(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 105450403 B
(45)授权公告日 2019.09.17

(21)申请号 201410313308.1

(22)申请日 2014.07.02

(65)同一申请的已公布的文献号
申请公布号 CN 105450403 A

(43)申请公布日 2016.03.30

(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 黄冕

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
US 2011/0219427 A1,2011.09.08,说明书第[0012]-[0079]和[0124]段,附图1-5.
US 8625796 B1,2014.01.07,全文.
CN 102300182 A,2011.12.28,全文.
CN 101023651 A,2007.08.22,全文.
EP 2482575 A1,2012.08.01,说明书第[0020]-[0028]段,附图1-2.

审查员 牛爽

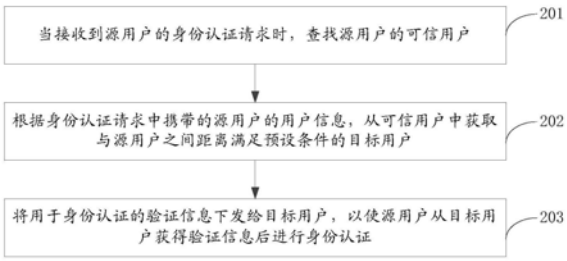
权利要求书4页 说明书10页 附图5页

(54)发明名称

身份认证方法、装置及服务器

(57)摘要

本申请实施例公开了身份认证方法、装置及服务器,所述方法包括:当接收到源用户的身份认证请求时,查找所述源用户的可信用户;根据所述身份认证请求中携带的源用户的用户信息,从所述可信用户中获取与所述源用户之间距离满足预设条件的目标用户;将用于所述身份认证的验证信息下发给所述目标用户,以使所述源用户从所述目标用户获得所述验证信息后进行身份认证。本申请实施例可以应用用户之间的社会网络关系信息,结合用户之间的位置信息,将验证信息下发给用户的亲友等可信人员所持有的用户终端,从而保证了用户身份验证的可靠性,即使用户的终端被恶意第三方盗取,也无法通过该终端进行身份验证,从而提高了身份验证的安全性。



CN 105450403 B

1.一种身份认证方法,其特征在于,所述方法包括:

当接收到源用户的身份认证请求时,从预先确定的可信度值中获取高于可信度阈值的可信度值,将获取的可信度值对应的关联用户确定为所述源用户的可信用户,其中,所述可信度值通过如下方式确定:根据所述源用户的历史用户信息,确定和所述源用户关联的关联用户以及关联用户的历史用户信息;根据所述历史用户信息计算所述源用户与关联用户之间的可信度值;

根据所述身份认证请求中携带的源用户的用户信息,从所述可信用户中获取与所述源用户之间距离满足预设条件的目标用户;

将用于所述身份认证的验证信息下发给所述目标用户,以使所述源用户从所述目标用户获得所述验证信息后进行身份认证。

2.根据权利要求1所述的方法,其特征在于,所述根据所述历史用户信息计算所述源用户与关联用户之间的可信度值包括:

当所述历史用户信息包括定位服务LBS信息时,根据所述LBS信息计算所述源用户与所述关联用户在预设时间周期内位于同一位置的位置可信度值。

3.根据权利要求1所述的方法,其特征在于,所述根据所述历史用户信息计算所述源用户与关联用户之间的可信度值包括:

当所述历史用户信息包括WIFI热点扫描信息时,根据所述扫描信息计算所述源用户与所述关联用户在预设时间周期内通过同一WIFI热点接入无线网络的网络连接可信度值。

4.根据权利要求1所述的方法,其特征在于,所述根据所述历史用户信息计算所述源用户与关联用户之间的可信度值包括:

当所述历史用户信息包括通信信息时,根据所述通信信息计算所述源用户与所述关联用户在预设时间周期内的通信频次可信度值。

5.根据权利要求1所述的方法,其特征在于,所述从所述可信用户中获取与所述源用户之间距离满足预设条件的目标用户包括:

根据当前所述源用户和所述可信用户的LBS信息,从所述可信用户中获取与所述源用户当前位于同一位置的目标用户。

6.根据权利要求1所述的方法,其特征在于,所述从所述可信用户中获取与所述源用户之间距离满足预设条件的目标用户包括:

根据当前所述源用户和所述可信用户的WIFI热点扫描信息,从所述可信用户中获取与所述源用户当前通过同一WIFI热点接入无线网络的目标用户。

7.根据权利要求1至6任意一项所述的方法,其特征在于,所述将用于所述身份认证的验证信息下发给所述目标用户包括:

当所述目标用户包括多个用户时,将所述多个用户的用户列表下发给所述源用户;

获取所述源用户从所述用户列表中选择的一个用户;

将用于所述身份认证的验证信息下发给所述源用户选择的一个用户。

8.一种身份认证方法,其特征在于,所述方法包括:

当接收到源用户的身份认证请求时,根据所述身份认证请求中携带的源用户的用户信息获取与所述源用户之间距离满足预设条件的目标用户;

从预先确定的可信度值中获取高于可信度阈值的可信度值,当获取的可信度值对应的

关联用户属于所述目标用户时，将所述对应的关联用户确定为所述源用户的可信用户，其中，所述可信度值通过如下方式确定：根据所述源用户的历史用户信息，确定和所述源用户关联的关联用户以及关联用户的历史用户信息；根据所述历史用户信息计算所述源用户与关联用户之间的可信度值；

将用于所述身份认证的验证信息下发给所述可信用户，以使所述源用户从所述可信用户获得所述验证信息后进行身份认证。

9.根据权利要求8所述的方法，其特征在于，所述根据所述身份认证请求中携带的源用户的用户信息获取与所述源用户之间距离满足预设条件的目标用户包括：

根据所述身份认证请求中携带的源用户的LBS信息和当前所有用户的LBS信息，从所有用户中获取与所述源用户当前位于同一位置的目标用户。

10.根据权利要求8所述的方法，其特征在于，所述根据所述身份认证请求中携带的源用户的用户信息获取与所述源用户之间距离满足预设条件的目标用户包括：

根据所述身份认证请求中携带的源用户的WIFI热点扫描信息和当前所有用户的WIFI热点扫描信息，从所述所有用户中获取与所述源用户当前通过同一WIFI热点接入无线网络的目标用户。

