(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 104580112 B
(45)授权公告日 2018.07.13

(21)申请号 201310512274.4

(22)申请日 2013.10.25

(65)同一申请的已公布的文献号
申请公布号 CN 104580112 A

(43)申请公布日 2015.04.29

(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岛资本大厦一座四层847号邮箱

(72)发明人 曹恺

(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 29/06(2006.01)
H04L 29/12(2006.01)

(56)对比文件
US 2011/0138483 A1,2011.06.09,
CN 101145905 A,2008.03.19,
US 2008318548 A1,2008.12.25,
CN 101114397 A,2008.01.30,
CN 101131756 A,2008.02.27,
CN 101025806 A,2007.08.29,

审查员 高伟

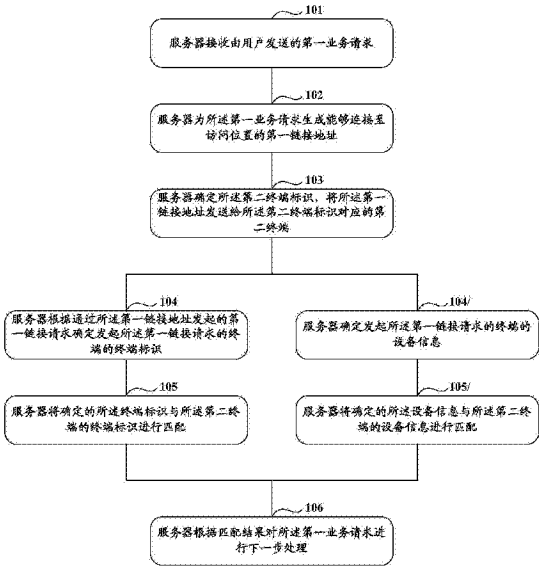
权利要求书2页 说明书11页 附图2页

(54)发明名称

一种业务认证方法、系统及服务器

(57)摘要

本申请公开了一种业务认证方法、系统及服务器，当服务器在接收到用户发送的业务请求时，生成一个能够链接至访问位置的链接地址，并将生成的链接地址发送给用户预先设定的终端标识对应的终端，即合法终端；之后，当服务器在接收到通过所述第一链接地址发起的第一链接请求时，通过判断发起所述第一链接请求的终端是否是合法终端来进行业务认证。即使服务器下发给合法终端的链接地址被非法盗用，但只要合法终端处于安全状态没有被非法使用，服务器就能够识别出通过所述链接地址链接至本地的终端不是合法终端，不会通过对业务请求的认证，以此来提高业务认证的可靠性。



CN 104580112 B

1.一种业务认证方法，其特征在于，所述方法包括：

服务器根据接收到的由用户发送的第一业务请求，生成能够链接至访问位置的第一链接地址；

服务器确定第二终端标识，将所述第一链接地址发送给所述第二终端标识对应的第二终端，所述第二终端标识是所述用户预先设定的终端标识；

服务器根据通过所述第一链接地址发起的第一链接请求确定发起该第一链接请求的终端的终端标识；

服务器将确定的所述终端标识与所述第二终端的终端标识进行匹配，并且将发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息进行匹配；在发起所述第一链接请求的终端的终端标识与所述第二终端的终端标识匹配且发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息匹配时，通过对所述第一业务请求的认证；否则，不通过对所述第一业务请求的认证；

其中，服务器通过以下方式确定第二终端的设备信息：

服务器根据所述第二终端访问该服务器的历史记录信息，确定所述第二终端的设备信息；或者，

服务器在以往接收到使用与所述第二终端绑定的用户账号的终端发送的第二业务请求时，生成能够链接至访问位置的第二链接地址；

服务器将所述第二链接地址发送给所述第二终端；

服务器根据通过所述第二链接地址发起的第二链接请求确定发起该第二链接请求的终端的终端标识和该终端的设备信息；

若服务器确定发起所述第二链接请求的终端的终端标识与所述第二终端的终端标识匹配，且在通过对所述第二业务请求的认证后的设定时长内没有接收到告警信息，则确定发起所述第二链接请求的终端的设备信息为第二终端的设备信息。

2.如权利要求1所述的方法，其特征在于，用户通过第一终端发送所述第一业务请求，其中，第一终端与第二终端为不同终端或第一终端与第二终端为同一终端。

3.一种业务认证系统，其特征在于，所述系统包括：

服务器，用于根据接收到的由用户发送的第一业务请求，生成能够链接至访问位置的第一链接地址，确定第二终端标识，将所述第一链接地址发送给所述第二终端标识对应的第二终端，所述第二终端标识是所述用户预先设定的终端标识，以及，根据通过所述第一链接地址发起的第一链接请求确定发起该第一链接请求的终端的终端标识，将确定的所述终端标识与所述第二终端的终端标识进行匹配，并且将发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息进行匹配；

在发起所述第一链接请求的终端的终端标识与所述第二终端的终端标识匹配且发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息匹配时，通过对所述第一业务请求的认证；否则，不通过对所述第一业务请求的认证；

其中，服务器通过以下方式确定第二终端的设备信息：

服务器根据所述第二终端访问该服务器的历史记录信息，确定所述第二终端的设备信息；或者，

服务器在以往接收到使用与所述第二终端绑定的用户账号的终端发送的第二业务请

求时，生成能够链接至访问位置的第二链接地址；

服务器将所述第二链接地址发送给所述第二终端；

服务器根据通过所述第二链接地址发起的第二链接请求确定发起该第二链接请求的终端的终端标识和该终端的设备信息；

若服务器确定发起所述第二链接请求的终端的终端标识与所述第二终端的终端标识匹配，且在通过对所述第二业务请求的认证后的设定时长内没有接收到告警信息，则确定发起所述第二链接请求的终端的设备信息为第二终端的设备信息；

