



(12)发明专利

(10)授权公告号 CN 105101196 B

(45)授权公告日 2018.11.02

(21)申请号 201410188430.0

(22)申请日 2014.05.06

(65)同一申请的已公布的文献号

申请公布号 CN 105101196 A

(43)申请公布日 2015.11.25

(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 钱剑波 倪行军 俞峰

(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)

H04W 12/06(2009.01)

(56)对比文件

W0 0152025 A2,2001.07.19,

KR 20050078308 A,2005.08.05,

US 2004210776 A1,2004.10.21,

US 7117528 B1,2006.10.03,

CN 101753309 A,2010.06.23,

审查员 薛永旭

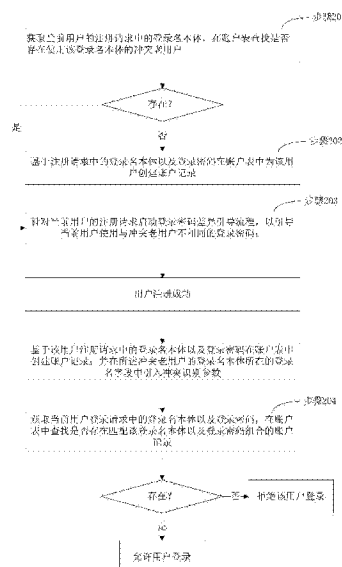
权利要求书4页 说明书10页 附图5页

(54)发明名称

一种用户账户管理方法及装置

(57)摘要

本申请提供一种用户账户管理方法,应用于服务器上包括:获取当前用户的注册请求中的登录名本体,查找是否存在使用该登录名本体的冲突老用户;若不存在,基于注册请求为该用户创建账户记录;若存在,针对当前用户的注册请求启动登录密码差异引导流程;在该用户注册成功时,在所述冲突老用户的登录名本体所在的登录名字段中引入冲突识别参数;获取当前用户登录请求中的登录名本体以及登录密码,在账户表中查找是否存在匹配该登录名本体以及登录密码组合的账户记录,若存在则允许用户登录,否则拒绝该用户登录。相较于现有技术,本申请有效地解决了二次放号等现象引发登录名冲突情况下所引发的用户体验下降,解决冲突人工客服成本高的问题。



1. 一种用户账户管理装置,应用于服务器上,包括:前置检查单元、常规注册单元、特殊注册单元以及登录管理单元,其特征在于:

前置检查单元,用于获取当前用户的注册请求中的登录名本体,在账户表查找是否存在使用该登录名本体的冲突老用户;若不存在,转常规注册单元处理,若存在,转特殊注册单元处理;

常规注册单元,用于基于注册请求中的登录名本体以及登录密码在账户表中为该用户创建账户记录;

特殊注册单元,用于针对当前用户的注册请求启动登录密码差异引导流程,以引导当前用户使用与冲突老用户不相同的登录密码;在该用户注册成功时,基于该用户注册请求中的登录名本体以及登录密码在账户表中创建账户记录;并在所述冲突老用户的登录名本体所在的登录名字段中引入冲突识别参数,以在所述冲突老用户登录成功的情况下检查到所述冲突老用户的登录名字段中包括有冲突识别参数时,引导该冲突老用户修改登录名本体;

登录管理单元,用于获取当前用户登录请求中的登录名本体以及登录密码,在账户表中查找是否存在匹配该登录名本体以及登录密码组合的账户记录,若存在则允许用户登录,否则拒绝该用户登录。

2. 如权利要求1所述的装置,其特征在于:其中

登录管理单元,还用于在当前用户登录成功的情况下检查该用户账户记录的登录名字段中是否包括有冲突识别参数;如果有,则向该用户发送登录名本体修改界面,以引导该用户修改登录名本体。

3. 如权利要求2所述的装置,其特征在于:其中

特殊注册单元,还用于获取当前用户通过登录名本体修改界面输入的登录名本体,在账户表查找是否存在使用该登录名本体的冲突新用户,如果不存在,则更新当前用户账户记录中的登录名本体,如果存在,则在该冲突新用户的登录名字段中添加冲突识别参数使其成为冲突老用户;将当前用户账户记录的登录名字段中的冲突识别参数消除。

4. 如权利要求1所述的装置,其特征在于:

所述登录密码差异引导流程的实现方式为拒绝注册引导方式或者密码规则引导方式。

5. 如权利要求4所述的装置,其特征在于:在所述拒绝注册引导方式中,所述特殊注册单元进一步用于获取当前用户注册请求中的登录密码,检查该登录密码与冲突老用户的登录密码是否相同,若相同,则拒绝本次注册请求,并输出登录密码不符合安全规则的提示,若不同,则确定当前用户注册成功。

6. 如权利要求5所述的装置,其特征在于:在所述拒绝注册引导方式中,

特殊注册单元进一步用于先选择一个随机的正整数N,拒绝当前用户的前N次注册请求,并在每次拒绝时均输出登录密码不符合安全规则的提示;在完成N次拒绝之后,针对第N+1次注册请求,获取N+1次注册请求中的登录密码,检查该登录密码与冲突老用户的登录密码是否相同,若相同,则拒绝本次注册请求,并输出登录密码不符合安全规则的提示;若不同,则确定当前用户注册成功。

7. 如权利要求4所述的装置,其特征在于:所述密码规则引导方式具体为长度规则引导方式、指定字符引导方式以及字符类型引导方式三种方式中的任意一种。

8. 如权利要求7所述的装置,其特征在于:

在所述长度规则引导方式中,特殊注册单元进一步用于检查当前用户的注册请求中的登录密码是否匹配预定长度规则,如果是,则确定用户注册成功,如果不是,则在当前页面上提示当前用户重新输入长度符合预定长度规则的登录密码,其中冲突老用户的登录密码的长度不符合该预定长度规则;

在所述指定字符引导方式中,特殊注册单元进一步用于检查当前用户的注册请求中的登录密码是否包括指定字符,若包括,则确定用户注册成功,如果不包括,则在当前页面上提示当前用户重新输入包括所述指定字符的登录密码,其中冲突老用户使用的登录密码中没有该指定字符;

在所述字符类型引导方式中,特殊注册单元进一步用于检查当前用户的注册请求中的登录密码是否匹配预定的字符类型规则,如果是,则确定用户注册成功,否则在当前页面上提示当前用户重新输入匹配所述字符类型规则的登录密码,其中冲突老用户使用的登录密码中不匹配所述字符类型规则。

9. 如权利要求1所述的装置,其特征在于:还包括:

密码找回单元,用于在接收到用户密码找回请求时,在账户表中检查该用户使用的登录名本体是否对应于多个账户记录,如果是,则向该用户发送选择性找回验证界面,其中该选择性找回验证界面包括与所述多个账户记录分别对应的校验选项,在确定任意一个账户对应的校验选项验证成功后,发送与该账户的密码重置界面给当前用户;其中各个校验选项均为登录名无关的校验选项。