11.根据权利要求8至10任意一项所述的方法，其特征在于，所述将用于所述身份认证的验证信息下发给所述可信用户包括：

当所述可信用户包括多个用户时，将所述多个用户的用户列表下发给所述源用户；

获取所述源用户从所述用户列表中选择的一个用户；

将用于身份认证的验证信息下发给所述源用户选择的一个用户。

12.一种身份认证装置，其特征在于，所述装置包括：

第一确定单元，用于根据源用户的历史用户信息，确定和所述源用户关联的关联用户以及关联用户的历史用户信息；

第一计算单元，用于根据所述历史用户信息计算所述源用户与关联用户之间的可信度值；

第一查找单元，用于当接收到源用户的身份认证请求时，从所述可信度值中获取高于可信度阈值的可信度值，将获取的可信度值对应的关联用户确定为所述源用户的可信用户；

第一获取单元，用于根据所述身份认证请求中携带的源用户的用户信息，从所述可信用户中获取与所述源用户之间距离满足预设条件的目标用户；

第一下发单元，用于将用于所述身份认证的验证信息下发给所述目标用户，以使所述源用户从所述目标用户获得所述验证信息后进行身份认证；

所述第一查找单元，具体用于从所述可信度值中获取高于可信度阈值的可信度值，将获取的可信度值对应的关联用户确定为所述源用户的可信用户。

13.根据权利要求12所述的装置，其特征在于，所述第一计算单元包括至少一个下述子单元：

第一位置可信度值计算子单元，用于当所述历史用户信息包括定位服务LBS信息时，根据所述LBS信息计算所述源用户与所述关联用户在预设时间周期内位于同一位置的位置可信度值；

第一网络连接可信度值计算子单元，用于当所述历史用户信息包括WIFI热点扫描信息时，根据所述扫描信息计算所述源用户与所述关联用户在预设时间周期内通过同一WIFI热点接入无线网络的网络连接可信度值；

第一通信频次可信度值计算子单元，用于当所述历史用户信息包括通信信息时，根据所述通信信息计算所述源用户与所述关联用户在预设时间周期内的通信频次可信度值。

14.根据权利要求12所述的装置，其特征在于，所述第一获取单元包括至少一个下述子单元：

第一位置目标获取子单元，用于根据当前所述源用户和所述可信用户的LBS信息，从所述可信用户中获取与所述源用户当前位于同一位置的目标用户；

第一热点目标获取子单元，用于根据当前所述源用户和所述可信用户的WIFI热点扫描信息，从所述可信用户中获取与所述源用户当前通过同一WIFI热点接入无线网络的目标用户。

15.根据权利要求12至14任意一项所述的装置，其特征在于，所述第一下发单元包括：

第一列表下发子单元，用于当所述目标用户包括多个用户时，将所述多个用户的用户列表下发给所述源用户；

第一选择获取子单元，用于获取所述源用户从所述用户列表中选择的一个用户；

第一信息下发子单元，用于将用于所述身份认证的验证信息下发给所述源用户选择的一个用户。

16.一种身份认证装置，其特征在于，所述装置包括：

第二确定单元，用于根据源用户的历史用户信息，确定和所述源用户关联的关联用户以及关联用户的历史用户信息；

第二计算单元，用于根据所述历史用户信息计算所述源用户与关联用户之间的可信度值；

第二获取单元，用于当接收到源用户的身份认证请求时，根据所述身份认证请求中携带的源用户的用户信息获取与所述源用户之间距离满足预设条件的目标用户；

第二查找单元，用于从所述可信度值中获取高于可信度阈值的可信度值，当获取的可信度值对应的关联用户属于所述目标用户时，将所述对应的关联用户确定为所述源用户的可信用户；

第二下发单元，用于将用于所述身份认证的验证信息下发给所述可信用户，以使所述源用户从所述可信用户获得所述验证信息后进行身份认证。

17.根据权利要求16所述的装置，其特征在于，所述第二获取单元包括至少一个下述子单元：

第二位置目标获取子单元，用于根据所述身份认证请求中携带的源用户的LBS信息和当前所有用户的LBS信息，从所有用户中获取与所述源用户当前位于同一位置的目标用户；

第二热点目标获取子单元，用于根据所述身份认证请求中携带的源用户的WIFI热点扫描信息和当前所有用户的WIFI热点扫描信息，从所述所有用户中获取与所述源用户当前通过同一WIFI热点接入无线网络的目标用户。

18.根据权利要求16至17任意一项所述的装置，其特征在于，所述第二下发单元包括：

第二列表下发子单元，用于当所述可信用户包括多个用户时，将所述多个用户的用户

列表下发给所述源用户；

第二选择获取子单元，用于获取所述源用户从所述用户列表中选择的一个用户；

第二信息下发子单元，用于将用于身份认证的验证信息下发给所述源用户选择的一个用户。

19.一种服务器，其特征在于，所述服务器包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

当接收到源用户的身份认证请求时，从预先确定的可信度值中获取高于可信度阈值的可信度值，将获取的可信度值对应的关联用户确定为所述源用户的可信用户，其中，所述可信度值通过如下方式确定：根据所述源用户的历史用户信息，确定和所述源用户关联的关联用户以及关联用户的历史用户信息；根据所述历史用户信息计算所述源用户与关联用户之间的可信度值；

根据所述身份认证请求中携带的源用户的用户信息，从所述可信用户中获取与所述源用户之间距离满足预设条件的目标用户；

将用于所述身份认证的验证信息下发给所述目标用户，以使所述源用户从所述目标用户获得所述验证信息后进行身份认证。

20.一种服务器，其特征在于，所述服务器包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

当接收到源用户的身份认证请求时，根据所述身份认证请求中携带的源用户的用户信息获取与所述源用户之间距离满足预设条件的目标用户；

从预先确定的可信度值中获取高于可信度阈值的可信度值，当获取的可信度值对应的关联用户属于所述目标用户时，将所述对应的关联用户确定为所述源用户的可信用户，其中，所述可信度值通过如下方式确定：根据所述源用户的历史用户信息，确定和所述源用户关联的关联用户以及关联用户的历史用户信息；根据所述历史用户信息计算所述源用户与关联用户之间的可信度值；

将用于所述身份认证的验证信息下发给所述可信用户，以使所述源用户从所述可信用户获得所述验证信息后进行身份认证。

身份认证方法、装置及服务器

技术领域

[0001] 本申请涉及移动通信技术领域，尤其涉及身份认证方法、装置及服务器。

背景技术

[0002] 随着智能终端的发展和网络应用的开发，用户可以通过终端上安装的应用(Application，APP)客户端对各种网络应用进行访问，在访问过程中，经常需要通过终端对用户身份进行双通道认证，例如，当用户忘记某个APP的登录密码时，向APP服务器发送密码找回请求后，APP服务器会通过短信向终端返回校验信息，用户输入该校验信息，APP服务器验证该校验信息正确后，就能够确认用户身份通过验证，从而向用户返回密码。

[0003] 然而，由于安装APP的终端与身份验证时接收校验信息的终端为同一个终端，因此当终端被恶意第三方盗取，或者终端被恶意软件入侵时，很容易通过该终端实现用户身份认证，从而导致身份验证的安全性不高，用户的私人信息容易被盗取。

