(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116821750 A
(43)申请公布日 2023.09.29

(21)申请号 202310627695.5

(22)申请日 2023.05.30

(71)申请人 北京东方通网信科技有限公司
地址 100044 北京市海淀区中关村南大街2号1号楼19层A座2201

(72)发明人 黄永军 李睿凡 周春楠 孙健

(74)专利代理机构 北京辰权知识产权代理有限公司 11619
专利代理师 刘广达

(51)Int.Cl.
G06F 18/24(2023.01)
G06Q 10/0639(2023.01)
G06F 16/2455(2019.01)
G06F 21/62(2013.01)

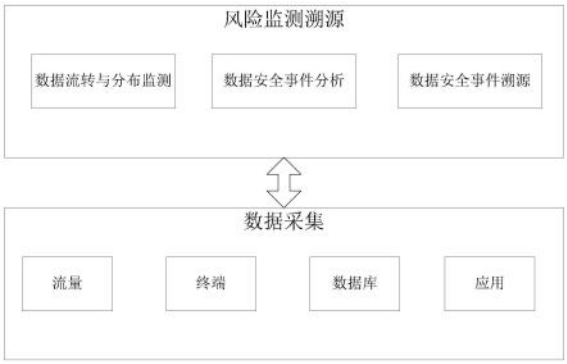
权利要求书3页 说明书8页 附图4页

(54)发明名称

一种基于人工智能的数据安全风险监测追溯系统

(57)摘要

本申请提供一种基于人工智能的数据安全风险监测追溯系统，包括：数据采集模块，用于实时采集企业侧各类安全事件信息，所述各类安全事件信息包括流量、终端、数据库、应用，建立数据识别特征库；数据流转与分布监测模块，用于解析所述各类安全事件信息的规则与策略，发现数据资产保护对象，生成数据资产清单，并动态监测数据分布与流转，获取数据流转规则和访问控制规则；数据安全事件分析模块，用于智能分析识别数据在采集共享处理过程中的安全风险，对数据分类分级管理，根据数据识别特征库、数据流转规则和访问控制规则建立数据安全风险监测策略库；数据安全事件溯源模块，基于人工智能对实时安全事件进行溯源分析，并将安全事件和溯源信息进行及时上报。



CN 116821750 A

1.一种基于人工智能的数据安全风险监测追溯系统,其特征在于,包括:

数据采集模块,用于实时采集企业侧各类安全事件信息,所述各类安全事件信息包括流量、终端、数据库、应用,建立数据识别特征库;

数据流转与分布监测模块,用于解析所述各类安全事件信息的规则与策略,发现数据资产保护对象,生成数据资产清单,并动态监测数据分布与流转,获取数据流转规则和访问控制规则;

数据安全事件分析模块,用于智能分析识别数据在采集共享处理过程中的安全风险,对数据分类分级管理,根据数据识别特征库、数据流转规则和访问控制规则建立数据安全风险监测策略库;

数据安全事件溯源模块,基于人工智能对实时安全事件进行溯源分析,并将安全事件和溯源信息进行及时上报。

2.根据权利要求1所述的系统,其特征在于,

所述数据采集模块,包括:

S1、根据预设安全事件类型集合,实时采集企业侧各类安全事件信息,所述各类安全事件信息包括流量、终端、数据库、应用;

S2、根据安全事件类型集合,判定获取到的安全事件信息是否可表征网络受到威胁,其中,所述安全事件信息为原始采集信息或异常行为信息;

S3、若判定所述安全事件信息可表征网络受到威胁,则根据所述安全事件类型集合、网络上下文信息和所述安全事件信息中的任意一种或多种,生成数据识别特征库,其中,所述数据识别特征库基于统一描述格式进行归一化描述。

3.根据权利要求2所述的系统,其特征在于,

所述步骤S1包括:获取安全事件特征和/或安全事件关联规则,以构建安全事件类型集合;其中,所述安全事件关联规则包括异常行为属性信息、异常行为属性值、异常行为属性阈值和运算符中的任意一种或多种;

步骤S2包括:

对原始采集信息进行解析,生成原始采集信息解析结果;

将所述原始采集信息解析结果与所述安全事件关联规则进行匹配,并根据匹配结果判定所述原始采集信息是否可表征网络受到威胁,包括:对安全事件关联规则进行实例化,形成实例化关联规则;将所述实例化关联规则中的异常行为属性信息与所述原始采集信息解析结果进行匹配;若匹配成功,则判断所述实例化关联规则是否满足第一预设条件;若所述实例化关联规则满足所述第一预设条件,则触发状态转移;若状态转移后为威胁状态,则将生成所述原始采集信息的原始安全事件定义为威胁事件,并判定所述原始采集信息可表征网络受到威胁。

4.根据权利要求3所述的系统,其特征在于,

所述数据流转与分布监测模块,具体包括如下步骤:

采集网络安全日志以及网络安全流量;

根据网络安全主站系统下发的日志/流量规则分析出IP设备的自身脆弱性安全事件以及所述IP设备遭受到的外部攻击安全事件;

根据所述网络安全主站系统下发的告警分析规则、自身日志的告警分析规则,提取网

络安全日志数据以及网络安全流量数据的外部攻击特征以及自身脆弱性特征，形成网络安全告警；

根据所述网络安全主站系统下发的控制指令，生成遭受到攻击行为的IP资产清单；

确定IP资产清单的数据血缘信息、数据流转信息，以及数据访问信息；

根据所述数据血缘信息和数据流转信息，形成数据维度的数据流转拓扑图；

根据所述数据血缘信息和数据访问信息，形成访问维度的数据流转拓扑图；

根据所述数据维度的数据流转拓扑图和所述访问维度的数据流转拓扑图，结合设定的数据流转规则检测数据访问异常。

5.根据权利要求4所述的系统，其特征在于，

所述数据安全事件分析模块，包括以下步骤：

对数据安全事件进行分类，确定其关键要素，实现风险数据的结构化；

采用事件语义抽取技术识别数据识别特征库的安全风险；

风险预警，构建多级风险传导预警模型，从数据识别特征库中获取风险数据，根据风险数据超出阈值的范围来动态调整各级指标的权重，实现各类安全风险以及综合风险的动态监测，并输出风险预测值；

