(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 106960148 B
(45)授权公告日 2021.05.14

(21)申请号 201610018126.0
(22)申请日 2016.01.12
(65)同一申请的已公布的文献号
申请公布号 CN 106960148 A
(43)申请公布日 2017.07.18
(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱
(72)发明人 陈辰 陈海兵
(74)专利代理机构 北京鸿德海业知识产权代理有限公司 11412
代理人 孟繁琦
(51)Int.Cl.
G06F 21/33(2013.01)
H04L 29/06(2006.01)
H04M 1/72403(2021.01)
H04W 8/26(2009.01)

审查员 张秋芳

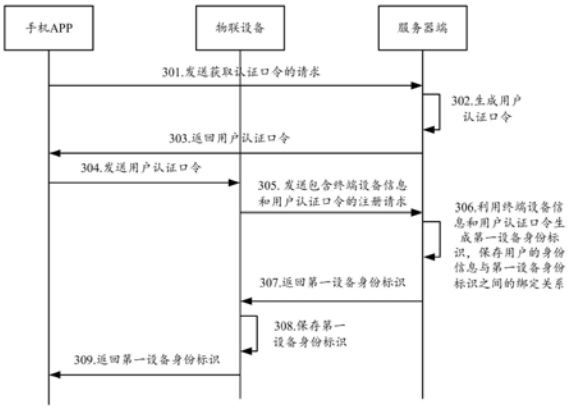
权利要求书5页 说明书13页 附图5页

(54)发明名称

一种设备标识的分配方法和装置

(57)摘要

本发明提供了一种设备标识的分配方法和装置，其中方法包括：接收第一请求，所述第一请求中包括终端设备信息和用户认证口令；所述用户认证口令是根据在所述第一请求之前发送的第二请求生成的；利用所述用户认证口令，生成所述终端设备对应的第一设备身份标识。本发明能够防止设备身份被假冒，提高安全性。



CN 106960148 B

1.一种设备标识的分配方法,其特征在于,该方法包括:

接收第一请求,所述第一请求中包括终端设备信息和用户认证口令;所述用户认证口令是根据在所述第一请求之前发送的第二请求包含的用户的身份信息生成的;

利用所述用户认证口令,生成所述终端设备对应的第一设备身份标识,保存所述用户的身份信息与所述第一设备身份标识之间的绑定关系,以依据所述绑定关系确定是否在终端设备和用户终端之间转发数据;

将所述第一设备身份标识发送给终端设备和所述用户终端;

接收携带所述第一设备身份标识的注销请求;

解除所述第一设备身份标识。

2.根据权利要求1所述的方法,其特征在于,所述第一请求由所述终端设备或用户终端发送;

所述第二请求由所述终端设备或所述用户终端发送。

3.根据权利要求1所述的方法,其特征在于,所述用户认证口令采用以下方式生成:

接收所述第二请求;

确定用户的身份信息,并利用所述用户的身份信息生成用户认证口令;

保存所述用户的身份信息对应的用户认证口令。

4.根据权利要求3所述的方法,其特征在于,利用所述用户的身份信息生成用户认证口令包括:

将所述用户的身份信息和随机信息按预设的顺序进行拼接后,对拼接得到的信息进行加密处理,得到用户认证口令。

5.根据权利要求1所述的方法,其特征在于,若接收到的第一请求中不包含用户认证口令,则该方法还包括:

利用接收到的第一请求中包含的终端设备信息,生成第二设备身份标识。

6.根据权利要求5所述的方法,其特征在于,该方法还包括:

将生成的第二设备身份标识返回给所述终端设备和用户终端。

7.根据权利要求1或5所述的方法,其特征在于,所述终端设备信息包括设备型号、设备MAC地址和设备的产品序列号中的至少一种。

8.根据权利要求1所述的方法,其特征在于,利用所述用户认证口令,生成第一设备身份标识包括:

将用户认证口令采用安全哈希算法进行处理,得到第一设备身份标识;或者,

将所述终端设备信息和用户认证口令按预设的顺序进行拼接后,采用安全哈希算法对所述拼接得到的信息进行处理,得到第一设备身份标识。

9.根据权利要求1所述的方法,其特征在于,该方法还包括:

接收携带所述第一设备身份标识的注销请求;

删除所述用户的身份信息与所述第一设备身份标识之间的绑定关系。

10.根据权利要求1所述的方法,其特征在于,利用所述用户认证口令,生成所述终端设备对应的第一设备身份标识之前,该方法还包括:

判断所述第一请求包含的用户认证口令是否超出有效期,如果是,则返回注册失败的响应;否则,执行利用所述用户认证口令,生成所述终端设备对应的第一设备身份标识的步

骤。

11.根据权利要求10所述的方法，其特征在于，该方法还包括：

接收登录请求；

判断所述登录请求包含的第一设备身份标识是否被解除，如果是，则登录失败；否则登录成功。

12.根据权利要求1所述的方法，其特征在于，该方法还包括：

接收包含第一设备身份标识的数据请求，判断本地是否存在与所述第一设备身份标识存在绑定关系的用户的身份信息；如果是，则将所述数据请求转发至所述用户的身份信息对应的用户终端，否则拒绝所述数据请求；或者，

接收包含用户的身份信息的数据请求，判断本地是否存在与所述用户的身份信息存在绑定关系的第一设备身份标识，如果是，则将所述数据请求转发至所述第一设备身份标识对应的终端设备；否则，拒绝所述数据请求。

13.根据权利要求1至6、8至12中任一项所述的方法，其特征在于，所述第一请求为身份注册请求；

所述第二请求为获取认证口令的请求。

14.一种设备标识的分配方法，其特征在于，该方法包括：

从服务器端获取用户认证口令，所述用户认证口令是服务器端依据用户的身份信息生成的；

将所述用户认证口令发送给终端设备，以触发所述终端设备利用所述用户认证口令从服务器端获取所述终端设备对应的第一设备身份标识以及实现在所述服务器端保存用户的身份信息与所述第一设备身份标识之间的绑定关系，以依据所述绑定关系确定是否在终端设备和用户终端之间转发数据；

向所述服务器端发送携带所述第一设备身份标识的注销请求以解除所述第一设备身份标识。

15.根据权利要求14所述的方法，其特征在于，该方法还包括：

接收所述终端设备返回的第一设备身份标识。

16.根据权利要求14所述的方法，其特征在于，所述从服务器端获取用户认证口令包括：

向所述服务器端发送获取认证口令的请求；

接收所述服务器端利用用户的身份信息生成并返回的用户认证口令。

17.根据权利要求14所述的方法，其特征在于，将所述用户认证口令发送给终端设备包括：

利用局域网或者近距离通信方式将所述用户认证口令发送给终端设备。

18.根据权利要求14至17任一项所述的方法，其特征在于，该方法还包括：

向所述服务器端发送包含所述第一设备身份标识的数据请求。

19.一种设备标识的分配方法，其特征在于，该方法包括：

从用户终端接收用户认证口令，所述用户认证口令是服务器端利用用户的身份信息生成并发送给所述用户终端的；

向服务器端发送包含终端设备信息和用户认证口令的第一请求，以便所述服务器端用

所述用户认证口令，生成所述终端设备对应的第一设备身份标识并保存用户的身份信息与所述第一设备身份标识之间的绑定关系，以依据所述绑定关系确定是否在终端设备和用户终端之间转发数据；

接收并保存所述服务器端返回的第一设备身份标识；

其中，所述第一设备身份标识能够依据携带所述第一设备身份标识的注销请求而被解除。

20.根据权利要求19所述的方法，其特征在于，该方法还包括：

将所述第一设备身份标识返回给所述用户终端。

21.根据权利要求19所述的方法，其特征在于，该方法还包括：

向所述服务器端发送包含所述第一设备身份标识的登录请求；

如果登录失败，则向所述服务器端发送包含终端设备信息的第一请求；

利用接收到的第二设备身份标识替换本地保存的第一设备身份标识。

22.根据权利要求19所述的方法，其特征在于，所述从用户终端接收用户认证口令包括：

通过局域网或近距离通信方式从用户终端接收用户认证口令。

23.根据权利要求19至22任一项所述的方法，其特征在于，该方法还包括：

向所述服务器端发送数据请求，所述数据请求包含本地保存的设备身份标识，该设备身份标识包括第一设备身份标识或第二设备身份标识。

24.一种设备标识的分配装置，设置于服务器端，其特征在于，该装置包括：

第二交互单元，用于接收第一请求，所述第一请求中包括终端设备信息和用户认证口令；所述用户认证口令是根据在所述第一请求之前发送的第二请求包含的用户的身份信息生成的；

标识维护单元，用于利用所述用户认证口令，生成所述终端设备对应的第一设备身份标识；

绑定处理单元，用于保存所述用户的身份信息与所述第一设备身份标识之间的绑定关系，以依据所述绑定关系确定是否在终端设备和用户终端之间转发数据；

第一交互单元，用于将所述第一设备身份标识发送给所述用户终端和所述终端设备；

所述第一交互单元，还用于接收携带第一设备身份标识的注销请求；

所述标识维护单元，还用于依据注销请求，解除所述第一设备身份标识。

25.根据权利要求24所述的装置，其特征在于，所述第一请求由所述终端设备或用户终端发送；

所述第二请求由所述终端设备或所述用户终端发送。

26.根据权利要求24所述的装置，其特征在于，该装置还包括：口令维护单元；

所述第一交互单元，用于接收所述第二请求；

所述口令维护单元，用于确定发送所述第二请求的用户的身份信息，并利用所述用户的身份信息生成用户认证口令；保存所述用户的身份信息对应的用户认证口令。

27.根据权利要求26所述的装置，其特征在于，所述口令维护单元在利用所述用户的身份信息生成用户认证口令时，具体执行：

将所述用户的身份信息和随机信息按预设的顺序进行拼接后，对拼接得到的信息进行

加密处理，得到用户认证口令。

28.根据权利要求24所述的装置，其特征在于，所述标识维护单元，还用于在所述第一请求中不包含用户认证口令时，利用所述第一请求中包含的终端设备信息，生成第二设备身份标识。

