



(12)发明专利申请

(10)申请公布号 CN 108564467 A

(43)申请公布日 2018.09.21

(21)申请号 201810436177.4

(22)申请日 2018.05.09

(71)申请人 平安普惠企业管理有限公司

地址 518000 广东省深圳市前海深港合作区前湾一路1号A栋201室(入驻深圳市前海商务秘书有限公司)

(72)发明人 任钢林 刘杰 李兆鹏 魏全勇

(74)专利代理机构 深圳中一专利商标事务所 44237

代理人 陈宇

(51)Int.Cl.

G06Q 40/02(2012.01)

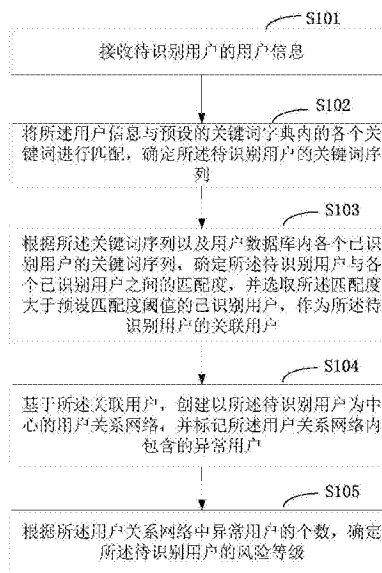
权利要求书3页 说明书13页 附图5页

(54)发明名称

一种用户风险等级的确定方法及设备

(57)摘要

本发明适用于信息处理技术领域,提供了一种用户风险等级的确定方法及设备,包括:接收待识别用户的用户信息;将用户信息与关键词字典内的各个关键词进行匹配,确定待识别用户的关键词序列;根据关键词序列以及用户数据库内各个已识别用户的关键词序列,确定待识别用户与各个已识别用户之间的匹配度,并选取匹配度大于预设匹配度阈值的已识别用户,作为待识别用户的关联用户;基于关联用户,创建以待识别用户为中心的用户关系网络,并标记用户关系网络内包含的异常用户;根据用户关系网络中异常用户的个数,确定待识别用户的风险等级。本发明中能够对于新添加的用户也能快速确定风险等级,对交易请求进行有效管控,降低了资金流失的风险。



1. 一种用户风险等级的确定方法,其特征在于,包括:

接收待识别用户的用户信息;

将所述用户信息与预设的关键词字典内的各个关键词进行匹配,确定所述待识别用户的关键词序列;

根据所述关键词序列以及用户数据库内各个已识别用户的关键词序列,确定所述待识别用户与各个已识别用户之间的匹配度,并选取所述匹配度大于预设匹配度阈值的已识别用户,作为所述待识别用户的关联用户;

基于所述关联用户,创建以所述待识别用户为中心的用户关系网络,并标记所述用户关系网络内包含的异常用户;所述异常用户具体为风险等级超过预设的风险阈值的用户;

根据所述用户关系网络中异常用户的个数,确定所述待识别用户的风险等级。

2. 根据权利要求1所述的确定方法,其特征在于,所述基于所述关联用户,创建以所述待识别用户为中心的用户关系网络,并标记所述用户关系网络内包含的异常用户,包括:

获取各个所述已识别用户的关联用户,以确定所述待识别用户的M度关联用户;其中,所述M度关联用户与所述待识别用户之间的关联路径上存在M-1个用户节点;M为大于或等于1的正整数;

根据所述M度关联用户,创建以所述待识别用户为中心的M度用户关系网,并标记所述M度用户关系网内包含的异常用户。

3. 根据权利要求1所述的确定方法,其特征在于,所述用户信息包含多个信息项目,所述用户的关键词序列包括多个关键词子序列,每个所述关键词子序列对应一个所述信息项目;

所述根据所述关键词序列以及用户数据库内各个已识别用户的关键词序列,确定所述待识别用户与各个已识别用户之间的匹配度,包括:

基于所述关键词子序列,分别计算所述待识别用户与各个已识别用户之间相同的信息项目的相似度;

将各个所述信息项目的相似度导入到匹配度转换模型,计算所述匹配度;所述匹配度转换模型为:

$$Q = \sum_{k=1}^n \alpha_k B_k$$

其中,Q为所述匹配度; $B_k$ 为任意两个所述用户的第k个所述信息项目之间的相似度; $\alpha_k$ 为第k个所述信息项目的匹配权重;n为信息项目的个数。

4. 根据权利要求1-3任一项所述的确定方法,其特征在于,还包括:

获取各个已识别用户的交易行为记录;

将各个所述交易行为记录分别导入到预设的调整系数确定模型,得到各个所述交易行为记录的调整系数;

基于所述调整系数以及各个已识别用户的风险等级,分别调整各个已识别用户的风险等级;

若调整后的所述风险等级超过预设的风险阈值,则识别所述已识别用户为所述异常用户。

5. 根据权利要求1所述的确定方法,其特征在于,所述用户数据库包括本地数据库以及云端数据库;所述本地数据库的初始状态为服务响应状态;所述云端数据库的初始状态为同步数据接收状态;所述确定方法还包括:

若接收到所述已识别用户的交易请求,则在所述本地数据库中创建一个关于所述交易请求的交易行为记录;所述交易行为记录用于记录所述交易请求的响应操作;

若当前时刻满足同步触发条件,则将所述本地数据库存储的所述交易行为记录同步至所述云端数据库;

若检测到所述本地数据库存在数据写入异常,则将所述云端服务器的工作状态调整为所述服务响应状态,以在再次接收到交易请求时,通过所述云端数据库创建并存储交易请求的交易行为记录。

6. 一种用户风险等级的确定设备,其特征在于,所述用户风险等级的确定设备包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序,所述处理器执行所述计算机程序时实现如下步骤:

接收待识别用户的用户信息;

将所述用户信息与预设的关键词字典内的各个关键词进行匹配,确定所述待识别用户的关键词序列;

根据所述关键词序列以及用户数据库内各个已识别用户的关键词序列,确定所述待识别用户与各个已识别用户之间的匹配度,并选取所述匹配度大于预设匹配度阈值的已识别用户,作为所述待识别用户的关联用户;

基于所述关联用户,创建以所述待识别用户为中心的用户关系网络,并标记所述用户关系网络内包含的异常用户;所述异常用户具体为风险等级超过预设的风险阈值的用户;

根据所述用户关系网络中异常用户的个数,确定所述待识别用户的风险等级。

7. 根据权利要求6所述的确定设备,其特征在于,所述基于所述关联用户,创建以所述待识别用户为中心的用户关系网络,并标记所述用户关系网络内包含的异常用户,包括:

获取各个所述已识别用户的关联用户,以确定所述待识别用户的M度关联用户;其中,所述M度关联用户与所述待识别用户之间的关联路径上存在M-1个用户节点;M为大于或等于1的正整数;

根据所述M度关联用户,创建以所述待识别用户为中心的M度用户关系网,并标记所述M度用户关系网内包含的异常用户。

8. 根据权利要求6所述的确定设备,其特征在于,所述用户信息包含多个信息项目,所述用户的关键词序列包括多个关键词子序列,每个所述关键词子序列对应一个所述信息项目;

所述根据所述关键词序列以及用户数据库内各个已识别用户的关键词序列,确定所述待识别用户与各个已识别用户之间的匹配度,包括:

基于所述关键词子序列,分别计算所述待识别用户与各个已识别用户之间相同的信息项目的相似度;

将各个所述信息项目的相似度导入到匹配度转换模型,计算所述匹配度;所述匹配度转换模型为:

$$Q = \sum_{k=1}^n \alpha_k B_k$$

其中,  $Q$ 为所述匹配度;  $B_k$ 为任意两个所述用户的第 $k$ 个所述信息项目之间的相似度;  $\alpha_k$ 为第 $k$ 个所述信息项目的匹配权重;  $n$ 为信息项目的个数。

