(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 114372295 A
(43)申请公布日 2022.04.19

(21)申请号 202111654366.7

(22)申请日 2021.12.30

(71)申请人 天翼物联科技有限公司
地址 510335 广东省广州市海珠区阅江西路366号广报中心南塔21层

(72)发明人 俞昊天 王亚磊 王一鸣 吕高锋 恽天翔

(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
代理人 郑宏谋

(51)Int.Cl.
G06F 21/64(2013.01)
G06F 11/14(2006.01)

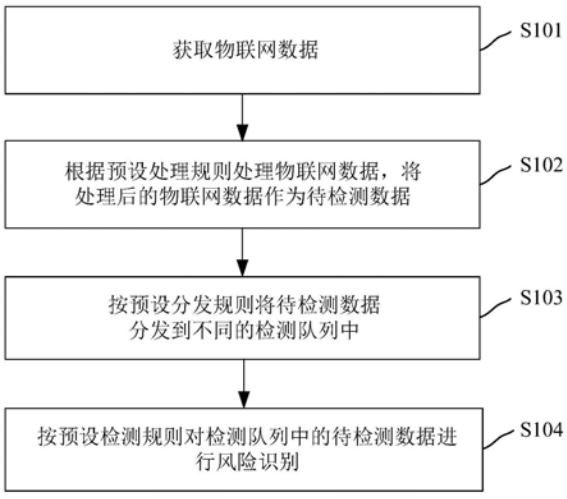
权利要求书2页 说明书10页 附图4页

(54)发明名称

一种检测物联网卡安全风险的方法、装置和存储介质

(57)摘要

本申请公开了一种检测物联网卡安全风险的方法，所述方法包括：获取物联网数据；根据预设处理规则处理所述物联网数据，将处理后的所述物联网数据作为待检测数据；按预设分发规则将所述待检测数据分发到不同的检测队列中；按预设检测规则对所述检测队列中的待检测数据进行风险识别。本申请通过将风险处理任务分发到不同队列检测的方法，能够在物联网出现安全风险时及时检测并作出相应的响应，提高物联网安全性。



CN 114372295 A

1.一种检测物联网卡安全风险的方法,其特征在于,所述方法包括:

获取物联网数据;

根据预设处理规则处理所述物联网数据,将处理后的所述物联网数据作为待检测数据;

按预设分发规则将所述待检测数据分发到不同的检测队列中;

按预设检测规则对所述检测队列中的待检测数据进行风险识别。

2.根据权利要求1所述的一种检测物联网卡安全风险的方法,其特征在于,所述根据预设处理规则处理所述物联网数据,包括:

对所述物联网数据进行解码,得到用户资料表和风险资料表;

对所述用户资料表和风险资料表进行同步处理和数据增强处理,其中,所述数据增强包括根据所述用户资料表增加所述物联网数据的获取量。

3.根据权利要求2所述的一种检测物联网卡安全风险的方法,其特征在于,所述对所述物联网数据进行解码,包括:

对所述物联网数据进行ASN.1解码。

4.根据权利要求1所述的一种检测物联网卡安全风险的方法,其特征在于,所述按预设分发规则将所述待检测数据分发到不同的检测队列中,包括:

按照所述物联网数据的用户资料表和风险资料表归属的类别匹配对应的检测队列;

将所述待检测数据分发到对应的检测队列中。

5.根据权利要求1所述的一种检测物联网卡安全风险的方法,其特征在于,所述检测队列至少包括以下之一:机卡分离监测队列、疑似手机终端监测队列、跨地区使用监测队列、短信超出套餐监测队列、超白名单使用监测队列、异常流量监测队列、异常短信使用监测队列、漫游至诈骗高发区监测队列。

6.根据权利要求5所述的一种检测物联网卡安全风险的方法,其特征在于,所述机卡分离监测队列的监测方法包括:

判断机卡绑定生效的用户信息和绑定的IMEI号对应的用户信息是否一致,若不一致,则确定所述物联网数据存在机卡分离安全风险,其中,所述IMEI号从原始话单中获取。

7.根据权利要求1所述的一种检测物联网卡安全风险的方法,其特征在于,所述按预设检测规则对所述检测队列中的待检测数据进行风险识别,包括:

按所述检测队列的优先级顺序对所述待检测数据进行风险识别;

若确定所述待检测数据有安全风险,则将所述待检测数据发送至对应的风险处理队列。

8.根据权利要求1所述的一种检测物联网卡安全风险的方法,其特征在于,所述方法还包括:

通过主服务器对所述物联网数据中的用户资料表和风险资料表进行备份;

通过第一从服务器读取所述主服务器的备份数据,对所述备份数据进行二次备份;

通过第二从服务器检测所述主服务器和第一从服务器的备份是否异常,若所述主服务器和第一从服务器的备份异常,则将异常的备份信息缓存在flink集群任务中并通过aof和rdb文件进行恢复,并将异常的备份信息进行告警。

9.一种检测物联网卡安全风险的装置,其特征在于,所述装置包括:

第一模块，用于获取物联网数据；

第二模块，用于根据预设处理规则处理所述物联网数据，将处理后的所述物联网数据作为待检测数据；

第三模块，用于按预设分发规则将所述待检测数据分发到不同的检测队列中；

第四模块，用于按预设检测规则对所述检测队列中的待检测数据进行风险识别。

10.存储介质，其特征在于，所述存储介质存储有处理器可执行的程序，所述处理器可执行的程序被处理器执行时实现如权利要求1-8中任一项所述的检测物联网卡安全风险的方法。

一种检测物联网卡安全风险的方法、装置和存储介质

技术领域

[0001] 本申请涉及物联网领域，尤其是一种检测物联网卡安全风险的方法、装置和存储介质。

背景技术

[0002] 物联网是新一代信息技术的重要组成部分，物联网应用呈现增长态势，而安全性对物联网的运行和发展十分重要。当前的物联网技术面临着网络安全、个人隐私安全、终端设备安全、人身安全等多种安全问题，并且当物联网出现安全风险时难以及时检测并作出相应的响应，导致物联网安全性较低。