29.根据权利要求28所述的装置，其特征在于，所述第一交互单元，还用于将所述第二设备身份标识返回给用户终端；和，

所述第二交互单元，还用于将所述第二设备身份标识返回给所述终端设备。

30.根据权利要求24或28所述的装置，其特征在于，所述终端设备信息包括设备型号、设备MAC地址和设备的产品序列号中的至少一种。

31.根据权利要求24所述的装置，其特征在于，所述标识维护单元，具体用于：

将用户认证口令采用安全哈希算法进行处理，得到第一设备身份标识；或者，

将所述终端设备信息和用户认证口令按预设的顺序进行拼接后，采用安全哈希算法对所述拼接得到的信息进行处理，得到第一设备身份标识。

32.根据权利要求24所述的装置，其特征在于，所述绑定处理单元，还用于依据所述注销请求，删除所述用户的身份信息与所述第一设备身份标识之间的绑定关系。

33.根据权利要求24所述的装置，其特征在于，该装置还包括：口令验证单元，用于在所述第二交互单元接收到所述第一请求后，判断所述第一请求包含的用户认证口令是否超出有效期，如果是，则触发所述第二交互单元返回注册失败的响应；否则，触发所述标识维护单元执行利用所述用户认证口令，生成所述终端设备对应的第一设备身份标识。

34.根据权利要求24所述的装置，其特征在于，该装置还包括：登录处理单元；

所述第二交互单元，还用于接收所述终端设备的登录请求；

所述登录处理单元，用于判断所述登录请求包含的第一设备身份标识是否被解除，如果是，则登录失败；否则登录成功。

35.根据权利要求34所述的装置，其特征在于，该装置还包括：

转发处理单元，用于在所述第二交互单元接收到所述终端设备发送的包含第一设备身份标识的数据请求时，判断本地是否存在与所述第一设备身份标识存在绑定关系的用户的身份信息，如果是，则将所述数据请求转发至所述用户的身份信息对应的用户终端，否则拒绝所述数据请求；或者，

在第一交互单元接收到包含用户的身份信息的数据请求时，判断本地是否存在与所述用户的身份信息存在绑定关系的第一设备身份标识，如果是，则通过所述第二交互单元将所述数据请求转发至所述第一设备身份标识对应的终端设备；否则，拒绝所述数据请求。

36.根据权利要求24至29、31至35任一项所述的装置，其特征在于，所述第一请求为身份注册请求；

所述第二请求为获取认证口令的请求。

37.一种设备标识的分配装置，该装置设置于用户终端，其特征在于，该装置包括：

服务端交互单元，用于从服务器端获取用户认证口令，所述用户认证口令是服务器端依据用户的身份信息生成的；

终端交互单元，用于将所述用户认证口令发送给终端设备，以触发所述终端设备利用所述用户认证口令从服务器端获取所述终端设备对应的第一设备身份标识以及实现在所

述服务器端保存用户的身份信息与所述第一设备身份标识之间的绑定关系，以依据所述绑定关系确定是否在终端设备和用户终端之间转发数据；

所述服务端交互单元，还用于向所述服务器端发送携带所述第一设备身份标识的注销请求以解除所述第一设备身份标识。

38.根据权利要求37所述的装置，其特征在于，所述终端交互单元，还用于接收所述终端设备返回的第一设备身份标识。

39.根据权利要求37所述的装置，其特征在于，所述服务端交互单元，具体用于向所述服务器端发送获取认证口令的请求；接收所述服务器端利用用户的身份信息生成并返回的用户认证口令。

40.根据权利要求37所述的装置，其特征在于，所述终端交互单元，具体利用局域网或者近距离通信方式将所述用户认证口令发送给终端设备。

41.根据权利要求37至40任一项所述的装置，其特征在于，所述服务端交互单元，还用于向所述服务器端发送包含所述第一设备身份标识的数据请求。

42.一种设备标识的分配装置，该装置设置于终端设备，其特征在于，该装置包括：

用户端交互单元，用于从用户终端接收用户认证口令，所述用户认证口令是服务器端利用用户的身份信息生成并发送给所述用户终端的；

服务端交互单元，用于向服务器端发送包含终端设备信息和用户认证口令的第一请求，以便所述服务器端用所述用户认证口令，生成所述终端设备对应的第一设备身份标识并保存用户的身份信息与所述第一设备身份标识之间的绑定关系，以依据所述绑定关系确定是否在终端设备和用户终端之间转发数据；接收所述服务器端返回的第一设备身份标识；

标识保存单元，用于保存所述服务端交互单元接收到的第一设备身份标识；

其中，所述第一设备身份标识能够依据携带所述第一设备身份标识的注销请求而被解除。

43.根据权利要求42所述的装置，其特征在于，所述用户端交互单元，还用于将所述第一设备身份标识返回给所述用户终端。

44.根据权利要求42所述的装置，其特征在于，所述服务端交互单元，还用于向所述服务器端发送包含所述第一设备身份标识的登录请求；如果登陆失败，则向所述服务器端发送包含终端设备信息的第一请求；接收所述服务器端返回的第二设备身份标识；

所述标识保存单元，还用于利用所述第二设备身份标识替换本地保存的第一设备身份标识。

45.根据权利要求42所述的装置，其特征在于，所述用户端交互单元，具体用于通过局域网或近距离通信方式从用户端接收用户认证口令。

46.根据权利要求42至45任一项所述的装置，其特征在于，所述服务端交互单元，还用于向所述服务器端发送数据请求，所述数据请求包含所述标识保存单元保存的设备身份标识，该设备身份标识包括第一设备身份标识或第二设备身份标识。

一种设备标识的分配方法和装置

【技术领域】

[0001] 本发明涉及计算机应用技术领域，特别涉及一种设备标识的分配方法和装置。

【背景技术】

[0002] 随着计算机技术的迅猛发展，为用户的生活提供了越来越多的便利，用户能够利用用户设备上的APP(应用软件)通过云端对与该用户绑定的终端设备进行数据交互。例如在物联网中，用户能够通过手机APP与物联设备绑定后，通过云端对物联设备进行数据交互，获取物联设备采集的私密数据。理想状况是，物联设备采集的数据通过物联网仅发送给与该物联设备绑定的用户。如图1中所示，物联设备A采集的数据发送给物联设备A的用户，物联设备B采集的数据发送给物联设备B的用户。

[0003] 为了实现上述目的，物联网云端的服务器首先为物联设备及用户注册，生成物联网全局内唯一的设备身份ID及用户身份ID，然后应用户请求建立设备身份ID和用户身份ID之间的绑定关系。其流程大致如图2中所示，用户首先通过手机APP注册并获取用户身份ID；在201中物联设备向物联网云端的服务器发送注册请求，在202中由服务器给物联设备分配设备身份ID；在203中用户通过手机APP对设备查询或扫码，并在204中获取物联设备的设备身份ID；在205中用户向服务器发出绑定请求，请求绑定设备身份ID，在206中服务器在本地存储设备身份ID和用户身份ID之间的绑定关系，并向用户返回绑定成功响应。至此完成绑定。在207中若物联设备将采集到的数据发送给服务器，在208中服务器依据绑定关系将该数据转发给用户。

[0004] 目前用户身份注册流程是有比较成熟的技术方案的，比如短信核对、email核对甚至实名注册审核等，用户身份注册是比较安全可靠的。但现有的设备身份注册流程是通过提供物联设备的原始物理信息，例如设备型号、设备MAC地址以及产品序列号，然后由物联网云端的服务器通过一定算法生成的设备身份ID。但这种方案存在明显的安全漏洞：由于设备身份ID来源于物联设备的原始物理信息，一旦原始物理信息被假冒，就会出现克隆设备和随之而来的数据攻击。例如克隆设备伪造了物联设备的原始物理信息进行注册，得到真实的设备身份ID，并以此设备身份ID向与该设备身份ID绑定的用户发送虚假信息。

