(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107872446 B
(45)授权公告日 2020.07.24

(21)申请号 201610868046.4

(22)申请日 2016.09.28

(65)同一申请的已公布的文献号
申请公布号 CN 107872446 A

(43)申请公布日 2018.04.03

(73)专利权人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 林耀城 陈焕葵 胡育辉 张少愚

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 郝传鑫 熊永强

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 105939401 A,2016.09.14
CN 101742499 A,2010.06.16
CN 103051639 A,2013.04.17
CN 105283898 A,2016.01.27
US 2008244697 A1,2008.10.02
CN 104243458 A,2014.12.24

审查员 刘金鑫

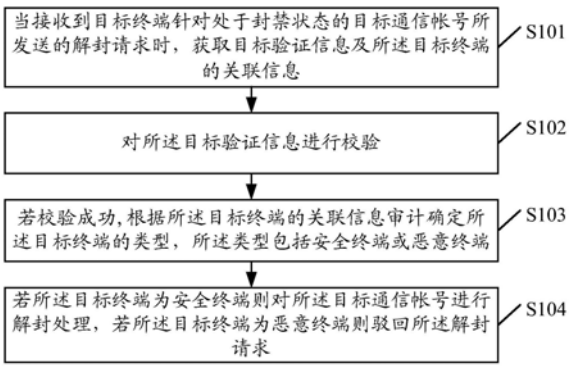
权利要求书3页 说明书11页 附图4页

(54)发明名称

一种通信帐号的管理方法、装置及服务器

(57)摘要

本发明实施例提供一种通信帐号的管理方法、装置及服务器，其中的方法可包括：当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，获取目标验证信息及所述目标终端的关联信息；对所述目标验证信息进行校验，若校验成功，根据所述目标终端的关联信息审计确定所述目标终端的类型，所述类型包括安全终端或恶意终端；若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求。本发明能够提升通信帐号的解封处理过程的安全性，提升对通信帐号的管理有效性。



CN 107872446 B

1.一种通信帐号的管理方法,其特征在于,包括:

当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时,输出解封配置页面;

记录所述目标终端在所述解封配置页面内所输入的标识信息;

若在所述解封配置页面内检测到验证信息获取请求,根据所述目标终端的标识信息向所述目标终端发送源验证信息;

接收所述目标终端根据所述源验证信息而反馈的目标验证信息,并获取所述目标终端的地址信息;

对所述目标验证信息进行校验,若校验成功,根据所述目标终端的地址信息及标识信息审计确定所述目标终端的类型,所述类型包括安全终端或恶意终端;

若所述目标终端为安全终端则对所述目标通信帐号进行解封处理,若所述目标终端为恶意终端则驳回所述解封请求。

2.如权利要求1所述的方法,其特征在于,在接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求之前,还包括:

预先设置用于审计确定终端类型的至少一种审计维度及每一种审计维度对应的权重指数,其中,所述每一种审计维度下包括至少一个审计结果;以及,

预先设置每一种审计维度下的每一个审计结果对应的恶意分值。

3.如权利要求2所述的方法,其特征在于,所述审计维度包括:地址信息维度、标识信息维度、绑定关系维度、历史解封记录维度、自动机操作维度、历史通信行为维度;

所述地址信息维度包括以下审计结果:安全地址信息或恶意地址信息;所述标识信息维度包括以下审计结果:安全标识信息或恶意标识信息;所述绑定关系维度包括以下审计结果:通信帐号的绑定标识信息或通信帐号未绑定的标识信息;所述历史解封记录维度包括以下审计结果:正常解封记录或异常解封记录;所述自动机操作维度包括以下审计结果:自动机操作或非自动机操作;所述历史通信行为维度包括以下审计结果:恶意历史通信行为或正常历史通信行为。

4.如权利要求2或3所述的方法,其特征在于,所述根据所述目标终端的地址信息及标识信息审计确定所述目标终端的类型,包括:

根据所述目标终端的关联信息获取所述目标终端在至少一种审计维度下的恶意分值;

采用每一种审计维度对应的权重指数对所述目标终端在每一种审计维度下的恶意分值进行加权处理;

对加权处理后的各恶意分值进行求和计算,获得所述目标终端的恶意总分;

根据所述目标终端的恶意总分确定所述目标终端的类型。

5.如权利要求4所述的方法,其特征在于,所述根据所述目标终端的恶意总分确定所述目标终端的类型,包括:

将所述目标终端的恶意总分与预设分数阀值进行比较;

若所述目标终端的恶意总分高于所述预设分数阀值,确定所述目标终端为恶意终端;

若所述目标终端的恶意总分低于或等于所述预设分数阀值,确定所述目标终端为安全终端。

6.一种通信帐号的管理装置,其特征在于,包括:

获取单元，用于当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，获取目标验证信息及所述目标终端的关联信息；所述关联信息包括：地址信息及标识信息；

校验单元，用于对所述目标验证信息进行校验；

审计单元，用于若校验成功，根据所述目标终端的关联信息审计确定所述目标终端的类型，所述类型包括安全终端或恶意终端；

管理单元，用于若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求；

所述获取单元包括：

页面输出单元，用于当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，输出解封配置页面；

标识记录单元，用于记录所述目标终端在所述解封配置页面内所输入的标识信息；

信息下发单元，用于若在所述解封配置页面内检测到验证信息获取请求，根据所述目标终端的标识信息向所述目标终端发送源验证信息；

信息获取单元，用于接收所述目标终端根据所述源验证信息而反馈的目标验证信息，并获取所述目标终端的地址信息。

7.如权利要求6所述的装置，其特征在于，还包括：

设置单元，用于预先设置用于审计确定终端类型的至少一种审计维度及每一种审计维度对应的权重指数，其中，所述每一种审计维度下包括至少一个审计结果；以及，预先设置每一种审计维度下的每一个审计结果对应的恶意分值。

8.如权利要求7所述的装置，其特征在于，所述审计维度包括：地址信息维度、标识信息维度、绑定关系维度、历史解封记录维度、自动机操作维度、历史通信行为维度；

所述地址信息维度包括以下审计结果：安全地址信息或恶意地址信息；所述标识信息维度包括以下审计结果：安全标识信息或恶意标识信息；所述绑定关系维度包括以下审计结果：通信帐号的绑定标识信息或通信帐号未绑定的标识信息；所述历史解封记录维度包括以下审计结果：正常解封记录或异常解封记录；所述自动机操作维度包括以下审计结果：自动机操作或非自动机操作；所述历史通信行为维度包括以下审计结果：恶意历史通信行为或正常历史通信行为。