风险态势监测，将选定时间范围内的各类安全风险变化趋势进行可视化，发送预警信息给相应接收端，并将风险信息在地图上展现出来；

将每个被识别为威胁的安全事件，根据数据识别特征库、数据流转规则和访问控制规则建立一条监测记录，将所有监测记录归并为数据安全风险监测策略库。

6.根据权利要求5所述的系统，其特征在于，

所述对数据安全事件进行分类，确定其关键要素，实现风险数据的结构化，包括如下步骤：基于安全事件样本，通过熵值法确定各类安全风险事件中二级指标和一级指标的权重，确定二级指标的阈值、一级指标的阈值和综合风险阈值，根据阈值将安全风险划分为一般、较重、严重、特别严重四个等级，并存入对应的数据库表中；确定时间区间，从数据识别特征库中抽取相应时间段内一级指标和对应二级指标的安全事件实例，根据事件实例中二级指标超出阈值的情况，对事件实例下的二级指标的权重进行调整，并对各项二级指标的值进行标准化处理，根据调整后的二级指标权重来计算一级指标的预测值；根据二级指标超出阈值的情况，对一级指标的权重进行调整，根据一级指标的预测值和调整后的权重计算综合风险的预测值；将综合风险的预测值以及各个一级指标的预测值输出到数据识别特征库中。

7.根据权利要求6所述的系统，其特征在于，

所述数据安全事件溯源模块，包括如下步骤：

将实时安全事件在所述数据安全风险监测策略库包括的数据维度的数据流转拓扑图和访问维度的数据流转拓扑图中进行查找，确定威胁事件或者遭受到攻击行为的IP资产；

基于所述威胁事件或者遭受到攻击行为的IP资产以及安全实体之间的关系生成风险信息对应的告警溯源信息；

对所述威胁事件或者遭受到攻击行为的IP资产进行标识，生成目标告警标识；

将所述目标告警标识添加至所述数据流转拓扑图中。

8.根据权利要求7所述的系统，其特征在于，

在生成所述告警溯源信息之后，还可以包括：

在接收到告警查询指令的情况下，通过所述告警查询指令中包括的第一告警标识在所述数据流转拓扑图中查找对应的IP资产；

基于所述IP资产以及安全实体之间的关系，获取所述告警查询指令对应的第一告警溯源信息。

9.一种电子设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，其特征在于，所述处理器运行所述计算机程序以实现如权利要求1-8任一项所述的系统。

10.一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实现如权利要求1-8中任一项所述的系统。

一种基于人工智能的数据安全风险监测追溯系统

技术领域

[0001] 本申请涉及数据安全技术领域，尤其涉及一种基于人工智能的数据安全风险监测追溯系统。

背景技术

[0002] 近年全球范围内来针对工业领域的网络攻击事件频发，涉及汽车生产、智能制造、能源电力、烟草等诸多行业，导致工业主机蓝屏、重要文件被加密，更严重的造成了工业企业停工停产，给企业带来重大损失。这一系列攻击事件表明，工业互联网已成为网络攻击的靶标。

[0003] 而在传统互联网时代，企业对网络安全习惯采取“事后补救”的措施，但是这种“头痛医头、脚痛医脚”的局部、针对单点的方法是无法满足当前新型工业互联网的安全需求的，工业企业亟需转变思维，改进网络安全措施和方法，才能跟上数字时代的步伐。

发明内容

[0004] 有鉴于此，本申请的目的在于提出一种基于人工智能的数据安全风险监测追溯系统，本申请能够针对性的解决现有的问题。

[0005] 基于上述目的，本申请还提出了一种基于人工智能的数据安全风险监测追溯系统，包括：

[0006] 数据采集模块，用于实时采集企业侧各类安全事件信息，所述各类安全事件信息包括流量、终端、数据库、应用，建立数据识别特征库；

[0007] 数据流转与分布监测模块，用于解析所述各类安全事件信息的规则与策略，发现数据资产保护对象，生成数据资产清单，并动态监测数据分布与流转，获取数据流转规则和访问控制规则；

[0008] 数据安全事件分析模块，用于智能分析识别数据在采集共享处理过程中的安全风险，对数据分类分级管理，根据数据识别特征库、数据流转规则和访问控制规则建立数据安全风险监测策略库；

[0009] 数据安全事件溯源模块，基于人工智能对实时安全事件进行溯源分析，并将安全事件和溯源信息进行及时上报。

[0010] 进一步地，所述数据采集模块，包括：

[0011] S1、根据预设安全事件类型集合，实时采集企业侧各类安全事件信息，所述各类安全事件信息包括流量、终端、数据库、应用；

[0012] S2、根据安全事件类型集合，判定获取到的安全事件信息是否可表征网络受到威胁，其中，所述安全事件信息为原始采集信息或异常行为信息；

[0013] S3、若判定所述安全事件信息可表征网络受到威胁，则根据所述安全事件类型集合、网络上下文信息和所述安全事件信息中的任意一种或多种，生成数据识别特征库，其中，所述数据识别特征库基于统一描述格式进行归一化描述。

[0014] 进一步地，所述步骤S1包括：获取安全事件特征和/或安全事件关联规则，以构建安全事件类型集合；其中，所述安全事件关联规则包括异常行为属性信息、异常行为属性值、异常行为属性阈值和运算符中的任意一种或多种；

