



(12) 发明专利申请

(10) 申请公布号 CN 113065748 A

(43) 申请公布日 2021.07.02

(21) 申请号 202110276380.1

(22) 申请日 2021.03.15

(71) 申请人 中国平安财产保险股份有限公司
地址 518000 广东省深圳市福田区益田路
5033号平安金融中心12、13、38、39、40
层

(72) 发明人 唐炳武 杨超

(74) 专利代理机构 深圳市力道知识产权代理事
务所(普通合伙) 44507
代理人 贺小旺

(51) Int. Cl.
G06Q 10/06 (2012.01)
G06K 9/62 (2006.01)
G06N 7/00 (2006.01)
H04L 29/06 (2006.01)

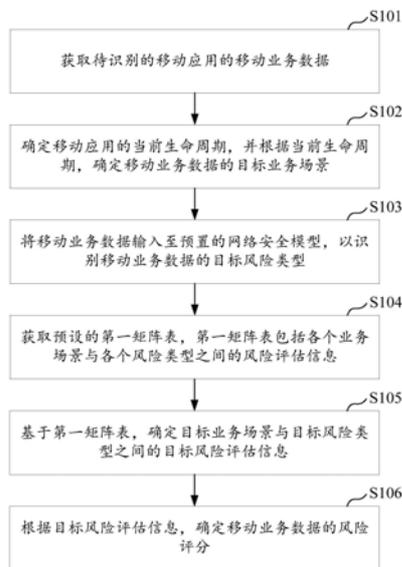
权利要求书2页 说明书12页 附图4页

(54) 发明名称

业务风险评估方法、装置、设备及存储介质

(57) 摘要

本申请涉及数据处理的技术领域,提供一种业务风险评估方法、装置、设备及存储介质,该方法包括:获取待识别的移动应用的移动业务数据;确定移动应用的当前生命周期,并根据当前生命周期,确定移动业务数据的目标业务场景;将移动业务数据输入至预置的网络安全模型,以识别移动业务数据的目标风险类型;获取预设的第一矩阵表,第一矩阵表包括各个业务场景与各个风险类型之间的风险评估信息;基于第一矩阵表,确定目标业务场景与目标风险类型之间的目标风险评估信息;根据目标风险评估信息,确定移动业务数据的风险评分。本申请涉及人工智能,能够提高移动业务的业务风险评估的灵活性和可靠性。



1. 一种业务风险评估方法,其特征在于,包括:
 - 获取待识别的移动应用的移动业务数据;
 - 确定所述移动应用的当前生命周期,并根据所述当前生命周期,确定所述移动业务数据的目标业务场景;
 - 将所述移动业务数据输入至预置的网络安全模型,以识别所述移动业务数据的目标风险类型;
 - 获取预设的第一矩阵表,所述第一矩阵表包括各个业务场景与各个风险类型之间的风险评估信息;
 - 基于所述第一矩阵表,确定所述目标业务场景与所述目标风险类型之间的目标风险评估信息;
 - 根据所述目标风险评估信息,确定所述移动业务数据的风险评分。
2. 如权利要求1所述的业务风险评估方法,其特征在于,所述根据所述当前生命周期,确定所述移动业务数据的目标业务场景,包括:
 - 获取生命周期与业务场景之间的映射关系表,根据所述映射关系表和当前生命周期,确定所述移动业务数据的目标业务场景;或者
 - 确定所述移动应用的当前活动场景,并根据所述当前生命周期和所述当前活动场景,确定所述移动业务数据的目标业务场景。
3. 如权利要求2所述的业务风险评估方法,其特征在于,所述根据所述当前生命周期和所述当前活动场景,确定所述移动业务数据的目标业务场景,包括:
 - 获取预设的第二矩阵表,所述第二矩阵表包括各个生命周期与各个活动场景之间的业务场景;
 - 基于所述第二矩阵表,确定所述当前生命周期和所述当前活动场景之间的目标业务场景。
4. 如权利要求2或3中任一项所述的业务风险评估方法,其特征在于,所述当前生命周期包括投融资期、用户增长期、活动获利期、业务维持期和业务扩张期,所述当前活动场景包括邀请注册、签到抽奖、优惠满减和红包抵扣。
5. 如权利要求1-3中任一项所述的业务风险评估方法,其特征在于,所述基于所述第一矩阵表,确定所述目标业务场景与所述目标风险类型之间的目标风险评估信息,包括:
 - 通过所述第一矩阵表,确定所述目标业务场景对应的多个风险评估信息;
 - 从所述目标业务场景对应的多个风险评估信息中选取与所述目标风险类型对应的目标风险评估信息;
 - 其中,所述目标风险评估信息包括风险评估权重、风险评估分值和风险评估等级。
6. 如权利要求5所述的业务风险评估方法,其特征在于,所述根据所述目标风险评估信息,确定所述移动业务数据的风险评分,包括:
 - 当所述目标风险评估信息包括多个风险评估权重时,获取风险评估的预设总分值;
 - 计算所述预设总分值与多个风险评估权重之间的乘积之和,得到所述移动业务数据的风险评分;或
 - 当所述目标风险评估信息包括多个风险评估分值时,计算所述多个风险评估分值之和,得到所述移动业务数据的风险评分;或

当所述目标风险评估信息包括多个风险评估等级时,获取各个风险评估等级对应的多个分值;

从所述各个风险评估等级对应的多个分值中确定所述多个风险评估等级对应的目标分值,并选取最高的目标分值作为所述移动业务数据的风险评分。

7.如权利要求1-3中任一项所述的业务风险评估方法,其特征在于,所述根据所述目标风险评估信息,确定所述移动业务数据的风险评分之后,还包括:

获取预设的第三矩阵表,所述第三矩阵表包括各个业务场景与各个风险处置信息之间的风险评分;

基于所述第三矩阵表,确定与所述移动业务数据的风险评分以及目标业务场景相对应的目标风险处置信息;

确定所述移动业务数据对应的账号信息,并按照所述目标风险处置信息对所述账号信息进行处置。

8.一种业务风险评估装置,其特征在于,所述业务风险评估装置包括:

获取模块,用于获取待识别的移动应用的移动业务数据;

确定模块,用于确定所述移动应用的当前生命周期,并根据所述当前生命周期,确定所述移动业务数据的目标业务场景;

识别模块,用于将所述移动业务数据输入至预置的网络安全模型,以识别所述移动业务数据的目标风险类型;

获取模块,还用于获取预设的第一矩阵表,所述第一矩阵表包括各个业务场景与各个风险类型之间的风险评估信息;

