(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114598550 A
(43)申请公布日 2022.06.07

(21)申请号 202210311454.5

(22)申请日 2022.03.28

(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 王贺超 朱明会 沙倩

(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 汤在彦 王维宁

(51)Int.Cl.
*H04L 9/40*(2022.01)
*H04W 12/122*(2021.01)

权利要求书2页 说明书8页 附图3页

(54)发明名称

短信验证码攻击防护方法及装置

(57)摘要

本申请提供了一种短信验证码攻击防护方法及装置，可用于金融领域或其他领域，该方法包括：接收目标用户的获取短信验证码请求，该获取短信验证码请求包括：所述目标用户的登录操作信息和登录地址信息；根据所述登录操作信息和登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数；判断所述已发送的短信验证码次数是否超出短信验证码次数阈值，若是，则拒绝所述获取短信验证码请求，完成所述获取短信验证码请求对应的短信验证码攻击防护。本申请能够避免短信炸弹问题，能够提高短信验证码攻击防护的准确性，进而能够提升用户体验。


CN 114598550 A

1.一种短信验证码攻击防护方法,其特征在于,包括:

接收目标用户的获取短信验证码请求,该获取短信验证码请求包括:所述目标用户的登录操作信息和登录地址信息;

根据所述登录操作信息和登录地址信息,获得在预设时间周期内向所述目标用户已发送的短信验证码次数;

判断所述已发送的短信验证码次数是否超出短信验证码次数阈值,若是,则拒绝所述获取短信验证码请求,完成所述获取短信验证码请求对应的短信验证码攻击防护。

2.根据权利要求1所述的短信验证码攻击防护方法,其特征在于,所述根据所述登录操作信息和登录地址信息,获得在预设时间周期内向所述目标用户已发送的短信验证码次数,包括:

判断所述登录操作信息是否包含有目标用户的已登陆状态标识和用户唯一标识,若是,则根据所述用户唯一标识,获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

3.根据权利要求1所述的短信验证码攻击防护方法,其特征在于,所述根据所述登录操作信息和登录地址信息,获得在预设时间周期内向所述目标用户已发送的短信验证码次数,包括:

判断所述登录操作信息是否包含有目标用户的未登陆状态标识和用户行为信息,若是,则根据所述用户行为信息,判断所述目标用户是否为真实用户;

若所述目标用户为真实用户,则根据所述登录地址信息,获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

4.根据权利要求3所述的短信验证码攻击防护方法,其特征在于,所述根据所述用户行为信息,判断所述目标用户是否为真实用户,包括:

根据所述用户行为信息和预设的用户分类模型,确定所述目标用户是否为真实用户;

其中,所述预设的用户分类模型是基于批量历史用户行为信息及其各自对应的标签对分类算法进行训练得到的,所述标签包括:真实用户标签和非真实用户标签。

5.根据权利要求1所述的短信验证码攻击防护方法,其特征在于,在所述接收目标用户的获取短信验证码请求之前,还包括:

接收目标用户的滑块验证请求;

根据所述滑块验证请求,确定通过所述目标用户的滑块验证。

6.根据权利要求1所述的短信验证码攻击防护方法,其特征在于,还包括:

若所述已发送的短信验证码次数未超出短信验证码次数阈值,则向所述目标用户的移动通信设备发送短信验证码。

7.一种短信验证码攻击防护装置,其特征在于,包括:

接收模块,用于接收目标用户的获取短信验证码请求,该获取短信验证码请求包括:所述目标用户的登录操作信息和登录地址信息;

获得模块,用于根据所述登录操作信息和登录地址信息,获得在预设时间周期内向所述目标用户已发送的短信验证码次数;

判断模块,用于判断所述已发送的短信验证码次数是否超出短信验证码次数阈值,若是,则拒绝所述获取短信验证码请求,完成所述获取短信验证码请求对应的短信验证码攻

击防护。

8.根据权利要求7所述的短信验证码攻击防护装置，其特征在于，所述获得模块包括：

第一获得单元，用于判断所述登录操作信息是否包含有目标用户的已登陆状态标识和用户唯一标识，若是，则根据所述用户唯一标识，获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

9.根据权利要求7所述的短信验证码攻击防护装置，其特征在于，所述获得模块包括：

判断单元，用于判断所述登录操作信息是否包含有目标用户的未登陆状态标识和用户行为信息，若是，则根据所述用户行为信息，判断所述目标用户是否为真实用户；

第二获得单元，用于若所述目标用户为真实用户，则根据所述登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

10.根据权利要求9所述的短信验证码攻击防护装置，其特征在于，所述判断单元包括：

分类子单元，用于根据所述用户行为信息和预设的用户分类模型，确定所述目标用户是否为真实用户；

其中，所述预设的用户分类模型是基于批量历史用户行为信息及其各自对应的标签对分类算法进行训练得到的，所述标签包括：真实用户标签和非真实用户标签。

11.一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求1至6任一项所述的短信验证码攻击防护方法。

12.一种计算机可读存储介质，其特征在于，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权利要求1至6任一项所述的短信验证码攻击防护方法。

