(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 118394996 B
(45)授权公告日 2024.08.20

(21)申请号 202410842383.0
(22)申请日 2024.06.27
(65)同一申请的已公布的文献号
申请公布号 CN 118394996 A
(43)申请公布日 2024.07.26
(73)专利权人 四川万物纵横科技股份有限公司
地址 610041 四川省成都市高新区天府大道中段1388号12栋7层1号
(72)发明人 谭利明 杨帆 孙凯
(74)专利代理机构 成都贞元会专知识产权代理有限公司 51390
专利代理师 韦海英
(51)Int.Cl.
G06F 16/953(2019.01)
G06F 18/241(2023.01)
G06F 18/214(2023.01)
(56)对比文件
CN 110020770 A,2019.07.16
CN 113163178 A,2021.07.23
审查员 王一

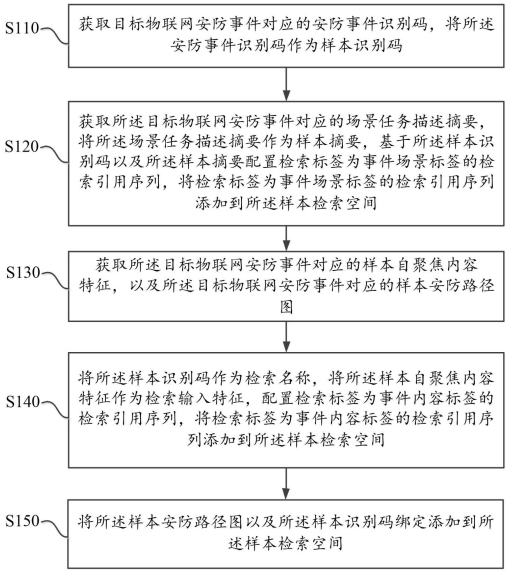
权利要求书4页 说明书19页 附图2页

(54)发明名称

一种基于人工智能的物联网数据处理方法及系统

(57)摘要

本申请提供一种基于人工智能的物联网数据处理方法及系统,专注于物联网安防事件的快速检索与分析。首先,通过获取目标物联网安防事件对应的安防事件识别码作为样本识别码,确保每个目标物联网安防事件具有唯一标识。接着,提取目标物联网安防事件的场景任务描述摘要,并结合识别码配置事件场景标签的检索引用序列,为事件检索提供场景化支持。同时,还捕获了目标物联网安防事件的自聚焦内容特征,为事件分析提供了全面视角。最后,通过将这些自聚焦内容特征和安防路径图与识别码绑定,添加至样本检索空间,实现了对安防事件的全面记录和高效检索,有效提升了安防事件处理的准确性和效率。该方法及系统可应用于校园或者工地的安防管理中。



CN 118394996 B

1.一种基于人工智能的物联网数据处理方法,其特征在于,所述方法包括:

获取目标物联网安防事件对应的安防事件识别码,将所述安防事件识别码作为样本识别码;

获取所述目标物联网安防事件对应的场景任务描述摘要,将所述场景任务描述摘要作为样本摘要,基于所述样本识别码以及所述样本摘要配置检索标签为事件场景标签的检索引用序列,将检索标签为事件场景标签的检索引用序列添加到样本检索空间;

获取所述目标物联网安防事件对应的样本自聚焦内容特征,以及所述目标物联网安防事件对应的样本安防路径图,其中,所述样本自聚焦内容特征包括样本异常行为矢量、样本违规操作矢量以及样本非法入侵矢量;

将所述样本识别码作为检索名称,将所述样本自聚焦内容特征作为检索输入特征,配置检索标签为事件内容标签的检索引用序列,将检索标签为事件内容标签的检索引用序列添加到所述样本检索空间;

将所述样本安防路径图以及所述样本识别码绑定添加到所述样本检索空间;

所述获取所述目标物联网安防事件对应的样本自聚焦内容特征,以及所述目标物联网安防事件对应的样本安防路径图,包括:

将所述目标物联网安防事件加载到安防事件分析网络,利用所述安防事件分析网络生成所述目标物联网安防事件的样本安全风险分布图;

将所述目标物联网安防事件加载到与所述样本安全风险分布图所对应的异常行为识别网络,利用所述异常行为识别网络提取所述目标物联网安防事件的异常行为特征,生成所述样本异常行为矢量;

将所述目标物联网安防事件加载到与所述样本安全风险分布图所对应的非法入侵识别网络,利用所述非法入侵识别网络提取所述目标物联网安防事件的非法入侵特征,生成所述样本非法入侵矢量;

将所述目标物联网安防事件加载到与所述样本安全风险分布图所对应的违规操作识别网络,利用所述违规操作识别网络提取所述目标物联网安防事件的违规操作特征,生成所述样本违规操作矢量;

将所述目标物联网安防事件加载到与所述样本安全风险分布图所对应的安防路径图生成网络,利用所述安防路径图生成网络,提取所述目标物联网安防事件的安防路径点特征以及所述目标物联网安防事件的安防路径点流转特征,对所述目标物联网安防事件的安防路径点特征以及所述目标物联网安防事件的安防路径点流转特征进行图生成,生成所述样本安防路径图;

所述方法还包括:将所述样本异常行为矢量以及所述样本识别码绑定添加到所述样本检索空间;

将所述样本非法入侵矢量以及所述样本识别码绑定添加到所述样本检索空间;

将所述样本违规操作矢量以及所述样本识别码绑定添加到所述样本检索空间。

2.根据权利要求1所述的基于人工智能的物联网数据处理方法,其特征在于,所述方法还包括:

获取物联网安防日志,提取所述物联网安防日志中的多个物联网安防事件;所述多个物联网安防事件包括物联网安防事件Xi,i为正整数,且i不大于所述多个物联网安防事件

的事件数量;

获取所述物联网安防事件Xi以及余下物联网安防事件之间的关联度;所述余下物联网安防事件包括所述多个物联网安防事件中除了所述物联网安防事件Xi之外的物联网安防事件;

如果所述关联度不小于设定关联度,则将所述物联网安防事件Xi标注为循环物联网安防事件,从所述多个物联网安防事件中删除所述循环物联网安防事件,生成候选物联网安防事件;

对所述候选物联网安防事件进行自注意力处理,生成所述候选物联网安防事件的自注意力处理数据,对所述候选物联网安防事件中的所述自注意力处理数据进行局部事件构建,生成所述目标物联网安防事件。

3.根据权利要求1所述的基于人工智能的物联网数据处理方法,其特征在于,所述事件场景标签包括关键节点标签;

所述基于所述样本识别码以及所述样本摘要配置检索标签为事件场景标签的检索引用序列,将检索标签为事件场景标签的检索引用序列添加到所述样本检索空间,包括:

对所述样本摘要进行分解,生成所述样本摘要对应的样本关键节点;

将所述样本识别码作为检索名称,将所述样本关键节点作为检索输入特征,配置检索标签为所述关键节点标签的检索引用序列;

将所述检索标签为所述关键节点标签的检索引用序列添加到所述样本检索空间。

4.根据权利要求1所述的基于人工智能的物联网数据处理方法,其特征在于,所述事件场景标签包括摘要主题标签;

所述基于所述样本识别码以及所述样本摘要配置检索标签为事件场景标签的检索引用序列,将检索标签为事件场景标签的检索引用序列添加到所述样本检索空间,包括:

获取所述样本摘要对应的样本摘要主题块;

将所述样本识别码作为检索名称,将所述样本摘要主题块作为检索输入特征,配置检索标签为所述摘要主题标签的检索引用序列;

将检索标签为所述摘要主题标签的检索引用序列添加到所述样本检索空间。

5.根据权利要求1所述的基于人工智能的物联网数据处理方法,其特征在于,所述将所述样本识别码作为检索名称,将所述样本自聚焦内容特征作为检索输入特征,配置检索标签为事件内容标签的检索引用序列,将检索标签为事件内容标签的检索引用序列添加到所述样本检索空间,包括:

将所述样本识别码作为检索主导名称,将所述样本异常行为矢量作为检索主导输入特征,配置检索标签为事件主导内容标签的检索主导引用序列,将所述样本识别码作为检索全局名称,将所述样本违规操作矢量作为检索全局输入特征,配置检索标签为事件全局内容标签的检索全局引用序列,将所述样本识别码作为检索细节名称,将所述样本非法入侵矢量作为检索细节输入特征,配置检索标签为事件细节内容标签的检索细节引用序列,将所述检索主导引用序列、所述检索全局引用序列以及所述检索细节引用序列均添加到所述样本检索空间;

或者,对所述样本异常行为矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本异常行为矢量,将所述样本识别码作为检索主导名称,将所述t-分布邻域嵌入后的样本异

常行为矢量作为检索主导输入特征,配置检索标签为事件主导内容标签的检索主导引用序列,对所述样本违规操作矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本违规操作矢量,将所述样本识别码作为检索全局名称,将所述t-分布邻域嵌入后的样本违规操作矢量作为检索全局输入特征,配置检索标签为事件全局内容标签的检索全局引用序列,对所述样本非法入侵矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本非法入侵矢量,将所述样本识别码作为检索细节名称,将所述t-分布邻域嵌入后的样本非法入侵矢量作为检索细节输入特征,配置检索标签为事件细节内容标签的检索细节引用序列,将所述检索主导引用序列、所述检索全局引用序列以及所述检索细节引用序列均添加到所述样本检索空间;

或者,对所述样本异常行为矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本异常行为矢量,对所述t-分布邻域嵌入后的样本异常行为矢量进行哈希处理,生成哈希处理后的样本异常行为矢量,将所述样本识别码作为检索主导名称,将所述哈希处理后的样本异常行为矢量作为检索主导输入特征,配置检索标签为事件主导内容标签的检索主导引用序列,对所述样本违规操作矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本违规操作矢量,对所述t-分布邻域嵌入后的样本违规操作矢量进行哈希处理,生成哈希处理后的样本违规操作矢量,将所述样本识别码作为检索全局名称,将所述哈希处理后的样本违规操作矢量作为检索全局输入特征,配置检索标签为事件全局内容标签的检索全局引用序列,对所述样本非法入侵矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本非法入侵矢量,对所述t-分布邻域嵌入后的样本非法入侵矢量进行哈希处理,生成哈希处理后的样本非法入侵矢量,将所述样本识别码作为检索细节名称,将所述哈希处理后的样本非法入侵矢量作为检索细节输入特征,配置检索标签为事件细节内容标签的检索细节引用序列,将所述检索主导引用序列、所述检索全局引用序列以及所述检索细节引用序列均添加到所述样本检索空间。

6.根据权利要求1-5中任意一项所述的基于人工智能的物联网数据处理方法,其特征在于,所述方法还包括:

获取包含检索摘要以及检索物联网安防事件的检索信息,从所述样本检索空间中获取与所述检索摘要所对应的第一样本;

获取所述检索物联网安防事件对应的检索安防路径图,以及所述检索物联网安防事件对应的检索自聚焦内容特征,从所述样本检索空间中获取与所述检索自聚焦内容特征所对应的第二样本;

将所述第一样本以及所述第二样本标注为参考样本,获取所述参考样本对应的目标样本安防路径图、所述参考样本对应的目标样本自聚焦内容特征以及所述参考样本对应的目标样本摘要;

依据所述检索摘要、所述检索自聚焦内容特征、所述检索安防路径图、所述目标样本摘要、所述目标样本自聚焦内容特征,以及所述目标样本安防路径图,确定所述参考样本与所述检索信息之间的样本关联度,基于所述样本关联度对所述参考样本进行降序排列,从降序排列后的参考样本中确定目标样本检索结果。

7.根据权利要求6所述的基于人工智能的物联网数据处理方法,其特征在于,所述获取所述检索物联网安防事件对应的检索安防路径图,以及所述检索物联网安防事件对应的检

索自聚焦内容特征,包括:

将所述检索物联网安防事件加载到安防事件分析网络,利用所述安防事件分析网络生成所述检索物联网安防事件的目标安全风险分布图;

获取与所述目标安全风险分布图所对应的自聚焦内容编码网络,以及与所述目标安全风险分布图所对应的安防路径图生成网络;

将所述检索物联网安防事件加载到所述自聚焦内容编码网络,利用所述自聚焦内容编码网络生成所述检索物联网安防事件对应的所述检索自聚焦内容特征;

将所述检索物联网安防事件加载到所述安防路径图生成网络,利用所述安防路径图生成网络的图卷积单元,提取所述检索物联网安防事件的图卷积矢量序列,基于所述图卷积矢量序列生成所述检索安防路径图。

8.一种基于人工智能的物联网数据处理系统,其特征在于,所述基于人工智能的物联网数据处理系统包括处理器和存储器,所述存储器和所述处理器连接,所述存储器用于存储程序、指令或代码,所述处理器用于执行所述存储器中的程序、指令或代码,以实现上述权利要求1-7任意一项所述的基于人工智能的物联网数据处理方法。

一种基于人工智能的物联网数据处理方法及系统

技术领域

[0001] 本申请涉及人工智能技术领域,具体而言,涉及一种基于人工智能的物联网数据处理方法及系统。

背景技术

[0002] 随着物联网技术的快速发展和广泛应用,物联网设备产生的数据量呈爆炸式增长,如何高效、准确地处理和分析这些数据成为了亟待解决的问题。特别是在物联网安防领域,对安防事件的快速响应和准确分析对于保障公共安全至关重要。

[0003] 相关技术通常依赖于人工分析,这不仅效率低下,而且容易受到人为因素的影响,导致分析结果的不准确。此外,随着物联网设备的不断增加,产生的安防事件数据也呈现出多样化和复杂化的特点,传统方法难以满足物联网安防事件检索实时性和准确性的要求。

[0004] 近年来,人工智能技术的兴起为物联网数据处理提供了新的思路。通过利用机器学习、深度学习等人工智能技术,可以对物联网数据进行自动分析和处理,提高数据处理的效率和准确性。特别是在物联网安防领域,人工智能技术可以帮助实现对安防事件的自动识别和快速响应,提高公共安全水平。

[0005] 然而,相关技术的方法仍存在一些局限性。一方面,这些方法通常只关注于单一的数据特征,缺乏对安防事件全面、多维度的描述和分析。另一方面,这些方法在数据检索和查询方面也存在不足,难以实现快速、准确的检索和查询。

发明内容

[0006] 鉴于上述提及的问题,结合本申请的第一方面,本申请实施例提供一种基于人工智能的物联网数据处理方法,所述方法包括:

[0007] 获取目标物联网安防事件对应的安防事件识别码,将所述安防事件识别码作为样本识别码;

[0008] 获取所述目标物联网安防事件对应的场景任务描述摘要,将所述场景任务描述摘要作为样本摘要,基于所述样本识别码以及所述样本摘要配置检索标签为事件场景标签的检索引用序列,将检索标签为事件场景标签的检索引用序列添加到所述样本检索空间;

[0009] 获取所述目标物联网安防事件对应的样本自聚焦内容特征,以及所述目标物联网安防事件对应的样本安防路径图,其中,所述样本自聚焦内容特征包括样本异常行为矢量、样本违规操作矢量以及样本非法入侵矢量;

[0010] 将所述样本识别码作为检索名称,将所述样本自聚焦内容特征作为检索输入特征,配置检索标签为事件内容标签的检索引用序列,将检索标签为事件内容标签的检索引用序列添加到所述样本检索空间;

[0011] 将所述样本安防路径图以及所述样本识别码绑定添加到所述样本检索空间。

[0012] 在第一方面的一种可能的实施方式中,所述方法还包括:

[0013] 获取物联网安防日志,提取所述物联网安防日志中的多个物联网安防事件;所述

多个物联网安防事件包括物联网安防事件Xi,i为正整数,且i不大于所述多个物联网安防事件的事件数量;

[0014] 获取所述物联网安防事件Xi以及余下物联网安防事件之间的关联度;所述余下物联网安防事件包括所述多个物联网安防事件中除了所述物联网安防事件Xi之外的物联网安防事件;