评估模块,用于基于所述第一矩阵表,确定所述目标业务场景与所述目标风险类型之间的目标风险评估信息;

评分模块,用于根据所述目标风险评估信息,确定所述移动业务数据的风险评分。

9.一种计算机设备,其特征在于,所述计算机设备包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的计算机程序,其中所述计算机程序被所述处理器执行时,实现如权利要求1至7中任一项所述的业务风险评估方法的步骤。

10.一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上存储有计算机程序,其中所述计算机程序被处理器执行时,实现如权利要求1至7中任一项所述的业务风险评估方法的步骤。

业务风险评估方法、装置、设备及存储介质

技术领域

[0001] 本申请涉及数据处理的技术领域,尤其涉及一种业务风险评估方法、装置、设备及存储介质。

背景技术

[0002] 业务安全是指保护业务系统免受安全威胁的措施或手段。目前,随着O2O和P2P等模式的飞速发展,各个行业的兴起都势必经历初期的野蛮生长、商业模式的盲目复制以及近乎疯狂的补贴大战,容易导致业务系统出现安全漏洞。特别是对于移动业务安全,移动业务安全相比传统网络安全要更加复杂,从移动应用的注册拉新到促销获利,在不同的生命周期阶段有不同的业务场景,不同的业务场景的安全目标也不一致,使得移动业务的安全管理和风险评估的复杂度高,且业内缺乏统一的解决方案,不能有效保障移动业务安全。

发明内容

[0003] 本申请的主要目的在于提供一种业务风险评估方法、装置、设备及存储介质,旨在提高移动业务的业务风险评估的灵活性和可靠性,保障移动业务安全。

[0004] 第一方面,本申请提供一种业务风险评估方法,包括:

[0005] 获取待识别的移动应用的移动业务数据;

[0006] 确定所述移动应用的当前生命周期,并根据所述当前生命周期,确定所述移动业务数据的目标业务场景;

[0007] 将所述移动业务数据输入至预置的网络安全模型,以识别所述移动业务数据的目标风险类型;

[0008] 获取预设的第一矩阵表,所述第一矩阵表包括各个业务场景与各个风险类型之间的风险评估信息;

[0009] 基于所述第一矩阵表,确定所述目标业务场景与所述目标风险类型之间的目标风险评估信息;

[0010] 根据所述目标风险评估信息,确定所述移动业务数据的风险评分。

[0011] 第二方面,本申请还提供一种业务风险评估装置,所述业务风险评估装置包括:

[0012] 获取模块,用于获取待识别的移动应用的移动业务数据;

[0013] 确定模块,用于确定所述移动应用的当前生命周期,并根据所述当前生命周期,确定所述移动业务数据的目标业务场景;

[0014] 识别模块,用于将所述移动业务数据输入至预置的网络安全模型,以识别所述移动业务数据的目标风险类型;

[0015] 获取模块,还用于获取预设的第一矩阵表,所述第一矩阵表包括各个业务场景与各个风险类型之间的风险评估信息;

[0016] 评估模块,用于基于所述第一矩阵表,确定所述目标业务场景与所述目标风险类型之间的目标风险评估信息;

[0017] 评分模块,用于根据所述目标风险评估信息,确定所述移动业务数据的风险评分。

[0018] 第三方面,本申请还提供一种计算机设备,所述计算机设备包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的计算机程序,其中所述计算机程序被所述处理器执行时,实现如上所述的业务风险评估方法的步骤。

[0019] 第四方面,本申请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上存储有计算机程序,其中所述计算机程序被处理器执行时,实现如上所述的业务风险评估方法的步骤。

[0020] 本申请提供一种业务风险评估方法、装置、设备及存储介质,本申请通过获取待识别的移动应用的移动业务数据;确定移动应用的当前生命周期,并根据当前生命周期,确定移动业务数据的目标业务场景;将移动业务数据输入至预置的网络安全模型,以识别移动业务数据的目标风险类型;获取预设的第一矩阵表,第一矩阵表包括各个业务场景与各个风险类型之间的风险评估信息;基于第一矩阵表,确定目标业务场景与目标风险类型之间的目标风险评估信息;根据目标风险评估信息,确定移动业务数据的风险评分。本申请实施例利用移动应用在不同的生命周期阶段有不同的业务场景的特性,灵活地对移动业务数据进行风险评估,能够有效确定移动业务数据的风险评估信息,提高移动业务的业务风险评估的针对性、灵活性和可靠性,有利于保障移动业务安全。

附图说明

[0021] 为了更清楚地说明本申请实施例技术方案,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。

[0022] 图1为本申请实施例提供的一种业务风险评估方法的步骤流程示意图;

[0023] 图2为图1中的业务风险评估方法的一子步骤流程示意图;

[0024] 图3为图1中的业务风险评估方法的又一子步骤流程示意图;

[0025] 图4为本申请实施例提供的一种业务风险评估装置的示意性框图;

[0026] 图5为图4中的业务风险评估装置的子模块的示意性框图;

[0027] 图6为本申请实施例提供的一种计算机设备的结构示意图。

[0028] 本申请目的的实现、功能特点及优点将结合实施例,参照附图做进一步说明。

具体实施方式

[0029] 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。

[0030] 附图中所示的流程图仅是示例说明,不是必须包括所有的内容和操作/步骤,也不是必须按所描述的顺序执行。例如,有的操作/步骤还可以分解、组合或部分合并,因此实际执行的顺序有可能根据实际情况改变。另外,虽然在装置示意图中进行了功能模块的划分,但是在某些情况下,可以以不同于装置示意图中的模块划分。

[0031] 本申请实施例提供一种业务风险评估方法、装置、设备及存储介质。其中,该业务

风险评估方法可应用于终端设备或服务器中,该终端设备可以为手机、平板电脑、笔记本电脑、台式电脑、个人数字助理和穿戴式设备等电子设备;该服务器可以为单台的服务器,也可以为由多台服务器组成的服务器集群。以下以该业务风险评估方法应用于服务器为例进行解释说明。

[0032] 下面结合附图,对本申请的一些实施方式作详细说明。在不冲突的情况下,下述的实施例及实施例中的特征可以相互组合。

[0033] 请参照图1,图1为本申请实施例提供的一种业务风险评估方法的步骤流程图。

[0034] 如图1所示,该业务风险评估方法包括步骤S101至步骤S106。

[0035] 步骤S101、获取待识别的移动应用的移动业务数据。

[0036] 移动业务安全主要是指移动业务方面的数据安全和数据泄漏问题。移动业务安全相比传统网络安全要更加复杂,从移动应用的注册拉新到促销获利,在不同的生命周期阶段有不同的业务场景,不同的业务场景的安全目标也不一致,使得移动业务的安全管理和风险评估的复杂度高,不能有效保障移动业务安全。

