(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 110955884 A
(43)申请公布日 2020.04.03

(21)申请号 201911224947.X

(22)申请日 2019.12.04

(71)申请人 中国银行股份有限公司
地址 100818 北京市西城区复兴门内大街1号

(72)发明人 朱江波 张盛素 高鹏 李开峰 刘真真 李谞玥 董海丰 邱丽娇 万荃 时福林

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 周达 刘飞

(51)Int.Cl.
G06F 21/46(2013.01)
G06Q 40/02(2012.01)

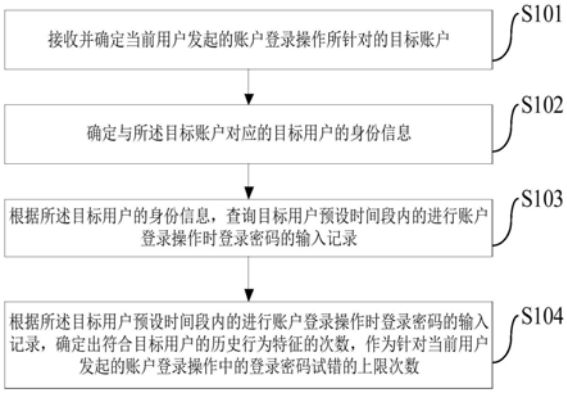
权利要求书2页 说明书15页 附图2页

(54)发明名称

密码试错的上限次数的确定方法和装置

(57)摘要

本申请实施例提供了一种密码试错的上限次数的确定方法和装置，其中，该方法包括：接收并确定当前用户发起的账户登录操作所针对的目标账户；确定出与目标账户对应的目标用户的身份信息；根据目标用户的身份信息，查询并根据目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数。从而解决了现有方法中存在的为用户进行账户登录操作时所设置的登录密码试错的上限次数不具有针对性，不够合理，影响用户正常进行账户登录操作时的使用体验的技术问题。



CN 110955884 A

1.一种密码试错的上限次数的确定方法,其特征在于,包括:

接收并确定当前用户发起的账户登录操作所针对的目标账户;

确定与所述目标账户对应的目标用户的身份信息;

根据所述目标用户的身份信息,查询目标用户预设时间段内的进行账户登录操作时登录密码的输入记录;

根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录,确定出符合目标用户的历史行为特征的次数,作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数。

2.根据权利要求1所述的方法,其特征在于,在根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录,确定出符合目标用户的历史行为特征的次数,作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数之后,所述方法还包括:

累计当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数;

在检测到当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数大于等于所述登录密码试错的上限次数的情况下,阻止当前用户继续进行针对目标账户的账户登录操作。

3.根据权利要求2所述的方法,其特征在于,阻止当前用户继续进行针对目标账户的账户登录操作,包括:

冻结目标账户,和/或,关闭当前用户进行针对目标账户的账户登录操作的操作界面。

4.根据权利要求3所述的方法,其特征在于,在阻止当前用户继续进行针对目标账户的账户登录操作之后,所述方法还包括:

生成警报提示信息,其中,所述警报提示信息用于提示当前用户不是目标用户的概率值大于预设的概率阈值。

5.根据权利要求1所述的方法,其特征在于,根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录,确定出符合目标用户的历史行为特征的次数,包括:

根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录,统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数;

将所述参考次数,与预设的容差次数的和,确定为符合目标用户的历史行为特征的次数。

6.根据权利要求5所述的方法,其特征在于,在根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录,统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数后,所述方法还包括:

根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录,确定出目标用户在预设时间段进行账户登录操作的操作频次;

根据所述操作频次,调整所述容差次数。

7.根据权利要求5所述的方法,其特征在于,在根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录,统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数后,所述方法还包括:

确定目标账户所涉及的账户数据的重要程度;

根据所述重要程度,调整所述容差次数。

8.根据权利要求5所述的方法，其特征在于，在根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数后，所述方法还包括：

确定当前用户发起的账户登录操作的当前时间点；

根据所述当前时间点，调整所述容差次数。

9.根据权利要求1所述的方法，其特征在于，所述目标账户包括以下至少之一：目标用户的银行卡账户、目标用户的电子支付账户、目标用户的社交软件账户、目标用户的购物网站账户。

10.一种密码试错的上限次数的确定装置，其特征在于，包括：

第一确定模块，用于接收并确定当前用户发起的账户登录操作所针对的目标账户；

第二确定模块，用于确定与所述目标账户对应的目标用户的身份信息；

查询模块，用于根据所述目标用户的身份信息，查询目标用户预设时间段内的进行账户登录操作时登录密码的输入记录；

第三确定模块，用于根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数。

11.根据权利要求10所述的装置，其特征在于，所述装置还包括累计模块和处理模块，其中，

所述累计模块，用于累计当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数；

所述处理模块，用于在检测到当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数大于等于所述登录密码试错的上限次数的情况下，阻止当前用户继续进行针对目标账户的账户登录操作。

12.一种电子设备，包括处理器以及用于存储处理器可执行指令的存储器，其特征在于，所述处理器执行所述指令时实现权利要求1至9中任一项所述方法的步骤。

13.一种计算机可读存储介质，其上存储有计算机指令，其特征在于，所述指令被执行时实现权利要求1至9中任一项所述方法的步骤。

密码试错的上限次数的确定方法和装置

技术领域

[0001] 本申请涉及业务数据处理技术领域，特别涉及一种密码试错的上限次数的确定方法和装置。

背景技术

[0002] 在许多业务应用场景中，用户如果想要登录某个账户，例如，银行卡账户等，进行相应的业务操作时，通常需要先在相关设备所展示的登录界面中输入要登录的账户名称，以及对应的登录密码，以请求登录该账户。系统服务器会通过对用户输入的账户名称和登录密码进行匹配验证，当通过了系统服务器的匹配验证后，用户才能登录该账户，进行相应的业务操作。

[0003] 系统服务器通常会为不同用户设置一个统一的登录密码试错的上限次数，以允许用户在该上限次数的次数范围内在输错了登录密码的情况下，可以有机会重新输入正确的登录密码，以进行账户登录。如果用户连续输入登录密码错误的次数大于等于该上限次数时，为了保护用户的账户数据的安全，避免违规用户通过进行多次的账户登录操作，尝试出用户的登录密码，系统服务器会暂时将该账户冻结，以保护该账户的账户数据安全。