[0015] 如果所述关联度不小于设定关联度,则将所述物联网安防事件Xi标注为循环物联网安防事件,从所述多个物联网安防事件中删除所述循环物联网安防事件,生成候选物联网安防事件;

[0016] 对所述候选物联网安防事件进行自注意力处理,生成所述候选物联网安防事件的自注意力处理数据,对所述候选物联网安防事件中的所述自注意力处理数据进行局部事件构建,生成所述目标物联网安防事件。

[0017] 在第一方面的一种可能的实施方式中,所述事件场景标签包括关键节点标签;

[0018] 所述基于所述样本识别码以及所述样本摘要配置检索标签为事件场景标签的检索引用序列,将检索标签为事件场景标签的检索引用序列添加到所述样本检索空间,包括:

[0019] 对所述样本摘要进行分解,生成所述样本摘要对应的样本关键节点;

[0020] 将所述样本识别码作为检索名称,将所述样本关键节点作为检索输入特征,配置检索标签为所述关键节点标签的检索引用序列;

[0021] 将所述检索标签为所述关键节点标签的检索引用序列添加到所述样本检索空间。

[0022] 在第一方面的一种可能的实施方式中,所述事件场景标签包括摘要主题标签;

[0023] 所述基于所述样本识别码以及所述样本摘要配置检索标签为事件场景标签的检索引用序列,将检索标签为事件场景标签的检索引用序列添加到所述样本检索空间,包括:

[0024] 获取所述样本摘要对应的样本摘要主题块;

[0025] 将所述样本识别码作为检索名称,将所述样本摘要主题块作为检索输入特征,配置检索标签为所述摘要主题标签的检索引用序列;

[0026] 将检索标签为所述摘要主题标签的检索引用序列添加到所述样本检索空间。

[0027] 在第一方面的一种可能的实施方式中,所述获取所述目标物联网安防事件对应的样本自聚焦内容特征,以及所述目标物联网安防事件对应的样本安防路径图,包括:

[0028] 将所述目标物联网安防事件加载到安防事件分析网络,利用所述安防事件分析网络生成所述目标物联网安防事件的样本安全风险分布图;

[0029] 将所述目标物联网安防事件加载到与所述样本安全风险分布图所对应的异常行为识别网络,利用所述异常行为识别网络提取所述目标物联网安防事件的异常行为特征,生成所述样本异常行为矢量;

[0030] 将所述目标物联网安防事件加载到与所述样本安全风险分布图所对应的非法入侵识别网络,利用所述非法入侵识别网络提取所述目标物联网安防事件的非法入侵特征,生成所述样本非法入侵矢量;

[0031] 将所述目标物联网安防事件加载到与所述样本安全风险分布图所对应的违规操作识别网络,利用所述违规操作识别网络提取所述目标物联网安防事件的违规操作特征,生成所述样本违规操作矢量;

[0032] 将所述目标物联网安防事件加载到与所述样本安全风险分布图所对应的安防路

径图生成网络,利用所述安防路径图生成网络,提取所述目标物联网安防事件的安防路径点特征以及所述目标物联网安防事件的安防路径点流转特征,对所述目标物联网安防事件的安防路径点特征以及所述目标物联网安防事件的安防路径点流转特征进行图生成,生成所述样本安防路径图。

[0033] 在第一方面的一种可能的实施方式中,所述将所述样本识别码作为检索名称,将所述样本自聚焦内容特征作为检索输入特征,配置检索标签为事件内容标签的检索引用序列,将检索标签为事件内容标签的检索引用序列添加到所述样本检索空间,包括:

[0034] 将所述样本识别码作为检索主导名称,将所述样本异常行为矢量作为检索主导输入特征,配置检索标签为事件主导内容标签的检索主导引用序列,将所述样本识别码作为检索全局名称,将所述样本违规操作矢量作为检索全局输入特征,配置检索标签为事件全局内容标签的检索全局引用序列,将所述样本识别码作为检索细节名称,将所述样本非法入侵矢量作为检索细节输入特征,配置检索标签为事件细节内容标签的检索细节引用序列,将所述检索主导引用序列、所述检索全局引用序列以及所述检索细节引用序列均添加到所述样本检索空间;

[0035] 或者,对所述样本异常行为矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本异常行为矢量,将所述样本识别码作为检索主导名称,将所述t-分布邻域嵌入后的样本异常行为矢量作为检索主导输入特征,配置检索标签为事件主导内容标签的检索主导引用序列,对所述样本违规操作矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本违规操作矢量,将所述样本识别码作为检索全局名称,将所述t-分布邻域嵌入后的样本违规操作矢量作为检索全局输入特征,配置检索标签为事件全局内容标签的检索全局引用序列,对所述样本非法入侵矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本非法入侵矢量,将所述样本识别码作为检索细节名称,将所述t-分布邻域嵌入后的样本非法入侵矢量作为检索细节输入特征,配置检索标签为事件细节内容标签的检索细节引用序列,将所述检索主导引用序列、所述检索全局引用序列以及所述检索细节引用序列均添加到所述样本检索空间;

[0036] 或者,对所述样本异常行为矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本异常行为矢量,对所述t-分布邻域嵌入后的样本异常行为矢量进行哈希处理,生成哈希处理后的样本异常行为矢量,将所述样本识别码作为检索主导名称,将所述哈希处理后的样本异常行为矢量作为检索主导输入特征,配置检索标签为事件主导内容标签的检索主导引用序列,对所述样本违规操作矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本违规操作矢量,对所述t-分布邻域嵌入后的样本违规操作矢量进行哈希处理,生成哈希处理后的样本违规操作矢量,将所述样本识别码作为检索全局名称,将所述哈希处理后的样本违规操作矢量作为检索全局输入特征,配置检索标签为事件全局内容标签的检索全局引用序列,对所述样本非法入侵矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本非法入侵矢量,对所述t-分布邻域嵌入后的样本非法入侵矢量进行哈希处理,生成哈希处理后的样本非法入侵矢量,将所述样本识别码作为检索细节名称,将所述哈希处理后的样本非法入侵矢量作为检索细节输入特征,配置检索标签为事件细节内容标签的检索细节引用序列,将所述检索主导引用序列、所述检索全局引用序列以及所述检索细节引用序列均添加到所述样本检索空间。

[0037] 在第一方面的一种可能的实施方式中,所述方法还包括:

[0038] 将所述样本异常行为矢量以及所述样本识别码绑定添加到所述样本检索空间;

[0039] 将所述样本非法入侵矢量以及所述样本识别码绑定添加到所述样本检索空间;

[0040] 将所述样本违规操作矢量以及所述样本识别码绑定添加到所述样本检索空间。

[0041] 在第一方面的一种可能的实施方式中,所述方法还包括:

[0042] 获取包含检索摘要以及检索物联网安防事件的检索信息,从所述样本检索空间中获取与所述检索摘要所对应的第一样本;

[0043] 获取所述检索物联网安防事件对应的检索安防路径图,以及所述检索物联网安防事件对应的检索自聚焦内容特征,从所述样本检索空间中获取与所述检索自聚焦内容特征所对应的第二样本;

[0044] 将所述第一样本以及所述第二样本标注为参考样本,获取所述参考样本对应的目标样本安防路径图、所述参考样本对应的目标样本自聚焦内容特征以及所述参考样本对应的目标样本摘要;

[0045] 依据所述检索摘要、所述检索自聚焦内容特征、所述检索安防路径图、所述目标样本摘要、所述目标样本自聚焦内容特征,以及所述目标样本安防路径图,确定所述参考样本与所述检索信息之间的样本关联度,基于所述样本关联度对所述参考样本进行降序排列,从降序排列后的参考样本中确定目标样本检索结果。

[0046] 在第一方面的一种可能的实施方式中,所述获取所述检索物联网安防事件对应的检索安防路径图,以及所述检索物联网安防事件对应的检索自聚焦内容特征,包括:

[0047] 将所述检索物联网安防事件加载到安防事件分析网络,利用所述安防事件分析网络生成所述检索物联网安防事件的目标安全风险分布图;