[0037] 例如移动APP在不同的生命周期,面对不同的风险类型时的业务安全目标不一致,对应的风险评估信息也不相同,风险评估信息包括风险评估权重、风险评估分值或者风险评估等级等。比如:在投融资期,业务可能允许虚假手机号注册,此时虚假手机号注册的风险评估信息对应的风险较低。在活动获利期,严禁第三方合作商欺诈作弊,此时欺诈作弊的风险评估信息对应的风险较高。基于此,本申请实施例利用移动应用在不同的生命周期阶段有不同的业务场景的特性,灵活地对移动业务数据进行风险评估,能够有效确定移动业务数据的风险评估信息,从而提高移动业务的业务风险评估的针对性、灵活性和可靠性,有利于保障移动业务安全。

[0038] 其中,移动业务数据包括移动应用(Mobile Application,MA)的业务数据,移动业务数据例如包括注册业务数据、登录业务数据、鉴权业务数据和/或活动防刷业务数据,等等。移动业务数据可以是http请求包,移动业务数据可以包括账号信息,账号信息例如为手机号、IP、用户名,通过对应的账号信息便于移动业务数据的安全管理和风险评估。

[0039] 在一实施例中,接收安装有移动应用的终端设备发送的移动业务数据,该终端设备发送的移动业务数据即为待识别的移动应用的移动业务数据。或者,通过云端数据库获取待识别的移动应用的移动业务数据,该云端数据库提供数据存储或者数据中转的功能,本申请实施例不做具体限定。

[0040] 步骤S102、确定移动应用的当前生命周期,并根据当前生命周期,确定移动业务数据的目标业务场景。

[0041] 移动应用可以包括多个生命周期,该生命周期是指移动应用在各个发展阶段的周期,移动应用的生命周期包括投融资期、用户增长期、活动获利期、业务维持期和业务扩张期等,目标业务场景可以根据移动应用的当前生命周期确定,例如,移动业务数据的当前生命周期即为移动应用的目标业务场景。通过移动业务数据在不同的生命周期阶段对应不同的业务场景的特性,有利于提高不同的业务场景下进行风险评估的针对性、灵活性和可靠性。

[0042] 在一实施例中,如图2所示,根据当前生命周期确定移动业务数据的目标业务场

景,包括:子步骤S1021至子步骤S1022。

[0043] 子步骤S1021、获取生命周期与业务场景之间的映射关系表。

[0044] 其中,生命周期与业务场景之间的映射关系表可以由用户根据实际情况灵活设置。业务场景是指移动应用业务所处的场景,不同业务场景下的风险评估信息不同。例如,映射关系表中投融资期与业务场景1对应,用户增长期与业务场景2对应,活动获利期与业务场景3对应、业务维持期与业务场景4对应和业务扩张期与业务场景5对应。

[0045] 子步骤S1022、根据映射关系表和当前生命周期,确定移动业务数据的目标业务场景。

[0046] 通过查找映射关系表,能够快速确定与当前生命周期对应的业务场景,得到移动业务数据的目标业务场景。例如,通过查找映射关系表能够快速确定与投融资期对应的业务场景1。需要说明的是,不同的业务场景下进行风险评估时,对应的风险评估信息不同,在不同风险类型下的风险评分也不相同,从而能够灵活地进行移动业务的业务风险评估。

[0047] 在一实施例中,如图3所示,根据当前生命周期确定移动业务数据的目标业务场景,包括:子步骤S1023至子步骤S1024。

[0048] 子步骤S1023、确定移动应用的当前活动场景。

[0049] 移动应用可以包括多个活动场景,当前活动场景是指移动应用业务正在进行的活动,当前活动场景包括但不限于邀请注册、签到抽奖、优惠满减和红包抵扣,可携带于移动业务数据中,即通过移动业务数据可以便捷地确定移动应用的当前活动场景。

[0050] 子步骤S1024、根据当前生命周期和当前活动场景,确定移动业务数据的目标业务场景。

[0051] 移动应用可以包括多个生命周期和多个活动场景,多个生命周期和多个活动场景可共同组成多个业务场景。其中,当前生命周期包括但不限于投融资期、用户增长期、活动获利期、业务维持期和业务扩张期,当前活动场景包括但不限于邀请注册、签到抽奖、优惠满减和红包抵扣。因此,业务场景信息包括生命周期-活动场景,例如业务场景信息为投融资期-签到抽奖。该当前生命周期和当前活动场景等相关信息可携带于移动业务数据中,即通过移动业务数据可以便捷地确定移动业务数据对应的目标业务场景。

[0052] 在一实施例中,获取预设的第二矩阵表,第二矩阵表包括各个生命周期与各个活动场景之间的业务场景;基于第二矩阵表,确定当前生命周期和当前活动场景之间的目标业务场景。需要说明的,第二矩阵表可以由用户根据实际情况灵活设置,通过查找第二矩阵表,能够快速确定当前生命周期和当前活动场景之间的目标业务场景。

[0053] 示例性的,第二矩阵表如表1所示:

[0054] 表1

生命周期 \ 活动场景	活动场景			
	邀请注册	签到抽奖	优惠满减	红包抵扣
[0055] 投融资期	业务场景 1		业务场景 8	
用户增长期	业务场景 2	业务场景 5	业务场景 9	
活动获利期	业务场景 3	业务场景 6	业务场景 10	业务场景 12
业务维持期	业务场景 4	业务场景 7	业务场景 11	业务场景 13

[0056] 步骤S103、将移动业务数据输入至预置的网络安全模型，以识别移动业务数据的目标风险类型。

[0057] 将移动业务数据输入至预置的网络安全模型，以对移动业务数据进行风险识别，得到移动业务数据的目标业务类型。其中，网络安全模型可以为一个或者多个，用于识别移动业务数据的目标业务类型。通过预置的网络安全模型能够快速准确地对输入的移动业务数据进行风险识别，得到移动业务数据的目标业务类型。

[0058] 在一实施例中，业务类型包括群控、脚本攻击、设备指纹篡改、物联网黑卡等，群控是指用群设备同时管理多个移动应用，例如同时管理多个手机进行APP操作，修改手机硬件信息，达到模拟人工使用APP的效果；脚本攻击是指用脚本操作移动应用，例如用脚本操作手机APP，利用APP漏洞从用户那里恶意盗取信息；设备指纹篡改是指通过移动应用的hook(钩子)伪造设备指纹，比如伪造领先设备的IMEI号；物联网黑卡是指运营商发给物联网厂商的通信卡，这种卡不能打电话但能收短信，黑客可能用这种卡注册移动应用MA。