[0003] 因此，相关技术存在的上述技术问题亟待解决。

发明内容

[0004] 本申请旨在解决相关技术中的技术问题之一。为此，本申请实施例提供一种检测物联网卡安全风险的方法、装置和存储介质，能够及时检测物联网安全风险并作出相应的响应，提高物联网的安全性。

[0005] 根据本申请实施例一方面，提供一种检测物联网卡安全风险的方法，所述方法包括：

[0006] 获取物联网数据；

[0007] 根据预设处理规则处理所述物联网数据，将处理后的所述物联网数据作为待检测数据；

[0008] 按预设分发规则将所述待检测数据分发到不同的检测队列中；

[0009] 按预设检测规则对所述检测队列中的待检测数据进行风险识别。

[0010] 在其中一个实施例中，所述根据预设处理规则处理所述物联网数据，包括：

[0011] 对所述物联网数据进行解码，得到用户资料表和风险资料表；

[0012] 对所述用户资料表和风险资料表进行同步处理和数据增强处理，其中，所述数据增强包括根据所述用户资料表增加所述物联网数据的获取量。

[0013] 在其中一个实施例中，所述对所述物联网数据进行解码，包括：

[0014] 对所述物联网数据进行ASN.1解码。

[0015] 在其中一个实施例中，所述按预设分发规则将所述待检测数据分发到不同的检测队列中，包括：

[0016] 按照所述物联网数据的用户资料表和风险资料表归属的类别匹配对应的检测队列；

[0017] 将所述待检测数据分发到对应的检测队列中。

[0018] 在其中一个实施例中，所述检测队列至少包括以下之一：机卡分离监测队列、疑似手机终端监测队列、跨地区使用监测队列、短信超出套餐监测队列、超白名单使用监测队列、异常流量监测队列、异常短信使用监测队列、漫游至诈骗高发区监测队列。

[0019] 在其中一个实施例中，所述机卡分离监测队列的监测方法包括：

[0020] 判断机卡绑定生效的用户信息和绑定的IMEI号对应的用户信息是否一致，若不一致，则确定所述物联网数据存在机卡分离安全风险，其中，所述IMEI号从原始话单中获取。

[0021] 在其中一个实施例中，所述按预设检测规则对所述检测队列中的待检测数据进行风险识别，包括：

[0022] 按所述检测队列的优先级顺序对所述待检测数据进行风险识别；

[0023] 若确定所述待检测数据有安全风险，则将所述待检测数据发送至对应的风险处理队列。

[0024] 在其中一个实施例中，所述方法还包括：

[0025] 通过主服务器对所述物联网数据中的用户资料表和风险资料表进行备份；

[0026] 通过第一从服务器读取所述主服务器的备份数据，对所述备份数据进行二次备份；

[0027] 通过第二从服务器检测所述主服务器和第一从服务器的备份是否异常，若所述主服务器和第一从服务器的备份异常，则将异常的备份信息缓存在flink集群任务中并通过aof和rdb文件进行恢复，并将异常的备份信息进行告警。

[0028] 根据本申请实施例一方面，提供一种检测物联网卡安全风险的装置，所述装置包括：

[0029] 第一模块，用于获取物联网数据；

[0030] 第二模块，用于根据预设处理规则处理所述物联网数据，将处理后的所述物联网数据作为待检测数据；

[0031] 第三模块，用于按预设分发规则将所述待检测数据分发到不同的检测队列中；

[0032] 第四模块，用于按预设检测规则对所述检测队列中的待检测数据进行风险识别。

[0033] 根据本申请实施例一方面，提供存储介质，所述存储介质存储有处理器可执行的程序，所述处理器可执行的程序被处理器执行时实现如前面实施例所述的检测物联网卡安全风险的方法。

[0034] 本申请实施例提供的一种检测物联网卡安全风险的方法的有益效果为：本申请通过获取物联网数据；根据预设处理规则处理所述物联网数据，将处理后的所述物联网数据作为待检测数据；按预设分发规则将所述待检测数据分发到不同的检测队列中；按预设检测规则对所述检测队列中的待检测数据进行风险识别。本申请将风险处理任务分发到不同队列再按规则进行风险识别的方法，能够在物联网出现安全风险时及时检测并作出相应的响应，提高物联网安全性。

[0035] 本申请的附加方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本申请的实践了解到。

附图说明

[0036] 为了更清楚地说明本申请实施例中的技术方案，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。

[0037] 图1为本申请实施例提供的一种检测物联网卡安全风险的方法的流程图；

[0038] 图2为本申请实施例根据预设处理规则处理所述物联网数据的流程图；

[0039] 图3为本申请实施例检测队列的种类示意图；

[0040] 图4为本申请实施例检测队列的检测过程示意图；

[0041] 图5为本申请实施例提供的备份方法流程图；

[0042] 图6为本申请实施例备份系统服务器分布示意图；

[0043] 图7为本申请实施例提供的一种检测物联网卡安全风险的装置的示意图。

具体实施方式

[0044] 为了使本技术领域的人员更好地理解本申请方案，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的实施例，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。

[0045] 本申请的说明书和权利要求书及附图中的术语“第一”、“第二”、“第三”和“第四”等是用于区别不同对象，而不是用于描述特定顺序。此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0046] 在本文中提及“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是，本文所描述的实施例可以与其它实施例相结合。

[0047] 物联网是新一代信息技术的重要组成部分，随着5G时代的来临，物联网应用呈现爆发式增长态势，基于物联网发起的基础设施攻击频发，物联网智能终端问题严峻。物联网已进入快车道，尤其是中国，已经是全球增速最快国家。在物联网领域，在实现NB-IoT全网商用部署，规模、覆盖、质量和应用范围都将居于业界领先地位；通过市将深耕智慧城市(公共服务、市政管理、基础设施)、垂直行业(制造、能源、车联网)和个人消费(可穿戴设备)等三类市场，2017年净增3000万物联网用户数，2018年用户过亿。这使得物联网面临网络安全、个人隐私安全、终端设备安全、人身安全等多种安全问题。由于物联网设备种类多、数量大且相互连接，必须加强对物联网安全的高度关注和警惕，使物联网业务安全风险可管可控。