9. 根据权利要求6-8任一项所述的确设置, 其特征在于, 所述处理器执行所述计算机程序时还实现如下步骤:

获取各个已识别用户的交易行为记录;

将各个所述交易行为记录分别导入到预设的调整系数确定模型, 得到各个所述交易行为记录的调整系数;

基于所述调整系数以及各个已识别用户的风险等级, 分别调整各个已识别用户的风险等级;

若调整后的所述风险等级超过预设的风险阈值, 则识别所述已识别用户为所述异常用户。

10. 一种计算机可读存储介质, 所述计算机可读存储介质存储有计算机程序, 其特征在于, 所述计算机程序被处理器执行时实现如权利要求1至5任一项所述方法的步骤。

## 一种用户风险等级的确定方法及设备

### 技术领域

[0001] 本发明属于信息处理技术领域,尤其涉及一种用户风险等级的确定方法及设备。

### 背景技术

[0002] 随着经济的不断发展,用户向各个金融机构发起交易请求的频率也越来越高,金融机构每天新增用户的数量也不断增加。对于新增用户发起的交易请求,由于金融机构并未记录有新增用户的历史交易记录,无法确定该类用户的信用等级,金融机构一般会同意响应发起新增用户的交易请求。然而部分不法的用户会通过身边的朋友或亲人的资料,注册新用户,利用金融机构无法对新注册用户的交易请求进行管理的漏洞来骗取资金,导致金融机构承担了较大的投资风险。由此可见,现有的用户风险等级的确定技术,主要是针对存在历史交易记录的用户才能够准确进行风险等级评估,而对于新添加的用户却无法进行确定,提高了资金流失的风险。

### 发明内容

[0003] 有鉴于此,本发明实施例提供了一种用户风险等级的确定方法及其设备,以解决现有的用户风险等级的确定方法,主要是针对存在历史交易记录的用户才能够准确进行风险等级评估,而对于新添加的用户却无法进行确定,提高了资金流失的风险的问题。

[0004] 本发明实施例的第一方面提供了一种用户风险等级的确定方法,包括:

[0005] 接收待识别用户的用户信息;

[0006] 将所述用户信息与预设的关键词字典内的各个关键词进行匹配,确定所述待识别用户的关键词序列;

[0007] 根据所述关键词序列以及用户数据库内各个已识别用户的关键词序列,确定所述待识别用户与各个已识别用户之间的匹配度,并选取所述匹配度大于预设匹配度阈值的已识别用户,作为所述待识别用户的关联用户;

[0008] 基于所述关联用户,创建以所述待识别用户为中心的用户关系网络,并标记所述用户关系网络内包含的异常用户;所述异常用户具体为风险等级超过预设的风险阈值的用户;

[0009] 根据所述用户关系网络中异常用户的个数,确定所述待识别用户的风险等级。

[0010] 本发明实施例的第二方面提供了一种用户风险等级的确定设备,包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序,所述处理器执行所述计算机程序时实现第一方面的各个步骤。

[0011] 本发明实施例的第三方面提供了一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,所述计算机程序被处理器执行时实现第一方面的各个步骤。

[0012] 实施本发明实施例提供的一种用户风险等级的确定方法及终端设备具有以下有益效果:

[0013] 本发明实施例通过接收到待识别用户,即新增用户的用户信息时,则确定该用户

信息对应的关键词序列,并基于该关键词序列与用户数据库中的各个已识别用户进行匹配,确定该待识别用户的关联用户,继而创建该待识别用户的用户关系网,并标记出该用户关系网中包含的异常用户;根据异常用户的个数确定该待识别用户的风险等级,从而基于该风险等级可以判定是否响应用户发起的交易请求。与现有的用户风险等级的确定方法相比,本发明实施例不依赖历史交易记录来确定用户的风险等级,而是可以基于该用户的关联用户中包含的异常用户的个数,判断该用户是否属于异常用户群中的成员,并基于个数的不同得到该用户的风险等级,从而对于新添加的用户也能快速确定风险等级,对交易请求进行有效管控,降低了资金流失的风险。

### 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,下面将对实施例或现有技术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。

[0015] 图1是本发明第一实施例提供的一种用户风险等级的确定方法的实现流程图;

[0016] 图2是本发明第二实施例提供的一种用户风险等级的确定方法S104的具体实现流程图;

[0017] 图3是本发明第三实施例提供的一种用户风险等级的确定方法S103的具体实现流程图;

[0018] 图4是本发明第四实施例提供的一种用户风险等级的确定方法具体实现流程图;

[0019] 图5是本发明第四实施例提供的一种用户风险等级的确定方法的具体实现流程图;

[0020] 图6是本发明一实施例提供的一种用户风险等级的确定设备的结构框图;

[0021] 图7是本发明另一实施例提供的一种用户风险等级的确定设备的示意图。

### 具体实施方式

[0022] 为了使本发明的目的、技术方案及优点更加清楚明白,以下结合附图及实施例,对本发明进行进一步详细说明。应当理解,此处所描述的具体实施例仅仅用以解释本发明,并不用于限定本发明。

[0023] 本发明实施例通过接收到待识别用户,即新增用户的用户信息时,则确定该用户信息对应的关键词序列,并基于该关键词序列与用户数据库中的各个已识别用户进行匹配,确定该待识别用户的关联用户,继而创建该待识别用户的用户关系网,并标记出该用户关系网中包含的异常用户;根据异常用户的个数确定该待识别用户的风险等级,从而基于该风险等级可以判定是否响应用户发起的交易请求,解决现有的用户风险等级的确定方法,主要是针对存在历史交易记录的用户才能够准确进行风险等级评估,而对于新添加的用户却无法进行确定,提高了资金流失的风险的问题。

[0024] 在本发明实施例中,流程的执行主体为用户风险等级的确定设备。该用户风险等级的确定设备包括但不限于:笔记本电脑、计算机、服务器、平板电脑以及智能手机等用户风险等级的确定设备。图1示出了本发明第一实施例提供的用户风险等级的确定方法的实

流程图,详述如下:

[0025] 在S101中,接收待识别用户的用户信息。

[0026] 在本实施例中,用户需要发起相关的交易操作之前,需要在该金融机构注册一个用户账号,并填写相关的用户信息。因此,用户风险等级的确定设备可以为用户发起注册请求的服务器,也可以为独立于该服务器外的风险等级的确定设备,用于对该服务器内的所有注册用户进行风险等级的确定操作。其中,该用户信息包括但不限于:姓名、性别、年龄、居住地址、公司名称、公司地址、社会关系等信息。

[0027] 在本实施例中,若用户风险等级的确定设备即为用户所需注册的服务器,则接收到用户的注册请求后,确定设备会采集该用户在注册页面中填写的各项信息,并生成该用户对应的用户信息,并执行S102的相关操作;若该确定设备是独立与用户所需注册的服务器,则服务器在接收到用户的用户信息后,会将该用户信息与用户数据库内各个已识别用户的用户信息进行匹配,确定该用户是否为已登记用户,若存在已识别用户的用户信息与该待识别用户的用户信息一致,则向该待识别用户的终端返回一个已注册信息;反之,若任一已识别用户的用户信息均与该待识别用户的用户信息不一致,则将该待识别用户的用户信息发送给确定设备,确定设备在接收到待识别的用户信息后,则执行S102的相关操作。

[0028] 可选地,S101的触发方式除了接收到注册请求信息这一事件触发模式外,确定设备还可以预设的时间间隔对用户数据库中的各个用户信息进行风险识别,即用户数据库在接收到待识别用户的用户信息后,则会对该待识别用户添加一个待识别标识,当到达预设的检测周期时,确定设备则会从用户数据库中提取带有待识别标识的用户信息执行用户风险等级的确定流程。