[0048] 获取与所述目标安全风险分布图所对应的自聚焦内容编码网络,以及与所述目标安全风险分布图所对应的安防路径图生成网络;

[0049] 将所述检索物联网安防事件加载到所述自聚焦内容编码网络,利用所述自聚焦内容编码网络生成所述检索物联网安防事件对应的所述检索自聚焦内容特征;

[0050] 将所述检索物联网安防事件加载到所述安防路径图生成网络,利用所述安防路径图生成网络的图卷积单元,提取所述检索物联网安防事件的图卷积矢量序列,基于所述图卷积矢量序列生成所述检索安防路径图。

[0051] 再一方面,本申请实施例还提供一种基于人工智能的物联网数据处理系统,包括处理器、机器可读存储介质,所述机器可读存储介质和所述处理器连接,所述机器可读存储介质用于存储程序、指令或代码,所述处理器用于执行所述机器可读存储介质中的程序、指令或代码,以实现上述的方法。

[0052] 基于以上方面,本申请实施例通过获取目标物联网安防事件的安防事件识别码,并将其作为样本识别码,确保了每个目标物联网安防事件在样本检索空间中的唯一标识性,极大地方便了后续的事件检索和跟踪。其次,通过提取目标物联网安防事件的场景任务描述摘要,并配置检索标签为事件场景标签的检索引用序列,使得用户能够基于事件场景进行快速检索,提高了检索效率和准确性。此外,将场景任务描述摘要作为样本摘要添加到样本检索空间,进一步丰富了样本数据的维度,为事件分析和预测提供了更多有价值的信息。在样本自聚焦内容特征的提取方面,不仅考虑了异常行为矢量、违规操作矢量等传统特

征,还引入了样本非法入侵矢量,这些特征共同构成了对安防事件全面、多维度的描述。将这些特征作为检索输入特征,配置检索标签为事件内容标签的检索引用序列,使得用户能够基于事件内容特征进行精确检索,进一步提高了检索的针对性和有效性。最后,将样本安防路径图与样本识别码绑定添加到样本检索空间,使得用户能够直观地了解安防事件的发生路径和流转过程,为事件分析和应急响应提供了有力支持。由此,实现了对物联网安防事件的高效处理和分析,提高了物联网安防事件处理的准确性和效率。

附图说明

[0053] 图1是本申请实施例提供的基于人工智能的物联网数据处理方法的执行流程示意图。

[0054] 图2是本申请实施例提供的基于人工智能的物联网数据处理系统的硬件架构示意图。

具体实施方式

[0055] 下面结合说明书附图对本申请进行具体说明,图1是本申请一种实施例提供的基于人工智能的物联网数据处理方法的流程示意图,下面对该基于人工智能的物联网数据处理方法进行详细介绍。

[0056] 步骤S110,获取目标物联网安防事件对应的安防事件识别码,将所述安防事件识别码作为样本识别码。

[0057] 本实施例中,服务器接收到一个目标物联网安防事件的数据包,该数据包中包含了一个安防事件的详细信息。服务器首先解析这个数据包,从中提取出该目标物联网安防事件的安防事件识别码,这个安防事件识别码是唯一的,用于标识这个特定的目标物联网安防事件。服务器将这个安防事件识别码作为样本识别码,存储在内存中,以便后续使用。

[0058] 例如,服务器处理了一个关于“仓库非法入侵”的目标物联网安防事件,该目标物联网安防事件的识别码为“EventID_001”,服务器就将“EventID_001”作为这个目标物联网安防事件的样本识别码。

[0059] 步骤S120,获取所述目标物联网安防事件对应的场景任务描述摘要,将所述场景任务描述摘要作为样本摘要,基于所述样本识别码以及所述样本摘要配置检索标签为事件场景标签的检索引用序列,将检索标签为事件场景标签的检索引用序列添加到所述样本检索空间。

[0060] 本实施例中,在获取了样本识别码后,服务器继续从数据包中解析出该目标物联网安防事件的场景任务描述摘要,该场景任务描述摘要简要描述了安防事件发生的环境、任务和关键信息等。服务器将这个场景任务描述摘要作为样本摘要,并且结合之前获取的样本识别码,来配置一个检索标签为“事件场景标签”的检索引用序列。

[0061] 以“仓库非法入侵”事件为例,场景任务描述摘要中的部分内容可以是:“夜间,仓库北门被非法打开,监控录像显示有未知人员进入。”服务器将这个场景任务描述摘要作为样本摘要,并且与样本识别码“EventID_001”关联起来,生成一个事件场景标签的检索引用序列,然后将这个检索引用序列添加到样本检索空间中。

[0062] 步骤S130,获取所述目标物联网安防事件对应的样本自聚焦内容特征,以及所述

目标物联网安防事件对应的样本安防路径图,其中,所述样本自聚焦内容特征包括样本异常行为矢量、样本违规操作矢量以及样本非法入侵矢量。

[0063] 本实施例中,接下来,服务器需要对目标物联网安防事件进行深入分析,以获取目标物联网安防事件的自聚焦内容特征和安防路径图。自聚焦内容特征包括了样本异常行为矢量、样本违规操作矢量和样本非法入侵矢量,这些矢量描述了事件中异常、违规和非法行为的具体特征。

[0064] 对于“仓库非法入侵”事件,服务器可能通过分析监控视频,识别出入侵者的行走路径、异常动作等,将这些特征转化为矢量形式。同时,服务器还会根据安防系统的日志和操作记录,分析出是否有违规操作或非法入侵的行为,同样将这些行为特征转化为矢量,这些矢量与样本识别码一起,构成了对这个目标物联网安防事件的全面描述。

[0065] 步骤S140,将所述样本识别码作为检索名称,将所述样本自聚焦内容特征作为检索输入特征,配置检索标签为事件内容标签的检索引用序列,将检索标签为事件内容标签的检索引用序列添加到所述样本检索空间。

[0066] 本实施例中,在获取了自聚焦内容特征后,服务器将这些自聚焦内容特征与样本识别码关联起来,配置检索标签为“事件内容标签”的检索引用序列,这些检索引用序列将被添加到样本检索空间中,以便后续根据这些特征进行快速检索。

[0067] 以“仓库非法入侵”事件为例,服务器将样本异常行为矢量、样本违规操作矢量和样本非法入侵矢量与样本识别码“EventID_001”关联起来,生成事件内容标签的检索引用序列,并将这些检索引用序列添加到样本检索空间中。

[0068] 步骤S150,将所述样本安防路径图以及所述样本识别码绑定添加到所述样本检索空间。

[0069] 最后,服务器还需要将样本安防路径图与样本识别码绑定起来,一同添加到样本检索空间中。样本安防路径图描述了安防事件中各关键节点的联系和流转路径,对于理解和分析安防事件具有重要意义。

[0070] 在“仓库非法入侵”事件的例子中,服务器根据分析出的入侵者行走路径、安防系统响应流程等信息,生成了一个安防路径图,该安防路径图与样本识别码“EventID_001”一起被添加到样本检索空间中,以便后续能够通过样本识别码快速检索到这个目标物联网安防事件的安防路径图。

[0071] 基于以上步骤,本申请实施例通过获取目标物联网安防事件的安防事件识别码,并将其作为样本识别码,确保了每个目标物联网安防事件在样本检索空间中的唯一标识性,极大地方便了后续的事件检索和跟踪。其次,通过提取目标物联网安防事件的场景任务描述摘要,并配置检索标签为事件场景标签的检索引用序列,使得用户能够基于事件场景进行快速检索,提高了检索效率和准确性。此外,将场景任务描述摘要作为样本摘要添加到样本检索空间,进一步丰富了样本数据的维度,为事件分析和预测提供了更多有价值的信息。在样本自聚焦内容特征的提取方面,不仅考虑了异常行为矢量、违规操作矢量等传统特征,还引入了样本非法入侵矢量,这些特征共同构成了对安防事件全面、多维度的描述。将这些特征作为检索输入特征,配置检索标签为事件内容标签的检索引用序列,使得用户能够基于事件内容特征进行精确检索,进一步提高了检索的针对性和有效性。最后,将样本安防路径图与样本识别码绑定添加到样本检索空间,使得用户能够直观地了解安防事件的发