[0048] 为了解决上述问题，本申请实施例提供一种检测物联网卡安全风险的方法，能够及时检测物联网安全风险并作出相应的响应，提高物联网的安全性。

[0049] 为方便阅读和理解，本说明书接下来对本申请实施例出现或可能出现的专业术语进行解释，具体如下：

[0050] 物联网：物联网(Internet of Things，简称IoT)是指通过各种信息传感器、射频识别技术、全球定位系统、红外感应器、激光扫描器等各种装置与技术，实时采集任何需要监控、连接、互动的物体或过程，采集其声、光、热、电、力学、化学、生物、位置等各种需要的

信息,通过各类可能的网络接入,实现物与物、物与人的泛在连接,实现对物品和过程的智能化感知、识别和管理。物联网是一个基于互联网、传统电信网等的信息承载体,它让所有能够被独立寻址的普通物理对象形成互联互通的网络。本实施例中的物联网泛指运营商平台与企业之间建立的物联网及物联网平台。

[0051] redis:redis是一个key-value存储系统。和Memcached类似,它支持存储的value类型相对更多,包括string(字符串)、list(链表)、set(集合)、zset(sorted set--有序集合)和hash(哈希类型)。这些数据类型都支持push/pop、add/remove及取交集并集和差集及更丰富的操作,而且这些操作都是原子性的。在此基础上,redis支持各种不同方式的排序。与memcached一样,为了保证效率,数据都是缓存在内存中。区别的是redis会周期性的把更新的数据写入磁盘或者把修改操作写入追加的记录文件,并且在此基础上实现了master-slave(主从)同步。

[0052] ASN.1解码:在电信和计算机网络领域,ASN.1(Abstract Svntax Noiation one)是一套标准,是街达数据的表示编码传输、解码的灵活的记法,提供了一套正式、无歧义和精确的规则以指达独立于待定计算机硬件的对爱结构。ASN.1包括几个标准化编码规则,如基本编码规则(BER).209」(CER》、识别名編码规则(DER)、压缩规则」(PER)和XML得码规则(XER)。这些规则描达了如何对ASN.1中定义的数值进行解码,以便用于传输,而不管计算机、缤程语言或它在应用程序中如何表示等因素。ASN.1的解码方法比许多与之相竞争的标记系统更先进,它支持可扩展信息快速可靠的传输一在无线亮带中。ASN.1已经成为了一种国际际准,它的編码规则已经成熟并在可靠性和兼容性方面拥有更丰富的历程。简洁的二选制编码规则(BER、CER、DER、PER,但不包括XER)可作更现代的替代。

[0053] IMEI号:国际移动设备识别码(International Mobile Equipment Identity,IMEI),即通常所说的手机序列号、手机“串号”,用于在移动电话网络中识别每一部独立的手机等移动通信设备,相当于移动电话的身份证。序列号共有15～17位数字,前8位(TAC)是型号核准号码(早期为6位),是区分手机品牌和型号的编码。接着2位(FAC)是最后装配号(仅在早期机型中存在),代表最终装配地代码。后6位(SNR)是串号,代表生产顺序号。国际移动设备识别码一般贴于机身背面与外包装上,同时也存在于手机存储器中,通过在手机拨号键盘中输入*#06#即可查询。

[0054] MQTT通信协议:MQTT(Message Queuing Telemetry Transport,消息队列遥测传输协议),是一种基于发布/订阅(publish/subscribe)模式的"轻量级"通讯协议,该协议构建于TCP/IP协议上,由IBM在1999年发布。MQTT最大优点在于,可以以极少的代码和有限的带宽,为连接远程设备提供实时可靠的消息服务。作为一种低开销、低带宽占用的即时通讯协议,使其在物联网、小型设备、移动应用等方面有较广泛的应用。MQTT是一个基于客户端-服务器的消息发布/订阅传输协议。MQTT协议是轻量、简单、开放和易于实现的,这些特点使它适用范围非常广泛。在很多情况下,包括受限的环境中,如:机器与机器(M2M)通信和物联网(IoT)。其在,通过卫星链路通信传感器、偶尔拨号的医疗设备、智能家居、及一些小型化设备中已广泛使用。

[0055] RDB:关系数据库(Relational Database,RDB),关系数据库就是基于关系型的数据库,是利用数据库进行数据组织的一种方式,是现代的数据库管理系统中应用最为普遍的一种,也是最有效的数据组织形式之一。RDB文件中存储的是数据。

[0056] AOF:Redis是内存数据库,所以持久化是必须的,redis提供RDB和AOF两种持久化方案,AOF即Append Only File,文件中存储的是写操作命令。

[0057] 图1为本申请实施例提供的一种检测物联网卡安全风险的方法的流程图,如图1所示,本申请实施例提供的一种检测物联网卡安全风险的方法具体包括:

[0058] S101、获取物联网数据。

[0059] 本步骤中,获取的物联网数据包括以下内容:用户资料表,包括用户开通的限制业务信息、待检测业务套餐信息、用户相关的ID关联信息;风险资料维表,包括基站与省份、地市对应关系表、诈骗高风险地区、基站表、终端IMEI型号对应关系表、用户销售地维表。获取物联网数据中的上述列表的作用在于为后续步骤提供数据基础和数据支持。

[0060] 需要说明,本步骤中获取物联网数据的方法和途径可以是通过无线信道从服务器或数据库中获取,也可以通过有线连接从数据库或数据存储设备中获取,本说明书不对此进行不当限定。

[0061] S102、根据预设处理规则处理所述物联网数据,将处理后的所述物联网数据作为待检测数据。

[0062] 在步骤S102中,所述按预设分发规则将所述待检测数据分发到不同的检测队列中具体可以包括:按照物联网数据的用户资料表和风险资料表归属的类别匹配对应的检测队列;将所述待检测数据分发到对应的检测队列中。其中,物联网数据的用户资料表和风险资料表可以从前述步骤获取的物联网数据解码得到,通过对物联网数据进行解码提取其中的用户资料表和风险资料表,之后根据物联网数据的类型匹配对应的检测队列。