发明内容

[0004] 本申请提供身份认证方法、装置及服务器，以解决现有通过终端实现双通道认证安全性不高的问题。

[0005] 根据本申请实施例的第一方面，提供一种身份认证方法，所述方法包括：

[0006] 当接收到源用户的身份认证请求时，查找所述源用户的可信用户；

[0007] 根据所述身份认证请求中携带的源用户的用户信息，从所述可信用户中获取与所述源用户之间距离满足预设条件的目标用户；

[0008] 将用于所述身份认证的验证信息下发给所述目标用户，以使所述源用户从所述目标用户获得所述验证信息后进行身份认证。

[0009] 根据本申请实施例的第二方面，提供另一种身份认证方法，所述方法包括：

[0010] 当接收到源用户的身份认证请求时，根据所述身份认证请求中携带的源用户的用户信息获取与所述源用户之间距离满足预设条件的目标用户；

[0011] 从所述目标用户中查找所述源用户的可信用户；

[0012] 将用于所述身份认证的验证信息下发给所述可信用户，以使所述源用户从所述可信用户获得所述验证信息后进行身份认证。

[0013] 根据本申请实施例的第三方面，提供一种身份认证装置，所述装置包括：

[0014] 第一查找单元，用于当接收到源用户的身份认证请求时，查找所述源用户的可信用户；

[0015] 第一获取单元，用于根据所述身份认证请求中携带的源用户的用户信息，从所述可信用户中获取与所述源用户之间距离满足预设条件的目标用户；

[0016] 第一下发单元，用于将用于所述身份认证的验证信息下发给所述目标用户，以使所述源用户从所述目标用户获得所述验证信息后进行身份认证。

[0017] 根据本申请实施例的第四方面，提供另一种身份认证装置，所述装置包括：

[0018] 第二获取单元，用于当接收到源用户的身份认证请求时，根据所述身份认证请求中携带的源用户的用户信息获取与所述源用户之间距离满足预设条件的目标用户；

[0019] 第二查找单元，用于从所述目标用户中查找所述源用户的可信用户；

[0020] 第二下发单元，用于将用于所述身份认证的验证信息下发给所述可信用户，以使所述源用户从所述可信用户获得所述验证信息后进行身份认证。

[0021] 根据本申请实施例的第五方面，提供一种服务器，所述服务器包括：

[0022] 处理器；

[0023] 用于存储处理器可执行指令的存储器；

[0024] 其中，所述处理器被配置为：

[0025] 当接收到源用户的身份认证请求时，查找所述源用户的可信用户；

[0026] 根据所述身份认证请求中携带的源用户的用户信息，从所述可信用户中获取与所述源用户之间距离满足预设条件的目标用户；

[0027] 将用于所述身份认证的验证信息下发给所述目标用户，以使所述源用户从所述目标用户获得所述验证信息后进行身份认证。

[0028] 根据本申请实施例的第六方面，提供另一种服务器，所述服务器包括：

[0029] 处理器；

[0030] 用于存储处理器可执行指令的存储器；

[0031] 其中，所述处理器被配置为：

[0032] 当接收到源用户的身份认证请求时，根据所述身份认证请求中携带的源用户的用户信息获取与所述源用户之间距离满足预设条件的目标用户；

[0033] 从所述目标用户中查找所述源用户的可信用户；

[0034] 将用于所述身份认证的验证信息下发给所述可信用户，以使所述源用户从所述可信用户获得所述验证信息后进行身份认证。

[0035] 应用本申请实施例对源用户进行身份认证时，可以按照源用户与其可信用户之间的距离关系筛选出距离源用户较近的目标用户，并将验证信息下发给目标用户，从而使得源用户可以从目标用户处获得验证信息并完成身份认证。本申请应用用户之间的社会网络关系信息，结合用户之间的位置信息，可以将验证信息下发给用户的亲友等可信人员所持有的终端，从而保证了用户身份验证的可靠性，即使用户的终端被恶意第三方盗取，也无法通过该终端进行身份验证，从而提高了身份验证的安全性。

[0036] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本申请。

附图说明

[0037] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本申请的实施例，并与说明书一起用于解释本申请的原理。

[0038] 图1是本申请实施例的应用场景示意图；

[0039] 图2A是本申请身份认证方法的一个实施例流程图；

[0040] 图2B是本申请身份认证方法的另一个实施例流程图；

[0041] 图3是本申请身份认证方法的另一个实施例流程图；

[0042] 图4是本申请身份认证装置的一个实施例框图；

[0043] 图5是本申请身份认证装置的另一个实施例框图；

[0044] 图6是本申请身份认证装置的另一个实施例框图；

[0045] 图7是本申请服务器的实施例框图。

具体实施方式

[0046] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0047] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0048] 在基于互联网通信的场景中，用户可以通过所持终端上安装的各种APP客户端实现对各种网络应用的访问，在访问过程中，经常需要通过终端对用户身份进行双通道认证。现有技术中在对源用户进行身份认证时，由源用户采用自身终端进行双通道身份认证，而本申请实施例中源用户可以采用可信用户的终端进行双通道身份认证。参见图1，为本申请实施例实现身份认证的应用场景示意图，其中n个用户的终端与服务器之间的通信过程基于互联网完成，当用户1要进行身份认证时，服务器可以将验证信息下发给该用户1信任的且与用户1距离相近的用户2，从而提高身份认证的可靠性和安全性，下面对本申请实施例进行详细说明。

[0049] 参见图2A，为本申请身份认证方法的一个实施例流程图，该实施例从服务器侧描述了一种身份认证过程：

[0050] 步骤201：当接收到源用户的身份认证请求时，查找源用户的可信用户。

[0051] 本申请实施例中，将待进行身份认证的用户统称为源用户，通常源用户所持有的终端上安装了各种APP，例如，常见的即时通信APP，当服务器监测到源用户的终端登录APP的IP(Internet Protocol，互联网协议)地址与惯常登录APP的IP地址不一致时，会对源用户进行身份认证。

[0052] 本申请实施例在对源用户进行身份认证时，采用源用户的可信用户所持有的终端实现双通道身份认证，因此服务器可以根据源用户的历史用户信息，确定和源用户关联的关联用户以及关联用户的历史用户信息，根据历史用户信息计算源用户与关联用户之间的可信度值，然后从可信度值中获取高于可信度阈值的可信度值，将获取的可信度值对应的关联用户确定为源用户的可信用户。

[0053] 其中，对于任意源用户来说，在确定其关联用户时，可以根据源用户上报的联系人信息确定其关联用户，或者也可以根据与源用户通过所安装的同一APP进行互动的好友确定其关联用户。参照图1，由于不同用户均可以通过终端与所安装的APP对应的APP服务器进行通信，因此这些终端可以按照预设的上报周期向服务器上报用户的用户信息，该预设的上报周期可以灵活设置，例如，设置上报周期为30分钟，本实施例中，用户信息可以包括LBS

(Location Based Services,定位服务)信息,WIFI(Wireless Fidelity,无线保真)热点扫描信息,通讯录中的联系人信息(联系人信息可以为通过哈希算法处理后的信息),通信信息(可以包括与任一联系人收发短信的次数,或者与任一联系人通话的次数)等。

