(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107196970 A
(43)申请公布日 2017.09.22

(21)申请号 201710577635.1

(22)申请日 2017.07.15

(71)申请人 深圳市华琥技术有限公司
地址 518000 广东省深圳市罗湖区东门街道解放路3002号港岛银座3321

(72)发明人 邓欢欢

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/12(2006.01)

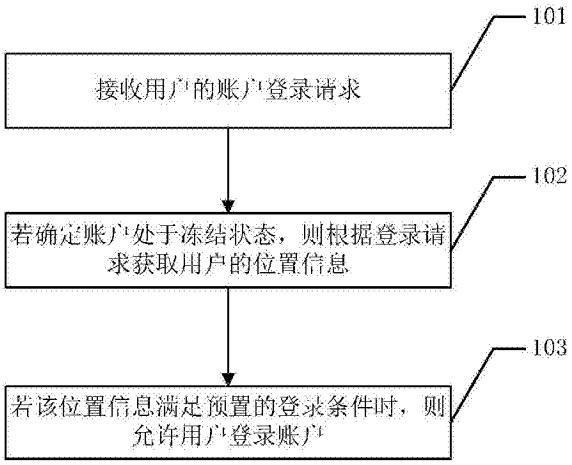
权利要求书2页 说明书12页 附图6页

(54)发明名称

一种安全认证方法、服务器

(57)摘要

本发明实施例公开了一种安全认证方法、服务器以及安全认证系统，能够避免冻结处理对正常用户使用账户的影响。本发明实施例方法包括：服务器接收用户发送的账户登录请求，所述登录请求中包含请求登录的账户的标识信息；所述服务器判断所述标识信息是否包含于冻结数据库中，所述冻结数据库中包含已被冻结的账户的标识信息；若所述标识信息包含于所述冻结数据库中，则所述服务器从所述账户登录请求中读取所述用户的网络地址；根据网络地址与位置信息之间的对应关系，查询所述用户的网络地址对应的所述用户的位置信息；判断所述位置信息是否满足预置的登录条件，若满足，则允许所述用户登录所述账户。



CN 107196970 A

1.一种安全认证方法,其特征在于,包括:

服务器接收用户发送的账户登录请求,所述登录请求中包含请求登录的账户的标识信息;

所述服务器判断所述标识信息是否包含于冻结数据库中,所述冻结数据库中包含已被冻结的账户的标识信息;

若所述标识信息包含于所述冻结数据库中,则所述服务器从所述账户登录请求中读取所述用户的网络地址;

根据网络地址与位置信息之间的对应关系,查询所述用户的网络地址对应的所述用户的位置信息;

判断所述位置信息是否满足预置的登录条件,若满足,则允许所述用户登录所述账户。

2.根据权利要求1所述的方法,其特征在于,所述根据网络地址与位置信息之间的对应关系,查询所述用户的网络地址对应的所述用户的位置信息之后,所述方法还包括:

所述服务器判断所述账户是否属于高风险账户;

若属于,则所述服务器从转发所述登录请求的消息转发网元获取所述用户的网络地址;

所述服务器判断从所述消息转发网元获取到的网络地址与从所述账户登录请求中读取到的网络地址是否匹配,若不匹配,则使用从所述消息转发网元获取到的网络地址进行后续操作。

3.根据权利要求2所述的方法,其特征在于,所述服务器判断所述账户是否属于高风险账户包括:

所述服务器判断所述账户在历史预置时间内是否发生过地址诈骗行为,若是,则确定所述账户属于高风险账户。

4.根据权利要求1至3中任一项所述的方法,其特征在于,所述方法还包括:

根据历史登录行为确定所述用户的常用登录区域;

所述判断所述位置信息是否满足预置的登录条件具体为:

判断所述位置信息是否属于所述常用登录区域,若属于,则确定满足所述预置的登录条件,若不属于,则确定不满足所述预置的登录条件。

5.根据权利要求4所述的方法,其特征在于,所述根据历史登录行为确定所述用户的常用登录区域包括:

根据历史登录行为确定所述用户的各登录区域;

查询登录次数达到预置数值的目标登录区域,并将所述目标登录区域作为所述用户的常用登录区域。

6.根据权利要求4所述的方法,其特征在于,所述根据历史登录行为确定所述用户的常用登录区域包括:

根据历史登录行为确定所述用户的各登录区域;

查询最近预置时长内登录次数达到预置数值的目标登录区域,并将所述目标登录区域作为所述用户的常用登录区域。

7.根据权利要求4所述的方法,其特征在于,所述根据历史登录行为确定所述用户的常用登录区域包括:

根据历史登录行为确定所述用户的各登录区域；

根据第一权值以及在各登录区域的登录次数确定各登录区域的第一参考值，根据第二权值以及在各登录区域的登录时间确定各登录区域的第二参考值，并将第一参考值与第二参考值之和作为该登录区域的综合参考值；

将综合参考值达到预置数值的登录区域作为所述用户的常用登录区域。

8.一种服务器，其特征在于，包括：

接收单元，用于接收用户的登录请求，所述登录请求中包含请求登录的账户的标识信息；

获取单元，用于当根据所述标识信息确定所述账户处于冻结状态时，根据所述登录请求获取所述用户的位置信息；

认证单元，用于判断所述位置信息是否满足预置的登录条件，若满足，则允许所述用户登录所述账户。

9.根据权利要求8所述的服务器，其特征在于，所述登录请求中还包括登录地址信息；

所述获取单元包括：

第一获取模块，用于从所述登录地址信息中解析出所述用户的网络地址，所述网络地址为互联网协议IP地址，或者为基于位置的服务LBS地址；

第一查询模块，用于根据网络地址与位置信息之间的对应关系，查询所述用户的网络地址对应的所述用户的位置信息。

10.根据权利要求8所述的服务器，其特征在于，所述获取单元包括：

第二获取模块，用于从转发所述登录请求的消息转发网元获取所述用户的网络地址，所述网络地址为互联网协议IP地址，或者为基于位置的服务LBS地址；

第二查询模块，用于根据网络地址与位置信息之间的对应关系，查询所述用户的网络地址对应的所述用户的位置信息。

一种安全认证方法、服务器

技术领域

[0001] 本发明涉及通信领域，尤其涉及一种安全认证方法、服务器以及安全认证系统。

背景技术

[0002] 随着互联网技术的不断发展，互联网的开放程度越来越高，相应的，木马病毒等也开始横行，互联网环境中用户的账户安全很难得到保证。账户被他人盗取的现象无法从根源上杜绝，被盗用的账户一般用来发色情、诈骗广告等恶意信息。

[0003] 现有技术中的账户保护方法一般为：当检测到某个用户的账户不断发送色情、诈骗广告等恶意信息时，则对会该账户进行冻结处理，使得该账户在一段时间内、甚至永久无法登陆。