[0059] 在一实施例中，网络安全模型包括动态贝叶斯网络模型(Dynamic Bayesian Network, DBN)。动态贝叶斯网络模型包括特征提取子层、风险识别子层和结果输出子层；通过预置的网络安全模型，对所述移动业务数据进行风险识别，以确定所述移动业务数据的目标业务类型包括：通过特征提取子层提取移动业务数据的特征信息；通过风险识别子层对特征信息进行分类识别，得到多个业务风险类型和各自对应的概率信息；通过结果输出子层根据多个概率信息从多个业务风险类型中选取目标业务风险类型，得到移动业务数据的目标业务类型。其中，特征提取子层用于提取移动业务数据的特征信息，风险识别子层用于对特征信息进行分类识别，结果输出子层用于选取并输出目标业务类型。通过动态贝叶斯网络模型的多层结构能够快速且准确地识别移动业务数据的目标业务类型。

[0060] 在一实施例中，网络安全模型为多个，每个网络安全模型用于识别一种业务类型。通过多个网络安全模型确定移动业务数据的目标业务类型。需要说明的是，通过多个存在标签信息的样本数据对网络安全模型进行训练，直至网络安全模型收敛，得到预置的网络安全模型，使得网络安全模型能够对移动业务数据进行风险识别，风险识别结果即为移动业务数据的目标业务类型。例如，目标业务类型包括群控、脚本攻击、设备指纹篡改、物联网黑卡中的至少一个，网络安全模型包括第一网络安全模型、第二网络安全模型、第三网络安全模型和第四网络安全模型，第一网络安全模型用于识别移动业务数据是否存在群控，第二网络安全模型用于识别移动业务数据是否存在脚本攻击，第三网络安全模型用于识别移动业务数据是否存在设备指纹篡改，第四网络安全模型用于识别移动业务数据是否存在物联网黑卡。

[0061] 需要说明的是,网络安全模型的识别结果是非黑即白,例如当移动业务数据为http包时,该http包是攻击包/正常请求包二选一。通过网络安全模型识别出移动业务数据的目标业务类型,并将识别出的目标业务类型与移动业务数据的账号信息进行关联,且保存到数据库表中,便于后续的风险处置。

[0062] 在一些实施例中,网络安全模型的技术手段包括前端编程埋点、日志监控、大数据分析 and AI模型、外来情报库、WAF安全网关等,本实施例不做具体限定。系统通过帐号信息对移动业务数据进行管理,帐号信息比如为注册手机号,向http请求包中增加注册手机号的标识,后台数据库存储http请求包和该注册手机号的对应记录,有利于后续的业务风险处置。

[0063] 步骤S104、获取预设的第一矩阵表,第一矩阵表包括各个业务场景与各个风险类型之间的风险评估信息。

[0064] 其中,风险评估信息包括风险评估权重、风险评估分值和/或风险评估等级等。比如:在拉新融资期,业务可能允许虚假手机号注册,此时虚假手机号注册的风险评估信息表明的风险较低。在营销活动期,严禁第三方合作商欺诈作弊,此时欺诈作弊的风险评估信息表明的风险较高。

[0065] 在一实施例中,其中,业务场景与风险类型之间的风险评估信息(即第一矩阵表)可以由业务部门非常熟悉业务目标和流程的人员进行管理和配置。业务部门结合移动应用的生命周期和业务关键绩效指标KPI进行设置。以第一矩阵表如表2为例,APP用户成长期-邀请注册(表2中的业务场景2)为例,若APP到了用户成长期,业务考核邀请注册不再是主要KPI,所以群控攻击的风险评估权重从投融资期-邀请注册(表2中的业务场景1)的80%降低到40%,其他三种风险类型对应的风险评估权重相应上调,加和为100%。

[0066] 示例性的,风险评估信息为风险评估权重,每个业务场景下的总权重为100%,第一矩阵表如表2所示:

[0067] 表2

[0068]

	业务场景1	业务场景2	业务场景3	业务场景N
群控	80%	40%	10%	50%
脚本攻击	20%	20%	40%	50%
设备指纹篡改	0	20%	30%	0
物联网黑卡	0	20%	20%	0

[0069] 示例性的,风险评估信息为风险评估分值,每个业务场景下的总分为100分,第一矩阵表如表3所示:

[0070] 表3

[0071]

	业务场景1	业务场景2	业务场景3	业务场景N
群控	80分	40分	10分	50分
脚本攻击	20分	20分	40分	50分
设备指纹篡改	0分	20分	30分	0分
物联网黑卡	0分	20分	20分	0分

[0072] 示例性的,风险评估信息为风险评估等级,每个业务场景下存在不同优先级的风险评估等级,例如设置一级风险的优先级较高,第一矩阵表如表4所示:

[0073] 表4

[0074]	业务场景1	业务场景2	业务场景3	业务场景N
群控	一级风险	二级风险	三级风险	一级风险
脚本攻击	二级风险	三级风险	二级风险	一级风险
设备指纹篡改		三级风险	二级风险	
物联网黑卡		三级风险	三级风险	

[0075] 需要说明的是,移动业务数据的风险评估等级的认定也可以结合生命周期和业务场景来定义,本实施例不做具体限定。

[0076] 步骤S105、基于第一矩阵表,确定目标业务场景与目标风险类型之间的目标风险评估信息。

[0077] 其中,第一矩阵表是基于业务场景信息和业务类型建立的,根据目标业务场景信息和目标业务类型查找第一矩阵表,确定第一矩阵表中的对应信息,得到移动业务数据的目标风险评估信息。第一矩阵表可根据实际情况进行灵活设置和调整,通过第一矩阵表可快速地确定移动业务数据的风险评估信息,极大地提高业务风险评估的灵活性和可靠性,有利于保障移动业务安全。

[0078] 在一实施例中,通过第一矩阵表,确定目标业务场景对应的多个风险评估信息;从目标业务场景对应的多个风险评估信息中选取与目标风险类型对应的目标风险评估信息;其中,目标风险评估信息包括风险评估权重、风险评估分值和风险评估等级。需要说明的是,目标风险类型可以是一个或者多个,当目标风险类型为多个时,通过第一矩阵表确定的目标风险评估信息也为多个。

[0079] 示例性的,第一矩阵表如表2所示,当目标业务场景为业务场景3时,确定业务场景3对应的多个风险评估权重,分别为群控-10%、脚本攻击-40%、设备指纹篡改-30%和物联网黑卡-20%。当目标风险类型包括群控和脚本攻击时,目标风险评估权重包括群控-10%和脚本攻击-40%。