[0054] 其中,根据用户信息类型的不同,可以采用多种方式计算源用户与关联用户之间的可信度值,包括:当用户信息包括LBS信息时,可以根据源用户与关联用户的LBS信息计算源用户与关联用户在预设时间周期内位于同一位置的位置可信度值;或者,当用户信息包括WIFI热点扫描信息时,可以根据源用户与关联用户的WIFI热点扫描信息计算源用户与关联用户在预设时间周期内通过同一WIFI热点接入无线网络的网络连接可信度值;或者,当用户信息包括通信信息时,可以根据源用户与关联用户的通信信息计算源用户与关联用户在预设时间周期内的通信频次可信度值。上述计算可信度值时的预设时间周期可以灵活设置,例如,预设时间周期为一年。

[0055] 步骤202:根据身份认证请求中携带的源用户的用户信息,从可信用户中获取与源用户之间距离满足预设条件的目标用户。

[0056] 本实施例中,当服务器查找到源用户的可信用户后,可以根据当前源用户和可信用户的位置信息选择距离源用户距离较近的目标用户。例如,服务器可以根据当前源用户和可信用户的LBS信息,从可信用户中获取与源用户当前位于同一位置的用户作为目标用户;或者,服务器也可以根据当前源用户和可信用户的WIFI热点扫描信息,从可信用户中获取与源用户当前通过同一WIFI热点接入无线网络的用户作为目标用户。

[0057] 步骤203:将用于身份认证的验证信息下发给目标用户,以使源用户从目标用户获得验证信息后进行身份认证。

[0058] 当服务器获取到源用户的一个目标用户时,可以直接将验证信息下发给该目标用户;当服务器获取到的目标用户包括多个用户时,可以将多个用户的用户列表下发给源用户,源用户从用户列表中选择一个目标用户,并通过源用户的终端将选择结果返回给服务器,服务器将验证信息下发给源用户选择的目标用户。

[0059] 参见图2B,为本申请身份认证方法的另一个实施例流程图,该实施例从服务器侧描述了另一种身份认证过程:

[0060] 步骤211:当接收到源用户的身份认证请求时,根据身份认证请求中携带的源用户的用户信息获取与源用户之间距离满足预设条件的目标用户。

[0061] 本步骤中,可以根据所述身份认证请求中携带的源用户的LBS信息和当前所有用户的LBS信息,从所有用户中获取与所述源用户当前位于同一位置的目标用户;也可以根据所述身份认证请求中携带的源用户的WIFI热点扫描信息和当前所有用户的WIFI热点扫描信息,从所述所有用户中获取与所述源用户当前通过同一WIFI热点接入无线网络的目标用户。

[0062] 步骤212:从目标用户中查找源用户的可信用户。

[0063] 本实施例中,在接收到源用户的身份认证请求前,可以根据所述源用户的历史用户信息,确定和所述源用户关联的关联用户以及关联用户的历史用户信息,根据所述历史用户信息计算所述源用户与关联用户之间的可信度值。在获取到目标用户时,从所述可信度值中获取高于可信度阈值的可信度值,当获取的可信度值对应的关联用户属于所述目标用户时,将所述对应的关联用户确定为所述源用户的可信用户。

[0064] 本实施例中，根据用户信息类型的不同，可以采用多种方式计算源用户与关联用户之间的可信度值，具体计算方式可以参见图2A步骤201中的相关描述，在此不再赘述。

[0065] 步骤213：将用于身份认证的验证信息下发给可信用户，以使源用户从可信用户获得验证信息后进行身份认证。

[0066] 本步骤中，当所述可信用户包括多个用户时，将所述多个用户的用户列表下发给所述源用户，获取所述源用户从所述用户列表中选择的一个用户，将用于身份认证的验证信息下发给所述源用户选择的一个用户。

[0067] 图2B示出的实施例与图2A示出的实施例不同在于，图2A中先获取源用户的可信用户，再从可信用户中获取用于接收验证信息的目标用户，而图2B中先获取与源用户满足距离条件的目标用户，再从目标用户中查找用户接收验证信息的可信用户。无论采用哪种方式，最终接收验证信息的用户都是在源用户附近且是该源用户的可信用户的用户。

[0068] 由上述方法实施例可见，该实施例可以应用用户之间的社会网络关系信息，结合用户之间的位置信息，将验证信息下发给用户的亲友等可信人员所持有的终端，从而保证了用户身份验证的可靠性，即使用户的终端被恶意第三方盗取，也无法通过该终端进行身份验证，从而提高了身份验证的安全性。

[0069] 参见图3，为本申请身份认证方法的另一个实施例流程图，该实施例通过用户终端与服务器之间的交互详细描述了身份认证过程：

[0070] 步骤301：用户终端按照预设上报周期向服务器上报用户信息。

[0071] 本实施例中，用户终端上可以安装各种APP客户端，在用户使用APP的过程中，APP客户端通过用户终端与APP服务器进行交互，在交互过程中，用户终端可以按照预设上报周期向服务器上报用户信息。

[0072] 其中，用户信息可以包括：LBS信息，该信息为通过移动网络运营商的无线电通讯网络或外部定位方式，获取到的终端用户的位置信息；WIFI热点扫描信息，该信息为用户接入无线网络时所扫描到的无线接入点设备的设备信息，由于无线接入点设备的位置固定，因此根据无线接入设备的设置信息也可以确定用户所在的位置；用户终端内的联系人信息，当用户终端为手机时，该联系人信息可以具体为通信录内的联系人的姓名和电话号码，为了保证信息安全性，上述联系人信息可以通过哈希算法处理后再发送到服务器；用户终端内的通信信息，当用户终端为手机时，该通信信息可以包括与通信录内的任一联系人收发短信的次数，或者与任一联系人通话的次数。需要说明的是，上述仅为用户信息的几个示例，实际应用中，可以根据需要向服务器上报其他能够确定用户间可信度的用户信息，对此本申请实施例不进行限制。

[0073] 步骤302：服务器根据接收到的用户信息计算每个用户与其关联用户之间的可信度值。

[0074] 其中，对于任意用户来说，在确定其关联用户时，可以根据该用户上报的联系人信息确定其关联用户，例如可以将用户上报的通信录中标签为亲戚、好友、同事的联系人确定为关联用户；或者，也可以根据与用户通过所安装的同一APP进行互动的好友确定其关联用户，例如对于即时通信APP，可以将好友列表中标签为家人、朋友的好友确定为其关联用户。

[0075] 其中，根据用户信息类型的不同，可以采用多种方式计算用户与关联用户之间的可信度值，包括：当用户信息包括LBS信息时，可以根据用户与其关联用户的LBS信息计算用

户与其关联用户在预设时间周期内位于同一位置的位置可信度值;或者,当用户信息包括WIFI热点扫描信息时,可以根据用户与其关联用户的WIFI热点扫描信息计算用户与其关联用户在预设时间周期内通过同一WIFI热点接入无线网络的网络连接可信度值;或者,当所述用户信息包括通信信息时,可以根据用户与其关联用户的通信信息计算用户与其关联用户在预设时间周期内的通信频次可信度值。进一步,也可以在计算不同类型的用户信息的多个可信度值后,根据每个可信度值的权值计算用户与其关联用户的最终可信度值。

