(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 113835947 A
(43)申请公布日 2021.12.24

(21)申请号 202010514155.2

(22)申请日 2020.06.08

(71)申请人 支付宝(杭州)信息技术有限公司
地址 310000 浙江省杭州市西湖区西溪路556号8层B段801-11

(72)发明人 吴新琪 苏煜 章鹏 车延辙

(74)专利代理机构 成都七星天知识产权代理有限公司 51253
代理人 杨永梅

(51)Int.Cl.
G06F 11/30(2006.01)

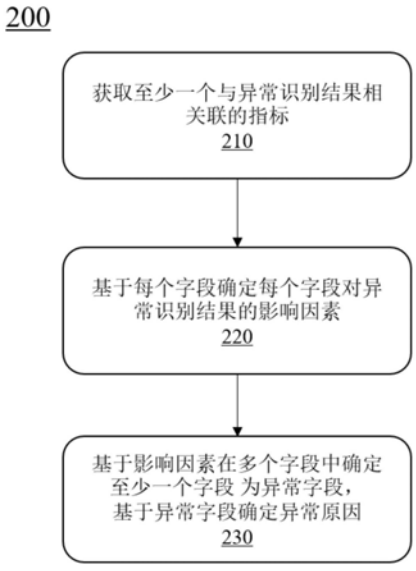
权利要求书3页 说明书13页 附图4页

(54)发明名称

一种基于异常识别结果确定异常原因的方法和系统

(57)摘要

本说明书公开了一种基于异常识别结果确定异常原因的方法和系统。该方法包括:获取至少一个与所述异常识别结果相关联的指标,每个所述指标包括多个字段,每个字段与某一预设的业务含义相关联;基于所述每个字段确定所述每个字段对所述异常识别结果的影响因素;所述影响因素包括所述每个字段的异常度和贡献度;基于所述影响因素在所述多个字段中确定至少一个字段为异常字段,基于所述异常字段确定异常原因。



CN 113835947 A

1.一种基于异常识别结果确定异常原因的方法,其包括:

获取至少一个与所述异常识别结果相关联的指标,每个所述指标包括多个字段,每个字段与某一预设的业务含义相关联;

基于所述每个字段确定所述每个字段对所述异常识别结果的影响因素;所述影响因素包括所述每个字段的异常度和贡献度;

基于所述影响因素在所述多个字段中确定至少一个字段为异常字段,基于所述异常字段确定异常原因。

2.如权利要求1所述的方法,其中:

所述异常度为群体稳定性指数、信息散度或詹森香农差异中的至少一个;

所述贡献度基于所述字段以及所述字段所属的指标确定。

3.如权利要求1所述的方法,其中:

所述影响因素包括先验风险度;

所述先验风险度为所述字段的风险预设权重。

4.如权利要求3所述的方法,其中,基于所述影响因素在所述多个字段中确定至少一个字段为异常字段包括:

基于所述异常度、所述贡献度和所述先验风险度在所述多个字段中确定至少一个对所述异常识别结果影响最大的字段,作为异常字段。

5.如权利要求1所述的方法,其中:

所述指标至少经过数据离散化处理。

6.如权利要求1所述的方法,其中,获取至少一个异常指标包括:

获取多个监控指标;每个所述监控指标包括多个字段,每个字段与某一预设的业务含义相关联;

基于时序分解算法去除所述监控指标中的周期分量,得到检验监控指标;

基于异常检测算法对所述检验监控指标进行处理,得到异常识别结果;

基于所述异常识别结果在所述监控指标中确定至少一个与所述异常识别结果相关联的指标。

7.如权利要求6所述的方法,其中:

所述异常检测算法为假设检验算法,所述异常识别结果为检验统计量;

基于所述检验统计量得到至少一个与所述异常识别结果相关联的指标。

8.如权利要求7所述的方法,还包括:

基于所述监控指标中包括的所述字段的数量,得到临界值;

所述检验统计量不大于所述临界值时,当前监控指标没有异常。

9.如权利要求7所述的方法,其中:

所述假设检验算法为混合泛化版极端学生化方差。

10.如权利要求6所述的方法,其中:

所述时序分解算法为基于局部加权回归的季节性和趋势分解方法。

11.如权利要求6所述的方法,其包括:

将所述异常字段从所述监控指标中剔除;

基于所述监控指标中剩余字段确定至少一个异常指标;

基于所述异常指标确定新的异常字段，直至满足迭代截止条件。

12.一种基于异常识别结果确定异常原因的系统，其包括：

异常识别结果获取模块，用于获取至少一个与所述异常识别结果相关联的指标，每个所述指标包括多个字段，每个字段与某一预设的业务含义相关联；

影响因素确定模块，用于基于所述每个字段确定所述每个字段对所述异常识别结果的影响因素；所述影响因素包括所述每个字段的异常度和贡献度；

异常原因确定模块，用于基于所述影响因素在所述多个字段中确定至少一个字段为异常字段，基于所述异常字段确定异常原因。

13.如权利要求12所述的系统，其中：

所述异常度为群体稳定性指数、信息散度或詹森香农差异中的至少一个；

所述贡献度基于所述字段以及所述字段所属的指标确定。

14.如权利要求12所述的系统，其中：

所述影响因素包括先验风险度；

所述先验风险度为所述字段的风险预设权重。

15.如权利要求14所述的系统，异常原因确定模块包括：

基于所述异常度、所述贡献度和先验风险度在所述多个字段中确定至少一个对所述异常识别结果影响最大的字段，作为异常字段。

16.如权利要求12所述的系统，其中：

所述指标至少经过数据离散化处理。

17.如权利要求12所述的系统，异常识别结果获取模块包括：

监控指标获取单元，用于获取多个监控指标；每个所述监控指标包括多个字段，每个字段与某一预设的业务含义相关联；

时序分解单元，用于基于时序分解算法去除所述监控指标中的周期分量，得到检验监控指标；

异常检测单元，用于基于异常检测算法对所述检验监控指标进行处理，得到异常识别结果；

异常识别结果确定单元，基于所述异常识别结果在所述监控指标中确定至少一个与所述异常识别结果相关联的指标。

18.如权利要求17所述的系统，其中：

所述异常检测算法为假设检验算法，所述异常识别结果为检验统计量；

基于所述检验统计量得到至少一个与所述异常识别结果相关联的指标。

19.如权利要求18所述的系统，还包括：

基于所述监控指标中包括的所述字段的数量，得到临界值；

所述检验统计量不大于所述临界值时，当前监控指标没有异常。

20.如权利要求18所述的系统，其中：

所述假设检验算法为混合泛化版极端学生化方差。

21.如权利要求17所述的系统，其中：

所述时序分解算法为基于局部加权回归的季节性和趋势分解方法。

22.如权利要求17所述的系统，其包括：

将所述异常字段从所述监控指标中剔除；

基于所述监控指标中剩余字段确定至少一个异常指标；

基于所述异常指标确定新的异常字段，直至满足迭代截止条件。

23.一种基于异常识别结果确定异常原因的装置，其中，包括处理器以及存储介质，所述存储介质用于存储计算机指令，所述处理器用于执行所述计算机指令中的至少一部分以实现如权利要求1～11中任一项所述的方法。

一种基于异常识别结果确定异常原因的方法和系统

技术领域

[0001] 本说明书涉及数据监控领域,特别涉及一种基于异常识别结果确定异常原因的方法和系统。

背景技术

[0002] 数据监控的作用是为了在数据平台内发现数据的潜在风险并能及时向业务人员告警,是故障诊断和异常分析的重要辅助利器,监控系统对各类数据平台重要性不言而喻。

[0003] 但在数据监控过程中发现数据中存在异常后,需要利用业务人员对异常数据进行排查从而找出异常原因,而排查所耗费的时间很大程度上决定风险是否能够被及时处理。