[0029] 在S102中,将所述用户信息与预设的关键词字典内的各个关键词进行匹配,确定所述待识别用户的关键词序列。

[0030] 在本实施例中,确定设备存储有一关键词字典,该关键词字典包含多个关键词,每个关键词以固定的顺序依次排列,即每个关键词在关键词字典中有一固定的字典编号。因此,将不同的用户信息与关键词字典进行匹配,得到的关键词序列中相同位置的元素所对应的关键词是相同的。

[0031] 在本实施例中,确定设备会将用户信息与该关键词字典中的各个关键词进行匹配,判断该用户信息中是否包含该关键词。若包含该关键词,则在关键词序列中对应位置的元素中填入该关键词,从而输出的关键词序列则表示该用户信息中包含了那些关键词。由于关键词匹配相对于用户信息匹配而言,精确度较高,能够确定该用户信息中包含的关键信息有哪些,继而将两个用户信息中包含的关键信息的个数进行比对,确定两个用户信息是否为存在关联,从而确定两个用户是否为关联用户。举例性地,某一用户的用户信息为“深圳市南山区海岸集团大厦16楼”,通过关键词字典后识别得到的关键词序列为:{深圳、南山、海岸、集团、16};而另一用户的用户信息为“深圳市福田区海岸集团大楼5楼”,通过关键词匹配后得到的关键词序列为:{深圳、福田、海岸、集团、5},由此可见,两个用户信息相同的关键词的个数为3个,可以识别两个用户信息为关联的用户信息。

[0032] 可选地,该关键词字典可以从上位服务器中获取得到,上位服务器会定时更新该关键词字典。随着社会的不断发展,常常会出现新兴词语,因此关键词字典需要定时进行更新,从而提高对用户信息中关键词识别的准确性。

[0033] 可选地,基于用户信息与关键词字典确定关键字序列的方法可以为:初始化关键词序列,关键词序列中的每个元素依序分别对应所述关键词字典中的一个关键词;根据各个关键词在所述关键词字典中的次序,依次判断所述用户信息中是否包含各个关键词;若所述关键词字典中的关键词被包含于所述用户信息,则设置该关键词在所述关键词序列中的元素为第一位值,例如用“1”标识包含该关键词;若所述关键词字典中的关键词不被包含于所述用户信息,则设置该关键词在所述关键词序列中的元素为第二位值,例如用“2”标识不包含该关键词;基于各个所述元素的位值生成所述用户的关键词序列。即该关键词序列具体为有第一位值以及第二位值所构成的有一定排列顺序的序列。

[0034] 在S103中,根据所述关键词序列以及用户数据库内各个已识别用户的关键词序列,确定所述待识别用户与各个已识别用户之间的匹配度,并选取所述匹配度大于预设匹配度阈值的已识别用户,作为所述待识别用户的关联用户。

[0035] 在本实施例中,记录了各个已识别用户的用户信息的用户数据库可以存储于用户风险等级的确定设备内,在该情况下,确定设备可以直接读取本地存储模块内的用户数据库即可获取得到各个用户的用户信息,特别地,该确定设备可以为一用户数据库服务器。该用户数据库还可以作为一外部独立的数据库服务器,在该情况下,确定设备与该数据库服务器建立通信连接,确定设备会向该数据库服务器发送一个用于鉴权的指令,数据库服务器接收到该指令后判断该识别设备所对应的用户数据库,若该指令鉴权成功,则开放该确定设备的用户数据的获取权限,继而识别设备可以通过该数据库服务器获取各个用户的用户信息。其中,每个已识别用户的用户信息中还记录了其对应的关键词序列。

[0036] 在本实施例中,确定了待识别用户以及已识别用户所对应的关键词序列后,可以基于关键词序列计算待识别用户与各个已识别用户之间的匹配度,继而根据匹配度是否大于预设的匹配度阈值确定两个用户之间是否为关联用户。

[0037] 在本实施例中,该匹配阈值可以为关键词序列中相同关键词的个数,在该情况下,确定设备会统计待识别用户的关键词序列与任一已识别用户的关键词序列中相同关键词的个数,将该个数作为两个用户之间的匹配度,若该两个用户之间的相同关键词的个数大于预设的匹配阈值,则识别两个用户互为关联用户;反之,若该相同关键词的个数小于预设的关联阈值,则识别两个用户为无关用户。该匹配阈值还可以为一相似度阈值,在该情况下,创建设备会计算两个关键词序列的相似度,即相同位置的元素是否相同,计算公式可以为 $\frac{S}{Q}$ ,其中,S为相同元素的个数,Q为元素的总个数,从而得到两个关键词序列之间的相似度,并将该相似度与相似度阈值进行比对,确定两个用户之间是否为关联用户。优选地,在确定两个关键词序列是否相似时,除了判定相同位置的元素是否相同外,还可以判定相同位置的元素是否相似,创建设备记录了与各个关键词关联的模糊关键词,例如“太阳”与“日”两个关键词由于指代的实物均相同,因此可以识别两个关键词之间具有关联性,并识别相同位置具有关键关系的关键词为相似关键词,在计算相似度时,除了考虑相同关键词个数外,还会考虑相似关键词的个数,在该情况下,计算相似度的公式可以为:

$$[0038] \quad Y = a_1 \frac{S}{Q} + a_2 \frac{Sl}{Q} \quad a_1 > a_2$$

[0039] 其中, $a_1$ 、 $a_2$ 为加权系数,Y为两个关键词序列之间的相似度;S为相同位置的元素也

相同的个数;S1为相同位置的元素相似的个数;Q为关键词序列中元素的总个数。

[0040] 在S104中,基于所述关联用户,创建以所述待识别用户为中心的用户关系网络,并标记所述用户关系网络内包含的异常用户;所述异常用户具体为风险等级超过预设的风险阈值的用户。

[0041] 在本实施例中,确定设备在确定了待识别用户的所有关联用户后,可以基于该关联用户构建以待识别用户为中心的用户关系网络,从而管理员可以通过该用户关系网络,快速确定待识别用户与各个已识别用户之间的关联关系。需要说明的是,每个已识别用户均有对应的用户属性,用户属性的取值可以为:正常用户以及异常用户。其中,正常用户具体为风险等级小于或等于预设的风险阈值的用户;而异常用户具体为风险等级超过预设的风险阈值的用户。当然,除了通过已识别用户的风险等级判断其用户属性外,还可以获取已识别用户的历史交易记录,提取历史交易记录的交易特征值,将该交易特征值与预设标准特征值范围进行比对,若该标准特征值范围内,则识别该用户为正常用户,反之,则识别该用户为异常用户。

[0042] 在本实施例中,该用户关系网络不仅记录了待识别用户与其关联用户之间的关联关系,还包含了该待识别用户的各个关联用户之间的关联关系。例如,用户A与用户B均为待识别用户的关联用户,且用户A与用户B之间也存在关联关系,则会在用户关系网络中存在一条关联通路,来表示上述两个用户之间存在关联。

[0043] 在S105中,根据所述用户关系网络中异常用户的个数,确定所述待识别用户的风险等级。

[0044] 在本实施例中,确定设备在标记了用户关系网络中所有异常用户后,会统计该用户关系网络中包含的异常用户的个数,将该个数作为计算待识别用户的风险等级,从而实现对于刚注册的用户也能够实现风险等级评估的目的。可选地,确定设备预设有风险等级的转换哈希函数,将用户关系网络中的异常用户的个数导入到该转换哈希函数内,即可输出一个该个数所对应的风险等级,作为该用户的风险等级。

