备使用密钥对中的私钥对登录账号和/或随机数进行加密，得到加密结果；第二加密模块，用于通过第一设备基于登录账号，以及如下至少之一的信息生成加密后的身份信息：加密结果和数字证书。

在一种可选的实施例中，第一加密模块还用于通过第一设备获取第一随机数，并通过第一设备使用密钥对中的私钥对登录账号和第一随机数进行加密，得到加密结果。

在一种可选的实施例中，上述装置还包括：发送单元，用于通过第一设备向认证服务器发起登录请求，其中，认证服务器根据登录请求生成加密信息，其中，加密信息包括如下至少之一：密钥对和数字证书。

在一种可选的实施例中，上述第一设备通过如下任意一种通信方式与第二设备建立通信连接：传输控制协议 TCP、用户数据报协议 UDP、蓝牙、Zigbee、WiFi。

在一种可选的实施例中，上述发送模块还用于通过第一设备将加密后的身份信息添加第一设备的数字签名，并通过第一设备将添加数字签名后的身份信息发送至第二设备。

在一种可选的实施例中，上述装置还包括：第一判断单元，用于通过第二设备基于预先安装的根证书，判断待验证的身份信息中包含的数字证书是否可信；其中，接收单元还用于在数字证书不可信的情况下，第一设备接收第二设备返回的身份验证失败的结果。

在一种可选的实施例中，在数字证书可信的情况下，上述装置还包括：提取单元，用于在数字证书可信的情况下，通过第二设备提取数字证书中包含的公钥，并通过数字签名验证接收到的数据是否被篡改；其中，接收单元还用于在接收到的数据被篡改的情况下，通过第一设备接收第二设备返回的身份验证失败的结果。

在一种可选的实施例中，在接收到的数据未被篡改的情况下，上述装置还包括：解密单元，用于通过第二设备利用公钥对加密结果进行解密，得到登录账号和/或第一随

机数；第二判断单元，用于通过第二设备判断登录账号是否存在于可信任列表中，其中，可信任列表包含允许登录第二设备的至少一个账户；其中，接收单元还用于在登录账号不存在于可信任列表的情况下，通过第一设备接收第二设备返回的身份验证失败的结果。

- 5 在一种可选的实施例中，在登录账号存在于可信任列表的情况下，上述装置还包括：生成单元，用于第一设备根据第一随机数和认证服务器返回的第二随机数，生成共享密钥，其中，第二随机数为第二设备在登录账号存在于可信任列表的情况下，第二设备生成的随机数；其中，第二设备根据第一随机数和第二随机数，生成共享密钥。

- 10 在一种可选的实施例中，上述装置包括：第三判断单元，用于通过第二设备判断可信任列表中是否存在登录账号；处理单元，用于在可信任列表中不存在登录账号的情况下，第二设备将解密得到的登录账号作为管理账号，并添加到可信任列表中，其中，管理账号用于管理可信任列表中的至少一个登录账号。

实施例 7

- 15 本申请的实施例可以提供一种计算机终端，该计算机终端可以是计算机终端群中的任意一个计算机终端。可选地，在本实施例中，上述计算机终端也可以替换为计算机终端等终端设备。

可选地，在本实施例中，上述计算机终端可以位于计算机网络的多个网络设备中的至少一个访问设备。

- 20 图 12 示出了一种计算机终端的硬件结构框图。如图 12 所示，计算机终端 12 可以包括一个或多个（图中仅示出一个）处理器 122（处理器 122 可以包括但不限于微处理器 MCU 或可编程逻辑器件 FPGA 等的处理装置）、用于存储数据的存储器 124、以及用于通信功能的传输装置 126。除此以外，还可以包括：显示器、输入/输出接口（I/O 接口）、通用串行总线（USB）端口（可以作为 I/O 接口的端口中的一个端口被包括）、网络接口、电源和/或相机。本领域普通技术人员可以理解，图 12 所示的结构仅为示意，其并不对上述电子装置的结构造成限定。例如，计算机终端 12 还可包括比图 12 中所示更多或者更少的组件，或者具有与图 12 所示不同的配置。