[0004] 但是，如果该账户是被他人盗取使用的，那么直接对该账户进行冻结处理则会影响正常用户对该账户的使用。

发明内容

[0005] 本发明实施例提供了一种安全认证方法、服务器以及安全认证系统，能够避免冻结处理对正常用户使用账户的影响。

[0006] 本发明实施例提供的安全认证方法，其特征在于，包括：

[0007] 服务器接收用户发送的账户登录请求，所述登录请求中包含请求登录的账户的标识信息；

[0008] 所述服务器判断所述标识信息是否包含于冻结数据库中，所述冻结数据库中包含已被冻结的账户的标识信息；

[0009] 若所述标识信息包含于所述冻结数据库中，则所述服务器从所述账户登录请求中读取所述用户的网络地址；

[0010] 根据网络地址与位置信息之间的对应关系，查询所述用户的网络地址对应的所述用户的位置信息；

[0011] 判断所述位置信息是否满足预置的登录条件，若满足，则允许所述用户登录所述账户。

[0012] 从以上技术方案可以看出，本发明实施例具有以下优点：

[0013] 本发明实施例中，服务器可以接收用户的登录请求，该登录请求中包含请求登录的账户的标识信息，当服务器根据该标识信息确定该账户处于冻结状态时，可以根据登录请求获取用户的位置信息，并判断位置信息是否满足预置的登录条件，若满足，则允许用户登录账户，所以当某个账户处于冻结状态时，服务器并不会拒绝所有用户对该账户的登录，而是根据用户登录时的位置信息来区分处理，当用户登录时的位置信息满足预置的登录条件时，则允许该用户登录该账户，由于账户所有人(即正常用户)一般都会在比较固定的区域进行登录，所以根据用户登录时的位置信息对用户的登录请求进行区分处理可以有效的避免冻结处理对正常用户使用账户的影响。

附图说明

[0014] 为了更清楚地说明本发明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单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0015] 图1为本发明实施例所提供的一种安全认证方法的一个实施例的步骤流程图。

[0016] 图2为本发明实施例所提供的一种安全认证方法的另一个实施例的步骤流程图。

[0017] 图3为本发明实施例所提供的确定用户的常用登录区域的一个实施例的步骤流程图。

[0018] 图4为本发明实施例所提供的确定用户的常用登录区域的另一个实施例的步骤流程图。

[0019] 图5为本发明实施例所提供的确定用户的常用登录区域的另一个实施例的步骤流程图。

[0020] 图6为本发明实施例所提供的一种服务器的一个实施例的结构示意图。

[0021] 图7为本发明实施例所提供的一种服务器的另一个实施例的结构示意图。

[0022] 图8为本发明实施例所提供的一种服务器的另一个实施例的结构示意图。

[0023] 图9为本发明实施例所提供的一种服务器的另一个实施例的结构示意图。

具体实施方式

[0024] 下面将结合本发明实施例中的附图，对本发明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发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域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，都属于本发明保护的范围。

[0025] 以下结合附图1说明本发明实施例是如何有效的避免冻结处理对正常用户使用账户的影响做详细说明。

[0026] 101、接收用户的账户登录请求；

[0027] 当有权用户通过手机登录互联网服务应用时，用户需要向手机发送账户登录请求，手机将其接收到的账户登录请求发送给服务器；

[0028] 当然用户还可通过平板电脑或PAD等移动终端发送账户登录请求；

[0029] 其中，该登录请求中包含请求登录账户的标识信息，且通过该标识信息能够判断出该账户是否处于冻结状态。

[0030] 102、若确定账户处于冻结状态，则根据登录请求获取用户的位置信息；

[0031] 当服务器根据其接收到的账户登录请求中的标识信息判断出该账户处于冻结状态时，则根据该登录请求获取用户的位置信息。

[0032] 103、若该位置信息满足预置的登录条件时，则允许用户登录账户；

[0033] 当服务器判断出其获取到的位置信息满足服务器预先设置的登录条件时，则服务器解除对该用户账户的限制措施，从而允许该用户正常登陆该账户。

[0034] 本实施例中，服务器可以接收用户的登录请求，该登录请求中包含请求登录的账

户的标识信息，当服务器根据该标识信息确定该账户处于冻结状态时，可以根据登录请求获取用户的位置信息，并判断位置信息是否满足预置的登录条件，若满足，则允许用户登录账户，所以当某个账户处于冻结状态时，服务器并不会拒绝所有用户对该账户的登录，而是根据用户登录时的位置信息来区分处理，当用户登录时的位置信息满足预置的登录条件时，则允许该用户登录该账户，由于账户所有人(即正常用户)一般都会在比较固定的区域进行登录，所以根据用户登录时的位置信息对用户的登录请求进行区分处理可以有效的避免冻结处理对正常用户使用账户的影响。

[0035] 以下结合图2对本发明是如何实现安全认证的方法做进一步的详细说明，其具体包括步骤：

[0036] 201、接收用户的账户登录请求；

[0037] 本实施例的步骤201的过程与前述图1所示的实施例中描述的步骤101过程相同，在此不再赘述。

[0038] 202、判断账户是否处于冻结状态；

[0039] 因该账户登录请求中包含有用于指示该账户是否处于冻结状态的标识信息；

[0040] 服务器根据其接收到的标识信息判断当前账户是否处于冻结状态；若否，则进入步骤203；若是，则进入步骤204。

[0041] 203、允许用户登录该账户；

[0042] 服务器根据其接收到的标识信息判断出用户当前账户没有处于冻结状态，即该账户没有进行发送色情、垃圾广告等异常行为，则服务器无需对该账户进行限制，所以用户可以正常登录该账户。

[0043] 204、判断用户是否通过消息转发网元访问互联网服务应用，若否，则进行205，若是，则进行207；

[0044] 因服务器已经根据标识信息判断出账户处于冻结状态，即该账户进行了异常行为，服务器为保障安全已经对该账户进行了限制，此时服务器需要进一步的获取该用户的位置信息，以使得服务器根据该用户的位置信息判断用户是否可以登录该处于冻结处理状态的账户；

[0045] 又因用户访问互联网服务应用时，可以是通过用户真实的网络地址访问互联网服务应用，也可以是通过消息转发网元即代理服务器访问互联网服务应用；

[0046] 即当通过204判断出用户没有通过消息转发网元访问互联网服务应用时，说明用户访问互联网应用时，使用的是其自身真实的网络地址，则进入步骤205；

[0047] 当通过204判断出用户通过消息转发网元访问互联网服务应用时，说明用户访问互联网服务应用时，其使用的不是用户真实的网络地址，为了获取到用户真实的位置信息，则进入207。

[0048] 205、获取该登陆请求中包括的登录地址信息；

[0049] 服务器解析用户发送的登陆请求，并获取该登录请求中包括的登录地址信息。

[0050] 206、从该登录地址信息中解析出用户的网络地址；

[0051] 服务器从登录地址信息中解析出用户的网络地址；

[0052] 其中，该网络地址为互联网协议IP地址，或者为LBS(基于位置的服务，Location Based Service)地址。

[0053] 207、从转发该登录请求的消息转发网元获取用户的网络地址；

[0054] 为了获取到用户真实的网络地址，则服务器从转发该登录请求的消息转发网元获取用户的网络地址；

[0055] 且该网络地址为互联网协议IP地址，或者为基于位置的服务LBS地址。

[0056] 通过206或207使得服务器能够获取到用户真实的网络地址，当服务器获取到真实的网络地址之后，则进行208。

[0057] 208、根据网络地址与位置信息之间的对应关系，查询用户的网络地址对应的用户的位置信息；

[0058] 即在服务器端预先建立一位置信息查询列表，该列表建立了网络地址与位置信息的对应关系，当服务器获取到用户的网络地址后，通过该网络地址查询该位置信息查询列表，进而能够获取到与该网络地址对应的用户的位置信息。