第二终端，用于接收所述服务器发送的第一链接地址，并通过该第一链接地址向服务器发起所述第一链接请求。

4.如权利要求3所述的系统，其特征在于，所述系统还包括：

第一终端，用于根据用户的指示发起所述第一业务请求；

其中，第一终端与第二终端为不同终端或第一终端与第二终端为同一终端。

5.一种服务器，其特征在于，所述服务器包括：

接收模块，用于接收由用户发送的第一业务请求；

链接地址生成模块，用于生成能够链接至访问位置的第一链接地址；

发送模块，用于将所述第一链接地址发送给确定的第二终端标识对应的第二终端，所述第二终端标识是用于预先设定的终端标识；

确定模块，用于根据通过所述第一链接地址发起的第一链接请求确定发起该第一链接请求的终端的终端标识；

匹配模块，用于将确定的所述终端标识与第二终端的终端标识进行匹配，并且将发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息进行匹配；在发起所述第一链接请求的终端的终端标识与所述第二终端的终端标识匹配且发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息匹配时，通过对所述第一业务请求的认证；否则，不通过对所述第一业务请求的认证；

其中，所述接收模块，还用于在以往接收使用与所述第二终端绑定的用户账号的终端发送的第二业务请求；

所述链接地址生成模块，还用于生成能够链接至访问位置的第二链接地址；

所述发送模块，还用于将所述第二链接地址发送给第二终端；

所述确定模块，还用于根据通过所述第二链接地址发起的第二链接请求确定发起该第二链接请求的终端的终端标识和该终端的设备信息；

所述匹配模块，还用于将发起所述第二链接请求的终端的终端标识与所述第二终端的终端标识进行匹配；

所述设备信息确定模块，具体用于在所述匹配模块确定发起所述第二链接请求的终端的终端标识与所述第二终端的终端标识匹配，且在通过对所述第二业务请求的认证后的设定时长内没有接收到告警信息，则确定发起所述第二链接请求的终端的设备信息为第二终端的设备信息；或者，根据所述第二终端访问该服务器的历史记录信息，确定所述第二终端的设备信息。

一种业务认证方法、系统及服务器

技术领域

[0001] 本申请涉及计算机技术领域，尤其涉及一种业务认证方法、系统及服务器。

背景技术

[0002] 终端通过用户输入的用户账号登录服务器后，向服务器发起业务请求，如支付业务请求或身份认证业务请求等，为了确保业务请求的合法性，服务器在接收到业务请求后，并不立即响应该业务请求，而是在本地产生一个校验码(一般为6位校验码)，并根据本地存储的用户账号与手机号之间的绑定关系，通过短信息将所述校验码发送给与终端登录服务器时所使用的用户账号绑定的手机。

[0003] 手机将服务器发送的校验码向用户展示，用户再将所述校验码通过终端的输入端口输入终端(如终端向用户展示可输入校验码的页面，用户在该页面中的输入框内输入所述校验码)，终端将用户输入的所述校验码上报给服务器，服务器将终端上报的校验码与本地产生的所述校验码进行比较，若相同，则通过对所述业务请求的合法性认证，响应所述业务请求。

[0004] 但是，在实际的业务认证过程中，可能出现与用户账号绑定的手机受木马软件入侵等情况，或是与用户账号绑定手机的使用者受到诈骗等情况，导致服务器向用户账号绑定的手机下发的校验码被非法盗用，如果被非法盗用的校验码被非法用户用于业务请求的合法性认证过程，则对业务请求的合法性认证的可靠性得不到保证。

发明内容

[0005] 本申请实施例提供了一种业务认证方法、系统及服务器，用以解决现有技术中存在的业务认证的可靠性低的问题

[0006] 一种业务认证方法，所述方法包括：

[0007] 服务器根据接收到的由用户发送的第一业务请求，生成能够链接至访问位置的第一链接地址；

[0008] 服务器确定第二终端标识，将所述第一链接地址发送给所述第二终端标识对应的第二终端，所述第二终端标识是所述用户预先设定的终端标识；

[0009] 服务器根据通过所述第一链接地址发起的第一链接请求确定发起该第一链接请求的终端的终端标识；

[0010] 服务器将确定的所述终端标识与所述第二终端的终端标识进行匹配，并根据匹配结果对所述第一业务请求进行下一步处理。

[0011] 通过本申请实施例的方案，将链接至服务器的终端与用户预先设定的终端标识对应的第二终端(即合法终端)进行适配，即使服务器下发给第二终端的链接地址被非法盗用，但只要第二终端处于安全状态没有被非法使用，服务器就能够识别出链接至本地的终端不是第二终端，不会通过对业务请求的认证，可提高业务认证的可靠性。