[0080] 步骤S106、根据目标风险评估信息,确定移动业务数据的风险评分。

[0081] 得到一个或者多个目标风险评估信息之后,根据一个或者多个目标风险评估信息可以确定移动业务数据的风险评分,从而利用移动应用在不同的生命周期阶段有不同的业务场景的特性,灵活地对移动业务数据进行风险评估,得出移动业务数据的风险评分,通常而言,风险评分越高表明业务风险越高,风险评分越低表明业务风险越低。

[0082] 在一实施例中,当目标风险评估信息包括多个风险评估权重时,获取风险评估的预设总分值;计算预设总分值与多个风险评估权重之间的乘积之和,得到移动业务数据的风险评分。示例性的,如表2所示,风险评估信息包括风险评估权重,同一业务场景下的多个业务类型的总权重为100%,例如业务场景1中群控对应的权重为80%,脚本攻击对应的权重为20%,假设预设总分值为100分,目标风险评估信息包括脚本攻击对应的第一权重和物联网黑卡对应的第二权重,计算业务场景1下的预设总分值与脚本攻击对应的第一权重、物联网黑卡对应的第二权重之间的乘积之和,得到风险评估分值为20分。

[0083] 在一实施例中,当目标风险评估信息包括多个风险评估分值时,计算多个风险评估分值之和,得到移动业务数据的风险评分。示例性的,如表3所示,风险评估信息包括风险评估分值,可以设置同一业务场景下的多个业务类型的总分值固定,例如总分值为100分,

网络安全识别的结果是非黑即白,风险评分的总分值是黑为100分,白为0分,例如业务场景2中群控对应的分值为40分,脚本攻击、设备指纹篡改和物联网黑卡对应的分值都为20分,假设预设总分为100分,目标风险评估信息包括脚本攻击对应的第一分值和物联网黑卡对应的第二分值,计算业务场景2下的脚本攻击对应的第一分值、物联网黑卡对应的第二分值之和,得到风险评估分值为40分。

[0084] 在一实施例中,当目标风险评估信息包括多个风险评估等级时,获取各个风险评估等级对应的多个分值;从各个风险评估等级对应的多个分值中确定多个风险评估等级对应的目标分值,并选取最高的目标分值作为移动业务数据的风险评分。示例性的,如表4所示,风险评估信息包括风险评估等级,例如业务场景3中群控、物联网黑卡对应的等级都为三级风险,脚本攻击和设备指纹篡改对应的等级都为二级风险,假设二级风险对应分值为35分,三级风险对应分值为15分,目标风险评估信息包括二级风险和三级风险,可以确定目标分值为35分和15分,选取最高的目标分值35分作为移动业务数据的风险评分,即风险评估分值为35分。

[0085] 在一实施例中,根据目标风险评估信息,确定移动业务数据的风险评分之后,还包括:获取预设的第三矩阵表,第三矩阵表包括各个业务场景与各个风险处置信息之间的风险评分;基于第三矩阵表,确定与移动业务数据的风险评分以及目标业务场景相对应的目标风险处置信息;确定移动业务数据对应的账号信息,并按照目标风险处置信息对账号信息进行处置。其中,风险处置信息包括但不限于拉黑拦截、人工审核和权益降级。拉黑拦截为将账号信息加入黑名单,例如不让手机号登录APP;人工审核为发放权益时需要增加人工审核的程序,例如手机号参与抽奖后,不直接发放礼品,要人工审核;权益降级为降低账号信息的权益等级,例如控制抽奖概率降低,不让手机号中奖。按照风险处理信息对所述账号信息进行风险处理,有效提高业务风险处置自动化能力。

[0086] 示例性的,第三矩阵表如表5所示:

[0087] 表5

[0088]

	业务场景1	业务场景2	业务场景3	业务场景N
拉黑拦截	评分>80	评分>90	评分>95	评分>99
人工审核	80>评分>60	90>评分>70	95>评分>60	99>评分>50
权益降级	60>评分>0	70>评分>0	60>评分>0	50>评分>0

[0089] 例如,第三矩阵表如表5所示,移动业务数据的风险评分为35分,目标业务场景为业务场景3,则通过第三矩阵表可以确定与移动业务数据的风险评分35分以及业务场景3相对应的目标风险处置信息为权益降级,按照该目标风险处置信息对账号信息进行权益降级处置,即关联账号信息的权益降级的相关信息,从而降低移动业务数据对应的账号信息的权益等级,例如控制账号信息的抽奖成功概率降低。

[0090] 上述实施例提供的业务风险评估方法,通过获取待识别的移动应用的移动业务数据;确定移动应用的当前生命周期,并根据当前生命周期,确定移动业务数据的目标业务场景;将移动业务数据输入至预置的网络安全模型,以识别移动业务数据的目标风险类型;获取预设的第一矩阵表,第一矩阵表包括各个业务场景与各个风险类型之间的风险评估信息;基于第一矩阵表,确定目标业务场景与目标风险类型之间的目标风险评估信息;根据目标风险评估信息,确定移动业务数据的风险评分。本申请实施例利用移动应用在不同的生

命周期阶段有不同的业务场景的特性,灵活地对移动业务数据进行风险评估,能够有效确定移动业务数据的风险评估信息,提高业务风险评估的针对性、灵活性和可靠性,有利于保障移动业务安全。

[0091] 请参照图4,图4为本申请实施例提供的一种业务风险评估装置的示意性框图。

[0092] 如图4所示,该业务风险评估装置200,包括:获取模块201、确定模块202、识别模块203、评估模块204和评分模块205。

[0093] 获取模块201,用于获取待识别的移动应用的移动业务数据;

[0094] 确定模块202,用于确定所述移动应用的当前生命周期,并根据所述当前生命周期,确定所述移动业务数据的目标业务场景;

[0095] 识别模块203,用于将所述移动业务数据输入至预置的网络安全模型,以识别所述移动业务数据的目标风险类型;

[0096] 获取模块201,还用于获取预设的第一矩阵表,所述第一矩阵表包括各个业务场景与各个风险类型之间的风险评估信息;

[0097] 评估模块204,用于基于所述第一矩阵表,确定所述目标业务场景与所述目标风险类型之间的目标风险评估信息;