9.如权利要求7或8所述的装置，其特征在于，所述审计单元包括：

分值获取单元，用于根据所述目标终端的关联信息获取所述目标终端在至少一种审计维度下的恶意分值；

加权处理单元，用于采用每一种审计维度对应的权重指数对所述目标终端在每一种审计维度下的恶意分值进行加权处理；

求和计算单元，用于对加权处理后的各恶意分值进行求和计算，获得所述目标终端的恶意总分；

类型确定单元，用于根据所述目标终端的恶意总分确定所述目标终端的类型。

10.如权利要求9所述的装置，其特征在于，所述类型确定单元包括：

分数比较单元，用于将所述目标终端的恶意总分与预设分数阀值进行比较；

结果确认单元，用于若所述目标终端的恶意总分高于所述预设分数阀值，确定所述目

标终端为恶意终端;若所述目标终端的恶意总分低于或等于所述预设分数阀值,确定所述目标终端为安全终端。

11.一种服务器,其特征在于,包括如权利要求6-10任一项所述的通信帐号的管理装置。

12.一种计算机可读取存储介质,其特征在于,所述计算机可读取存储介质中存储有计算机程序,所述计算机程序在执行时包括如权利要求1-5任一项所述的通信帐号的管理方法。

一种通信帐号的管理方法、装置及服务器

技术领域

[0001] 本发明涉及互联网技术领域，尤其涉及一种通信帐号的管理方法、装置及服务器。

背景技术

[0002] 通信帐号是指各种通信平台所分配的、用于在通信平台内唯一标记一个用户的帐号，可以指QQ(一款即时通信软件)帐号、MSN(Microsoft Service Network，一款即时通信软件)帐号、微信帐号等等。通信平台的服务器对通信平台内的所有通信帐号进行统一管理，例如对通信帐号进行封禁处理，以保证通信平台的信息安全。现有技术中，通信帐号被封禁后，通信平台的服务器通常会向用户提示解封操作的流程，以常用的短消息解封操作为例：用户进入解封配置页面请求解封某通信帐号，通信平台的服务器向用户手机下发短信验证码，用户在解封配置页面内输入所接收到的正确的短信验证码即可解除通信帐号的封禁。通过上述描述可知，现有技术中针对通信帐号的解封处理过程太过简单，使用任何终端均可执行解封操作，安全性较低，从而导致对通信帐号的管理有效性较低。

发明内容

[0003] 本发明实施例提供一种通信帐号的管理方法、装置及服务器，能够提升通信帐号的解封处理过程的安全性，提升对通信帐号的管理有效性。

[0004] 本发明实施例第一方面提供一种通信帐号的管理方法，可包括：

[0005] 当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，获取目标验证信息及所述目标终端的关联信息；

[0006] 对所述目标验证信息进行校验，若校验成功，根据所述目标终端的关联信息审计确定所述目标终端的类型，所述类型包括安全终端或恶意终端；

[0007] 若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求。

[0008] 优选地，所述关联信息包括：地址信息及标识信息；

[0009] 所述当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，获取目标验证信息及所述目标终端的关联信息，包括：

[0010] 当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，输出解封配置页面；

[0011] 记录所述目标终端在所述解封配置页面内所输入的标识信息；

[0012] 若在所述解封配置页面内检测到验证信息获取请求，根据所述目标终端的标识信息向所述目标终端发送源验证信息；

[0013] 接收所述目标终端根据所述源验证信息而反馈的目标验证信息，并获取所述目标终端的地址信息。

[0014] 优选地，在接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求之前，还包括：

[0015] 预先设置用于审计确定终端类型的至少一种审计维度及每一种审计维度对应的权重指数，其中，所述每一种审计维度下包括至少一个审计结果；以及，

[0016] 预先设置每一种审计维度下的每一个审计结果对应的恶意分值。

[0017] 优选地，所述审计维度包括：地址信息维度、标识信息维度、绑定关系维度、历史解封记录维度、自动机操作维度、历史通信行为维度；

[0018] 所述地址信息维度包括以下审计结果：安全地址信息或恶意地址信息；所述标识信息维度包括以下审计结果：安全标识信息或恶意标识信息；所述绑定关系维度包括以下审计结果：通信帐号的绑定标识信息或通信帐号未绑定的标识信息；所述历史解封记录维度包括以下审计结果：正常解封记录或异常解封记录；所述自动机操作维度包括以下审计结果：自动机操作或非自动机操作；所述历史通信行为维度包括以下审计结果：恶意历史通信行为或正常历史通信行为。

[0019] 优选地，所述根据所述目标终端的关联信息审计确定所述目标终端的类型，包括：

[0020] 根据所述目标终端的关联信息获取所述目标终端在至少一种审计维度下的恶意分值；

[0021] 采用每一种审计维度对应的权重指数对所述目标终端在每一种审计维度下的恶意分值进行加权处理；

[0022] 对加权处理后的各恶意分值进行求和计算，获得所述目标终端的恶意总分；

[0023] 根据所述目标终端的恶意总分确定所述目标终端的类型。

[0024] 优选地，所述根据所述目标终端的恶意总分确定所述目标终端的类型，包括：

[0025] 将所述目标终端的恶意总分与预设分数阀值进行比较；

[0026] 若所述目标终端的恶意总分高于所述预设分数阀值，确定所述目标终端为恶意终端；

[0027] 若所述目标终端的恶意总分低于或等于所述预设分数阀值，确定所述目标终端为安全终端。

[0028] 本发明实施例第二方面提供一种通信帐号的管理装置，可包括：

[0029] 获取单元，用于当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，获取目标验证信息及所述目标终端的关联信息；