13.一种计算机程序产品，其特征在于，所述计算机程序产品包括计算机程序，所述计算机程序被处理器执行时实现权利要求1至6任一项所述的短信验证码攻击防护方法。

# 短信验证码攻击防护方法及装置

## 技术领域

[0001] 本申请涉及数据处理技术领域，尤其涉及一种短信验证码攻击防护方法及装置。

## 背景技术

[0002] 本部分旨在为权利要求书中陈述的本发明实施例提供背景或上下文。此处的描述不因为包括在本部分中就承认是现有技术。

[0003] 随着网上银行在全球的发展和推广，网上银行服务于越来越多的客户；网上银行有很多场景需要向客户发送短信验证码或者短信通知来提升安全性；网上银行服务具有大规模群发短信的能力，若这种能力不能被有效保护就有可能被恶意使用。比如，攻击者利用网上银行恶意向指定的手机号发送大量垃圾短信，进行短信炸弹攻击。

[0004] 目前，通常通过图形验证码防止短信验证码攻击；网上银行在发送短信验证码之前需要用户提交图形验证码，用来防止机器人大量调用发送短信的接口。

[0005] 但是，通过图形验证码进行短信验证码攻击防护仍存在一些问题：只是在发送短信触发场景防护，没有收信人短信炸弹的控制；只是防止机器人攻击，如果大量客户同时进行人工攻击还是无法防范，存在可靠性较低的问题。

## 发明内容

[0006] 针对现有技术中的问题，本申请提出了一种短信验证码攻击防护方法及装置，能够避免短信炸弹问题，能够提高短信验证码攻击防护的准确性，进而能够提升用户体验。

[0007] 为了解决上述技术问题，本申请提供以下技术方案：

[0008] 第一方面，本申请提供一种短信验证码攻击防护方法，包括：

[0009] 接收目标用户的获取短信验证码请求，该获取短信验证码请求包括：所述目标用户的登录操作信息和登录地址信息；

[0010] 根据所述登录操作信息和登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数；

[0011] 判断所述已发送的短信验证码次数是否超出短信验证码次数阈值，若是，则拒绝所述获取短信验证码请求，完成所述获取短信验证码请求对应的短信验证码攻击防护。

[0012] 进一步地，所述根据所述登录操作信息和登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数，包括：

[0013] 判断所述登录操作信息是否包含有目标用户的已登陆状态标识和用户唯一标识，若是，则根据所述用户唯一标识，获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

[0014] 进一步地，所述根据所述登录操作信息和登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数，包括：

[0015] 判断所述登录操作信息是否包含有目标用户的未登陆状态标识和用户行为信息，若是，则根据所述用户行为信息，判断所述目标用户是否为真实用户；

[0016] 若所述目标用户为真实用户，则根据所述登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

[0017] 进一步地，所述根据所述用户行为信息，判断所述目标用户是否为真实用户，包括：

[0018] 根据所述用户行为信息和预设的用户分类模型，确定所述目标用户是否为真实用户；

[0019] 其中，所述预设的用户分类模型是基于批量历史用户行为信息及其各自对应的标签对分类算法进行训练得到的，所述标签包括：真实用户标签和非真实用户标签。

[0020] 进一步地，在所述接收目标用户的获取短信验证码请求之前，还包括：

[0021] 接收目标用户的滑块验证请求；

[0022] 根据所述滑块验证请求，确定通过所述目标用户的滑块验证。

[0023] 进一步地，所述的短信验证码攻击防护方法，还包括：

[0024] 若所述已发送的短信验证码次数未超出短信验证码次数阈值，则向所述目标用户的移动通信设备发送短信验证码。

[0025] 第二方面，本申请提供一种短信验证码攻击防护装置，包括：

[0026] 接收模块，用于接收目标用户的获取短信验证码请求，该获取短信验证码请求包括：所述目标用户的登录操作信息和登录地址信息；

[0027] 获得模块，用于根据所述登录操作信息和登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数；

[0028] 判断模块，用于判断所述已发送的短信验证码次数是否超出短信验证码次数阈值，若是，则拒绝所述获取短信验证码请求，完成所述获取短信验证码请求对应的短信验证码攻击防护。

[0029] 进一步地，所述获得模块包括：

[0030] 第一获得单元，用于判断所述登录操作信息是否包含有目标用户的已登陆状态标识和用户唯一标识，若是，则根据所述用户唯一标识，获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

[0031] 进一步地，所述获得模块包括：

[0032] 判断单元，用于判断所述登录操作信息是否包含有目标用户的未登陆状态标识和用户行为信息，若是，则根据所述用户行为信息，判断所述目标用户是否为真实用户；

[0033] 第二获得单元，用于若所述目标用户为真实用户，则根据所述登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