生路径和流转过程,为事件分析和应急响应提供了有力支持。由此,实现了对物联网安防事件的高效处理和分析,提高了物联网安防事件处理的准确性和效率。

[0072] 在一种可能的实施方式中,所述方法还包括:

[0073] 步骤A110,获取物联网安防日志,提取所述物联网安防日志中的多个物联网安防事件。所述多个物联网安防事件包括物联网安防事件Xi,i为正整数,且i不大于所述多个物联网安防事件的事件数量。

[0074] 在物联网安防系统中,服务器负责处理和分析大量的安防日志数据,以识别出各种物联网安防事件。为了有效地管理和分析这些物联网安防事件,服务器执行了一系列步骤来提取、关联和构建这些物联网安防事件。

[0075] 详细地,服务器定期从物联网安防系统中获取物联网安防日志,这些物联网安防日志记录了各种传感器、摄像头和其他设备的活动数据。服务器解析这些物联网安防日志,提取出多个物联网安防事件。例如,服务器从物联网安防日志中提取出三个物联网安防事件:事件X1(仓库门异常开启)、事件X2(非法入侵警报触发)和事件X3(消防系统测试)。

[0076] 步骤A120,获取所述物联网安防事件Xi以及余下物联网安防事件之间的关联度。所述余下物联网安防事件包括所述多个物联网安防事件中除了所述物联网安防事件Xi之外的物联网安防事件。

[0077] 本实施例中,服务器接下来分析这些物联网安防事件之间的关联度。例如,使用预先训练的关联度计算模型,该关联度计算模型基于物联网安防事件的时间戳、地理位置、涉及的设备和事件类型等因素来计算物联网安防事件之间的关联度。例如,服务器发现事件X1和事件X2在时间上非常接近(几乎同时发生),且地理位置相同(都在仓库区域),因此计算出的关联度很高。而事件X3(消防系统测试)与前两个物联网安防事件没有直接的关联。

[0078] 步骤A130,如果所述关联度不小于设定关联度,则将所述物联网安防事件Xi标注为循环物联网安防事件,从所述多个物联网安防事件中删除所述循环物联网安防事件,生成候选物联网安防事件。

[0079] 本实施例中,如果服务器发现某个物联网安防事件(如事件X1)与其他多个物联网安防事件(如事件X2)的关联度都超过了设定的阈值(例如0.8),它可能将这个事件标注为“循环物联网安防事件”,意味着这个物联网安防事件可以是其他物联网安防事件的触发因素或与之高度相关。在这种情况下,服务器可以从原始物联网安防事件列表中删除事件X1,以避免在后续分析中重复考虑它。

[0080] 步骤A140,对所述候选物联网安防事件进行自注意力处理,生成所述候选物联网安防事件的自注意力处理数据,对所述候选物联网安防事件中的所述自注意力处理数据进行局部事件构建,生成所述目标物联网安防事件。

[0081] 经过上一步的处理,服务器得到了一个候选物联网安防事件的列表(在这个例子中,可以是事件X2和事件X3)。服务器接下来使用自注意力机制对这些候选物联网安防事件进行处理。自注意力机制允许模型关注于输入序列中最重要的部分。在这个场景下,服务器将候选物联网安防事件作为输入序列,通过自注意力机制生成每个候选物联网安防事件的自注意力处理数据,这些自注意力处理数据捕捉了候选物联网安防事件中最关键的特征和与其他事件的关联。

[0082] 最后,服务器利用自注意力处理数据对候选物联网安防事件进行局部事件构建,

该过程可以包括进一步的事件分类、特征提取和事件关系的细化。例如,服务器可能根据自注意力处理数据确定事件X2(非法入侵警报触发)是一个独立的关键事件,而事件X3(消防系统测试)虽然被记录,但在当前情境下不是主要关注点。因此,服务器可能将事件X2作为目标物联网安防事件进行后续的分析和报告。

[0083] 通过以上步骤,服务器能够有效地从大量的物联网安防日志中提取出关键事件,并分析这些事件之间的关系和特征,为后续的安防决策提供有力支持。

[0084] 在一种可能的实施方式中,所述事件场景标签包括关键节点标签。

[0085] 步骤S120包括:

[0086] 步骤S121,对所述样本摘要进行分解,生成所述样本摘要对应的样本关键节点。

[0087] 本实施例中,继续假设服务器正在处理一个关于“智能仓库非法入侵”的目标物联网安防事件,该目标物联网安防事件的目标是从大量的安防数据中提取、分析和检索相关信息,以便后续的安全分析和策略制定。

[0088] 服务器首先接收到关于“智能仓库非法入侵”的事件数据包,并从中解析出安防事件识别码(假设为“EventID_WarehouseIntrusion”)作为样本识别码。同时,服务器也提取出该目标物联网安防事件的场景任务描述摘要,内容大致如下:“凌晨2点,智能仓库南门被非法打开,监控显示有不明人员进入,警报系统已触发。”

[0089] 服务器接下来对样本摘要进行分解,识别出其中的关键节点。在这个例子中,关键节点可以包括:

[0090] 时间节点:“凌晨2点”

[0091] 地点节点:“智能仓库南门”

[0092] 行为节点:“非法打开”、“不明人员进入”

[0093] 系统响应节点:“警报系统已触发”

[0094] 这些关键节点是理解事件场景的关键信息。

[0095] 步骤S122,将所述样本识别码作为检索名称,将所述样本关键节点作为检索输入特征,配置检索标签为所述关键节点标签的检索引用序列。

[0096] 本实施例中,服务器将样本识别码“EventID_WarehouseIntrusion”作为检索名称,并将上述识别出的关键节点作为检索输入特征。对于每一个关键节点,服务器都会配置一个检索标签为“关键节点标签”的检索引用序列。例如:

[0097] 时间节点检索引用序列:EventID_WarehouseIntrusion - 时间节点 - 凌晨2点

[0098] 地点节点检索引用序列:EventID_WarehouseIntrusion - 地点节点 - 智能仓库南门

[0099] 行为节点检索引用序列(非法打开):EventID_WarehouseIntrusion - 行为节点 - 非法打开

[0100] 行为节点检索引用序列(不明人员进入):EventID_WarehouseIntrusion - 行为节点 - 不明人员进入

[0101] 系统响应节点检索引用序列:EventID_WarehouseIntrusion - 系统响应节点 - 警报系统已触发

[0102] 步骤S123,将所述检索标签为所述关键节点标签的检索引用序列添加到所述样本检索空间。

[0103] 最后,服务器将这些配置了关键节点标签的检索引用序列添加到样本检索空间中,这样,当后续需要检索与“智能仓库非法入侵”事件相关的关键节点信息时,就可以通过样本检索空间快速定位到相关的数据。

[0104] 通过这个过程,服务器不仅能够对单个安防事件进行详细的场景分析,还能够为后续的检索和分析提供结构化的数据支持,提高了数据处理的效率和准确性。

[0105] 在一种可能的实施方式中,所述事件场景标签包括摘要主题标签。

[0106] 步骤S120包括:

[0107] 步骤S124,获取所述样本摘要对应的样本摘要主题块。

[0108] 本实施例中,继续假设服务器正在处理一个关于“智能仓库非法入侵”的物联网安防事件,该物联网安防事件的目标是从大量的安防数据中提取、分析和检索相关信息,以便后续的安全分析和策略制定。

[0109] 服务器首先接收到关于“智能仓库非法入侵”的事件数据包,并从中解析出安防事件的识别码(假设为“EventID_WarehouseIntrusion”)作为样本识别码。同时,服务器也提取出该事件的场景任务描述摘要,内容大致如下:“凌晨2点,智能仓库南门被非法打开,监控显示有不明人员进入,警报系统已触发,安保人员已赶往现场。”

[0110] 服务器接下来分析样本摘要的内容,识别出其中的主题块。在这个例子中,主题块可以包括“非法入侵行为”、“警报系统响应”和“安保人员行动”等。每个主题块都是摘要中围绕一个核心主题的信息集合。