[0012] 可选地，用户通过第一终端发送所述第一业务请求，其中，第一终端与第二终端为

不同终端或第一终端与第二终端为同一终端。

[0013] 通过本申请实施例的方案，用于可通过与所述第二终端为同一终端或不同终端的第一终端发送所述第一业务请求，增加本申请实施例的实现手段。

[0014] 可选地，服务器确定第二终端设备信息，以及确定发起所述第一链接请求的终端的设备信息；

[0015] 服务器将发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息进行匹配。

[0016] 通过本申请实施例的方案，通过设备信息来进一步判断发起所述第一链接请求的终端是否是第二终端，可进一步提高业务认证的可靠性。

[0017] 可选地，服务器通过以下方式确定第二终端的设备信息：

[0018] 服务器根据所述第二终端访问该服务器的历史记录信息，确定所述第二终端的设备信息；或者，

[0019] 服务器在以往接收到使用与所述第二终端绑定的用户账号的终端发送的第二业务请求时，生成能够链接至访问位置的第二链接地址；

[0020] 服务器将所述第二链接地址发送给所述第二终端；

[0021] 服务器根据通过所述第二链接地址发起的第二链接请求确定发起该第二链接请求的终端的终端标识和该终端的设备信息；

[0022] 若服务器确定发起所述第二链接请求的终端的终端标识与所述第二终端的终端标识匹配，且在通过对所述第二业务请求的认证后的设定时长内没有接收到告警信息，则确定发起所述第二链接请求的终端的设备信息为第二终端的设备信息。

[0023] 通过本申请实施例的方案，可准确识别第二终端的设备信息，在利用设备信息来判断发起所述第一链接请求的终端是否是第二终端时，可提高判断的准确性。

[0024] 可选地，所述设备信息包括以下至少一种信息：

[0025] 终端的设备型号、终端内操作系统的版本号、终端内浏览器的版本号、终端显示屏的大小和分辨率。

[0026] 通过本申请实施例的方案，可通过多种形式的信息来反映设备信息。

[0027] 一种业务认证系统，所述系统包括：

[0028] 服务器，用于根据接收到的由用户发送的第一业务请求，生成能够链接至访问位置的第一链接地址，确定第二终端标识，将所述第一链接地址发送给所述第二终端标识对应的第二终端，所述第二终端标识是所述用户预先设定的终端标识，以及，根据通过所述第一链接地址发起的第一链接请求确定发起该第一链接请求的终端的终端标识，将确定的所述终端标识与所述第二终端的终端标识进行匹配，并根据匹配结果对所述第一业务请求进行下一步处理；

[0029] 第二终端，用于接收所述服务器发送的第一链接地址，并通过该第一链接地址向服务器发起所述第一链接请求。

[0030] 通过本申请实施例的方案，将链接至服务器的终端与用户预先设定的终端标识对应的第二终端(即合法终端)进行适配，即使服务器下发给第二终端的链接地址被非法盗用，但只要第二终端处于安全状态没有被非法使用，服务器就能够识别出链接至本地的终端不是第二终端，不会通过对业务请求的认证，可提高业务认证的可靠性。

[0031] 可选地，所述系统还包括：

[0032] 第一终端，用于根据用户的指示发起所述第一业务请求；

[0033] 其中，第一终端与第二终端为不同终端或第一终端与第二终端为同一终端。

[0034] 通过本申请实施例的方案，用于可通过与所述第二终端为同一终端或不同终端的第一终端发送所述第一业务请求，增加本申请实施例的实现手段。

[0035] 可选地，所述服务器，还用于确定第二终端设备信息，以及确定发起所述第一链接请求的终端的设备信息，并将发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息进行匹配。

[0036] 通过本申请实施例的方案，通过设备信息来判断发起所述第一链接请求的终端是否是第二终端，可进一步提高业务认证的可靠性。

[0037] 可选地，所述服务器，还用于根据所述第二终端访问该服务器的历史记录信息，确定所述第二终端的设备信息；或者，

[0038] 在以往接收到使用与所述第二终端绑定的用户账号的终端发送的第二业务请求时，生成能够链接至访问位置的第二链接地址，将所述第二链接地址发送给所述第二终端，并根据通过所述第二链接地址发起的第二链接请求确定发起该第二链接请求的终端的终端标识和该终端的设备信息，以及，若确定发起所述第二链接请求的终端的终端标识与所述第二终端的终端标识匹配，且在通过对所述第二业务请求的认证后的设定时长内没有接收到告警信息，则确定发起所述第二链接请求的终端的设备信息为第二终端的设备信息。

[0039] 通过本申请实施例的方案，可准确识别第二终端的设备信息，在利用设备信息来判断发起所述第一链接请求的终端是否是第二终端时，可提高判断的准确性。

[0040] 一种服务器，所述服务器包括：

[0041] 接收模块，用于接收由用户发送的第一业务请求；

[0042] 链接地址生成模块，用于生成能够链接至访问位置的第一链接地址；

[0043] 发送模块，用于将所述第一链接地址发送给确定的第二终端标识对应的第二终端，所述第二终端标识是用于预先设定的终端标识；

[0044] 确定模块，用于根据通过所述第一链接地址发起的第一链接请求确定发起该第一连接请求的终端的终端标识；

[0045] 匹配模块，用于将确定的所述终端标识与第二终端的终端标识进行匹配，并根据匹配结果对所述第一业务请求进行下一步处理。

[0046] 通过本申请实施例的方案，将链接至服务器的终端与用户预先设定的终端标识对应的第二终端(即合法终端)进行适配，即使服务器下发给第二终端的链接地址被非法盗用，但只要第二终端处于安全状态没有被非法使用，服务器就能够识别出链接至本地的终端不是第二终端，不会通过对业务请求的认证，可提高业务认证的可靠性。