[0034] 进一步地，所述判断单元包括：

[0035] 分类子单元，用于根据所述用户行为信息和预设的用户分类模型，确定所述目标用户是否为真实用户；

[0036] 其中，所述预设的用户分类模型是基于批量历史用户行为信息及其各自对应的标签对分类算法进行训练得到的，所述标签包括：真实用户标签和非真实用户标签。

[0037] 第三方面，本申请提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在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所述的短信验证码攻击防护方法。

[0038] 第四方面，本申请提供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所述的短信验证码攻击防护方法。

[0039] 第五方面，本申请提供一种计算机程序产品，所述计算机程序产品包括计算机程序，所述计算机程序被处理器执行时实现所述的短信验证码攻击防护方法。

[0040] 由上述技术方案可知，本申请提供一种短信验证码攻击防护方法及装置。其中，该方法包括：接收目标用户的获取短信验证码请求，该获取短信验证码请求包括：所述目标用户的登录操作信息和登录地址信息；根据所述登录操作信息和登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数；判断所述已发送的短信验证码次数是否超出短信验证码次数阈值，若是，则拒绝所述获取短信验证码请求，完成所述获取短信验证码请求对应的短信验证码攻击防护，能够避免短信炸弹问题，能够提高短信验证码攻击防护的准确性，进而能够提升用户体验；具体地，能够在保证正常的发送短信能力的同时防范短信炸弹，能够保证不同场景下的发送短信功能，为客户提供安全、可用的短信服务，提升客户体验；利用服务端记录发送短信次数，提供更加严密的防范短信炸弹能力。

## 附图说明

[0041] 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的前提下，还可以根据这些附图获得其他的附图。

[0042] 图1是本申请实施例中的短信验证码攻击防护方法的第一流程示意图；

[0043] 图2是本申请实施例中的短信验证码攻击防护方法的第二流程示意图；

[0044] 图3是本申请实施例中的短信验证码攻击防护方法的第三流程示意图；

[0045] 图4是本申请实施例中的短信验证码攻击防护方法的第四流程示意图；

[0046] 图5是本申请实施例中短信验证码攻击防护装置的结构示意图。

## 具体实施方式

[0047] 为了使本技术领域的人员更好地理解本说明书中的技术方案，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，都属于本申请保护的范围。

[0048] 为了便于对本方案的理解，下面对与本方案相关的技术内容进行说明。

[0049] 短信炸弹：利用互联网服务发送不断向一手机号发送重复的垃圾短信，以达到骚扰和恶搞的效果。

[0050] 网银：网上银行又称网络银行、在线银行或电子银行，是各银行在互联网中设立的虚拟柜台，银行利用网络技术，通过互联网向客户提供查询、对账、转账、支付、信贷、理财等服务，使客户在网络条件具备的情况下随时随地享受银行服务。

[0051] 需要说明的是，本申请公开的短信验证码攻击防护方法及装置可用于金融技术领域，也可用于除金融技术领域之外的任意领域，本申请公开的短信验证码攻击防护方法及

装置的应用领域不做限定。本申请技术方案中对数据的获取、存储、使用、处理等均符合国家法律法规的相关规定。

[0052] 具体通过下述各个实施例进行说明。

[0053] 为了避免短信炸弹问题，提高短信验证码攻击防护的准确性，进而提升用户体验，本实施例提供一种执行主体是短信验证码攻击防护装置的短信验证码攻击防护方法，该短信验证码攻击防护装置包括但不限于服务器，如图1所示，该方法具体包含有如下内容：

[0054] 步骤101：接收目标用户的获取短信验证码请求，该获取短信验证码请求包括：所述目标用户的登录操作信息和登录地址信息。

[0055] 具体地，可以接收目标用户在前端发送的获取短信验证码请求；当所述目标用户处于登录状态时，所述登录操作信息可以包含有：已登陆状态标识和用户唯一标识；当所述目标用户处于离线状态时，所述登录操作信息可以包含有：未登陆状态标识和用户行为信息；可以用“0”表示已登陆状态标识，“1”表示未登陆状态标识；所述用户唯一标识用于区分不同的用户，可以是由数字和字母组成的字符串，如，账号或手机号等；所述登录地址信息可以是IP地址。

[0056] 步骤102：根据所述登录操作信息和登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

[0057] 具体地，所述预设时间周期可以根据实际需要进行设置，本申请对此不作限制，如，30秒或1分钟等。

[0058] 步骤103：判断所述已发送的短信验证码次数是否超出短信验证码次数阈值，若是，则拒绝所述获取短信验证码请求，完成所述获取短信验证码请求对应的短信验证码攻击防护。

[0059] 具体地，若所述已发送的短信验证码次数超出短信验证码次数阈值，则中止当前操作，完成所述获取短信验证码请求对应的短信验证码攻击防护；还可以输出所述获取短信验证码请求对应的报警信息。