10. 如权利要求1所述的装置,其特征在于:

特殊注册单元,在用户登录成功后接收到该用户发送的子账户创建请求时,向用户推送子账户创建界面,检查用户在该界面上输入的登录密码与用户当前登录账户的登录密码是否相同,如果相同则提示该用户重新输入登录密码,否则基于当前登录账户的登录名本体以及用户输入的登录密码创建子账户,并在子账户登录名字段中添加关联识别参数。

11. 如权利要求1所述的装置,其特征在于:所述登录名字段中还包括随机字符串以及分隔符,其中冲突识别参数均位于登录名本体与该随机字符串之间;所述分隔符位于冲突识别参数与登录名本体之间。

12. 一种用户账户管理方法,应用于服务器上,其特征在于,该方法包括:

获取当前用户的注册请求中的登录名本体,在账户表查找是否存在使用该登录名本体的冲突老用户;

若不存在使用该登录名本体的冲突老用户,基于注册请求中的登录名本体以及登录密码在账户表中为该用户创建账户记录;

若存在使用该登录名本体的冲突老用户,针对当前用户的注册请求启动登录密码差异引导流程,以引导当前用户使用与冲突老用户不相同的登录密码;在该用户注册成功时,基于该用户注册请求中的登录名本体以及登录密码在账户表中创建账户记录;并在所述冲突老用户的登录名本体所在的登录名字段中引入冲突识别参数,以在所述冲突老用户登录成功的情况下检查到所述冲突老用户的登录名字段中包括有冲突识别参数时,引导该冲突老用户修改登录名本体;

获取当前用户登录请求中的登录名本体以及登录密码,在账户表中查找是否存在匹配

该登录名本体以及登录密码组合的账户记录,若存在则允许用户登录,否则拒绝该用户登录。

13. 如权利要求12所述的方法,其特征在于:还包括:

在当前用户登录成功的情况下检查该用户账户记录的登录名字段中是否包括有冲突识别参数;如果有,则向该用户发送登录名本体修改界面,以引导该用户修改登录名本体。

14. 如权利要求13所述的方法,其特征在于:还包括:

获取当前用户通过登录名本体修改界面输入的登录名本体,在账户表查找是否存在使用该登录名本体的冲突新用户,如果不存在,则更新当前用户账户记录中的登录名本体,如果存在,则在该冲突新用户的登录名字段中添加冲突识别参数使其成为冲突老用户;将当前用户账户记录的登录名字段中的冲突识别参数消除。

15. 如权利要求12所述的方法,其特征在于:

所述登录密码差异引导流程的实现方式为拒绝注册引导方式或者密码规则引导方式。

16. 如权利要求15所述的方法,其特征在于:在所述拒绝注册引导方式中,获取当前用户注册请求中的登录密码,检查该登录密码与冲突老用户的登录密码是否相同,若相同,则拒绝本次注册请求,并输出登录密码不符合安全规则的提示,若不同,则确定当前用户注册成功。

17. 如权利要求16所述的方法,其特征在于:在所述拒绝注册引导方式中,

先选择一个随机的正整数N,拒绝当前用户的前N次注册请求,并在每次拒绝时均输出登录密码不符合安全规则的提示;在完成N次拒绝之后,针对第N+1次注册请求,获取N+1次注册请求中的登录密码,检查该登录密码与冲突老用户的登录密码是否相同,若相同,则拒绝本次注册请求,并输出登录密码不符合安全规则的提示;若不同,则确定当前用户注册成功。

18. 如权利要求15所述的方法,其特征在于:所述密码规则引导方式具体为长度规则引导方式、指定字符引导方式以及字符类型引导方式三种方式中的任意一种。

19. 如权利要求18所述的方法,其特征在于:

在所述长度规则引导方式中,检查当前用户的注册请求中的登录密码是否匹配预定长度规则,如果是,则确定用户注册成功,如果不是,则在当前页面上提示当前用户重新输入长度符合预定长度规则的登录密码,其中冲突老用户的登录密码的长度不符合该预定长度规则;

在所述指定字符引导方式中,检查当前用户的注册请求中的登录密码是否包括指定字符,若包括,则确定用户注册成功,如果不包括,则在当前页面上提示当前用户重新输入包括所述指定字符的登录密码,其中冲突老用户使用的登录密码中没有该指定字符;

在所述字符类型引导方式中,检查当前用户的注册请求中的登录密码是否匹配预定的字符类型规则,如果是,则确定用户注册成功,否则在当前页面上提示当前用户重新输入匹配所述字符类型规则的登录密码,其中冲突老用户使用的登录密码中不匹配所述字符类型规则。

20. 如权利要求12所述的方法,其特征在于:还包括:

在接收到用户密码找回请求时,在账户表中检查该用户使用的登录名本体是否对应于多个账户记录,如果是,则向该用户发送选择性找回验证界面,其中该选择性找回验证界面

包括与所述多个账户记录分别对应的校验选项,在确定任意一个账户对应的校验选项验证成功后,发送与该账户的密码重置界面给当前用户;其中各个校验选项均为登录名无关的校验选项。

21.如权利要求12所述的方法,其特征在于:还包括:

在用户登录成功后接收到该用户发送的子账户创建请求时,向用户推送子账户创建界面,检查用户在该界面上输入的登录密码与用户当前登录账户的登录密码是否相同,如果相同则提示该用户重新输入登录密码,否则基于当前登录账户的登录名本体以及用户输入的登录密码创建子账户,并在子账户登录名字段中添加关联识别参数。

22.如权利要求12所述的方法,其特征在于:所述登录名字段中还包括随机字符串以及分隔符,其中冲突识别参数均位于登录名本体与该随机字符串之间;所述分隔符位于冲突识别参数与登录名本体之间。

一种用户账户管理方法及装置

技术领域

[0001] 本申请涉及互联网技术领域,尤其涉及一种用户账户管理方法及装置。

背景技术

[0002] 在互联网的世界中,除了传统的媒体类应用之外,目前更多的应用需要用户以特定的身份参与,比如电子商务以及社交类应用。用户在该应用下进行账户注册,登录方式一般采用登录名(也称为“登录号”)和登录密码来实现。在大部分应用中,登录名通常为一串数字(如QQ号)、昵称或者邮箱名,也有一些系统采用手机号作为登录名。