[0045] 可选地,在计算该待识别用户的风险等级时,还会考虑各个异常用户的风险等级。首先确定设备会基于异常用户的个数确定该待识别用户的风险初始值,并将各个异常用户的风险等级以及风险初始值导入到风险等级计算模型,确定该待识别用户的风险等级。其中,该风险等级计算模型如下:

[0046]

$$RiskDegree = \sum_{i=1}^N Cofft_i \cdot Riskdegree_0(Abnmluser_i) + InitalRisk(N)$$

[0047] 其中,RiskDegree为待识别用户的风险等级;InitalRisk(N)为待识别用户的风险初始值;Riskdegree<sub>0</sub>(Abnmluser<sub>i</sub>)为各个异常用户的风险等级,Cofft<sub>i</sub>为第i个异常用户的预设权重;N为待识别用户中异常用户的个数。

[0048] 以上可以看出,本发明实施例提供的一种用户风险等级的确定方法通过接收到待识别用户,即新增用户的用户信息时,则确定该用户信息对应的关键词序列,并基于该关键词序列与用户数据库中的各个已识别用户进行匹配,确定该待识别用户的关联用户,继而创建该待识别用户的用户关系网,并标记出该用户关系网中包含的异常用户;根据异常用

户的个数确定该待识别用户的风险等级,从而基于该风险等级可以判定是否响应用户发起的交易请求。与现有的用户风险等级的确定方法相比,本发明实施例不依赖历史交易记录来确定用户的风险等级,而是可以基于该用户的关联用户中包含的异常用户的个数,判断该用户是否属于异常用户群中的成员,并基于个数的不同得到该用户的风险等级,从而对于新添加的用户也能快速确定风险等级,对交易请求进行有效管控,降低了资金流失的风险。

[0049] 图2示出了本发明第二实施例提供的一种用户风险等级的确定方法S104的具体实现流程图。参见图2所示,相对于图1所述实施例,本实施例提供的一种用户风险等级的确定方法中S104包括S1041以及S1042,具体详述如下:

[0050] 在S1041中,获取各个所述已识别用户的关联用户,以确定所述待识别用户的M度关联用户;其中,所述M度关联用户与所述待识别用户之间的关联路径上存在M-1个用户节点;M为大于或等于1的正整数。

[0051] 在本实施例中,用户风险等级的确定设备在构建待识别用户的用户关系网络时,不但获取该待识别用户的关联用户,还会获取已识别用户的关联用户,确定待识别用户的M度关联用户。其中,该M度关联用户与待识别用户之间的关联路径上存在M-1个用户节点,即表示M度关联用户需要与待识别用户进行沟通、交互,需要该路径上的M-1个用户协作才能完成。

[0052] 需要说明的是,待识别用户与M度关联用户之间可能存在多条关联路径,而本实施例在确定M度关联用户时所选取的是待识别用户与M度关联用户之间最短的关联路径,即所经过的用户节点数最少的关联路径。

[0053] 在本实施例中,M的数值可以由用户基于需求进行设置,特别地,当M的值为1时,则表示该用户关系网络中只包含待识别用户的关联用户。优选地,M的值不大于6。基于六度人脉的关系原理,任意所有自然人之间只需经过5个用户即可存在关联,因此为了减少网络的冗余度,该M的值应不大于6。

[0054] 需要说明的是,在S1041中在获取M度关联用户的过程中,确定设备还会获取M度以内的关联用户,即M-1度关联用户、M-2度关联用户、...、1度关联用户(即待识别用户的关联用户)。

[0055] 在S1042中,根据所述M度关联用户,创建以所述待识别用户为中心的M度用户关系网,并标记所述M度用户关系网内包含的异常用户。

[0056] 在本实施例中,在确定了待识别用户的M度关联用户后,会创建以待识别用户为中心的M度用户关系网,该M度用户关系网中,包含了待识别用户M度以内的关联用户,并M度用户关系网中各个已识别用户的用户状态,标记各出包含的异常用户的数量。

[0057] 优选地,在基于异常用户的个数确定待识别用户的风险等级的过程中,各度关联用户所对应的权重值各不相同,其中,度数越高的关联用户,其对应的权重值越低,由于度数越高的关联用户,则表示该已识别用户对待识别用户的影响较小,而度数越小,则表示该已识别用户与待识别用户之间的关系更密切,影响较大,从而其对应的权重值也较大。可选地,计算待识别用户的风险等级的计算模型可以为:

[0058]

$$RiskDegree = \sum_{j=1}^M \sum_{i=1}^{N_j} Cofft_{ji} \cdot Riskdegree_j(Abnmluser_i) + InitalRisk(\sum_{j=1}^M N_j)$$

[0059] 在本实施例中， $N_j$ 为第 $i$ 度关联用户的个数。

[0060] 在本发明实施例中，不仅获取待识别用户的关联用户，还获取 $M$ 度以内的关联用户，从而能够提高用户关系网络的关联范围，从而提高了风险等级的准确性。

[0061] 图3示出了本发明第三实施例提供的一种用户风险等级的确定方法S103的具体实现流程图。参见图3所示，相对于图1所述实施例，本实施例提供的一种用户风险等级的确定方法S103包括S1031以及S1032，具体详述如下：

[0062] 进一步地，所述用户信息包含多个信息项目，所述用户的关键词序列包括多个关键词子序列，每个所述关键词子序列对应一个所述信息项目；

[0063] 所述根据所述关键词序列以及用户数据库内各个已识别用户的关键词序列，确定所述待识别用户与各个已识别用户之间的匹配度，包括：

[0064] 在S1031中，基于所述关键词子序列，分别计算所述待识别用户与各个已识别用户之间相同的信息项目的相似度。

[0065] 在本实施例中，用户信息包含多个信息项目，不同的信息项目用于记录该用户不同类型的用户信息。举例性地，用户信息包含：性别、电话号码、住所、工作地点、所在单位、配偶关系6项信息项目，分别记录该用户在各个维度的对应的用户资料，因此确定设备会为每个信息项目确定对应的关键词子序列，从而通过关键词子序列构建该待识别用户所对应的关键词序列。

[0066] 可选地，在本实施例中，在确定不同信息项目的关键词子序列时，确定设备会查询该信息项目的关键词字典，即确定设备会为每个关键词序列生成与之对应的关键词列表。由于某些关键词只会出现在某些信息项目中，而必然不会出现在部分信息项目，例如对于关键词“深圳”与“广州”，上述两个关键词属于地理位置的关键词，则必然不会出现在“性别”、“配偶关系”以及“电话号码”这三项信息项目内。因此，为了避免单个关键词字典的数据量过大并且在确定关键词序列时进行过多无效的匹配操作，创建设备会为不同的信息项目确定与之对应的关键词字典，从而提高了关键词序列的生成效率。

[0067] 在本实施例中，确定设备在确定了各个信息项目的关键词子序列后，在计算各个用户之间的匹配度之前，会计算各个用户对应信息项目之间关键词子序列的相似度。例如，在计算用户A和用户B之间的匹配度时，会计算用户A的居住地的关键词子序列与用户B的居住地的关键词子序列之间的相似度，然后在计算用户A工作单位的关键词子序列与用户B工作单位的关键词子序列之间的相似度，直到计算了两个用户之间所有信息项目之间的相似度，则执行S1032的相关操作。

[0068] 在本实施例中，计算两个关键词子序列的相似度的具体方式可以为：统计两个关键词子序列相同关键词的第一个数，并计算第一个数与关键词序列总的元素个数之间的比值，作为两个关键词子序列之间的相似度。若部分用户某些信息项目缺失，则识别关于该信息项目的相似度为0。