[0060] 为了实现登录状态时的短信验证码攻击防护，提高短信验证码攻击防护的准确性，参见图2，在本申请一个实施例中，步骤102包括：

[0061] 步骤201：判断所述登录操作信息是否包含有目标用户的已登陆状态标识和用户唯一标识，若是，则根据所述用户唯一标识，获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

[0062] 具体地，可以利用服务端即上述短信验证码攻击防护装置缓存目标用户的用户唯一标识及其对应的在预设时间周期内的已发送的短信验证码次数；从短信验证码攻击防护装置缓存中，获得所述用户唯一标识对应的预设时间周期内的已发送的短信验证码次数，确定为在预设时间周期内向所述目标用户已发送的短信验证码次数。进一步地，若所述已发送的短信验证码次数未超出短信验证码次数阈值，则向所述目标用户的移动通信设备发送短信验证码，短信验证码发送成功之后，可以判断当前系统时间是否刚好完成一次预设时间周期，若是，则可以将缓存中在预设时间周期内所述用户唯一标识对应的已发送的短信验证码次数重置为1，否则，可以将缓存中在预设时间周期内所述用户唯一标识对应的已发送的短信验证码次数加1。

[0063] 也就是说，在目标用户登录网银之后发送短信验证码的场景中，可以利用服务端

缓存记录向目标用户的发送短信次数并加以控制。

[0064] 为了实现未登录状态时的短信验证码攻击防护，提高短信验证码攻击防护的准确性，参见图3，在本申请一个实施例中，步骤102包括：

[0065] 步骤301：判断所述登录操作信息是否包含有目标用户的未登陆状态标识和用户行为信息，若是，则根据所述用户行为信息，判断所述目标用户是否为真实用户。

[0066] 具体地，所述用户行为信息可以包括：鼠标移动轨迹、鼠标移动速度、屏幕分辨率和屏幕颜色深度等。

[0067] 步骤302：若所述目标用户为真实用户，则根据所述登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

[0068] 具体地，由于此时目标用户处于未登陆状态，服务端未缓存用户唯一标识及其对应的预设时间周期内的已发送的短信验证码次数，可以利用登录地址信息作为关键要素通过数据库记录预设时间周期内所述登录地址信息对应的已发送的短信验证码次数；可以从数据库中获得所述登录地址信息对应的在预设时间周期内的已发送的短信验证码次数，确定为在预设时间周期内的向所述目标用户已发送的短信验证码次数。进一步地，若所述已发送的短信验证码次数未超出短信验证码次数阈值，则向所述目标用户的移动通信设备发送短信验证码，短信验证码发送成功之后，可以当前系统时间是否刚好已完成一次预设时间周期，若是，则可以将数据库中在预设时间周期内所述登录地址信息对应的已发送的短信验证码次数重置为1，否则，可以将数据库中在预设时间周期内所述登录地址信息对应的已发送的短信验证码次数加1。

[0069] 也就是说，在客户未登录网银时发送短信验证码的场景中，服务端没有缓存信息控制，可以利用目标用户的IP信息等作为关键要素通过数据库记录目标用户处于未登录状态时发送短信的次数并加以控制；可以不关注是哪些客户触发发送短信信息的动作，仅关注向收信人发送短信的次数并加以控制。

[0070] 为了进一步提高短信验证码攻击防护的准确性和智能化程度，在本申请一个实施例中，步骤301中所述的根据所述用户行为信息，判断所述目标用户是否为真实用户，包括：

[0071] 步骤401：根据所述用户行为信息和预设的用户分类模型，确定所述目标用户是否为真实用户；其中，所述预设的用户分类模型是基于批量历史用户行为信息及其各自对应的标签对分类算法进行训练得到的，所述标签包括：真实用户标签和非真实用户标签。

[0072] 具体地，所述分类算法可以是决策树算法和KNN算法等；可以将所述用户行为信息输入预设的用户分类模型，根据所述预设的用户分类模型的输出结果确定目标用户是否为真实用户。

[0073] 为了进一步提高短信验证码攻击防护的准确性，参见图4，在本申请一个实施例中，步骤101之前还包括：

[0074] 步骤501：接收目标用户的滑块验证请求。

[0075] 步骤502：根据所述滑块验证请求，确定通过所述目标用户的滑块验证。

[0076] 具体地，在本实施例中，在目标用户手工完成滑块验证之后才能够向目标用户的移动通信设备发送短信验证码；也就是说，在向目标用户指定手机号发送短信验证码的场景中，在发送短信验证码之前需要用户提交滑块验证，用来防止机器人大量调用发送短信的接口。

[0077] 为了进一步说明本方案,本申请提供一种短信验证码攻击防护方法的应用实例,具体包含有:

[0078] 步骤1:获取客户指定手机号。

[0079] 步骤2:提供滑块验证,保证客户必须手工完成滑块验证后才能向手机号发送短信。

[0080] 步骤3:在客户处于登录状态时,控制客户发送短信的频度。

[0081] 具体地,可以设立登录状态缓存机制,在服务端缓存设置计数器,用于控制客户发送短信的频度;可以设立收信人控制机制,服务端按照收信人设置计数器,用于控制收信人接收短信的频度。

[0082] 步骤4:在客户处于登录状态时,通过服务端缓存记录向客户发送短信的次数,并控制向客户发送短信的频度。

[0083] 步骤5:利用数据库控制在无登录状态下向客户发送短信的频度;即通过识别客户在无登录状态下的关键要素,并以此在数据库记录发送短信的次数,控制向客户发送短信的频度。

[0084] 具体地,可以设立无登录状态数据库记录机制,利用客户IP等关键要素来识别真实的服务场景,并利用数据库记录开控制向客户发送短信的频度。

[0085] 步骤6:在服务端控制收信人接收短信的频度;即记录收信人接收短信的次数,控制接收短信的频度。

[0086] 步骤7:根据客户发送短信的频度,向客户指定手机号发送短信验证码。

[0087] 由上述描述可知,本应用实例提供的短信验证码攻击防护方法,能够在发送触发、登录状态发送、无登录状态发送、收信人控制环节进行频度控制,解决短信炸弹的问题,提高防范短信炸弹能力,实现更为复杂的场景要求;在满足客户正常使用的同时更大限度的保护收信人。

[0088] 为了避免短信炸弹问题,提高短信验证码攻击防护的准确性,进而提升用户体验,本申请提供一种用于实现所述短信验证码攻击防护方法中全部或部分内容的短信验证码攻击防护装置的实施例,参见图5,所述短信验证码攻击防护装置具体包含有如下内容:

[0089] 接收模块10,用于接收目标用户的获取短信验证码请求,该获取短信验证码请求包括:所述目标用户的登录操作信息和登录地址信息;

[0090] 获得模块20,用于根据所述登录操作信息和登录地址信息,获得在预设时间周期内向所述目标用户已发送的短信验证码次数;

[0091] 判断模块30,用于判断所述已发送的短信验证码次数是否超出短信验证码次数阈值,若是,则拒绝所述获取短信验证码请求,完成所述获取短信验证码请求对应的短信验证码攻击防护。

[0092] 在本申请一个实施例中,所述获得模块包括:

[0093] 第一获得单元,用于判断所述登录操作信息是否包含有目标用户的已登陆状态标识和用户唯一标识,若是,则根据所述用户唯一标识,获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

[0094] 在本申请一个实施例中,所述获得模块包括:

[0095] 判断单元,用于判断所述登录操作信息是否包含有目标用户的未登陆状态标识和

用户行为信息，若是，则根据所述用户行为信息，判断所述目标用户是否为真实用户；

[0096] 第二获得单元，用于若所述目标用户为真实用户，则根据所述登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数。

[0097] 在本申请一个实施例中，所述判断单元包括：

[0098] 分类子单元，用于根据所述用户行为信息和预设的用户分类模型，确定所述目标用户是否为真实用户；其中，所述预设的用户分类模型是基于批量历史用户行为信息及其各自对应的标签对分类算法进行训练得到的，所述标签包括：真实用户标签和非真实用户标签。

[0099] 本说明书提供的短信验证码攻击防护装置的实施例具体可以用于执行上述短信验证码攻击防护方法的实施例的处理流程，其功能在此不再赘述，可以参照上述短信验证码攻击防护方法实施例的详细描述。

[0100] 本发明实施例还提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在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上述短信验证码攻击防护方法。

[0101] 本发明实施例还提供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上述短信验证码攻击防护方法。

[0102] 本发明实施例还提供一种计算机程序产品，所述计算机程序产品包括计算机程序，所述计算机程序被处理器执行时实现上述短信验证码攻击防护方法。

[0103] 由上述描述可知，本申请提供的短信验证码攻击防护方法及装置，能够避免短信炸弹问题，能够提高短信验证码攻击防护的准确性，进而能够提升用户体验；具体地，能够在保证正常的发送短信能力的同时防范短信炸弹，能够保证不同场景下的发送短信功能，为客户提供安全、可用的短信服务。

[0104] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明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，本发明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。

[0105] 本发明是参照根据本发明实施例的方法、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。

[0106] 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。

[0107] 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。

[0108] 以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限定本发明的保护范围，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