发明内容

[0004] 本说明书实施例之一提供一种基于异常识别结果确定异常原因的方法,该方法包括:获取至少一个与所述异常识别结果相关联的指标,每个所述指标包括多个字段,每个字段与某一预设的业务含义相关联;基于所述每个字段确定所述每个字段对所述异常识别结果的影响因素;所述影响因素包括所述每个字段的异常度和贡献度;基于所述影响因素在所述多个字段中确定至少一个字段为异常字段,基于所述异常字段确定异常原因。

[0005] 本说明书实施例之一提供一种基于异常识别结果确定异常原因的系统,该系统包括:异常识别结果获取模块,用于获取至少一个与所述异常识别结果相关联的指标,每个所述指标包括多个字段,每个字段与某一预设的业务含义相关联;影响因素确定模块,用于基于所述每个字段确定所述每个字段对所述异常识别结果的影响因素;所述影响因素包括所述每个字段的异常度和贡献度;异常原因确定模块,用于基于所述影响因素在所述多个字段中确定至少一个字段为异常字段,基于所述异常字段确定异常原因。

[0006] 本说明书实施例之一提供一种基于异常识别结果确定异常原因的装置,其中,包括处理器以及存储介质,所述存储介质用于存储计算机指令,所述处理器用于执行所述计算机指令中的至少一部分以实现如上述的方法。

附图说明

[0007] 本说明书将以示例性实施例的方式进一步说明,这些示例性实施例将通过附图进行详细描述。这些实施例并非限制性的,在这些实施例中,相同的编号表示相同的结构,其中:

[0008] 图1是根据本说明书一些实施例所示的一种基于异常识别结果确定异常原因的系统的应用场景示意图;

[0009] 图2是根据本说明书一些实施例所示的一种基于异常识别结果确定异常原因的方法的示例性流程图;

[0010] 图3是根据本说明书一些实施例所示的获取至少一个与异常识别结果相关联的指标的示例性流程图;

[0011] 图4是根据本说明书一些实施例所示的另一种基于异常识别结果确定异常原因的方法的示例性流程图；

[0012] 图5是根据本说明书一些实施例所示的一种基于异常识别结果确定异常原因的系统的示例性系统框图；

[0013] 图6是根据本说明书一些实施例所示的异常识别结果获取模块的系统框图。

具体实施方式

[0014] 为了更清楚地说明本说明书实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单的介绍。显而易见地，下面描述中的附图仅仅是本说明书的一些示例或实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图将本说明书应用于其它类似情景。除非从语言环境中显而易见或另做说明，图中相同标号代表相同结构或操作。

[0015] 应当理解，本文使用的“服务端”、“平台”、“后台”、“服务器”等可以互换，“用户端”、“用户终端”、“请求者”、“前端”、“用户设备”|等可以互换。本文使用的“系统”、“装置”、“单元”和/或“模块”是用于区分不同级别的不同组件、元件、部件、部分或装配的一种方法。然而，如果其他词语可实现相同的目的，则可通过其他表达来替换所述词语。

[0016] 如本说明书和权利要求书中所示，除非上下文明确提示例外情形，“一”、“一个”、“一种”和/或“该”等词并非特指单数，也可包括复数。一般说来，术语“包括”与“包含”仅提示包括已明确标识的步骤和元素，而这些步骤和元素不构成一个排它性的罗列，方法或者设备也可能包含其它的步骤或元素。

[0017] 本说明书中使用了流程图用来说明根据本说明书的实施例的系统所执行的操作。应当理解的是，前面或后面操作不一定按照顺序来精确地执行。相反，可以按照倒序或同时处理各个步骤。同时，也可以将其他操作添加到这些过程中，或从这些过程移除某一步或数步操作。

[0018] 图1是根据本说明书一些实施例所示的一种基于异常识别结果确定异常原因的系统的应用场景示意图。

[0019] 在一些实施例中，图1中应用场景中可以包括服务器110、处理器120、网络130和存储设备140。

[0020] 在一些应用场景中，基于异常识别结果确定异常原因的系统100可以被广泛应用于各种服务平台的后端，例如，电商平台、支付平台、安全监控平台等。

[0021] 服务器110在处理时可以获取存储设备140上的数据或将数据保存到存储设备。在一些实施例中，本说明书中的操作可以通过处理器120执行程序指令进行。上述方式仅为方便理解，本系统亦可以其他可行的操作方式实施本说明书中的方法。

[0022] 在一些实施例中，服务器110或其他可能的系统组成部分中可以包括存储设备140。在一些实施例中，服务器110或其他可能的系统组成部分中可以包括处理器120。

[0023] 在一些实例中，可以在不同的设备上分别进行不同的功能，比如数据的筛选、预处理、模块的执行等等，本说明书对此不作限制。

[0024] 服务器110可以用于管理资源以及处理来自本系统至少一个组件或外部数据源(例如，云数据中心)的数据和/或信息。在一些实施例中，服务器110可以是单一服务器或服

务器组。该服务器组可以是集中式或分布式的(例如,服务器110可以是分布式系统),可以是专用的也可以由其他设备或系统同时提供服务。在一些实施例中,服务器110可以是区域的或者远程的。在一些实施例中,服务器110可以在云平台上实施,或者以虚拟方式提供。仅作为示例,所述云平台可以包括私有云、公共云、混合云、社区云、分布云、内部云、多层云等或其任意组合。

[0025] 处理器120可以处理从其他设备或系统组成部分中获得的数据和/或信息。处理器可以基于这些数据、信息和/或处理结果执行程序指令,以执行一个或多个本说明书中描述的功能。在一些实施例中,处理器120可以包含一个或多个子处理设备(例如,单核处理设备或多核多芯处理设备)。仅作为示例,处理器120可以包括中央处理器(CPU)、专用集成电路(ASIC)、专用指令处理器(ASIP)、图形处理器(GPU)、物理处理器(PPU)、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、可编辑逻辑电路(PLD)、控制器、微控制器单元、精简指令集电脑(RISC)、微处理器等或以上任意组合。

[0026] 网络130可以连接系统的各组成部分和/或连接系统与外部资源部分。网络130使得各组成部分之间,以及与系统之外其他部分之间可以进行通讯,促进数据和/或信息的交换。在一些实施例中,网络130可以是有线网络或无线网络中的任意一种或多种。例如,网络130可以包括电缆网络、光纤网络、电信网络、互联网、局域网络(LAN)、广域网络(WAN)、无线局域网络(WLAN)、城域网(MAN)、公共交换电话网络(PSTN)、蓝牙网络、紫蜂网络(ZigBee)、近场通信(NFC)、设备内总线、设备内线路、线缆连接等或其任意组合。各部分之间的网络连接可以是采用上述一种方式,也可以是采取多种方式。在一些实施例中,网络可以是点对点的、共享的、中心式的等各种拓扑结构或者多种拓扑结构的组合。在一些实施例中,网络130可以包括一个或以上网络接入点。例如,网络130可以包括有线或无线网络接入点,例如基站和/或网络交换点130-1、130-2、…,通过这些点进出系统100的一个或多个组件可连接到网络130上以交换数据和/或信息。

[0027] 存储设备140可以用于存储数据和/或指令。存储设备140可以包括一个或多个存储组件,每个存储组件可以是一个独立的设备,也可以是数据库或其他设备的一部分。在一些实施例中,存储设备140可包括随机存取存储器(RAM)、只读存储器(ROM)、大容量存储器、可移动存储器、易失性读写存储器等或其任意组合。示例性的,大容量储存器可以包括磁盘、光盘、固态磁盘等。在一些实施例中,所述存储设备140可在云平台上实现。