[0069] 在S1032中，将各个所述信息项目的相似度导入到匹配度转换模型，计算所述匹配

度;所述匹配度转换模型为:

$$[0070] \quad Q = \sum_{k=1}^n \alpha_k B_k$$

[0071] 其中,Q为所述匹配度; $B_k$ 为任意两个所述用户的第k个所述信息项目之间的相似度; $\alpha_k$ 为第k个所述信息项目的匹配权重;n为信息项目的个数。

[0072] 在本实施例中,确定设备将各个信息项目所对应的相似度导入到预设的匹配度转换模型内,该匹配转换模型定义了不同信息项在计算匹配度时所占的匹配权重,创建设备会根据各个匹配权重以及对应信息项目的相似度,计算两个用户之间的匹配度。

[0073] 在本实施例中,匹配权重可以从上位机服务器中下载得到,还可以有用户根据实际场景的需求,调整不同信息项目的匹配权重。当然,若用户需要忽略部分信息项目对于匹配度计算的影响,可以设置该类的信息项目的匹配权重为0,从而不考虑该部分信息项目对于用户关联判定的影响。

[0074] 在本发明实施例中,通过分类计算不同信息项目之间的相似度,并基于多个信息项目确定两个用户之间的匹配度,从而提高了关联用户识别的准确性,进一步提高了风险等级的准确性。

[0075] 图4示出了本发明第四实施例提供的一种用户风险等级的确定方法的具体实现流程图。参见图4所示,相对于图1~图3所述实施例,本实施例提供的一种用户风险等级的确定方法中还包括:S401~S404,具体详述如下:

[0076] 进一步地,在所述基于所述关联用户,创建以所述待识别用户为中心的用户关系网络,并标记所述用户关系网络内包含的异常用户之前,还包括:

[0077] 在S401中,获取各个已识别用户的交易行为记录。

[0078] 在本实施例中,用户风险等级的确定设备在确定已识别用户是否为异常用户时,可以基于用户的交易行为记录,对该用户的用户属性进行确定。已识别用户由于是预先录入的用户,因此可以通过金融机构的服务器发起交易操作,每一次交易操作会产生一条交易行为记录,确定设备可以基于已识别用户的用户标识,提取该用户的所有交易行为记录。

[0079] 在S402中,将各个所述交易行为记录分别导入到预设的调整系数确定模型,得到各个所述交易行为记录的调整系数。

[0080] 在本实施例中,分别将某一已识别用户的各个交易行为记录导入到预设的调整系数的确定模型,确定每一个交易行为记录所对应的调整系数,既然执行S403的相关操作。具体地,确定每个交易行为记录的所对应的调整系数的方式可以为:提取交易行为记录中的交易特征值,该交易特征值可以为:交易频率、交易金额、交易属性、交易地址等信息,需要说明的是交易属性具体用于规定该交易为正面交易还是反面交易,正面交易为符合交易行为规范的交易操作,例如如期还款、如期交付利息等交易操作;而反面交易行为则为违反了交易行为规则的交易操作,例如逾期未还款、用户失联等情况。在确定了各个交易特征值后,将该交易特征值导入到预设的信用调整系数的转换模型,例如可以为一预设的哈希函数,确定该交易行为记录所对应的信用调整系数。

[0081] 可选地,在确定每个交易行为记录的信用调整系数之前,会首先确定该用户的行为习惯,因此会从根据各个交易行为记录确定该用户的历史行为特征值。具体地,该历史交

易特征值可以为基于各个交易行为记录所对应的行为特征值的均值。可选地,该历史交易特征值还可以为基于各个交易行为记录所对应的行为特征值的标准差,用于确定该用户的历史交易行为的浮动情况,在该情况下,计算历史交易特征值的过程如下:

[0082]

$$HistoryValue = \sqrt{\frac{1}{HistoryNum} \sum_{Hty=1}^{HistoryNum} (HistoryFig_i - \overline{HistoryFig})^2}$$

[0083] 其中,HistoryValue为所述历史交易特征值,HistoryNum为交易行为记录的个数;HistoryFig<sub>i</sub>为第i个交易行为记录的行为特征值; $\overline{HistoryFig}$ 为行为特征值的均值。

[0084] 并且,计算调整系数时可通过以下公式进行计算;

$$[0085] \quad Adjust = \ln \left[ A_p \cdot \left| \frac{TradeValue - HistoryFig}{HistoryValue} \right| \right]$$

[0086] 其中,Adjust为信用调整系数,TradeValue为交易行为特征值,A<sub>p</sub>为预设系数。

[0087] 在S403中,基于所述调整系数以及各个已识别用户的风险等级,分别调整各个已识别用户的风险等级。

[0088] 在本实施例中,确定设备在计算了各个交易行为记录所对应的信用调整系数后,会基于该用户的信用调整系数以及已识别用户所对应的原始的风险等级,对已识别用户的风险等级进行调整,其中,计算的过程可以为在风险等级的初始值的基础上与各个调整系数进行累加操作。优选地,基于各个交易行为记录与当前时刻的之间的差值,确定该交易行为记录的调整权重,基于各个调整系数的调整权重与风险等级的初始值进行加权运算,具体的计算模型如下:

$$[0089] \quad Cdit_t(user_n) = Cdit_0(user_n) + \sum_{trade=1}^{tradenum} \ln \left( \frac{T_0}{T_0 - T_{trade}} \right) \cdot CditA_{trade}$$

[0090] 其中,Cdit<sub>t</sub>(user<sub>n</sub>)为调整后第n个已识别用户的风险等级;T<sub>0</sub>为当前时刻对应的的时间值;T<sub>trade</sub>为交易行为记录的交易时刻;tradenum为交易行为记录的个数,CditA<sub>trade</sub>为调整系数;Cdit<sub>0</sub>(user<sub>n</sub>)为第n个已识别用户的风险等级的初始值。

[0091] 在S404中,若调整后的所述风险等级超过预设的风险阈值,则识别所述已识别用户为所述异常用户。

[0092] 在本实施例中,确定设备在对已识别用户的风险等级进行调整后,会将各个调整后的风险等级与风险阈值进行对比,确定该用户是否为异常用户,若该风险系数小于或等于风险阈值,则识别该用户为正常用户,反之,若该用户的风险系数大于风险阈值,则识别该用户为异常用户。

[0093] 在本发明实施例中,通过交易行为记录对每个已识别用户的风险等级进行调整,从而能够及时调整各个用户的用户属性,从而提高了计算风险等级的准确率。

[0094] 图5示出了本发明第五实施例提供的一种用户风险等级的确定方法的具体实现流程图。参见图5所示,相对于图1所述实施例,本实施例提供的一种用户风险等级的确定方法

还包括:S501~S503,具体详述如下:

[0095] 进一步地,所述用户数据库包括本地数据库以及云端数据库;所述本地数据库的初始状态为服务响应状态;所述云端数据库的初始状态为同步数据接收状态;所述确定方法还包括:

[0096] 在S501中,若接收到所述已识别用户的交易请求,则在所述本地数据库中创建一个关于所述交易请求的交易行为记录;所述交易行为记录用于记录所述交易请求的响应操作。

[0097] 在本实施例中,用户风险等级的确定设备关联了两个数据库,一个是存储于本地的本地数据,以及一个是用于备份资料的云端数据库。上述两个数据库可以采用网络附属存储(Network Attached Storage,NAS)方式实现Neo4j社区版的高可用方案,从而无需购买Neo4j商业版也能实现数据备份,提高了安全性。在该情况下,本地数据库以及云端数据库不仅用于同步交易行为记录,还能够用户同步各个已识别用户的用户关系网络,由于Neo4j数据库是用于存储网络拓扑机构的数据库,因此在存储用户关系网络时具有很高的存储效率。