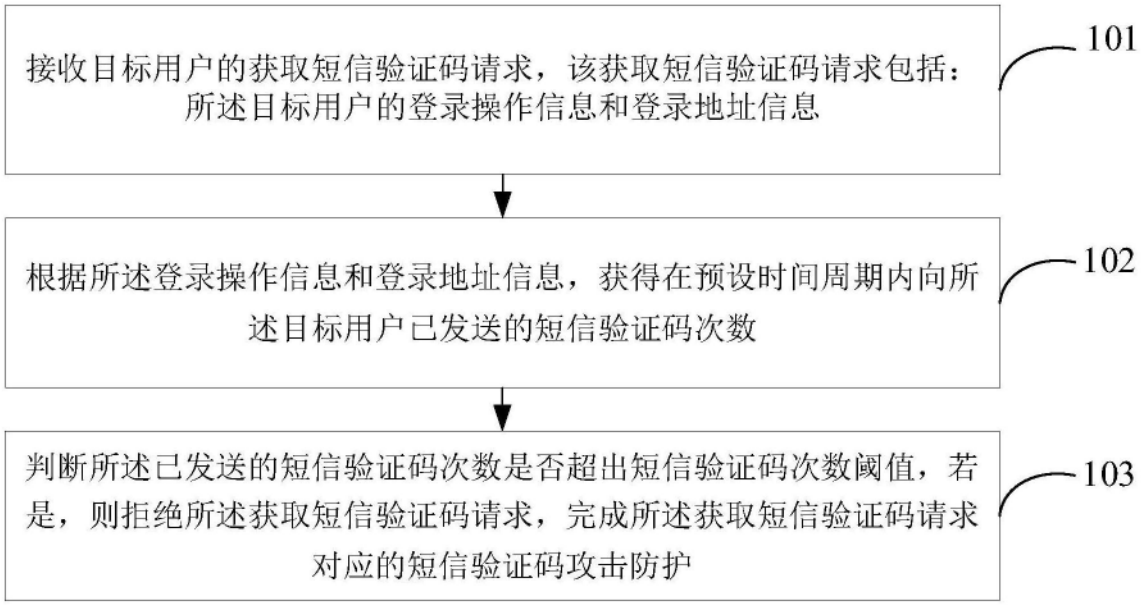
接收目标用户的获取短信验证码请求，该获取短信验证码请求包括：所述目标用户的登录操作信息和登录地址信息
101
根据所述登录操作信息和登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数
102
判断所述已发送的短信验证码次数是否超出短信验证码次数阈值，若是，则拒绝所述获取短信验证码请求，完成所述获取短信验证码请求对应的短信验证码攻击防护
103

图1

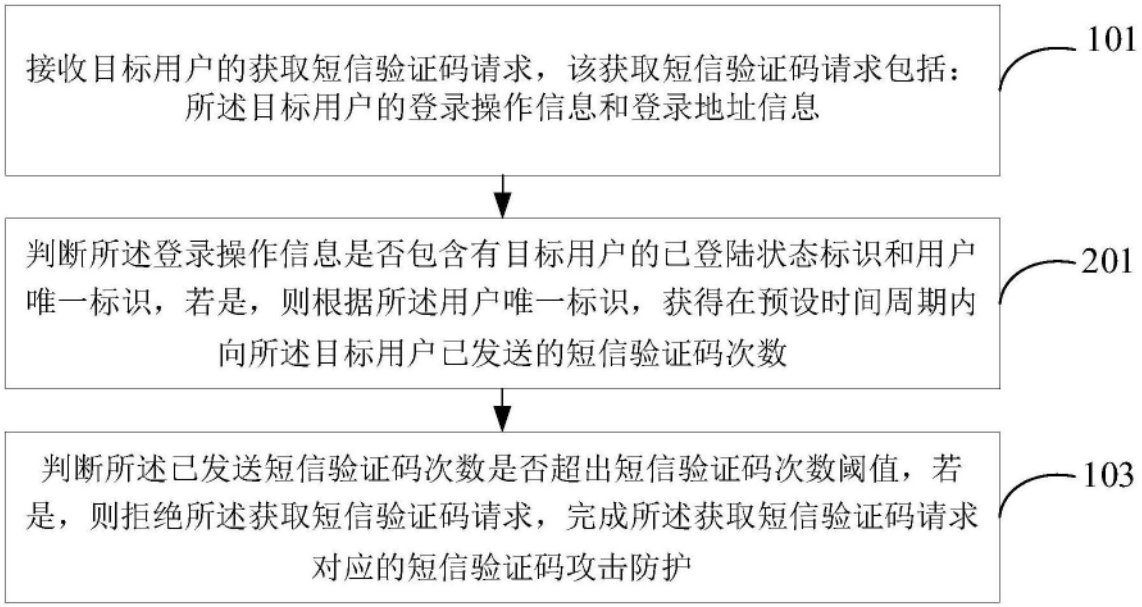
接收目标用户的获取短信验证码请求，该获取短信验证码请求包括：所述目标用户的登录操作信息和登录地址信息
101
判断所述登录操作信息是否包含有目标用户的已登陆状态标识和用户唯一标识，若是，则根据所述用户唯一标识，获得在预设时间周期内向所述目标用户已发送的短信验证码次数
201
判断所述已发送短信验证码次数是否超出短信验证码次数阈值，若是，则拒绝所述获取短信验证码请求，完成所述获取短信验证码请求对应的短信验证码攻击防护
103