【发明内容】

[0005] 有鉴于此，本发明提供了一种设备标识的分配方法和装置，以便于防止设备身份被假冒，提高安全性。

[0006] 具体技术方案如下：

[0007] 本发明提供了一种设备标识的分配方法，该方法包括：

[0008] 接收第一请求，所述第一请求中包括终端设备信息和用户认证口令；所述用户认证口令是根据在所述第一请求之前发送的第二请求生成的；

[0009] 利用所述用户认证口令，生成所述终端设备对应的第一设备身份标识。

[0010] 根据本发明一优选实施方式，所述第一请求由所述终端设备或用户终端发送；

[0011] 所述第二请求由所述终端设备或所述用户终端发送。

[0012] 根据本发明一优选实施方式，该方法还包括：

[0013] 将所述第一设备标识发送给所述终端设备和/或所述用户终端。

[0014] 根据本发明一优选实施方式，该方法还包括：

[0015] 保存用户的身份信息与所述第一设备身份标识之间的绑定关系。

[0016] 根据本发明一优选实施方式，所述用户认证口令采用以下方式生成：

[0017] 接收所述第二请求；

[0018] 确定用户的身份信息，并利用所述用户的身份信息生成用户认证口令；

[0019] 保存所述用户的身份信息对应的用户认证口令。

[0020] 根据本发明一优选实施方式，利用所述用户的身份信息生成用户认证口令包括：

[0021] 将所述用户的身份信息和随机信息按预设的顺序进行拼接后，对拼接得到的信息进行加密处理，得到用户认证口令。

[0022] 根据本发明一优选实施方式，若接收到的第一请求中不包含用户认证口令，则该方法还包括：

[0023] 利用接收到的第一请求中包含的终端设备信息，生成第二设备身份标识。

[0024] 根据本发明一优选实施方式，该方法还包括：

[0025] 将生成的第二设备身份标识返回给所述终端设备和/或用户终端。

[0026] 根据本发明一优选实施方式，所述终端设备信息包括设备型号、设备MAC地址和设备的产品序列号中的至少一种。

[0027] 根据本发明一优选实施方式，利用所述用户认证口令，生成第一设备身份标识包括：

[0028] 将用户认证口令采用安全哈希算法进行处理，得到第一设备身份标识；或者，

[0029] 将所述终端设备信息和用户认证口令按预设的顺序进行拼接后，采用安全哈希算法对所述拼接得到的信息进行处理，得到第一设备身份标识。

[0030] 根据本发明一优选实施方式，该方法还包括：

[0031] 接收携带所述第一设备身份标识的注销请求；

[0032] 解除所述第一设备身份标识。

[0033] 根据本发明一优选实施方式，该方法还包括：

[0034] 接收携带所述第一设备身份标识的注销请求；

[0035] 删除所述用户的身份信息与所述第一设备身份标识之间的绑定关系。

[0036] 根据本发明一优选实施方式，利用所述用户认证口令，生成所述终端设备对应的第一设备身份标识之前，该方法还包括：

[0037] 判断所述第一请求包含的用户认证口令是否超出有效期，如果是，则返回注册失败的响应；否则，执行利用所述用户认证口令，生成所述终端设备对应的第一设备身份标识的步骤。

[0038] 根据本发明一优选实施方式，该方法还包括：

[0039] 接收登录请求；

[0040] 判断所述登录请求包含的第一设备身份标识是否被解除，如果是，则登录失败；否则登录成功。

[0041] 根据本发明一优选实施方式，该方法还包括：

[0042] 接收包含第一设备身份标识的数据请求，判断本地是否存在与所述第一设备身份标识存在绑定关系的用户的身份信息；如果是，则将所述数据请求转发至所述用户的身份信息对应的用户终端，否则拒绝所述数据请求；或者，

[0043] 接收包含用户的身份信息的数据请求，判断本地是否存在与所述用户的身份信息存在绑定关系的第一设备身份标识，如果是，则将所述数据请求转发至所述第一设备身份标识对应的终端设备；否则，拒绝所述数据请求。

[0044] 根据本发明一优选实施方式，所述第一请求为身份注册请求；

[0045] 所述第二请求为获取认证口令的请求。

[0046] 本发明还提供了一种设备标识的分配方法，该方法包括：

[0047] 从服务器端获取用户认证口令；

[0048] 将所述用户认证口令发送给终端设备以触发所述终端设备利用所述用户认证口令从服务器端获取所述终端设备对应的第一设备身份标识。

[0049] 根据本发明一优选实施方式，该方法还包括：

[0050] 接收所述终端设备返回的第一设备身份标识。

[0051] 根据本发明一优选实施方式，所述从服务器端获取用户认证口令包括：

[0052] 向所述服务器端发送获取认证口令的请求；

[0053] 接收所述服务器端利用用户的身份信息生成并返回的用户认证口令。

[0054] 根据本发明一优选实施方式，将所述用户认证口令发送给终端设备包括：

[0055] 利用局域网或者近距离通信方式将所述用户认证口令发送给终端设备。

[0056] 根据本发明一优选实施方式，该方法还包括：

[0057] 向所述服务器端发送携带所述第一设备身份标识的注销请求。

[0058] 根据本发明一优选实施方式，该方法还包括：

[0059] 向所述服务器端发送包含所述第一设备身份标识的数据请求。

[0060] 本发明还提供了一种设备标识的分配方法，该方法包括：

[0061] 从用户终端接收用户认证口令；

[0062] 向服务器端发送包含终端设备信息和用户认证口令的第一请求；

[0063] 接收并保存所述服务器端返回的第一设备身份标识。

[0064] 根据本发明一优选实施方式，该方法还包括：

[0065] 将所述第一设备身份标识返回给所述用户终端。

[0066] 根据本发明一优选实施方式，该方法还包括：

[0067] 向所述服务器端发送包含所述第一设备身份标识的登录请求；

[0068] 如果登录失败，则向所述服务器端发送包含终端设备信息的第一请求；

[0069] 利用接收到的第二设备身份标识替换本地保存的第一设备身份标识。

[0070] 根据本发明一优选实施方式，所述从用户终端接收用户认证口令包括：

[0071] 通过局域网或近距离通信方式从用户终端接收用户认证口令。

[0072] 根据本发明一优选实施方式，该方法还包括：

[0073] 向所述服务器端发送数据请求，所述数据请求包含本地保存的设备身份标识，该设备身份标识包括第一设备身份标识或第二设备身份标识。

[0074] 本发明还提供了一种设备标识的分配装置，设置于服务器端，该装置包括：

[0075] 第二交互单元，用于接收第一请求，所述第一请求中包括终端设备信息和用户认证口令；所述用户认证口令是根据在所述第一请求之前发送的第二请求生成的；

[0076] 标识维护单元，用于利用所述用户认证口令，生成第一设备身份标识。

[0077] 根据本发明一优选实施方式，所述第一请求由所述终端设备或用户终端发送；

[0078] 所述第二请求由所述终端设备或所述用户终端发送。

[0079] 根据本发明一优选实施方式，该装置还包括：第一交互单元，用于将所述第一设备标识发送给所述用户终端；和/或，

[0080] 所述第一交互单元，用于将所述第一设备标识发送给所述终端设备。

[0081] 根据本发明一优选实施方式，该装置还包括：

[0082] 绑定处理单元，用于保存用户的身份信息与所述第一设备身份标识之间的绑定关系。

[0083] 根据本发明一优选实施方式，第一交互单元和口令维护单元；

[0084] 所述第一交互单元，用于接收所述第二请求；

[0085] 所述口令维护单元，用于确定发送所述第二请求的用户的身份信息，并利用所述用户的身份信息生成用户认证口令；保存所述用户的身份信息对应的用户认证口令。

[0086] 根据本发明一优选实施方式，所述口令维护单元在利用所述用户的身份信息生成用户认证口令时，具体执行：

[0087] 将所述用户的身份信息和随机信息按预设的顺序进行拼接后，对拼接得到的信息进行加密处理，得到用户认证口令。

[0088] 根据本发明一优选实施方式，所述标识维护单元，还用于在所述第一请求中不包含用户认证口令时，利用所述第一请求中包含的终端设备信息，生成第二设备身份标识。

[0089] 根据本发明一优选实施方式，该装置还包括：第一交互单元，用于将所述第二设备身份标识返回给用户终端；和/或，

[0090] 所述第二交互单元，还用于将所述第二设备身份标识返回给所述终端设备。

[0091] 根据本发明一优选实施方式，所述终端设备信息包括设备型号、设备MAC地址和设备的产品序列号中的至少一种。

[0092] 根据本发明一优选实施方式，所述标识维护单元，具体用于：

[0093] 将用户认证口令采用安全哈希算法进行处理，得到第一设备身份标识；或者，

[0094] 将所述终端设备信息和用户认证口令按预设的顺序进行拼接后，采用安全哈希算法对所述拼接得到的信息进行处理，得到第一设备身份标识。

[0095] 根据本发明一优选实施方式，该装置还包括：第一交互单元，用于接收携带第一设备身份标识的注销请求；

[0096] 所述标识维护单元，还用于依据注销请求，解除所述第一设备身份标识。

[0097] 根据本发明一优选实施方式，该装置还包括：第一交互单元，用于接收携带第一设备身份标识的注销请求；

[0098] 所述绑定处理单元，还用于依据所述注销请求，删除所述用户的身份信息与所述第一设备身份标识之间的绑定关系。

[0099] 根据本发明一优选实施方式，该装置还包括：口令验证单元，用于在所述第二交互

单元接收到所述第一请求后，判断所述第一请求包含的用户认证口令是否超出有效期，如果是，则触发所述第二交互单元返回注册失败的响应；否则，触发所述标识维护单元执行利用所述用户认证口令，生成所述终端设备对应的第一设备身份标识。