[0030] 校验单元，用于对所述目标验证信息进行校验；

[0031] 审计单元，用于若校验成功，根据所述目标终端的关联信息审计确定所述目标终端的类型，所述类型包括安全终端或恶意终端；

[0032] 管理单元，用于若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求。

[0033] 优选地，所述关联信息包括：地址信息及标识信息；所述获取单元包括：

[0034] 页面输出单元，用于当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，输出解封配置页面；

[0035] 标识记录单元，用于记录所述目标终端在所述解封配置页面内所输入的标识信息；

[0036] 信息下发单元，用于若在所述解封配置页面内检测到验证信息获取请求，根据所述目标终端的标识信息向所述目标终端发送源验证信息；

[0037] 信息获取单元，用于接收所述目标终端根据所述源验证信息而反馈的目标验证信息，并获取所述目标终端的地址信息。

[0038] 优选地，该装置还包括：

[0039] 设置单元，用于预先设置用于审计确定终端类型的至少一种审计维度及每一种审计维度对应的权重指数，其中，所述每一种审计维度下包括至少一个审计结果；以及，预先设置每一种审计维度下的每一个审计结果对应的恶意分值。

[0040] 优选地，所述审计维度包括：地址信息维度、标识信息维度、绑定关系维度、历史解封记录维度、自动机操作维度、历史通信行为维度；

[0041] 所述地址信息维度包括以下审计结果：安全地址信息或恶意地址信息；所述标识信息维度包括以下审计结果：安全标识信息或恶意标识信息；所述绑定关系维度包括以下审计结果：通信帐号的绑定标识信息或通信帐号未绑定的标识信息；所述历史解封记录维度包括以下审计结果：正常解封记录或异常解封记录；所述自动机操作维度包括以下审计结果：自动机操作或非自动机操作；所述历史通信行为维度包括以下审计结果：恶意历史通信行为或正常历史通信行为。

[0042] 优选地，所述审计单元包括：

[0043] 分值获取单元，用于根据所述目标终端的关联信息获取所述目标终端在至少一种审计维度下的恶意分值；

[0044] 加权处理单元，用于采用每一种审计维度对应的权重指数对所述目标终端在每一种审计维度下的恶意分值进行加权处理；

[0045] 求和计算单元，用于对加权处理后的各恶意分值进行求和计算，获得所述目标终端的恶意总分；

[0046] 类型确定单元，用于根据所述目标终端的恶意总分确定所述目标终端的类型。

[0047] 优选地，所述类型确定单元包括：

[0048] 分数比较单元，用于将所述目标终端的恶意总分与预设分数阀值进行比较；

[0049] 结果确认单元，用于若所述目标终端的恶意总分高于所述预设分数阀值，确定所述目标终端为恶意终端；若所述目标终端的恶意总分低于或等于所述预设分数阀值，确定所述目标终端为安全终端。

[0050] 本发明实施例第三方面提供一种服务器，可包括上述第二方面所述的通信帐号的管理装置。

[0051] 本发明实施例中，在响应目标终端针对处于封禁状态的目标通信帐号所发送的解封请求而执行的解封处理过程中，会根据所述目标终端的关联信息审计确定所述目标终端属于安全终端或恶意终端，若为安全终端才执行解封处理，若为恶意终端则驳回所述解封请求；这使得针对通信帐号的解封操作局限于安全终端内执行，有效地提升了解封处理过程的安全性，并且提升了对通信帐号的管理有效性。

附图说明

[0052] 为了更清楚地说明本发明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的前提下，还可以

根据这些附图获得其他的附图。

[0053] 图1为本发明实施例提供的一种通信帐号的管理方法的流程图；

[0054] 图2为本发明实施例提供的另一种通信帐号的管理方法的流程图；

[0055] 图3为本发明实施例提供的一种服务器的结构示意图；

[0056] 图4为本发明实施例提供的一种通信帐号的管理装置的结构示意图。

具体实施方式

[0057] 下面将结合本发明实施例中的附图，对本发明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发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0058] 通信帐号是指各种通信平台所分配的、用于在通信平台内唯一标记一个用户的帐号。此处的通信平台可以包括但不限于：即时通信平台、SNS(Social Networking Services，社交网络服务)通信平台等等，此处的通信帐号可以包括但不限于：诸如QQ帐号、MSN帐号等的即时通信帐号，或者诸如微信帐号、陌陌帐号等的SNS通信帐号等等。通信平台的服务器对通信平台内的所有通信帐号进行统一管理，以保证通信平台的信息安全；例如：若某用户通过某通信帐号发布恶意消息时，通信平台的服务器可对该通信帐号进行封禁处理，以禁止再使用该通信帐号发布消息；再如：若检测到某通信帐号存在盗号风险时，通信平台的服务器可对该通信帐号进行封禁处理，以防止恶意用户盗取该通信帐号并使用该通信帐号进行恶意通信行为。

[0059] 本发明实施例中，当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，获取目标验证信息及所述目标终端的关联信息；对所述目标验证信息进行校验，若校验成功，根据所述目标终端的关联信息审计确定所述目标终端的类型；若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求。这使得针对通信帐号的解封操作局限于安全终端内执行，有效地提升了解封处理过程的安全性，并且提升了对通信帐号的管理有效性。需要说明的是，本发明实施例的终端可以包括但不限于：手机、智能手机、PDA(平板电脑)、智能可穿戴设备等等。服务器可以是通信平台的服务器，即是指承担通信平台的通信功能职能，并且用于对通信平台内的通信帐号进行统一管理的后台服务器。

[0060] 基于上述描述，本发明实施例提供了一种通信帐号的管理方法，请参见图1，该方法可包括以下步骤S101-步骤S104。

[0061] S101，当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，获取目标验证信息及所述目标终端的关联信息。

[0062] 按照所处的状态进行划分，通信平台内的通信帐号可大致分为两类，一类是处于正常状态(非封禁状态)的通信帐号，用户可以使用此类通信帐号进行诸如平台登录、消息发布或消息交互等操作。另一类是处于封禁状态的通信帐号，通信平台的服务器通常会将此类通信帐号添加一个标记以表示封禁状态，或者将此类通信帐号集中存储于一个封禁数据库中；在封禁期间，用户无法使用该类通信帐号进行诸如平台登录、消息发布或消息交互等任何操作；具体地，服务器在接收到处于封禁状态的通信帐号的上述相关操作时均不作