[0063] S103、按预设分发规则将所述待检测数据分发到不同的检测队列中。

[0064] S104、按预设检测规则对所述检测队列中的待检测数据进行风险识别。

[0065] 在步骤S104中,所述按预设检测规则对所述检测队列中的待检测数据进行风险识别,包括:按所述检测队列的优先级顺序对所述待检测数据进行风险识别;若确定所述待检测数据有安全风险,则将所述待检测数据发送至对应的风险处理队列。

[0066] 此外,本申请实施例还包括对物联网数据进行实时维护的方法,具体包括:对redis中的用户资料表与风险资料维表数据进行实时更新与维护,数据非常重要,定期的进行数据备份并支持高可靠的数据恢复机制,确保redis集群或系统异常时候,具备快速恢复以及数据完整的能力。

[0067] 可选地,针对上述实施例的根据预设处理规则处理所述物联网数据,图2为本申请实施例根据预设处理规则处理所述物联网数据的流程图,如图2所示,具体如下:

[0068] S201、对所述物联网数据进行解码,得到用户资料表和风险资料表。

[0069] 在步骤S201中,对得到的物联网数据进行解码的过程包括:设置一个前置处理模块,前置处理模块对五梁湾数据进行前置解码,对各个话单进行接收、解码,并送回实时队列中。前置解码的过程包括一般解码以及ASN.1解码,其中,ASN.1解码用于对实时流量、实时语音与实时短信、CRM和DCP的数据进行解码。通过前置解码后,能够得到本实施例所需要的用户资料表和风险资料表,并将得到的用户资料表和风险资料表存储在对应的区域备用。

[0070] S202、对所述用户资料表和风险资料表进行同步处理和数据增强处理,其中,所述数据增强包括根据所述用户资料表增加所述物联网数据的获取量。

[0071] 需要说明的是，本实施例中对所述用户资料表和风险资料表进行同步处理和数据增强处理可以包括：对待检测的用户进行数据增强，是根据用户待检测项目进行针对性的增加待检测的条件数据，如短信超套餐检测，会在处理后的用户话单数据后增加短信套餐数据；本实施例中对所述用户资料表和风险资料表进行同步处理和数据增强处理还可以包括：设置一个前置处理模块，前置处理模块对五梁湾数据进行前置解码，对各个话单进行接收、解码，并送回实时队列中。前置解码的过程包括一般解码以及ASN.1解码，其中，ASN.1解码用于对实时流量、实时语音与实时短信、CRM和DCP的数据进行解码。

[0072] 需要说明的是，本实施例中通过按预设分发规则将所述待检测数据分发到不同的检测队列中，图3为本申请实施例检测队列的种类示意图，如图3所示，不同的检测队列具体可以包括：机卡分离监测队列、疑似手机终端监测队列、跨地区使用监测队列、短信超出套餐监测队列、超白名单使用监测队列、异常流量监测队列、异常短信使用监测队列、漫游至诈骗高发区监测队列。需要说明，本说明书列举了上述八种检测队列的种类，不代表本实施例提出的检测物联网卡安全风险的方法仅能使用上述八种检测队列，出本实施例提出的八种检测队列外的其他检测队列也属于本申请提出的检测物联网卡安全风险的方法中的检测队列，本说明书不对此构成不当限定。

[0073] 图4为本申请实施例检测队列的检测过程示意图，如图4所示，本申请实施例中的机卡分离监测队列、疑似手机终端监测队列、跨地区使用监测队列、短信超出套餐监测队列、超白名单使用监测队列、异常流量监测队列、异常短信使用监测队列、漫游至诈骗高发区监测队列的具体工作流程如下所示：

[0074] 具体地，本实施例中的机卡分离风险点检测具有第一优先级，判断条件为判断出机卡绑定生效的用户和对应绑定的IMEI号；根据原始话单中最新IMEI记录，识别出IMEI不一致的情况记录下来。

[0075] 具体地，本实施例中的疑似手机终端风险点检测具有第二优先级，判断条件为结合CRM实时资料库，识别除定向访问、NB、拆机、停机、黑名单限制用户。剩余用户根据原始话单中的IMEI，实时识别是否手机终端。

[0076] 具体地，本实施例中的漫游至诈骗高发区使用风险点检测具有第三优先级3，判断条件为实时监控漫游至公安17个诈骗区域，且销售市与使用市(如公安区域为区县，则找出其地市)不一致的用户，(业务提供基站对应关系表)。

[0077] 具体地，本实施例中的超白名单使用风险点检测具有第四优先级，CRM语音、短信判断条件：根据CRM资料库判断语音短信出访入访内容；根据原始话单，判断语音短信是否超白名单(DCP语音、短信待确认)。

[0078] 具体地，本实施例中的跨地区使用风险点检测第五优先级，判断条件为结合CRM实时资料库，识别行业类型为(行业细类＝智能抄表、市政设施管理、安防监控、气象与环境监测)或开通区域限制用户，剔除测试期，建立用户+使用区域信息表；剩余用户根据原始话单识别区域是否出现跨省。

[0079] 具体地，本实施例中的异常流量使用量风险点检测具有第六优先级，判断条件为批处理计算出激活时间在3个月以上的卡，以及前三个月的月均流量；根据批价后详单计算当月累计1流量是否大于前三个月的月均流量2倍以上。

[0080] 具体地，本实施例中的异常短信使用量风险点检测第七优先级，判断条件为批处

理计算出激活时间在3个月以上的卡,以及前三个月的月均短信条数;根据批价后详单计算当月累计短信条数是否大于前三个月的月均条数2倍以上。

[0081] 具体地,本实施例中的超出短信使用量风险点检测具有第八优先级,判断条件为根据CRM资料库判断短信套餐信息,识别出号码+套餐内短信条数;根据批价后话单,判断短信条数是否超套。

[0082] 图5为本申请实施例提供的备份方法流程图,如图5所示,本申请实施例还提供一种物联网卡安全检测时的备份方法,具体为:

[0083] S501、通过主服务器对所述物联网数据中的用户资料表和风险资料表进行备份。

[0084] S502、通过第一从服务器读取所述主服务器的备份数据,对所述备份数据进行二次备份。

[0085] S503、通过第二从服务器检测所述主服务器和第一从服务器的备份是否异常。

[0086] S504、若所述主服务器和第一从服务器的备份异常,则将异常的备份信息缓存在flink集群任务中并通过aof和rdb文件进行恢复,并将异常的备份信息进行告警。