[0100] 根据本发明一优选实施方式，该装置还包括：登录处理单元；

[0101] 所述第二交互单元，还用于接收所述终端设备的登录请求；

[0102] 所述登录处理单元，用于判断所述登录请求包含的第一设备身份标识是否被解除，如果是，则登录失败；否则登录成功。

[0103] 根据本发明一优选实施方式，该装置还包括：

[0104] 转发处理单元，用于在所述第二交互单元接收到所述终端设备发送的包含第一设备身份标识的数据请求时，判断本地是否存在与所述第一设备身份标识存在绑定关系的用户的身份信息，如果是，则将所述数据请求转发至所述用户的身份信息对应的用户终端，否则拒绝所述数据请求；或者，

[0105] 在第一交互单元接收到包含用户的身份信息的数据请求时，判断本地是否存在与所述用户的身份信息存在绑定关系的第一设备身份标识，如果是，则通过所述第二交互单元将所述数据请求转发至所述第一设备身份标识对应的终端设备；否则，拒绝所述数据请求。

[0106] 根据本发明一优选实施方式，所述第一请求为身份注册请求；

[0107] 所述第二请求为获取认证口令的请求。

[0108] 本发明提供了一种设备标识的分配装置，该装置设置于用户终端，该装置包括：

[0109] 服务端交互单元，用于从服务器端获取用户认证口令；

[0110] 终端交互单元，用于将所述用户认证口令发送给终端设备以触发所述终端设备利用所述用户认证口令从服务器端获取所述终端设备对应的第一设备身份标识。

[0111] 根据本发明一优选实施方式，所述终端交互单元，还用于接收所述终端设备返回的第一设备身份标识。

[0112] 根据本发明一优选实施方式，所述服务端交互单元，具体用于向所述服务器端发送获取认证口令的请求；接收所述服务器端利用用户的身份信息生成并返回的用户认证口令。

[0113] 根据本发明一优选实施方式，所述终端交互单元，具体利用局域网或者近距离通信方式将所述用户认证口令发送给终端设备。

[0114] 根据本发明一优选实施方式，所述服务端交互单元，还用于向所述服务器端发送携带所述第一设备身份标识的注销请求。

[0115] 根据本发明一优选实施方式，所述服务端交互单元，还用于向所述服务器端发送包含所述第一设备身份标识的数据请求。

[0116] 本发明还提供了一种设备标识的分配装置，该装置设置于终端设备，该装置包括：

[0117] 用户端交互单元，用于从用户终端接收用户认证口令；

[0118] 服务端交互单元，用于向服务器端发送包含终端设备信息和用户认证口令的第一请求；接收所述服务器端返回的第一设备身份标识；

[0119] 标识保存单元，用于保存所述服务端交互单元接收到的第一设备身份标识。

[0120] 根据本发明一优选实施方式，所述用户端交互单元，还用于将所述第一设备身份

标识返回给所述用户终端。

[0121] 根据本发明一优选实施方式，所述服务端交互单元，还用于向所述服务器端发送包含所述第一设备身份标识的登录请求；如果登陆失败，则向所述服务器端发送包含终端设备信息的第一请求；接收所述服务器端返回的第二设备身份标识；

[0122] 所述标识保存单元，还用于利用所述第二设备身份标识替换本地保存的第一设备身份标识。

[0123] 根据本发明一优选实施方式，所述用户端交互单元，具体用于通过局域网或近距离通信方式从用户端接收用户认证口令。

[0124] 根据本发明一优选实施方式，所述服务端交互单元，还用于向所述服务器端发送数据请求，所述数据请求包含所述标识保存单元保存的设备身份标识，该设备身份标识包括第一设备身份标识或第二设备身份标识。

[0125] 由以上技术方案可以看出，在本发明中，服务器端依据用户认证口令生成终端设备对应的第一设备身份标识，而并非单纯依据终端设备信息来生成第一设备身份标识。这种方式即便终端设备被克隆，由于其无法得到用户认证口令，因此无法假冒终端设备的身份，提高了安全性。

【附图说明】

[0126] 图1为物联网中物联设备与用户之间的数据交互示意图；

[0127] 图2为现有技术中物联设备和用户之间的绑定流程示意图；

[0128] 图3为本发明实施例提供的身份注册的主要方法流程图；

[0129] 图4为本发明实施例提供的解除物联设备认证的方法流程图；

[0130] 图5为本发明实施例提供的另一种身份注册的方法流程图；

[0131] 图6为本发明实施例提供的设置于服务器端的装置结构图；

[0132] 图7为本发明实施例提供的设置于用户终端的装置结构图；

[0133] 图8为本发明实施例提供的设置于终端设备的装置结构图。

【具体实施方式】

[0134] 为了使本发明的目的、技术方案和优点更加清楚，下面结合附图和具体实施例对本发明进行详细描述。

[0135] 首先需要说明的是，本发明所提供的方法和装置并不限于物联网下的物联设备身份认证，对于任意通过服务器与用户终端进行互通的终端设备，本发明均适用。这里的用户终端可以包括但不限于手机、平板电脑、笔记本电脑、PDA(个人数字助理)等能够运行APP的智能用户设备。与用户终端互通的终端设备可以包括但不限于智能家电设备、网络设备、可穿戴式设备、智能医疗设备、PC(个人计算机)等。其中智能移动设备可以包括诸如手机、平板电脑、笔记本电脑、PDA(个人数字助理)等。智能家电设备可以包括诸如智能电视、智能空调、智能热水器、智能冰箱、智能空气净化器等等。网络设备可以包括诸如交换机、无线AP、服务器等。可穿戴式设备可以包括诸如智能手表、智能眼镜、智能手环等等。智能医疗设备可以包括诸如智能体温计、智能血压仪、智能血糖仪等等。为了方便描述，本发明均以手机与物联设备为例进行描述。

[0136] 图3为本发明实施例提供的身份注册的主要方法流程图，如图3中所示，该方法可以包括以下步骤：

[0137] 在301中，用户通过手机APP向服务器端发送获取认证口令的请求。

[0138] 在本发明实施例中，由用户端触发物联设备的身份注册和绑定。当用户想要通过手机与某物联设备实现绑定时，登录手机APP，通过该手机APP向服务器端发送获取认证口令的请求，在该请求中包含用户的身份信息。其中用户的身份信息可以是用户的登录账号，也可以是服务器端为用户分配的用户标识(User ID)，也可以是用户向服务器端注册获取的用户身份ID等。

[0139] 在302中，服务器端利用用户的身份信息生成用户认证口令。

[0140] 若获取认证口令的请求中包含的是用户的登录账号，则可以利用用户的登录账号确定对应的User ID，然后利用User ID生成用户认证口令。若获取认证口令的请求中包含的是User ID，则可以直接利用该User ID生成用户认证口令。当然也可以利用用户身份ID等其他用户的身份信息来生成用户认证口令，在本实施例中仅以利用User ID生成用户认证口令为例。

[0141] 生成用户认证口令的过程可以包括：将User ID和随机信息按顺序进行拼接后，对得到的信息进行加密处理，得到用户认证口令。例如，可以将User ID、当前时间以及服务器端随机生成的十进制3位随机数进行一次拼接后，对拼接得到的字符串计算MD5值，将得到的值作为用户认证口令。

[0142] 上述方式生成的用户认证口令具备如下特点：1)可回溯性，即可以由用户认证口令回溯到用户的身份信息；2)随机性，即服务器端针对同一用户的多次认证请求，生成各不相同的用户认证口令；3)唯一性，即任何一个用户认证口令在服务器端均是唯一的，用户认证口令不可重复。

[0143] 用户认证口令生成后，将用户的身份信息与用户认证口令之间的对应关系存储于本地。另外，每个用户认证口令可以存在有效期，当超出有效期后，用户认证口令失效。用户认证口令在服务器端存储的形式可以如表1中所示。

[0144] 表1

[0145]

User ID	用户认证口令	是否有效	口令生成时间	口令终止时间
1111111	a95bf5213cdcd1eb600687e380860f74	是	2015.12.12 11:15	2015.12.12 11:20

[0146] 一旦用户认证口令被使用，即在后续利用用户认证口令生成并下发了设备身份标识，则该用户认证口令失效。另外，对于超出有效期的用户认证口令，也被设置为无效。

[0147] 在303中，服务器端将生成的用户认证口令返回给用户端的手机APP。

[0148] 在304中，手机APP将用户认证口令发送给物联设备。

[0149] 获取用户认证口令后，用户可以通过手机APP向该用户认证口令提供给要绑定的物联设备。在本步骤中若手机和物联设备处于同一局域网，则手机APP可以通过局域网将用户认证口令发送给物联设备。或者也可以通过近距离通信方式将用户认证口令发送给物联设备，例如通过蓝牙、红外传输、NFC(近场通信)等方式。