[0059] 209、判断位置信息是否满足预置的登录条件；

[0060] 若是，则返回203；即位置信息满足预置的登陆条件，则服务器允许用户登录该账户；

[0061] 若否，则进行210；

[0062] 其中，服务器预先设置的预置条件为：服务器所获取到的位置信息是否属于用户常用登陆区域；

[0063] 服务器预先根据用户的历史登陆行为确定该用户的常用登陆区域；其中，如何根据历史登陆行为确定用户的常用登陆区域的具体实现方法在后续实施例中详细描述，在此不再赘述。

[0064] 210、禁止用户登陆；

[0065] 当服务器判断出位置信息不满足预置的登陆条件时，即服务器判断出该位置信息不属于用户常用的登陆区域时，则可判断出当前要求进行登陆的用户属于不安全的无权用户，则禁止该用户进行登陆，从而有效的保障了该账户的安全。

[0066] 本实施例中，服务器可判断其接收到的账户登陆请求是否处于冻结状态，并当其处于冻结状态时，进一步判断用户是否通过消息转发网元访问互联网服务应用，并根据判断结果使得服务器从登陆地址信息中解析出用户的网络地址或从转发该登陆请求的消息转发网元获取用户的网络地址，从而使得服务器能够获取到用户真实的网络地址，并根据用户的网络地址获取到用户的位置信息，当确定用户的位置信息满足服务器预置的登陆条件时，则用户可登陆账户，当确定用户的位置信息不满足服务器预置的登陆条件时，则用户不能登陆账户。采用本实施例，使得服务器能够获取到用户真实的位置信息，并能够判断该真实的位置信息是否满足预置的登陆条件，若满足则允许用户登陆，若不满足则禁止用户登陆，其可根据用户登陆时的位置信息对用户的登陆请求进行区分出来，从而有效的避免了冻结处理对正常用户使用账户的影响。

[0067] 在进行图2所示的209时，服务器需要判断位置信息是否属于用户的常用登陆区域，以下结合图3对本实施例是如何确定用户的常用登录区域的一种方法做详细说明；

[0068] 301、根据历史登录行为确定用户的各登录区域；

[0069] 服务器分析用户的历史登陆行为；

[0070] 其中，该历史登陆行为是指，用户在过去登陆互联网应用时的各个登陆区域，并分

别获取各个登陆区域的登陆次数；

[0071] 且服务器建立一登陆区域查询列表，该登陆区域查询列表存储了用户登陆过的各个区域，还存储了与各个登陆过的区域对应的登陆次数。

[0072] 302、查询登录次数达到预置数值的目标登录区域，并将目标登录区域作为用户的常用登录区域；

[0073] 服务器设置一预置数值，该预置数值用于判断用户的常用登陆区域；

[0074] 且该预置数值可以是服务器端统一设置的，也可以是用户根据自身情况通过服务器设置的；例如用户经常需要出差，其常用登陆区域一般就会有多个，那么设置的预置数值可以适当的小些；再如用户基本上在一地，其常用登陆区域一般会有一个，那么设置的预置数值可适当的大些；

[0075] 服务器查询该登陆区域查询列表，并获取登陆次数达到预置数值的目标登陆区域，并将获取到的登陆区域设置为常用登陆区域；

[0076] 其中，常用登陆区域可以是一个，也可以是多个。

[0077] 本实施例中，服务器可根据各个登陆区域的登陆次数确定用户的常用登陆区域，且若用户因各种原因需要多地点停留，则可确定出多个常用登陆区域，这样，可以更准确的根据用户常用登陆区域判断用户是否为安全的有权的登陆用户。

[0078] 本实施在具体应用中可为：

[0079] 服务器获取到甲在北京登陆305次，在广州登陆300次，在上海登陆100次，在深圳登陆50次；

[0080] 服务器分别建立北京与305、广州与300、上海与100、深圳与50的对应关系；

[0081] 服务器设置的预置数值为200；

[0082] 服务器获取登陆次数大于200的登陆区域，即获取到了北京与广州；

[0083] 则服务器确定北京与广州就是用户的常用登陆区域。

[0084] 结合图2与图3所示的实施例，使得服务器能够根据其获取到的用户的位置信息对用户的常用登陆区域进行判断，将用户登陆的次数达到预置数值的登陆区域设置为常用登陆区域，服务器根据该常用登陆区域判断请求登陆的用户是否是安全的有权用户，若是，则允许用户登陆，若否，则禁止用户登陆，进而使得服务器可根据用户登陆时的位置信息对用户的登陆请求进行区分，进而有效的避免了冻结处理对正常用户使用账户的影响。

[0085] 在进行图2所示的209时，服务器需要判断位置信息是否属于用户的常用登陆区域，以下结合图4对本实施例是如何确定用户的常用登录区域的另一种方法做详细说明。

[0086] 401、根据历史登录行为确定用户的各登录区域；

[0087] 即服务器建立登陆区域查询列表，该登陆区域查询列表存储了用户登陆过的各个区域，还存储了与各个登陆过的区域对应的登陆次数；

[0088] 且该登陆区域查询列表还记录有用户分别登录各个登录区域的时间，其中，该登录时间与用户分别登录各个登录区域的登陆次数对应。

[0089] 402、查询最近预置时长内登录次数达到预置数值的目标登录区域，并将目标登录区域作为用户的常用登录区域；

[0090] 服务器设置一预置时长，该预置时长可以是服务器设置的，也可以是用户通过服务器设置的；

[0091] 因用户的生活或工作的方式往往不是一成不变的，如用户从经常出差的工作模式变更为不太需要出差的工作模式，所以服务器根据用户最近一段时间内，即预置时长内用户登陆各个登陆区域的次数获取用户的常用登陆区域，更能够反映出用户生活模式的改变，进而使得获取到的常用登陆区域也会更为准确；

[0092] 其中，本实施例中预置数值的设置方式与图3中302所示的设置方式是相同的，在此不再赘述；

[0093] 具体地，服务器根据预置时长获取常用登陆区域的具体方式是：

[0094] 1、服务器查询登陆区域查询列表所记录的各个登陆区域的登陆时间，并获取登陆时间在该预置时长内的登陆区域；

[0095] 2、服务器获取与登陆时间在预置时长内的登陆区域对应的登陆次数，并获取登陆次数达到预置数值的目标登陆区域；

[0096] 3、将获取到的目标登陆区域设置为常用登陆区域；

[0097] 其中，常用登陆区域可以是一个，也可以是多个。

[0098] 本实施例中，服务器可获取用户在最近预置时长内登陆各个登陆区域的次数，并获取次数达到预置数值的目标登陆区域，并将该目标登陆区域作为用户的常用登陆区域，使得即便用户的工作或生活方式发生很大的改变，也能够准确的获取用户的常用登陆区域。

[0099] 本实施例在具体应用中可为：

[0100] 服务器获取到甲在北京登陆300次，在广州登陆100次，在上海登陆100次，在深圳登陆200次；

[0101] 服务器分别建立了北京与300、广州与100、上海与100、深圳与200的对应关系；

[0102] 服务器分别记录用户每次在北京、广州、上海和深圳的登陆时间；

[0103] 服务器设置的预置时长为30天，则服务器根据其记录的各个登陆区域的登陆时间分别获取用户在以今天为起点的近30天内分别登陆上述各地的次数；

[0104] 即获取到在近30天内，甲在北京登陆0次，在广州和上海各登陆5次，在深圳登陆200次；

[0105] 服务器设置的预置数值为50；

[0106] 则登陆次数达到该预置数值50的仅有深圳；

[0107] 则深圳即为用户的常用登陆区域。

[0108] 结合图2与图4所示的实施例，使得服务器能够根据获取到的用户的位置信息对用户的常用登陆区域进行判断，服务器获取到常用登陆区域需要同时满足两个条件，一个是用户登陆各个登陆区域的时间在预置时长内；另一个是，获取到的登陆区域在预置时长内的登陆次数达到了预置数值；服务器根据该常用登陆区域判断请求登陆的用户是否是安全的有权用户，进而使得服务器可根据用户登陆时的位置信息对用户的登陆请求进行区分，有效的避免了冻结处理对正常用户使用账户的影响。而且即便用户的工作或生活习惯发生较大的改变，也会获取到较为准确的常用登陆区域，服务器更为准确，快速地判断登陆用户是否为安全的有权用户。