[0015] 步骤S2包括：

[0016] 对原始采集信息进行解析，生成原始采集信息解析结果；

[0017] 将所述原始采集信息解析结果与所述安全事件关联规则进行匹配，并根据匹配结果判定所述原始采集信息是否可表征网络受到威胁，包括：对安全事件关联规则进行实例化，形成实例化关联规则；将所述实例化关联规则中的异常行为属性信息与所述原始采集信息解析结果进行匹配；若匹配成功，则判断所述实例化关联规则是否满足第一预设条件；若所述实例化关联规则满足所述第一预设条件，则触发状态转移；若状态转移后为威胁状态，则将生成所述原始采集信息的原始安全事件定义为威胁事件，并判定所述原始采集信息可表征网络受到威胁。

[0018] 进一步地，所述数据流转与分布监测模块，具体包括如下步骤：

[0019] 采集网络安全日志以及网络安全流量；

[0020] 根据网络安全主站系统下发的日志/流量规则分析出IP设备的自身脆弱性安全事件以及所述IP设备遭受到的外部攻击安全事件；

[0021] 根据所述网络安全主站系统下发的告警分析规则、自身日志的告警分析规则，提取网络安全日志数据以及网络安全流量数据的外部攻击特征以及自身脆弱性特征，形成网络安全告警；

[0022] 根据所述网络安全主站系统下发的控制指令，生成遭受到攻击行为的IP资产清单；

[0023] 确定IP资产清单的数据血缘信息、数据流转信息，以及数据访问信息；

[0024] 根据所述数据血缘信息和数据流转信息，形成数据维度的数据流转拓扑图；

[0025] 根据所述数据血缘信息和数据访问信息，形成访问维度的数据流转拓扑图；

[0026] 根据所述数据维度的数据流转拓扑图和所述访问维度的数据流转拓扑图，结合设定的数据流转规则检测数据访问异常。

[0027] 进一步地，所述数据安全事件分析模块，包括以下步骤：

[0028] 对数据安全事件进行分类，确定其关键要素，实现风险数据的结构化；

[0029] 采用事件语义抽取技术识别数据识别特征库的安全风险；

[0030] 风险预警，构建多级风险传导预警模型，从数据识别特征库中获取风险数据，根据风险数据超出阈值的范围来动态调整各级指标的权重，实现各类安全风险以及综合风险的动态监测，并输出风险预测值；

[0031] 风险态势监测，将选定时间范围内的各类安全风险变化趋势进行可视化，发送预警信息给相应接收端，并将风险信息在地图上展现出来；

[0032] 将每个被识别为威胁的安全事件，根据数据识别特征库、数据流转规则和访问控制规则建立一条监测记录，将所有监测记录归并为数据安全风险监测策略库。

[0033] 进一步地，所述对数据安全事件进行分类，确定其关键要素，实现风险数据的结构化，包括如下步骤：步骤2-1、基于安全事件样本，通过熵值法确定各类安全风险事件中二级指标和一级指标的权重，确定二级指标的阈值、一级指标的阈值和综合风险阈值，根据阈值

将安全风险划分为一般、较重、严重、特别严重四个等级，并存入对应的数据库表中；步骤2-2、确定时间区间，从数据识别特征库中抽取相应时间段内一级指标和对应二级指标的安全事件实例，根据事件实例中二级指标超出阈值的情况，对事件实例下的二级指标的权重进行调整，并对各项二级指标的值进行标准化处理，根据调整后的二级指标权重来计算一级指标的预测值；步骤2-3、根据二级指标超出阈值的情况，对一级指标的权重进行调整，根据一级指标的预测值和调整后的权重计算综合风险的预测值；步骤2-4、将综合风险的预测值以及各个一级指标的预测值输出到数据识别特征库中。

[0034] 进一步地，所述数据安全事件溯源模块，包括如下步骤：

[0035] 将实时安全事件在所述数据安全风险监测策略库包括的数据维度的数据流转拓扑图和访问维度的数据流转拓扑图中进行查找，确定威胁事件或者遭受到攻击行为的IP资产；

[0036] 基于所述威胁事件或者遭受到攻击行为的IP资产以及安全实体之间的关系生成风险信息对应的告警溯源信息；

[0037] 对所述威胁事件或者遭受到攻击行为的IP资产进行标识，生成目标告警标识；

[0038] 将所述目标告警标识添加至所述数据流转拓扑图中。

[0039] 进一步地，在生成所述告警溯源信息之后，还可以包括：

[0040] 在接收到告警查询指令的情况下，通过所述告警查询指令中包括的第一告警标识在所述数据流转拓扑图中查找对应的IP资产；

[0041] 基于所述IP资产以及安全实体之间的关系，获取所述告警查询指令对应的第一告警溯源信息。

[0042] 总的来说，本申请的优势及给用户带来的体验在于：

[0043] 通过体系化数据安全管控建设，梳理数据资产，制定分级分类策略，联动企业侧监测系统，实现对数据安全风险的实时监测、主动识别、精准定位、自动溯源，保障工业互联网数据安全，护航工业企业数字化转型。

附图说明

[0044] 在附图中，除非另外规定，否则贯穿多个附图相同的附图标记表示相同或相似的部件或元素。这些附图不一定是按照比例绘制的。应该理解，这些附图仅描绘了根据本申请公开的一些实施方式，而不应将其视为是对本申请范围的限制。