出响应。

[0063] 针对处于封禁状态的通信帐号，通信平台的服务器通常会向用户提示解封操作的流程，常见的解封操作可包括的但不限于：短消息解封操作、email(电子邮件)解封操作等等，以短消息解封操作为例：用户进入解封配置页面请求解封目标通信帐号，服务器以短消息方式向用户使用的目标终端(如手机)下发一个源验证信息，此处的源验证信息可以是由图形、字符、音视频等方式或由几种方式的结合而形成的信息，例如源验证信息可以为由四个字符所组成的验证码；用户依据接收到的短消息方式的源验证信息在解封配置页面内输入目标验证信息，服务器则可以从解封配置页面内获得目标验证信息，并进一步获取用户所使用的目标终端的关联信息。所述关联信息可包括：地址信息及标识信息；其中，地址信息可以是目标终端的IP(Internet Protocol，网络协议)地址或者MAC地址(Media Access Control Address，硬件地址)等等；当用户进入解封配置页面时，服务器可获取目标终端的地址信息。其中，标识信息可以是目标终端所属的运营商网络号码(如手机号码)等，当用户在解封配置页面内输入标识信息以获取源验证信息时，服务器由此记录该目标终端的标识信息。

[0064] S102，对所述目标验证信息进行校验；若校验成功则转入执行步骤S103。

[0065] 校验的目的是确认目标验证信息的准确性；以短消息解封操作为例：目标验证信息是基于服务器下发的源验证信息而由用户主动输入的，那么，对目标验证信息的校验过程即是将源验证信息与目标验证信息之间进行比对的过程，如果二者相匹配校验成功，否则校验失败。需要说明的是，此处的相匹配是指完全一致或完全对应，例如：源验证信息为“ab12”四个字符组成的验证码，那么目标验证信息与源验证信息完全一致为“ab12”时校验成功，否则校验失败。再如：源验证信息包括一幅图片，该图片被划分为上下两部分且上下错开，其文字内容包括“请拼接为完整图片”；那么，目标验证信息需要将该上下错开的图片拼接为完整图片后才校验通过，此时二者完全对应，否则校验失败。本实施例中，若校验失败可以向目标终端输出提示信息，提醒用户输入的目标验证信息错误，无法进行解封处理。

[0066] S103，根据所述目标终端的关联信息审计确定所述目标终端的类型，所述类型包括安全终端或恶意终端。

[0067] S104，若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求。

[0068] 目前许多通信平台存在这样一种情况：许多恶意用户在通信平台注册多个通信帐号，并使用多个通信帐号执行诸如发布恶意消息、传播谣言或盗取其他用户的信息等恶意行为；此种情况下，通信平台的服务器通常会对恶意用户的通信帐号进行封禁处理。然而，通信帐号被封禁处理后，恶意用户会利用一些恶意终端对处于封禁状态的通信帐号进行解封操作，此处的恶意终端是指存在恶意通信行为的终端，例如：猫池设备(一种可以插入多个手机卡的设备)。为了保证解封处理过程的安全性，将解封处理过程局限在安全终端内，步骤S103-S104中，在获取目标终端的关联信息之后，需要依据该关联信息对目标终端进行审计，判断该目标终端是恶意终端还是安全终端；如果是安全终端则对所述目标通信帐号进行解封处理，如果是恶意终端则驳回所述解封请求。其中，解封处理是指解除目标通信帐号的封禁状态，使用户能够正常使用目标通信帐号；具体可以是指删除目标通信帐号的表示封禁状态的标记，或者将目标通信帐号从封禁数据库中移除。服务器在接收到解封处理

后的目标通信帐号的平台登录、消息发布或消息交互等相关操作时均作出相应响应。其中，驳回所述解封请求是指继续保持目标通信帐号的封禁状态，并可向目标终端返回提示信息，提醒用户由于目标终端存在恶意风险，因此无法使用该目标终端对目标通信帐号进行解封处理。

[0069] 本发明实施例的通信帐号的管理方法，当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，获取目标验证信息及所述目标终端的关联信息；对所述目标验证信息进行校验，若校验成功，根据所述目标终端的关联信息审计确定所述目标终端的类型；若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求。这使得针对通信帐号的解封操作局限于安全终端内执行，有效地提升了解封处理过程的安全性，并且提升了对通信帐号的管理有效性。

[0070] 本发明实施例提供了另一种通信帐号的管理方法，请参见图2，该方法可包括以下步骤S201-步骤S211。

[0071] S201，预先设置用于审计确定终端类型的至少一种审计维度及每一种审计维度对应的权重指数，其中，所述每一种审计维度下包括至少一个审计结果；以及，预先设置每一种审计维度下的每一个审计结果对应的恶意分值。

[0072] 具体实现中，可以采用下述表一来存储预先设置的内容，如下：

[0073] 表一：审计表

[0074]

审计维度	审计结果	恶意分值	权重指数
地址信息维度	安全地址信息	dim_{1-1}	pro_1
	恶意地址信息	dim_{1-2}	
标识信息维度	安全标识信息	dim_{2-1}	pro_2
	恶意标识信息	dim_{2-2}	
绑定关系维度	通信帐号的绑定标识信息	dim_{3-1}	pro_3
	通信帐号未绑定的标识信息	dim_{3-2}	

[0075]

历史解封记录维度	正常解封记录	dim_{4-1}	pro_4
	异常解封记录	dim_{4-2}	
自动机操作维度	自动机操作	dim_{5-1}	pro_5
	非自动机操作	dim_{5-2}	
历史行为维度	恶意历史通信行为	dim_{6-1}	pro_6
	正常历史通信行为	dim_{6-2}	
…	…	…	…

[0076] 本实施例主要从上述表一所示的审计维度来审计确定终端的类型。如表一所示，所述审计维度包括：地址信息维度、标识信息维度、绑定关系维度、历史解封记录维度、自动

机操作维度、历史通信行为维度。需要说明的是，每一种审计维度下的每一个审计结果对应的恶意分值可以根据经验值或实际需要进行设定。每一种审计维度对应的权重指数也可以根据经验值或实际需要进行设定，所有审计维度的权重指数总和为1，即：$pro_1+pro_2+pro_3+pro_4+pro_5+pro_6+...=1$。

[0077] 再请参见表一：所述地址信息维度包括以下审计结果：安全地址信息或恶意地址信息。所述标识信息维度包括以下审计结果：安全标识信息或恶意标识信息。所述绑定关系维度包括以下审计结果：通信帐号的绑定标识信息或通信帐号未绑定的标识信息。所述历史解封记录维度包括以下审计结果：正常解封记录或异常解封记录。所述自动机操作维度包括以下审计结果：自动机操作或非自动机操作。所述历史通信行为维度包括以下审计结果：恶意历史通信行为或正常历史通信行为。