[0003] 无论采用哪种形式的登录名,对于提供服务的系统来说,基本上都有系统内登录名唯一性的控制机制。以手机号这样的登录名为例,因为二次放号的问题,会导致应用系统内登录名唯一性控制要求与用户体验之间产生矛盾。二次放号是指手机号的原使用者主动/被动放弃使用该手机号后,该手机号基于特定条件被电信运营商回收之后分配给新用户使用的过程。二次放号现象发生后,新用户面临手机号无法注册特定应用的问题。比如说手机号的老用户使用该手机号注册了支付宝账户。那么新用户再使用该手机号注册支付宝账户时,支付宝服务系统会发现登录名冲突,因而可能会暂时拒绝该注册,直到冲突解除。此外,若老用户未有及时更改手机号,其可能会导致业务短信或者安全校验短信发到该手机号,被该手机号新用户接收到的问题。由此可见,二次放号一方面可能会造成用户体验降低的问题,另一方面还可能引发安全隐患。

[0004] 事实上,随着互联网的发展,二次放号现象不仅仅局限于手机号,还存在于邮箱以及QQ号等领域。比如说QQ靓号的转让,就会在事实上导致QQ号的二次放号,而大型的Web邮件服务商往往会回收那些长期不使用的邮件账户,然后给新用户注册使用,这也导致事实上二次放号的产生。由此可见,二次放号的现象广泛存在与互联网应用中。

[0005] 目前上述问题的解决主要依赖人工处理。比如手机号的新用户找到支付宝的人工客服,证明自己是该手机号的合法拥有者,由人工客服在后台强行处理,将该手机号的原用户留存在系统中的手机号进行修改,这样就可以达到释放手机号的目标。释放之后,系统内该手机号不存在,那么新用户使用该手机号注册就满足唯一性的控制要求,注册于是就能够成功。

[0006] 这种人工处理方式弊端显著:第一,人工成本高,在大型的互联网应用中,比如淘宝或新浪微博等,用户数量巨大,二次放号的数量不小,用人力去解决问题,成本太高;第二,用户体验差,人工客服通常需要手机号的新用户提供各种证据来证明自己对手机号的合法拥有,这无疑增加了用户很多额外的操作要求;第三,人工客服进行信息核对以及处理需要较长的时间,用户无法及时完成注册;第四,老用户账户中的手机号被修改,如何妥善处理又是一个需要人工再次解决的问题。

发明内容

[0007] 有鉴于此,本申请提供一种用户账户管理装置,应用于服务器上,包括:前置检查

单元、常规注册单元、特殊注册单元以及登录管理单元,其中:

[0008] 前置检查单元,用于获取当前用户的注册请求中的登录名本体,在账户表查找是否存在使用该登录名本体的冲突老用户;若不存在,转常规注册单元处理,若存在,转特殊注册单元处理;

[0009] 常规注册单元,用于基于注册请求中的登录名本体以及登录密码在账户表中为该用户创建账户记录;

[0010] 特殊注册单元,用于针对当前用户的注册请求启动登录密码差异引导流程,以引导当前用户使用与冲突老用户不相同的登录密码;在该用户注册成功时,基于该用户注册请求中的登录名本体以及登录密码在账户表中创建账户记录;并在所述冲突老用户的登录名本体所在的登录名字段中引入冲突识别参数;

[0011] 登录管理单元,用于获取当前用户登录请求中的登录名本体以及登录密码,在账户表中查找是否存在匹配该登录名本体以及登录密码组合的账户记录,若存在则允许用户登录,否则拒绝该用户登录。

[0012] 本申请还提供一种用户账户管理方法,应用于服务器上,该方法包括:

[0013] 获取当前用户的注册请求中的登录名本体,在账户表查找是否存在使用该登录名本体的冲突老用户;

[0014] 若不存在使用该登录名本体的冲突老用户,基于注册请求中的登录名本体以及登录密码在账户表中为该用户创建账户记录;

[0015] 若存在使用该登录名本体的冲突老用户,针对当前用户的注册请求启动登录密码差异引导流程,以引导当前用户使用与冲突老用户不相同的登录密码;在该用户注册成功时,基于该用户注册请求中的登录名本体以及登录密码在账户表中创建账户记录;并在所述冲突老用户的登录名本体所在的登录名字段中引入冲突识别参数;

[0016] 获取当前用户登录请求中的登录名本体以及登录密码,在账户表中查找是否存在匹配该登录名本体以及登录密码组合的账户记录,若存在则允许用户登录,否则拒绝该用户登录。

[0017] 相较于现有技术,本申请有效地解决了二次放号等现象引发登录名冲突情况下所导致的用户体验下降,解决冲突人工客服成本高的问题。

附图说明

[0018] 图1是本申请一个例子中用户帐户管理装置的逻辑结构以及硬件环境图。

[0019] 图2是本申请一个例子中用户帐户管理方法的处理流程图。

[0020] 图3是本申请一个例子中登录密码差异引导流程的界面示意图。

[0021] 图4是本申请一个例子中引导用户修改手机号的流程图。

[0022] 图5是本申请一个例子中用户找回密码的界面示意图。

具体实施方式

[0023] 本申请通过改进应用系统内部的数据组织方式,以及对应的处理流程来大幅度改善二次放号引发注册冲突而导致用户体验下降的问题。请参考表1,在本申请一种实施方式中,在特殊业务场景的驱动下,在系统内记录每个用户账户信息的账户表(请参考表1的示

例)中,登录名字段(字段一)中除了登录名本体之外还可以包括更多的参数,但是任意一条账户记录的登录名字段中的数据在应用系统的数据库表中具有唯一性,系统通过冲突识别参数的引入保证登录名字段内登录名数据的唯一性,而登录名本体则允许重复。从用户的使用角度来说,其依然会继续将登录名本体作为登录名,也就是说登录名字段的数据结构的变化对于用户而言是无需感知的,事实上用户认为的登录名在系统中事实上是登录名本体,其可能是系统中的登录名数据本身,也可能只是登录名数据的一部分。

[0024] 请参考表1的示例,其中用户Tony使用手机号18611180751作为登录名,在系统中该用户账户记录的登录名字段中的登录名数据则是“18611180751”,而用户Kevin也使用18611180751作为登录名,在系统中用户Kevin账户记录的登录名字段中的登录名数据则是“18611180751|R”。通过这样的数据组织方式,系统数据库中的登录名的唯一性得到了保证,以下将继续描述基于该数据组织方式如何为用户提供体验更好的服务。值得注意的是,在本示例中,登录名字段中还包括预先定义的分隔符“|”,分隔符的引入是考虑到业务的可扩展性,但并不是必须的选择。比如说在中国大陆地区,目前所有的手机号都是11位的,因为对于那些业务集中在中国大陆地区的服务商而言,实施过程中并不需要引入分隔符,因为系统可以根据手机号的长度来确定手机号与冲突识别参数的分界,从而准确地确定出手机号与冲突识别参数。但是对于服务更多国家/地区用户的服务商而言,由于各个国家/地区手机号码的位数不尽相同,因此在登录名本体与冲突识别参数之间引入分隔符来协助区分登录名本体以及冲突识别参数。

[0025]

序号	字段一	字段二
	登录名+分隔符+识别因子	登录密码
1	13900100110	aaaaaaa
2	18611180751 R	bbbbbbb
3	18611180751	ccccccc
4	13988888888	aaaaaaa
.....		