[0076] 上述计算可信度值时的预设时间周期可以灵活设置,比如预设时间周期为一年。例如,用户2相对于用户1的位置可信度值P1=一年内用户1与用户2在同一位置时的秒长/(365*24*60);又例如,用户2相对于用户1的通信频次可信度值P2=一年内用户1与用户2之间通信次数*一年内发生通信的天数/365;上述P1或P2越大说明用户2与用户1的可信度关系越强。

[0077] 步骤303:服务器保存每个用户的用户标识与用户信息之间的第一对应关系,以及每个用户的用户标识与关联用户的用户标识及可信度值之间的第二对应关系。

[0078] 由于步骤301中用户终端按照预设上报周期上报用户信息,根据上报周期的不同,用户信息实时发生变化;相应的,步骤302中服务器根据用户信息计算的可信度值也实时发生变化。因此,服务器可以通过第一对应关系保存每个用户的用户标识与当前上报周期上报的用户信息之间的对应关系;以及,通过第二对应关系保存每个用户的用户标识与其关联用户的用户标识及当前上报周期计算出的可信度值之间的对应关系,如下表1所示,为结合图1示出的一种第二对应关系示例,其中用户1的关联用户为用户2和用户3:

[0079] 表1

[0080]

用户标识	关联用户标识	可信度值
用户 1	用户 2	P12
	用户 3	P13

[0081] 步骤304:当对源用户进行身份认证时,服务器通过查找第二对应关系,获得与该源用户对应的可信度值中高于可信度阈值的可信度值。

[0082] 本申请实施例,将待进行身份认证的用户统称为源用户,服务器可以根据源用户的用户标识查找第二对应关系,获得当前源用户与其关联用户的可信度值,然后从这些可信度值中选择高于预设的可信度阈值的可信度值。

[0083] 步骤305:服务器将获取的可信度值对应的关联用户确定为源用户的可信用户。

[0084] 步骤304中,服务器选择出高于预设的可信度阈值的可信度值后,可以将该可信度值对应的关联用户确定为源用户的可信用户,

[0085] 步骤306:服务器从可信用户中获取与源用户之间距离满足预设条件的目标用户。

[0086] 本实施例中,当服务器查找到源用户的可信用户后,可以根据当前源用户和可信用户的位置信息选择距离源用户距离较近的目标用户。例如,服务器可以根据当前源用户和可信用户的LBS信息,从可信用户中获取与源用户当前位于同一位置的用户作为目标用户;或者,服务器也可以根据当前源用户和可信用户的WIFI热点扫描信息,从可信用户中获取与源用户当前通过同一WIFI热点接入无线网络的用户作为目标用户。

[0087] 步骤307:服务器判断目标用户是否为一个,若是,则执行步骤308;否则,执行步骤

309。

[0088] 步骤308:服务器将用于身份认证的验证信息下发给该一个目标用户,执行步骤312。

[0089] 步骤309:服务器将包含多个用户的用户列表下发给源用户。

[0090] 步骤310:源用户终端将源用户从用户列表中选择的一个目标用户发送给服务器。

[0091] 步骤311:服务器将用于身份认证的验证信息下发给源用户选择的目标用户。

[0092] 步骤312:源用户从目标用户处获得验证信息后完成身份认证。

[0093] 由上述方法实施例可见,该实施例可以应用用户之间的社会网络关系信息,结合用户之间的位置信息,将验证信息下发给用户的亲友等可信人员所持有的终端,从而保证了用户身份验证的可靠性,即使用户的终端被恶意第三方盗取,也无法通过该终端进行身份验证,从而提高了身份验证的安全性。

[0094] 与本申请身份认证方法的实施例相对应,本申请还提供了身份认证装置及服务器的实施例。

[0095] 参见图4,为本申请身份认证装置的一个实施例框图:

[0096] 该身份认证装置包括:第一查找单元410、第一获取单元420和第一下发单元430。

[0097] 其中,第一查找单元410,用于当接收到源用户的身份认证请求时,查找所述源用户的可信用户;

[0098] 第一获取单元420,用于根据所述身份认证请求中携带的源用户的用户信息,从所述可信用户中获取与所述源用户之间距离满足预设条件的目标用户;

[0099] 第一下发单元430,用于将用于所述身份认证的验证信息下发给所述目标用户,以使所述源用户从所述目标用户获得所述验证信息后进行身份认证。

[0100] 参见图5,为本申请身份认证装置的另一个实施例框图:

[0101] 该装置包括:第一确定单元510、第一计算单元520、第一查找单元530、第一获取单元540和第一下发单元550。

[0102] 其中,第一确定单元510,用于根据所述源用户的历史用户信息,确定和所述源用户关联的关联用户以及关联用户的历史用户信息;

[0103] 第一计算单元520,用于根据所述历史用户信息计算所述源用户与关联用户之间的可信度值;

[0104] 第一查找单元530,用于当对源用户进行身份认证时,从所述可信度值中获取高于可信度阈值的可信度值,将获取的可信度值对应的关联用户确定为所述源用户的可信用户;

[0105] 第一获取单元540,用于根据所述身份认证请求中携带的源用户的用户信息,从所述可信用户中获取与所述源用户之间距离满足预设条件的目标用户;

[0106] 第一下发单元550,用于将用于所述身份认证的验证信息下发给所述目标用户,以使所述源用户从所述目标用户获得所述验证信息后进行身份认证。

[0107] 在一个可选的实现方式中:

[0108] 所述第一计算单元520可以包括至少一个下述子单元(图5中未示出):

[0109] 第一位置可信度值计算子单元,用于当所述历史用户信息包括基于位置的服务LBS信息时,根据所述LBS信息计算所述源用户与所述关联用户在预设时间周期内位于同一

位置的位置可信度值；

[0110] 第一网络连接可信度值计算子单元，用于当所述历史用户信息包括WIFI热点扫描信息时，根据所述扫描信息计算所述源用户与所述关联用户在预设时间周期内通过同一WIFI热点接入无线网络的网络连接可信度值；

[0111] 第一通信频次可信度值计算子单元，用于当所述历史用户信息包括通信信息时，根据所述通信信息计算所述源用户与所述关联用户在预设时间周期内的通信频次可信度值。

[0112] 在另一个可选的实现方式中：

[0113] 所述第一获取单元540可以包括至少一个下述子单元(图5中未示出)：

[0114] 第一位置目标获取子单元，用于根据当前所述源用户和所述可信用户的LBS信息，从所述可信用户中获取与所述源用户当前位于同一位置的目标用户；

[0115] 第一热点目标获取子单元，用于根据当前所述源用户和所述可信用户的WIFI热点扫描信息，从所述可信用户中获取与所述源用户当前通过同一WIFI热点接入无线网络的目标用户。