- 30 应当注意到的是上述一个或多个处理器 122 和/或其他数据处理电路在本文中通常可以被称为“数据处理电路”。该数据处理电路可以全部或部分的体现为软件、硬件、固件或其他任意组合。此外，数据处理电路可为单个独立的处理模块，或全部或部分的结合到计算机终端 12 中的其他元件中的任意一个内。如本申请实施例中所涉及到的，

该数据处理电路作为一种处理器控制（例如与接口连接的可变电阻终端路径的选择）。

处理器 122 可以通过传输装置调用存储器存储的信息及应用程序，以执行下述步骤：基于用户对订单的操作，生成会话交互界面，会话交互界面对应的会话是基于订单创建；在会话交互界面，实现针对订单的用户间即时通讯功能。

5 存储器 124 可用于存储应用程序的软件程序以及模块，如本申请实施例中的身份认证方法对应的程序指令/数据存储装置，处理器 122 通过运行存储在存储器 124 内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的应用程序的身份认证方法。存储器 124 可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器 124
10 可进一步包括相对于处理器 122 远程设置的存储器，这些远程存储器可以通过网络连接至计算机终端 12。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

传输装置 126 用于经由一个网络接收或者发送数据。上述的网络具体实例可包括计算机终端 12 的通信供应商提供的无线网络。在一个实例中，传输装置 126 包括一个网络
15 适配器（Network Interface Controller，NIC），其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中，传输装置 126 可以为射频（Radio Frequency，RF）模块，其用于通过无线方式与互联网进行通讯。

显示器可以例如触摸屏式的液晶显示器（LCD），该液晶显示器可使得用户能够与计算机终端 12 的用户界面进行交互。

20 此处需要说明的是，在一些可选实施例中，上述图 12 所示的计算机终端 12 可以包括硬件元件（包括电路）、软件元件（包括存储在计算机可读介质上的计算机代码）、或硬件元件和软件元件两者的结合。应当指出的是，图 12 仅为特定具体实例的一个实例，并且旨在示出可存在于上述计算机终端 12 中的部件的类型。

此处需要说明的是，在一些实施例中，上述图 12 所示的计算机终端具有触摸显示器（也被称为“触摸屏”或“触摸显示屏”）。在一些实施例中，上述图 12 所示的计算机终端具有图像用户界面（GUI），用户可以通过触摸触敏表面上的手指接触和/或手势来与 GUI 进行人机交互，此处的人机交互功能可选的包括如下交互：创建网页、绘图、文字处理、制作电子文档、游戏、视频会议、即时通信、收发电子邮件、通话界面、播放数字视频、播放数字音乐和/或网络浏览等、用于执行上述人机交互功能的可执行指令被配置/存储在一个或多个处理器可执行的计算机程序产品或可读存储介质中。
25
30

在本实施例中，上述计算机终端 12 可以执行应用程序的身份认证方法中以下步骤的程序代码：第一设备与第二设备建立通信连接，并通过互联网获取加密信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备；第一设备使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备；第一设备接收第二设备返回的验证结果，其中，第二设备基于验证信息来验证加密后的身份信息。

可选的，上述处理器还可以执行如下步骤的程序代码：第一设备与第二设备建立通信连接，并通过互联网获取加密信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备；第一设备使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备；第一设备接收第二设备返回的验证结果，其中，第二设备基于验证信息来验证加密后的身份信息。

可选的，上述处理器还可以执行如下步骤的程序代码：第一设备获取登录账号，并接收认证服务器返回的加密信息，其中，加密信息包括如下至少之一：密钥对和数字证书；第一设备根据登录账号和加密信息，生成加密后的身份信息；第一设备发送加密后的身份信息至第二设备。

可选的，上述处理器还可以执行如下步骤的程序代码：第一设备使用密钥对中的私钥对登录账号和/或随机数进行加密，得到加密结果；第一设备基于登录账号，以及如下至少之一的信息生成加密后的身份信息：加密结果和数字证书。

可选的，上述处理器还可以执行如下步骤的程序代码：第一设备获取第一随机数；第一设备使用密钥对中的私钥对登录账号和第一随机数进行加密，得到加密结果。

可选的，上述处理器还可以执行如下步骤的程序代码：第一设备向认证服务器发起登录请求，其中，认证服务器根据登录请求生成加密信息，其中，加密信息包括如下至少之一：密钥对和数字证书。