[0004] 但是，具体实施时发现基于上述方法所设置的登录密码试错的上限次数对于一些用户而言往往不够合理，使得一些用户在正常进行账户登录操作的使用体验相对较差。

[0005] 针对上述问题，目前尚未提出有效的解决方案。

发明内容

[0006] 本申请实施例提供了一种密码试错的上限次数的确定方法和装置，以解决现有方法中存在的为用户进行账户登录操作时所设置的登录密码试错的上限次数不具有针对性，不够合理，影响用户正常进行账户登录操作时的使用体验的技术问题，达到能够根据不同用户具体的行为特征，有针对性地为不同用户分别设置对应合适的登录密码试错的上限次数，从而可以兼顾用户正常进行账户登录操作时的使用体验，较好地管控用户进行账户登录操作，保护账户的数据安全的技术效果。

[0007] 本申请实施例提供了一种密码试错的上限次数的确定方法，包括：

[0008] 接收并确定当前用户发起的账户登录操作所针对的目标账户；

[0009] 确定与所述目标账户对应的目标用户的身份信息；

[0010] 根据所述目标用户的身份信息，查询目标用户预设时间段内的进行账户登录操作时登录密码的输入记录；

[0011] 根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数。

[0012] 在一个实施例中，在根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的

账户登录操作中的登录密码试错的上限次数之后，所述方法还包括：

[0013] 累计当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数；

[0014] 在检测到当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数大于等于所述登录密码试错的上限次数的情况下，阻止当前用户继续进行针对目标账户的账户登录操作。

[0015] 在一个实施例中，阻止当前用户继续进行针对目标账户的账户登录操作，包括：

[0016] 冻结目标账户，和/或，关闭当前用户进行针对目标账户的账户登录操作的操作界面。

[0017] 在一个实施例中，在阻止当前用户继续进行针对目标账户的账户登录操作之后，所述方法还包括：

[0018] 生成警报提示信息，其中，所述警报提示信息用于提示当前用户不是目标用户的概率值大于预设的概率阈值。

[0019] 在一个实施例中，根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，包括：

[0020] 根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数；

[0021] 将所述参考次数，与预设的容差次数的和，确定为符合目标用户的历史行为特征的次数。

[0022] 在一个实施例中，在根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数后，所述方法还包括：

[0023] 根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出目标用户在预设时间段进行账户登录操作的操作频次；

[0024] 根据所述操作频次，调整所述容差次数。

[0025] 在一个实施例中，在根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数后，所述方法还包括：

[0026] 确定目标账户所涉及的账户数据的重要程度；

[0027] 根据所述重要程度，调整所述容差次数。

[0028] 在一个实施例中，在根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数后，所述方法还包括：

[0029] 确定当前用户发起的账户登录操作的当前时间点；

[0030] 根据所述当前时间点，调整所述容差次数。

[0031] 在一个实施例中，所述目标账户包括以下至少之一：目标用户的银行卡账户、目标用户的电子支付账户、目标用户的社交软件账户、目标用户的购物网站账户。

[0032] 本申请实施例还提供了一种密码试错的上限次数的确定装置，包括：

[0033] 第一确定模块，用于接收并确定当前用户发起的账户登录操作所针对的目标账

户；

[0034] 第二确定模块，用于确定与所述目标账户对应的目标用户的身份信息；

[0035] 查询模块，用于根据所述目标用户的身份信息，查询目标用户预设时间段内的进行账户登录操作时登录密码的输入记录；

[0036] 第三确定模块，用于根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数。

[0037] 在一个实施例中，所述装置还包括累计模块和处理模块，其中，

[0038] 所述累计模块，用于累计当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数；

[0039] 所述处理模块，用于在检测到当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数大于等于所述登录密码试错的上限次数的情况下，阻止当前用户继续进行针对目标账户的账户登录操作。

[0040] 本申请实施例还提供了一种电子设备，包括处理器以及用于存储处理器可执行指令的存储器，所述处理器执行所述指令时实现接收并确定当前用户发起的账户登录操作所针对的目标账户；确定与所述目标账户对应的目标用户的身份信息；根据所述目标用户的身份信息，查询目标用户预设时间段内的进行账户登录操作时登录密码的输入记录；根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数。

[0041] 本申请实施例还提供了一种计算机可读存储介质，其上存储有计算机指令，所述指令被执行时实现接收并确定当前用户发起的账户登录操作所针对的目标账户；确定与所述目标账户对应的目标用户的身份信息；根据所述目标用户的身份信息，查询目标用户预设时间段内的进行账户登录操作时登录密码的输入记录；根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数。

[0042] 在本申请实施例中，考虑到了不同用户具体的行为特征，通过获取并根据目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，来有针对性地确定出与当前用户想要登录的目标账户的目标用户的历史行为特征相符的登录密码试错的上限次数，以便后续可以根据该上限次数对当前用户所发起的针对目标账户的账户登录操作进行有效、合理管控。从而解决了现有方法中存在的为用户进行账户登录操作时所设置的登录密码试错的上限次数不具有针对性，不够合理，影响用户正常进行账户登录操作时的使用体验的技术问题，达到能够根据不同用户具体的行为特征，有针对性地为不同用户分别设置对应合适的登录密码试错的上限次数，来兼顾用户正常进行账户登录操作时的使用体验，并能较好地管控用户进行账户登录操作，保护目标账户的账户数据安全的技术效果。

附图说明

[0043] 为了更清楚地说明本申请实施例或现有技术中的技术方案，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

申请中记载的一些实施例，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。

[0044] 图1是根据本申请实施方式提供的业务操作的操作时间的确定方法的处理流程图；

[0045] 图2是根据本申请实施方式提供的密码试错的上限次数的确定装置的组成结构图；

[0046] 图3是基于本申请实施例提供的密码试错的上限次数的确定方法的电子设备组成结构示意图。

具体实施方式

[0047] 为了使本技术领域的人员更好地理解本申请中的技术方案，下面将结合本申请实施例中的附图，对本申请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他实施例，都应当属于本申请保护的范围。