[0098] 在本实施例中,本地数据库初始状态会设置为服务响应状态,即响应用户发起的交易操作过程时,会通过本地数据库进行记录,并将交易操作过程中产生的数据,生成交易行为记录。云端数据库会设置为同步数据接收状态,本地数据库会以预设的时间间隔将新增的数据增量备份至该云端服务器内,从而实现数据备份的目的。

[0099] 在本实施例中,确定设备若接收到已识别用户发起的交易请求,由于本地数据库为响应优先度较高的数据库,因此会在本地数据库中创建一个关于该交易请求的交易行为记录,并将响应该交易请求中的相关数据记录在该交易行为记录内。

[0100] 在S502中,若当前时刻满足同步触发条件,则将所述本地数据库存储的所述交易行为记录同步至所述云端数据库。

[0101] 在本实施例中,同步触发条件包括事件触发条件以及时间触发条件。例如,确定设备可以预设的时间间隔将所存储的交易行为记录和/或用户关系网络同步上传到云端数据库内,也可以在预设的各个时间节点执行上述上传操作;当然,也可以当新增的数据量到达数据量阈值时执行上述同步操作。在此不一一进行限定。

[0102] 在S503中,若检测到所述本地数据库存在数据写入异常,则将所述云端服务器的工作状态调整为所述服务响应状态,以在再次接收到交易请求时,通过所述云端数据库创建并存储交易请求的交易行为记录。

[0103] 在本实施例中,确定设备若检测到笨死数据库存在写入异常时,则表示本地数据库无法继续完成存储操作,需要进行异常处理,在该情况下,为了能够继续响应用户发起的交易请求,确定设备会将云端服务器的工作状态调整为服务器响应状态,将本地数据库的工作状态调整为数据同步状态,从而在后续接收到交易请求时,可以通过云端数据库创建并存储交易请求的交易行为记录,提高了整个系统的鲁棒性。

[0104] 可选地,在本地数据库的异常情况已被修复后,可以将云端数据库中新增的数据同步至本地数据库,并将本地数据库的工作状态调整为服务响应状态,将云端服务器的工作状态调整为数据同步状态。

[0105] 在本发明实施例中,通过设置本地数据库以及云端数据库进行数据备份,能够提

高用户风险等级的确定方法的鲁棒性。

[0106] 应理解,上述实施例中各步骤的序号的大小并不意味着执行顺序的先后,各过程的执行顺序应以其功能和内在逻辑确定,而不应对本发明实施例的实施过程构成任何限定。

[0107] 图6示出了本发明一实施例提供的一种用户风险等级的确定设备的结构框图,该用户风险等级的确定设备包括的各单元用于执行图1对应的实施例中的各步骤。具体请参阅图1与图1所对应的实施例中的相关描述。为了便于说明,仅示出了与本实施例相关的部分。

[0108] 参见图6,所述用户风险等级的确定设备包括:

[0109] 用户信息接收单元61,用于接收待识别用户的用户信息;

[0110] 关键词序列确定单元62,用于将所述用户信息与预设的关键词字典内的各个关键词进行匹配,确定所述待识别用户的关键词序列;

[0111] 关联用户识别单元63,用于根据所述关键词序列以及用户数据库内各个已识别用户的关键词序列,确定所述待识别用户与各个已识别用户之间的匹配度,并选取所述匹配度大于预设匹配度阈值的已识别用户,作为所述待识别用户的关联用户;

[0112] 用户关系网络创建单元64,用于基于所述关联用户,创建以所述待识别用户为中心的用户关系网络,并标记所述用户关系网络内包含的异常用户;所述异常用户具体为风险等级超过预设的风险阈值的用户;

[0113] 风险等级确定单元65,用于根据所述用户关系网络中异常用户的个数,确定所述待识别用户的风险等级。

[0114] 可选地,用户关系网络创建单元64包括:

[0115] 多度关联用户识别单元,用于获取各个所述已识别用户的关联用户,以确定所述待识别用户的M度关联用户;其中,所述M度关联用户与所述待识别用户之间的关联路径上存在M-1个用户节点;M为大于或等于1的正整数;

[0116] 多度用户网络创建单元,用于根据所述M度关联用户,创建以所述待识别用户为中心的M度用户关系网,并标记所述M度用户关系网内包含的异常用户。

[0117] 可选地,所述用户信息包含多个信息项目,所述用户的关键词序列包括多个关键词子序列,每个所述关键词子序列对应一个所述信息项目;

[0118] 关键词序列确定单元62包括:

[0119] 相似度计算单元,用于基于所述关键词子序列,分别计算所述待识别用户与各个已识别用户之间相同的信息项目的相似度;

[0120] 匹配度计算单元,用于将各个所述信息项目的相似度导入到匹配度转换模型,计算所述匹配度;所述匹配度转换模型为:

$$[0121] \quad Q = \sum_{k=1}^n \alpha_k B_k$$

[0122] 其中,Q为所述匹配度; $B_k$ 为任意两个所述用户的第k个所述信息项目之间的相似度; $\alpha_k$ 为第k个所述信息项目的匹配权重;n为信息项目的个数。

[0123] 可选地,所述用户风险等级的确定设备还包括:

[0124] 交易行为记录获取单元,用于获取各个已识别用户的交易行为记录;

[0125] 调整系数确定单元,用于将各个所述交易行为记录分别导入到预设的调整系数确定模型,得到各个所述交易行为记录的调整系数;

[0126] 风险等级调整单元,用于基于所述调整系数以及各个已识别用户的风险等级,分别调整各个已识别用户的风险等级;

[0127] 异常用户识别单元,用于若调整后的所述风险等级超过预设的风险阈值,则识别所述已识别用户为所述异常用户。

[0128] 可选地,所述用户数据库包括本地数据库以及云端数据库;所述本地数据库的初始状态为服务响应状态;所述云端数据库的初始状态为同步数据接收状态;所述用户风险等级的确定设备还包括:

[0129] 交易请求接收单元,用于若接收到所述已识别用户的交易请求,则在所述本地数据库中创建一个关于所述交易请求的交易行为记录;所述交易行为记录用于记录所述交易请求的响应操作;

[0130] 数据同步单元,用于若当前时刻满足同步触发条件,则将所述本地数据库存储的所述交易行为记录同步至所述云端数据库;

[0131] 异常响应单元,用于若检测到所述本地数据库存在数据写入异常,则将所述云端服务器的工作状态调整为所述服务响应状态,以在再次接收到交易请求时,通过所述云端数据库创建并存储交易请求的交易行为记录。

[0132] 因此,本发明实施例提供的用户风险等级的确定设备同样可以不依赖历史交易记录来确定用户的风险等级,而是可以基于该用户的关联用户中包含的异常用户的个数,判断该用户是否属于异常用户群中的成员,并基于个数的不同得到该用户的风险等级,从而对于新添加的用户也能快速确定风险等级,对交易请求进行有效管控,降低了资金流失的风险。

[0133] 图7是本发明另一实施例提供的一种用户风险等级的确定设备的示意图。如图7所示,该实施例的用户风险等级的确定设备7包括:处理器70、存储器71以及存储在所述存储器71中并可在所述处理器70上运行的计算机程序72,例如用户风险等级的确定程序。所述处理器70执行所述计算机程序72时实现上述各个用户风险等级的确定方法实施例中的步骤,例如图1所示的S101至S105。或者,所述处理器70执行所述计算机程序72时实现上述各装置实施例中各单元的功能,例如图6所示模块61至65功能。