[0028] 数据指对信息的数字化表示,可以包括各种类型,比如二进制数据、文本数据、图像数据、视频数据等。指令指可控制设备或器件执行特定功能的程序。

[0029] 在一些实施例中,服务平台(如购物平台、交易平台、支付平台或银行机构等)随着时间会收集到大量流水数据,流水数据通常包括若干与服务平台所提供的服务相关的信息。为保证平台稳定、安全的运行,需要针对收集到的流水数据进行风险的监测,并及时将所监测到的异常汇报相关的部门。仅作为示例,服务平台作为银行机构或支付平台,需要跟进识别平台内用户是否存在诸如接口滥用、赌博、洗钱等风险时,需要定位哪些商户行为异常(如交易突增、渠道聚焦),哪些买家交易行为异常(复购、可疑夜间、整数交易),设备环境高度聚集等,以便监管部门将结果推送回被监管机构,跟进相应的风险敞口治理。另一个示例,服务平台为购物平台或支付平台,在某大型营销活动进行时,需要识别是否存在批量恶意“薅羊毛”的行为时,需要根据流水数据定位出行为具体的场景、地区、人群、介质主体等

信息，以便准确实时地跟进相应风控策略的攻防。

[0030] 在一些实施例中，针对上述风险，服务器110同时获取历史汇总指标(如日交易笔数)，采用同比或环比的方式，通过设置阈值进行监控，如可疑行为通常发生在夜晚12点至凌晨1点之间，服务器110可以获取前一日或前一周夜晚12点至凌晨1点交易中指标的平均值与当前流水数据对比，当数据浮动超过指标预设阈值(如20％)时，进行异常提示。但由于采用同比或环比的方式的局限性，那么可能会在一些情况中漏过风险，如总体看似平稳的交易笔数，交易量小的商户的剧烈波动会被交易量大的商户的相对平稳所掩盖，又如“薅羊毛”订单通常支付金额较小(如不超过20元)，与其他较大金额订单一起统计，可能从交易总量等指标上并不会体现出明显异常，从而漏过风险。此外，由于采用历史汇总指标，该方案还缺少对于其他不容易量化指标的关注，如总体看似平稳的交易笔数，可能背后的支付渠道(如卡交易、移动支付等)、支付类型(如网关、快捷、代付、提现等)已经发生了变化。

[0031] 在一些实施例中，当通过对流水数据监控发现异常后，通常将数据交给业务人员，通过业务人员的经验对异常数据进行判断，确定异常的原因。例如，通过监控发现“日交易笔数”同比下降了50％，业务人员收到异常后，需要根据其业务理解程度和二次探索数据分析，才能逐渐定位可采取实际措施的原因，较为耗时耗力，并且同样存在漏过风险的情况。

[0032] 在一些实施例中，考虑到对流水数据中多指标进行分析，提供了一种基于异常识别结果确定异常原因的系统，通过算法的配合，更准确的确定异常原因，能够弥补在一些其他实施例中存在的缺陷。

[0033] 图2是根据本说明书一些实施例所示的一种基于异常识别结果确定异常原因的方法的示例性流程图。

[0034] 图2所示的一种基于异常识别结果确定异常原因的方法200中的一个或多个操作可以通过图1中系统100实现。

[0035] 步骤210，获取至少一个与所述异常识别结果相关联的指标。在一些实施例中，步骤210可以由异常识别结果获取模块510执行。

[0036] 异常识别结果表示一个类型的数据相对于过往数据或预设关注值存在异常，可以理解的是，数据出现了异常不等同于出现了风险，如在进行移动支付的推广过程中，检测到商户支付渠道中现金支付比例下降，则不能代表出现风险，无需对支付渠道进行过多关注。

[0037] 在一些实施例中，异常识别结果可以通过采用传统模式获取还可以是利用特定算法基于流水数据获取还可以是通过网络130接收其他系统获取的异常识别结果。关于异常识别结果的获取方式在后文中详细说明。

[0038] 在一些实施例中，异常识别结果通常具有一个相关联的指标，该指标能够表示一类数据，如时间指标、支付渠道指标、支付金额指标、是否高危时间段指标、商户账户指标、交易笔数指标等。

[0039] 在一些实施例中，每个异常识别结果相关联的指标包括多个字段，每个字段与某一预设的业务含义相关联。可以理解的是，在一些实施例中，字段为存储设备140中的一段数据，当异常识别结果相关联的指标为时间指标时，与该字段相关联的预设业务含义即代表某一个时间段，具体的，时间指标中包括24个均匀分隔的字段，即每个字段相关联的预设业务含义为一天中的一个小时的交易相关数据。需要说明的是，在一些其他实施例中，时间指标还可以包括其他数量的字段，如3个或4个，此外各个字段并不是均匀分隔，如在交易量

较少的凌晨时段可以将6个小时分隔为一个字段，而在交易活跃的黄金时段可以将一个小时分隔为一个字段。

[0040] 在一些实施例中，指标至少经过数据离散化处理，即指标中包括的多个字段是经过预处理的，以保证后续可解释的维度都是可枚举的。离散化处理是数据处理中常用的方式，它可以有效的降低时间复杂度，提高算法的时空效率。仅作为示例，异常识别结果交易金额指标，交易金额通常跨度较大，并且具有小数，那么为了降低算法时间复杂度，通过离散化处理，将交易金额以区间的形式表示，如十元以内枚举值表示为1、十元至百元枚举值表示为2、百元至千元枚举值表示为3、千元至万元枚举值表示为4、万元以上枚举值表示为5。

[0041] 在一些实施例中，指标还可以进行缺失值填充、连续离散判断、数值归一化等处理，仅作为示例，如在凌晨4点时，没有交易产生，那么通过缺失值填充，添加凌晨4点交易金额为0，以使维度可枚举。又如是否为高危时间指标中，通过归一化处理，将22点至次日6点表示为1，其余时间表示为0。在一些实施例中，指标根据其业务类型不同，可以进行缺失值填充、连续离散判断、数值归一化处理中的一个或多个，此外还可以进行其他形式的预处理，如正则化或降维处理等。

[0042] 在一些实施例中，以指标为日交易笔数为例，处理后的第i笔交易可以表示为$(X_i, Y_i) = (X_{i,1}, X_{i,2}, \cdots, X_{i,p}, Y_i)$，其中每个维度字段$X_i$都是可枚举的，$Y_i$是交易笔数(单笔则为1，也可以是各维度拆分后的日汇总值)，Y为交易笔数，即异常识别结果相关联的指标，X为除交易笔数外其他指标(如交易时间、交易金额区间等)，$X_{i,p}$为字段的枚举值，p为其他指标的数量。

[0043] 步骤220，基于所述每个字段确定所述每个字段对所述异常识别结果的影响因素。在一些实施例中，步骤220可以由影响因素确定模块520执行。

[0044] 指标与异常识别结果相关联，说明在该包括多个字段的指标中，至少有一个字段存在异常，即需要确定每个字段对异常识别结果(指标)的影响因素。

[0045] 在一些实施例中，所述影响因素包括所述每个字段的异常度和贡献度。贡献度用于表示字段局部的变动能够多大程度上解释整体变动。仅作为示例，如发生在白天的交易量大大高于发生在夜晚的，那么根据现有的数据，在交易时段指标中，白天的贡献度可能明显高于夜晚，容易出现错误归因于白天的情况。异常度用于表示字段占总体分布的变化程度，用于弥补贡献度在某些情况下的不足。

[0046] 在一些实施例中，所述异常度为群体稳定性指数(PSI)、信息散度(KL散度)或詹森香农差异(Jensen-Shannon divergence，又称JS散度)中的至少一个。具体的，在本实施例中，由于具备对称性和值域分布在[0,1]这两点优良特性，故选择詹森香农差异值作为异常度，詹森香农差异可以通过以下公式进行计算：

$$D_{JS}(P,Q) = 0.5\left(\Sigma_i p_i \log\frac{2p_i}{p_i+q_i} + \Sigma_i q_i \log\frac{2q_i}{p_i+q_i}\right) \qquad (1)$$

