



(12) 发明专利

(10) 授权公告号 CN 110635966 B

(45) 授权公告日 2022.09.09

(21) 申请号 201910768875.9

H04L 43/0876 (2022.01)

(22) 申请日 2019.08.20

审查员 陈雨姗

(65) 同一申请的已公布的文献号

申请公布号 CN 110635966 A

(43) 申请公布日 2019.12.31

(73) 专利权人 华能四川能源开发有限公司

地址 610000 四川省成都市武侯区人民南路四段47号华能大厦

(72) 发明人 延帅 李太斌 张冲 颜天成

(74) 专利代理机构 南京禹为知识产权代理事务

所(特殊普通合伙) 32272

专利代理师 康伟

(51) Int. Cl.

H04L 43/04 (2022.01)

H04L 43/045 (2022.01)

权利要求书2页 说明书8页 附图1页

(54) 发明名称

一种流量数据的可视化展示系统、方法、介质和电子设备

(57) 摘要

本发明提供了一种流量数据的可视化展示系统、方法、介质和电子设备,该系统包括:流量数据收集单元,用于从流量缓存中间件的缓存队列中消费第一流量数据,将第一流量数据转换为符合预设数据格式类型的第二流量数据,并将第二流量数据批量插入时序数据库中;流量统计服务单元,用于根据检索请求接入至对应的第二流量数据的统计接口,并根据检索请求从时序数据库中调取对应类型的第二流量数据,并对调取的第二流量数据进行统计,得到统计结果;可视化展示单元,用于对统计结果进行可视化展示。本公开通过引入可视化展示单元,对流量统计服务单元的统计结果进行可视化展示,可以更加直观地看到统计结果,提高了用户体验度。



1. 一种流量数据的可视化展示系统,其特征在于,包括:

流量缓存中间件,用于通过多个流量引擎收集流量数据,并将收集到的流量数据缓存至本地磁盘;

流量数据收集单元,用于从所述流量缓存中间件的缓存队列中消费第一流量数据,将所述第一流量数据转换为符合预设数据格式类型的第二流量数据,并将所述第二流量数据批量插入时序数据库中;

所述时序数据库,用于存储和管理所述流量数据收集单元转换得到的所述第二流量数据;

流量统计服务单元,用于根据检索请求接入至对应的所述时序数据库存储的第二流量数据的统计接口,并根据所述检索请求从所述时序数据库中调取对应类型的第二流量数据,并对调取的所述第二流量数据进行统计,得到统计结果,同时对接收到的流量数据进行分析,分析当前流量数据的数据格式,并根据不同流量数据的不同数据格式,选择与当前流量数据的数据格式匹配的可视化展示方式;

可视化展示单元,用于根据流量统计服务单元所选择的可视化展示方式对所述统计结果进行可视化展示;

获取单元,用于获取所述第二流量数据的格式类型信息;

其中,所述获取单元获取到的所述第二流量数据的所述数据格式类型信息至少包括:

属性名信息、类型信息、字段类型信息和对应的描述信息;

可视化展示单元还用于:

可视化展示所述第二流量数据的各项数据格式类型信息。

2. 根据权利要求 1 所述的系统,其特征在于,

通过所述可视化展示单元对所述第二流量数据的各项数据格式类型信息以地图展示的方式进行可视化展示。

3. 根据权利要求 1 所述的系统,其特征在于,

通过所述可视化展示单元对所述第二流量数据的各项数据格式类型信息以表格展示的方式进行可视化展示。

4. 根据权利要求 1 所述的系统,其特征在于,

通过所述可视化展示单元对所述第二流量数据的各项数据格式类型信息以图表展示的方式进行可视化展示。

5. 一种使用如权利要求 1-4 任一项所述的系统对流量数据进行可视化展示的方法,其特征在于,包括:

从所述流量缓存中间件的缓存队列中消费第一流量数据,将所述第一流量数据转换为符合预设数据格式类型的第二流量数据,并将所述第二流量数据批量插入所述时序数据库中;

对所述时序数据库中的所述第二流量数据进行分析,并分析出对应的数据格式类型信息;