[0109] 在进行图2所示的209时，服务器需要判断位置信息是否属于用户的常用登陆区域，以下结合图5对本实施例是如何确定用户的常用登录区域的另一种方法做详细说明。

[0110] 501、根据历史登录行为确定用户的各登录区域；

[0111] 其中，本实施例501所示的过程与图4实施例所示的过程401相同，在此不再赘述。

[0112] 502、根据第一权值以及在各登录区域的登录次数确定各登录区域的第一参考值；

[0113] 服务器设置有第一权值，其还获取用户在各个登陆区域的登陆次数；

[0114] 服务器分别获取各个登陆区域的登陆次数与该第一权值的乘积，并将该乘积作为第一参考值。

[0115] 503、根据第二权值以及在各登录区域的登录时间确定各登录区域的第二参考值；

[0116] 服务器设置有第二权值，其还获取在预置时长内各个登陆区域的登陆次数；

[0117] 且本实施例中503的预置时长的设置方式与图4过程402所示的预置时长的设置方式相同，在此不再赘述；

[0118] 服务器获取登陆次数与该第二权值的乘积，并将该乘积作为第二参考值；

[0119] 其中，该第一权值与第二权值可以是服务器统一设置的，也可以是用户根据自己的实际情况进行设置的；

[0120] 例如，若用户处于经常出差的状态，即其经常登陆区域一般有多个的情况下，用户可通过服务器将第一权值设置的大些，将第二权值设置的小些，从而能够获取到更为准确的常用登陆区域；

[0121] 又如，用户的工作或生活模式发生了改变，从经常需要出差变更为不需要出差的情况，那么用户就可以通过服务器将第二权值设置的大些，将第一权值设置的小些。

[0122] 504、将第一参考值与第二参考值之和作为该登录区域的综合参考值；

[0123] 服务器分别获取各个登陆区域的第一参考值与第二参考值，并分别求出第一参考值与第二参考值的和，并将该和作为登陆区域的综合参考值；

[0124] 其中，服务器获取综合参考值的方式不仅仅局限于分别求取各个登陆区域第一参考值与第二参考值的和，其还可以获取第一参考值与第二参考值的乘积等其他方式，在此不作限定；

[0125] 且服务器还分别建立各个登陆区域与其综合参考值的对应关系。

[0126] 505、将综合参考值达到预置数值的登录区域作为用户的常用登录区域；

[0127] 服务器预先设置有一预置数值，并获取综合参考值达到该预置数值的登陆区域，并将该登陆区域设置为常用登陆区域。

[0128] 本实施例通过该综合参考值对用户账户的常用登陆区域进行判断，其优势是，能够更为精确的获取用户的常用登陆区域，减少判断误差和错误的出现；因现代社会沟通交流的频繁，用户的工作或生活模式并不是一成不变的，采用本实施例更能够符合人们多样化的生活方式，即使用户的生活方式发生较大程度的改变，也依旧能够获取准确的常用登陆区域，从而为服务器准确的判断该登陆用户是否为安全的有权用户打下基础，而且用户可根据自己的生活习惯设置第一权值和第二权值，从而更加的个人化，使得服务器能够针对性的对常用登陆区域进行判断，获取到更为精确的常用登陆区域。

[0129] 本实施例在具体应用中可为：

[0130] 服务器获取到甲在北京登陆300次，在广州登陆100次，在上海登陆50次，在深圳登陆200次；

[0131] 服务器预先设定的第一权值为1；

[0132] 则北京的第一参考值为300*1＝300，广州的第一参考值为100*1＝100，上海的第一参考值为50*1＝50，深圳的第一参考值为200*1＝200；

[0133] 服务器预先设定的第二权值为0.2；

[0134] 服务器设置的预置时长为30天，则获取从用户发送账户登录请求的今日起30日内各个登陆区域的登陆次数；

[0135] 服务器获取到在30日内，用户在北京登陆50次，广州登陆20次，上海登陆0次，深圳登陆150次；

[0136] 则北京的第二参考值为50*0.2＝10，广州的第二参考值为20*0.2＝4，上海的第二参考值为0*0.2＝0，深圳的第二参考值为150*0.2＝30；

[0137] 则服务器获取到：

[0138] 北京的综合参考值为300+10＝310；

[0139] 广州的综合参考值为100+4＝104；

[0140] 上海的综合参考值为50+0＝50；

[0141] 深圳的综合参考值为200+30＝230；

[0142] 服务器设置的预置数值为200；

[0143] 则在本应用例中，北京和深圳的综合参考值大于预置数值200，服务器确定北京和深圳为用户的常用登录区域。

[0144] 结合图2与图5所示的实施例，使得服务器能够根据获取到的用户的位置信息对用户的常用登陆区域进行判断，且服务器计算并获取用户登陆各个登陆区域的综合参考值，根据该综合参考值获取用户的常用登陆地，使得服务器获取到的常用登陆地更为准确，这样，服务器就可根据该常用登陆区域判断请求登陆的用户是否是安全的有权用户，进而使得服务器可根据用户登陆时的位置信息对用户的登陆请求进行区分，从而有效的避免冻结处理对正常用户使用账户的影响。

[0145] 上面对本发明实施例中安全认证方法进行了描述，下面对本发明实施例中服务器的结构进行描述，请参阅图6，本发明实施例中的服务器具体包括：

[0146] 接收单元601，用于接收用户的登录请求，登录请求中包含请求登录的账户的标识信息；

[0147] 获取单元602，用于当根据标识信息确定账户处于冻结状态时，根据登录请求获取用户的位置信息；

[0148] 认证单元603，用于判断位置信息是否满足预置的登录条件，若满足，则允许用户登录所述账户。

[0149] 本实施例中，接收单元601可以接收用户的登录请求，该登录请求中包含请求登录的账户的标识信息，当接收单元601根据该标识信息确定该账户处于冻结状态时，获取单元602可以根据登录请求获取用户的位置信息，认证单元603判断位置信息是否满足预置的登录条件，若满足，则允许用户登录账户，所以当某个账户处于冻结状态时，认证单元603并不会拒绝所有用户对该账户的登录，而是根据用户登录时的位置信息来区分处理，当用户登录时的位置信息满足预置的登录条件时，则允许该用户登录该账户，由于账户所有人(即正常用户)一般都会在比较固定的区域进行登录，所以根据用户登录时的位置信息对用户的登录请求进行区分处理可以有效的避免冻结处理对正常用户使用账户的影响。