[0047] 可选地，所述服务器还包括：

[0048] 设备信息确定模块，用于确定第二终端的设备信息；

[0049] 所述确定模块，还用于确定发起所述第一链接请求的终端的设备信息；

[0050] 所述匹配模块，还用于将发起所述第一链接请求的终端的设备信息与第二终端的设备信息进行匹配。

[0051] 通过本申请实施例的方案，通过设备信息来判断发起所述第一链接请求的终端是

否是第二终端，可进一步提高业务认证的可靠性。

[0052] 可选地，所述接收模块，还用于在以往接收使用与所述第二终端绑定的用户账号的终端发送的第二业务请求；

[0053] 所述链接地址生成模块，还用于生成能够链接至访问位置的第二链接地址；

[0054] 所述发送模块，还用于将所述第二链接地址发送给第二终端；

[0055] 所述确定模块，还用于根据通过所述第二链接地址发起的第二链接请求确定发起该第二链接请求的终端的终端标识和该终端的设备信息；

[0056] 所述匹配模块，还用于将发起所述第二链接请求的终端的终端标识与所述第二终端的终端标识进行匹配；

[0057] 所述设备信息确定模块，具体用于在所述匹配模块确定发起所述第二链接请求的终端的终端标识与所述第二终端的终端标识匹配，且在通过对所述第二业务请求的认证后的设定时长内没有接收到告警信息，则确定发起所述第二链接请求的终端的设备信息为第二终端的设备信息；或者，根据所述第二终端访问该服务器的历史记录信息，确定所述第二终端的设备信息。

[0058] 通过本申请实施例的方案，可准确识别第二终端的设备信息，在利用设备信息来判断发起所述第一链接请求的终端是否是第二终端时，可提高判断的准确性。

附图说明

[0059] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0060] 图1为本申请实施例一中业务认证方法的步骤示意图；

[0061] 图2为本申请实施例二中业务认证系统的结构示意图；

[0062] 图3为本申请实施例三中服务器的结构示意图。

具体实施方式

[0063] 为了使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请作进一步地详细描述，显然，所描述的实施例仅仅是本申请一部分实施例，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它实施例，都属于本申请保护的范围。

[0064] 为了解决当服务器向合法终端下发的校验码被非法盗用，导致对业务请求的合法性认证的可靠性低的问题，本申请实施例提出一种新的业务认证方案，当服务器在接收到由用户发送的业务请求时，生成一个能够链接至该服务器中一个访问位置的链接地址，并将生成的链接地址发送给用户预先设定的终端标识对应的终端。之后，当服务器在接收到通过所述第一链接地址发起的第一链接请求时，将发起该第一链接请求的终端与用户预先设定的终端标识对应的终端进行匹配，如果确定发起所述第一链接请求的终端是用户预先设定的终端标识对应的终端，可通过对业务请求的认证；否则，不通过对业务请求的认证。

[0065] 由于本申请实施例的方案中，将通过链接请求链接至服务器的终端与用户预先设

定的终端标识对应的终端进行适配，也就是将通过链接请求链接至服务器的终端与认定的合法终端进行适配，即使服务器下发给合法终端的链接地址被非法盗用，但只要该合法终端处于安全状态没有被非法使用，服务器就能够识别出通过所述链接地址链接至本地的终端不是合法终端，不会通过对业务请求的认证，以此来提高业务认证的可靠性。

[0066] 本申请实施例所涉及的链接地址可以是统一资源定位符(Uniform Resource Locator，URL)，所述URL也可称为网页地址，通过URL可以链接至服务器中的特定访问位置的页面。本申请实施例所涉及的链接地址也不限于其他形式的地址，如所述链接地址可以是短链接，所述短链接就是将长的URL通过程序计算等方式，转换为简短的网址字符串。

[0067] 本申请实施例中涉及的终端可以是PC机，也可以手机等移动终端，本申请实施例并不对终端的类型做限定。

[0068] 本申请实施例中涉及的业务请求可以是诸如支付业务请求或身份认证业务请求等对安全性要求较高的业务请求。

[0069] 下面通过具体实施例对本申请的方案做详细描述。

[0070] 实施例一：

[0071] 本申请实施例一描述了一种业务认证方法，如图1所示，所述业务认证方法主要包括以下步骤：

[0072] 步骤101：服务器接收由用户发送的第一业务请求。

[0073] 优选地，用户可以通过第一终端向服务器发起发送所述第一业务请求。

[0074] 本申请实施例中涉及的所述服务器可以是任何应用类型的服务器，如游戏网站服务器、网上银行服务器、购物网站的支付服务器等，本申请实施例并不对服务器的类型做限定。

[0075] 在本步骤101中，第一终端可受用户指示，使用预先注册的用户账号登陆服务器后，再向所述服务器发起针对某一业务的业务请求。以所述第一终端是PC机，服务器是网上银行服务器为例，本步骤101的具体实现过程为：

[0076] 所述PC机通过互联网与网上银行服务器建立连接后，可向用户展示登录网上银行服务器的页面，并接收用户通过登录页面的输入框输入的已预先注册的用户账号(如用户名和密码)。所述PC机将所述用户账号发送给网上银行服务器，当网上银行服务器通过对所述用户账号的认证后，完成登录过程。之后，所述PC机可通过展示页面接收用户输入的第一业务请求(如支付业务)，并将该第一业务请求发送给所述网上银行服务器。

[0077] 步骤102：服务器为所述第一业务请求生成能够连接至访问位置的第一链接地址。

[0078] 服务器可以在每次接收到一个业务请求时，就为该业务请求动态生成一个链接地址，例如，生成的链接地址为：http://jy.abc.com/jy.htm?pwd_id。

[0079] 每个链接地址能够链接至服务器中的一个访问位置，所述访问位置可以是服务器中的认证页面。

[0080] 步骤103：服务器确定所述第二终端标识，将所述第一链接地址发送给所述第二终端标识对应的第二终端。

[0081] 所述第二终端标识是用户预先设定的终端标识。

[0082] 在本申请实施例的方案中，当用户在服务器内注册用户账号时，可以为注册的用户账号绑定预先设定的终端标识(所述第二终端标识)，即在服务器内记录用户账号与第二