图2

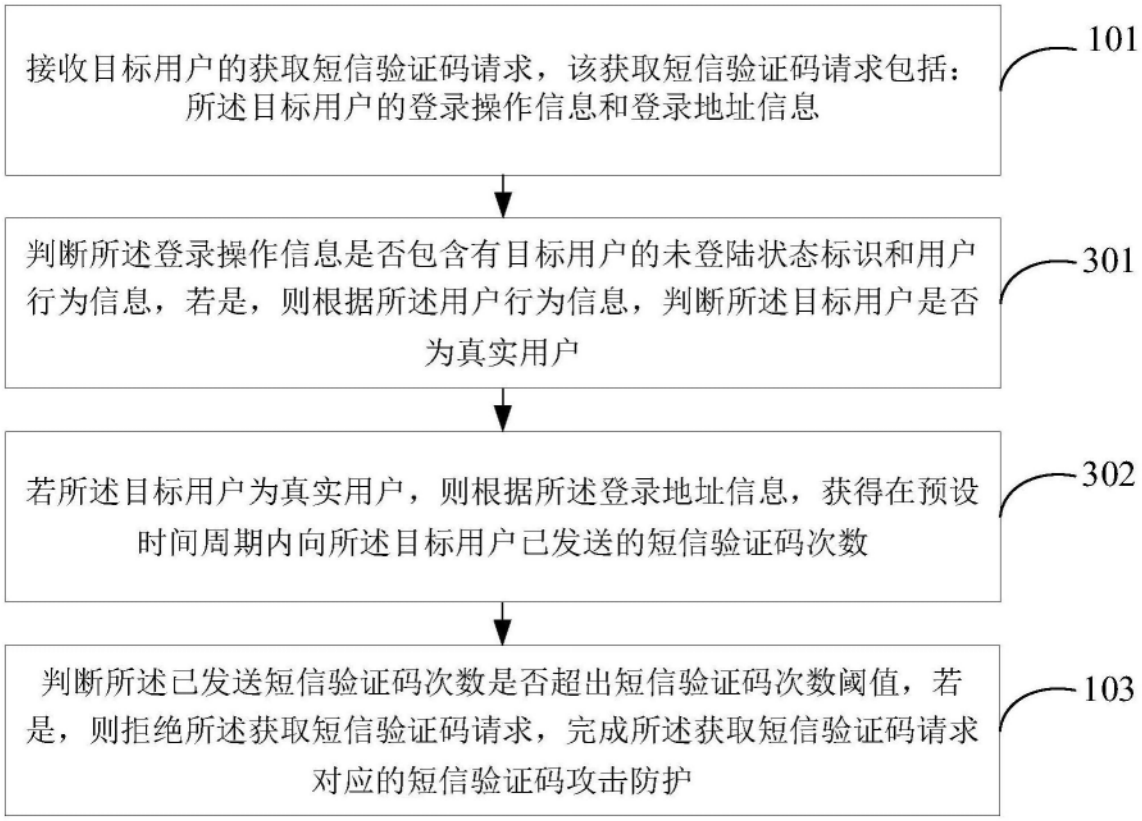
接收目标用户的获取短信验证码请求，该获取短信验证码请求包括：所述目标用户的登录操作信息和登录地址信息
101
判断所述登录操作信息是否包含有目标用户的未登陆状态标识和用户行为信息，若是，则根据所述用户行为信息，判断所述目标用户是否为真实用户
301
若所述目标用户为真实用户，则根据所述登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数
302
判断所述已发送短信验证码次数是否超出短信验证码次数阈值，若是，则拒绝所述获取短信验证码请求，完成所述获取短信验证码请求对应的短信验证码攻击防护
103