[0045] 图1示出根据本申请实施例的基于人工智能的数据安全风险监测追溯系统的构成图。

[0046] 图2示出数据采集模块的具体实现方法示意图。

[0047] 图3示出根据本申请实施例的数据安全事件分析的具体实现方法示意图。

[0048] 图4示出根据本申请实施例的数据安全事件溯源的具体实现方法示意图。

[0049] 图5示出了本申请一实施例所提供的一种电子设备的结构示意图。

[0050] 图6示出了本申请一实施例所提供的一种存储介质的示意图。

具体实施方式

[0051] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是，此处所描

述的具体实施例仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与有关发明相关的部分。

[0052] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0053] 本申请的数据安全风险监测追溯系统，研发数据安全风险监测追溯与综合管理平台，旨在掌握重要工业基础设施数据安全状态，支撑国家工业互联网安全监管工作，提升企业工业互联网数据安全水平，有效带动工业互联网安全技术创新和产业发展，助力制造强国和网络强国建设。依据数据分类分级标准，结合行业场景对行业数据依据敏感度建立流转与交换使用的规范，提高行业数据开放共享水平，从标准层面支撑数据资产的有效分级分类管理。

[0054] 申请实施例提供了一种基于人工智能的数据安全风险监测追溯系统，如图1所示，该系统包括：

[0055] 数据采集模块，用于实时采集企业侧各类安全事件信息，所述各类安全事件信息包括流量、终端、数据库、应用，建立数据识别特征库；

[0056] 数据流转与分布监测模块，用于解析所述各类安全事件信息的规则与策略，发现数据资产保护对象，生成数据资产清单，并动态监测数据分布与流转，获取数据流转规则和访问控制规则；

[0057] 数据安全事件分析模块，用于智能分析识别数据在采集共享处理过程中的安全风险，对数据分类分级管理，根据数据识别特征库、数据流转规则和访问控制规则所述建立数据安全风险监测策略库；

[0058] 数据安全事件溯源模块，基于人工智能对实时安全事件进行溯源分析，并将安全事件和溯源信息进行及时上报。

[0059] 如此，本申请与行业侧联动强化数据资产分类分级管理，实现实时监测数据安全风险态势，对风险源头角色自动追踪溯源。

[0060] 以下详细介绍每个模块的具体实现方式及技术细节：

[0061] 数据采集模块，如图2所示，包括以下步骤：

[0062] S1、根据预设安全事件类型集合，实时采集企业侧各类安全事件信息，所述各类安全事件信息包括流量、终端、数据库、应用；

[0063] 具体的，步骤S1包括：获取安全事件特征和/或安全事件关联规则，以构建安全事件类型集合；其中，所述安全事件关联规则包括异常行为属性信息、异常行为属性值、异常行为属性阈值和运算符中的任意一种或多种；

[0064] S2、根据安全事件类型集合，判定获取到的安全事件信息是否可表征网络受到威胁，其中，所述安全事件信息为原始采集信息或异常行为信息；

[0065] 具体的，步骤S2包括：

[0066] 对原始采集信息进行解析，生成原始采集信息解析结果；

[0067] 将所述原始采集信息解析结果与所述安全事件关联规则进行匹配，并根据匹配结果判定所述原始采集信息是否可表征网络受到威胁，包括：对安全事件关联规则进行实例化，形成实例化关联规则；将所述实例化关联规则中的异常行为属性信息与所述原始采集信息解析结果进行匹配；若匹配成功，则判断所述实例化关联规则是否满足第一预设条件；

若所述实例化关联规则满足所述第一预设条件，则触发状态转移；若状态转移后为威胁状态，则将生成所述原始采集信息的原始安全事件定义为威胁事件，并判定所述原始采集信息可表征网络受到威胁。

[0068] S3、若判定所述安全事件信息可表征网络受到威胁，则根据所述安全事件类型集合、网络上下文信息和所述安全事件信息中的任意一种或多种，生成数据识别特征库，其中，所述数据识别特征库基于统一描述格式进行归一化描述。

[0069] 所述统一描述格式包括：威胁类型、威胁对象、威胁对象特征、威胁对象表现特征、威胁范围、威胁级别、威胁起止时间、攻击者、攻击者特征、攻击方式、攻击路径、信息共享者和信息接收者中的任意一种或多种。

[0070] 数据流转与分布监测模块，具体包括如下步骤：

[0071] 采集网络安全日志以及网络安全流量；

[0072] 根据网络安全主站系统下发的日志/流量规则分析出IP设备的自身脆弱性安全事件以及所述IP设备遭受到的外部攻击安全事件；

[0073] 根据所述网络安全主站系统下发的告警分析规则、自身日志的告警分析规则，提取网络安全日志数据以及网络安全流量数据的外部攻击特征以及自身脆弱性特征，形成网络安全告警；

[0074] 根据所述网络安全主站系统下发的控制指令，生成遭受到攻击行为的IP资产清单；

[0075] 确定IP资产清单的数据血缘信息、数据流转信息，以及数据访问信息；

[0076] 根据所述数据血缘信息和数据流转信息，形成数据维度的数据流转拓扑图；

[0077] 根据所述数据血缘信息和数据访问信息，形成访问维度的数据流转拓扑图；

[0078] 根据所述数据维度的数据流转拓扑图和所述访问维度的数据流转拓扑图，结合设定的数据流转规则检测数据访问异常。

[0079] 在这个模块中，上述的数据血缘信息能够用于描述IP资产清单中的数据(可以被称为第一数据，第一数据存储在IP资产清单对应的后台数据库中)，与IP资产清单所属的原始数据库(可以被称为第二数据)之间的血缘信息。

[0080] 数据安全事件分析模块，如图3所示，包括如下步骤：

[0081] S21、对数据安全事件进行分类，确定其关键要素，实现风险数据的结构化；

[0082] S22、采用事件语义抽取技术识别数据识别特征库的安全风险；

[0083] S23、风险预警，构建多级风险传导预警模型，从数据识别特征库中获取风险数据，根据风险数据超出阈值的范围来动态调整各级指标的权重，实现各类安全风险以及综合风险的动态监测，并输出风险预测值；