根据所述数据格式类型信息,通过所述可视化展示单元对所述第二流量数据进行可视化展示;

其中,所述数据格式类型信息至少包括:

属性名信息、类型信息、字段类型信息和对应的描述信息。

6. 根据权利要求 5 所述的方法, 其特征在于,

通过所述可视化展示单元对所述第二流量数据的可视化展示方式至少包括:

以地图展示的方式、以表格展示的方式和以图表展示的方式。

7. 一种计算机可读存储介质, 其上存储有计算机程序, 其特征在于, 所述程序被处理器执行时实现如权利要求 1-4 所述的系统。

8. 一种电子设备, 其特征在于, 包括: 一个或多个处理器;

存储装置, 用于存储一个或多个程序, 当所述一个或多个程序被所述一个或多个处理器执行时, 使得所述一个或多个处理器实现如权利要求 1-4 所述的系统。

一种流量数据的可视化展示系统、方法、介质和电子设备

技术领域

[0001] 本发明涉及计算机技术领域,具体而言,涉及一种流量数据的可视化展示系统、方法、介质和电子设备。

背景技术

[0002] 工控系统面临着日益严峻的安全风险,工控安全已经提升到国家战略层面,如果可以对网络流量大数据进行有效的分析和存储,并对流量数据进行统计计算,进而利用可视化技术对流量数据进行展现,对整个工控网络设计优化、网络威胁的实时监测、以及安全事件的定位追溯都具有重要意义。

[0003] 传统的基于关系型数据库的schema设计往往基于确定的数据结构(属性列),无法满足针对灵活的不可预知属性的动态扩展存储,同时也无法满足对大数据集的复杂逻辑的聚合查询功能;目前比较流行的NOSQL数据库,如Redis,MongoDB等无法满足面对大数据集的聚合分析功能。

[0004] 由于网络流量数据量大、且统计方式与展现方式多样灵活等特征,因此,给流量数据的存储结构设计、统计检索性能、以及灵活易用的界面展现带来了挑战。因此,在长期的研发当中,发明人对流量展示方法进行了大量的研究,提出了一种流量展示方法,以解决上述技术问题之一。

发明内容

[0005] 本发明的目的在于提供一种流量数据的可视化展示系统、方法、介质和电子设备,能够解决上述提到的至少一个技术问题。具体方案如下:

[0006] 根据本发明的具体实施方式,第一方面,本公开提供一种流量数据的可视化展示系统,包括:

[0007] 流量缓存中间件,用于通过多个流量引擎收集流量数据,并将收集到的流量数据缓存至本地磁盘;

[0008] 流量数据收集单元,用于从所述流量缓存中间件的缓存队列中消费第一流量数据,将所述第一流量数据转换为符合预设数据格式类型的第二流量数据,并将所述第二流量数据批量插入所述时序数据库中;

[0009] 所述时序数据库,用于存储和管理所述流量数据收集单元转换得到的所述第二流量数据;

[0010] 流量统计服务单元,用于根据检索请求接入至对应的所述时序数据库存储的第二流量数据的统计接口,并根据所述检索请求从所述时序数据库中调取对应类型的第二流量数据,并对调取的所述第二流量数据进行统计,得到统计结果;

[0011] 可视化展示单元,用于对所述统计结果进行可视化展示。

[0012] 可选的,所述系统还包括:

[0013] 获取单元,用于获取所述第二流量数据的格式类型信息;

[0014] 其中,所述获取单元获取到的所述第二流量数据的所述数据格式类型信息至少包括:

[0015] 属性名信息、类型信息、字段类型信息和对应的描述信息。

[0016] 可选的,可视化展示单元还用于:

[0017] 可视化展示所述第二流量数据的各项数据格式类型信息。

[0018] 可选的,通过所述可视化展示单元对所述第二流量数据的各项数据格式类型信息以地图展示的方式进行可视化展示。

[0019] 可选的,通过所述可视化展示单元对所述第二流量数据的各项数据格式类型信息以表格展示的方式进行可视化展示。

[0020] 可选的,通过所述可视化展示单元对所述第二流量数据的各项数据格式类型信息以图表展示的方式进行可视化展示。

[0021] 根据本发明的具体实施方式,第二方面,本发明提供一种使用可视化展示系统对流量数据进行可视化展示的方法,包括:

[0022] 从所述流量缓存中间件的缓存队列中消费第一流量数据,将所述第一流量数据转换为符合预设数据格式类型的第二流量数据,并将所述第二流量数据批量插入所述时序数据库中;

[0023] 对所述时序数据库中的所述第二流量数据进行分析,并分析出对应的数据格式类型信息;

[0024] 根据所述数据格式类型信息,通过所述可视化展示单元对所述第二流量数据进行可视化展示;

[0025] 其中,所述数据格式类型信息至少包括:

[0026] 属性名信息、类型信息、字段类型信息和对应的描述信息。

[0027] 可选的,通过所述可视化展示单元对所述第二流量数据的可视化展示方式至少包括:

[0028] 以地图展示的方式、以表格展示的方式和以图表展示的方式。

[0029] 根据本发明的具体实施方式,第三方面,本发明提供一种计算机可读存储介质,其上存储有计算机程序,所述程序被处理器执行时实现如上任一项所述的可视化展示的方法。

[0030] 根据本发明的具体实施方式,第四方面,本发明提供一种电子设备,包括:一个或多个处理器;存储装置,用于存储一个或多个程序,当所述一个或多个程序被所述一个或多个处理器执行时,使得所述一个或多个处理器实现如上任一项所述的可视化展示的方法。

[0031] 本发明实施例的上述方案与现有技术相比,至少具有以下有益效果:本公开通过提供一种流量数据的可视化展示系统、方法、介质和电子设备,通过引入可视化展示单元,对流量统计服务单元的统计结果进行可视化展示,可以更加直观地看到统计结果,提高了用户体验度。

附图说明

[0032] 此处的附图被并入说明书中并构成本说明书的一部分,示出了符合本发明的实施例,并与说明书一起用于解释本发明的原理。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。在附图中:

[0033] 图1示出了根据本发明实施例的流量数据的可视化系统结构示意图;

[0034] 图2示出了根据本发明的实施例的流量数据的可视化方法流程图;

[0035] 图3示出了根据本发明的实施例的电子设备连接结构示意图。

具体实施方式

[0036] 为了使本发明的目的、技术方案和优点更加清楚,下面将结合附图对本发明作进一步地详细描述,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做出创造性劳动前提下所获得的所有其它实施例,都属于本发明保护的范围。

[0037] 在本发明实施例中使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本发明。在本发明实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义,“多种”一般包含至少两种。

[0038] 应当理解,本文中使用的术语“和/或”仅仅是一种描述关联对象的关联关系,表示可以存在三种关系,例如,A和/或B,可以表示:单独存在A,同时存在A和B,单独存在B这三种情况。另外,本文中字符“/”,一般表示前后关联对象是一种“或”的关系。

[0039] 应当理解,尽管在本发明实施例中可能采用术语第一、第二、第三等来描述……,但这些……不应限于这些术语。这些术语仅用来将……区分开。例如,在不脱离本发明实施例范围的情况下,第一……也可以被称为第二……,类似地,第二……也可以被称为第一……。

[0040] 取决于语境,如在此所使用的词语“如果”、“若”可以被解释成为“在……时”或“当……时”或“响应于确定”或“响应于检测”。类似地,取决于语境,短语“如果确定”或“如果检测(陈述的条件或事件)”可以被解释成为“当确定时”或“响应于确定”或“当检测(陈述的条件或事件)时”或“响应于检测(陈述的条件或事件)”。

[0041] 还需要说明的是,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商品或者装置不仅包括那些要素,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商品或者装置所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的商品或者装置中还存在另外的相同要素。

[0042] 下面结合附图详细说明本发明的可选实施例。

[0043] 实施例1

[0044] 如图1所示,根据本公开的具体实施方式,第一方面,本公开提供一种流量数据的可视化展示系统,包括:

[0045] 流量缓存中间件102,用于通过多个流量引擎收集流量数据,并将收集到的流量数据缓存至本地磁盘;