[0150] 进一步的参见图7，获取单元602包括：

[0151] 第一获取模块701，用于从登录地址信息中解析出用户的网络地址；

[0152] 网络地址为互联网协议IP地址，或者为基于位置的服务LBS地址；

[0153] 其中，登录请求中预先包括有登录地址信息，所以第一获取模块701即可从登录请求中获取登录地址信息；

[0154] 第一查询模块702，用于根据网络地址与位置信息之间的对应关系，查询用户的网络地址对应的用户的位置信息；

[0155] 即该第一查询模块702根据第一获取模块701获取到的网络地址查询用户的位置信息；

[0156] 第二获取模块703，用于从转发登录请求的消息转发网元获取用户的网络地址，网络地址为互联网协议IP地址，或者为基于位置的服务LBS地址；

[0157] 第二查询模块704，用于根据网络地址与位置信息之间的对应关系，查询用户的网络地址对应的用户的位置信息；

[0158] 即该第二查询模块704根据第二获取模块703获取到的网络地址查询用户的位置信息。

[0159] 为便于理解，下面以一个实际应用场景对本实施例服务器进行详细描述：

[0160] 接收单元601接收用户发送的账户登录请求，且该账户登录请求包含有标识信息；当接收单元601根据该标识信息确定账户是否处于冻结状态时，该接收单元601判断用户是否通过消息转发网元访问互联网服务应用；

[0161] 若用户没有通过消息转发网元访问互联网服务应用，则接收单元601使得第一获取模块701从登录地址信息中解析出用户的网络地址；

[0162] 其中，网络地址为互联网协议IP地址，或者为基于位置的服务LBS地址；且登录请求中预先包括有登录地址信息，所以第一获取模块701即可从登录请求中获取登录地址信息；

[0163] 当第一获取模块701获取到网络地址后，第一查询模块702根据网络地址与位置信息之间的对应关系，查询与用户的网络地址对应的位置信息；

[0164] 若用户通过消息转发网元访问互联网服务应用，则第二获取模块703从转发登录请求的消息转发网元获取用户的网络地址，网络地址为互联网协议IP地址，或者为基于位置的服务LBS地址；当第二获取模块703获取到网络地址后，第二查询模块704根据网络地址与位置信息之间的对应关系，查询用户的网络地址对应的用户的位置信息；

[0165] 认证单元603获取第一查询模块702或二查询模块704查询得到的用户的位置信息，判断该位置信息是否满足预置的登录条件，若满足，则允许用户登录所述账户；若不满足，则禁止用户登陆。

[0166] 本实施例中，接收单元601可判断其接收到的账户登陆请求是否处于冻结状态，并当其处于冻结状态时，进一步判断用户是否通过消息转发网元访问互联网服务应用，进而使得第一获取模块701从登录地址信息中解析出用户的网络地址或使得第二获取模块703从转发登录请求的消息转发网元获取用户的网络地址，从而第一查询模块702或第二查询模块704能够获取到用户真实的网络地址，并根据用户的网络地址获取到用户的位置信息；当认证单元603确定用户的位置信息满足服务器预置的登陆条件时，则用户可登陆账户，当

确定用户的位置信息不满足服务器预置的登陆条件时，则用户不能登陆账户。采用本实施例，使得服务器能够获取到用户真实的位置信息，并能够判断该真实的位置信息是否满足预置的登陆条件，若满足则允许用户登陆，若不满足则禁止用户登陆，其可根据用户登陆时的位置信息对用户的登陆请求进行区分出来，从而有效的避免了冻结处理对正常用户使用账户的影响。

[0167] 更进一步的，结合图8所示，服务器还包括有：

[0168] 确定单元801，用于根据历史登录行为确定用户的常用登录区域；

[0169] 认证单元603具体用于判断位置信息是否属于常用登录区域，若属于，则确定满足预置的登录条件，若不属于，则确定不满足预置的登录条件。

[0170] 其中，结合图9所示，该确定单元801具体包括：

[0171] 第一确定模块8011，用于根据历史登录行为确定用户的各登录区域；

[0172] 第三查询模块8012，用于查询登录次数达到预置数值的目标登录区域，并将目标登录区域作为用户的常用登录区域；

[0173] 第二确定模块8013，用于根据历史登录行为确定用户的各登录区域；

[0174] 第四查询模块8014，查询最近预置时长内登录次数达到预置数值的目标登录区域，并将目标登录区域作为用户的常用登录区域；

[0175] 第三确定模块8015，根据历史登录行为确定所述用户的各登录区域；

[0176] 计算模块8016，用于根据第一权值以及在各登录区域的登录次数确定各登录区域的第一参考值，根据第二权值以及在各登录区域的登录时间确定各登录区域的第二参考值，并将第一参考值与第二参考值之和作为该登录区域的综合参考值；

[0177] 第四确定模块8017，用于将综合参考值达到预置数值的登录区域作为所述用户的常用登录区域。

[0178] 为便于理解，下面以实际应用场景对本实施例服务器是如何确定用户的常用登陆区域进行详细描述：

[0179] 即接收单元601接收用户发送的账户登录请求，该登录请求中包含请求登录的账户的标识信息，当接收单元601根据该标识信息确定该账户处于冻结状态时，获取单元602可以根据登录请求获取用户的位置信息；

[0180] 确定单元801根据历史登录行为确定用户的常用登录区域；

[0181] 具体地，确定单元801的第一确定模块8011根据历史登录行为确定用户的各登录区域，并分别获取各个登陆区域的登陆次数；

[0182] 其中，该历史登陆行为是指，用户在过去登陆互联网应用时的各个登陆区域，服务器建立一登陆区域查询列表，该登陆区域查询列表存储了用户登陆过的各个区域，还存储了与各个登陆过的区域对应的登陆次数；

[0183] 第三查询模块8012根据第一确定模块8011获取的各个登陆区域的登陆次数，查询登录次数达到预置数值的目标登录区域，并将目标登录区域作为用户的常用登录区域；其中第三查询模块8012设置一预置数值，该预置数值用于判断用户的常用登陆区域；

[0184] 或，

[0185] 确定单元801的第二确定模块8013根据历史登录行为确定用户的各登录区域；

[0186] 即第二确定模块8013建立登陆区域查询列表，该登陆区域查询列表存储了用户登

陆过的各个区域，还存储了与各个登陆过的区域对应的登陆次数；且该登陆区域查询列表还记录有分别与各个登陆次数对应的登陆各个登陆区域的时间；

[0187] 第四查询模块8014查询最近预置时长内登录次数达到预置数值的目标登录区域，并将所述目标登录区域作为用户的常用登录区域；

[0188] 或，

[0189] 确定单元801的第三确定模块8015根据历史登录行为确定用户的各登录区域；

[0190] 计算模块8016设置有第一权值，其还获取用户在各个登陆区域的登陆次数，计算模块8016分别获取各个登陆区域的登陆次数与该第一权值的乘积，并将该乘积作为第一参考值；

[0191] 计算模块8016设置有第二权值，其还获取用户在各个登陆区域的登陆时间，并分别获取各个登陆区域的登陆时间与该第二权值的乘积，并将该乘积作为第二参考值，分别获取各个登陆区域的第一参考值与第二参考值；

[0192] 计算模块8016分别求出第一参考值与第二参考值的和，并将该和作为登陆区域的综合参考值；且计算模块8016还分别建立各个登陆区域与其综合参考值的对应关系；

[0193] 其中，计算模块8016获取综合参考值的方式不仅仅局限于分别求取各个登陆区域第一参考值与第二参考值的和，其还可以获取第一参考值与第二参考值的乘积等其他方式，在此不作限定；