[0048] 考虑到基于现有的密码试错的上限次数的确定方法，往往没有考虑不同用户的具体情况，对用户不同的行为特征不作区分，而是对所有的用户都设置一个统一次数作为不同用户进行账户登录操作时，登录密码试错的上限次数。进而可以根据该上限次数对用户的账户登录操作进行相应管控，如果用户在进行账户登录操作时，输入登录密码的错误次数大于等于上述上限次数，则会直接冻结该账户。基于上述方法，具体实施时，所确定出的登录密码试错的上限次数往往不具有针对性，导致存在上限次数设置不够合理，甚至会影响用户正常进行账户登录操作时的使用体验。

[0049] 例如，用户A是一位老人，年纪比较大，记性相对不好，常常会出现在进行银行账户的登录操作时，多次输错登录密码之后，才会找到并输入正确的登录密码，以登录自己的银行账户。对于用户A而言，系统服务器所设置的登录密码试错的上限次数往往不够，导致可能用户A在连续输错多次登录密码，还找到正确的登录密码之前，登录密码的输错次数就已经达到了系统服务器统一设置的登录密码试错的上限次数，进而使得用户A无法正常登录自己的银行账户，影响用户A进行账户登录操作的使用体验。

[0050] 又例如，用户B是一位年轻人，记性相对比较好，通常在登录自己的银行账户时，不会出现输错登录密码的情况，这时系统服务器所设置的登录密码试错的上限次数对于用户B又显得太多了，反而会为其他用户通过对用户B的银行账户密码进行多次尝试提供方便，影响到用户B的银行账户的数据安全。

[0051] 可见，现有的密码试错的上限次数的确定方法，具体实施时，往往存在为用户进行账户登录操作时所设置的登录密码试错的上限次数不具有针对性，不够合理，影响用户正常进行账户登录操作时的使用体验的技术问题。

[0052] 针对产生上述技术问题的根本原因，本申请考虑可以根据不同账户所对应的用户的历史行为特征，有区分地为不同账户设置对应、合适的登录密码试错的上限次数，这样可以充分考虑到账户所对应的用户的具体情况，兼顾用户正常进行账户登录操作的使用体验的同时，较为有效地保护用户的账户数据的安全。从而可以较好地解决现有方法中存在的

为用户进行账户登录操作时所设置的登录密码试错的上限次数不具有针对性，不够合理，影响用户正常进行账户登录操作时的使用体验的技术问题。

[0053] 基于上述思考思路，本申请实施例提供了一种密码试错的上限次数的确定方法。具体请参阅图1所示的根据本申请实施方式提供的密码试错的上限次数的确定方法的处理流程图。本申请实施例提供的密码试错的上限次数的确定方法，具体实施时，可以包括以下内容。

[0054] S101：接收并确定当前用户发起的账户登录操作所针对的目标账户。

[0055] 在一个实施例中，上述密码试错的上限次数的确定方法具体可以应用于相关业务场景的系统服务器中。具体实施时，可以通过上述系统服务器负责为各个账户生成对应该账户的登录密码试错的上限次数。

[0056] 在一个实施例中，上述密码试错的上限次数的确定方法还可以应用于业务服务方提供的自助业务操作设备中，例如，银行的ATM机(Automatic Teller Machine，自动取款机)，也或者设置银行中用于引导、服务客户自助服务机、自助查询机等等。当然，上述所列举的自助业务操作设备只是一种示意性说明。具体实施时，可以根据具体的应用场景，应用于其他业务场景下的自助业务操作设备中。例如，设置于火车站的自助购票机等。

[0057] 此外，上述密码试错的上限次数的确定方法还可以应用于用户自己拥有、使用的客户端设备，例如，用户的智能手机、台式电脑、笔记本电脑等设备。

[0058] 在一个实施例中，上述账户具体可以包括银行卡账户，也可以包括电子支付账户，还可以包括社交软件账户等等。当然，上述所列举的账户只是一种示意性说明。具体实施时，根据具体的应用场景，还可以包括其他类型的账户。对此，本说明书不作限定。

[0059] 在一个实施例中，当前用户具体可以包括当前发起账户登录操作，想要登录账户登录操作所针对的目标账户的用户。上述目标账户具体可以包括当前用户想要登录的账户。其中，真正有权限登录并使用上述目标账户的用户可以记为目标用户。

[0060] 在一个实施例中，上述当前用户具体可以是目标用户。也可以是除目标用户之外的原本没有权限登录使用目标账户的其他用户，例如，想要通过多次尝试套出目标账户的登录密码的违规用户等。

[0061] 在一个实施例中，当前用户可以通过客户端设备，或者自助业务操作设备，进入账户登录界面；通过在上述账户登录界面进行相应操作发起针对目标账户的账户登录操作。具体的，例如，当前用户可以在该账户登录界面中展示的账户输入栏中输入要登录的目标账户的账户名，或者注册目标账户时使用的手机号、身份证号等与目标用户相关的身份信息。同时，在该账户登录界面中展示的密码输入栏中输入对应的登录密码。再点击该账户登录界面中的确认按键，生成并向系统服务器发出对应的针对目标账户的账户登录请求。从而发起针对目标账户的账户登录操作。相应的，系统服务器可以接收到上述账户登录请求，接收到当前用户所发起的账户登录操作。当然，需要说明的是，上述所列举的当前用户发起针对目标账户的账户登录操作的方式只是一种示意性说明。具体实施时，根据具体的应用场景，当前用户也可以采用其他合适的方式发起针对目标账户的账户登录操作。

[0062] 在一个实施例中，以系统的服务器为例，服务器在接收到上述当前用户发起的账户登录操作后，可以确定出当前用户发起的账户登录操作所针对的，即当前用户想要登录到目标账户。

[0063] 具体的，服务器可以从所接收到的账户登录请求中解析提取出当前用户输入的目标账户的名称，或者目标用户注册目标账户时使用的手机号、身份证号等身份信息等数据，再根据上述数据，确定出当前用户发起的账户登录操作所针对的目标账户。

[0064] S102：确定与所述目标账户对应的目标用户的身份信息。

[0065] 在本实施例中，上述目标用户的身份信息具体可以包括目标用户在注册目标账户时使用的手机号、身份证号、注册邮箱等等。当然，上述所列举的目标用户的身份信息只是一种示意性说明。具体实施时，根据具体的应用场景，上述目标用户的身份信息还可以包括除上述所列举的身份信息之外其他能够指示目标用户的信息。