[0087] 本实施例提供了一种用户资料表与风险资料表备份与恢复机制,redis集群支持RDB和AOF机制将内存中的数据定期、准实时的写入到磁盘中。当redis集群异常宕机后,可通过磁盘上的RDB和AOF文件进行恢复,RDB文件可定期转移到其他非redis主机或者大数据平台实现异地备份。

[0088] 需要说明的是,RDB持久化与AOF持久化的优缺点如下:

[0089] RDB持久化的优点:RDB方式备份,整个Redis数据库最终备份成一个文件,这对于文件备份而言是完美的(方便管理、还原、压缩、转储);对服务进程影响最小,唯一需要做的是fork出子进程,之后所有的持久化工作交由子进程处理;相比于AOF机制,如果数据量比较大,RDB的启动效率会更高(记录的是源数据,而非数据操作)。

[0090] RDB持久化的缺点:数据的可用性得不到太大的保障,如果在定时持久化之前出现宕机现象,此前没来得及写入磁盘的数据都将丢失;如果数据量较大,fork子进程的操作可能会使服务短暂停止(通常是几百毫秒)。

[0091] AOF持久化的优点:拥有更高的数据可用性,数据持久化最完整;日志文件采用append模式,即使在写入过程中出现宕机现象,也不会破坏日志文件之前已经存在的内容;提供rewrite机制,当日志过大时,Redis以append模式不断将修改的日志写入老的磁盘文件,同时Redis还会创建一个新的文件用于记录此期间有哪些命令被执行。

[0092] AOF持久化的缺点:对于相同数量的数据,AOF文件通常大于RDB文件,RDB文件在恢复大数据集的速度比AOF恢复的更快(RDB省去了执行的步骤,直接导入源数据)。

[0093] 因此,RDB持久化,性能更好(所有操作均由子进程处理,主进程不进行任何IO操作),数据一致性一般。AOF持久化,数据一致性更好,性能一般(记录操作日志,写入日志和执行日志恢复数据的时间都比RDB更长)。因此,单独采用RDB和AOF方式进行持久化都会存在相应的问题。采用如下方案:redis集群采用主从配置,1主2从服务器,具体为:

[0094] (1)配置1台主节点服务器在redis集群的master节点同时是配置RDB与AOF持久化,RDB持久化每小时或每2小时执行,并将RDB文件传输到其他服务器进行异地备份。如果redis集群出现问题,先使用aof文件进行恢复,或结合rdb文件进行恢复。主节点只负责写入操作。

[0095] (2)配置2台从节点,每秒钟从主服务器同步数据。从服务只负责数据读取。

[0096] (3)后台配置一个异常任务检测脚本,通过定期扫描我们的任务表发现在运行的任务是否发生异常,对于出现异常而挂起的任务,检测任务会将任务信息写入短信告警表中,通过发短信给运维与支撑人员进行处理。

[0097] 当redis集群出现异常后,实时任务挂起,数据会缓存在flink集群任务中。可通过redis的aof和rdb文件进行恢复,恢复后启用redis集群flink任务可继续运行。

[0098] 更多地,本说明书还提供了图6解释说明多个服务器之间在进行备份恢复时的工作关系示意图。图6为本申请实施例备份系统服务器分布示意图,如图6所示,在Redis集群中,主服务器分别与第一服务器和第二服务器连接,主服务器的作用在于通过RDB持久化和AOF持久化对备份的文件进行恢复。

[0099] 本实施例还提供了一种检测物联网卡安全风险的装置,如图7所示,所述装置包括:第一模块701,用于获取物联网数据;第二模块702,用于根据预设处理规则处理所述物联网数据,将处理后的所述物联网数据作为待检测数据;第三模块703,用于按预设分发规则将所述待检测数据分发到不同的检测队列中;第四模块704,用于按预设检测规则对所述检测队列中的待检测数据进行风险识别。

[0100] 可见,上述方法实施例中的内容均适用于本装置实施例中,本装置实施例所具体实现的功能与上述方法实施例相同,并且达到的有益效果与上述方法实施例所达到的有益效果也相同。

[0101] 本实施例还提供了一种存储介质,所述存储介质存储有处理器可执行的程序,所述处理器可执行的程序被处理器执行时实现如前面实施例所述的检测物联网卡安全风险的方法。

[0102] 上述的方法实施例中的内容均适用于本存储介质实施例中,本存储介质实施例所具体实现的功能与上述的方法实施例相同。

[0103] 同理,上述方法实施例中的内容均适用于本存储介质实施例中,本存储介质实施例所具体实现的功能与上述方法实施例相同,并且达到的有益效果与上述方法实施例所达到的有益效果也相同。

[0104] 在一些可选择的实施例中,在方框图中提到的功能/操作可以不按照操作示图提到的顺序发生。例如,取决于所涉及的功能/操作,连续示出的两个方框实际上可以被大体上同时地执行或方框有时能以相反顺序被执行。此外,在本申请的流程图中所呈现和描述的实施例以示例的方式被提供,目的在于提供对技术更全面的理解。所公开的方法不限于本文所呈现的操作和逻辑流程。可选择的实施例是可预期的,其中各种操作的顺序被改变以及其中被描述为较大操作的一部分的子操作被独立地执行。

[0105] 此外,虽然在功能性模块的背景下描述了本申请,但应当理解的是,除非另有相反说明,功能和/或特征中的一个或多个可以被集成在单个物理装置和/或软件模块中,或者一个或多个功能和/或特征可以在单独的物理装置或软件模块中被实现。还可以理解的是,有关每个模块的实际实现的详细讨论对于理解本申请是不必要的。更确切地说,考虑到在本文中公开的装置中各种功能模块的属性、功能和内部关系的情况下,在工程师的常规技术内将会了解该模块的实际实现。因此,本领域技术人员运用普通技术就能够在无需过度试验的情况下实现在权利要求书中所阐明的本申请。还可以理解的是,所公开的特定概念