[0026] 表1

[0027] 基于上述数据组织结构的变化,在一种软件实施方式中,本申请提供一种用户账户管理装置及对应的管理方法。请参考图1,该用户账户管理装置可以理解为服务器上运行的一个逻辑装置。在硬件层面,该服务器包括处理器、内存以及非易失性存储器,当然还可能包括其他业务所需要的硬件。所述处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行,在逻辑层面上形成所述用户管理装置,该用户管理装置可以理解为应用系统对外服务的一个部分,比如支付宝服务系统对外服务的一个部分。当然,除了软件实现方式之外,本申请并不排除其他实现方式,比如逻辑器件抑或软硬件结合的方式等等,也就是说以下管理方法的处理流程的执行主体并不限定于各个逻辑单元,管理方法的执行主体也可以是硬件或逻辑器件。

[0028] 在软件实施方式中,该用户管理装置包括前置检查单元、常规注册单元、特殊注册单元以及登录管理单元。请参考图2,在运行过程中该装置执行如下处理过程。

[0029] 步骤201,前置检查单元获取当前用户的注册请求中的登录名本体,在账户表查找

是否存在使用该登录名本体的冲突老用户;若不存在,转步骤202,若存在,转步骤203;

[0030] 步骤202,常规注册单元基于注册请求中的登录名本体以及登录密码在账户表中为该用户创建账户记录;

[0031] 步骤203,特殊注册单元针对当前用户的注册请求启动登录密码差异引导流程,以引导当前用户使用与冲突老用户不相同的登录密码;在该用户注册成功时,基于该用户注册请求中的登录名本体以及登录密码在账户表中创建账户记录;并在所述冲突老用户的登录名本体所在的登录名字段中引入冲突识别参数;

[0032] 步骤204,登录管理单元获取当前用户登录请求中的登录名本体以及登录密码,在账户表中查找是否存在匹配该登录名本体以及登录密码组合的账户记录,若存在则允许用户登录,否则拒绝该用户登录。

[0033] 从以上的步骤中可以看出,本申请允许不同用户使用相同登录名进行注册,避免了二次放号引发的注册与登录不便的问题。在正常的注册过程中,若用户使用的登录名本体在账户表中是唯一的,也就是说没有冲突老用户的存在,此时发起注册请求的用户显然不是一个冲突新用户,其注册请求将按照正常的方式处理。当然常规注册过程中也可能需要发起校验等额外处理过程,这些处理可参考已有技术实现。

[0034] 请参考表1,假设表1中第2条以及第3条记录分别是用户Kevin以及Tony的账户记录(也称为“用户记录”)。假设登录名本体是手机号,用户Kevin使用手机号18611180751注册账户在先,后来用户Kevin不再使用该手机号,运营商回收该号码之后分配给Tony使用。用户Tony使用该手机号又进行账户注册,经过步骤203的特殊处理,Kevin的登录名在手机号的基础上又被添加了冲突识别参数,在账户表中,Kevin和Tony的登录名不再相同,同一字段中登录名的唯一性得到了保证。此时允许用户Tony进行账户注册并不会影响用户Kevin的登录。

[0035] 在传统处理方式中,应用系统是不关注不同账户的密码是否相同问题,因为理论上应用系统中所有用户使用相同的登录密码也是可以的。在本申请步骤203的处理中,用户Tony若想注册成功,则必须使用与用户Kevin不同的登录密码,这是在登录过程中,本申请是基于登录名与密码的组合进行匹配。当18611180751对应的账户记录存在多个时,需要逐一比对登录密码。在传统方案中,由于18611180751这个登录名本体并不会存在于两条账户记录中,于是查找过程使用18611180751进行查找发现一条账户记录,但密码不匹配,则立刻退出查找提示登录失败,而本申请在此情况下还需要继续遍历过程,直到所有18611180751对应的账户记录中的登录密码都不匹配时才确定用户登录失败。

[0036] 基于上述的登录机制,本申请在请求注册的当前用户是一个与冲突老用户对应的冲突新用户(比如Tony)时,在其注册过程中使用登录密码差异引导流程来引导Tony使用与冲突老用户Kevin不同的登录密码。登录密码差异引导流程的实现方式有多种,现列举以下示例作为实施参考。在较佳的实施方式中,从大类上来说,登录密码差异引导流程包括两大类,一类是拒绝注册引导方式,另一类是密码规则引导方式。当然本领域普通技术人员也可以使用其他方式开发登录密码差异的引导流程。

[0037] a.拒绝注册引导方式

[0038] 在实现上,特殊注册单元进一步获取当前用户Tony注册请求中的登录密码,检查该登录密码与冲突老用户Kevin的登录密码是否相同,若不同,则确定当前用户注册成功;

若相同,则拒绝本次注册请求,并输出登录密码不符合安全规则的提示,以要求用户重新输入登录密码。一般来说,两个用户设置相同登录密码的概率已经很低了,二次放号的新老用户设置相同的登录密码可能性则更低,几乎接近于零。但本申请考虑到一些对安全性要求极其严苛的应用场景,比如互联网金融的应用,对Tony设置登录密码进行检查和引导,在发现密码冲突时,通过输出登录密码不符合安全规则的提示来引导其使用不同的登录密码。请参考图3a的示例,当前用户Tony在发现这种提示后一般会尝试密码强度更高的登录密码,这样一来其输入的登录密码必然与之前输入的登录密码(也是Kevin的登录密码)不同,这样就实现了密码差异的引导。这种引导方式非常简洁,能满足绝大部分的场景需求。

[0039] 在优选的方式中,本申请还对该引导方式进行优化,提升其安全性。假设Tony在注册请求中输入的登录密码刚好与Kevin的登录密码相同(虽然这种情况的概率极低),此时系统提示“登录密码不符合安全规则”,那么Tony会猜到自己当前输入的登录密码可能与Kevin正在使用的的登录密码一致,这可能会造成Kevin的账户面临被盗用的风险。为了规避这种概率极低的安全漏洞,特殊注册单元进一步用于先选择一个随机的正整数N(比如小于8的正整数),拒绝当前用户Tony的前N次注册请求,并在每次拒绝时均输出登录密码不符合安全规则的提示;在完成N次拒绝之后,针对Tony的第N+1次注册请求,获取第N+1次注册请求中的登录密码,检查该登录密码与冲突老用户的登录密码是否相同,若相同,则拒绝本次注册请求,并输出登录密码不符合安全规则的提示;若不同,则确定当前用户注册成功。这样一来引入随机拒绝次数机制,Tony无法得知自己输入的密码到底是因为何种原因被系统拒绝的,这样可以有效保护Kevin的登录密码,避免因小概率意外情况的发生而被Tony轻易猜测到。当然,为了照顾Tony的用户体验,可以事先在页面上输出响应的解释给用户。比如说系统可以提示:当前流程属于特殊冲突注册流程,需要用户耐心配合,为了保障存在登录名冲突用户的安全,因此需要用户尝试多次输入不同的登录密码,由系统来随机选择合理的登录密码。