[0047] 其中，公式(1)中P和Q表示两个概率分布，i为字段标号，p_i和q_i分别表示字段的异常值和正常值。

[0048] 可以理解的是，詹森香农差异较低时，可以认为该字段无法区分正常与异常的分布，而詹森香农差异较高时，说明当前字段更具有是否异常的区分能力。而在异常原因的确

定中，更加倾向于对具有异常区分能力的指标进行下探。例如，网银支付渠道詹森香农差异为2%，移动支付渠道詹森香农差异为8%，此时，更倾向于选择移动支付渠道进行下探。

[0049] 在一些实施例中，贡献度通常利用贡献分析法进行计算，即贡献度基于所述字段以及所述字段所属的指标确定，在一些实施例中，贡献度可以通过以下公式进行计算：

$$C_{ij}=(A_{ij}-N_{ij})/(A_m-N_m) \quad (2)$$

[0050] 其中，A_{ij}表示维度i(即第i个字段)下的维值j所对应的异常取值，N_{ij}表示维度i下的维值j所对应的正常取值，A_m和N_m则表示总的正常和异常的取值。仅作为示例，假设在交易时段的指标中，有如下数据：

[0051] 白天：正常用户量为980，异常用户量为490；

[0052] 夜晚：正常用户量为20，异常用户量为10；

[0053] 由以上数据可知，白天所对应的A_{ij}为490、N_{ij}为980、A_m为500、N_m为1000，通过公式(2)可得白天在交易时段指标中贡献度为98%，同理可以计算夜间贡献度为2%。实际上，在一些场景下夜间更容易出现风险，而技术负责人员更希望在夜晚数据正常，因此该数据也揭示了之前提到的在一些实施例中，单纯使用贡献度可能造成错误归因的问题。

[0054] 在一些实施例中，利用过往经验，往往对风险有一定程度上先验的风险判断，仅作为示例，如在交易时，更倾向于交易金额指标中大额字段时进行风险下探，又如在交易时间段指标中，更倾向于夜间字段的风险下探，利用该先验知识在业务上具备更好的解释性和关注程度，故引入了先验风险度。在一些实施例中，影响因素还包括先验风险度，可以理解的是，先验风险度为字段根据其业务含义，在进行异常原因确定前就已经预设好的权重。仅作为示例，先验风险度根据其权重可以设置成不同的数值，如希望对夜间字段进行双倍的关注，可以将夜间字段的权重设为2，将交易时段指标中其他字段权重设为1。需要说明的是，在其他实施例中，该权重还可以是0.5、0.8、1.5或3等。

[0055] 步骤230，基于所述影响因素在所述多个字段中确定至少一个字段为异常字段，基于所述异常字段确定异常原因。在一些实施例中，步骤230可以由异常原因确定模块530执行。

[0056] 在一些实施例中，基于步骤220中得到的影响因素，能够在指标中包括的多个字段中，至少确定一个字段。可以理解的是，所确定的一个或多个字段很大程度上影响了该指标，从而使该指标被识别为异常。将确定的字段作为异常字段，基于异常字段加以分析确定异常原因。

[0057] 在一些实施例中，基于异常字段确定异常原因的方式可以利用人工经验进行分析，仅作为示例，例如异常原因定位到日交易笔数的下降的原因是，某交易渠道在夜间交易时段上的交易笔数跌零导致的，那么业务负责人就可以更加有的放矢地跟进相应渠道的对接排查工作，同时还能提供该渠道主要问题发生在夜间，缩小排查范围，提高异常原因的确定及解决效率。

[0058] 在一些实施例中，也可以在数据库中建立每个字段成为异常字段时，对应的原因，当确定异常字段后，进行匹配操作，得到异常原因。

[0059] 在一些实施例中，基于所述异常度、所述贡献度和所述先验风险度在所述多个字段中确定至少一个对所述异常识别结果影响最大的字段，作为异常字段。示例性的，影响最大的确定方式为异常度、贡献度和先验风险度三者相乘，乘积最大的一个或多个字段作为

异常字段。

[0060] 在一些实施例中，由公式(1)得到贡献度$_{ij}$，由公式(2)得到异常度JS_{ij}，同时将步骤220中得到的先验风险度表示为$Weigt_{ij}$，影响因素可以表示为：

$$Score_{ij}=C_{ij}*JS_{ij}*Weigt_{ij} \quad (3)$$

[0061] 公式(3)中的i和j与公式(1)相同，用于表示维度i(即第i个字段)下的维值j的异常取值。

[0062] 需要说明的是，在一些具体实施方式中，影响因素的确定还可以是将异常度、贡献度和先验风险度相加或进行分布差异的度量。

[0063] 图3是根据本说明书一些实施例所示的获取至少一个与异常识别结果相关联的指标的示例性流程图。

[0064] 在一些实施例中，基于异常识别结果确定异常原因的方法200中的异常识别结果同样可以由系统100中的服务器110获取。仅处于说明的目的，本说明书以服务器110获取异常识别结果对披露的技术方案进行详细描述，并不旨在限制本说明书的范围，在一些实施例中，异常识别结果还可以是其他服务器或通过网络130发送至服务器110。

[0065] 参考图3，在一些实施例中，步骤210中获取至少一个异常指标包括以下步骤：

[0066] 步骤211，获取多个监控指标。在一些实施例中，步骤211可以通过监控指标获取单元511执行。

[0067] 在一些实施例中，监控指标与步骤210中指标类似，即能够表示一类数据，不同之处在于，步骤211中监控指标通常包括多个，需要在众多数据中识别异常结果，通常需要对多种类型数据进行监控，而根据实际场景的不同，多种类型数据的监控形成多个监控指标。仅作为示例，如对交易平台进行异常识别，监控指标可以包括时间指标、支付渠道指标、支付金额指标、是否高危时间段指标、商户账户指标、交易笔数指标、金额末两位指标、交易日期指标、商户账户id等。

[0068] 在一些实施例中，每个所述监控指标包括多个字段，每个字段与某一预设的业务含义相关联。该字段与异常识别结果相关联指标中字段相同，具体可以参见步骤210中相关描述，在此不过多赘述。

[0069] 步骤213，基于时序分解算法去除所述监控指标中的周期分量，得到检验监控指标。在一些实施例中，步骤213可以通过时序分解单元513执行。

[0070] 时序分解算法是对于一个时间序列，假设它是加性模型(Additive decomposition)，那么对于时间序列$Total_t$可以分解为周期分量(seasonal component)、趋势分量(trend component)和余项(remainder component)，在一些实施例中，可以表示为：

$$Total_t=Seasonal_t+Trend_t+Residual_t, t=1,2,\cdots,n \quad (4)$$

[0071] 在一些实施例中，监控指标作为一种时间序列，可以基于上述公式(4)去除周期分量$Seasonal_t$，即将趋势分量$Trend_t$和余项$Residual_t$相加，得到检验监控指标。将监控指标中的周期分量去除后，使得在后续的数据处理过程中，收到周期性的影响减小，能够更加关注除周期性影响外的其他异常。

[0072] 在一些实施例中，所述时序分解算法为基于局部加权回归的季节性和趋势分解方法(Seasonal-Trend decomposition procedure based on Loess,STL)。基于局部加权回

归的季节性和趋势分解方法是时间序列分解的一种多用途和更具鲁棒性的方法。该算法为现有技术中较为成熟的方案，其利用局部加权回归(Loess)作为回归算法进行时间序列的分解，在此不过多赘述。在一些实施例中，时序分解算法还可以为MSTL算法等。

[0073] 步骤215，基于异常检测算法对所述检验监控指标进行处理，得到异常识别结果。在一些实施例中，步骤215可以通过异常检测单元515执行。

[0074] 在一些实施例中，对于去除周期分量后得到的检验监控指标，需要找出其中出现异常的异常识别结果，需要说明的是，一个指标中出现异常不代表一定出现了风险，可以理解的是，异常存在好的异常和坏的异常，如在进行营销活动时，交易量指标会因为短时间大量上涨出现异常，此时交易量的异常一定程度上能够表示营销活动的成功。