[0098] 评分模块205,用于根据所述目标风险评估信息,确定所述移动业务数据的风险评分。

[0099] 在一个实施例中,如图5所示,确定模块202包括:第一确定子模块2021或者第二确定子模块2022。

[0100] 第一确定子模块2021,用于获取生命周期与业务场景之间的映射关系表,根据所述映射关系表和当前生命周期,确定所述移动业务数据的目标业务场景。

[0101] 第二确定子模块2022,用于确定所述移动应用的当前活动场景,并根据所述当前生命周期和所述当前活动场景,确定所述移动业务数据的目标业务场景。

[0102] 在一个实施例中,第二确定子模块2022还用于:

[0103] 获取预设的第二矩阵表,所述第二矩阵表包括各个生命周期与各个活动场景之间的业务场景;

[0104] 基于所述第二矩阵表,确定所述当前生命周期和所述当前活动场景之间的目标业务场景。

[0105] 在一个实施例中,所述当前生命周期包括投融资期、用户增长期、活动获利期、业务维持期和业务扩张期,所述当前活动场景包括邀请注册、签到抽奖、优惠满减和红包抵扣。

[0106] 在一个实施例中,评估模块204还用于:

[0107] 通过所述第一矩阵表,确定所述目标业务场景对应的多个风险评估信息;

[0108] 从所述目标业务场景对应的多个风险评估信息中选取与所述目标风险类型对应的目标风险评估信息;

[0109] 其中,所述目标风险评估信息包括风险评估权重、风险评估分值和风险评估等级。

[0110] 在一个实施例中,评估模块204还用于:

[0111] 当所述目标风险评估信息包括多个风险评估权重时,获取风险评估的预设总分值;

[0112] 计算所述预设总分值与多个风险评估权重之间的乘积之和,得到所述移动业务数据的风险评分;或者

[0113] 当所述目标风险评估信息包括多个风险评估分值时,计算所述多个风险评估分值之和,得到所述移动业务数据的风险评分;或者

[0114] 当所述目标风险评估信息包括多个风险评估等级时,获取各个风险评估等级对应的多个分值;

[0115] 从所述各个风险评估等级对应的多个分值中确定所述多个风险评估等级对应的目标分值,并选取最高的目标分值作为所述移动业务数据的风险评分。

[0116] 在一个实施例中,评分模块205还用于:

[0117] 获取预设的第三矩阵表,所述第三矩阵表包括各个业务场景与各个风险处置信息之间的风险评分;

[0118] 基于所述第三矩阵表,确定与所述移动业务数据的风险评分以及目标业务场景相对应的目标风险处置信息;

[0119] 确定所述移动业务数据对应的账号信息,并按照所述目标风险处置信息对所述账号信息进行处置。

[0120] 需要说明的是,所属领域的技术人员可以清楚地了解到,为了描述的方便和简洁,上述描述的装置和各模块及单元的具体工作过程,可以参考前述业务风险评估方法实施例中的对应过程,在此不再赘述。

[0121] 上述实施例提供的装置可以实现为一种计算机程序的形式,该计算机程序可以在如图6所示的计算机设备上运行。

[0122] 请参阅图6,图6为本申请实施例提供的一种计算机设备的结构示意图。该计算机设备可以为服务器或终端设备。

[0123] 如图6所示,该计算机设备包括通过系统总线连接的处理器、存储器和网络接口,其中,存储器可以包括非易失性存储介质和内存储器。

[0124] 非易失性存储介质可存储操作系统和计算机程序。该计算机程序包括程序指令,该程序指令被执行时,可使得处理器执行任意一种业务风险评估方法。

[0125] 处理器用于提供计算和控制能力,支撑整个计算机设备的运行。

[0126] 内存储器为非易失性存储介质中的计算机程序的运行提供环境,该计算机程序被处理器执行时,可使得处理器执行任意一种业务风险评估方法。

[0127] 该网络接口用于进行网络通信,如发送分配的任务等。本领域技术人员可以理解,图6中示出的结构,仅仅是与本申请方案相关的部分结构的框图,并不构成对本申请方案所应用于其上的计算机设备的限定,具体的计算机设备可以包括比图中所示更多或更少的部件,或者组合某些部件,或者具有不同的部件布置。

[0128] 应当理解的是,处理器可以是中央处理单元(Central Processing Unit,CPU),该处理器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)、现场可编程门阵列(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。其中,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。

[0129] 其中,在一个实施例中,所述处理器用于运行存储在存储器中的计算机程序,以实现如下步骤:

[0130] 获取待识别的移动应用的移动业务数据;

[0131] 确定所述移动应用的当前生命周期,并根据所述当前生命周期,确定所述移动业务数据的目标业务场景;

[0132] 将所述移动业务数据输入至预置的网络安全模型,以识别所述移动业务数据的目标风险类型;

[0133] 获取预设的第一矩阵表,所述第一矩阵表包括各个业务场景与各个风险类型之间的风险评估信息;

[0134] 基于所述第一矩阵表,确定所述目标业务场景与所述目标风险类型之间的目标风险评估信息;

[0135] 根据所述目标风险评估信息,确定所述移动业务数据的风险评分。

[0136] 在一个实施例中,所述处理器在实现所述根据所述当前生命周期,确定所述移动业务数据的目标业务场景时,用于实现:

[0137] 获取生命周期与业务场景之间的映射关系表,根据所述映射关系表和当前生命周期,确定所述移动业务数据的目标业务场景;或者

[0138] 确定所述移动应用的当前活动场景,并根据所述当前生命周期和所述当前活动场景,确定所述移动业务数据的目标业务场景。

[0139] 在一个实施例中,所述处理器在实现所述根据所述当前生命周期和所述当前活动场景,确定所述移动业务数据的目标业务场景时,用于实现:

[0140] 获取预设的第二矩阵表,所述第二矩阵表包括各个生命周期与各个活动场景之间的业务场景;

[0141] 基于所述第二矩阵表,确定所述当前生命周期和所述当前活动场景之间的目标业务场景。

[0142] 在一个实施例中,所述当前生命周期包括投融资期、用户增长期、活动获利期、业务维持期和业务扩张期,所述当前活动场景包括邀请注册、签到抽奖、优惠满减和红包抵扣。

[0143] 在一个实施例中,所述处理器在实现所述基于所述第一矩阵表,确定所述目标业务场景与所述目标风险类型之间的目标风险评估信息时,用于实现:

[0144] 通过所述第一矩阵表,确定所述目标业务场景对应的多个风险评估信息;

[0145] 从所述目标业务场景对应的多个风险评估信息中选取与所述目标风险类型对应的目标风险评估信息;

[0146] 其中,所述目标风险评估信息包括风险评估权重、风险评估分值或者风险评估等级。

[0147] 在一个实施例中,所述处理器在实现所述根据所述目标风险评估信息,确定所述移动业务数据的风险评分时,用于实现:

[0148] 当所述目标风险评估信息包括多个风险评估权重时,获取风险评估的预设总分值;

[0149] 计算所述预设总分值与多个风险评估权重之间的乘积之和,得到所述移动业务数

据的风险评分;或者

[0150] 当所述目标风险评估信息包括多个风险评估分值时,计算所述多个风险评估分值之和,得到所述移动业务数据的风险评分;或者

[0151] 当所述目标风险评估信息包括多个风险评估等级时,获取各个风险评估等级对应的多个分值;

[0152] 从所述各个风险评估等级对应的多个分值中确定所述多个风险评估等级对应的目标分值,并选取最高的目标分值作为所述移动业务数据的风险评分。

[0153] 在一个实施例中,所述处理器在实现所述根据所述目标风险评估信息,确定所述移动业务数据的风险评分之后,还用于实现:

[0154] 获取预设的第三矩阵表,所述第三矩阵表包括各个业务场景与各个风险处置信息之间的风险评分;

[0155] 基于所述第三矩阵表,确定与所述移动业务数据的风险评分以及目标业务场景相对应的目标风险处置信息;

[0156] 确定所述移动业务数据对应的账号信息,并按照所述目标风险处置信息对所述账号信息进行处置。

[0157] 需要说明的是,所属领域的技术人员可以清楚地了解到,为了描述的方便和简洁,上述描述计算机设备的具体工作过程,可以参考前述业务风险评估方法实施例中的对应过程,在此不再赘述。

[0158] 本申请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上存储有计算机程序,所述计算机程序中包括程序指令,所述程序指令被执行时所实现的方法可参照本申请业务风险评估方法的各个实施例。

[0159] 其中,所述计算机可读存储介质可以是前述实施例所述的计算机设备的内部存储单元,例如所述计算机设备的硬盘或内存。所述计算机可读存储介质也可以是所述计算机设备的外部存储设备,例如所述计算机设备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。

[0160] 应当理解,在此本申请说明书中所使用的术语仅仅是出于描述特定实施例的目的而并不意在限制本申请。如在本申请说明书和所附权利要求书中所使用的那样,除非上下文清楚地指明其它情况,否则单数形式的“一”、“一个”及“该”意在包括复数形式。

[0161] 还应当理解,在本申请说明书和所附权利要求书中使用的术语“和/或”是指相关列出的项中的一个或多个的任何组合以及所有可能组合,并且包括这些组合。需要说明的是,在本文中,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、物品或者系统不仅包括那些要素,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、物品或者系统所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[0162] 上述本申请实施例序号仅仅为了描述,不代表实施例的优劣。以上所述,仅为本申请的具体实施方式,但本申请的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本申请揭露的技术范围内,可轻易想到各种等效的修改或替换,这些修改或替换都应涵盖在本申请的保护范围之内。因此,本申请的保护范围应以权利要求的保护范围为准。