[0046] 流量数据收集单元104,用于从流量缓存中间件102的缓存队列中消费第一流量数据,将第一流量数据转换为符合预设数据格式类型的第二流量数据,并将第二流量数据批量插入时序数据库106中;

[0047] 需要说明的是,缓存队列负责将收集到的流量数据缓存打本次磁盘,避免当流量过多时,如果消费者消费能力有限导致的数据丢失问题。

[0048] 时序数据库106,用于存储和管理流量数据收集单元104转换得到的第二流量数据;

[0049] 流量统计服务单元108,用于根据检索请求接入至对应的时序数据库106存储的第二流量数据的统计接口,并根据检索请求从时序数据库106中调取对应类型的第二流量数据,并对调取的第二流量数据进行统计,得到统计结果;

[0050] 可视化展示单元110,用于对统计结果进行可视化展示。

[0051] 表1 示出了预先对网络流量结构的定义,具体如下所述:

	属性名	类型	字段类型	描述
	srcIp	字符串	tag	源 ip
	srcPort	字符串	tag	源端口
	srcMac	字符串	tag	源 mac
[0052]	srcVender	字符串	tag	源厂商
	dstIp	字符串	tag	目的 ip
	dstPort	字符串	tag	目的端口
	dstMac	字符串	tag	目的 mac
	dstVendor	字符串	tag	目的厂商
	traType	字符串	tag	传输层协议
	appType	字符串	tag	应用层协议
	fSeen	长整型	tag	时间片内链路首次出现时间
[0053]	lSeen	长整型	tag	时间片内链路最后出现时间
	deviceId	字符串	tag	采集引擎设备的 id
	packages	长整型	field	时间片内相同链路总包数
	bytes	长整型	field	时间片内相同链路总字节数

[0054] 其中,packages和bytes两个字段主要用于针对流量的大小按照bps和pps做聚合分析使用的,其他字段属于链路的基本属性信息字段,主要用于标识链路属性,可以按照这些属性的一个或者多个做分组。

[0055] 可选的,所述系统还包括:

[0056] 获取单元(在图1中未示出),用于获取第二流量数据的格式类型信息;

[0057] 其中,获取单元获取到的第二流量数据的数据格式类型信息至少包括:

[0058] 属性名信息、类型信息、字段类型信息和对应的描述信息。

[0059] 可选的,可视化展示单元110还用于:

[0060] 可视化展示第二流量数据的各项数据格式类型信息。

[0061] 可选的,通过可视化展示单元110对第二流量数据的各项数据格式类型信息以地图展示的方式进行可视化展示。

[0062] 可选的,通过可视化展示单元110对第二流量数据的各项数据格式类型信息以表格展示的方式进行可视化展示。

[0063] 可选的,通过可视化展示单元110对第二流量数据的各项数据格式类型信息以图表展示的方式进行可视化展示。

[0064] 本公开通过提供一种流量数据的可视化展示系统、方法、介质和电子设备,通过引入可视化展示单元,对流量统计服务单元的统计结果进行可视化展示,可以更加直观地看到统计结果,提高了用户体验度。

[0065] 除此之外,本公开通过提供一种流量数据的可视化展示系统、方法、介质和电子设备,还具有如下优点:

[0066] 1.流量数据不丢失,支持缓存,满足瞬时大并发量的场景;

[0067] 2.不限定流量数据的结构,自适应流量数据结构的动态变化;

[0068] 3.支持集群部署,对系统的容量和性能可动态扩展;

[0069] 4.流量数据的实时和历史统计速度极快,实时性高;

[0070] 5.流量统计方式灵活多变,统计的维度多种多样。

[0071] 6.根据实时数据并发页面显示,全方面展示动态效果

[0072] 7.同时并发动态展示效果,快速高效的分析数据

[0073] 8.更简单更直观的展示了数据,提高了这个项目的流畅性和完整度。

[0074] 实施例2

[0075] 如图2所示,根据本公开的具体实施方式,第二方面,本公开提供一种使用可视化展示系统对流量数据进行可视化展示的方法,包括:

[0076] S202:从流量缓存中间件的缓存队列中消费第一流量数据,将第一流量数据转换为符合预设数据格式类型的第二流量数据,并将第二流量数据批量插入时序数据库中;