[0150] 在305中，物联设备向服务器端发送包含终端设备信息和用户认证口令的注册请

求。

[0151] 其中，终端设备信息可以包括但不限于设备型号、设备MAC地址和设备的SN(Serial Number，产品序列号)中的至少一种。

[0152] 在306中，服务器端利用注册请求包含的终端设备信息和用户认证口令，生成第一设备身份标识，保存用户的身份信息与第一设备身份标识之间的绑定关系。

[0153] 其中生成第一设备身份标识所采用的算法需保证生成的第一设备身份标识唯一，在本发明实施例中可以采用安全哈希算法(SHA，Secure Hash Algorithm)。例如，可以将设备型号、设备MAC地址和设备的SN按预设的顺序进行拼接，然后采用诸如SHA-256算法对拼接后得到的信息进行处理，得到第一设备身份标识。

[0154] 除了本步骤中所提供的利用终端设备信息和用户认证口令生成第一设备身份标识之外，还可以采用仅利用用户认证口令生成第一设备身份标识的方式，例如采用SHA-256算法对用户认证口令进行处理，得到第一设备身份标识。甚至可以直接将用户认证口令作为第一设备身份标识。然后在服务器端存储终端设备信息和用户认证口令之间的对应关系。

[0155] 另外，在本步骤中，服务器可以首先对接收到的注册请求中包含的用户认证口令进行验证，即验证本地是否保存有该用户认证口令且该用户认证口令是有效的，如果是，则验证通过，生成第一设备身份标识。否则，验证失败。可以向物联设备返回注册失败的响应。

[0156] 在保存绑定关系时，可以保存诸如User ID与第一设备身份标识之间的对应关系，从而实现用户与物联设备之间的绑定。

[0157] 在307中，服务器端将第一设备身份标识返回给物联设备。

[0158] 本步骤可以将第一设备身份标识携带在注册成功的响应中返回给物联设备。

[0159] 在308中，物联设备在本地保存第一设备身份标识。

[0160] 在本发明实施例中，一个物联设备可以允许仅与一个用户绑定，也可以允许与多个用户绑定。当与多个用户绑定时，该物联设备具有多个第一设备身份标识，在服务器端存储有该多个第一设备身份标识与不同用户之间的绑定关系。但考虑到物联设备的数据私密性，优选前一种方式，即仅允许一个物联设备与一个用户绑定。

[0161] 若仅允许一个物联设备与一个用户绑定，那么物联设备可以利用接收到的第一设备身份标识替换本地已保存的设备身份标识。也就是说，一个物联设备在同一时间仅能够具有一个设备身份标识。

[0162] 在309中，物联设备将第一设备身份标识返回给手机APP。

[0163] 通过图3所示流程就可以完成物联设备的身份注册以及用户与物联设备的绑定。

[0164] 对于物联设备发送给用户端的数据请求，服务器端判断本地是否存在该数据请求所包含第一设备身份标识的绑定关系，如果否，则可以拒绝该数据请求。如果是，则将数据请求转发至第一设备身份标识存在绑定关系的用户。

[0165] 对于用户端发送给物联设备的数据请求，服务器端判断本地是否存在与该用户的身份标识存在绑定关系的第一设备身份标识，如果是，则将该数据请求转发至该第一设备身份标识对应的物联设备；否则，拒绝该数据请求。

[0166] 通过本实施例可以看出，物联设备一旦被用户认证后，就需要更新使用新的第一设备身份标识，物联设备和用户端的绑定关系隐藏于第一设备身份标识中。当物联设备被

某个用户认证后，该物联设备的数据仅归属于该用户，并接受该用户的访问控制。

[0167] 需要说明的是，在上述实施例中是终端设备进行身份注册为例进行的描述，但本发明并不限于身份注册，也可以适用于除了身份注册之外任意需要进行设备标识分配的过程，相应地，上述的注册请求替换为其他相应类型的业务请求。

[0168] 另外，图3所示流程中的步骤也可以存在其他可替换的实现方式，例如步骤304～305可以替换为：用户终端通过诸如扫描设备二维码等方式从物联设备获取终端设备信息，然后由手机APP将用户认证口令和终端设备信息发送给服务器端，然后服务器端执行306为物联设备分配第一设备身份标识。

[0169] 再例如，步骤307～309也可以替换为：服务器端将第一设备身份标识返回给手机APP，由手机APP将该第一设备身份标识提供给物联设备，物联设备保存该第一设备身份标识。或者服务器端将第一设备身份标识返回给手机APP和物联设备，物联设备保存该第一设备身份标识。

[0170] 若用户想要解除物联设备认证，可以通过图4所示流程实现。图4为本发明实施例提供的解除物联设备认证的方法流程图，如图4所示，该方法可以包括以下步骤：

[0171] 在401中，用户通过手机APP向服务器端发送注销请求，该注销请求携带要解除的第一设备身份标识。

[0172] 在402中，服务器端依据注销请求中携带的第一设备身份标识，解除该第一设备身份标识，并删除用户的身份信息与第一设备身份标识之间的绑定关系。

[0173] 本步骤中所述解除第一设备身份标识可以是将该第一设备身份标识设置为无效/非法，或者将该第一设备身份标识从服务器端删除等。

[0174] 在403中，服务器端向手机APP返回注销成功的响应。

[0175] 服务器解除该第一设备身份标识后，后续利用该第一设备身份标识进行的登录和数据请求均会被拒绝。例如，用户端向服务器端解除物联设备的身份标识后，该物联设备又向服务器端发送登录请求，该登录请求中包含该物联设备的第一设备身份标识；服务器端判断该第一设备身份标识已被解除，则拒绝该物联设备的登录，向物联设备返回登录失败响应。

[0176] 再例如，用户端向服务器端解除物联设备的第一设备身份标识后，该物联设备又向服务器端发送数据请求，该数据请求中包含该物联设备的第一设备身份标识；服务器端判断该第一设备身份标识已被解除，则拒绝该物联设备的数据请求。

[0177] 在互联网、物联网等网络下，会存在多种多样的设备。同样以物联网为例，有一些网络设备，例如设置于公共场所的温度计，温度计采集的数据是需要服务器端收集后存储于数据库的，并不与特定的用户绑定。再例如路由器，通常也不经由服务器端与特定的用户绑定。这类设备可以称为“无主设备”，对于无主设备其身份注册还是需要采用现有的注册方式，即在服务器端仅依据终端设备的终端设备信息生成第二设备身份标识。其流程可以如图5所示，包括以下步骤：

[0178] 在501中，物联设备向服务器端发送注册请求，该注册请求中包含终端设备信息。

[0179] 其中终端设备信息可以包括诸如设备型号、设备MAC地址和设备的SN。

[0180] 对于无主物联设备可以由其主动发起注册请求。或者无主物联设备在向服务器端发送登录请求时，由于在服务器端并没有该无主物联设备的设备身份标识以及绑定关系，

则在拒绝其登录的同时，会通知其采用终端设备信息进行身份注册。终端设备信息接收到该通知后，主动发起注册请求，其中包含终端设备信息。还有一种情况，即已被解除身份认证的物联设备，其向服务器端发送登录请求时，由于服务器端确定该物联设备的第一身份认证标识已被解除，并返回登录失败响应。物联设备接收到该登录失败响应后，可以主动发起注册请求，其中仅包含终端设备信息。

[0181] 在502中，服务器端利用终端设备信息，生成第二设备身份标识。

[0182] 这种情况下，服务器端仅利用诸如设备型号、设备MAC地址和设备的SN这些原始物理信息，生成第二设备身份标识。这种方式与现有技术中的方式相同，在此不再详述。

[0183] 在503中，服务器端向物联设备返回第二设备身份标识。

[0184] 在504中，物联设备保存接收到的第二设备身份标识。

[0185] 如果物联设备仅允许同时具有一个设备身份标识，且在物联设备本地已经存储有第一设备身份标识，则可以利用接收到的第二设备身份标识更新本地已经存储的第一设备身份标识。

[0186] 对于无主物联设备发送的数据请求，服务器端接收到该数据请求后，确定其包含的是第二设备身份标识，则可以按照预设的处理方式对该数据请求进行处理，例如将该数据请求携带的数据送入数据库。

[0187] 以上是对本发明所提供方法进行的详细描述，下面结合实施例对本发明提供的装置进行详细描述。

[0188] 图6为本发明实施例提供的设置于服务器端的装置结构图，如图6中所示，该装置包括：第二交互单元03和标识维护单元04，还可以包括口令维护单元01、第一交互单元02、绑定处理单元05、口令验证单元06、登录处理单元07和转发处理单元08。各组成单元的主要功能如下：

[0189] 第二交互单元03负责接收第一请求，该第一请求中包括终端设备信息和用户认证口令；该用户认证口令是根据在第一请求之前发送的第二请求生成的。

[0190] 其中第一请求可以由终端设备或用户终端发送；第二请求可以由终端设备或用户终端发送。

[0191] 第一交互单元02可以将第一设备标识发送给用户终端；和/或，将第一设备标识发送给终端设备。

[0192] 口令维护单元01负责针对用户生成用户认证口令。具体地，第一交互单元02从用户端接收第二请求；再由口令维护单元01确定发送第一请求的用户的身份信息，并利用用户的身份信息生成用户认证口令；保存用户的身份信息对应的用户认证口令。

[0193] 其中口令维护单元01在利用用户的身份信息生成用户认证口令时，可以将用户的身份信息和随机信息按预设的顺序进行拼接后，对拼接得到的信息进行加密处理，得到用户认证口令。