[0194] 第四确定模块8017将综合参考值达到预置数值的登录区域作为用户的常用登录区域；

[0195] 认证单元603判读其从获取单元602处获取到的位置信息是否属于确定单元801所确定的用户常用登录区域；若属于，则确定满足预置的登录条件，允许用户正常登陆；若不属于，则确定不满足预置的登录条件，则禁止用户登陆。

[0196] 通过本实施例使得服务器能够根据不同的方式获取用户常用登陆区域，在实际使用中，服务器可向用户提供一个选择列表，用户根据自身的实际情况通过该选择列表选择适合自己的获取方式，从而使得即便用户工作或生活习惯发生较大的改变服务器也能够准确获取到的常用登陆区域。

[0197] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考上述方法实施例中的对应过程，在此不再赘述。

[0198] 在本申请所提供的几个实施例中，应该理解到，所揭露的系统，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，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，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0199] 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。

[0200] 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，也可以采用软件功能单元的形式实现。

[0201] 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时，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，本发明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(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而上述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0202] 以上所述，以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照上述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对上述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

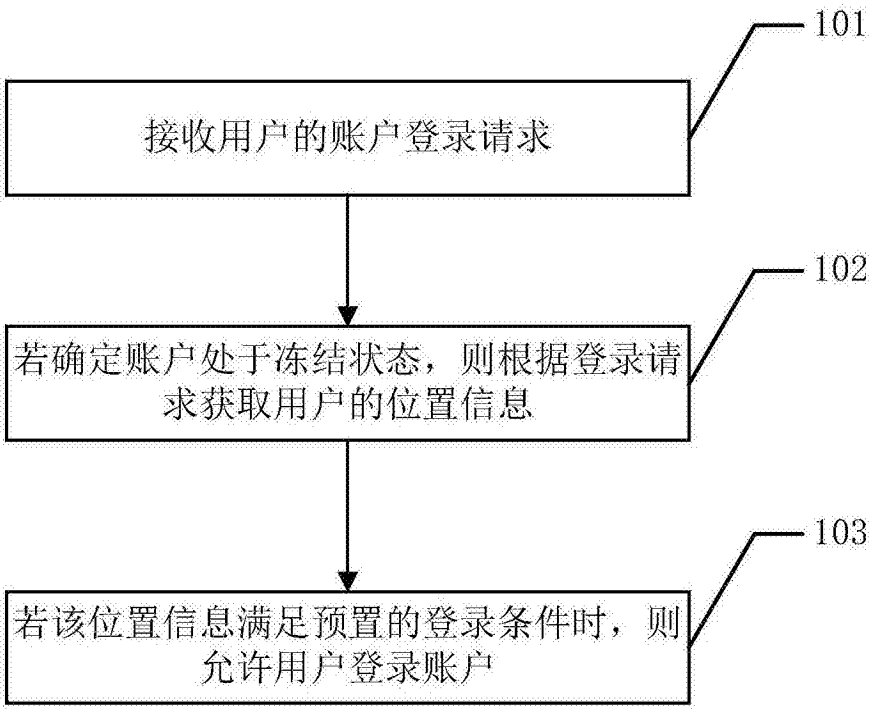

101
接收用户的账户登录请求
102
若确定账户处于冻结状态，则根据登录请求获取用户的位置信息
103
若该位置信息满足预置的登录条件时，则允许用户登录账户

图1

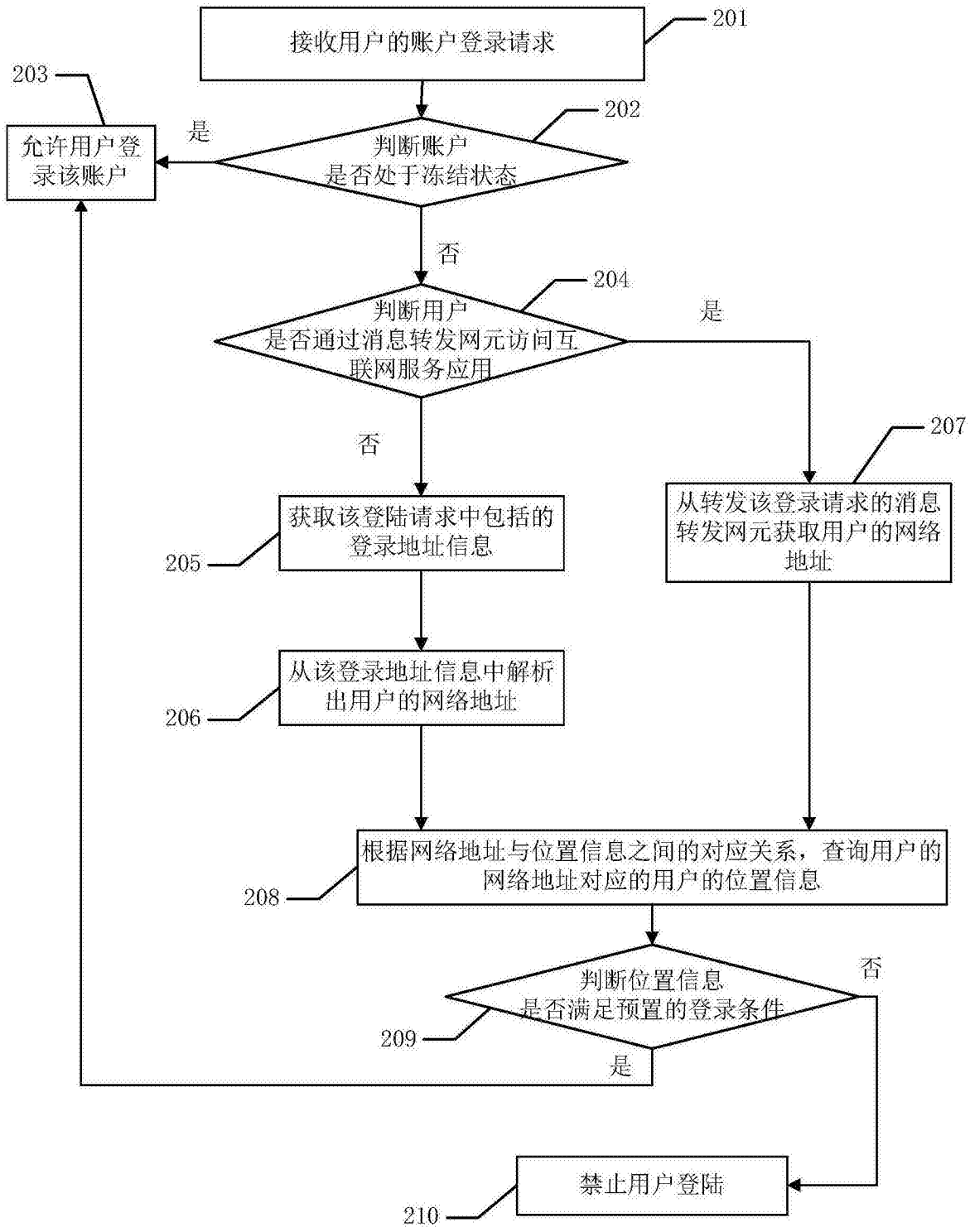

接收用户的账户登录请求
201
判断账户
是否处于冻结状态
202
是
允许用户登
录该账户
203
否
判断用户
是否通过消息转发网元访问互
联网服务应用
204
是
否
获取该登陆请求中包括的
登录地址信息
205
从该登录地址信息中解析
出用户的网络地址
206
从转发该登录请求的消息
转发网元获取用户的网络
地址
207
根据网络地址与位置信息之间的对应关系，查询用户的
网络地址对应的用户的位置信息
208
判断位置信息
是否满足预置的登录条件
209
否
是
禁止用户登陆
210