[0111] 对于“非法入侵行为”主题块,可能包含“凌晨2点,智能仓库南门被非法打开,监控显示有不明人员进入”等描述;

[0112] 对于“警报系统响应”主题块,可能包含“警报系统已触发”的描述;

[0113] 对于“安保人员行动”主题块,可能包含“安保人员已赶往现场”的描述。

[0114] 步骤S125,将所述样本识别码作为检索名称,将所述样本摘要主题块作为检索输入特征,配置检索标签为所述摘要主题标签的检索引用序列。

[0115] 服务器将样本识别码“EventID_WarehouseIntrusion”作为检索名称,并将上述识别出的样本摘要主题块作为检索输入特征。对于每一个主题块,服务器都会配置一个检索标签为“摘要主题标签”的检索引用序列。例如:

[0116] 非法入侵行为主题检索引用序列:EventID_WarehouseIntrusion - 摘要主题 - 非法入侵行为

[0117] 警报系统响应主题检索引用序列:EventID_WarehouseIntrusion - 摘要主题 - 警报系统响应

[0118] 安保人员行动主题检索引用序列:EventID_WarehouseIntrusion - 摘要主题 - 安保人员行动

[0119] 步骤S126,将检索标签为所述摘要主题标签的检索引用序列添加到所述样本检索空间。

[0120] 最后,服务器将这些配置了摘要主题标签的检索引用序列添加到样本检索空间中,这样,当后续需要检索与“智能仓库非法入侵”事件相关的摘要主题信息时,就可以通过样本检索空间快速定位到相关的数据。

[0121] 通过这个过程,服务器不仅能够对单个安防事件进行详细的场景分析,提取出摘

要中的关键主题信息,还能够为后续的检索和分析提供结构化的数据支持,提高了数据处理的效率和准确性,这对于快速响应安防事件、制定应对策略具有重要意义。

[0122] 在一种可能的实施方式中,步骤S130包括:

[0123] 步骤S131,将所述目标物联网安防事件加载到安防事件分析网络,利用所述安防事件分析网络生成所述目标物联网安防事件的样本安全风险分布图。

[0124] 本实施例中,继续假设服务器正在处理一个关于“智能仓库非法入侵”的物联网安防事件。该物联网安防事件的数据包已经包含了事件的详细信息,服务器需要从这个数据包中提取出样本自聚焦内容特征以及样本安防路径图。

[0125] 服务器首先将“智能仓库非法入侵”事件的数据包加载到预先训练好的安防事件分析网络中,该安防事件分析网络能够根据事件的数据内容,自动分析出事件中的安全风险分布情况。

[0126] 安防事件分析网络对“智能仓库非法入侵”事件的数据进行分析后,生成了一个样本安全风险分布图,该样本安全风险分布图展示了事件中各个安全风险点的分布情况,例如非法入侵的路径、异常行为发生的位置等。

[0127] 步骤S132,将所述目标物联网安防事件加载到与所述样本安全风险分布图所对应的异常行为识别网络,利用所述异常行为识别网络提取所述目标物联网安防事件的异常行为特征,生成所述样本异常行为矢量。

[0128] 本实施例中,服务器接下来将“智能仓库非法入侵”事件的数据以及样本安全风险分布图加载到与之对应的异常行为识别网络中,该异常行为识别网络专门用于识别事件中的异常行为特征。

[0129] 异常行为识别网络对事件数据进行分析,提取出与样本安全风险分布图相匹配的异常行为特征,如入侵者的行走轨迹异常、停留时间过长等,这些特征被量化并编码成矢量形式,生成了样本异常行为矢量。

[0130] 步骤S133,将所述目标物联网安防事件加载到与所述样本安全风险分布图所对应的非法入侵识别网络,利用所述非法入侵识别网络提取所述目标物联网安防事件的非法入侵特征,生成所述样本非法入侵矢量。

[0131] 本实施例中,服务器再次将“智能仓库非法入侵”事件的数据以及样本安全风险分布图加载到非法入侵识别网络中,该非法入侵识别网络专注于识别事件中的非法入侵行为特征。

[0132] 非法入侵识别网络分析事件数据,提取出与样本安全风险分布图相匹配的非法入侵特征,如入侵者的未授权访问、破坏安防设备等,这些特征同样被量化并编码成矢量形式,生成了样本非法入侵矢量。

[0133] 步骤S134,将所述目标物联网安防事件加载到与所述样本安全风险分布图所对应的违规操作识别网络,利用所述违规操作识别网络提取所述目标物联网安防事件的违规操作特征,生成所述样本违规操作矢量。

[0134] 接下来,服务器将事件数据和样本安全风险分布图加载到违规操作识别网络中,这个违规操作识别网络用于识别事件中的违规操作行为。

[0135] 违规操作识别网络对事件数据进行分析,提取出与样本安全风险分布图相匹配的违规操作特征,如安防人员的操作失误、设备的不当使用等,这些特征也被量化并编码成矢

量形式,生成了样本违规操作矢量。

[0136] 步骤S135,将所述目标物联网安防事件加载到与所述样本安全风险分布图所对应的安防路径图生成网络,利用所述安防路径图生成网络,提取所述目标物联网安防事件的安防路径点特征以及所述目标物联网安防事件的安防路径点流转特征,对所述目标物联网安防事件的安防路径点特征以及所述目标物联网安防事件的安防路径点流转特征进行图生成,生成所述样本安防路径图。

[0137] 最后,服务器将事件数据和样本安全风险分布图加载到安防路径图生成网络中,该安防路径图生成网络用于根据事件中的关键节点和流转路径生成安防路径图。

[0138] 安防路径图生成网络从事件数据中提取安防路径点特征以及安防路径点流转特征,如入侵者的行进路线、警报系统的响应路径等。然后,利用这些特征进行图生成,最终生成了样本安防路径图,该样本安防路径图直观地展示了事件中各关键节点的联系和流转路径。

[0139] 通过这个过程,服务器能够全面地从目标物联网安防事件中提取出样本自聚焦内容特征(包括异常行为、非法入侵和违规操作特征)以及样本安防路径图,为后续的事件分析和检索提供了重要的数据支持。

[0140] 在一种可能的实施方式中,步骤S140可以包括:

[0141] A、将所述样本识别码作为检索主导名称,将所述样本异常行为矢量作为检索主导输入特征,配置检索标签为事件主导内容标签的检索主导引用序列,将所述样本识别码作为检索全局名称,将所述样本违规操作矢量作为检索全局输入特征,配置检索标签为事件全局内容标签的检索全局引用序列,将所述样本识别码作为检索细节名称,将所述样本非法入侵矢量作为检索细节输入特征,配置检索标签为事件细节内容标签的检索细节引用序列,将所述检索主导引用序列、所述检索全局引用序列以及所述检索细节引用序列均添加到所述样本检索空间。

[0142] 本实施例中,继续假设服务器已经处理了一个关于“智能仓库非法入侵”的物联网安防事件,并生成了样本识别码(如“EventID_WarehouseIntrusion”)以及样本自聚焦内容特征,包括样本异常行为矢量、样本违规操作矢量和样本非法入侵矢量。

[0143] 服务器首先将样本识别码“EventID_WarehouseIntrusion”作为检索主导名称。然后,它选择样本异常行为矢量作为检索主导输入特征,因为这个矢量直接关联到事件的核心行为——非法入侵。接下来,服务器配置检索标签为“事件主导内容标签”的检索主导引用序列,该标签表明这个引用序列主要用于检索与事件主导内容(即异常行为)相关的信息。

[0144] 例如,检索主导引用序列可能形如:“EventID_WarehouseIntrusion - 事件主导内容 - 异常行为特征矢量(包含具体矢量数据)”。

[0145] 服务器继续使用样本识别码“EventID_WarehouseIntrusion”作为检索全局名称。然后,它选择样本违规操作矢量作为检索全局输入特征,因为这个矢量提供了事件全局视角下的信息,如可能的安防系统操作失误或设备不当使用。服务器配置检索标签为“事件全局内容标签”的检索全局引用序列,该标签表明这个引用序列主要用于检索与事件全局内容相关的信息。