仅仅是说明性的，并不意在限制本申请的范围，本申请的范围由所附权利要求书及其等同方案的全部范围来决定。

[0106] 功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。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或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，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，服务器，或者网络设备等)执行本申请各个实施例方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0107] 在流程图中表示或在此以其他方式描述的逻辑和/或步骤，例如，可以被认为是用于实现逻辑功能的可执行指令的定序列表，可以具体实现在任何计算机可读介质中，以供指令执行系统、装置或设备(如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统)使用，或结合这些指令执行系统、装置或设备而使用。就本说明书而言，“计算机可读介质”可以是任何可以包含、存储、通信、传播或传输程序以供指令执行系统、装置或设备或结合这些指令执行系统、装置或设备而使用的装置。

[0108] 计算机可读介质的更具体的示例(非穷尽性列表)包括以下：具有一个或多个布线的电连接部(电子装置)，便携式计算机盘盒(磁装置)，随机存取存储器(RAM)，只读存储器(ROM)，可擦除可编辑只读存储器(EPROM或闪速存储器)，光纤装置，以及便携式光盘只读存储器(CDROM)。另外，计算机可读介质甚至可以是可在其上打印程序的纸或其他合适的介质，因为可以例如通过对纸或其他介质进行光学扫描，接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得程序，然后将其存储在计算机存储器中。

[0109] 应当理解，本申请的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列(PGA)，现场可编程门阵列(FPGA)等。

[0110] 在本说明书的上述描述中，参考术语“一个实施方式/实施例”、“另一实施方式/实施例”或“某些实施方式/实施例”等的描述意指结合实施方式或示例描述的具体特征、结构、材料或者特点包含于本申请的至少一个实施方式或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施方式或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施方式或示例中以合适的方式结合。

[0111] 尽管已经示出和描述了本申请的实施方式，本领域的普通技术人员可以理解：在不脱离本申请的原理和宗旨的情况下可以对这些实施方式进行多种变化、修改、替换和变型，本申请的范围由权利要求及其等同物限定。

[0112] 以上，以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改

或者替换,并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

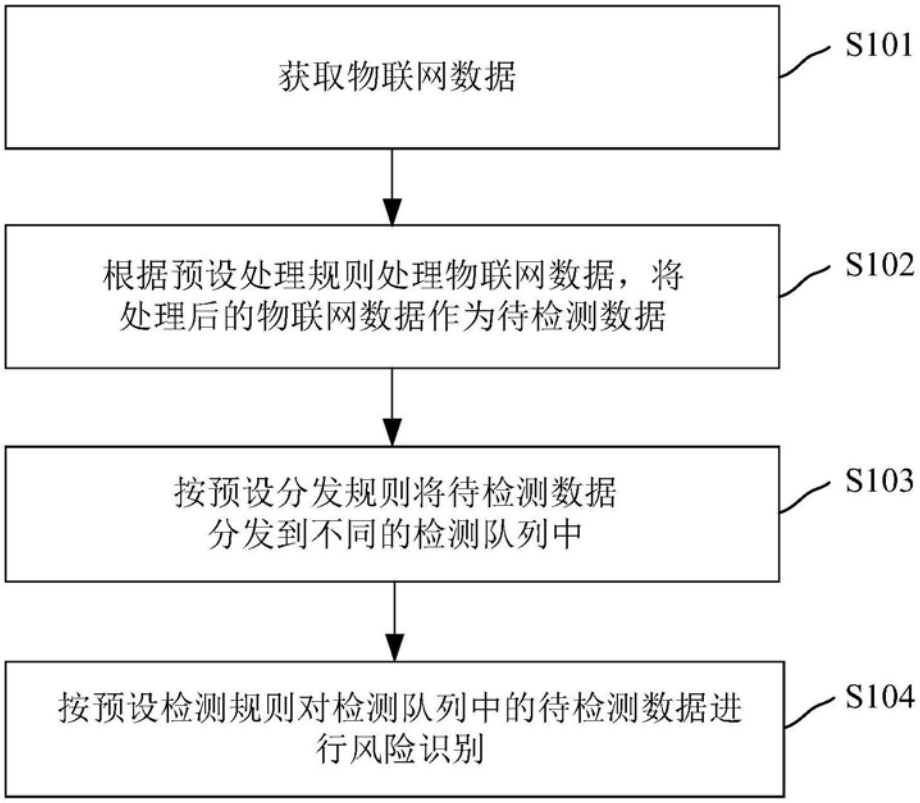

获取物联网数据
S101
根据预设处理规则处理物联网数据，将处理后的物联网数据作为待检测数据
S102
按预设分发规则将待检测数据分发到不同的检测队列中
S103
按预设检测规则对检测队列中的待检测数据进行风险识别
S104