[0066] 在一个实施例中，系统服务器可以根据上述目标账户，通过检索系统服务器记录保存的账户数据库，确定出与目标账户对应的目标用户的身份信息。

[0067] 其中，上述账户数据库中记录保存了各个账户，以及与各个账户分别对应的用户和用户的身份信息。

[0068] 在一个实施例中，系统服务器可以通过检索上述账户数据库，找到与目标账户对应的用户确定为目标用户，进一步可以通过查询上述账户数据库，获取上述目标用户的身份信息。

[0069] S103：根据所述目标用户的身份信息，查询目标用户预设时间段内的进行账户登录操作时登录密码的输入记录。

[0070] 在一个实施例中，上述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，具体可以包括在历史上的预设时间段内，目标用户每次进行登录操作输入登录密码时的密码输入时间、密码输错次数等记录数据。

[0071] 其中，上述预设时间段具体可以是最近的五天，或者最近的一个月等。当然，上述所列举的预设时间段只是一种示意性说明。具体实施时，根据具体情况可以灵活设置上述预设时间段。对此，本说明书不作限定。

[0072] 在本实施例中，系统服务器采集并记录下各个用户每一次进行账户登录操作时，输入登录密码时的历史行为数据，例如，用户的身份信息、用户本次所要登录的账户名称、用户本次输入登录密码的时间、用户本次输入登录密码时输错的次数等等。进而可以根据上述历史行为数据，分别为每一个用户建立对应的登录密码的历史输入记录。

[0073] 在一个实施例中，具体实施时，系统服务器可以先根据目标用户的身份信息，找到与目标用户对应的登录密码的历史输入记录。再从所述与目标用户对应的登录密码的历史输入记录中查询出预设时间段内的记录，以确定出目标用户预设时间段内的进行账户登录操作时登录密码的输入记录。

[0074] S104：根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数。

[0075] 在一个实施例中，上述登录密码试错的上限次数具体可以理解为一种阈值次数。如果用户输入登录密码的错误次数大于等于上述登录密码试错的上限次数，为了保护目标账户的账户数据安全，避免违规用户想要通过进行多次账户登录操作尝试出目标账户的登录密码，将会阻止用户继续针对该目标账户发起账户登录操作。

[0076] 在本实施例中，具体实施时，可以根据目标用户预设时间段内的进行账户登录操

作时登录密码的输入记录，确定出目标用户最近一段时间内输入登录密码时的行为特征。例如，根据用户C预设时间段内的进行账户登录操作时登录密码的输入记录，可以确定出用户C最近一段时间正常进行针对账户名称为T1121账户的账户登录操作时登录密码输错次数较多，平均每次进行账户登陆操作时会输错6次，其中，输错密码次数最高的一次账户登陆操作输错了8次。进一步，可以根据上述确定出的目标用户最近一段时间内输入登录密码时的行为特征，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数。例如，可以选择用户C最近一段时间中在一次账户登录操作中输错登陆密码次数的最大值6次作为参考次数，再将上述参考次数与预设的容差次数(例如1次)相加，得到的和(7次)确定为符合用户C最近一段时间的李思行为特征的次数据。进而可以将上述次数确定针对当前用户发起的针对用户C的账户名称为T1121账户的账户登录操作中登录密码试错的上限次数。

[0077] 通过上述方式设置的登录密码试错的上限次数，充分考虑到目标账户的目标用户的历史行为特征，使得所确定出的登录密码试错的上限次数更具有针对性、更加合理，不会影响到目标用户正常登录目标账户进行账户登录操作时的使用体验。

[0078] 例如，基于现有方法，确定出的当前用户发起的针对用户C的账户名称为T1121账户的账户登录操作中登录密码试错的上限次数为一个与其他账户的登录密码试错的上限次数相同，例如，为一个统一的固定值3次。而基于用户C历史的行为特征，实际上，如果用户C本人自己正常发起针对该账户的账户登录操作，却很可能出现用户C还没有登录成功，就已经因为自己登录密码的输错次数超过了上限次数，而被系统服务器冻结账户，导致无法正常地登录自己的账户，从而影响了用户C的使用体验。

[0079] 而基于本申请实施例所提供的密码试错的上限次数的确定方法，能有针对性地确定出符合用户C最近一段时间的行为特征的次数，例如6次，作为当前用户发起的针对用户C的账户名称为T1121账户的账户登录操作中登录密码试错的上限次数。这样用户C可能在第5次输入登录密码时，就能成功地登录自己的账户了。

[0080] 在一个实施例中，在确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数之后，进一步，服务器会根据上述上限次数对当前用户发起的针对目标账户的账户登录操作进项监控管理。

[0081] 在一个实施例中，具体实施时，服务器会累计当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数。例如，服务器每发现当前用户在一次账户登录操作时输错的登录密码是错误，则将原有的累积输错次数加1，对累积输错次数进行更新，得到新的累积输错次数。同时，在每次对累积输错次数进行更新后，会将新的累积输错次数与所确定登录密码试错的上限次数进行数值比较，确定当前用户的累积输错次数是否大于登录密码试错的上限次数。在检测到当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数大于等于所述登录密码试错的上限次数的情况下，可以判断当前用户具有较高概率可能不时目标用户，存在违规登录目标账户的风险，这时可以阻止当前用户继续进行针对目标账户的账户登录操作，以避免其他用户通过进行多次的账户登录操作，尝试出目标账户的登录密码。

[0082] 在一个实施例中，在检测到当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数大于等于所述登录密码试错的上限次数的情况下，具体实施时，可以

通过冻结目标账户，和/或，关闭当前用户进行针对目标账户的账户登录操作的操作界面来阻止当前用户继续进行针对目标账户的账户登录操作，保护目标账户的账户数据安全。当然，上述所列举的阻止方式只是一种示意性说明，具体实施时，还可以根据具体情况，采用其他合适的阻止方式来阻止当前用户继续进行针对目标账户的账户登录操作。例如，还可以拒绝接受当前用户所在的IP发出的账户登录请求等等。

[0083] 在一个实施例中，为了能更好地保护目标账户的账户数据安全，在按照上述所列举的阻止方式阻止当前用户继续进行针对目标账户的账户登录操作之后，还可以进一步生成对应警报提示信息。其中，所述警报提示信息具体可以用于提示当前用户不是目标用户的概率值大于预设的概率阈值。具体实施时，可以将该警报提示信息发送至监控服务器，以便监控服务器能够根据该警报提示信息，对当前用户是否是目标用户进行进一步的确认。