可选的，第一设备通过如下任意一种通信方式与第二设备建立通信连接：传输控制协议 TCP、用户数据报协议 UDP、蓝牙、Zigbee、WiFi。

可选的，上述处理器还可以执行如下步骤的程序代码：第一设备将加密后的身份信息添加第一设备的数字签名；第一设备将添加数字签名后的身份信息发送至第二设备。

可选的，上述处理器还可以执行如下步骤的程序代码：第二设备基于预先安装的根证书，判断待验证的身份信息中包含的数字证书是否可信；在数字证书不可信的情况下，第一设备接收第二设备返回的身份验证失败的结果。

可选的，在数字证书可信的情况下，上述处理器还可以执行如下步骤的程序代码：在数字证书可信的情况下，第二设备提取数字证书中包含的公钥，并通过数字签名验证接收到的数据是否被篡改；在接收到的数据被篡改的情况下，第一设备接收第二设备返回的身份验证失败的结果。

5 可选的，在接收到的数据未被篡改的情况下，上述处理器还可以执行如下步骤的程序代码：第二设备利用公钥对加密结果进行解密，得到登录账号和/或第一随机数；第二设备判断登录账号是否存在于可信任列表中，其中，可信任列表包含允许登录第二设备的至少一个账户；在登录账号不存在于可信任列表的情况下，第一设备接收第二设备返回的身份验证失败的结果。

10 可选的，在登录账号存在于可信任列表的情况下，上述处理器还可以执行如下步骤的程序代码：第一设备根据第一随机数和认证服务器返回的第二随机数，生成共享密钥，其中，第二随机数为第二设备在登录账号存在于可信任列表的情况下，第二设备生成的随机数；其中，第二设备根据第一随机数和第二随机数，生成共享密钥。

可选的，上述处理器还可以执行如下步骤的程序代码：第二设备判断可信任列表中
15 是否存在登录账号；在可信任列表中不存在登录账号的情况下，第二设备将解密得到的登录账号作为管理账号，并添加到可信任列表中，其中，管理账号用于管理可信任列表中的至少一个登录账号。

本领域普通技术人员可以理解，图 12 所示的结构仅为示意，计算机终端也可以是
20 智能手机（如 Android 手机、iOS 手机等）、平板电脑、掌上电脑以及移动互联网设备（Mobile Internet Devices, MID）、PAD 等终端设备。图 12 其并不对上述电子装置的结构造成限定。例如，计算机终端 12 还可包括比图 12 中所示更多或者更少的组件（如网络接口、显示装置等），或者具有与图 12 所示不同的配置。

本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以
25 通过程序来指令终端设备相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器（Read-Only Memory, ROM）、随机存取器（Random Access Memory, RAM）、磁盘或光盘等。

实施例 8

本申请的实施例还提供了一种存储介质。可选的，在本实施例中，上述存储介质可以
30 用于保存上述实施例所提供的身份认证方法所执行的程序代码，其中，在程序运行时控制存储介质所在设备执行实施例中任意一项的可选的或优选的订单处理方法。

可选的，在本实施例中，上述存储介质可以位于计算机网络中移动终端群中的任意一个移动终端中，或者位于移动终端群中的任意一个移动终端中。

可选的，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：第一设备与第二设备建立通信连接，并通过互联网获取加密信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备；第一设备使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备；第一设备接收第二设备返回的验证结果，其中，第二设备基于验证信息来验证加密后的身份信息。

可选的，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：第一设备获取登录账号，并接收认证服务器返回的加密信息，其中，加密信息包括如下至少之一：密钥对和数字证书；第一设备根据登录账号和加密信息，生成加密后的身份信息；第一设备发送加密后的身份信息至第二设备。

可选的，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：第一设备使用密钥对中的私钥对登录账号和/或随机数进行加密，得到加密结果；第一设备基于登录账号，以及如下至少之一的信息生成加密后的身份信息：加密结果和数字证书。

可选的，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：第一设备获取第一随机数；第一设备使用密钥对中的私钥对登录账号和第一随机数进行加密，得到加密结果。

可选的，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：第一设备向认证服务器发起登录请求，其中，认证服务器根据登录请求生成加密信息，其中，加密信息包括如下至少之一：密钥对和数字证书。