[0075] 在一些实施例中，异常检测算法可以是基于统计假设检验的异常检测算法，也可以是采用时间序列模型如3-Sigma模型、孤立森林(Isolation Forest)等异常检测常见的算法，在本说明书的一些实施例中，在后文中，采用基于统计假设检验的异常检测算法进行进一步描述。

[0076] 步骤217，基于所述异常识别结果在所述监控指标中确定至少一个与所述异常识别结果相关联的指标。在一些实施例中，步骤217可以通过异常识别结果确定单元517执行。

[0077] 在一些实施例中，通过异常识别结果的形式可以是一个值或者概率等，利用异常识别结果在监控指标中确定至少一个与所述异常识别结果相关联的指标。由图4中可以看出，在一些实施例中，步骤217中确定的异常识别结果相关联的指标即为步骤210中进行进一步确定异常原因的指标。

[0078] 在一些实施例中，步骤215中的异常检测算法为假设检验算法。进一步的，在假设检验算法中，异常识别结果为检验统计量(test statistic)，步骤217中基于该检验统计量得到至少一个与所述异常识别结果相关联的指标。

[0079] 在一些实施例中，选用Grubbs'Test作为假设检验方法，其常被用来检验服从正态分布的单变量数据集(univariate data set)Y中的单个异常值，即对上述检验监控指标进行检验，若有异常值，则其必为数据集中的最大值或最小值。在一些实施例中，Grubbs'Test检验假设的所用到的检验统计量可以表示为：

$$G = \frac{\max_t |Y_t - \bar{Y}|}{s} \qquad (5)$$

[0080] 公式(5)中，$\bar{Y}$为均值，s为标准差。但在现实数据集中，异常值往往是多个而非单个。为了将Grubbs'Test扩展到k个异常值检测，则需要在数据集中逐步删除与均值偏离最大的值(为最大值或最小值)，同步更新对应的t分布临界值，检验原假设是否成立。基于此，提出了Grubbs'Test的泛化版ESD(Extreme Studentized Deviate test)，可以表示为：

$$R_j = \frac{\max_t |Y_t - \tilde{Y}|}{s}, \quad 1 \le j \le k \qquad (6)$$

[0081] 公式(6)中，计算与均值$\tilde{Y}$偏离最远的残差。

[0082] 由于个别异常值会极大地拉伸均值和方差，从而导致Grubbs'Test的泛化版ESD方案未能很好地捕获到部分异常点，召回率偏低。进而在一些实施例中，选用假设检验算法为混合泛化版极端学生化方差(Hybrid GESD)，该算法采用了更具鲁棒性的中位数与绝对中

位差(Median Absolute Deviation,MAD)替换公式(6)中的均值与标准差,在一些实施例中,可以表示为:

$$R_j = \frac{\max_t |Y_t - \text{median}(Y)|}{\text{MAD}}, \quad 1 \le j \le k \qquad (7)$$

[0083] 公式(7)中MAD=median(|Y_t-median(Y|)。

[0084] 在一些实施例中,上文中所定义的检验统计量,其用于验证检验监控指标中是否存在异常,以及存在多少(或至多、至少)异常值。

[0085] 在一些实施例中,公式(7)中检验统计量R_j用于一下假设检验问题:

[0086] H0(原假设):数据集中没有异常值;

[0087] H1(备择假设):数据集中至多有k个异常值。

[0088] 基于公式(7)计算得到检验统计量R_j后,基于所述监控指标中包括的所述字段的数量,得到临界值(critical value),在一些实施例中,可以表示为:

$$\lambda_j = \frac{(n-j)\cdot t_{p,n-j-1}}{\sqrt{\left(n-j-1+t^2_{p,n-j-1}\right)(n-j+1)}}, 1 \le j \le k \qquad (8)$$

[0089] 公式(8)中,n为数据集的样本数,$t_{p,n-j-1}$为显著度(significance level)等于p、自由度(degrees of freedom)等于(n-j-1)的t分布临界值。

[0090] 基于公式(8)计算得到临界值λ_j后,检验原假设,比较检验统计量R_j与临界值λ_j,若检验统计量大于临界值,则原假设H0不成立,该对应时刻的样本点为异常点,重复以上步骤k次至算法结束。相应的,可以理解成,检验统计量不大于所述临界值时,当前监控指标没有异常。

[0091] 图4是根据本说明书一些实施例所示的另一种基于异常识别结果确定异常原因的方法的示例性流程图。

[0092] 参考图4,在本说明书的一些实施例中,基于异常识别结果确定异常原因的方法400在确定异常原因后,因为无法保证所有数据中仅存在这一个异常,故根据实际需要通常还需要对剩余数据进行下一轮基于监控指标获取异常识别结果并确定异常原因或基于异常识别结果确定异常原因,方法400还包括:

[0093] 将所述异常字段从所述监控指标中剔除;基于所述监控指标中剩余字段确定至少一个异常指标;基于所述异常指标确定新的异常字段,直至满足迭代截止条件。

[0094] 同一个与所述异常识别结果相关联的指标中可能存在一个以上的异常字段,故在一些实施例中,基于异常字段确定异常原因后,仅将该异常字段从与所述异常识别结果相关联的指标中剔除。在一些实施例中,由前文中可以看出,异常识别结果相关联的指标为监控指标之一,故此处将异常字段从监控指标中剔除,以便于基于监控指标中剩余字段继续识别异常。

[0095] 基于监控指标中剩余字段确定至少一个异常指标即为了寻找下一个异常识别结果相关联的指标,在一些实施例中,可以采用图2和图3中确定与异常识别结果相关联的指标的方式处理,具体可以参见步骤210以及步骤211～217相关描述,在此不过多赘述。

[0096] 基于所述异常指标确定新的异常字段,在一些实施例中,可以采用图2中确定异常字段的方式处理,具体可以参见步骤210～230相关描述,在此不过多赘述。

[0097] 可以看出，在一些实施例中，在将异常字段从监控指标中剔除后，针对监控指标中剩余字段进行了新的一轮迭代，以实现对异常原因进行归因下探，直至满足迭代截止条件。在每一次迭代时，对上一轮获取的异常原因和相关数据进行保存。继续采用步骤230中的示例，如第一次迭代确定异常原因为交易渠道指标中的网银指标出现异常，第二次迭代确定异常原因为交易时间指标中夜间出现异常，第三次迭代确定异常原因为交易笔数指标出现异常，那么可以针对日交易笔数的下降确定的原因是，某交易渠道在夜间交易时段上的交易笔数跌零导致的。

[0098] 在一些实施例中，迭代截止条件可以是一个预设的次数(如3次、5次、15次等)，还可以是基于异常识别结果无法在监控指标中确定至少一个与异常识别结果相关联的指标时截止。

[0099] 在一些实施例中，当迭代截止时，可以使该系统则输出时间粒度下(如每天/每小时)的运行结果，包括每一轮的异常归因详情(下探指标和字段、异常指标等)和相应的中间结果(如每一轮贡献度、JS散度等计算结果)，以便于业务负责人对数据加以分析。

[0100] 应当注意的是，上述图2～图4中有关流程的描述仅仅是为了示例和说明，而不限定本说明书的一些实施例的适用范围。对于本领域技术人员来说，在本说明书的一些实施例的指导下可以对流程进行各种修正和改变。然而，这些修正和改变仍在本说明书的范围之内。例如，步骤211～217与步骤210可以独立进行，两步骤没有必然的先后顺序。