[0040] b. 密码规则引导方式,该方式可以有多种实现方式,典型的方式包括:

[0041] I、长度规则引导方式

[0042] 特殊注册单元进一步用于检查当前用户Tony的注册请求中的登录密码是否匹配预定长度规则,如果是,则确定用户注册成功,如果不是,则在当前页面上提示当前用户Tony重新输入长度符合预定长度规则的登录密码,其中冲突老用户的登录密码的长度不符合该预定长度规则。请参考图3b的示例,假设Kevin使用的登录密码是10位,则特殊处理单元可以选择任意一个长度不是10位的密码长度区间,比如11位到13位这个长度区间作为预定长度规则,若Tony提交的密码长度不符合这个长度规则,则拒绝其注册请求,直到其输入的密码长度符合预定长度规则。由于长度规则的使用,Tony的登录密码在长度上必然与Kevin的登录密码有差异,两者必然不同。此时理论上Tony只是知道Kevin的登录密码长度不在11到13这个区间,显然无法猜到Kevin的登录密码。再考虑一种极限情况,假设冲突老用户不止一个,也就是说二次放号放生了两次,实际上是三次放号了。此时还有一个冲突老用户Mike,密码长度为13位,那么Kevin和Mike的密码长度都不能符合预定长度规则,预定长度规则可以调整为大于13位或者是11到12位。

[0043] II、指定字符引导方式:特殊注册单元进一步用于检查当前用户的注册请求中的登录密码是否包括指定字符,若包括,则确定用户注册成功,如果不包括,则在当前页面上

提示当前用户重新输入包括所述指定字符的登录密码,其中冲突老用户使用的登录密码中没有该指定字符。这种方式强制要求Tony在登录密码中必须使用一个Kevin登录密码中没有的字符,这样一来Tony注册成功时,其登录密码必然与Kevin的登录密码不同。而理论上,Tony只能知道Kevin的登录密码不包括某个指定字符,比如“A”,显然无法猜到Kevin的登录密码。针对更多次放号的情况,显然是所有冲突老用户的密码都不包括该字符。

[0044] III、类型数量引导方式:特殊注册单元进一步用于检查当前用户Tony的注册请求中的登录密码是否匹配预定的字符类型规则,如果是,则确定用户注册成功,否则在当前页面上提示Tony重新输入匹配所述字符类型规则的登录密码,其中冲突老用户使用的登录密码中不匹配所述字符类型规则。比如说,Kevin的密码包括字母和数字这两种字符,则特殊注册单元在当前页面输出提示要求Tony输入的密码必须且仅仅包括字母、数字以及符号这三种字符,也就是说Kevin和Tony的登录密码至少有一种字符类型上的差异,要么Kevin比Tony至少多一种类型字符,要么Tony比Kevin至少多一种类型字符,两者的密码必然存在差异,而Tony也无法猜测到Kevin的密码。更多实现方式本领域普通技术人员可以根据安全性以及用户体验的综合需要,结合上述实施方式来开发符合业务需要的密码差异引导流程。

[0045] 以下在上述实施方式的基础上,结合更多的应用实际通过一个较佳的实施方式来阐述本申请的技术优势。在以下的描述中,登录名将以手机号为例。在一个接近实际部署的方案中,本申请提出以下几个优化措施来进一步提高本申请在实际使用中的实施效果,当然这些措施并不是必须的,而且各种优化措施如何组合可以根据需要来灵活选择。

[0046] 在上述实施方式的基础上本申请可进一步引入冲突消除机制。在一种实施方式中,本申请在步骤201到204的基础上进一步包括冲突解决机制。前述实施方式解决了注册冲突和登录冲突问题。虽然两个用户同时使用一个手机号登录并无问题,但是从用户使用应用服务的角度而言,手机号对于用户而言无疑是比较重要的,比如说接收校验短信等。若一项应用需要接收校验短信并在页面上回填该短信,则此时由于手机号同一时刻只会被一个用户(比如Tony)拥有,那么另一个用户(比如Kevin)此时就无法接收到自己的校验短信。对于这样的情况本申请进行特别处理,在用户登录成功的情况下,检查该用户登录名中是否包括有冲突识别参数,如果有则所述登录管理单元进一步向该用户推送手机号修改界面引导该冲突老用户修改手机号,在接收到用户输入新手机号之后在对应的账户记录中将手机号更新,用户下次再此进行登录时,需要使用新手机号作为登录名本体进行登录。在具体实现上,用户输入新手机号之后,登录管理单元通常会进一步发送针对该手机号发起校验,比如发送包括校验码的校验短信给该新手机号,并对比用户在界面上提交的校验码是否正确来确认用户是否确实拥有该手机号,这个过程与常规注册过程是类似的,此处不再详述。

[0047] 冲突老用户根据引导修改手机号依然可能存在一种特殊的情况。假设用户Kevin输入的手机号依然是18611180751,与原手机号一致,并不是新手机号,此时系统无法确定到底Kevin还是Tony拥有该手机号。一种简单的处理方式是,Kevin必须更改手机号,否则不允许其继续登录。然而事实上,Tony可能只是临时使用Kevin的手机号,Kevin才是真正的手续号主人,请参考图4,针对这种情况,在一种较为完整的实施方式中,引导用户修改手机号的流程包括如下步骤:

[0048] 步骤401,登录管理单元在当前用户登录成功的情况下检查该用户账户记录的登录名字段中是否包括有冲突识别参数;如果有,则向该用户发送登录名本体修改界面,以引

导该用户修改登录名本体；

[0049] 步骤402,特殊注册单元获取当前用户通过登录名本体修改界面输入的登录名本体,在账户表查找是否存在使用该登录名本体的冲突新用户,如果不存在,则更新当前用户账户记录中的登录名本体,如果存在,则在该冲突新用户的登录名字段中添加冲突识别参数使其成为冲突老用户;将当前用户账户记录的登录名字段中的冲突识别参数消除。

[0050] 仍然以用户Kevin与用户Tony为例,假设用户Kevin作为冲突老用户,其在登录名修改界面上提交的手机号确实发生了变化,比如变更为18611223344,此时根据步骤401到402的处理,用户Kevin与用户Tony之间将不存在冲突,用户Kevin的登录名将变成一个唯一使用的手机号,此时账户表将从表1更新为表2的示例。

[0051]

序号	字段一	字段二
	登录名+分隔符+识别因子	登录密码
1	13900100110	aaaaaa
2	18611223344	bbbbbb
3	18611180751	cccccc
4	13988888888	aaaaaa
.....		