终端的终端标识之间的绑定关系，服务器可以根据第一终端登录服务器时使用的用户账号确定对应的第二终端的终端标识，进而通过确定的第二终端的终端标识，将所述第一链接地址发送给第二终端。

[0083] 本申请实施例中的所涉及的所述第一终端和所述第二终端可以是分别独立的两个终端设备，如第一终端是PC机，第二终端是手机；所述第一终端和所述第二终端也可以是同一终端设备中的部件，如第一终端和第二终端是同一手机中的部件。当所述第一终端和所述第二终端是指同一终端设备中的部件时，该终端设备分别具有所述第一终端和所述第二终端的功能部件以执行本实施例一的步骤。

[0084] 可选地，在所述第二终端是手机时，所述服务器可以通过下行短信(或其他无线通信方式)将所述第一链接地址发送给第二终端。

[0085] 步骤104：服务器根据通过所述第一链接地址发起的第一链接请求确定发起所述第一链接请求的终端的终端标识。

[0086] 若发起所述第一链接请求的终端是手机、该终端的终端标识是手机号，则本步骤104的具体做法可以为：服务器可以通过网络运营商公开的应用程序编程接口(Application Programming Interface,API)接口查询出发起所述第一链接请求的手机的手机号。

[0087] 在本步骤104的方案中，可以是第二终端根据接收到的第一链接地址直接向服务器发起第一链接请求。例如，若所述第二终端是具有触摸屏的手机，用户可以点击第二终端展示的第一链接地址，第二终端识别出用户的点击操作后，通过所述第一链接地址向所述服务器发起所述第一链接请求。

[0088] 如果服务器发送给第二终端的第一链接地址被盗用，则非法终端受非法用户的触发，也可以通过盗用的所述第一链接地址向所述服务器发起所述第一链接请求。

[0089] 步骤105：服务器将确定的所述终端标识与所述第二终端的终端标识进行匹配。

[0090] 服务器将确定的发起所述第一链接请求的终端的终端标识与所述第二终端的终端标识进行匹配是指：服务器判断发起所述第一链接请求的终端的终端标识是否与所述第二终端的终端标识相同，若相同，则匹配结果为发起所述第一链接请求的终端的终端标识与所述第二终端的终端标识匹配，此时，确定向服务器发起所述第一链接请求的终端是第二终端；若不相同，则匹配结果为发起所述第一链接请求的终端的终端标识与所述第二终端的终端标识不匹配，此时，确定向服务器发起所述第一链接请求的终端不是第二终端。

[0091] 步骤106：服务器根据匹配结果对所述第一业务请求进行下一步处理。

[0092] 在本步骤106中，若匹配结果为发起所述第一链接请求的终端的终端标识与所述第二终端的终端标识匹配，则对第一业务请求进行下一步处理可以为：通过对所述第一业务请求的认证，服务器将响应所述第一业务请求；否则，对第一业务请求进行下一步处理可以为：不通过对所述第一业务请求的认证，服务器将向所述第一终端返回认证失败的消息。

[0093] 通过以上步骤101至步骤106的方案，将链接至服务器的终端与服务器认定的合法终端(即用户预先设定的终端标识对应的终端)进行适配，即使服务器下发给合法终端的链接地址被非法盗用，但只要合法终端处于安全状态没有被非法使用，服务器就能够识别出链接至本地的终端不是合法终端，不会通过对业务请求的认证，可提高业务认证的可靠性。

[0094] 上述步骤101至步骤106方案是以终端标识来判断发起所述第一链接请求的终端

是否是合法终端，进一步地，还可以以终端的设备信息来判断发起所述第一链接请求的终端是否是合法终端，本申请实施例所涉及的设备信息可以为以下至少一个信息：

[0095] 终端的设备型号、终端内操作系统的版本号、终端内浏览器的版本号、终端显示屏的大小和分辨率。

[0096] 以终端的设备信息来判断发起所述第一链接请求的终端是否是合法终端的具体实现方式为：

[0097] 步骤104′：服务器确定发起所述第一链接请求的终端的设备信息。

[0098] 本步骤104′可以是与步骤104同时执行的步骤，也可以是在步骤104之前执行或是之后执行，本实施例一并不对步骤104′和步骤104之间的先后执行顺序做限定。

[0099] 步骤105′：服务器将确定的所述设备信息与所述第二终端的设备信息进行匹配。

[0100] 本步骤105′可以是与步骤105同时执行的步骤，也可以是在步骤105之前执行或是之后执行，本实施例一并不对步骤105′和步骤105之间的先后执行顺序做限定。

[0101] 服务器将发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息进行匹配是指：服务器判断发起所述第一链接请求的终端的设备信息是否与所述第二终端的设备信息相同，若相同，则匹配结果为发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息匹配；若不相同，则匹配结果为发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息不匹配。

[0102] 服务器除了将发起所述第一链接请求的终端的设备信息直接与第二终端的设备信息进行是否相同的匹配操作外，也可以将设备信息转换为数值后通过诸如散列(hash，也可称之为哈希)运算得到的运算结果进行匹配。

[0103] 例如，服务器将第二终端的设备信息转换为数值(例如，所述第二终端的设备信息为终端内浏览器的版本号，该版本号为2.3.7，将该版本号转换为数值2×100+3×10+7=237)后，通过hash运算等方式，生成包含N(N为正整数)位字母或数字的散列字符串；然后服务器将发起所述第一链接请求的终端的设备信息按照相同的运算生成N位散列字符串后，将发起所述第一链接请求的终端的设备信息生成的N位散列字符串与第二终端的设备信息生成的N位散列字符串进行匹配，若这两个N位散列字符串相同，则匹配结果为发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息匹配；否则，匹配结果为发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息不匹配。