[0078] S202，当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，输出解封配置页面。

[0079] S203，记录所述目标终端在所述解封配置页面内所输入的标识信息。

[0080] S204，若在所述解封配置页面内检测到验证信息获取请求，根据所述目标终端的标识信息向所述目标终端发送源验证信息。

[0081] S205，接收所述目标终端根据所述源验证信息而反馈的目标验证信息，并获取所述目标终端的地址信息。

[0082] 本实施例的步骤S202-S205可以为图1所示实施例的步骤S101的具体细化步骤。

[0083] 在步骤S202-S205中，当目标通信帐号被封禁处理后，服务器通常会向用户提示解封操作的流程，以短消息解封操作为例：服务器输出的解封操作的流程中可包含解封配置页面的网址，用户基于该网址触发拉取并在目标终端显示解封配置页面，此时，服务器可以记录目标终端的地址信息。用户可以在该解封配置页面内输入一些基本信息，包括：待解封的目标通信帐号、目标终端的标识信息(如手机号码)等等，并且请求服务器下发用于解封的验证信息。此时，服务器可以记录目标终端的标识信息，并且服务器根据目标终端的标识信息，以短消息方式向目标终端(如手机)下发一个源验证信息。用户依据接收到的短消息方式的源验证信息在解封配置页面内输入目标验证信息，服务器则可以从解封配置页面内获得目标验证信息。

[0084] S206，对所述目标验证信息进行校验；若校验成功则转入执行步骤S207。

[0085] 本实施例的步骤S206可以参见图1所示实施例的步骤S102，在此不赘述。

[0086] S207，根据所述目标终端的关联信息获取所述目标终端在至少一种审计维度下的恶意分值。

[0087] 首先需要根据目标终端的关联信息确认目标终端在每一种审计维度下的审计结果，具体过程可结合上述表一阐述如下：

[0088] (1)针对地址信息维度：通信平台的服务器可以预先收集一些已知的恶意地址信息，将目标终端的地址信息与预先收集的恶意地址信息进行比对，可确认目标终端的地址信息属于恶意地址信息或安全地址信息，从而可确定目标终端在地址信息维度下的审计结果。

[0089] (2)针对标识信息维度：服务器可预先收集一些已知的恶意标识信息，将目标终端的标识信息信息与预先收集的恶意标识信息进行比对，可确认目标终端的地址信息属于恶

意标识信息或安全标识信息，从而可确定目标终端在地址信息维度下的审计结果。

[0090] (3)针对绑定关系维度：服务器可以预先存储与目标通信帐号存在绑定关系的所有标识信息，将目标终端的标识信息与预先存储的这些标识信息进行比对，可确认目标终端的标识信息是属于目标通信帐号的绑定标识信息或未绑定的标识信息，从而可确定目标终端在绑定关系维度下的审计结果。

[0091] (4)针对历史解封记录维度：此处的历史解封记录包括预设时间段内所执行的解封总次数及解封频率。那么，服务器根据目标终端的标识信息或地址信息可以查询目标终端的历史解封记录，如果其解封总次数超过预设次数阀值，或者解封频率超出预设频率阀值，则确认为异常解封记录；如果其解封总次数未预设次数阀值，且解封频率未超出预设频率阀值，则确认为正常解封记录；从而确定目标终端在历史解封记录维度下的审计结果。

[0092] (5)针对自动机操作维度：此处的自动机操作是基于目标终端请求下发源验证信息的时间与反馈目标验证信息的时间差来审计判定的，如果时间差小于预设时间阀值，确定为自动机操作；如果时间差大于或等于预设时间阀值，确定为非自动机操作；从而确定目标终端在自动机操作维度下的审计结果。

[0093] (6)针对历史通信行为维度：服务器可以根据目标终端的地址信息或标识信息查询目标终端在各通信平台中所进行的历史通信行为，包括：拨打电话、交互消息等行为，如果查询到该目标终端曾执行诸如拨打骚扰电话、发布恶意消息等行为，确定为恶意历史通信行为；否则为正常历史通信行为；从而确定目标终端在历史通信行为维度下的审计结果。

[0094] 进一步，结合上述表一可获取目标终端在每一种审计维度下的审计结果对应的恶意分值。

[0095] S208，采用每一种审计维度对应的权重指数对所述目标终端在每一种审计维度下的恶意分值进行加权处理。

[0096] S209，对加权处理后的各恶意分值进行求和计算，获得所述目标终端的恶意总分。

[0097] S210，根据所述目标终端的恶意总分确定所述目标终端的类型。

[0098] 具体实现中，该方法在执行步骤S210的过程中，具体执行如下步骤s11-s12：

[0099] s11，将所述目标终端的恶意总分与预设分数阀值进行比较。

[0100] s12，若所述目标终端的恶意总分高于所述预设分数阀值，确定所述目标终端为恶意终端；若所述目标终端的恶意总分低于或等于所述预设分数阀值，确定所述目标终端为安全终端。

[0101] 本实施例的步骤S207-S210可以为图1所示实施例的步骤S103的具体细化步骤，主要描述了基于至少一个审计维度来对目标终端的类型进行审计确定的过程。

[0102] 下面以一个具体实例来说明步骤S207-S210所示的审计过程：

[0103] 假设目标终端在每一种审计维度下的审计结果如下：目标终端的地址信息属于安全地址信息，目标终端的标识信息属于恶意标识信息，目标终端的标识信息不是通信帐号的绑定标识，目标终端具备正常解封记录，目标终端在解封过程中执行非自动机操作，并且目标终端执行恶意历史通信行为。那么，参考上述表一，目标终端在每个审计维度下的恶意分值分别为：dim_{1-1}、dim_{2-2}、dim_{3-2}、dim_{4-1}、dim_{5-2}、dim_{6-1}；采用下述公式可计算得到该目标终端的恶意总分Evil为：

[0104] $Evil = dim_{1-1}*pro_1+dim_{2-2}*pro_2+dim_{3-2}*pro_3+dim_{4-1}*pro_4+dim_{5-2}*pro_5+dim_{6-1}*pro_6$

[0105] 最后，将Evil的值与预设分数阀值进行比较确认目标终端的类型。此处的预设分数阀值可以根据实际需要进行设定；例如：假设Evil的值为30，而预设分数阀值为29，则确认目标终端为恶意终端；再如：假设Evil的值为30，而预设分数阀值为35，则确认目标终端为安全终端。