[0077] S204:对时序数据库中的第二流量数据进行分析,并分析出对应的数据格式类型信息;

[0078] S206:根据数据格式类型信息,通过可视化展示单元对第二流量数据进行可视化展示;

[0079] 其中,数据格式类型信息至少包括:

[0080] 属性名信息、类型信息、字段类型信息和对应的描述信息。

[0081] 正如实施例1中的表1所示,示出了预先对网络流量结构的定义,烦请参见前述实施例1中的表1,在此不再赘述。

[0082] 可选的,通过可视化展示单元对第二流量数据的可视化展示方式至少包括:

[0083] 以地图展示的方式、以表格展示的方式和以图表展示的方式。

[0084] 在具体示例中,对接收到的流量数据进行分析,分析当前流量数据的数据格式,并根据不同流量数据的不同数据格式,选择与当前流量数据的数据格式匹配的可视化展示方式。

[0085] 若通过分析当前流量数据的数据格式获知:与当前流量数据的数据格式匹配的可视化展示方式为以地图展示的方式可视化展示当前流量数据,则以地图展示的方式可视化展示当前流量数据。

[0086] 或者,若通过分析当前流量数据的数据格式获知:与当前流量数据的数据格式匹配的可视化展示方式为以表格展示的方式可视化展示当前流量数据,则以表格展示的方式可视化展示当前流量数据。

[0087] 再者,若通过分析当前流量数据的数据格式获知:与当前流量数据的数据格式匹配的可视化展示方式为以图表展示的方式可视化展示当前流量数据,则以图表展示的方式可视化展示当前流量数据。

[0088] 在具体示例中,可以根据不同的用户需求选择符合用户所需的不同可视化展示方式,在此不再赘述。

[0089] 本公开通过提供一种流量数据的可视化展示系统、方法、介质和电子设备,通过引入可视化展示单元,对流量统计服务单元的统计结果进行可视化展示,可以更加直观地看到统计结果,提高了用户体验度。

[0090] 除此之外,本公开通过提供一种流量数据的可视化展示系统、方法、介质和电子设备,还具有如下优点:

[0091] 1. 流量数据不丢失,支持缓存,满足瞬时大并发量的场景;

[0092] 2. 不限定流量数据的结构,自适应流量数据结构的动态变化;

[0093] 3. 支持集群部署,对系统的容量和性能可动态扩展;

[0094] 4. 流量数据的实时和历史统计速度极快,实时性高;

[0095] 5. 流量统计方式灵活多变,统计的维度多种多样。

[0096] 6. 根据实时数据并发页面显示,全方面展示动态效果

[0097] 7. 同时并发动态展示效果,快速高效的分析数据

[0098] 8. 更简单更直观的展示了数据,提高了这个项目的流畅性和完整度。

[0099] 实施例3

[0100] 如图3所示,本实施例提供一种电子设备,该设备用于流量数据的可视化展示的方法,所述电子设备,包括:至少一个处理器;以及,与所述至少一个处理器通信连接的存储器;其中,

[0101] 所述存储器存储有可被所述一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够:通过引入可视化展示单元,对流量统计服务单元的统计结果进行可视化展示,可以更加直观地看到统计结果,提高了用户体验度。

[0102] 实施例4

[0103] 本公开实施例提供了一种非易失性计算机存储介质,所述计算机存储介质存储有计算机可执行指令,该计算机可执行指令可执行上述任意方法实施例中的对流量数据进行可视化展示的方法。

[0104] 实施例5

[0105] 下面参考图3,其示出了适于用来实现本公开实施例的电子设备300的结构示意图。本公开实施例中的终端设备可以包括但不限于诸如移动电话、笔记本电脑、数字广播接收器、PDA(个人数字助理)、PAD(平板电脑)、PMP(便携式多媒体播放器)、车载终端(例如车载导航终端)等等的移动终端以及诸如数字TV、台式计算机等等的固定终端。图3示出的电子设备仅仅是一个示例,不应对本公开实施例的功能和使用范围带来任何限制。