[0084] 例如，监控服务器可以调用设置于自助业务操作设备上的监控摄像头，获取正在自助业务操作设备上操作的当前用户的人脸照片，再查询用户的账户数据库，获取所记录保存的与目标账户对应的目标用户的人脸图片，将当前用户的人脸照片和目标用户的人脸图片进行人脸比对，以确定出当前用户是否为目标用户，得到对应的人脸比对结果，再把人脸比对结果反馈给系统服务器。

[0085] 系统服务器可以根据比对结果确定当前用户是否是目标用户，如果根据比对结果确定当前用户为目标用户本人，则可以解除之前对当前用户的继续进行针对目标账户的账户登录操作的阻止。例如，可以解除对目标账户的冻结状态等。相对的，如果根据比对结果确定当前用户不是目标用户本人，则可以继续保持阻止当前用户的进行针对目标账户的账户登录操作。例如，保持目标账户的冻结状态等。此外，也可以将上述警报提示信息发送给目标用户本人，以提示目标用户自行确认等。

[0086] 在本申请实施例中，相较于现有方法，由于考虑到了不同用户具体的行为特征，通过获取并根据目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，来有针对性地确定出与当前用户想要登录的目标账户的目标用户的历史行为特征相符的登录密码试错的上限次数，以便后续可以根据该上限次数对当前用户所发起的针对目标账户的账户登录操作进行有效、合理管控。从而解决了现有方法中存在的为用户进行账户登录操作时所设置的登录密码试错的上限次数不具有针对性，不够合理，影响用户正常进行账户登录操作时的使用体验的技术问题，达到能够根据不同用户具体的行为特征，有针对性地为不同用户分别设置对应合适的登录密码试错的上限次数，来兼顾用户正常进行账户登录操作时的使用体验，较好地管控用户进行账户登录操作的技术效果。

[0087] 在一个实施例中，在根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数之后，所述方法具体实施时，还可以包括以下内容：累计当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数；在检测到当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数大于等于所述登录密码试错的上限次数的情况下，阻止当前用户继续进行针对目标账户的账户登录操作。

[0088] 在一个实施例中，上述阻止当前用户继续进行针对目标账户的账户登录操作，具体实施时，可以包括以下内容：冻结目标账户，和/或，关闭当前用户进行针对目标账户的账

户登录操作的操作界面等。当然，具体实施时，根据具体情况，也可以采用其他合适的阻止方式来阻止当前用户继续进行针对目标账户的账户登录操作，从而避免当前用户通过进行多次的账户登录操作尝试出目标账户的登录密码。

[0089] 在一个实施例中，在阻止当前用户继续进行针对目标账户的账户登录操作之后，所述方法具体实施时，还可以包括以下内容：生成警报提示信息，其中，所述警报提示信息用于提示当前用户不是目标用户的概率值大于预设的概率阈值。

[0090] 在一个实施例中，上述根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，具体实施时，可以包括以下内容：根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数；将所述参考次数，与预设的容差次数的和，确定为符合目标用户的历史行为特征的次数。

[0091] 在一个实施例中，所述目标账户具体可以包括以下至少之一：目标用户的银行卡账户、目标用户的电子支付账户、目标用户的社交软件账户、目标用户的购物网站账户等等。当然，上述所列举的目标账户只是一种示意性说明。具体实施时，根据具体的应用场景，上述目标账户还可以包括其他类型的账户。对此，本说明书不作限定。

[0092] 在一个实施例中，考虑到很多情况下，有的用户如果很长时间都没有登录自己的账户，或者很少登录自己的账户，正常情况下，这类用户在输入登录密码时相对于其他经常登录账户的用户更容易输错密码，这时为了保证这类用户的使用体验，可以考虑适当地增加这类用户的密码试错的上限次数。

[0093] 基于上述考虑，在根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数后，所述方法具体实施时，还可以包括以下内容：根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出目标用户在预设时间段进行账户登录操作的操作频次；根据所述操作频次，调整所述容差次数。

[0094] 在本实施例中，具体实施时可以根据目标用户在预设时间段进行账户登录操作的操作频次，通过调整容差次数对当前用户发起的账户登录操作中的登录密码试错的上限次数进行相应的调整。

[0095] 例如，如果确定目标用户在预设时间段进行账户登录操作的操作频次为小于等于每月2次，则可以判断该用户最近很少进行账户登录操作，相对的更有可能遗忘登录密码，这时可以通过对容差次数加1，来增加这类用户的登录密码试错的上限次数，以便该用户能正常登录自己的账户，提高用户的使用体验。如果确定目标用户在预设时间段进行账户登录操作的操作频次为小于等于每月5次，大于每月2次，则可以判断该用户最近进行账户登录操作的操作频次正常，这时可以不调整容差次数。如果确定目标用户在预设时间段进行账户登录操作的操作频次为大于每月5次，则可以判断该用户最近频繁进行账户登录操作，相对的更不可能遗忘登录密码，这时可以通过对容差次数减1，来减少这类用户的登录密码试错的上限次数，以使得在不影响用户使用体验的情况下，保护用户的账户数据安全。

[0096] 当然，需要说明的是，上述所列举的根据操作频次对容差次数的调整只是一种示意性说明。具体实施时，根据具体情况和安全要求，还可以采用其他方式来根据操作频次对

容差次数进行相应调整。

[0097] 在一个实施例中，又考虑到对于同一个目标用户的不同目标账户，由于涉及到的账户数据的重要程度不同，对数据安全的要求也会存在差异。例如，银行账户涉及到用户的资金数据重要程度较高，对数据安全的要求也相对较高。而聊天账户涉及到的聊天数据重要程度较低，对数据安全的要求也相对较低。

[0098] 基于上述考虑，为了能够更好地兼顾用户的使用体验和数据安全，具体实施时，还可以通过根据目标账户所涉及的账户数据的重要程度，适当地调整容差次数来调整登录密码试错的上限次数。

[0099] 具体的，在根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数后，所述方法还可以包括：确定目标账户所涉及的账户数据的重要程度；根据所述重要程度，调整所述容差次数。

[0100] 例如，对于所涉及的账户数据重要程度较高的目标账户，可以通过对容差次数做减一处理进行调整，来减少登录密码试错的上限次数，以更好地保护目标账户的账户数据。对于所涉及的账户数据重要程度较低的目标账户，可以通过对容差次数做加一处理进行调整，来增加登录密码试错的上限次数，以使得用户具有较好的使用体验。