[0106] S211，若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求。

[0107] 本实施例的步骤S211可以参见图1所示实施例的步骤S104，在此不赘述。

[0108] 本发明实施例的通信帐号的管理方法，当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，获取目标验证信息及所述目标终端的关联信息；对所述目标验证信息进行校验，若校验成功，根据所述目标终端的关联信息审计确定所述目标终端的类型；若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求。这使得针对通信帐号的解封操作局限于安全终端内执行，有效地提升了解封处理过程的安全性，并且提升了对通信帐号的管理有效性。

[0109] 基于上述实施例所示的通信帐号的管理方法，本发明实施例还提供了一种服务器，实际应用中该服务器可以是通信平台的后台服务器。请参见图3，该服务器的内部结构可包括但不限于：处理器、网络接口及存储器。其中，服务器内的处理器、网络接口及存储器可通过总线或其他方式连接，在本发明实施例所示图3中以通过总线连接为例。

[0110] 其中，处理器(或称CPU(Central Processing Unit，中央处理器))是服务器的计算核心以及控制核心。网络接口可选的可以包括标准的有线接口、无线接口(如WI-FI、移动通信接口等)。存储器(Memory)是服务器中的记忆设备，用于存放程序和数据。可以理解的是，此处的存储器可以是高速RAM存储器，也可以是非不稳定的存储器(non-volatile memory)，例如至少一个磁盘存储器；可选的还可以是至少一个位于远离前述处理器的存储装置。存储器提供存储空间，该存储空间存储了服务器的操作系统，可包括但不限于：Windows系统(一种操作系统)、Linux(一种操作系统)系统等等，本发明对此并不作限定。存储器的存储空间还存储了通信帐号的管理装置。

[0111] 在本发明实施例中，服务器通过运行存储器中的通信帐号的管理装置来执行上述图1-图2所示方法流程的相应步骤。请一并参见图4，该通信帐号的管理装置运行如下单元：

[0112] 获取单元101，用于当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，获取目标验证信息及所述目标终端的关联信息。

[0113] 校验单元102，用于对所述目标验证信息进行校验。

[0114] 审计单元103，用于若校验成功，根据所述目标终端的关联信息审计确定所述目标终端的类型，所述类型包括安全终端或恶意终端。

[0115] 管理单元104，用于若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求。

[0116] 具体实现中，所述关联信息包括：地址信息及标识信息；该装置在运行所述获取单元101的过程中，具体运行如下单元：

[0117] 页面输出单元1001，用于当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，输出解封配置页面。

[0118] 标识记录单元1002，用于记录所述目标终端在所述解封配置页面内所输入的标识

信息。

[0119] 信息下发单元1003，用于若在所述解封配置页面内检测到验证信息获取请求，根据所述目标终端的标识信息向所述目标终端发送源验证信息。

[0120] 信息获取单元1004，用于接收所述目标终端根据所述源验证信息而反馈的目标验证信息，并获取所述目标终端的地址信息。

[0121] 具体实现中，可选地，该装置还运行如下单元：

[0122] 设置单元105，用于预先设置用于审计确定终端类型的至少一种审计维度及每一种审计维度对应的权重指数，其中，所述每一种审计维度下包括至少一个审计结果；以及，预先设置每一种审计维度下的每一个审计结果对应的恶意分值。

[0123] 具体实现中，所述审计维度包括：地址信息维度、标识信息维度、绑定关系维度、历史解封记录维度、自动机操作维度、历史通信行为维度；

[0124] 所述地址信息维度包括以下审计结果：安全地址信息或恶意地址信息；所述标识信息维度包括以下审计结果：安全标识信息或恶意标识信息；所述绑定关系维度包括以下审计结果：通信帐号的绑定标识信息或通信帐号未绑定的标识信息；所述历史解封记录维度包括以下审计结果：正常解封记录或异常解封记录；所述自动机操作维度包括以下审计结果：自动机操作或非自动机操作；所述历史通信行为维度包括以下审计结果：恶意历史通信行为或正常历史通信行为。

[0125] 具体实现中，该装置在运行所述审计单元103的过程中，具体运行如下单元：

[0126] 分值获取单元2001，用于根据所述目标终端的关联信息获取所述目标终端在至少一种审计维度下的恶意分值。

[0127] 加权处理单元2002，用于采用每一种审计维度对应的权重指数对所述目标终端在每一种审计维度下的恶意分值进行加权处理。

[0128] 求和计算单元2003，用于对加权处理后的各恶意分值进行求和计算，获得所述目标终端的恶意总分。

[0129] 类型确定单元2004，用于根据所述目标终端的恶意总分确定所述目标终端的类型。

[0130] 具体实现中，该装置在运行所述类型确定单元2004的过程中，具体运行如下单元：

[0131] 分数比较单元3001，用于将所述目标终端的恶意总分与预设分数阀值进行比较。

[0132] 结果确认单元3002，用于若所述目标终端的恶意总分高于所述预设分数阀值，确定所述目标终端为恶意终端；若所述目标终端的恶意总分低于或等于所述预设分数阀值，确定所述目标终端为安全终端。

[0133] 由于服务器通过运行图4所示的通信帐号的管理装置来执行图1-图2所示的通信帐号的管理方法，因此，图4所示的通信帐号的管理装置的各单元的功能可参见图1-图2所示的通信帐号的管理方法的各步骤的相关描述，在此不赘述。

[0134] 与方法同理，本发明实施例的服务器及通信帐号的管理装置，当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，获取目标验证信息及所述目标终端的关联信息；对所述目标验证信息进行校验，若校验成功，根据所述目标终端的关联信息审计确定所述目标终端的类型；若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求。这使得针对通信帐号的解封操

作局限于安全终端内执行,有效地提升了解封处理过程的安全性,并且提升了对通信帐号的管理有效性。

[0135] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的程序可存储于一计算机可读取存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory,ROM)或随机存储记忆体(Random Access Memory,RAM)等。