[0104] 当经过步骤105和步骤105′的匹配操作后，在步骤106中，服务器需同时参考这两个步骤的匹配结果，只有在两个步骤的匹配结果为：发起所述第一链接请求的终端的终端标识与所述第二终端的终端标识匹配且发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息匹配时，通过对所述第一业务请求的认证；否则，不通过对所述第一业务请求的认证。

[0105] 在本申请实施例的方案中，服务器需要在步骤105′之前确定第二终端的设备信息，以便于在步骤105′中可根据确定的第二终端的设备信息进行匹配操作。服务器包括但不限于通过以下两种方式确定第二终端的设备信息：

[0106] 方式一：

[0107] 在本实施例一的方案执行之前，若第二终端以往访问过所述服务器，则服务器根据第二终端访问本地时的历史记录信息，确定所述第二终端的设备信息。

[0108] 方式二：

[0109] 在本实施例一的方案执行之前，服务器可按照与实施例一类似方式与使用与所述第二终端绑定的所述用户账号的终端进行交互，在确定该终端是第二终端时，存储该第二终端的设备信息，以在执行实施例一时，确定第二终端的设备信息，具体执行过程为：

[0110] 第一步：服务器在以往接收到使用与所述第二终端绑定的用户账号的终端发送的第二业务请求时，生成能够链接至访问位置的第二链接地址。

[0111] 发送所述第二业务请求的终端可以是第一终端，也可以其他使用与所述第二终端绑定的用户账号的终端。

[0112] 所述第二业务请求与所述第一业务请求可以是相同内容的业务请求，也可以是不同内容的业务请求，这里的“第一”、“第二”用于区分两次发送的业务请求。

[0113] 所述第一链接地址与所述第二链接地址是服务器分别为第一业务请求和第二业务请求生成的不同的链接地址。

[0114] 第二步：服务器将所述第二链接地址发送给所述第二终端。

[0115] 第三步：服务器根据通过所述第二链接地址发起的第二链接请求确定发起第二链接请求的终端的终端标识和该终端的设备信息。

[0116] 所述第一链接请求和第二链接请求可以是相同类型的链接请求，这里的“第一”、“第二”用于区分两次业务认证过程中涉及的链接请求。

[0117] 第四步：服务器根据发起所述第二链接地址的终端的终端标识与所述第二终端的终端标识的匹配结果，判断是否通过对所述第二业务请求的认证，若通过，且设定时长内没有接收到告警信息，表示向服务器发起第二链接请求的终端确实是合法的第二终端，服务器在本地存储发起所述第二链接请求的终端的设备信息，并确定该设备信息是第二终端的设备信息。

[0118] 通过本申请实施例一的方案，通过链接至服务器的终端的终端标识与用户预先设定的终端标识对应的合法终端进行适配(优选地，将链接至服务器的终端的终端标识和设备信息与合法终端的终端标识和设备信息进行适配)，即使服务器下发给合法终端的链接地址被非法盗用，但只要合法终端处于安全状态没有被非法使用，服务器就能够识别出通过所述链接地址链接至本地的终端不是合法终端，不会通过对业务请求的认证，以此来提高业务认证的可靠性。

[0119] 需要说明的是，本申请实施例一的方案可以与传统的业务认证方法结合使用，如：将本申请实施例一的方案与背景技术中描述的校验码方法结合进行业务认证。

[0120] 实施例二：

[0121] 本申请实施例二还提供了一种与实施例一属于同一发明构思下的业务认证系统，如图2所示，所述系统包括服务器11和第二终端12，其中：

[0122] 服务器11用于根据接收到的由用户发送的第一业务请求，生成能够链接至访问位置的第一链接地址，确定第二终端标识，将所述第一链接地址发送给所述第二终端标识对应的第二终端12，所述第二终端标识是所述用户预先设定的终端标识，以及，根据通过所述第一链接地址发起的第一链接请求确定发起该第一链接请求的终端的终端标识，将确定的所述终端标识与所述第二终端的终端标识进行匹配，并根据匹配结果对所述第一业务请求进行下一步处理；

[0123] 第二终端12用于接收所述服务器11发送的第一链接地址，并通过该第一链接地址向服务器11发起所述第一链接请求。

[0124] 所述系统还包括：

[0125] 第一终端13，用于根据用户的指示发起所述第一业务请求。

[0126] 其中，第一终端与第二终端为不同终端或第一终端与第二终端为同一终端。

[0127] 进一步地，所述服务器11还用于确定第二终端设备信息，以及确定发起所述第一链接请求的终端的设备信息，并将发起所述第一链接请求的终端的设备信息与所述第二终端的设备信息进行匹配。

[0128] 进一步地，所述服务器11可通过两种方式来确定第二终端的设备信息，分别描述如下：

[0129] 方式一：

[0130] 所述服务器11还用于根据所述第二终端访问该服务器的历史记录信息，确定所述第二终端的设备信息。

[0131] 方式二：

[0132] 所述服务器11还用于在以往接收到使用与所述第二终端绑定的用户账号的终端发送的第二业务请求时，生成能够链接至访问位置的第二链接地址，将所述第二链接地址发送给所述第二终端，并根据通过所述第二链接地址发起的第二链接请求确定发起该第二链接请求的终端的终端标识和该终端的设备信息，以及，若确定发起所述第二链接请求的终端的终端标识与所述第二终端的终端标识匹配，且在通过对所述第二业务请求的认证后的设定时长内没有接收到告警信息，则确定发起所述第二链接请求的终端的设备信息为第二终端的设备信息。