[0101] 图5是根据本说明书一些实施例所示的一种基于异常识别结果确定异常原因的系统的示例性系统框图。

[0102] 如图5所示，一种基于异常识别结果确定异常原因的系统500可以包括异常识别结果获取模块510、影响因素确定模块520和异常原因确定模块530。这些模块也可以作为应用程序或一组由处理引擎读取和执行的指令实现。此外，模块可以是硬件电路和应用/指令的任何组合。例如，当处理引擎或处理器执行应用程序/一组指令时，模块可以是处理器的一部分。

[0103] 异常识别结果获取模块510可以用于获取至少一个与所述异常识别结果相关联的指标，每个所述指标包括多个字段，每个字段与某一预设的业务含义相关联。

[0104] 关于异常识别结果的更多描述，可以在本说明书的其他地方(如步骤210及其相关描述中)找到，在此不作赘述。

[0105] 影响因素确定模块520可以用于基于所述每个字段确定所述每个字段对所述异常识别结果的影响因素；所述影响因素包括所述每个字段的异常度和贡献度。

[0106] 关于影响因素的更多描述，可以在本说明书的其他地方(如步骤220及其相关描述中)找到，在此不作赘述。

[0107] 异常原因确定模块530可以用于基于所述影响因素在所述多个字段中确定至少一个字段为异常字段，基于所述异常字段确定异常原因。

[0108] 关于异常字段和异常原因的更多描述，可以在本说明书的其他地方(如步骤230及其相关描述中)找到，在此不作赘述。

[0109] 在一些实施例中，影响因素确定模块520中，所述异常度为群体稳定性指数、信息散度或詹森香农差异中的至少一个；所述贡献度基于所述字段以及所述字段所属的指标确定。

[0110] 在一些实施例中，影响因素确定模块520中，所述影响因素包括先验风险度；所述先验风险度为所述字段的风险预设权重。

[0111] 在一些实施例中，影响因素确定模块520中，基于所述异常度、所述贡献度和所述先验风险度在所述多个字段中确定至少一个对所述异常识别结果影响最大的字段，作为异常字段。

[0112] 在一些实施例中，异常识别结果获取模块510中，所述指标至少经过数据离散化处理。

[0113] 图6是根据本说明书一些实施例所示的异常识别结果获取模块的系统框图。

[0114] 如图6所示，在一些实施例中，异常识别结果获取模块510可以包括监控指标获取单元511、时序分解单元513、异常检测单元515和异常识别结果确定单元517。这些单元也可以作为应用程序或一组由处理引擎读取和执行的指令实现。此外，单元可以是硬件电路和应用/指令的任何组合。

[0115] 监控指标获取单元511可以用于获取多个监控指标；每个所述监控指标包括多个字段，每个字段与某一预设的业务含义相关联。

[0116] 关于监控指标的更多描述，可以在本说明书的其他地方(如步骤211及其相关描述中)找到，在此不作赘述。

[0117] 时序分解单元513可以用于基于时序分解算法去除所述监控指标中的周期分量，得到检验监控指标；

[0118] 关于时序分解算法和检验监控指标的更多描述，可以在本说明书的其他地方(如步骤213及其相关描述中)找到，在此不作赘述。

[0119] 异常检测单元515可以用于基于异常检测算法对所述检验监控指标进行处理，得到异常识别结果；

[0120] 关于异常检测算法和异常识别结果的更多描述，可以在本说明书的其他地方(如步骤215及其相关描述中)找到，在此不作赘述。

[0121] 异常识别结果确定单元517可以基于所述异常识别结果在所述监控指标中确定至少一个与所述异常识别结果相关联的指标。

[0122] 关于异常识别结果相关联的指标的更多描述，可以在本说明书的其他地方(如步骤217、步骤210及其相关描述中)找到，在此不作赘述。

[0123] 在一些实施例中，所述异常检测算法为假设检验算法，所述异常识别结果为检验统计量；基于所述检验统计量得到至少一个与所述异常识别结果相关联的指标。

[0124] 在一些实施例中，基于所述监控指标中包括的所述字段的数量，得到临界值；所述检验统计量不大于所述临界值时，当前监控指标没有异常。

[0125] 在一些实施例中，所述假设检验算法为混合泛化版极端学生化方差。

[0126] 在一些实施例中，所述时序分解算法为基于局部加权回归的季节性和趋势分解方法。

[0127] 在一些实施例中，将所述异常字段从所述监控指标中剔除；基于所述监控指标中剩余字段确定至少一个异常指标；基于所述异常指标确定新的异常字段，直至满足迭代截止条件。

[0128] 应当理解，图5和图6所示的装置及其模块、单元可以利用各种方式来实现。例如，

在一些实施例中，装置及其模块可以通过硬件、软件或者软件和硬件的结合来实现。其中，硬件部分可以利用专用逻辑来实现；软件部分则可以存储在存储器中，由适当的指令执行装置，例如微处理器或者专用设计硬件来执行。本领域技术人员可以理解上述的方法和装置可以使用计算机可执行指令和/或包含在处理器控制代码中来实现，例如在诸如磁盘、CD或DVD-ROM的载体介质、诸如只读存储器(固件)的可编程的存储器或者诸如光学或电子信号载体的数据载体上提供了这样的代码。本说明书的装置及其模块不仅可以有诸如超大规模集成电路或门阵列、诸如逻辑芯片、晶体管等的半导体、或者诸如现场可编程门阵列、可编程逻辑设备等的可编程硬件设备的硬件电路实现，也可以用例如由各种类型的处理器所执行的软件实现，还可以由上述硬件电路和软件的结合(例如，固件)来实现。

[0129] 需要注意的是，以上对于基于隐私保护的加密系统及其模块的描述，仅为描述方便，并不能把本说明书限制在所举实施例范围之内。可以理解，对于本领域的技术人员来说，在了解该装置的原理后，可能在不背离这一原理的情况下，对各个模块或单元进行任意组合，或者构成子装置与其他模块连接。例如，图6中时序分解单元513和异常检测单元515可以同为一个具备计算能力的单元，同一计算单元执行两种算法。又例如，基于异常识别结果确定异常原因的系统中的各个模块可以位于同一服务器上，也可以分属不同的服务器。诸如此类的变形，均在本说明书的保护范围之内。

[0130] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[0131] 本说明书实施例可能带来的有益效果包括但不限于：(1)通过引入了异常度、贡献度以及先验风险度的概念，对异常背后的真正原因进行启发式地搜索，从各维度聚集的数据异常出发并快速定位出合理的异常原因；(2)通过对各维度聚集的数据异常进一步下探，进行递归式搜索，逐层给出潜在维度的异常原因；(3)采用改良后的异常检测算法，一方面通过对时间序列进行分解并消除周期影响后生成新的时序；另一方面通过对检验统计量进行改良，使得异常检测达到稳健的效果。

[0132] 需要说明的是，不同实施例可能产生的有益效果不同，在不同的实施例里，可能产生的有益效果可以是以上任意一种或几种的组合，也可以是其他任何可能获得的有益效果。

[0133] 上文已对基本概念做了描述，显然，对于本领域技术人员来说，上述详细披露仅仅作为示例，而并不构成对本说明书的限定。虽然此处并没有明确说明，本领域技术人员可能会对本说明书进行各种修改、改进和修正。该类修改、改进和修正在本说明书中被建议，所以该类修改、改进、修正仍属于本说明书示范实施例的精神和范围。

[0134] 同时，本说明书使用了特定词语来描述本说明书的实施例。如“一个实施例”、“一实施例”、和/或“一些实施例”意指与本说明书至少一个实施例相关的某一特征、结构或特点。因此，应强调并注意的是，本说明书中在不同位置两次或多次提及的“一实施例”或“一个实施例”或“一个替代性实施例”并不一定是指同一实施例。此外，本说明书的一个或多个实施例中的某些特征、结构或特点可以进行适当的组合。