图1

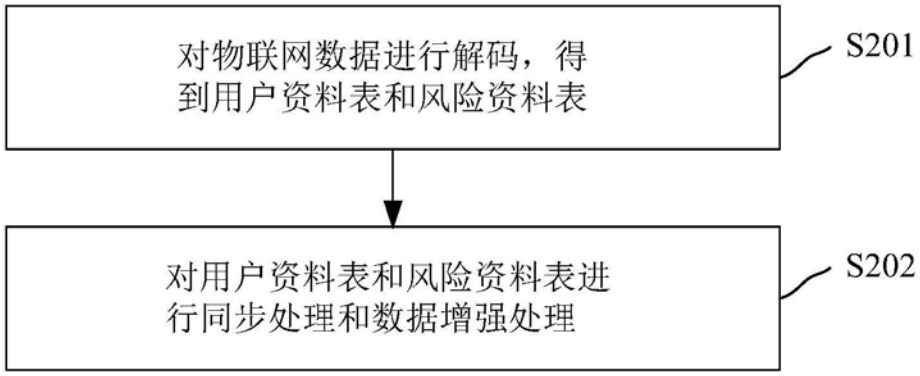

对物联网数据进行解码，得到用户资料表和风险资料表
S201
对用户资料表和风险资料表进行同步处理和数据增强处理
S202

图2

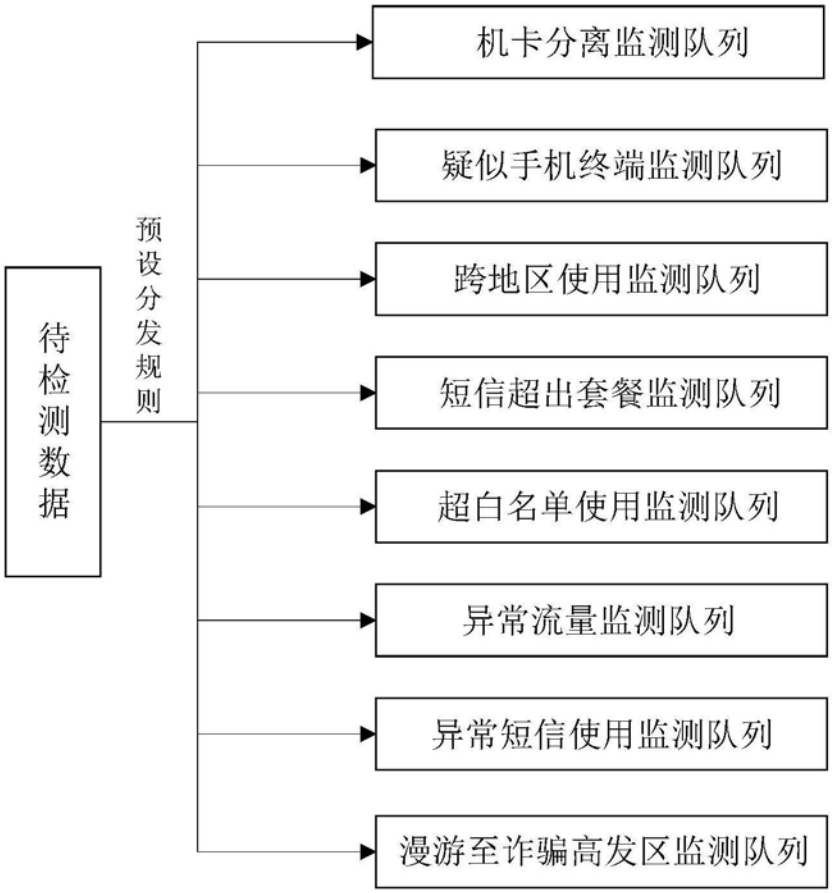

待检测数据
预设分发规则
机卡分离监测队列
疑似手机终端监测队列
跨地区使用监测队列
短信超出套餐监测队列
超白名单使用监测队列
异常流量监测队列
异常短信使用监测队列
漫游至诈骗高发区监测队列

图3

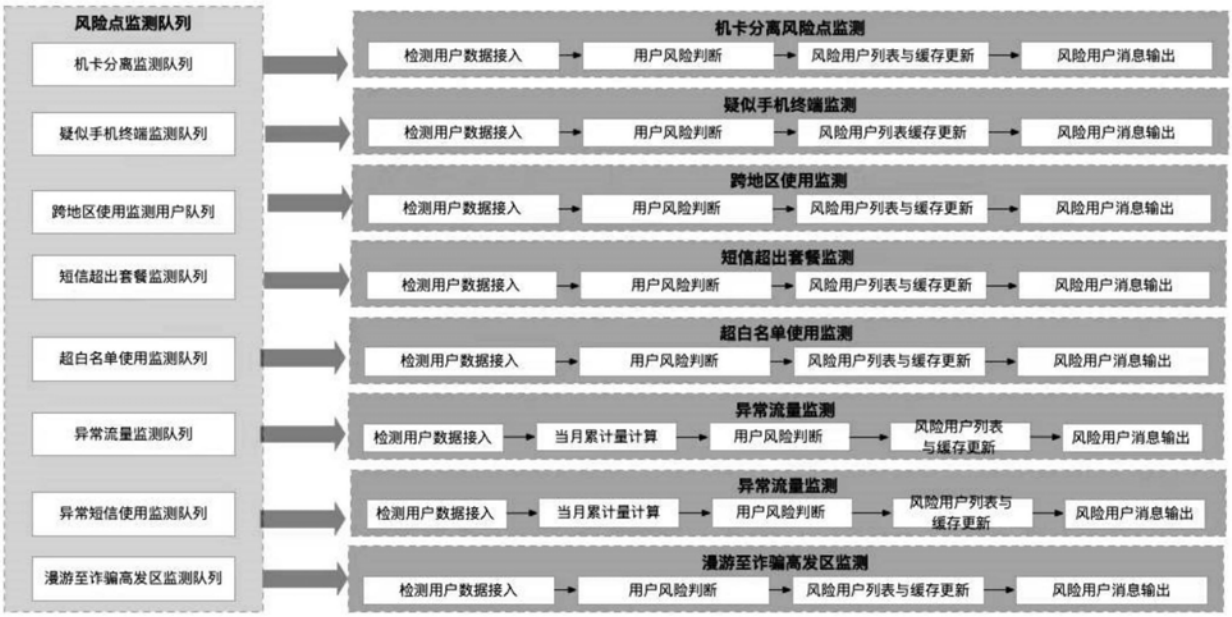

风险点监测队列
机卡分离监测队列
疑似手机终端监测队列
跨地区使用监测用户队列
短信超出套餐监测队列
超白名单使用监测队列
异常流量监测队列
异常短信使用监测队列
漫游至诈骗高发区监测队列
机卡分离风险点监测
检测用户数据接入
用户风险判断
风险用户列表与缓存更新
风险用户消息输出
疑似手机终端监测
检测用户数据接入
用户风险判断
风险用户列表缓存更新
风险用户消息输出
跨地区使用监测
检测用户数据接入
用户风险判断
风险用户列表与缓存更新
风险用户消息输出
短信超出套餐监测
检测用户数据接入
用户风险判断
风险用户列表与缓存更新
风险用户消息输出
超白名单使用监测
检测用户数据接入
用户风险判断
风险用户列表与缓存更新
风险用户消息输出
异常流量监测
检测用户数据接入
当月累计量计算
用户风险判断
风险用户列表与缓存更新
风险用户消息输出
异常流量监测
检测用户数据接入
当月累计量计算
用户风险判断
风险用户列表与缓存更新
风险用户消息输出
漫游至诈骗高发区监测
检测用户数据接入
用户风险判断
风险用户列表与缓存更新
风险用户消息输出