[0084] S24、风险态势监测，将选定时间范围内的各类安全风险变化趋势进行可视化，发送预警信息给相应接收端，并将风险信息在地图上展现出来；

[0085] S25、将每个被识别为威胁的安全事件，根据数据识别特征库、数据流转规则和访问控制规则建立一条监测记录，将所有监测记录归并为数据安全风险监测策略库。

[0086] 步骤S32包括如下步骤：步骤2-1、基于安全事件样本，通过熵值法确定各类安全风险事件中二级指标和一级指标的权重，确定二级指标的阈值、一级指标的阈值和综合风险阈值，根据阈值将安全风险划分为一般、较重、严重、特别严重四个等级，并存入对应的数据

库表中;步骤2-2、确定时间区间,从数据识别特征库中抽取相应时间段内一级指标和对应二级指标的安全事件实例,根据事件实例中二级指标超出阈值的情况,对事件实例下的二级指标的权重进行调整,并对各项二级指标的值进行标准化处理,根据调整后的二级指标权重来计算一级指标的预测值;步骤2-3、根据二级指标超出阈值的情况,对一级指标的权重进行调整,根据一级指标的预测值和调整后的权重计算综合风险的预测值;步骤2-4、将综合风险的预测值以及各个一级指标的预测值输出到数据识别特征库中。

[0087] 数据安全事件溯源模块,如图4所示,包括如下步骤:

[0088] S31、将实时安全事件在所述数据安全风险监测策略库包括的数据维度的数据流转拓扑图和访问维度的数据流转拓扑图中进行查找,确定威胁事件或者遭受到攻击行为的IP资产;

[0089] S32、基于所述威胁事件或者遭受到攻击行为的IP资产以及安全实体之间的关系生成风险信息对应的告警溯源信息;

[0090] S33、对所述威胁事件或者遭受到攻击行为的IP资产进行标识,生成目标告警标识;

[0091] S34、将所述目标告警标识添加至所述数据流转拓扑图中。

[0092] 进一步的,在生成所述告警溯源信息之后,还可以包括:

[0093] 在接收到告警查询指令的情况下,通过所述告警查询指令中包括的第一告警标识在所述数据流转拓扑图中查找对应的IP资产;

[0094] 基于所述IP资产以及安全实体之间的关系,获取所述告警查询指令对应的第一告警溯源信息。

[0095] 请参考图5,其示出了本申请的一些实施方式所提供的一种电子设备的示意图。如图5所示,所述电子设备20包括:处理器200,存储器201,总线202和通信接口203,所述处理器200、通信接口203和存储器201通过总线202连接;所述存储器201中存储有可在所述处理器200上运行的计算机程序,所述处理器200运行所述计算机程序时执行本申请前述任一实施方式所提供的基于人工智能的数据安全风险监测追溯系统。

[0096] 其中,存储器201可能包含高速随机存取存储器(RAM:Random Access Memory),也可能还包括非不稳定的存储器(non-volatile memory),例如至少一个磁盘存储器。通过至少一个通信接口203(可以是有线或者无线)实现该系统网元与至少一个其他网元之间的通信连接,可以使用互联网、广域网、本地网、城域网等。

[0097] 总线202可以是ISA总线、PCI总线或EISA总线等。所述总线可以分为地址总线、数据总线、控制总线等。其中,存储器201用于存储程序,所述处理器200在接收到执行指令后,执行所述程序,前述本申请实施例任一实施方式揭示的所述基于人工智能的数据安全风险监测追溯系统可以应用于处理器200中,或者由处理器200实现。

[0098] 处理器200可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器200中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器200可以是通用处理器,包括中央处理器(Central Processing Unit,简称CPU)、网络处理器(Network Processor,简称NP)等;还可以是数字信号处理器(DSP)、专用集成电路(ASIC)、现成可编程门阵列(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。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑

框图。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。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器201，处理器200读取存储器201中的信息，结合其硬件完成上述方法的步骤。

[0099] 本申请实施例提供的电子设备与本申请实施例提供的基于人工智能的数据安全风险监测追溯系统出于相同的发明构思，具有与其采用、运行或实现的方法相同的有益效果。

[0100] 本申请实施方式还提供一种与前述实施方式所提供的基于人工智能的数据安全风险监测追溯系统对应的计算机可读存储介质，请参考图6，其示出的计算机可读存储介质为光盘30，其上存储有计算机程序(即程序产品)，所述计算机程序在被处理器运行时，会执行前述任意实施方式所提供的基于人工智能的数据安全风险监测追溯系统。

[0101] 需要说明的是，所述计算机可读存储介质的例子还可以包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他光学、磁性存储介质，在此不再一一赘述。

[0102] 本申请的上述实施例提供的计算机可读存储介质与本申请实施例提供的基于人工智能的数据安全风险监测追溯系统出于相同的发明构思，具有与其存储的应用程序所采用、运行或实现的方法相同的有益效果。

[0103] 需要说明的是：

[0104] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备有固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本申请也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本申请的内容，并且上面对特定语言所做的描述是为了披露本申请的最佳实施方式。

[0105] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本申请的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0106] 类似地，应当理解，为了精简本申请并帮助理解各个发明方面中的一个或多个，在上面对本申请的示例性实施例的描述中，本申请的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本申请要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本申请的单独实施例。

[0107] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或

子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0108] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本申请的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0109] 本申请的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本申请实施例的虚拟机的创建系统中的一些或者全部部件的一些或者全部功能。本申请还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者系统程序(例如，计算机程序和计算机程序产品)。这样的实现本申请的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0110] 应该注意的是上述实施例对本申请进行说明而不是对本申请进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本申请可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干系统的单元权利要求中，这些系统中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0111] 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，可轻易想到其各种变化或替换，这些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所述权利要求的保护范围为准。