[0134] 示例性的,所述计算机程序72可以被分割成一个或多个单元,所述一个或者多个单元被存储在所述存储器71中,并由所述处理器70执行,以完成本发明。所述一个或多个单元可以是能够完成特定功能的一系列计算机程序指令段,该指令段用于描述所述计算机程序72在所述用户风险等级的确定设备7中的执行过程。例如,所述计算机程序72可以被分割成用户信息接收单元、关键词序列确定单元、关联用户识别单元、用户关系网络创建单元以及风险等级确定单元,各单元具体功能如上所述。

[0135] 所述用户风险等级的确定设备7可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。所述用户风险等级的确定设备可包括,但不仅限于,处理器70、存储器71。本领域技术人员可以理解,图7仅仅是用户风险等级的确定设备7的示例,并不构成对用户风险等级的确定设备7的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或

者不同的部件,例如所述用户风险等级的确定设备还可以包括输入输出设备、网络接入设备、总线等。

[0136] 所称处理器70可以是中央处理单元(Central Processing Unit,CPU),还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0137] 所述存储器71可以是所述用户风险等级的确定设备7的内部存储单元,例如用户风险等级的确定设备7的硬盘或内存。所述存储器71也可以是所述用户风险等级的确定设备7的外部存储设备,例如所述用户风险等级的确定设备7上配备的插接式硬盘,智能存储卡(Smart Media Card,SMC),安全数字(Secure Digital,SD)卡,闪存卡(Flash Card)等。进一步地,所述存储器71还可以既包括所述用户风险等级的确定设备7的内部存储单元也包括外部存储设备。所述存储器71用于存储所述计算机程序以及所述用户风险等级的确定设备所需的其他程序和数据。所述存储器71还可以用于暂时地存储已经输出或者将要输出的数据。

[0138] 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。

[0139] 以上所述实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前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:其依然可以对前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,均应包含在本发明的保护范围之内。