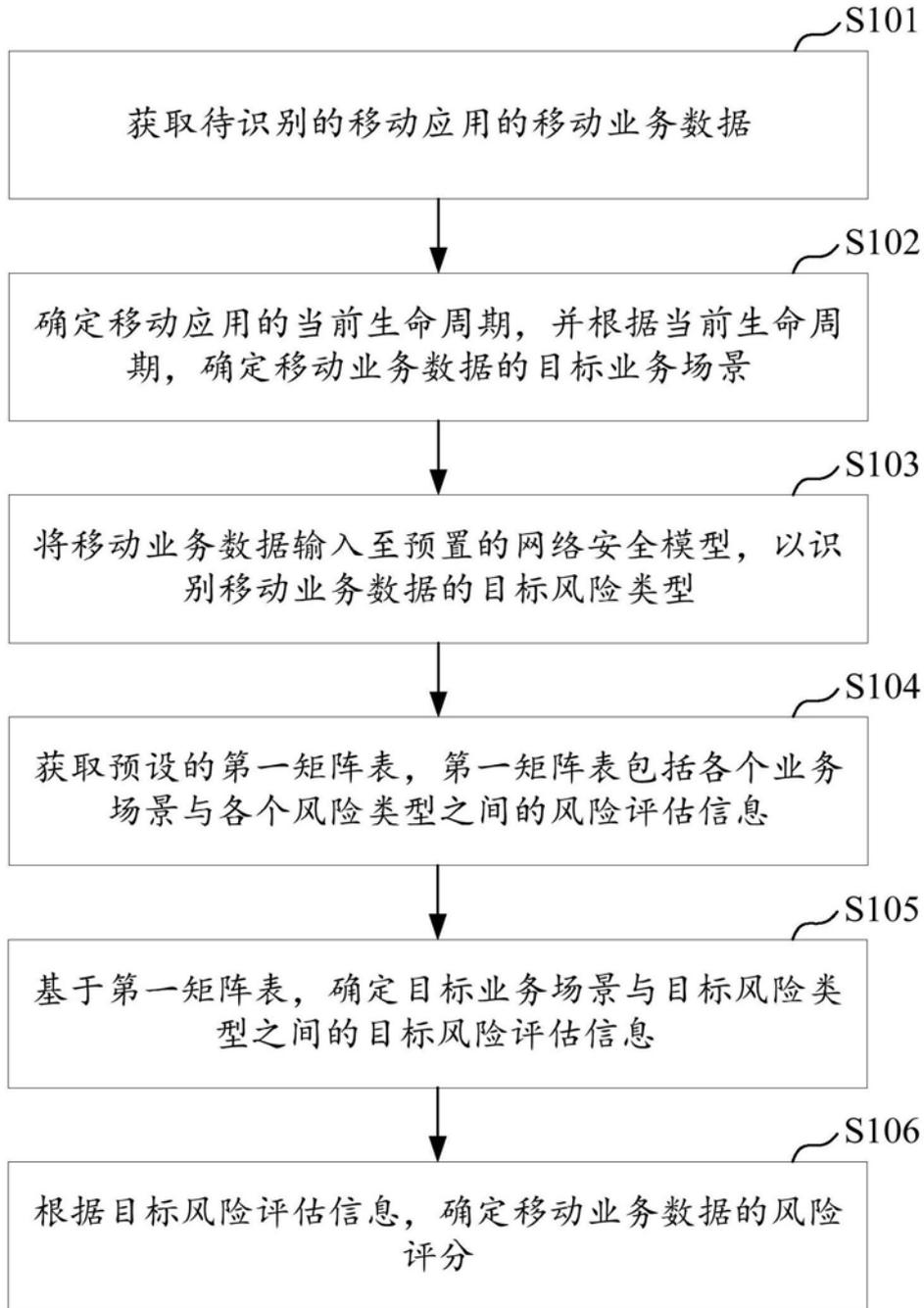


图1

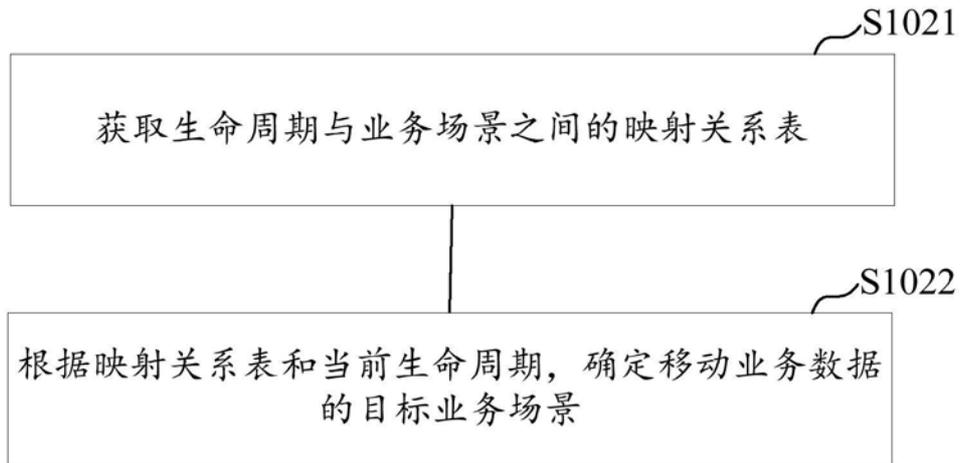


图2

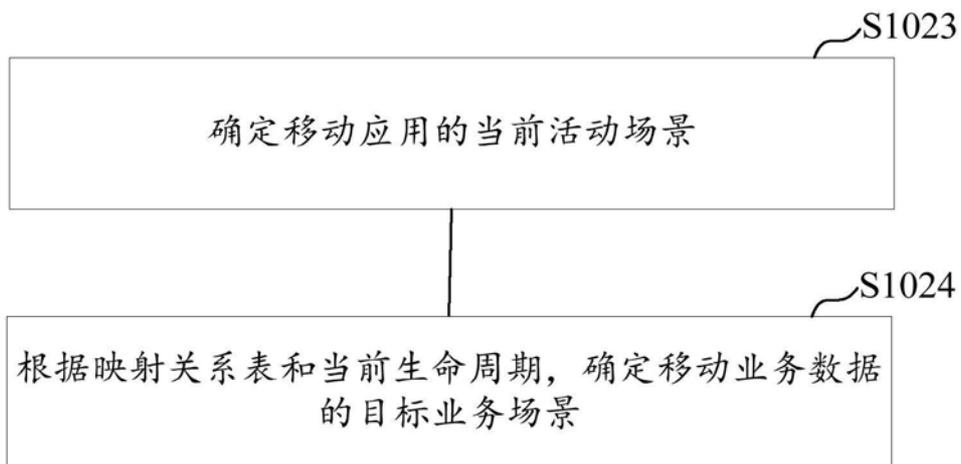


图3

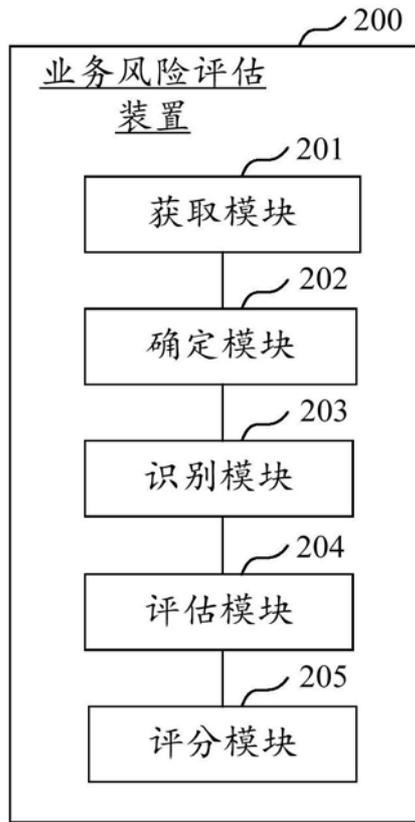


图4

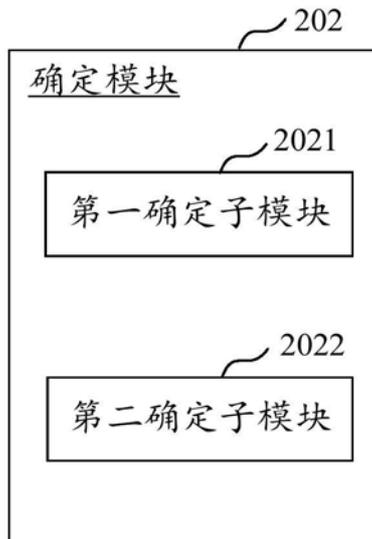


图5

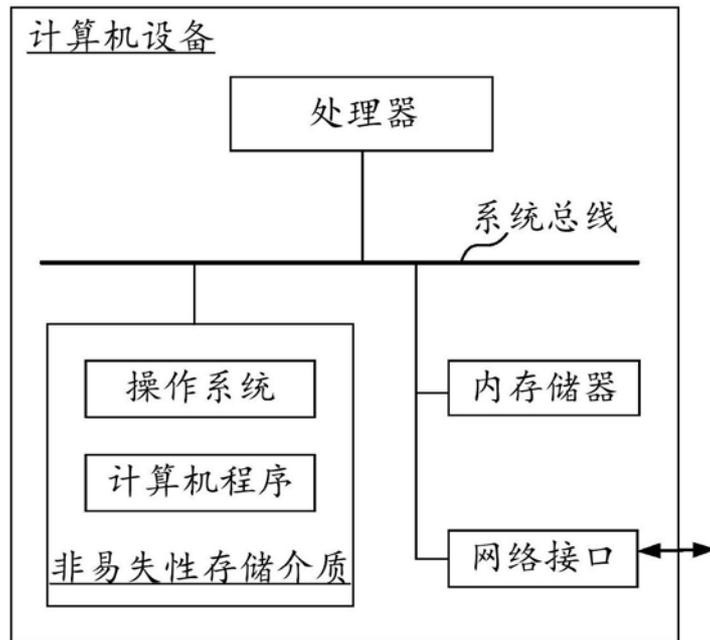


图6