[0194] 第一交互单元02负责将生成的用户认证口令发送给用户终端。

[0195] 标识维护单元04利用用户认证口令，生成第一设备身份标识后，再由第二交互单元03将标识维护单元04生成的第一设备身份标识返回给终端设备，并由绑定处理单元05保存用户的身份信息与第一设备身份标识之间的绑定关系。

[0196] 其中标识维护单元04可以仅利用用户认证口令生成第一设备身份标识，例如将用

户认证口令采用安全哈希算法进行处理，得到第一设备身份标识，甚至可以直接将用户认证口令作为第一设备身份标识。

[0197] 标识维护单元04也可以利用终端设备信息和用户认证口令，生成第一设备身份标识。例如将终端设备信息和用户认证口令按预设的顺序进行拼接后，采用安全哈希算法对拼接得到的信息进行处理，得到第一设备身份标识。

[0198] 另外，用户认证口令可以存在一定的有效期，在第二交互单元03接收到第一请求后，口令验证单元06可以判断第一请求包含的用户认证口令是否超出有效期，如果是，则触发第二交互单元03向终端设备返回注册失败的响应；否则，触发标识维护单元04执行上述利用第一请求包含的终端设备信息和用户认证口令，生成第一设备身份标识的操作。

[0199] 若第二交互单元03接收到的第一请求中不包含用户认证口令，则标识维护单元04可以利用接收到的第一请求中包含的终端设备信息，生成第二设备身份标识。第二交互单元03将第二设备身份标识返回给终端设备和/或用户终端。

[0200] 上述第一交互单元02会接收到携带第一设备身份标识的注销请求。标识维护单元04依据注销请求中携带的第一设备身份标识，解除第一设备身份标识。绑定处理单元05依据注销请求中携带的第一设备身份标识，删除用户的身份信息与第一设备身份标识之间的绑定关系。

[0201] 第二交互单元03接收到终端设备的登录请求后，登录处理单元07可以判断登录请求包含的第一设备身份标识是否被解除，如果是，则登录失败；否则登录成功。

[0202] 对于用户终端和终端设备之间的数据交互，可以由转发处理单元08处理。即在第二交互单元03接收到终端设备发送的包含第一设备身份标识的数据请求时，转发处理单元08判断本地是否存在数据请求所包含第一设备身份标识的绑定关系，如果是，则将数据请求通过第一交互单元02转发至与第一设备身份标识存在绑定关系的用户身份信息对应的用户终端，否则拒绝数据请求。

[0203] 在第一交互单元02接收到用户发送的数据请求时，转发处理单元08判断本地是否存在与用户的身份信息存在绑定关系的第一设备身份标识，如果是，则通过第二交互单元03将数据请求转发至第一设备身份标识对应的终端设备；否则，拒绝数据请求。

[0204] 上述装置可以应用于终端设备的身份注册流程中，在这种应用场景下，上述的第一请求为身份注册请求，第二请求为获取认证口令的请求。

[0205] 图7为本发明实施例提供的设置于用户终端的装置结构图，如图7中所示，该装置包括：服务端交互单元11和终端交互单元12。各组成单元的主要功能如下：

[0206] 服务端交互单元11负责从服务器端获取用户认证口令。具体地，服务端交互单元11可以向服务器端发送获取认证口令的请求；接收服务器端利用用户的身份信息生成并返回的用户认证口令。

[0207] 终端交互单元12负责将用户认证口令发送给终端设备以触发终端设备从服务器端获取所述终端设备对应的第一设备身份标识。还可以进一步接收终端设备返回的第一设备身份标识。

[0208] 具体地，终端交互单元12可以利用局域网或者近距离通信方式将用户认证口令发送给终端设备。其中近距离通信方式可以包括但不限于蓝牙、红外、NFC等。

[0209] 当用户希望解除某终端设备的认证以及绑定关系时，可以由服务端交互单元11向

服务器端发送注销请求，该注销请求中携带第一设备身份标识。

[0210] 另外，当用户希望向与其绑定的终端设备发送数据时，可以将该数据携带在数据请求中向服务器端发送，或者，当用户希望获取与其绑定的终端设备的数据时，也可以将所请求数据的信息携带在数据请求中向服务器端发送。即由服务端交互单元11向服务器端发送包含第一设备身份标识的数据请求。

[0211] 图8为本发明实施例提供的设置于终端设备的装置结构图，如图8中所示，该装置可以包括：用户端交互单元21、服务端交互单元22和标识保存单元23，各组成单元的主要功能如下：

[0212] 用户端交互单元21负责从用户终端接收用户认证口令。

[0213] 服务端交互单元22负责向服务器端发送包含终端设备信息和用户认证口令的第一请求；接收服务器端返回的第一设备身份标识。

[0214] 标识保存单元23负责保存服务端交互单元22接收到的第一设备身份标识。

[0215] 再由用户端交互单元21将服务端交互单元22接收到的第一设备身份标识返回给用户终端。

[0216] 另外，服务端交互单元22可以向服务器端发送包含第一设备身份标识的登录请求；如果登陆失败，则向服务器端发送包含终端设备信息的第一请求；接收服务器端返回的第二设备身份标识。由标识保存单元23利用第二设备身份标识替换本地保存的第一设备身份标识。

[0217] 上述第一设备身份标识是服务器端利用终端设备信息和用户认证口令生成的，第二设备身份标识是服务器端仅利用终端设备信息生成的。

[0218] 当该装置应用于终端设备的身份注册时，上述第一请求可以为注册请求。

[0219] 用户端交互单元21可以通过局域网或近距离通信方式从用户端接收用户认证口令。其中近距离通信方式可以包括但不限于蓝牙、红外、NFC等。

[0220] 服务端交互单元22后续向服务器端发送数据请求时，在数据请求中携带标识保存单元23保存的设备身份标识。

[0221] 本发明提供的上述方法和装置能够被广泛地应用于物联网中，例如用户通过手机APP采用上述方式触发设置于固定地点的火警探头进行身份注册，并成功与该火警探头绑定。当该火警探头探测到异常数据时，就能够向服务器端发送包含该异常数据的数据请求，由服务器端根据身份注册过程中保存的用户的身份信息与该火警探头的身份标识之间的绑定关系，将异常数据转发给用户的手机APP。由于是手机APP从服务器端获取用户认证口令后，将用户认证口令提供给火警探头并触发火警探头向服务器请求的身份注册，在身份注册过程中服务器端需要利用用户认证口令针对火警探头生成设备身份标识，即便存在克隆设备获取了该火警探头的原始物理信息，但由于无法获取用户认证口令，因此无法仿冒火警探头的身份而产生攻击数据或虚假数据。

[0222] 在本发明所提供的几个实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，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。

[0223] 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。

[0224] 另外，在本发明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，也可以采用硬件加软件功能单元的形式实现。

[0225] 上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元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(可以是个人计算机，服务器，或者网络设备等)或处理器(processor)执行本发明各个实施例所述方法的部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0226] 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，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