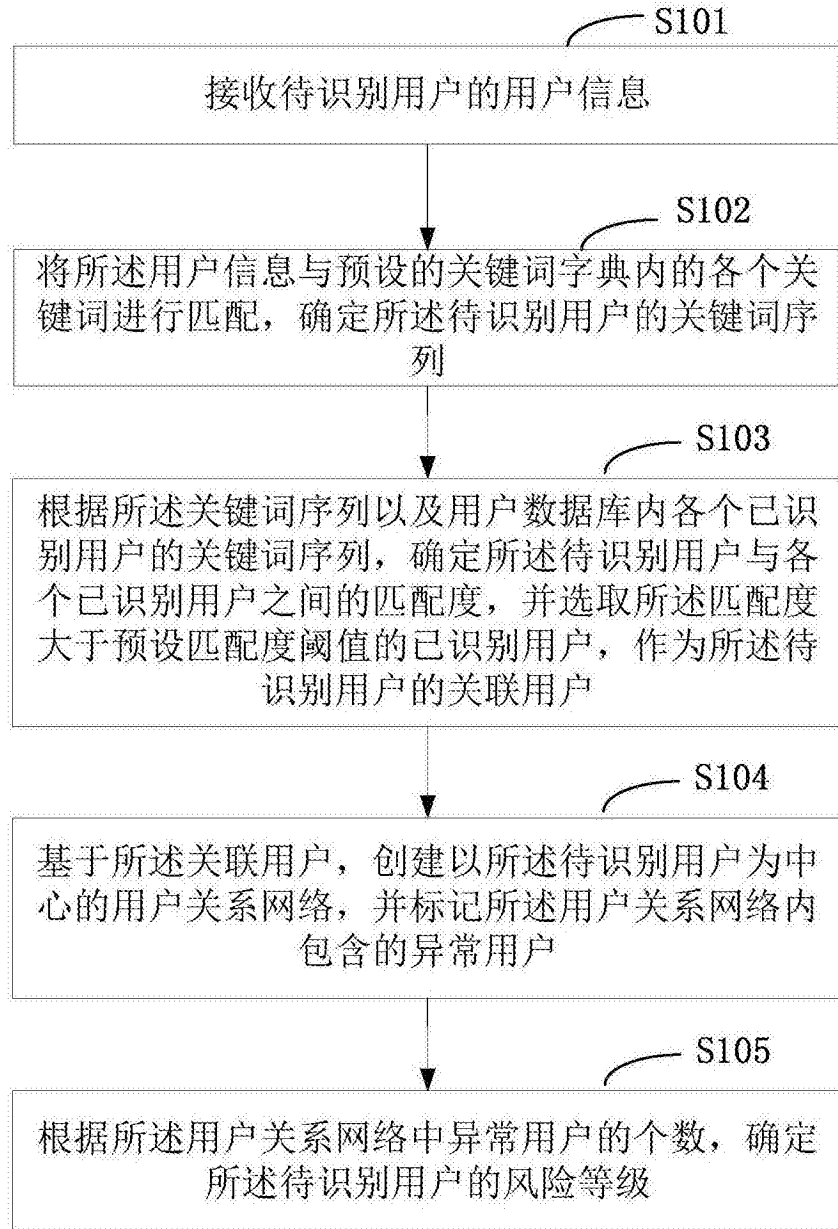


图1

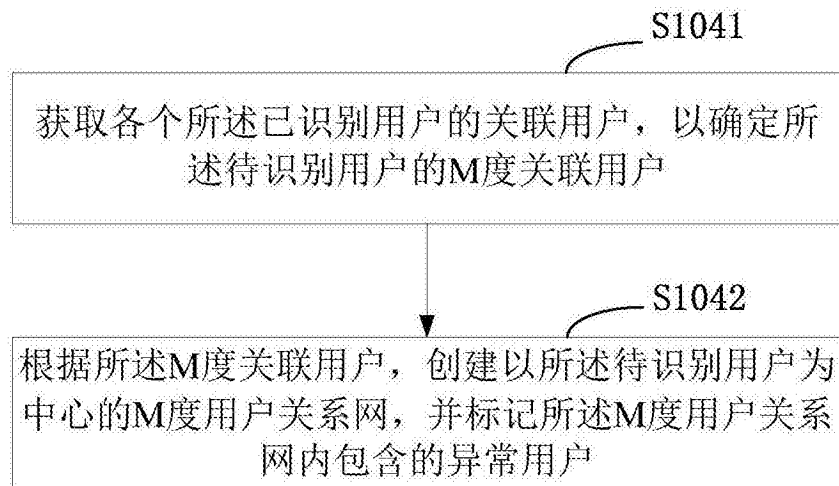


图2

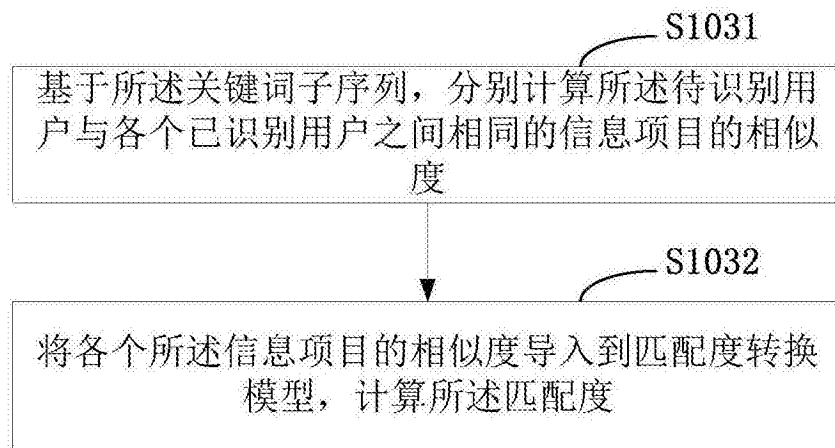


图3

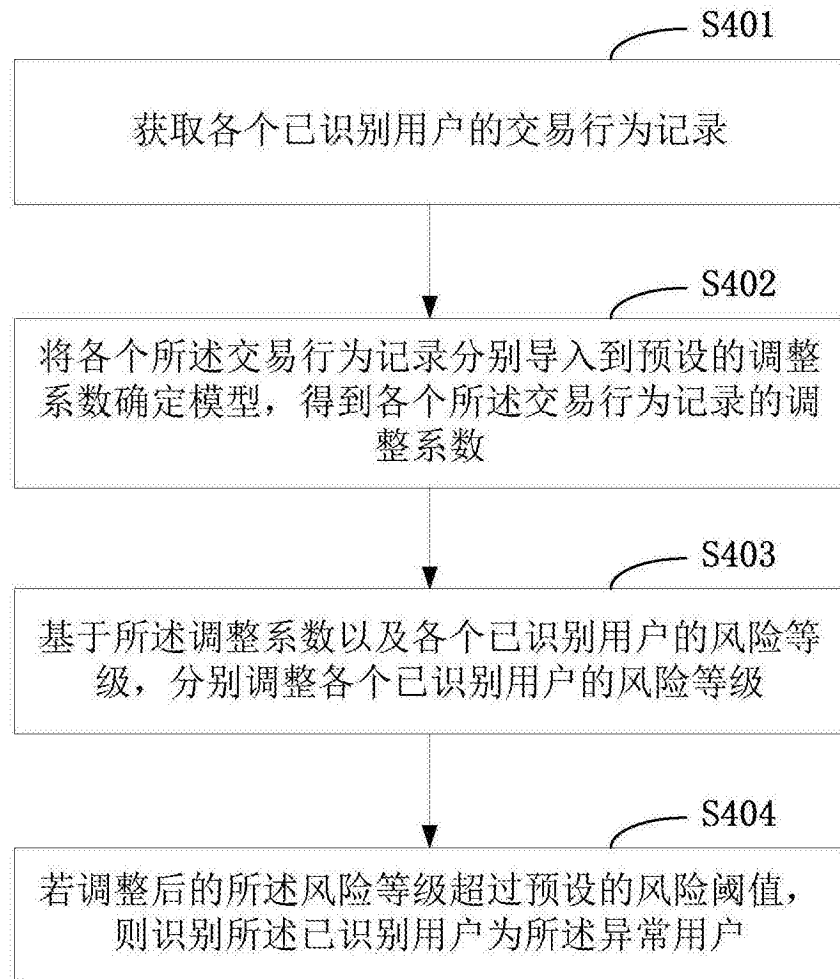


图4

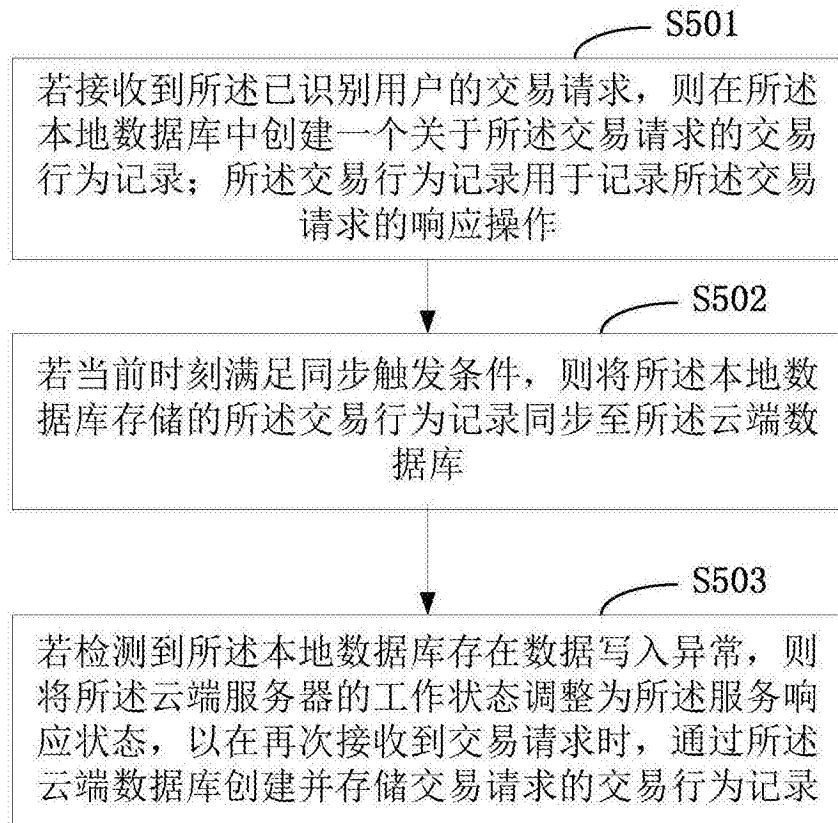


图5

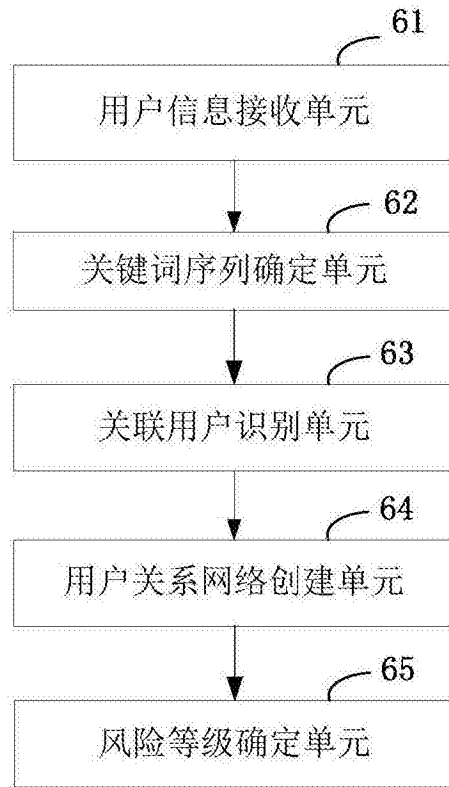


图6

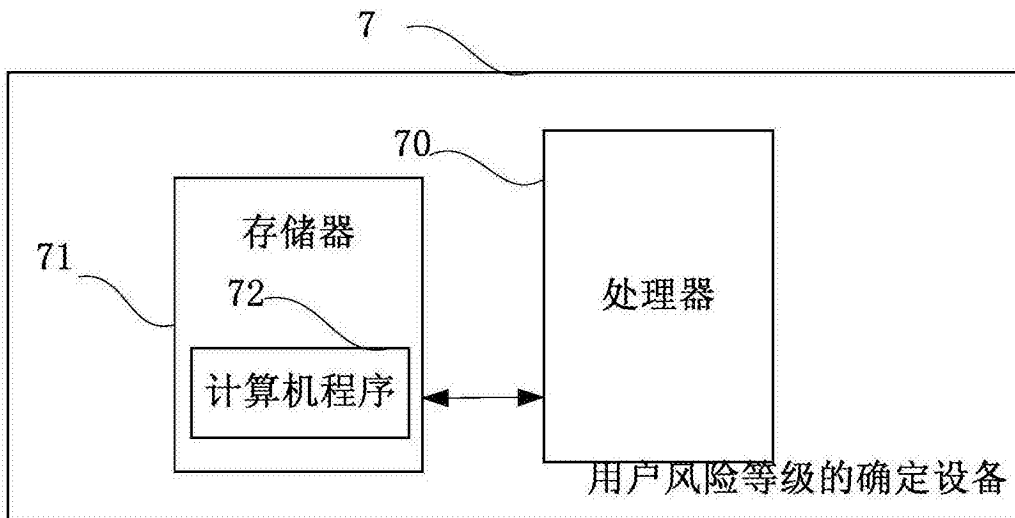


图7