图2

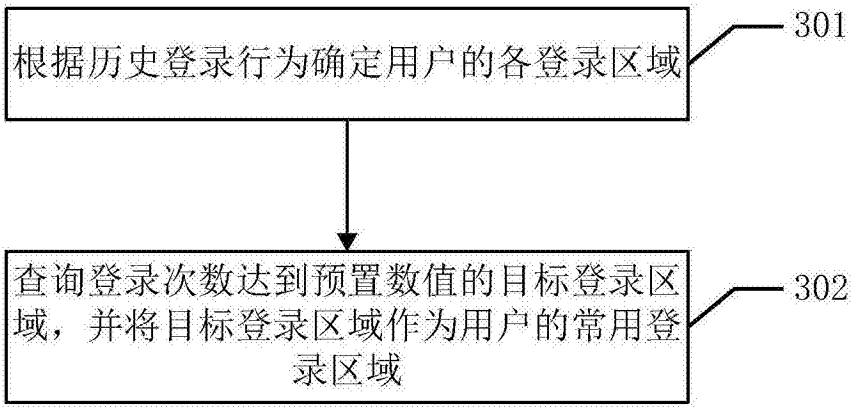

根据历史登录行为确定用户的各登录区域
301
查询登录次数达到预置数值的目标登录区域，并将目标登录区域作为用户的常用登录区域
302

图3

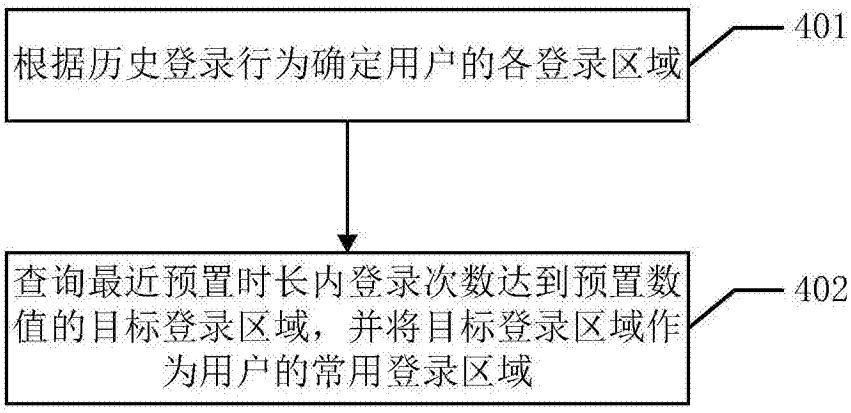

根据历史登录行为确定用户的各登录区域
401
查询最近预置时长内登录次数达到预置数值的目标登录区域，并将目标登录区域作为用户的常用登录区域
402

图4

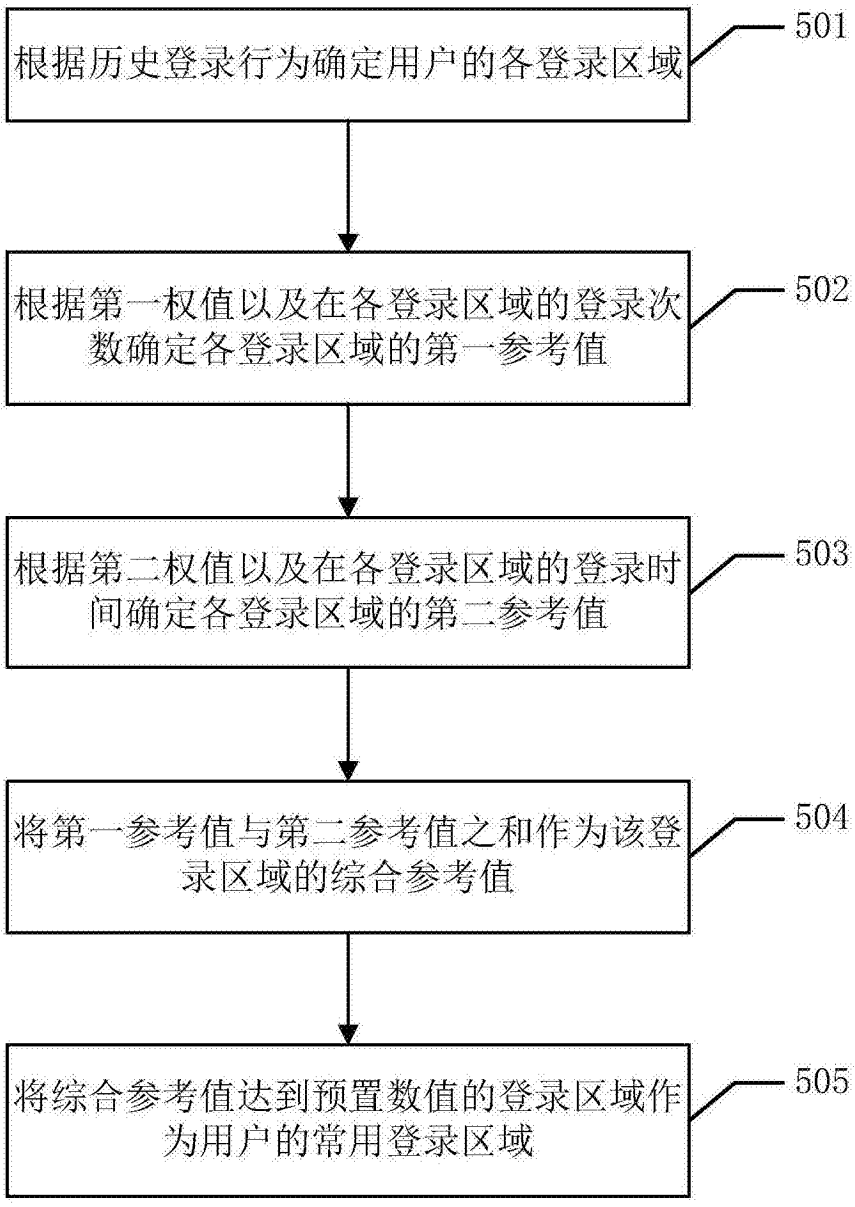

根据历史登录行为确定用户的各登录区域
501
根据第一权值以及在各登录区域的登录次数确定各登录区域的第一参考值
502
根据第二权值以及在各登录区域的登录时间确定各登录区域的第二参考值
503
将第一参考值与第二参考值之和作为该登录区域的综合参考值
504
将综合参考值达到预置数值的登录区域作为用户的常用登录区域
505