[0116] 在另一个可选的实现方式中：

[0117] 所述第一下发单元550可以包括(图5中未示出)：

[0118] 第一列表下发子单元，用于当所述目标用户包括多个用户时，将所述多个用户的用户列表下发给所述源用户；

[0119] 第一选择获取子单元，用于获取所述源用户从所述用户列表中选择的一个用户；

[0120] 第一信息下发子单元，用于将用于所述身份认证的验证信息下发给所述源用户选择的一个用户。

[0121] 参见图6，为本申请身份认证装置的另一个实施例框图：

[0122] 该装置包括：第二获取单元610、第二查找单元620和第二下发单元630。

[0123] 其中，第二获取单元610，用于当接收到源用户的身份认证请求时，根据所述身份认证请求中携带的源用户的用户信息获取与所述源用户之间距离满足预设条件的目标用户；

[0124] 第二查找单元620，用于从所述目标用户中查找所述源用户的可信用户；

[0125] 第二下发单元630，用于将用于所述身份认证的验证信息下发给所述可信用户，以使所述源用户从所述可信用户获得所述验证信息后进行身份认证。

[0126] 在一个可选的实现方式中：

[0127] 所述第二获取单元610可以包括至少一个下述子单元(图6中未示出)：

[0128] 第二位置目标获取子单元，用于根据所述身份认证请求中携带的源用户的LBS信息和当前所有用户的LBS信息，从所有用户中获取与所述源用户当前位于同一位置的目标用户；

[0129] 第二热点目标获取子单元，用于根据所述身份认证请求中携带的源用户的WIFI热点扫描信息和当前所有用户的WIFI热点扫描信息，从所述所有用户中获取与所述源用户当前通过同一WIFI热点接入无线网络的目标用户。

[0130] 在另一个可选的实现方式中：

[0131] 所述装置还可以包括(图6中未示出)：

[0132] 第二确定单元，用于根据所述源用户的历史用户信息，确定和所述源用户关联的关联用户以及关联用户的历史用户信息；

[0133] 第二计算单元，用于根据所述历史用户信息计算所述源用户与关联用户之间的可信度值；

[0134] 所述第二查找单元620，可以具体用于从所述可信度值中获取高于可信度阈值的可信度值，当获取的可信度值对应的关联用户属于所述目标用户时，将所述对应的关联用户确定为所述源用户的可信用户。

[0135] 在另一个可选的实现方式中：

[0136] 所述第二下发单元630可以包括(图6中未示出)：

[0137] 第二列表下发子单元，用于当所述可信用户包括多个用户时，将所述多个用户的用户列表下发给所述源用户；

[0138] 第二选择获取子单元，用于获取所述源用户从所述用户列表中选择的一个用户；

[0139] 第二信息下发子单元，用于将用于身份认证的验证信息下发给所述源用户选择的一个用户。

[0140] 上述装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[0141] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中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模块来实现本申请方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0142] 参见图7，为本申请服务器的实施例框图：

[0143] 该服务器包括：处理器710，以及用于存储所述处理器710可执行指令的存储器720；进一步，该服务器还可以包括输入/输出接口，网络接口，各种硬件等。

[0144] 在一个可选的实现方式中，所述处理器710可以被配置为：

[0145] 当接收到源用户的身份认证请求时，查找所述源用户的可信用户；

[0146] 根据所述身份认证请求中携带的源用户的用户信息，从所述可信用户中获取与所述源用户之间距离满足预设条件的目标用户；

[0147] 将用于所述身份认证的验证信息下发给所述目标用户，以使所述源用户从所述目标用户获得所述验证信息后进行身份认证。

[0148] 在另一个可选的实现方式中，所述处理器710可以被配置为：

[0149] 当接收到源用户的身份认证请求时，根据所述身份认证请求中携带的源用户的用户信息获取与所述源用户之间距离满足预设条件的目标用户；

[0150] 从所述目标用户中查找所述源用户的可信用户；

[0151] 将用于所述身份认证的验证信息下发给所述可信用户，以使所述源用户从所述可信用户获得所述验证信息后进行身份认证。

[0152] 由上述实施例可见，应用本申请实施例对源用户进行身份认证时，可以按照源用户与其可信用户之间的距离关系筛选出距离源用户较近的目标用户，并将验证信息下发给

目标用户，从而使得源用户可以从目标用户处获得验证信息并完成身份认证。本申请应用用户之间的社会网络关系信息，结合用户之间的位置信息，将验证信息下发给用户的亲友等可信人员所持有的终端，从而保证了用户身份验证的可靠性，即使用户的终端被恶意第三方盗取，也无法通过该终端进行身份验证，从而提高了身份验证的安全性。