[0101] 在一个实施例中，进一步考虑到在不同的时间点，用户的账户数据安全受威胁的情况也会存在差异。例如，晚上相对于白天，用户的账户数据安全受到威胁的风险会相对更高。因此，为了能够更好地保护用户的账户数据安全，还可以结合当前用户发起的账户登录操作的当前时间点，来调整容差次数，再利用上述容差次数对登录密码试错的上限次数进行相应调整。

[0102] 在本实施例中，在根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数后，所述方法具体实施时，还可以包括以下内容：确定当前用户发起的账户登录操作的当前时间点；根据所述当前时间点，调整所述容差次数。

[0103] 在一个实施例中，具体实施时，可以根据当前时间点和预设的调整规则，来调整容差次数。

[0104] 其中，上述预设的调整规则，具体可以包括：在当前时点在晚上10点到凌晨5点之间的时间段内时，对容差次数作减二调整；在当前时间点在凌晨5点到上午8点之间的时间段内，或者在下午6点到晚上10点之间的时间段内时，对容差次数作减一调整；在当前时间点在上午8点到下午6点之间的时间段内时，对容差次数不作调整。当然，上述所列举的预设的调整规则只是一种示意性说明。具体实施时，可以根据具体情况灵活调整。

[0105] 在一个实施例中，上述根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数，具体可以是根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，找到目标用户预设时间段内进行针对目标账户的登录操作；再根据目标用户预设时间段内进行针对目标账户的登录操作，统计目标用户在预设时间段内进行针对目标账户的账户登录操作时登录密码输错次数的最大值作为参考次数。

[0106] 在一个实施例中，具体实施时，还可以统计目标用户在预设时间段内进行针对目

标账户的账户登录操作时登录密码输错次数的平均值作为参考次数。也可以从目标用户在预设时间段内进行针对目标账户的账户登录操作时登录密码输错次数中筛选出登录密码输错次数的第二大值作为上述参考次数等。

[0107] 在一个实施例中，如果根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，没有找到目标用户预设时间段内进行针对目标账户的登录操作时，也可以查询目标用户预设时间段内进行针对与目标账户的近似度较高的关联账户的登录操作，并统计目标用户在预设时间段内进行针对关联账户的账户登录操作时登录密码输错次数的最大值作为参考次数。进而可以将所述参考次数，与预设的容差次数的和，确定为符合目标用户的历史行为特征的次数。

[0108] 从以上的描述中，可以看出，本申请实施例提供的密码试错的上限次数的确定方法，由于考虑到了不同用户具体的行为特征，通过获取并根据目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，来有针对性地确定出与当前用户想要登录的目标账户的目标用户的历史行为特征相符的登录密码试错的上限次数，以便后续可以根据该上限次数对当前用户所发起的针对目标账户的账户登录操作进行有效、合理管控。从而解决了现有方法中存在的为用户进行账户登录操作时所设置的登录密码试错的上限次数不具有针对性，不够合理，影响用户正常进行账户登录操作时的使用体验的技术问题，达到能够根据不同用户具体的行为特征，有针对性地为不同用户分别设置对应合适的登录密码试错的上限次数，来兼顾用户正常进行账户登录操作时的使用体验，较好地管控用户进行账户登录操作的技术效果。还通过累计当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数，并通过检测累积输错次数与登录密码试错的上限次数的数值大小来判断是否阻止当前用户继续进行针对目标账户的账户登录操作，从而可以及时、有效地发现并阻止违规用户通过进行多次账户登录操作，尝试出目标账户的登录密码，从而保护了目标账户的账户数据安全。

[0109] 基于同一发明构思，本申请实施例中还提供了一种密码试错的上限次数的确定装置，如下面的实施例所述。由于密码试错的上限次数的确定装置解决问题的原理与密码试错的上限次数的确定方法相似，因此密码试错的上限次数的确定装置的实施可以参见密码试错的上限次数的确定方法的实施，重复之处不再赘述。以下所使用的，术语“单元”或者“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。请参阅图2所示，是本申请实施例提供的密码试错的上限次数的确定装置的一种组成结构图，该装置具体可以包括：第一确定模块201、第二确定模块202、查询模块203和第三确定模块204，下面对该结构进行具体说明。

[0110] 第一确定模块201，具体可以用于接收并确定当前用户发起的账户登录操作所针对的目标账户；

[0111] 第二确定模块202，具体可以用于确定与所述目标账户对应的目标用户的身份信息；

[0112] 查询模块203，具体可以用于根据所述目标用户的身份信息，查询目标用户预设时间段内的进行账户登录操作时登录密码的输入记录；

[0113] 第三确定模块204，具体可以用于根据所述目标用户预设时间段内的进行账户登

录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数。

[0114] 在一个实施例中，所述装置具体还可以包括累计模块和处理模块，其中，

[0115] 所述累计模块，具体可以用于累计当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数；

[0116] 所述处理模块，具体可以用于在检测到当前用户在进行针对目标账户的账户登录操作时登录密码的累积输错次数大于等于所述登录密码试错的上限次数的情况下，阻止当前用户继续进行针对目标账户的账户登录操作。

[0117] 在一个实施例中，所述装置具体还可以包括阻止模块，具体可以用于通过冻结目标账户，和/或，关闭当前用户进行针对目标账户的账户登录操作的操作界面等阻止方式，阻止当前用户继续进行针对目标账户的账户登录操作。

[0118] 在一个实施例中，所述装置具体还可以包括生成模块，具体可以用于生成警报提示信息，其中，所述警报提示信息用于提示当前用户不是目标用户的概率值大于预设的概率阈值。

[0119] 在一个实施例中，为了能够根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，上述第三确定模块204具体可以包括以下结构单元：

[0120] 统计单元，具体可以用于根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，统计目标用户在预设时间段内进行账户登录操作时登录密码输错次数的最大值作为参考次数；

[0121] 确定单元，具体可以用于将所述参考次数，与预设的容差次数的和，确定为符合目标用户的历史行为特征的次数。

[0122] 在一个实施例中，所述目标账户具体可以包括以下至少之一：目标用户的银行卡账户、目标用户的电子支付账户、目标用户的社交软件账户、目标用户的购物网站账户等等。当然，上述所列举的目标账户只是一种示意性说明。具体实施时，根据具体的应用场景，上述目标账户还可以包括其他类型的账户。对此，本说明书不作限定。