[0133] 实施例三：

[0134] 本申请实施例还描述了实施例一和实施例二中所涉及的服务器，如图3所示，所述服务器包括接收模块21、链接地址生成模块22、发送模块23、确定模块24和匹配模块25，其中：

[0135] 接收模块21用于接收由用户发送的第一业务请求；

[0136] 链接地址生成模块22用于生成能够链接至访问位置的第一链接地址；

[0137] 发送模块23用于将所述第一链接地址发送给确定的第二终端标识对应的第二终端，所述第二终端标识是用于预先设定的终端标识；

[0138] 确定模块24用于根据通过所述第一链接地址发起的第一链接请求确定发起该第一连接请求的终端的终端标识；

[0139] 匹配模块25用于将确定的所述终端标识与第二终端的终端标识进行匹配，并根据匹配结果对所述第一业务请求进行下一步处理。

[0140] 进一步地，所述服务器还包括设备信息确定模块26，用于确定第二终端的设备信息；

[0141] 所述确定模块24还用于确定发起所述第一链接请求的终端的设备信息；

[0142] 所述匹配模块25还用于将发起所述第一链接请求的终端的设备信息与第二终端的设备信息进行匹配。

[0143] 所述设备信息确定模块26确定第二终端的设备信息的方式包括以下两种方式：

[0144] 方式一：

[0145] 所述设备信息确定模块26，具体用于根据所述第二终端访问该服务器的历史记录信息，确定所述第二终端的设备信息。

[0146] 方式二：

[0147] 所述设备信息确定模块26与服务器中的其他模块共同确定第二终端的设备信息，具体为：

[0148] 所述接收模块21还用于在以往接收使用与所述第二终端绑定的用户账号的终端发送的第二业务请求；

[0149] 所述链接地址生成模块22还用于生成能够链接至访问位置的第二链接地址；

[0150] 所述发送模块23还用于将所述第二链接地址发送给第二终端；

[0151] 所述确定模块24还用于根据通过所述第二链接地址发起的第二链接请求确定发起该第二链接请求的终端的终端标识和该终端的设备信息；

[0152] 所述匹配模块25还用于将发起所述第二链接请求的终端的终端标识与所述第二终端的终端标识进行匹配；

[0153] 所述设备信息确定模块26具体用于在所述匹配模块25确定发起所述第二链接请求的终端的终端标识与所述第二终端的终端标识匹配，且在通过对所述第二业务请求的认证后的设定时长内没有接收到告警信息，则确定发起所述第二链接请求的终端的设备信息为第二终端的设备信息。

[0154] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0155] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0156] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0157] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0158] 在一个典型的配置中，所述计算机设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。内存可能包括计算机可读介质中的非永久性存储器，随机存取存储

器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带,磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括非持续性的电脑可读媒体(transitory media),如调制的数据信号和载波。

[0159] 尽管已描述了本申请的优选实施例,但本领域内的技术人员一旦得知了基本创造性概念,则可对这些实施例做出另外的变更和修改。所以,所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

[0160] 显然,本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样,倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内,则本申请也意图包含这些改动和变型在内。