图3

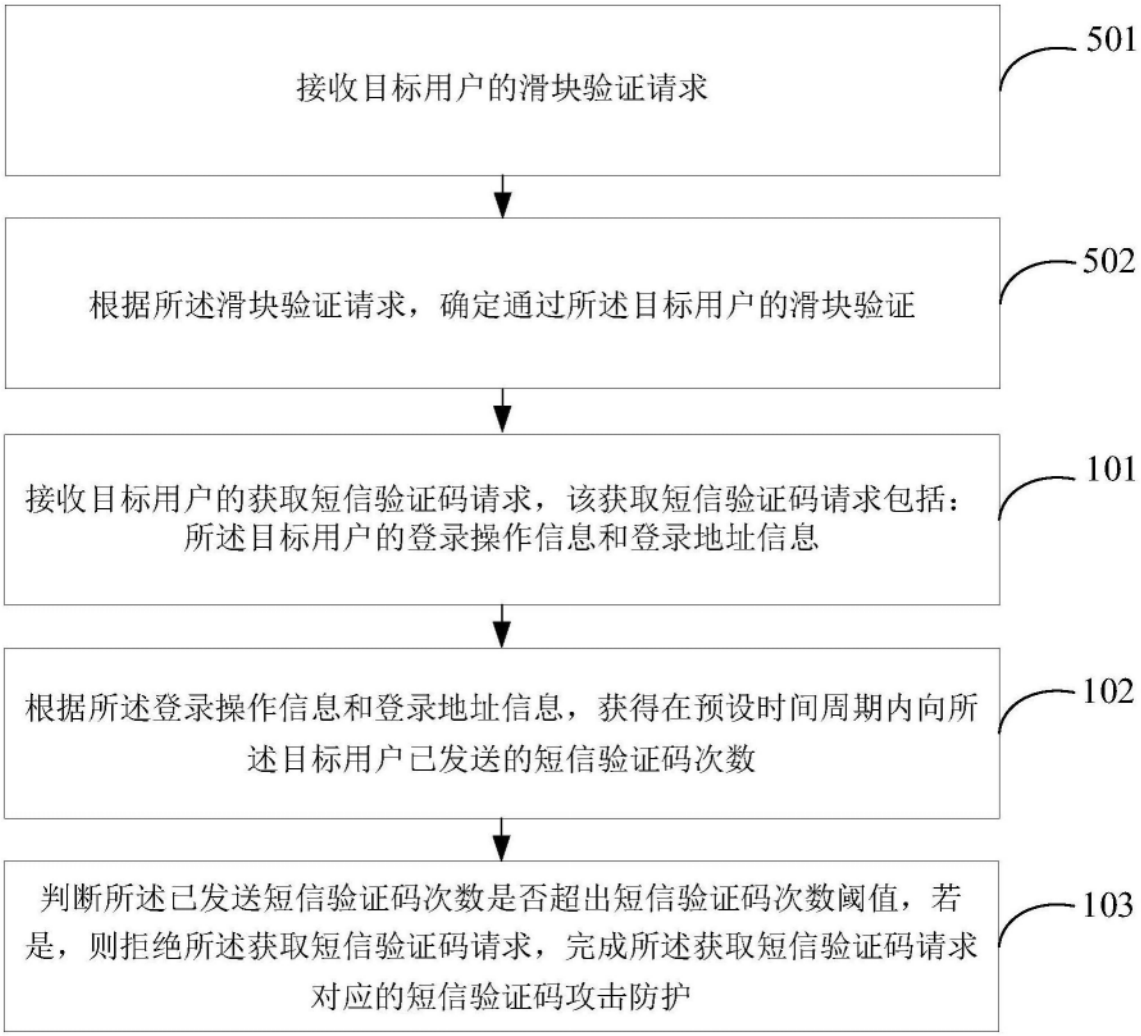
接收目标用户的滑块验证请求
501
根据所述滑块验证请求，确定通过所述目标用户的滑块验证
502
接收目标用户的获取短信验证码请求，该获取短信验证码请求包括：所述目标用户的登录操作信息和登录地址信息
101
根据所述登录操作信息和登录地址信息，获得在预设时间周期内向所述目标用户已发送的短信验证码次数
102
判断所述已发送短信验证码次数是否超出短信验证码次数阈值，若是，则拒绝所述获取短信验证码请求，完成所述获取短信验证码请求对应的短信验证码攻击防护
103

图4

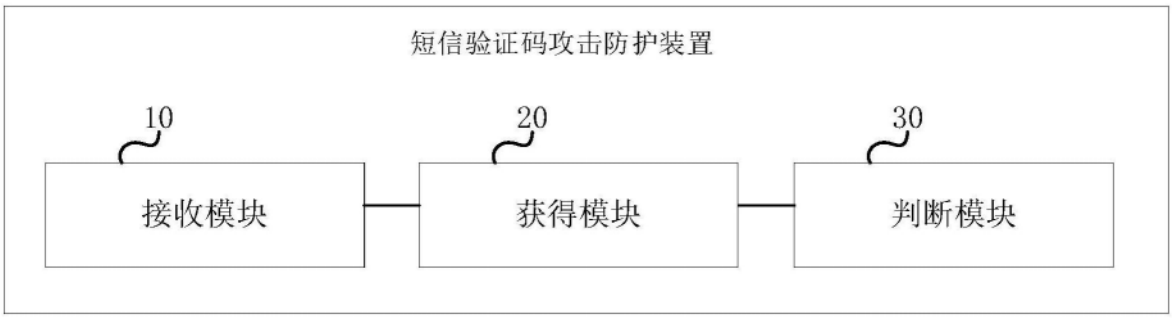
短信验证码攻击防护装置
10
20
30
接收模块
获得模块
判断模块

图5