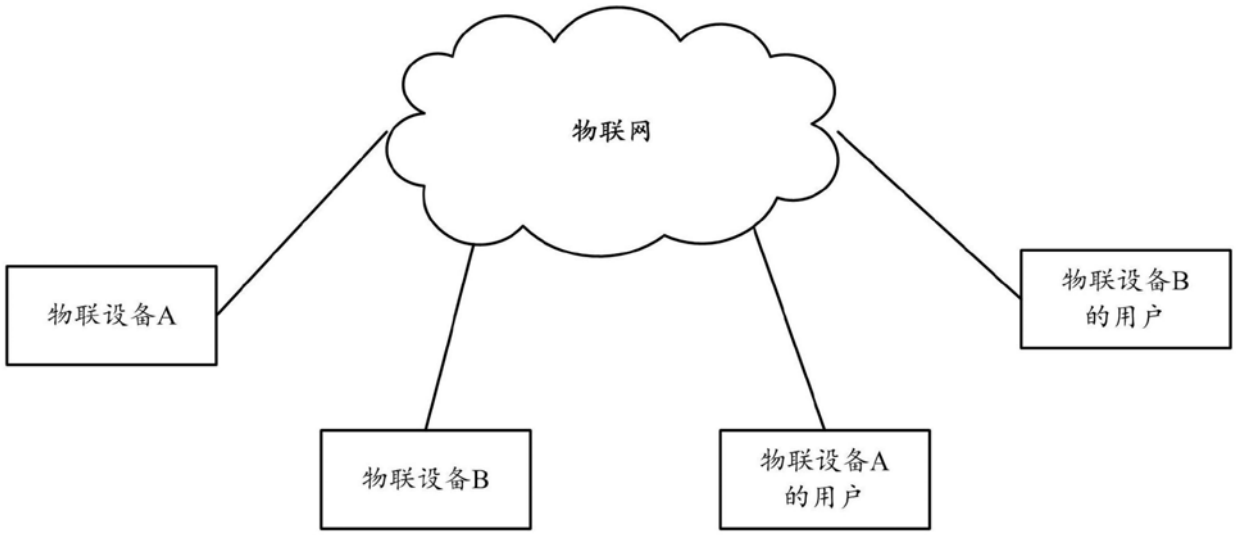

物联网
物联设备A
物联设备B
物联设备A
的用户
物联设备B
的用户

图1

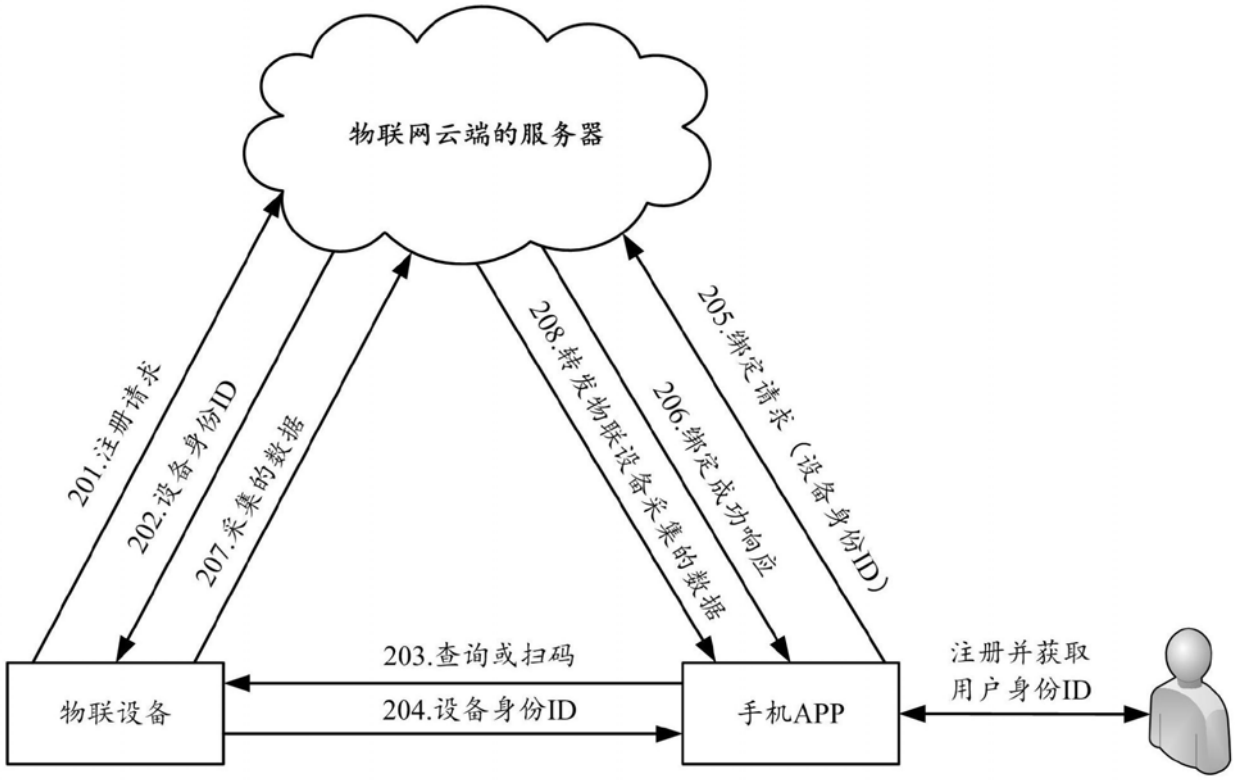

物联网云端的服务器
201.注册请求
202.设备身份ID
207.采集的数据
208.转发物联设备采集的数据
206.绑定成功响应
205.绑定请求（设备身份ID）
203.查询或扫码
204.设备身份ID
注册并获取
用户身份ID
物联设备
手机APP

图2

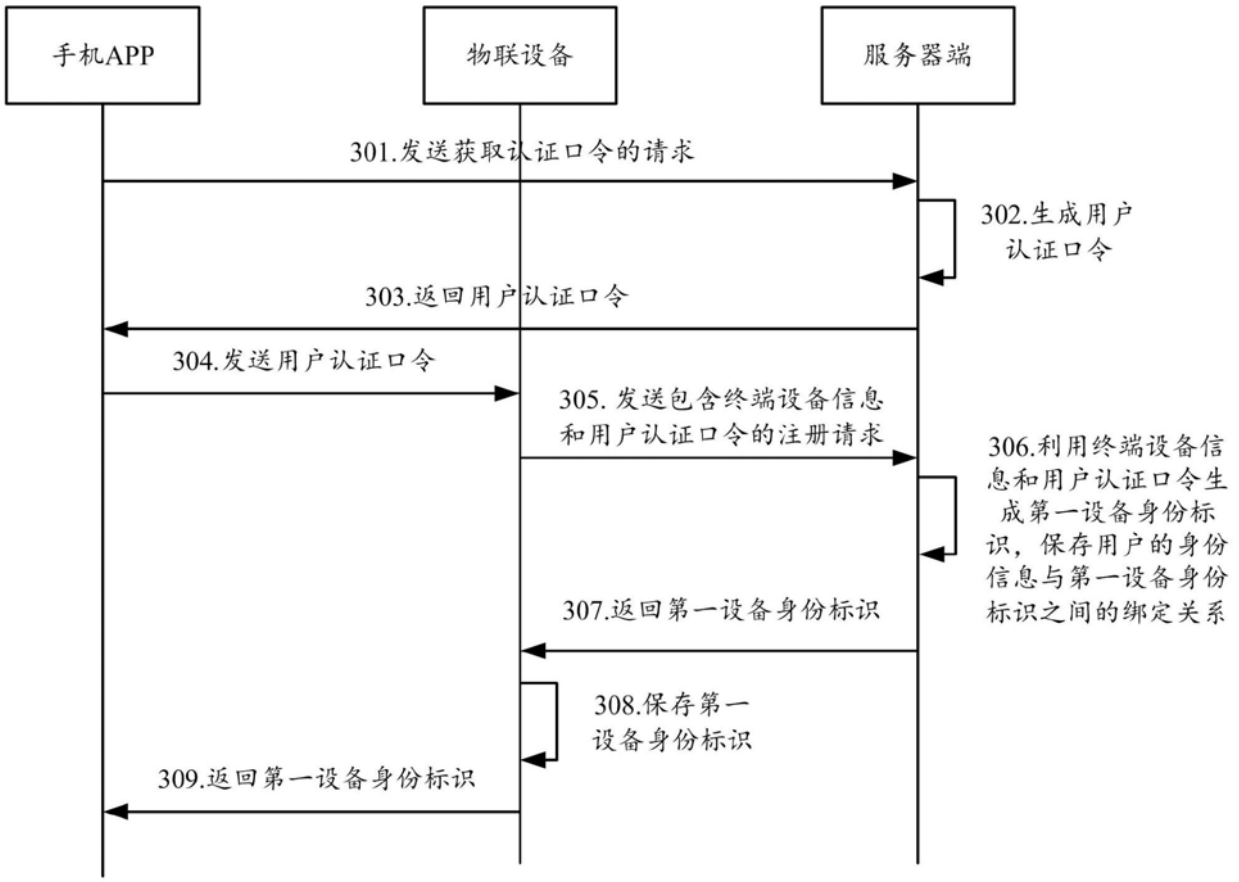

手机APP
物联设备
服务器端
301.发送获取认证口令的请求
302.生成用户认证口令
303.返回用户认证口令
304.发送用户认证口令
305. 发送包含终端设备信息和用户认证口令的注册请求
306.利用终端设备信息和用户认证口令生成第一设备身份标识，保存用户的身份信息与第一设备身份标识之间的绑定关系
307.返回第一设备身份标识
308.保存第一设备身份标识
309.返回第一设备身份标识

图3

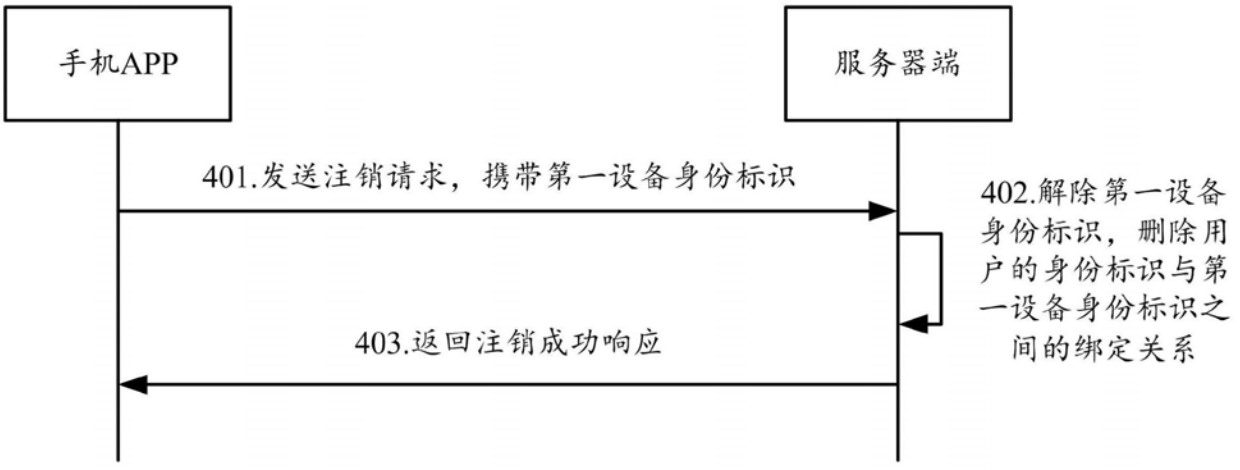

手机APP
服务器端
401.发送注销请求，携带第一设备身份标识
402.解除第一设备身份标识，删除用户的身份标识与第一设备身份标识之间的绑定关系
403.返回注销成功响应