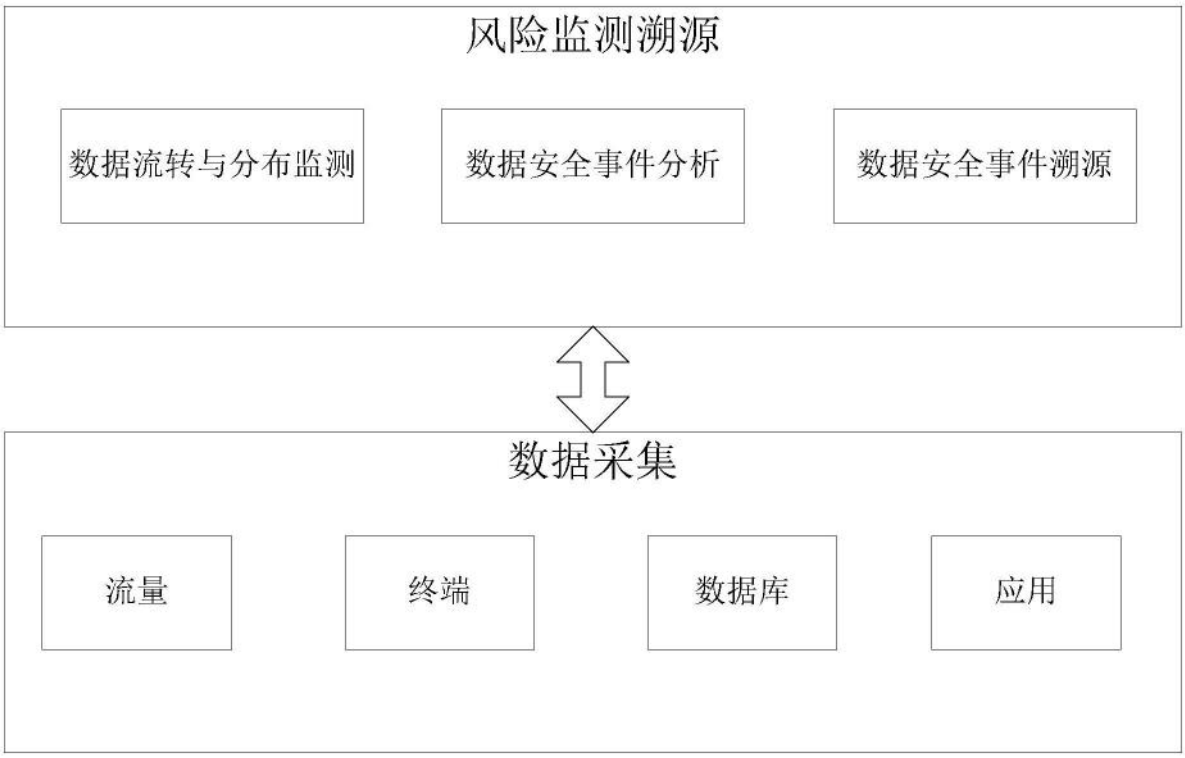

风险监测溯源
数据流转与分布监测
数据安全事件分析
数据安全事件溯源
数据采集
流量
终端
数据库
应用

图1

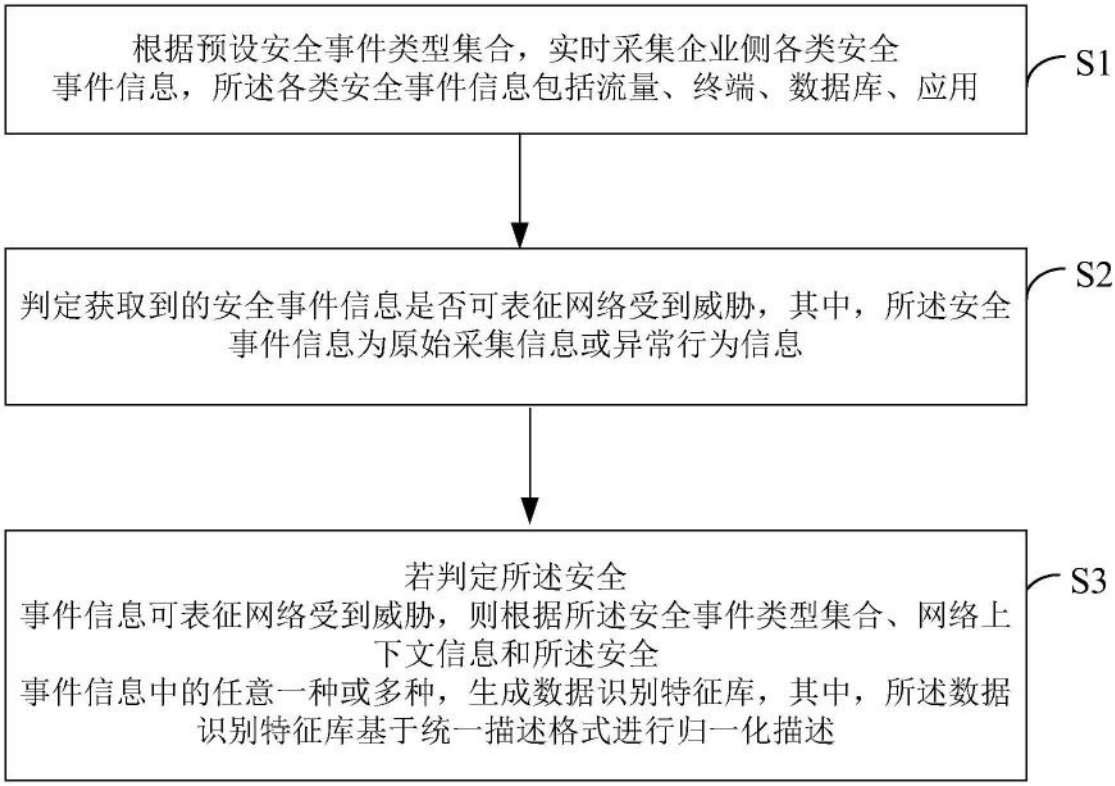

根据预设安全事件类型集合，实时采集企业侧各类安全事件信息，所述各类安全事件信息包括流量、终端、数据库、应用
S1
判定获取到的安全事件信息是否可表征网络受到威胁，其中，所述安全事件信息为原始采集信息或异常行为信息
S2
若判定所述安全事件信息可表征网络受到威胁，则根据所述安全事件类型集合、网络上下文信息和所述安全事件信息中的任意一种或多种，生成数据识别特征库，其中，所述数据识别特征库基于统一描述格式进行归一化描述
S3