[0135] 此外，除非权利要求中明确说明，本说明书所述处理元素和序列的顺序、数字字母的使用、或其他名称的使用，并非用于限定本说明书流程和方法的顺序。尽管上述披露中通过各种示例讨论了一些目前认为有用的发明实施例，但应当理解的是，该类细节仅起到说明的目的，附加的权利要求并不仅限于披露的实施例，相反，权利要求旨在覆盖所有符合本说明书实施例实质和范围的修正和等价组合。例如，虽然以上所描述的系统组件可以通过硬件设备实现，但是也可以只通过软件的解决方案得以实现，如在现有的服务器或移动设备上安装所描述的系统。

[0136] 同理，应当注意的是，为了简化本说明书披露的表述，从而帮助对一个或多个发明实施例的理解，前文对本说明书实施例的描述中，有时会将多种特征归并至一个实施例、附图或对其的描述中。但是，这种披露方法并不意味着本说明书对象所需要的特征比权利要求中提及的特征多。实际上，实施例的特征要少于上述披露的单个实施例的全部特征。

[0137] 一些实施例中使用了描述成分、属性数量的数字，应当理解的是，此类用于实施例描述的数字，在一些示例中使用了修饰词“大约”、“近似”或“大体上”来修饰。除非另外说明，“大约”、“近似”或“大体上”表明所述数字允许有±20％的变化。相应地，在一些实施例中，说明书和权利要求中使用的数值参数均为近似值，该近似值根据个别实施例所需特点可以发生改变。在一些实施例中，数值参数应考虑规定的有效数位并采用一般位数保留的方法。尽管本说明书一些实施例中用于确认其范围广度的数值域和参数为近似值，在具体实施例中，此类数值的设定在可行范围内尽可能精确。

[0138] 针对本说明书引用的每个专利、专利申请、专利申请公开物和其他材料，如文章、书籍、说明书、出版物、文档等，特此将其全部内容并入本说明书作为参考。与本说明书内容不一致或产生冲突的申请历史文件除外，对本说明书权利要求最广范围有限制的文件(当前或之后附加于本说明书中的)也除外。需要说明的是，如果本说明书附属材料中的描述、定义、和/或术语的使用与本说明书所述内容有不一致或冲突的地方，以本说明书的描述、定义和/或术语的使用为准。

[0139] 最后，应当理解的是，本说明书中所述实施例仅用以说明本说明书实施例的原则。其他的变形也可能属于本说明书的范围。因此，作为示例而非限制，本说明书实施例的替代配置可视为与本说明书的教导一致。相应地，本说明书的实施例不仅限于本说明书明确介绍和描述的实施例。

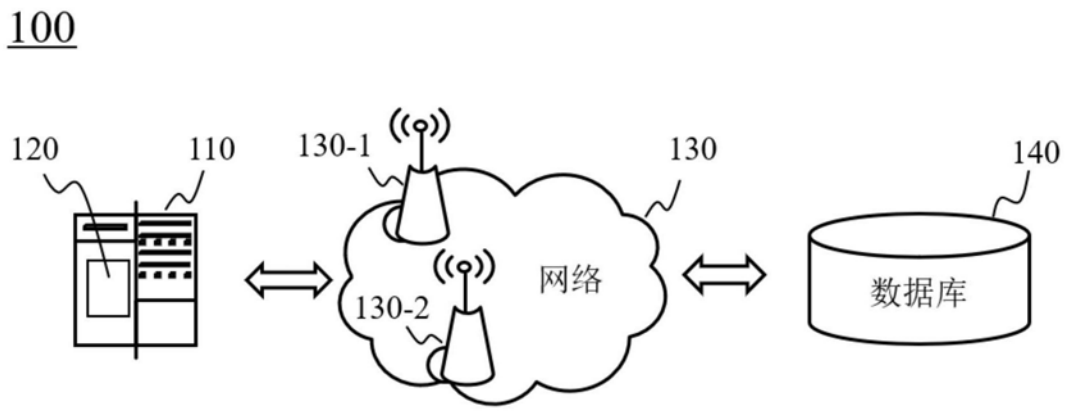

100
120
110
130-1
130
140
网络
130-2
数据库

图1

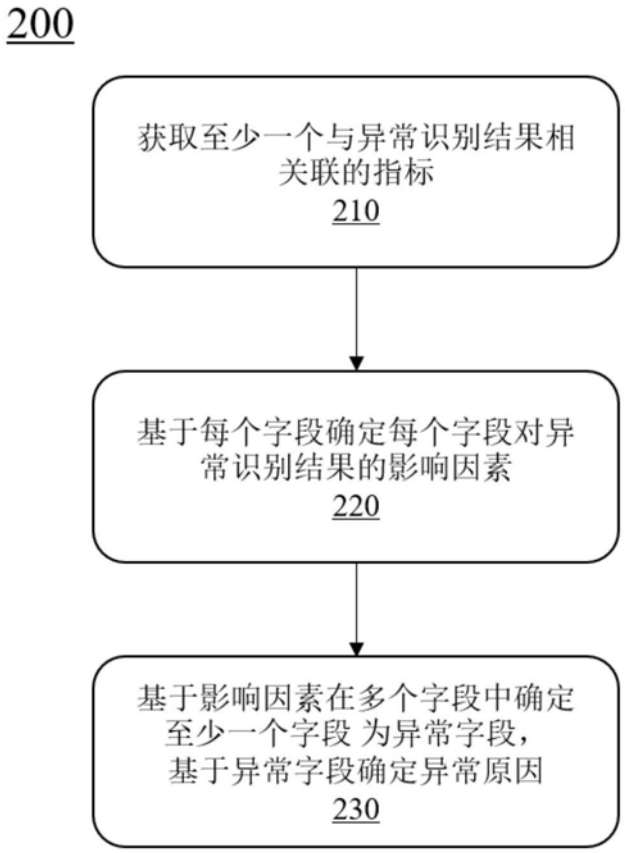

200
获取至少一个与异常识别结果相关联的指标
210
基于每个字段确定每个字段对异常识别结果的影响因素
220
基于影响因素在多个字段中确定至少一个字段 为异常字段，基于异常字段确定异常原因
230

图2

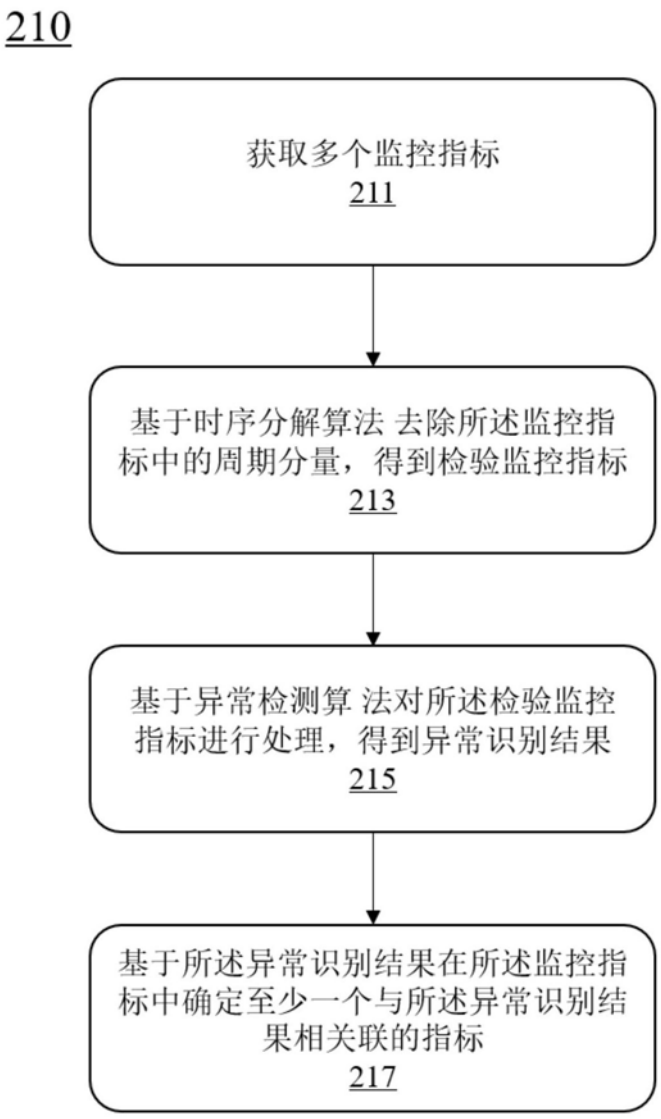

210
获取多个监控指标
211
基于时序分解算法 去除所述监控指标中的周期分量，得到检验监控指标
213
基于异常检测算 法对所述检验监控指标进行处理，得到异常识别结果
215
基于所述异常识别结果在所述监控指标中确定至少一个与所述异常识别结果相关联的指标
217