[0136] 以上所揭露的仅为本发明较佳实施例而已,当然不能以此来限定本发明之权利范围,因此依本发明权利要求所作的等同变化,仍属本发明所涵盖的范围。

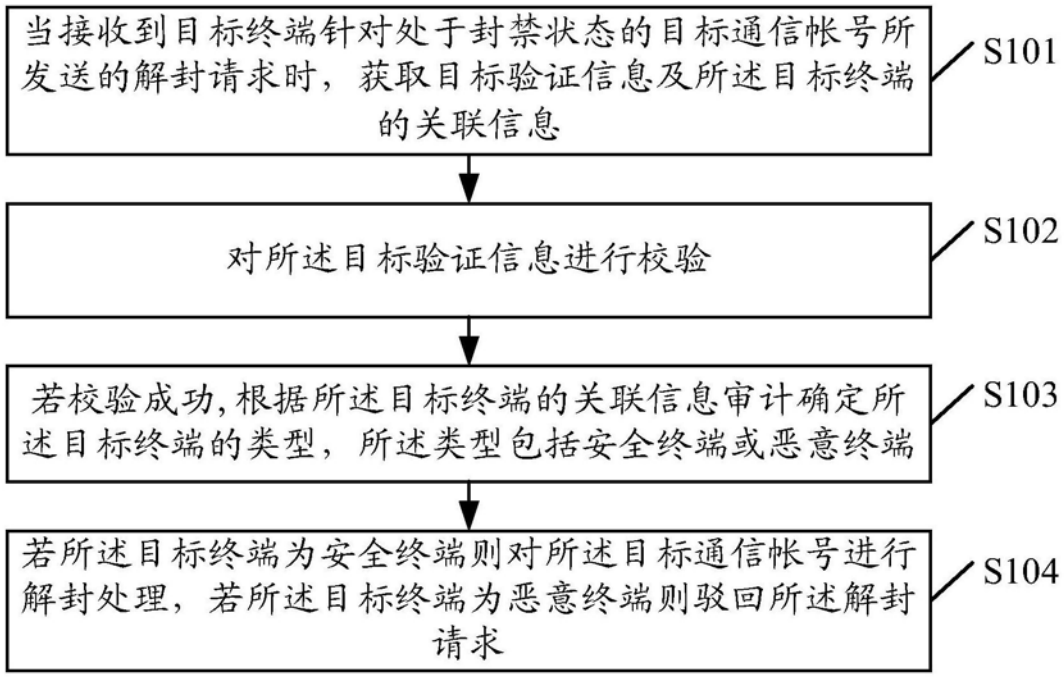

当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，获取目标验证信息及所述目标终端的关联信息
S101
对所述目标验证信息进行校验
S102
若校验成功,根据所述目标终端的关联信息审计确定所述目标终端的类型，所述类型包括安全终端或恶意终端
S103
若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求
S104