图2

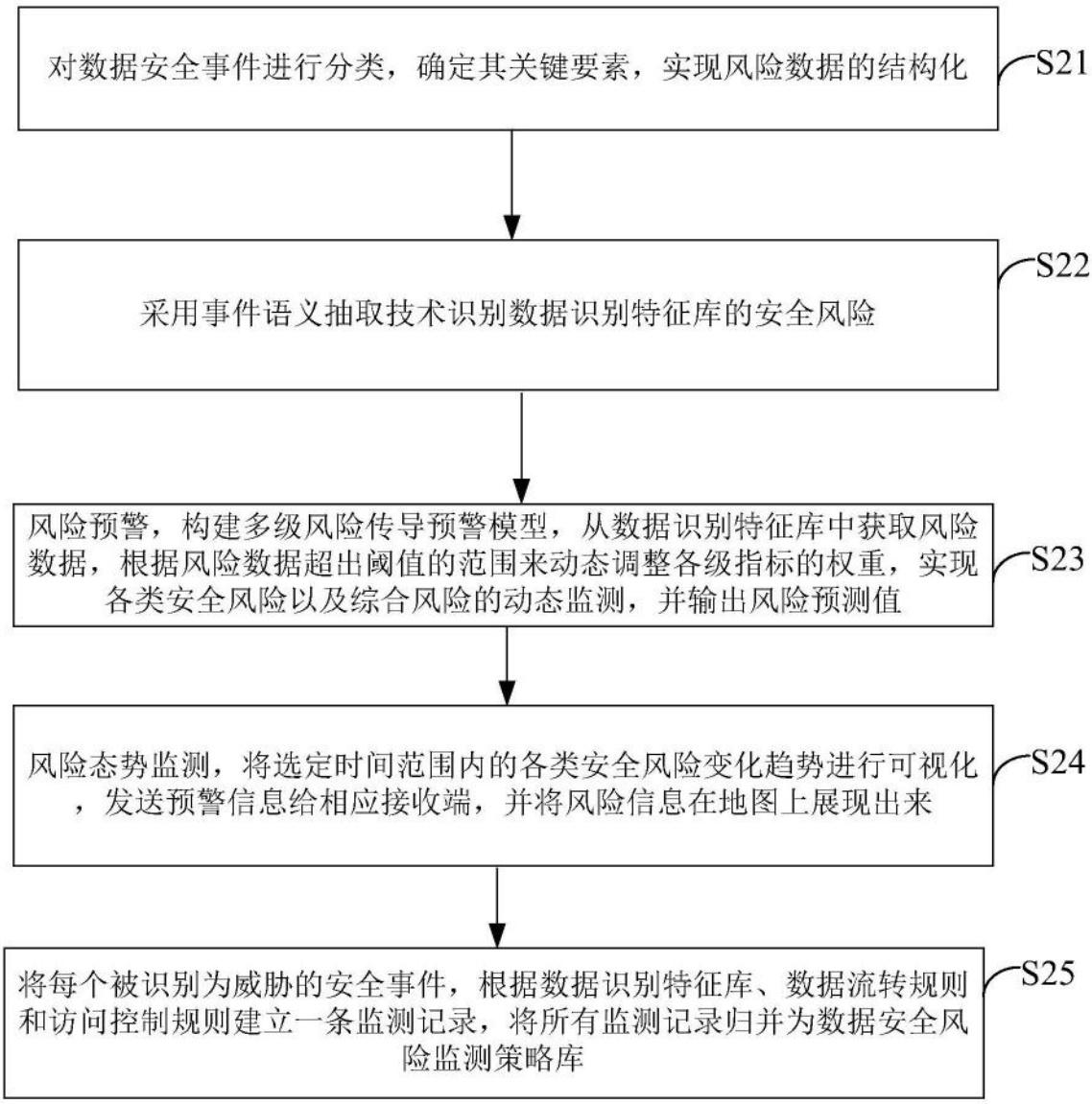

对数据安全事件进行分类，确定其关键要素，实现风险数据的结构化
S21
采用事件语义抽取技术识别数据识别特征库的安全风险
S22
风险预警，构建多级风险传导预警模型，从数据识别特征库中获取风险数据，根据风险数据超出阈值的范围来动态调整各级指标的权重，实现各类安全风险以及综合风险的动态监测，并输出风险预测值
S23
风险态势监测，将选定时间范围内的各类安全风险变化趋势进行可视化，发送预警信息给相应接收端，并将风险信息在地图上展现出来
S24
将每个被识别为威胁的安全事件，根据数据识别特征库、数据流转规则和访问控制规则建立一条监测记录，将所有监测记录归并为数据安全风险监测策略库
S25