[0153] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

[0154] 应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

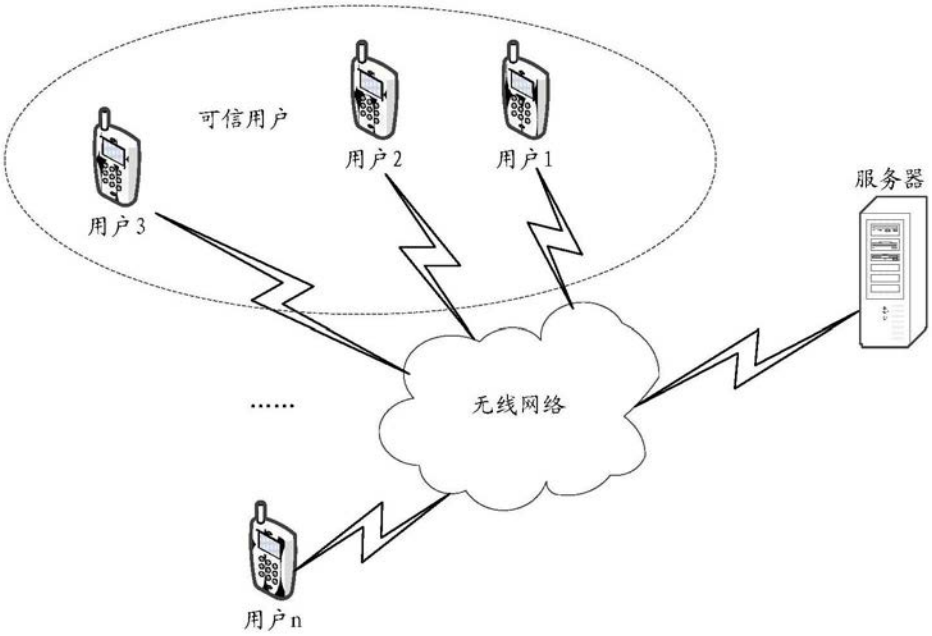

可信用户
用户2
用户1
用户3
服务器
无线网络
.....
用户n

图1

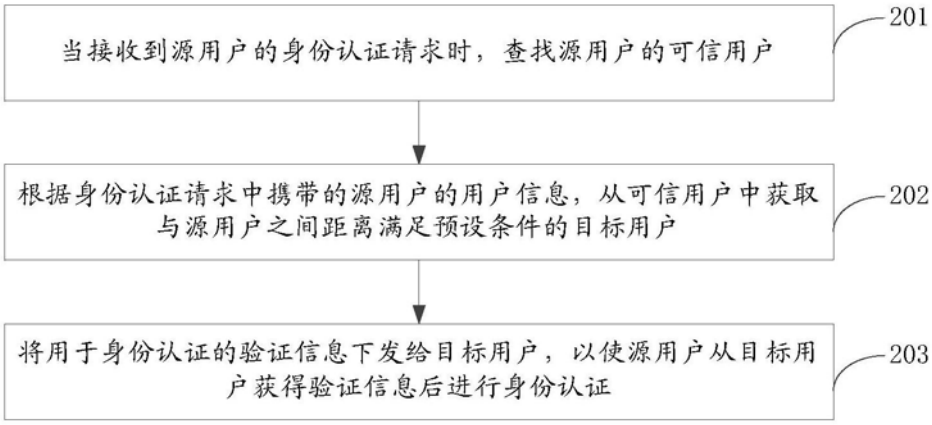

当接收到源用户的身份认证请求时，查找源用户的可信用户
201
根据身份认证请求中携带的源用户的用户信息，从可信用户中获取与源用户之间距离满足预设条件的目标用户
202
将用于身份认证的验证信息下发给目标用户，以使源用户从目标用户获得验证信息后进行身份认证
203

图2A

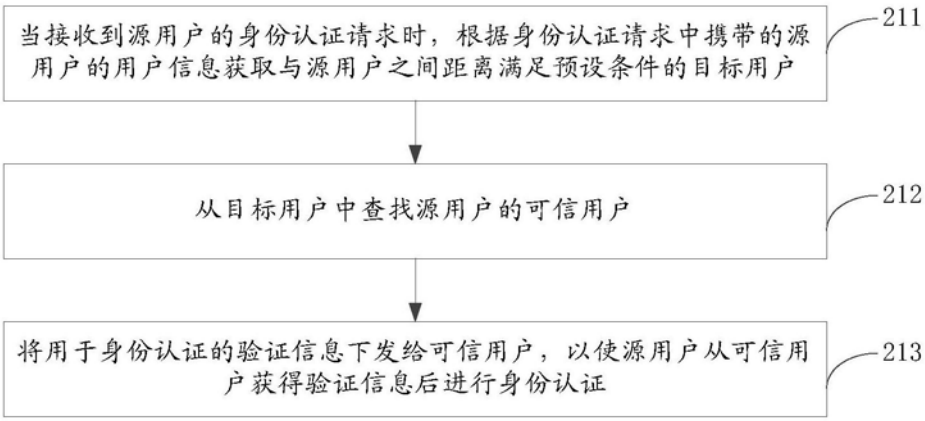

当接收到源用户的身份认证请求时，根据身份认证请求中携带的源用户的用户信息获取与源用户之间距离满足预设条件的目标用户
211
从目标用户中查找源用户的可信用户
212
将用于身份认证的验证信息下发给可信用户，以使源用户从可信用户获得验证信息后进行身份认证
213

图2B

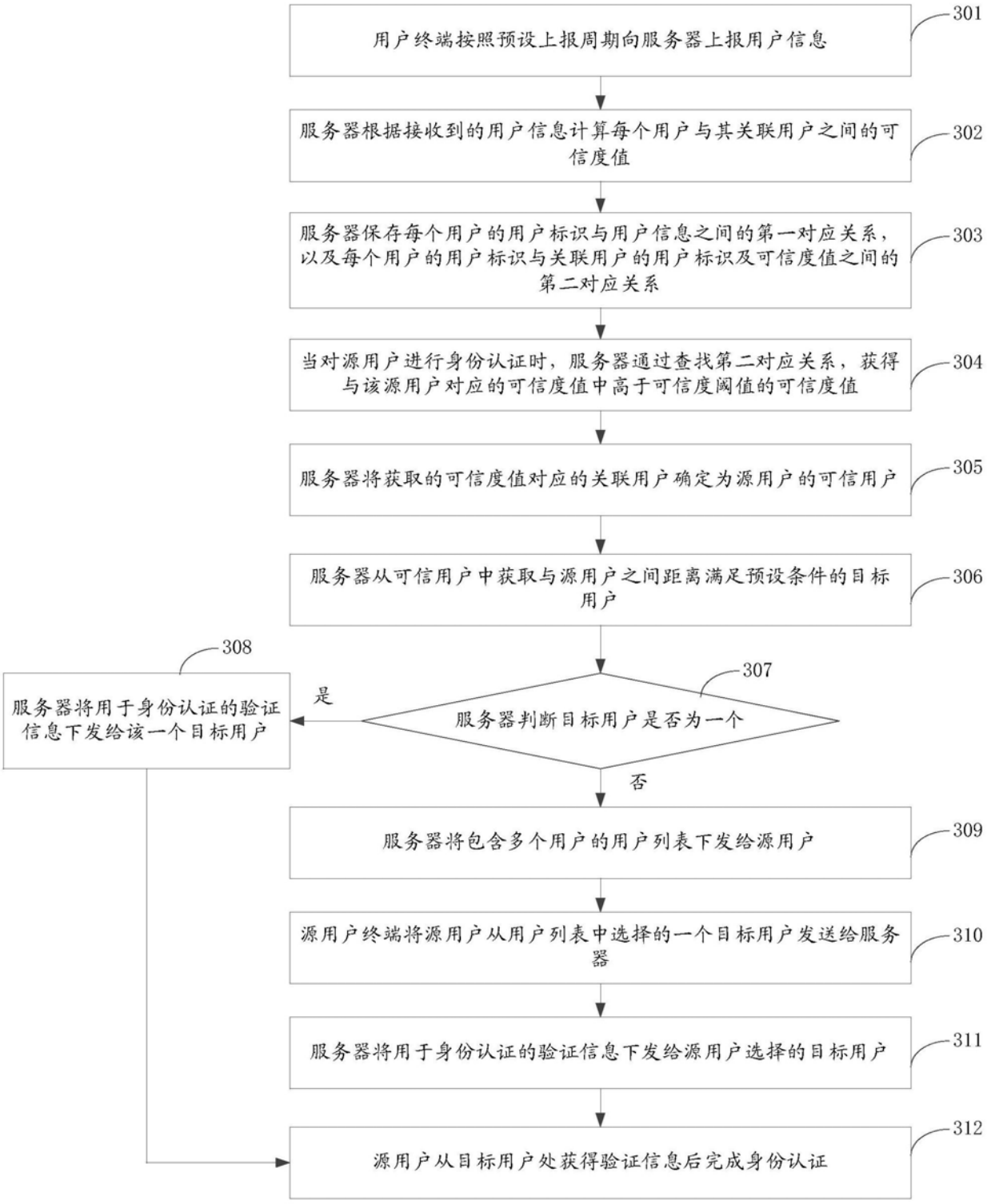

用户终端按照预设上报周期向服务器上报用户信息
301
服务器根据接收到的用户信息计算每个用户与其关联用户之间的可信度值
302
服务器保存每个用户的用户标识与用户信息之间的第一对应关系，以及每个用户的用户标识与关联用户的用户标识及可信度值之间的第二对应关系
303
当对源用户进行身份认证时，服务器通过查找第二对应关系，获得与该源用户对应的可信度值中高于可信度阈值的可信度值
304
服务器将获取的可信度值对应的关联用户确定为源用户的可信用户
305
服务器从可信用户中获取与源用户之间距离满足预设条件的目标用户
306
服务器判断目标用户是否为一个
307
是
服务器将用于身份认证的验证信息下发给该一个目标用户
308
否
服务器将包含多个用户的用户列表下发给源用户
309
源用户终端将源用户从用户列表中选择的一个目标用户发送给服务器
310
服务器将用于身份认证的验证信息下发给源用户选择的目标用户
311
源用户从目标用户处获得验证信息后完成身份认证
312