[0123] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0124] 需要说明的是，上述实施方式阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。为了描述的方便，在本说明书中，描述以上装置时以功能分为各种单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0125] 此外，在本说明书中，诸如第一和第二这样的形容词仅可以用于将一个元素或动作与另一元素或动作进行区分，而不必要求或暗示任何实际的这种关系或顺序。在环境允许的情况下，参照元素或部件或步骤(等)不应解释为局限于仅元素、部件、或步骤中的一个，而可以是元素、部件、或步骤中的一个或多个等。

[0126] 从以上的描述中，可以看出，本申请实施例提供的密码试错的上限次数的确定装

置，通过查询模块和第三确定模块获取并根据目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，来有针对性地确定出与当前用户想要登录的目标账户的目标用户的历史行为特征相符的登录密码试错的上限次数，以便后续可以根据该上限次数对当前用户所发起的针对目标账户的账户登录操作进行有效、合理管控。从而解决了现有方法中存在的为用户进行账户登录操作时所设置的登录密码试错的上限次数不具有针对性，不够合理，影响用户正常进行账户登录操作时的使用体验的技术问题，达到能够根据不同用户具体的行为特征，有针对性地为不同用户分别设置对应合适的登录密码试错的上限次数，来兼顾用户正常进行账户登录操作时的使用体验，较好地管控用户进行账户登录操作的技术效果。

[0127] 本申请实施例还提供了一种电子设备，具体可以参阅图3所示的基于本申请实施例提供的密码试错的上限次数的确定方法的电子设备的组成结构示意图，所述电子设备具体可以包括输入设备31、处理器32、存储器33。其中，所述输入设备31具体可以用于接收当前用户发起的账户登录操作所针对的目标账户。所述处理器32具体可以用于确定当前用户发起的账户登录操作所针对的目标账户；确定与所述目标账户对应的目标用户的身份信息；根据所述目标用户的身份信息，查询目标用户预设时间段内的进行账户登录操作时登录密码的输入记录；根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数。所述存储器33具体可以用于存储相应的指令程序。

[0128] 在本实施方式中，所述输入设备具体可以是用户和计算机系统之间进行信息交换的主要装置之一。所述输入设备可以包括键盘、鼠标、摄像头、扫描仪、光笔、手写输入板、语音输入装置等；输入设备用于把原始数据和处理这些数的程序输入到计算机中。所述输入设备还可以获取接收其他模块、单元、设备传输过来的数据。所述处理器可以按任何适当的方式实现。例如，处理器可以采取例如微处理器或处理器以及存储可由该(微)处理器执行的计算机可读程序代码(例如软件或固件)的计算机可读介质、逻辑门、开关、专用集成电路(Application Specific Integrated Circuit，ASIC)、可编程逻辑控制器和嵌入微控制器的形式等等。所述存储器具体可以是现代信息技术中用于保存信息的记忆设备。所述存储器可以包括多个层次，在数字系统中，只要能保存二进制数据的都可以是存储器；在集成电路中，一个没有实物形式的具有存储功能的电路也叫存储器，如RAM、FIFO等；在系统中，具有实物形式的存储设备也叫存储器，如内存条、TF卡等。

[0129] 在本实施方式中，该电子设备具体实现的功能和效果，可以与其它实施方式对照解释，在此不再赘述。

[0130] 本申请实施例还提供了一种基于密码试错的上限次数的确定方法的计算机存储介质，所述计算机存储介质存储有计算机程序指令，在所述计算机程序指令被执行时实现：接收并确定当前用户发起的账户登录操作所针对的目标账户；确定与所述目标账户对应的目标用户的身份信息；根据所述目标用户的身份信息，查询目标用户预设时间段内的进行账户登录操作时登录密码的输入记录；根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数。

[0131] 在本实施方式中，上述存储介质包括但不限于随机存取存储器(Random Access

Memory,RAM)、只读存储器(Read-Only Memory,ROM)、缓存(Cache)、硬盘(Hard Disk Drive,HDD)或者存储卡(Memory Card)。所述存储器可以用于存储计算机程序指令。网络通信单元可以是依照通信协议规定的标准设置的,用于进行网络连接通信的接口。

[0132] 在本实施方式中,该计算机存储介质存储的程序指令具体实现的功能和效果,可以与其它实施方式对照解释,在此不再赘述。

[0133] 尽管本申请内容中提到不同的具体实施例,但是,本申请并不局限于必须是行业标准或实施例所描述的情况等,某些行业标准或者使用自定义方式或实施例描述的实施基础上略加修改后的实施方案也可以实现上述实施例相同、等同或相近、或变形后可预料的实施效果。应用这些修改或变形后的数据获取、处理、输出、判断方式等的实施例,仍然可以属于本申请的可选实施方案范围之内。

[0134] 虽然本申请提供了如实施例或流程图所述的方法操作步骤,但基于常规或者无创造性的手段可以包括更多或者更少的操作步骤。实施例中列举的步骤顺序仅仅为众多步骤执行顺序中的一种方式,不代表唯一的执行顺序。在实际中的装置或客户端产品执行时,可以按照实施例或者附图所示的方法顺序执行或者并行执行(例如并行处理器或者多线程处理的环境,甚至为分布式数据处理环境)。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、产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、产品或者设备所固有的要素。在没有更多限制的情况下,并不排除在包括所述要素的过程、方法、产品或者设备中还存在另外的相同或等同要素。

[0135] 上述实施例阐明的装置或模块等,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。为了描述的方便,描述以上装置时以功能分为各种模块分别描述。当然,在实施本申请时可以把各模块的功能在同一个或多个软件和/或硬件中实现,也可以将实现同一功能的模块由多个子模块的组合实现等。以上所描述的装置实施例仅仅是示意性的,例如,所述模块的划分,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,例如多个模块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。

[0136] 本领域技术人员也知道,除了以纯计算机可读程序代码方式实现控制器以外,完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件,而对其内部包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至,可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[0137] 本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述,例如程序模块。一般地,程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构、类等等。也可以在分布式计算环境中实践本申请,在这些分布式计算环境中,由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中,程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0138] 通过以上的实施方式的描述可知,本领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解,本申请的技术方案本质