[0146] 例如,检索全局引用序列可能形如:“EventID_WarehouseIntrusion - 事件全局

内容 - 违规操作特征矢量(包含具体矢量数据)”。

[0147] 同样,服务器再次使用样本识别码“EventID_WarehouseIntrusion”作为检索细节名称,这次,它选择样本非法入侵矢量作为检索细节输入特征,因为这个矢量提供了事件的细节信息,如入侵者的具体行为或安防系统的详细响应。服务器配置检索标签为“事件细节内容标签”的检索细节引用序列,该检索标签表明这个引用序列主要用于检索与事件细节内容相关的信息。

[0148] 例如,检索细节引用序列可能形如:“EventID_WarehouseIntrusion - 事件细节内容 - 非法入侵特征矢量(包含具体矢量数据)”。

[0149] 最后,服务器将上述配置好的检索主导引用序列、检索全局引用序列和检索细节引用序列都添加到样本检索空间中,这样,当需要检索与“智能仓库非法入侵”事件相关的特定内容时,服务器可以迅速从样本检索空间中检索到相应的引用序列,进而定位到具体的样本数据。

[0150] 通过这个过程,服务器不仅能够对单个安防事件进行详细的特征提取和标签化,还能够为后续的快速检索和分析提供结构化的数据支持,提高了数据处理的效率和准确性。

[0151] 或者,B、对所述样本异常行为矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本异常行为矢量,将所述样本识别码作为检索主导名称,将所述t-分布邻域嵌入后的样本异常行为矢量作为检索主导输入特征,配置检索标签为事件主导内容标签的检索主导引用序列,对所述样本违规操作矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本违规操作矢量,将所述样本识别码作为检索全局名称,将所述t-分布邻域嵌入后的样本违规操作矢量作为检索全局输入特征,配置检索标签为事件全局内容标签的检索全局引用序列,对所述样本非法入侵矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本非法入侵矢量,将所述样本识别码作为检索细节名称,将所述t-分布邻域嵌入后的样本非法入侵矢量作为检索细节输入特征,配置检索标签为事件细节内容标签的检索细节引用序列,将所述检索主导引用序列、所述检索全局引用序列以及所述检索细节引用序列均添加到所述样本检索空间。

[0152] 本实施例中,继续假设服务器已经处理了一个关于“智能仓库非法入侵”的物联网安防事件,并生成了样本识别码(如“EventID_WarehouseIntrusion”)以及样本自聚焦内容特征,包括样本异常行为矢量、样本违规操作矢量和样本非法入侵矢量。服务器现在准备将这些特征进行t-分布邻域嵌入处理,以改善检索效果。

[0153] 服务器首先加载样本异常行为矢量,这是一个多维的特征向量,描述了非法入侵事件中的异常行为特性。服务器使用t-分布邻域嵌入(t-SNE)算法对这个矢量进行处理,将其从原始的高维空间映射到一个低维空间,同时保持数据点之间的局部和全局结构,该处理过程降低了数据的维度,使得数据可视化更加直观,同时也提高了检索效率。

[0154] 经过t-分布邻域嵌入处理后,服务器得到了一个降维后的样本异常行为矢量,这个降维后的样本异常行为矢量依然保留了原始矢量的关键信息,但更加便于后续的处理和检索。

[0155] 服务器将样本识别码“EventID_WarehouseIntrusion”作为检索主导名称。然后,它选择t-分布邻域嵌入后的样本异常行为矢量作为检索主导输入特征。由于这个特征直接

关联到事件的核心行为——非法入侵的异常行为,因此服务器配置检索标签为“事件主导内容标签”的检索主导引用序列,该标签表明这个引用序列主要用于检索与事件主导内容(即异常行为)相关的信息。

[0156] 例如,检索主导引用序列可能形如:“EventID_WarehouseIntrusion - 事件主导内容 - t-SNE嵌入后的异常行为特征矢量(包含具体矢量数据)”。

[0157] 接下来,服务器对样本违规操作矢量进行同样的t-分布邻域嵌入处理,得到一个降维后的违规操作矢量。然后,服务器将这个降维后的矢量作为检索全局输入特征,与样本识别码一起配置检索标签为“事件全局内容标签”的检索全局引用序列,该标签表明这个引用序列主要用于检索与事件全局内容(如可能的安防系统操作失误或设备不当使用)相关的信息。

[0158] 例如,检索全局引用序列可能形如:“EventID_WarehouseIntrusion - 事件全局内容 - t-SNE嵌入后的违规操作特征矢量(包含具体矢量数据)”。

[0159] 类似地,服务器对样本非法入侵矢量进行t-分布邻域嵌入处理,得到一个降维后的非法入侵矢量。然后,服务器将这个降维后的矢量作为检索细节输入特征,与样本识别码一起配置检索标签为“事件细节内容标签”的检索细节引用序列,该标签表明这个引用序列主要用于检索与事件细节内容(如入侵者的具体行为或安防系统的详细响应)相关的信息。

[0160] 例如,检索细节引用序列可能形如:“EventID_WarehouseIntrusion - 事件细节内容 - t-SNE嵌入后的非法入侵特征矢量(包含具体矢量数据)”。

[0161] 最后,服务器将上述配置好的检索主导引用序列、检索全局引用序列和检索细节引用序列都添加到样本检索空间中,这样,当需要检索与“智能仓库非法入侵”事件相关的特定内容时,服务器可以迅速从样本检索空间中检索到相应的引用序列,进而定位到具体的样本数据。

[0162] 通过这个过程,服务器不仅能够对单个安防事件进行详细的特征提取和标签化,还通过t-分布邻域嵌入技术改善了特征的可视化和检索效果,为后续的快速检索和分析提供了更加结构化和高效的数据支持。

[0163] 或者,C、对所述样本异常行为矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本异常行为矢量,对所述t-分布邻域嵌入后的样本异常行为矢量进行哈希处理,生成哈希处理后的样本异常行为矢量,将所述样本识别码作为检索主导名称,将所述哈希处理后的样本异常行为矢量作为检索主导输入特征,配置检索标签为事件主导内容标签的检索主导引用序列,对所述样本违规操作矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本违规操作矢量,对所述t-分布邻域嵌入后的样本违规操作矢量进行哈希处理,生成哈希处理后的样本违规操作矢量,将所述样本识别码作为检索全局名称,将所述哈希处理后的样本违规操作矢量作为检索全局输入特征,配置检索标签为事件全局内容标签的检索全局引用序列,对所述样本非法入侵矢量进行t-分布邻域嵌入,生成t-分布邻域嵌入后的样本非法入侵矢量,对所述t-分布邻域嵌入后的样本非法入侵矢量进行哈希处理,生成哈希处理后的样本非法入侵矢量,将所述样本识别码作为检索细节名称,将所述哈希处理后的样本非法入侵矢量作为检索细节输入特征,配置检索标签为事件细节内容标签的检索细节引用序列,将所述检索主导引用序列、所述检索全局引用序列以及所述检索细节引用序列均添加到所述样本检索空间。

[0164] 本实施例中,继续假设服务器已经处理了一个关于“智能仓库非法入侵”的物联网安防事件,并生成了样本识别码(如“EventID_WarehouseIntrusion”)以及样本自聚焦内容特征,包括样本异常行为矢量、样本违规操作矢量和样本非法入侵矢量。服务器现在准备对这些特征进行t-分布邻域嵌入和哈希处理,以提高检索效率和准确性。

[0165] 服务器首先加载样本异常行为矢量,这是一个多维的特征向量,描述了非法入侵事件中的异常行为特性。服务器使用t-分布邻域嵌入(t-SNE)算法对这个矢量进行处理,将其从原始的高维空间映射到一个低维空间,该处理过程降低了数据的维度,使得数据可视化更加直观,同时也提高了检索效率。

[0166] 服务器接着对t-分布邻域嵌入后的样本异常行为矢量进行哈希处理。哈希处理是一种将任意长度的数据映射为固定长度数据的技术,通常用于快速查找和比较。通过哈希处理,服务器将嵌入后的异常行为矢量转换为一个哈希值,这个哈希值唯一标识了原始矢量,并且具有较短的长度,便于存储和检索。