[0052] 表2

[0053] 但是假设用户Kevin输入的手机号仍然是18611180751,也就意味着用户Kevin在向系统表明其拥有该手机号,此时系统无法确定到底是Kevin还是Tony拥有该手机号。因此系统在步骤402之前可以向用户发起校验,校验成功的话,校验过程不再详述,可参考现有技术执行。此时Kevin将变为冲突新用户,而Tony则从冲突新用户变为冲突老用户。此时表1将更新为表3的示例。这种设计可以很好地解决“伪二次放号”问题,真实的二次放号是一个手机号的主人发生了变更。而“伪二次放号”则是通过手机号的交叉使用产生了二次放号现象,这种交叉使用导致了应用系统认为发生的二次放号。比如说Kevin是18611180751的真实主人,其在支付宝使用该手机号进行了注册,支付宝系统拥有一条账户记录。Tony是Kevin的弟弟,其在一些特殊的或临时性的应用需求下,Tony临时使用Kevin的手机号注册了支付宝账户,这个过程将触发步骤201到204的处理,这导致Kevin在支付宝系统中变成了冲突老用户,而Tony通过“抢夺”行为则成为冲突新用户。Kevin再次登录时,系统在步骤401针对冲突老用户Kevin发送登录名修改界面引导Kevin修改手机号,此时由于Kevin是18611180751真实主人,其可能仍然输入了18611180751。系统此时可以认为是Kevin在执行“反抢”操作,通过校验短信对Kevin的“反抢”行为进行验证,若通过,则将Kevin变更为冲突新用户,而Tony则变为冲突老用户。Tony再次登录,系统仍然会通过登录名修改界面来引导Tony修改手机号。若Tony将自己的手机号修改,比如修改为18622223333,那么冲突将消失。

[0054]

序号	字段一	字段二
	登录名+分隔符+识别因子	登录密码
1	13900100110	aaaaaa
2	18611180751	bbbbbb

3	18611180751 R	cccccc
4	13988888888	aaaaaa
.....		

[0055] 表3

[0056] 请继续参考图5,在步骤204处理机制的基础上,本申请可进一步为用户提供创建与主账户具有关联关系的独立子账户的机制。假设用户Jack的手机号是13988888888,Jack使用该手机号注册了支付宝账户Jack1,其利用该账户为自己的公司购置办公用品,但Jack同时希望自己能够用该手机号注册另外一个支付宝账户Jack2,然后利用该账户Jack2为自己购买私人用品,这样可以清晰地区分公司采购与个人消费。在传统技术中,这种用户需求是无法满足的。在本申请中,特殊注册单元在当前用户通过当前账户(设为主账户)登录成功后接收到该用户发送的子账户创建请求时,向用户推送子账户创建界面,检查用户在该界面上输入的登录密码与用户当前登录账户的登录密码是否相同,如果相同则提示该用户重新输入登录密码,否则基于当前登录账户的登录名本体以及用户输入的登录密码创建子账户,并在子账户登录名字段中添加关联识别参数。请参考表4的示例,在本实施方式中,使用字符“T”作为关联识别参数。子账户创建成功之后,Jack可以用“13988888888”作为登录名来分别登录两个账户,输入密码aaaaaa则可以登录Jack1这个主账户,而输入密码dddddd,则可以子账户。

[0057]

序号	字段一	字段二
	登录名+分隔符+识别因子	登录密码
1	13900100110	aaaaaa
2	18611180751 R	bbbbbb
3	18611180751	cccccc
4	13988888888	aaaaaa
5	13988888888 T	dddddd
.....		

[0058] 表4

[0059] 在以上实施方式的基础上,本申请进一步考虑密码找回的处理机制。在优选的方式中,本申请所述用户管理装置还包括密码找回单元,密码找回单元在接收到用户密码找回请求时,在账户表中检查该用户使用的登录名本体是否对应于多个账户记录,如果是,则向该用户发送选择性找回验证界面,其中该选择性找回验证界面包括与所述多个账户记录分别对应的校验选项,在确定任意一个账户对应的校验选项验证成功后,发送与该账户的密码重置界面给当前用户;其中各个校验选项均为登录名无关的校验选项。

[0060] 假设Tony和Kevin任意一个人忘记了自身的密码,其会在对应的页面上发起密码找回请求。若按照传统实现,用户可能需要在界面上填入自身的手机号,但是由于手机号18611180751被Tony和Kevin同时使用,因此应用系统此时无法确定哪个用户在请求找回密码。一种处理方式时,回避手机号,转而让用户填入绑定邮箱或其他信息来确定用户的身份,然而有些用户可能没有绑定邮箱,这样的处理方式不够通用;另一中处理方式是Tony或Kevin可以通过人工客服来解决该问题,但这样依然比较影响用户的体验。

[0061] 在本申请中,密码找回单元并不会通过给18611180751发送校验短信息来进行校验,因为这样有可能会出现问题Tony重置了Kevin的密码,或者Kevin重置了Tony的密码。在本申请中,请参考图5的示例,密码找回单元生成包括与Tony和Kevin两个用户对应的校验选项的选择性找回验证界面,并发送给当前用户。在实现上,可以把这些校验选项都放在一个下拉菜单中,因为每个用户通常都知道自己的校验选项(比如密码问题或密码问题组合)。考虑到仍然有少数用户会忘记自己当初设定的密码问题本身是什么,在一种比较贴近用户使用体验的优化方案中,所述选择性找回验证界面包括与用户账户对应的校验子界面,每个用户的校验选项在各自的子界面中。此时当前用户可以选择在任意一个校验子界面上完成校验。同样的道理,对于使用一个手机号的主账户以及子账户而言,密码找回的处理也可以采用上述流程。

[0062] 假设左侧校验子界面与Tony对应,右侧校验子界与Kevin对应。此时若用户是Tony,则其会在左侧的校验子界面上完成“母亲生日”以及“父亲出生地”这些校验选项,因为右侧校验子界面中的校验选项并不是Tony的,因此Tony一般情况下是无法完成的。相反此时若用户是Kevin,则其会在右侧的校验子界面上完成“小学三年级班主任是谁”以及“最喜欢的电影”两个密码问题组合构成的校验选项,当然校验选项除了密码问题或密码问题组合之外,还可能是其他的校验方式,本申请对此并无特别限制。本实施方式事实上将多个登录名冲突用户的校验选项在同一个界面下分类列举,这个方式通常并不影响当前用户通过校验选项的操作来找回密码。事实上,只要用户操作了任意一个校验子界面下的校验选项,并且校验成功的话,那么此时系统就知道当前用户的账户记录了,因为每一个用户的账户记录中通常都有对应的校验选项(如果用户在注册时进行了相应的设定)。