上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，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，移动终端，服务器，或者网络设备等)执行本申请各个实施例或者实施例的某些部分所述的方法。

[0139] 本说明书中的各个实施例采用递进的方式描述，各个实施例之间相同或相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。本申请可用于众多通用或专用的计算机系统环境或配置中。例如：个人计算机、服务器计算机、手持设备或便携式设备、平板型设备、多处理器系统、基于微处理器的系统、置顶盒、可编程的电子设备、网络PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境等等。

[0140] 虽然通过实施例描绘了本申请，本领域普通技术人员知道，本申请有许多变形和变化而不脱离本申请的精神，希望所附的实施方式包括这些变形和变化而不脱离本申请。

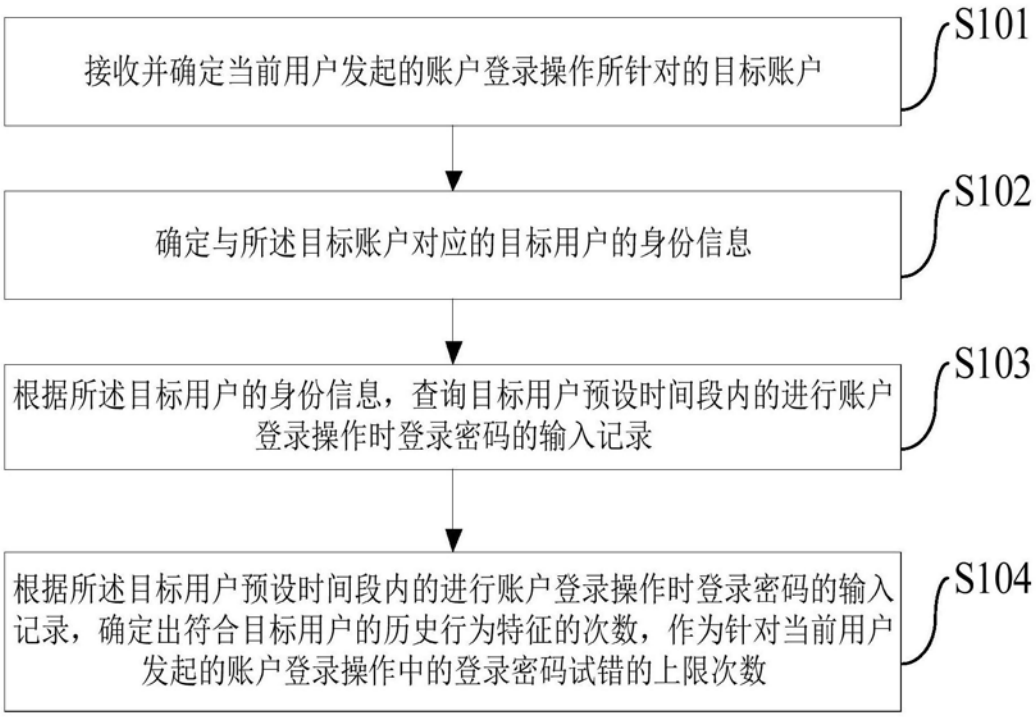

接收并确定当前用户发起的账户登录操作所针对的目标账户
S101
确定与所述目标账户对应的目标用户的身份信息
S102
根据所述目标用户的身份信息，查询目标用户预设时间段内的进行账户登录操作时登录密码的输入记录
S103
根据所述目标用户预设时间段内的进行账户登录操作时登录密码的输入记录，确定出符合目标用户的历史行为特征的次数，作为针对当前用户发起的账户登录操作中的登录密码试错的上限次数
S104

图1

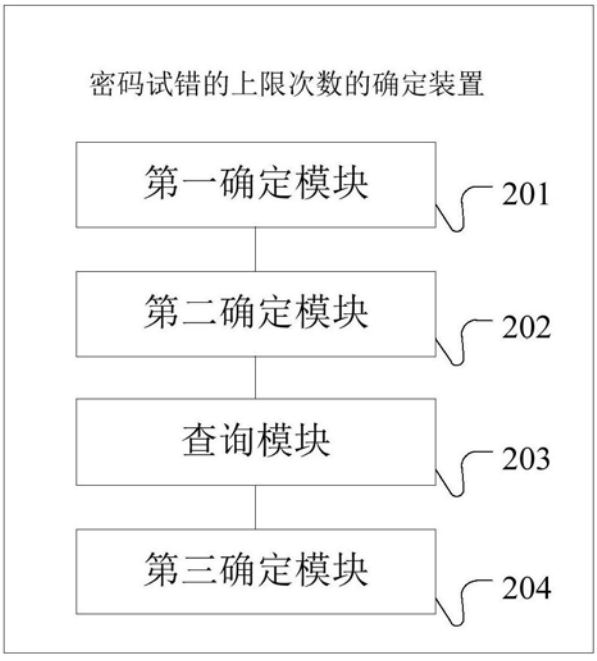

密码试错的上限次数的确定装置
第一确定模块
201
第二确定模块
202
查询模块
203
第三确定模块
204

图2

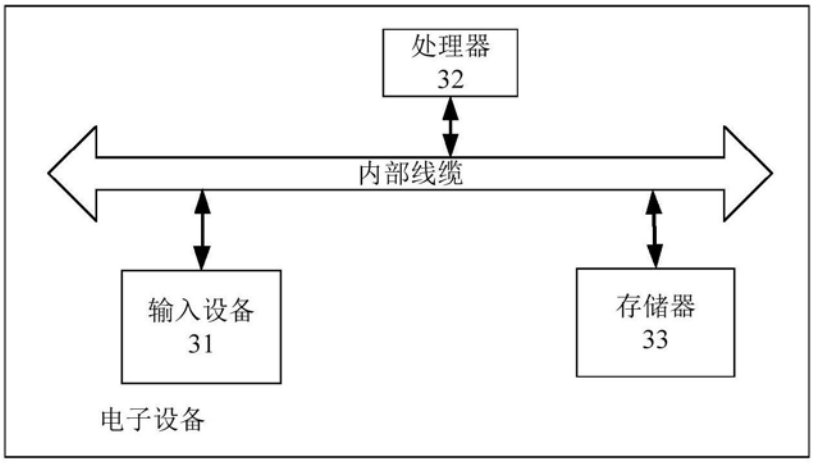


图3