图4

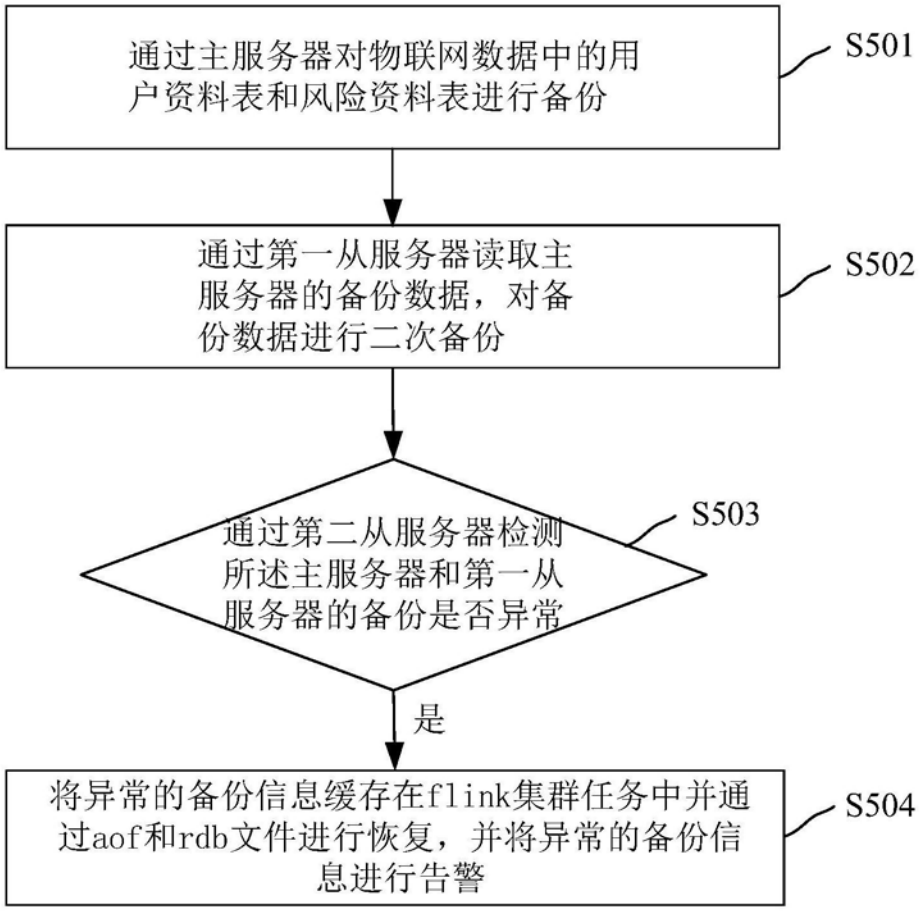

通过主服务器对物联网数据中的用户资料表和风险资料表进行备份
S501
通过第一从服务器读取主服务器的备份数据，对备份数据进行二次备份
S502
通过第二从服务器检测所述主服务器和第一从服务器的备份是否异常
S503
是
将异常的备份信息缓存在flink集群任务中并通过aof和rdb文件进行恢复，并将异常的备份信息进行告警
S504

图5

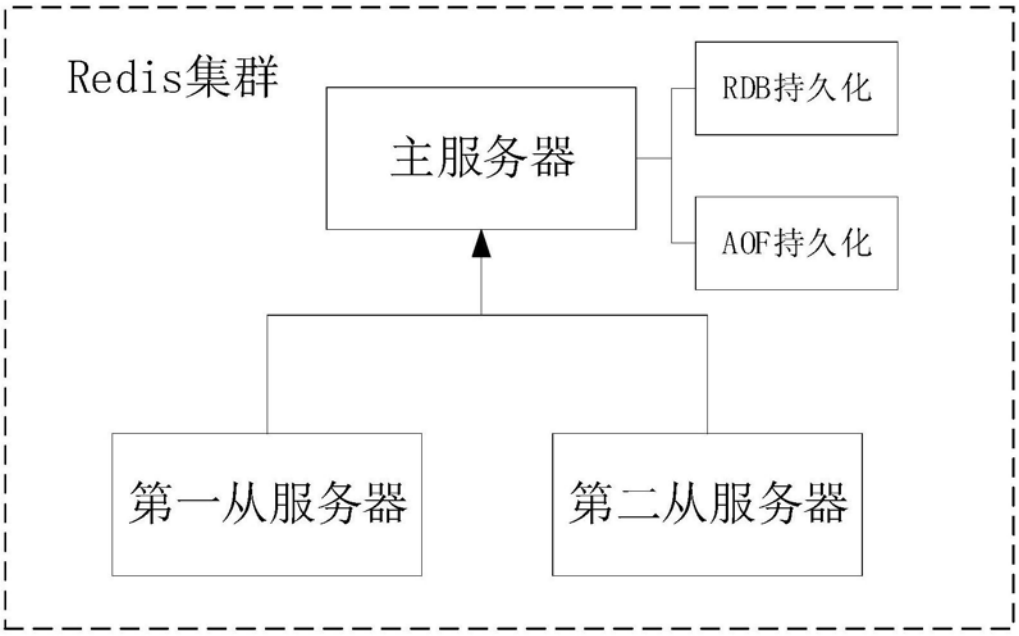

Redis集群
主服务器
RDB持久化
AOF持久化
第一从服务器
第二从服务器

图6

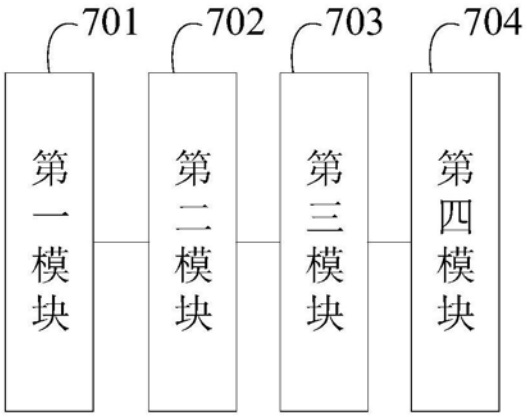


图7