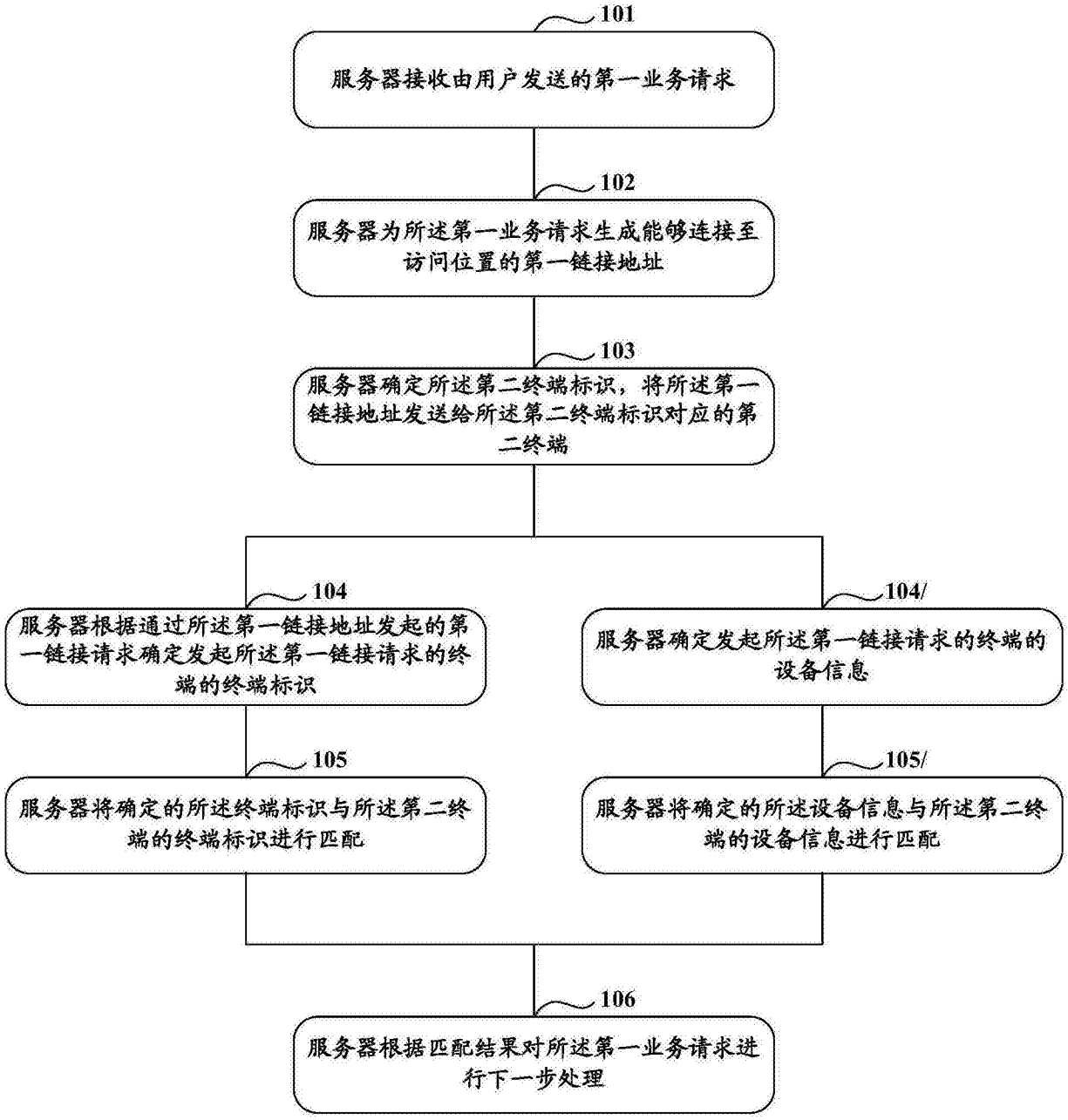

101
服务器接收由用户发送的第一业务请求
102
服务器为所述第一业务请求生成能够连接至访问位置的第一链接地址
103
服务器确定所述第二终端标识，将所述第一链接地址发送给所述第二终端标识对应的第二终端
104
服务器根据通过所述第一链接地址发起的第一链接请求确定发起所述第一链接请求的终端的终端标识
104/
服务器确定发起所述第一链接请求的终端的设备信息
105
服务器将确定的所述终端标识与所述第二终端的终端标识进行匹配
105/
服务器将确定的所述设备信息与所述第二终端的设备信息进行匹配
106
服务器根据匹配结果对所述第一业务请求进行下一步处理

图1

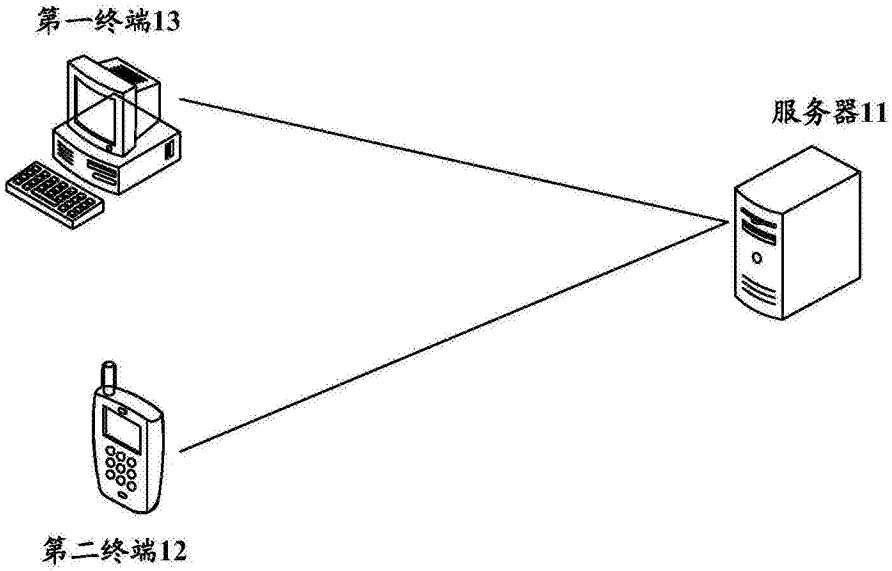

第一终端13
服务器11
第二终端12

图2

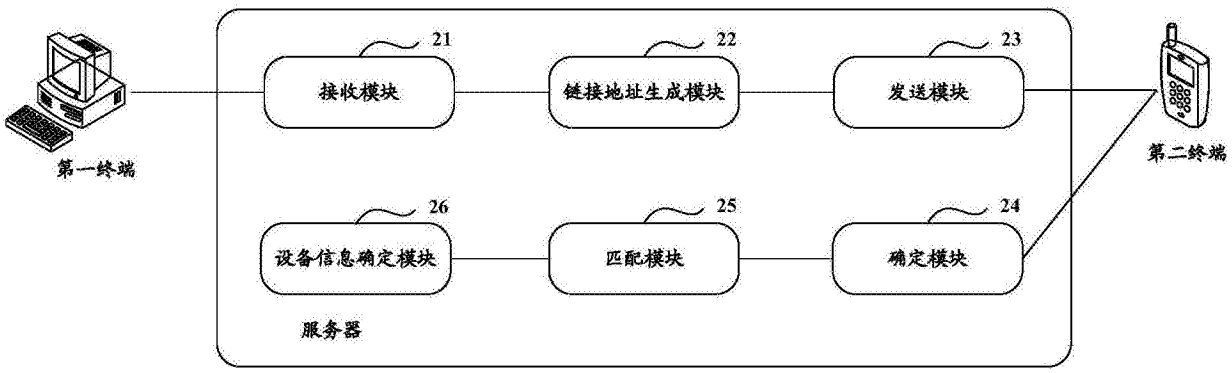

21
接收模块
22
链接地址生成模块
23
发送模块
第一终端
第二终端
26
设备信息确定模块
25
匹配模块
24
确定模块
服务器

图3