可选的，第一设备通过如下任意一种通信方式与第二设备建立通信连接：传输控制协议 TCP、用户数据报协议 UDP、蓝牙、Zigbee、WiFi。

可选的，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：第一设备将加密后的身份信息添加第一设备的数字签名；第一设备将添加数字签名后的身份信息发送至第二设备。

可选的，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：第二设备基于预先安装的根证书，判断待验证的身份信息中包含的数字证书是否可信；在数字证书不可信的情况下，第一设备接收第二设备返回的身份验证失败的结果。

可选的，在本实施例中，在数字证书可信的情况下，存储介质被设置为存储用于执行以下步骤的程序代码：在数字证书可信的情况下，第二设备提取数字证书中包含的公钥，并通过数字签名验证接收到的数据是否被篡改；在接收到的数据被篡改的情况下，第一设备接收第二设备返回的身份验证失败的结果。

5 可选的，在本实施例中，在接收到的数据未被篡改的情况下，存储介质被设置为存储用于执行以下步骤的程序代码：第二设备利用公钥对加密结果进行解密，得到登录账号和/或第一随机数；第二设备判断登录账号是否存在于可信任列表中，其中，可信任列表包含允许登录第二设备的至少一个账户；在登录账号不存在于可信任列表的情况下，第一设备接收第二设备返回的身份验证失败的结果。

10 可选的，在本实施例中，在登录账号存在于可信任列表的情况下，存储介质被设置为存储用于执行以下步骤的程序代码：第一设备根据第一随机数和认证服务器返回的第二随机数，生成共享密钥，其中，第二随机数为第二设备在登录账号存在于可信任列表的情况下，第二设备生成的随机数；其中，第二设备根据第一随机数和第二随机数，生成共享密钥。

15 可选的，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：第二设备判断可信任列表中是否存在登录账号；在可信任列表中不存在登录账号的情况下，第二设备将解密得到的登录账号作为管理账号，并添加到可信任列表中，其中，管理账号用于管理可信任列表中的至少一个登录账号。

实施例 9

20 本申请的实施例还提供了一种身份认证系统，包括：处理器；以及存储器，与处理器连接，用于为处理器提供处理以下处理步骤的指令：

第一设备与第二设备建立通信连接，并通过互联网获取加密信息，其中，第一设备为允许访问互联网的设备，第二设备为不允许访问互联网的设备；

25 第一设备使用加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至第二设备；

第一设备接收第二设备返回的验证结果，其中，第二设备基于验证信息来验证加密后的身份信息。

30 由上可知，在本申请上述实施例中，通过允许访问互联网的第一设备从互联网上获取加密信息，并使用该加密信息加密第一设备登录第二设备的账户的身份信息，以便第二设备可以通过验证信息，对接收到的身份信息进行验证，以便在确定第一设备的身份

信息为可信的情况下，才与第一设备进行通信。

容易注意的是，第二设备中验证信息可以对第一设备获取到的加密信息进行验证，以根据验证结果，来确定第一设备的身份是否可信。因而，通过本申请上述实施例公开的方案，达到了根据非联网设备中内置的验证信息对用于操作该非联网设备的对象的身份信息进行验证的目的，从而实现了在通过客户端操作非联网设备的时候，非联网设备

5 对客户端身份进行认证以提高客户端与非联网设备之间数据传输的安全性的技术效果。

由此，本申请提供的上述实施例 9 的方案解决了现有技术中，在联网设备对非联网设备进行操作的过程中，由于非联网设备无法连接认证服务器，导致接入该非联网设备的联网设备无法完成身份认证的技术问题。

10 上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。

在本申请的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中沒有详述的部分，可以参见其他实施例的相关描述。

在本申请所提供的几个实施例中，应该理解到，所揭露的技术内容，可通过其它的方式实现。其中，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，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，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可为个人计算机、服务器或者网络设备）执行本申请各个实施例所述方法

30

的全部或部分步骤。而前述的存储介质包括：U 盘、只读存储器（ROM, Read-Only Memory）、随机存取存储器（RAM, Random Access Memory）、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

5 以上所述仅是本申请的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本申请原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本申请的保护范围。