[0106] 如图3所示,电子设备300可以包括处理装置(例如中央处理器、图形处理器等)301,其可以根据存储在只读存储器(ROM)302中的程序或者从存储装置308加载到随机访问存储器(RAM)303中的程序而执行各种适当的动作和处理。在RAM 303中,还存储有电子设备300操作所需的各种程序和数据。处理装置301、ROM 302以及RAM 303通过总线304彼此相连。输入/输出(I/O)接口305也连接至总线304。

[0107] 通常,以下装置可以连接至I/O接口305:包括例如触摸屏、触摸板、键盘、鼠标、摄像头、麦克风、加速度计、陀螺仪等的输入装置306;包括例如液晶显示器(LCD)、扬声器、振动器等的输出装置307;包括例如磁带、硬盘等的存储装置308;以及通信装置309。通信装置309可以允许电子设备300与其他设备进行无线或有线通信以交换数据。虽然图3示出了具有各种装置的电子设备300,但是应理解的是,并不要求实施或具备所有示出的装置。可以替代地实施或具备更多或更少的装置。

[0108] 特别地,根据本公开的实施例,上文参考流程图描述的过程可以被实现为计算机软件程序。例如,本公开的实施例包括一种计算机程序产品,其包括承载在计算机可读介质上的计算机程序,该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中,该计算机程序可以通过通信装置309从网络上被下载和安装,或者从存储装置308被安装,或者从ROM 302被安装。在该计算机程序被处理装置301执行时,执行本公开实施例的方法中限定的上述功能。

[0109] 本技术领域技术人员可以理解,本发明包括涉及用于执行本申请中所述操作中的一项或多项的设备。这些设备可以为所需的目的而专门设计和制造,或者也可以包括通用计算机中的已知设备。这些设备具有存储在其内的计算机程序,这些计算机程序选择性地激活或重构。这样的计算机程序可以被存储在设备(例如,计算机)可读介质中或者存储在适于存储电子指令并分别耦联到总线的任何类型的介质中,所述计算机可读介质包括但不限于任何类型的盘(包括软盘、硬盘、光盘、CD-ROM、和磁光盘)、ROM(Read-Only Memory,只读存储器)、RAM(Random Access Memory,随机存储器)、EPROM(Erasable Programmable Read-Only Memory,可擦写可编程只读存储器)、EEPROM(Electrically Erasable Programmable Read-Only Memory,电可擦可编程只读存储器)、闪存、磁性卡片或光线卡片。也就是,可读介质包括由设备(例如,计算机)以能够读的形式存储或传输信息的任何介质。

[0110] 本技术领域技术人员可以理解,可以用计算机程序指令来实现这些结构图和/或框图和/或流程图中的每个框以及这些结构图和/或框图和/或流程图中的框的组合。本技术领域技术人员可以理解,可以将这些计算机程序指令提供给通用计算机、专业计算机或其他可编程数据处理方法的处理器来实现,从而通过计算机或其他可编程数据处理方法的处理器来执行本发明公开的结构图和/或框图和/或流程图的框或多个框中指定的方案。

[0111] 本技术领域技术人员可以理解,本发明中已经讨论过的各种操作、方法、流程中的步骤、措施、方案可以被交替、更改、组合或删除。进一步地,具有本发明中已经讨论过的各种操作、方法、流程中的其他步骤、措施、方案也可以被交替、更改、重排、分解、组合或删除。进一步地,现有技术中的具有与本发明中公开的各种操作、方法、流程中的步骤、措施、方案也可以被交替、更改、重排、分解、组合或删除。