图5

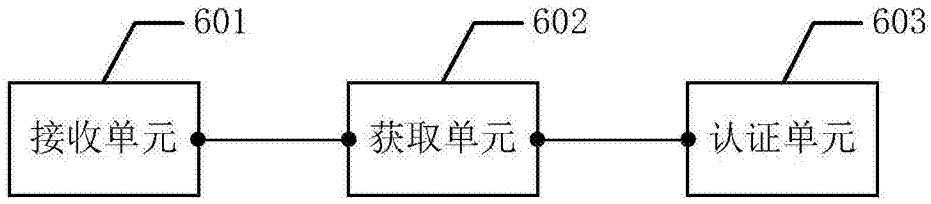

601
接收单元
602
获取单元
603
认证单元

图6

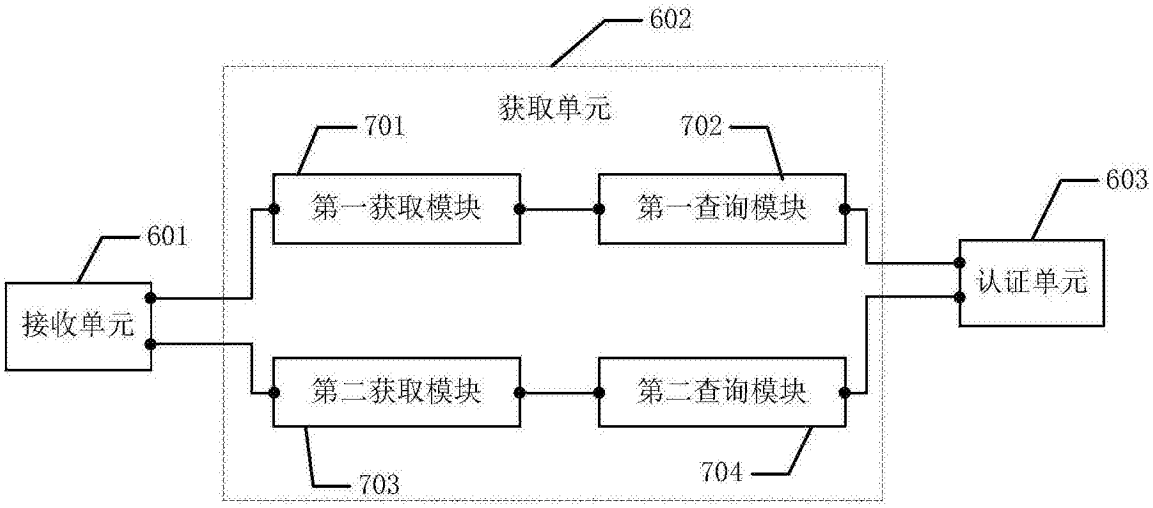

602
获取单元
701
702
第一获取模块
第一查询模块
603
601
认证单元
接收单元
第二获取模块
第二查询模块
703
704

图7

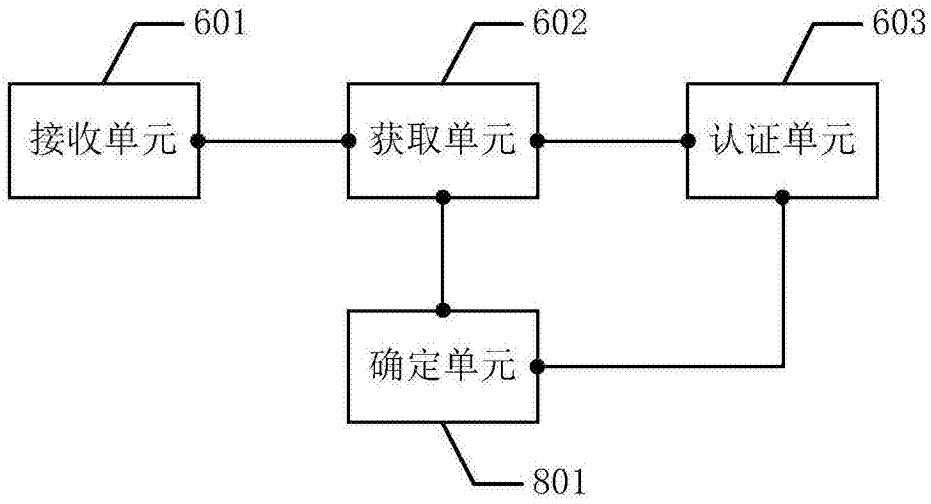

601
602
603
接收单元
获取单元
认证单元
确定单元
801

图8

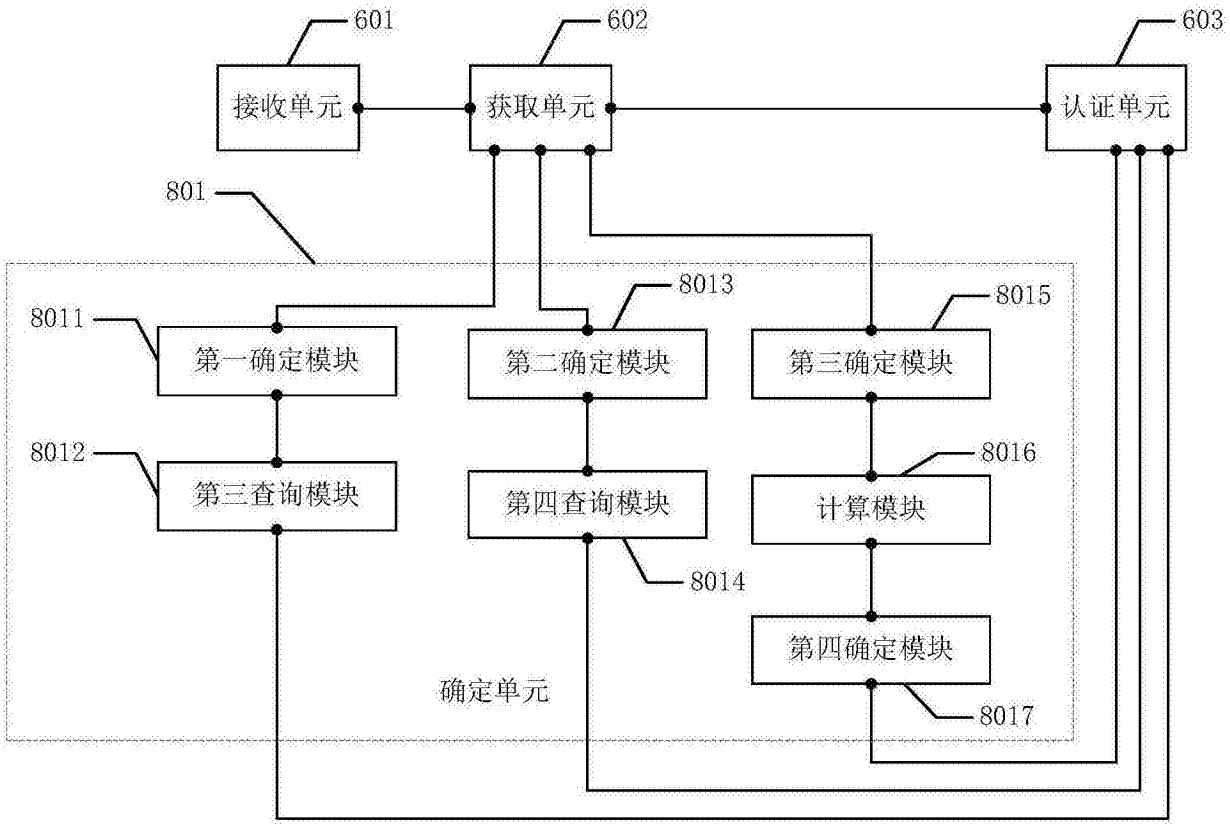

601
602
603
接收单元
获取单元
认证单元
801
8011
8013
8015
第一确定模块
第二确定模块
第三确定模块
8012
8016
第三查询模块
第四查询模块
计算模块
8014
第四确定模块
确定单元
8017

图9