图3

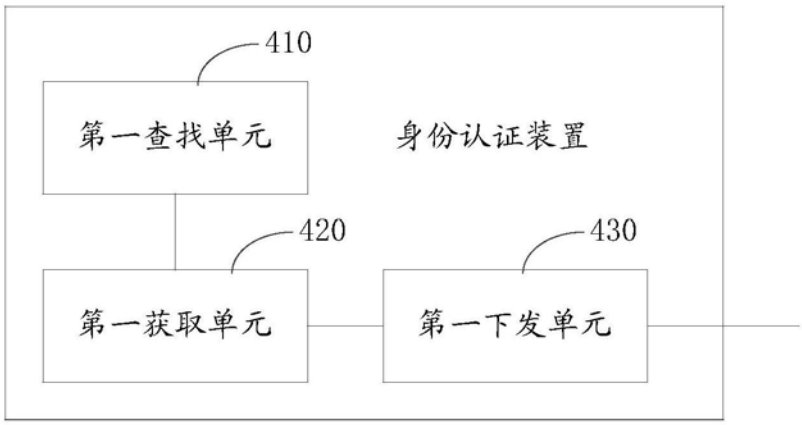

410
第一查找单元
身份认证装置
420
430
第一获取单元
第一下发单元

图4

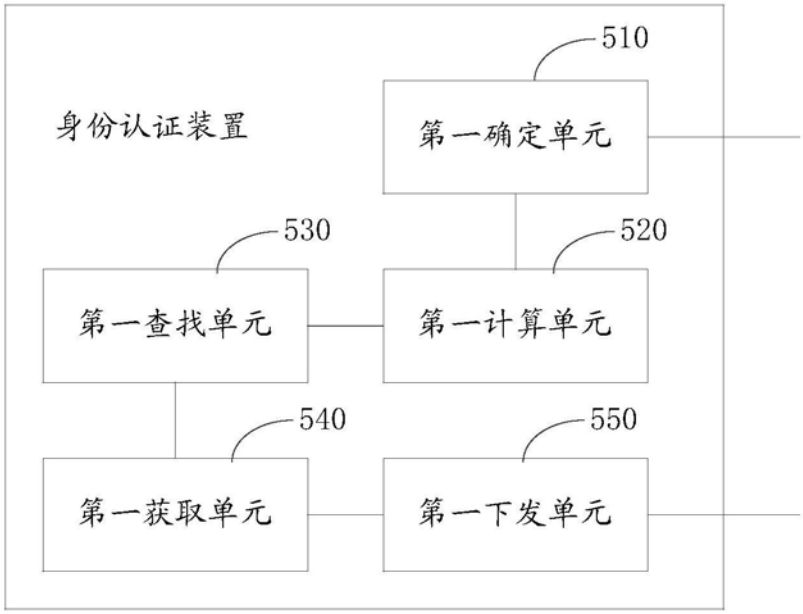

510
身份认证装置
第一确定单元
530
520
第一查找单元
第一计算单元
540
550
第一获取单元
第一下发单元

图5

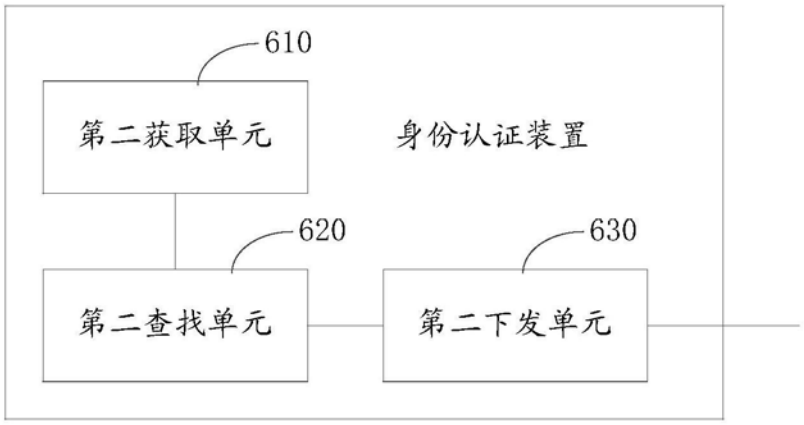

610
第二获取单元
身份认证装置
620
630
第二查找单元
第二下发单元

图6

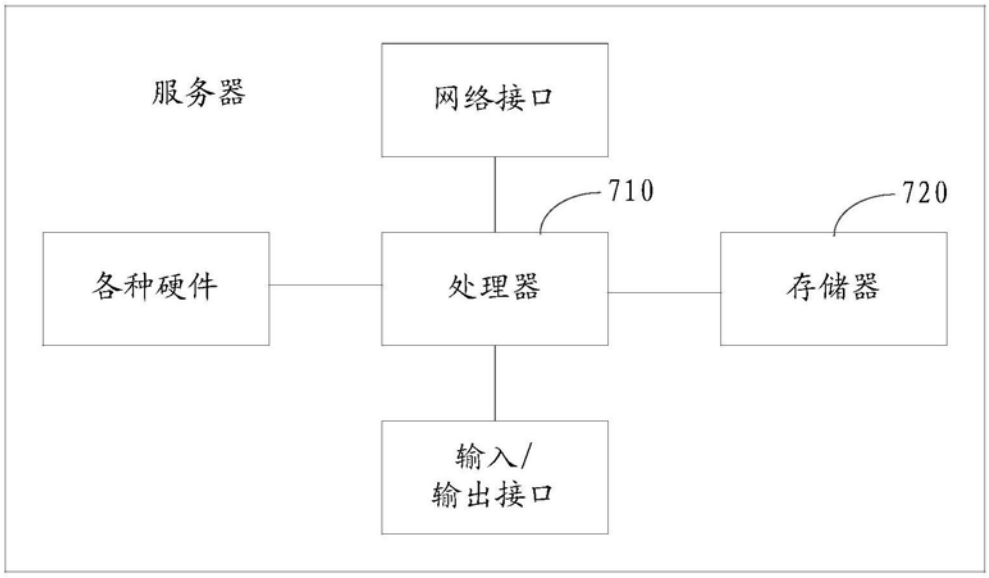

服务器
网络接口
710
720
各种硬件
处理器
存储器
输入/
输出接口

图7