[0063] 如前所述,在本申请中,账户表中每个用户的登录名字段可能会包括冲突识别参数或者关联识别参数,首先这两种参数并不冲突。请参考表5的示例,对于应用系统的流程处理而言,只要定义好两种参数的字符选择以及对应的位置即可。比如说,冲突识别参数选择字符“R”,位置在分隔符“|”右侧,而关联识别参数选择“T”,位置在冲突识别参数“R”的右侧;当然本领域技术人员也可以采用其他的符合实际业务应用需求的数据格式定义方式。其次,考虑到极其少量的情况下,可能会发生三次放号的情况,或者系统允许用户基于一个主账户创建多个关联的子账户时,仅凭一个冲突识别参数无法满足这种很特殊的需求(当然这种需求系统也可以不支持)。为了满足这种特殊需求,可以在识别参数之后再添加上一串包括多个字符的随机数。请参考表5的示例,在一种优选的实施方式中,为了开发便利,对于常规账户(不是冲突老用户,也不是子账户)也可以引入识别参数,比如用字符“A”

[0064] 表示正常账户。表5中“13900100110|A987688ab”表征一个常规账户;而“18611180751|Rktt dihss”则表征一个冲突老用户。“13988888888|RT0208adkz”表征一个冲突老用户,同时该用户的账户还是其他用户账户的子账户。

[0065]

序号	字段一	字段二
	登录名+分隔符+识别因子	登录密码
1	13900100110 A987688ab	aaaaaa
2	18611180751 Rktt dihss	bbbbbb
3	18611180751 Akt sd098	cccccc

4	13988888888 R36derdd	aaaaaa
5	13988888888 RT0208adkz	dddddd
6	13988888888 A9963tyf	Eeeeeee
.....		

[0066] 表5

[0067] 在一个典型的配置中,服务器这样的计算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。

[0068] 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。

[0069] 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暂存电脑可读媒体(transitory media),如调制的数据信号和载波。

[0070] 还需要说明的是,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0071] 以上所述仅为本申请的较佳实施例而已,并不用以限制本申请,凡在本申请的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本申请保护的范围之内。