[0112] 以上所述仅是本发明的部分实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。



图1

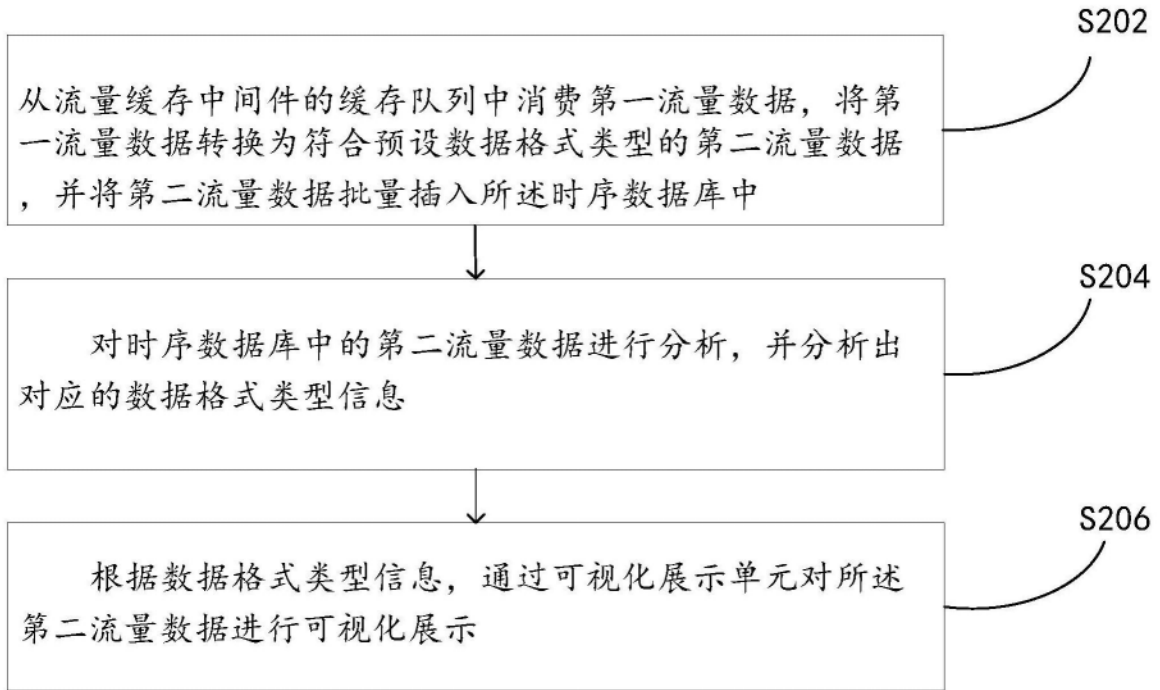


图2

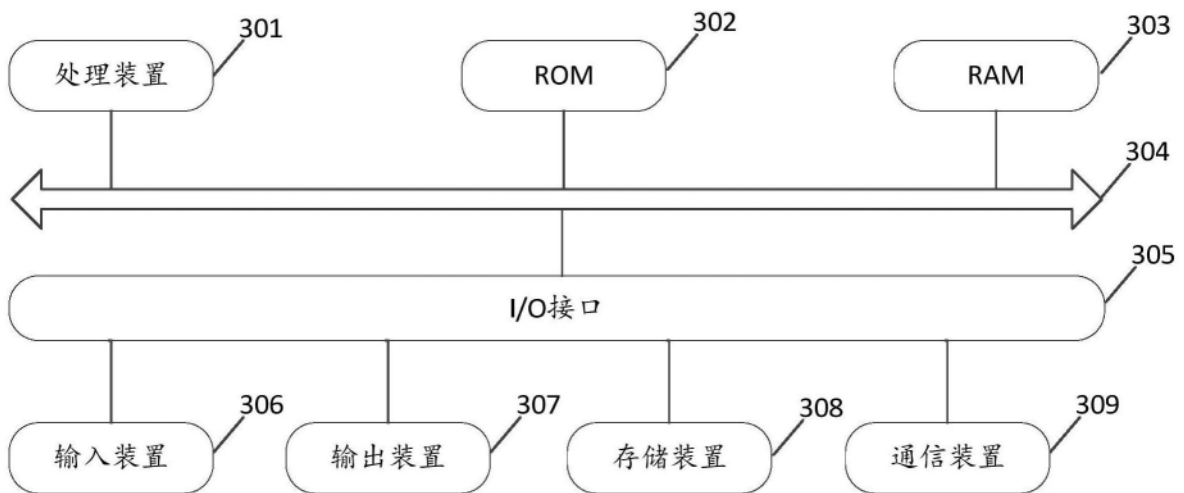


图3