图3

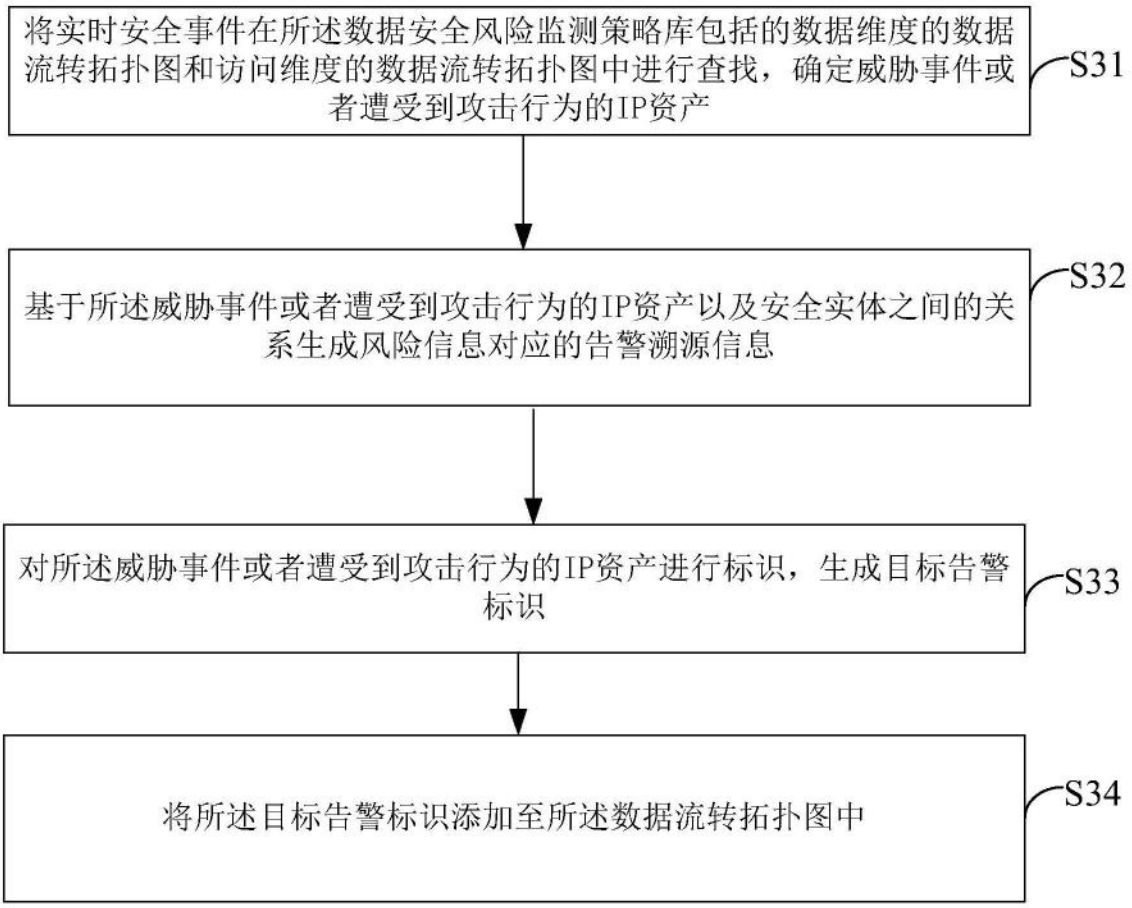

将实时安全事件在所述数据安全风险监测策略库包括的数据维度的数据流转拓扑图和访问维度的数据流转拓扑图中进行查找，确定威胁事件或者遭受到攻击行为的IP资产
S31
基于所述威胁事件或者遭受到攻击行为的IP资产以及安全实体之间的关系生成风险信息对应的告警溯源信息
S32
对所述威胁事件或者遭受到攻击行为的IP资产进行标识，生成目标告警标识
S33
将所述目标告警标识添加至所述数据流转拓扑图中
S34

图4

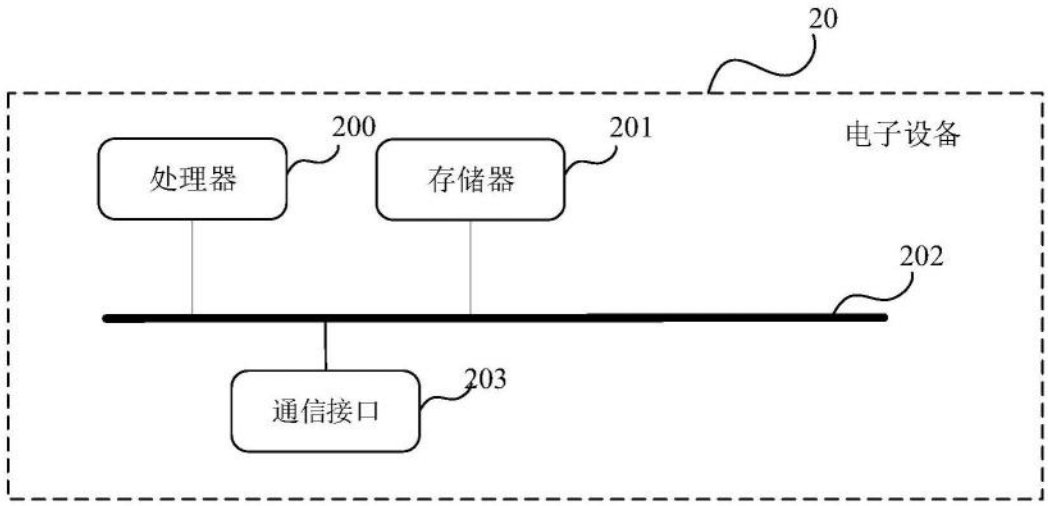

20
电子设备
200
处理器
201
存储器
202
203
通信接口

图5

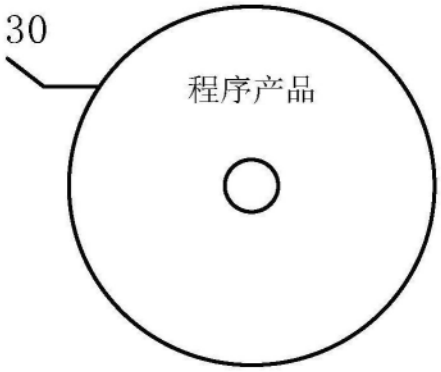


图6