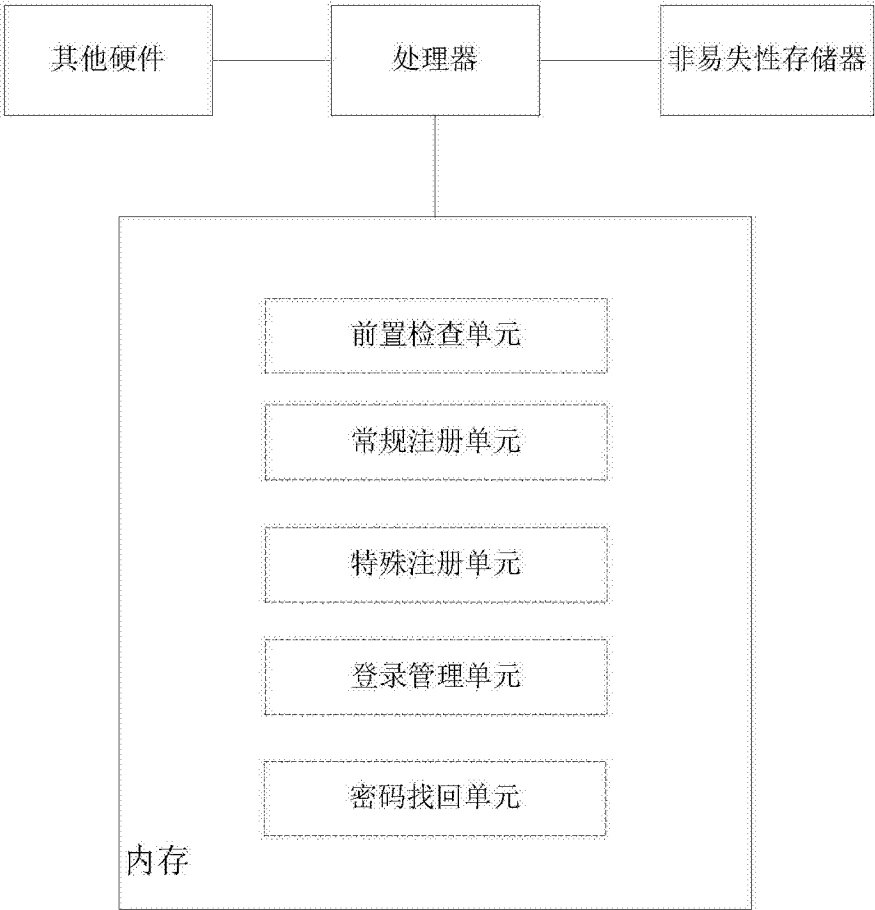


图1

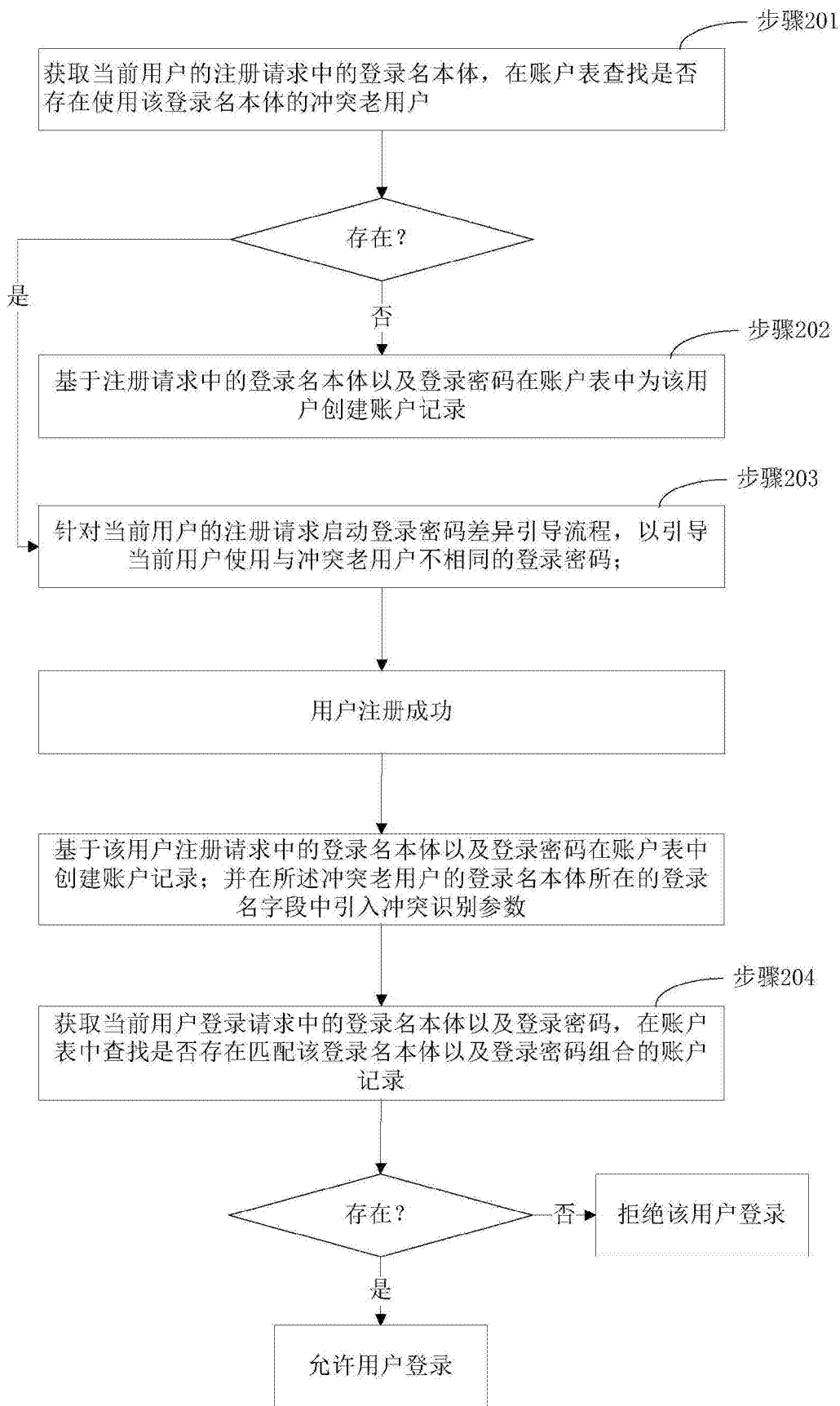


图2

手机号:	18611180751	
登录密码:		 您设置的登录密码不符合安全规则，请重新输入！
确认登录密码:		

图3a

手机号:	18611180751	
登录密码:		 您设置的登录密码不符合安全规则，请设置长度为11-13位的登录密码！
确认登录密码:		

图3b

手机号:	18611180751	
登录密码:		 您设置的登录密码不符合安全规则，请务必设置包括字符“A”的登录密码！
确认登录密码:		

图3c

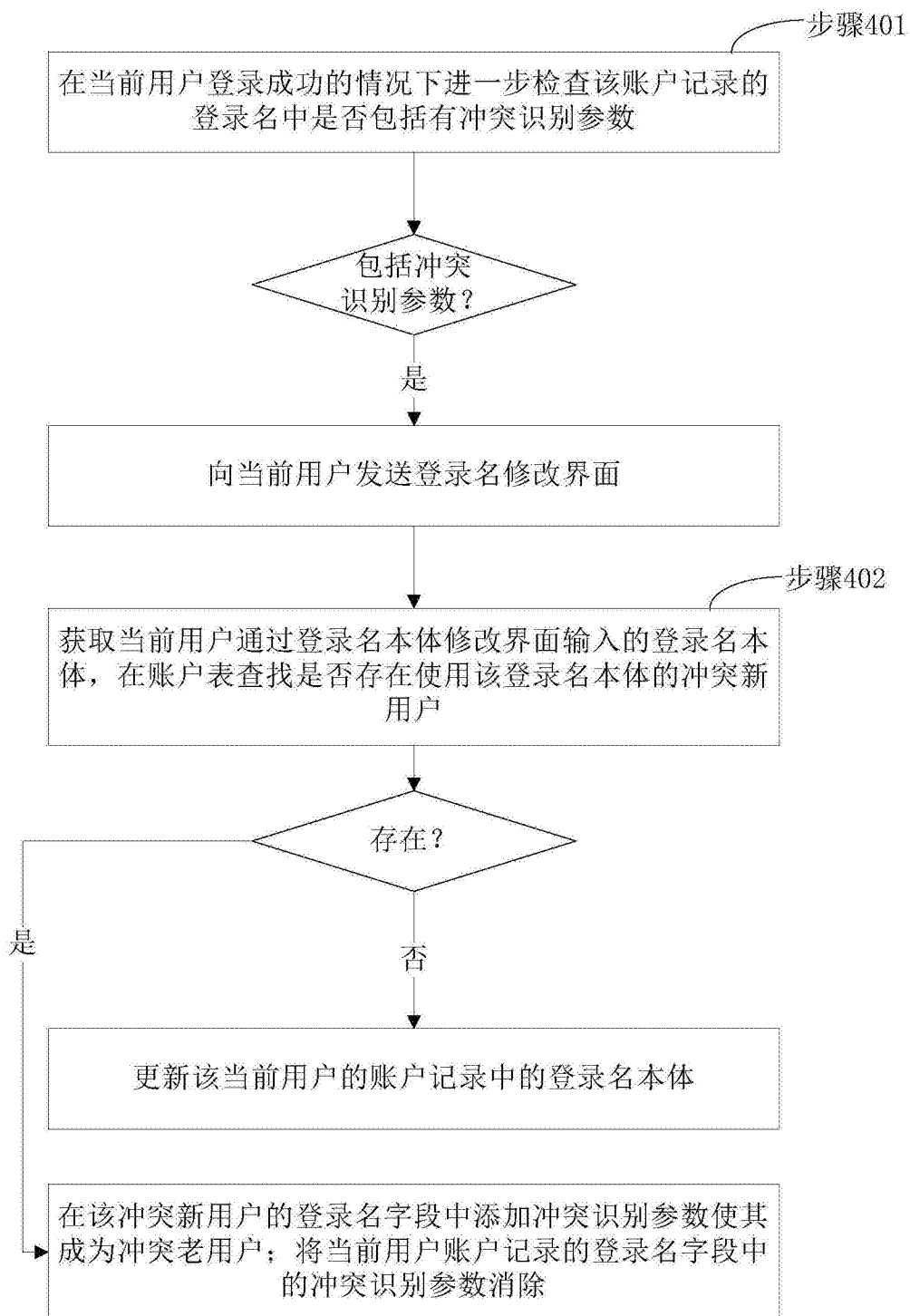


图4

左右两侧中只有一侧的密码问题是您设定的，
请选择您设定的密码问题进行回答

与用户Tony对应的校验子界面

与用户Kevin对应的校验子界面

母亲生日：

父亲出生地：

下一步

小学三年级班主任是谁：

最喜欢的电影：

下一步

图5