图3

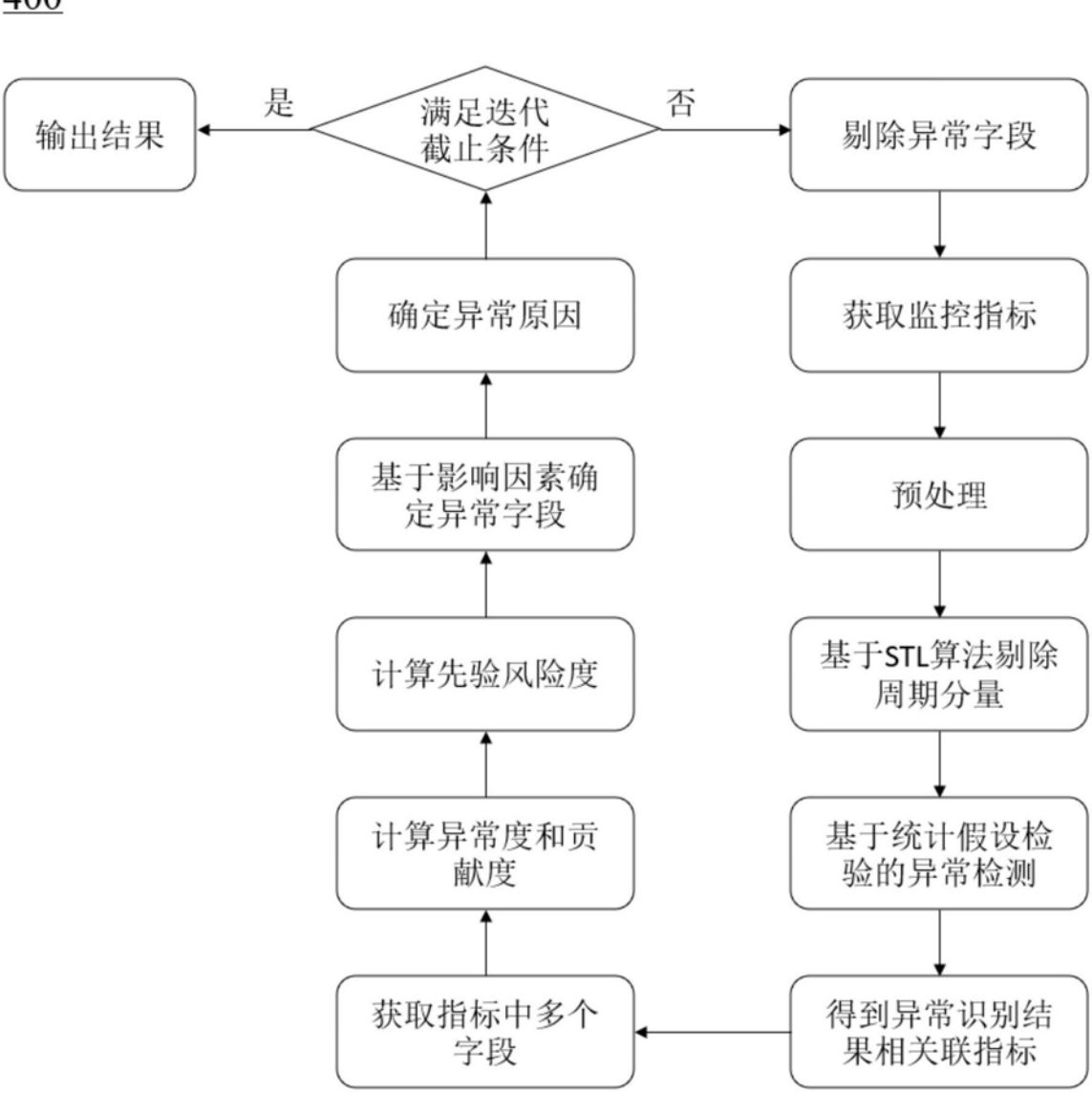

400
输出结果
是
满足迭代截止条件
否
剔除异常字段
获取监控指标
预处理
基于STL算法剔除周期分量
基于统计假设检验的异常检测
得到异常识别结果相关联指标
获取指标中多个字段
计算异常度和贡献度
计算先验风险度
基于影响因素确定异常字段
确定异常原因

图4

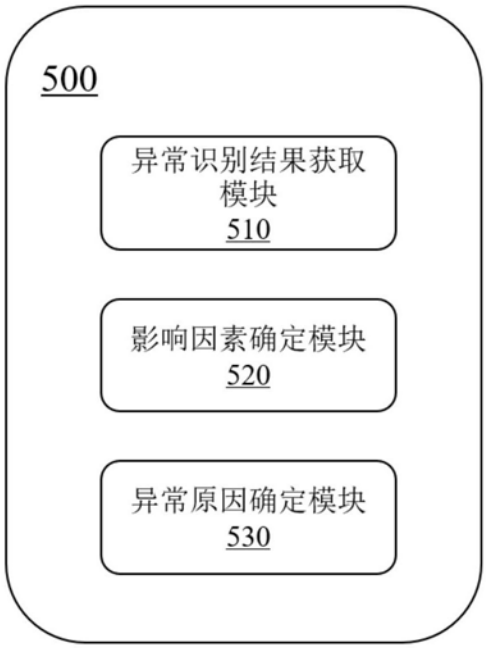

500
异常识别结果获取模块
510
影响因素确定模块
520
异常原因确定模块
530

图5

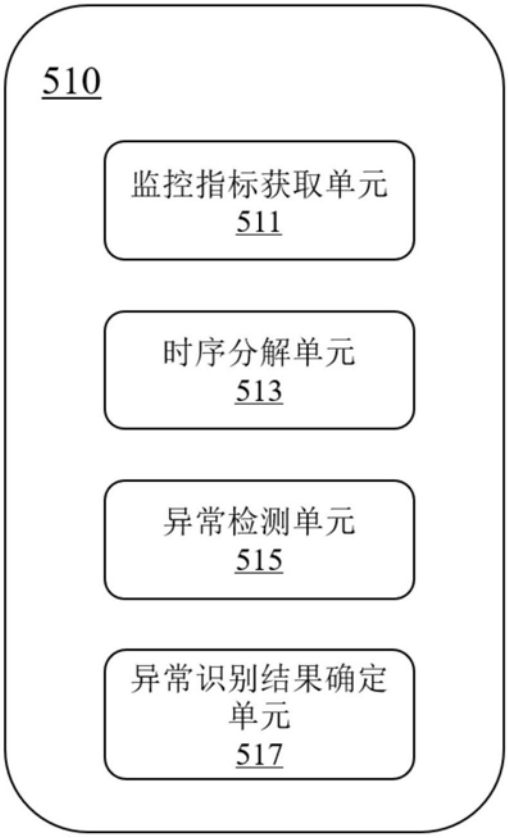

510
监控指标获取单元
511
时序分解单元
513
异常检测单元
515
异常识别结果确定单元
517

图6