图4

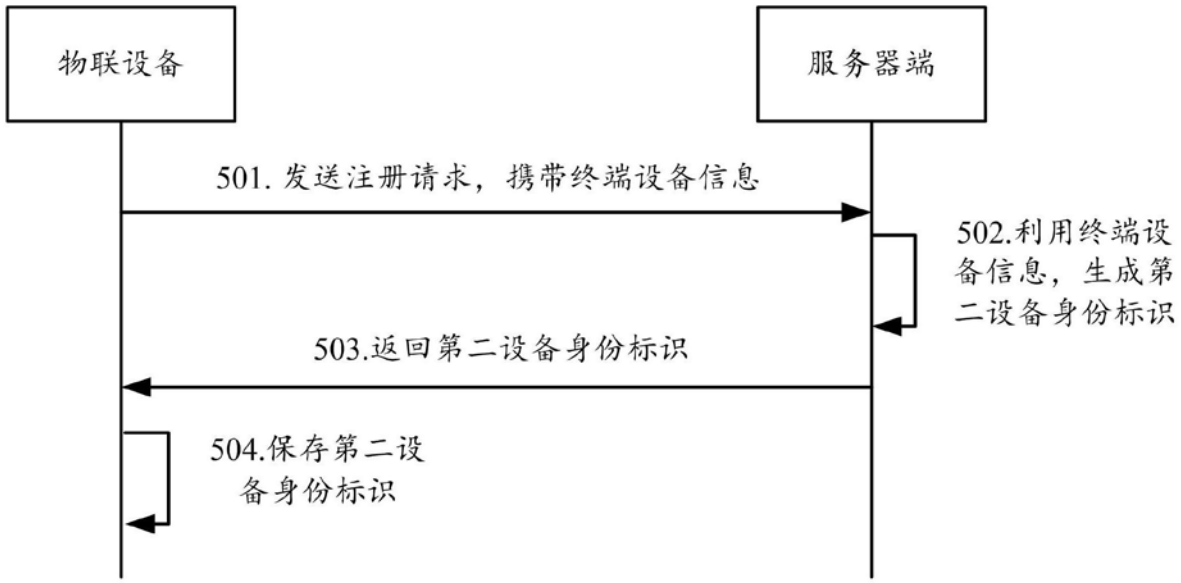

物联设备
服务器端
501. 发送注册请求，携带终端设备信息
502.利用终端设备信息，生成第二设备身份标识
503.返回第二设备身份标识
504.保存第二设备身份标识

图5

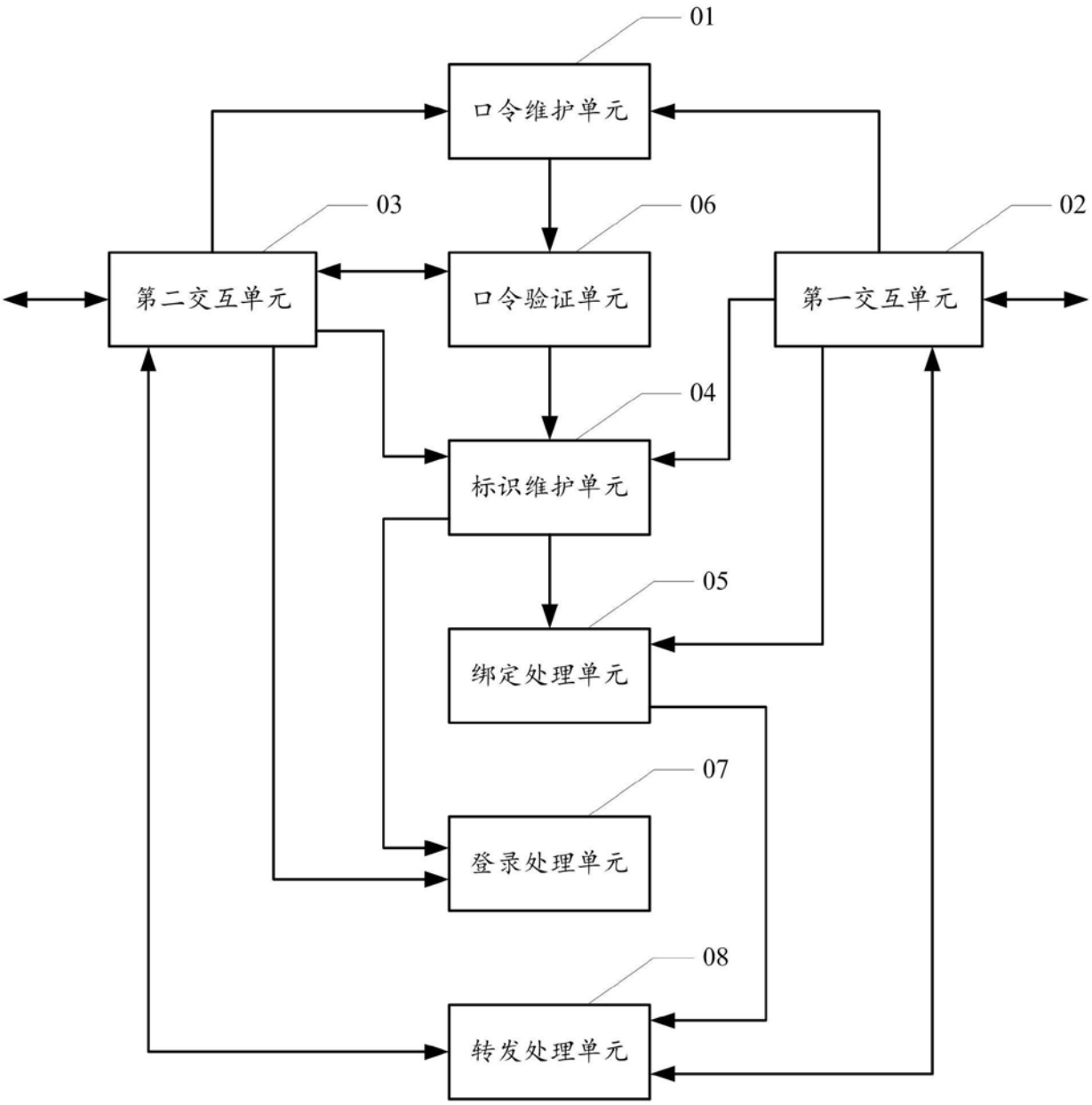

01
口令维护单元
03
06
02
第二交互单元
口令验证单元
第一交互单元
04
标识维护单元
05
绑定处理单元
07
登录处理单元
08
转发处理单元

图6

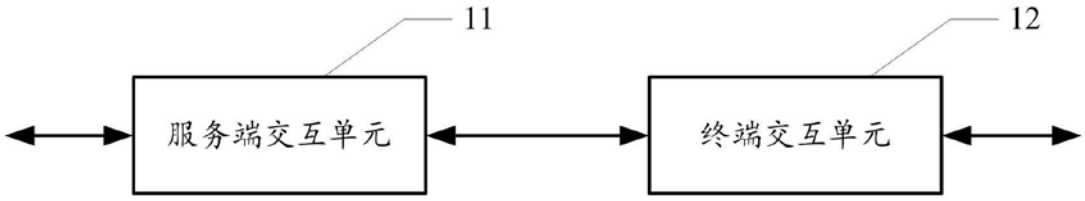

11
12
服务端交互单元
终端交互单元

图7

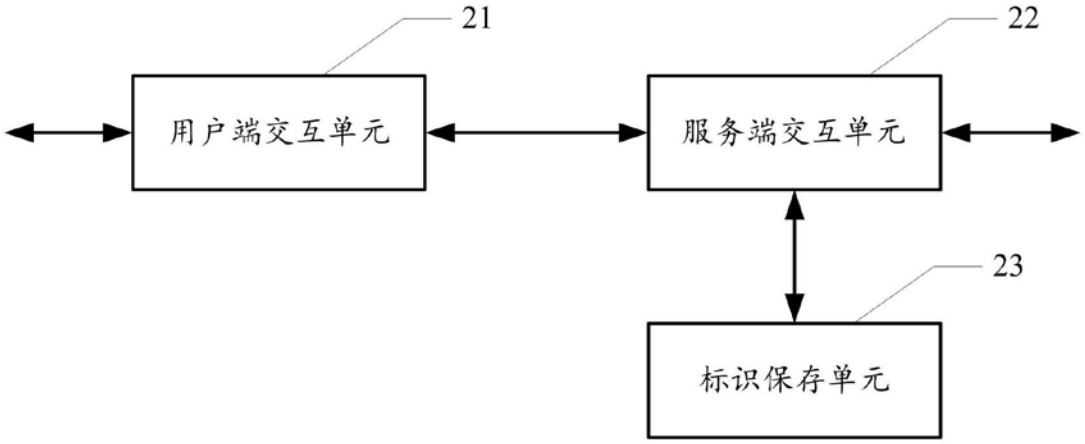


图8