图1

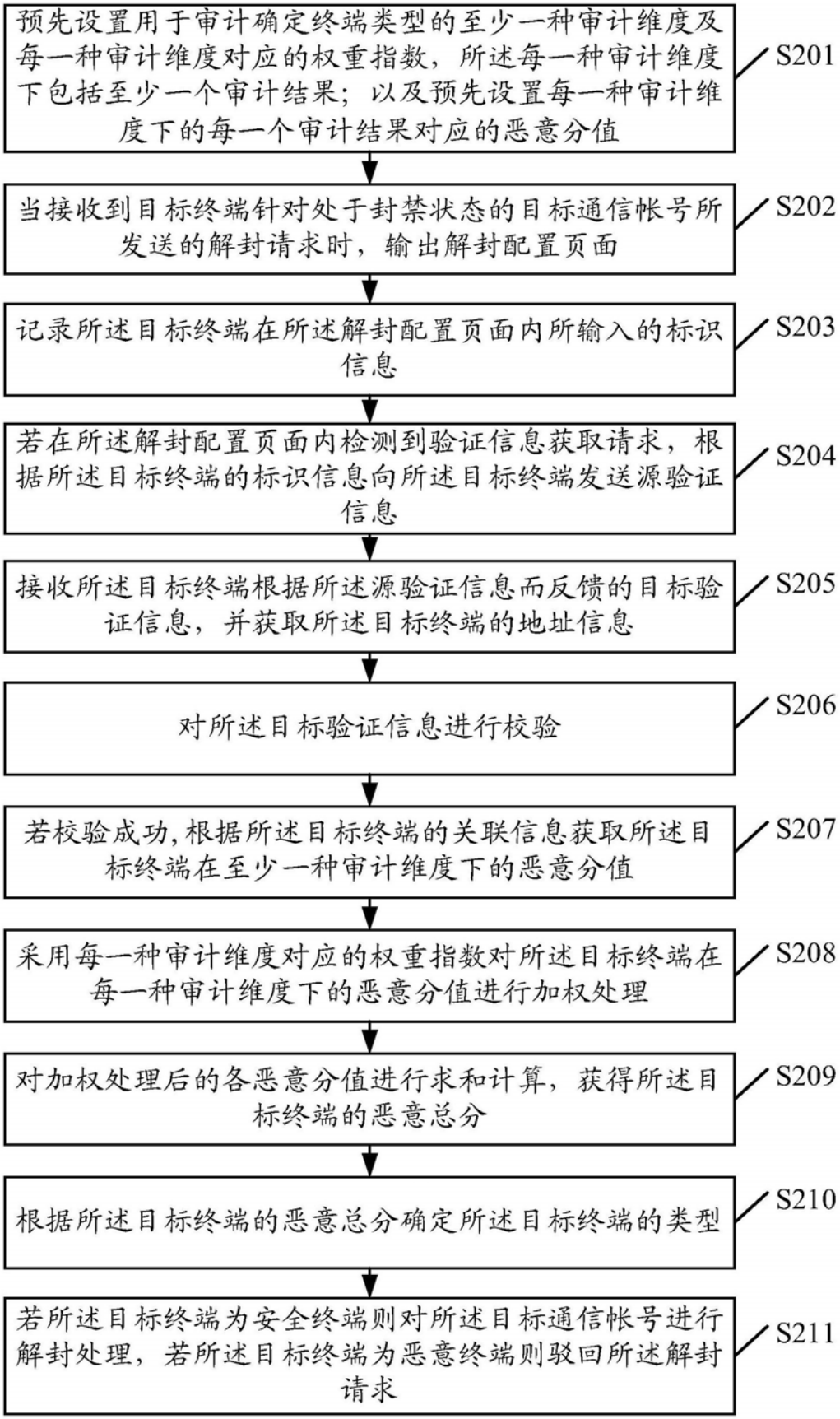

预先设置用于审计确定终端类型的至少一种审计维度及每一种审计维度对应的权重指数，所述每一种审计维度下包括至少一个审计结果；以及预先设置每一种审计维度下的每一个审计结果对应的恶意分值
S201
当接收到目标终端针对处于封禁状态的目标通信帐号所发送的解封请求时，输出解封配置页面
S202
记录所述目标终端在所述解封配置页面内所输入的标识信息
S203
若在所述解封配置页面内检测到验证信息获取请求，根据所述目标终端的标识信息向所述目标终端发送源验证信息
S204
接收所述目标终端根据所述源验证信息而反馈的目标验证信息，并获取所述目标终端的地址信息
S205
对所述目标验证信息进行校验
S206
若校验成功,根据所述目标终端的关联信息获取所述目标终端在至少一种审计维度下的恶意分值
S207
采用每一种审计维度对应的权重指数对所述目标终端在每一种审计维度下的恶意分值进行加权处理
S208
对加权处理后的各恶意分值进行求和计算，获得所述目标终端的恶意总分
S209
根据所述目标终端的恶意总分确定所述目标终端的类型
S210
若所述目标终端为安全终端则对所述目标通信帐号进行解封处理，若所述目标终端为恶意终端则驳回所述解封请求
S211

图2

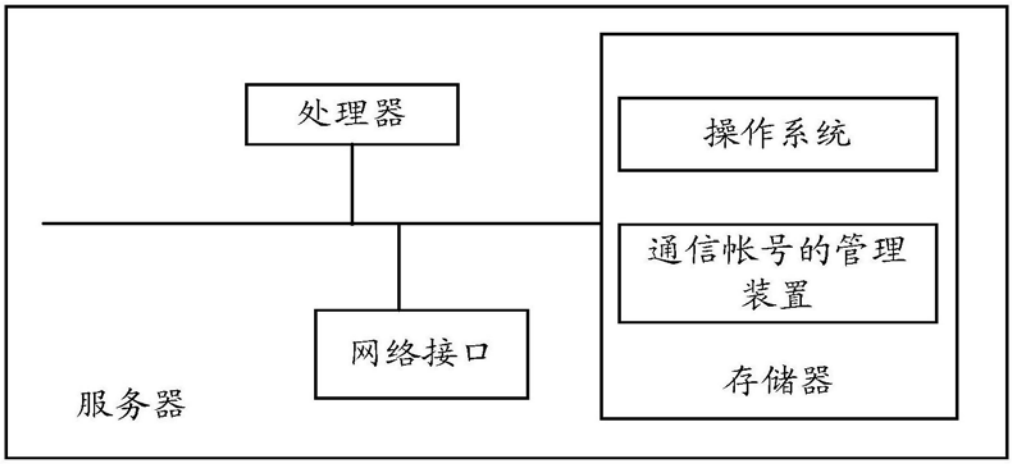


图3

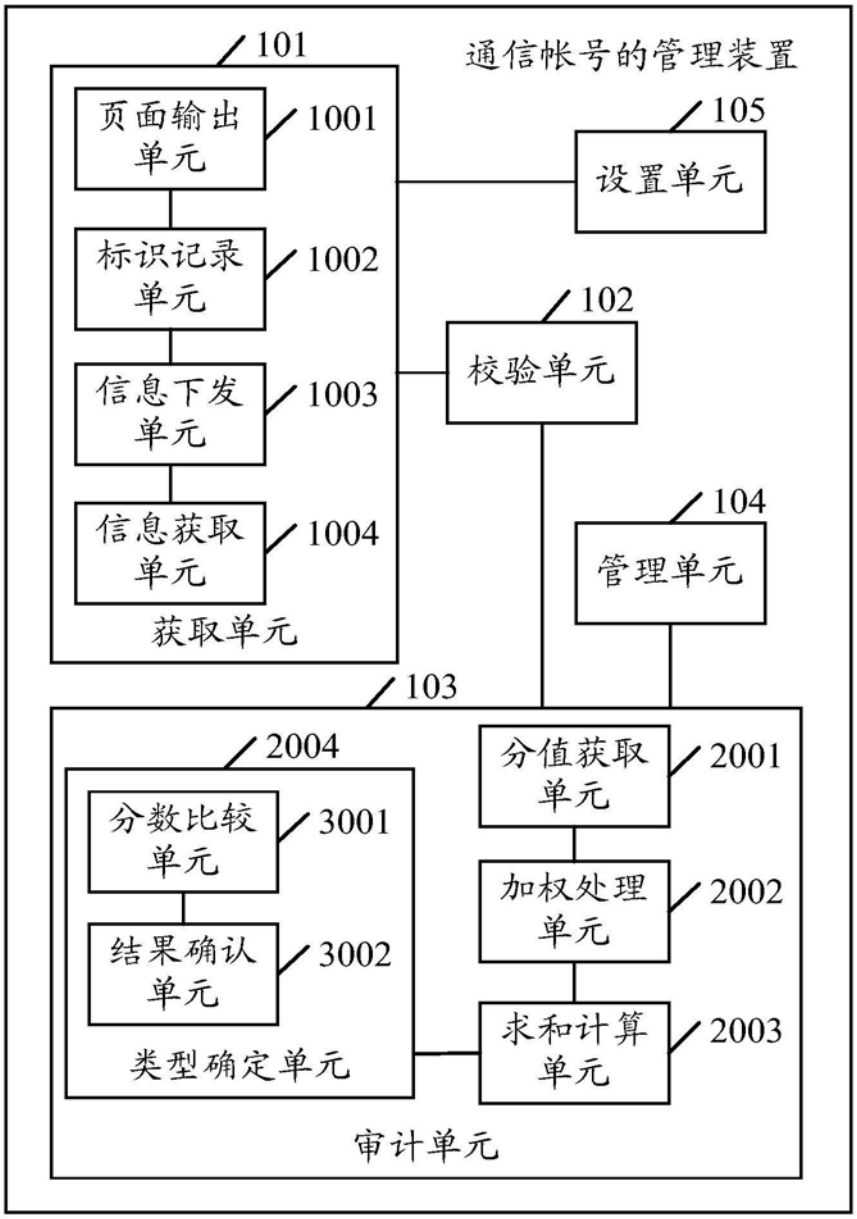

通信帐号的管理装置
101
页面输出单元
1001
标识记录单元
1002
信息下发单元
1003
信息获取单元
1004
获取单元
105
设置单元
102
校验单元
104
管理单元
103
2004
分数比较单元
3001
结果确认单元
3002
类型确定单元
分值获取单元
2001
加权处理单元
2002
求和计算单元
2003
审计单元

图4