[0167] 服务器将样本识别码“EventID_WarehouseIntrusion”作为检索主导名称。然后,它选择哈希处理后的样本异常行为矢量作为检索主导输入特征。由于这个特征直接关联到事件的核心行为——非法入侵的异常行为,因此服务器配置检索标签为“事件主导内容标签”的检索主导引用序列,该标签表明这个引用序列主要用于检索与事件主导内容(即异常行为)相关的信息。

[0168] 例如,检索主导引用序列可能形如:“EventID_WarehouseIntrusion - 事件主导内容 - 哈希值(异常行为特征的t-SNE嵌入后哈希处理结果)”。

[0169] 服务器对样本违规操作矢量的处理流程与异常行为矢量类似。首先进行t-分布邻域嵌入处理,然后对嵌入后的矢量进行哈希处理。得到哈希处理后的违规操作矢量后,服务器将其作为检索全局输入特征,与样本识别码一起配置检索标签为“事件全局内容标签”的检索全局引用序列,该标签表明这个引用序列主要用于检索与事件全局内容相关的信息。

[0170] 服务器对样本非法入侵矢量的处理流程也相同。先进行t-分布邻域嵌入处理,再对嵌入后的矢量进行哈希处理。得到哈希处理后的非法入侵矢量后,服务器将其作为检索细节输入特征,与样本识别码一起配置检索标签为“事件细节内容标签”的检索细节引用序列,该标签表明这个引用序列主要用于检索与事件细节内容相关的信息。

[0171] 最后,服务器将上述配置好的检索主导引用序列、检索全局引用序列和检索细节引用序列都添加到样本检索空间中,这样,当需要检索与“智能仓库非法入侵”事件相关的特定内容时,服务器可以迅速从样本检索空间中检索到相应的引用序列,进而定位到具体的样本数据。

[0172] 通过这个过程,服务器不仅能够对单个安防事件进行详细的特征提取和标签化,还通过t-分布邻域嵌入和哈希处理技术进一步提高了特征的可视化、检索效率和准确性,为后续的快速检索和分析提供了更加结构化和高效的数据支持。

[0173] 在一种可能的实施方式中,所述方法还包括:

[0174] 步骤B110,将所述样本异常行为矢量以及所述样本识别码绑定添加到所述样本检索空间。

[0175] 本实施例中,服务器在处理完一个关于“智能仓库非法入侵”的物联网安防事件后,已经生成了样本识别码(如“EventID_WarehouseIntrusion”)以及样本自聚焦内容特征

矢量,包括样本异常行为矢量、样本非法入侵矢量和样本违规操作矢量。现在,服务器准备将这些特征矢量与样本识别码绑定,并添加到样本检索空间中,以便后续能够快速检索和定位这些特征数据。

[0176] 服务器首先获取样本异常行为矢量,这个样本异常行为矢量包含了事件中异常行为的详细特征数据。接着,服务器将样本识别码“EventID_WarehouseIntrusion”与样本异常行为矢量进行绑定。绑定操作意味着服务器在内部数据结构中建立了一个关联关系,使得通过样本识别码可以快速定位到对应的样本异常行为矢量。

[0177] 例如,服务器可以在内部数据库中创建一个条目,该条目包含样本识别码和样本异常行为矢量的引用或实际数据,这样,当需要检索与“EventID_WarehouseIntrusion”事件相关的异常行为特征时,服务器可以直接查找这个条目,快速获取到对应的样本异常行为矢量。

[0178] 步骤B120,将所述样本非法入侵矢量以及所述样本识别码绑定添加到所述样本检索空间。

[0179] 完成绑定操作后,服务器将包含样本识别码和样本异常行为矢量的条目添加到样本检索空间中。样本检索空间是服务器内部用于存储和检索样本数据的一个区域或数据结构。通过将数据添加到样本检索空间,服务器使得这些数据变得可检索和可访问。

[0180] 在添加数据时,服务器可以使用特定的数据结构或索引技术来优化检索性能。例如,服务器可以使用哈希表来存储数据,以便通过样本识别码快速定位到对应的条目。或者,服务器可以使用倒排索引技术,将特征矢量中的数据项与包含这些项的条目相关联,以便通过特征数据来检索样本。

[0181] 步骤B130,将所述样本违规操作矢量以及所述样本识别码绑定添加到所述样本检索空间。

[0182] 服务器接下来会重复上述绑定和添加操作,以处理样本非法入侵矢量和样本违规操作矢量。对于每个特征矢量,服务器都会将其与样本识别码进行绑定,并将绑定后的数据添加到样本检索空间中。

[0183] 例如,对于样本非法入侵矢量,服务器可以将其与“EventID_WarehouseIntrusion”进行绑定,并将绑定后的数据添加到样本检索空间。同样地,对于样本违规操作矢量,服务器也会执行相同的操作。

[0184] 经过上述步骤后,服务器将样本自聚焦内容特征矢量(包括样本异常行为矢量、样本非法入侵矢量和样本违规操作矢量)与样本识别码绑定,并将绑定后的数据添加到了样本检索空间中,这样,服务器就能够通过样本识别码快速检索和定位到与“智能仓库非法入侵”事件相关的特征数据,为后续的分析和处理提供了便利。

[0185] 在一种可能的实施方式中,所述方法还包括:

[0186] 步骤C110,获取包含检索摘要以及检索物联网安防事件的检索信息,从所述样本检索空间中获取与所述检索摘要所对应的第一样本。

[0187] 本实施例中,服务器在处理物联网安防事件时,不仅存储了样本数据,还提供了检索功能,以便用户能够快速地查找与特定事件相关的数据。假设现在有一个用户想要查找与“智能仓库夜间非法入侵”相关的安防事件数据。

[0188] 用户向服务器发送了检索请求,其中包含检索摘要“智能仓库夜间非法入侵”以及

检索物联网安防事件的具体描述。服务器首先解析这个检索请求,提取出检索摘要。

[0189] 接着,服务器在样本检索空间中搜索与检索摘要“智能仓库夜间非法入侵”相关的样本,这些样本可能包含与检索摘要相匹配的关键词或描述,服务器通过检索算法(如文本匹配、语义相似度计算等)找到与检索摘要最相关的样本,将其作为第一样本。

[0190] 步骤C120,获取所述检索物联网安防事件对应的检索安防路径图,以及所述检索物联网安防事件对应的检索自聚焦内容特征,从所述样本检索空间中获取与所述检索自聚焦内容特征所对应的第二样本。

[0191] 服务器进一步解析检索请求中的检索物联网安防事件描述,并尝试从该描述中提取出自聚焦内容特征和安防路径图的相关信息,这些信息可以包括异常行为、非法入侵行为、违规操作等的具体描述,以及事件发生的路径和流程。

[0192] 然后,服务器在样本检索空间中搜索与这些自聚焦内容特征和安防路径图相匹配的样本。服务器通过特征匹配、图结构对比等技术找到最相关的样本,将其作为第二样本。

[0193] 步骤C130,将所述第一样本以及所述第二样本标注为参考样本,获取所述参考样本对应的目标样本安防路径图、所述参考样本对应的目标样本自聚焦内容特征以及所述参考样本对应的目标样本摘要。

[0194] 本实施例中,服务器将第一样本和第二样本标注为参考样本,这些样本是初步检索结果,可能与用户想要查找的安防事件相关。

[0195] 接着,服务器从样本存储中获取这些参考样本对应的目标样本数据,包括目标样本安防路径图、目标样本自聚焦内容特征以及目标样本摘要,这些数据提供了关于参考样本的详细信息,有助于进一步分析和确定参考样本与检索信息的关联性。

[0196] 步骤C140,依据所述检索摘要、所述检索自聚焦内容特征、所述检索安防路径图、所述目标样本摘要、所述目标样本自聚焦内容特征,以及所述目标样本安防路径图,确定所述参考样本与所述检索信息之间的样本关联度,基于所述样本关联度对所述参考样本进行降序排列,从降序排列后的参考样本中确定目标样本检索结果。

[0197] 本实施例中,服务器依据检索摘要、检索自聚焦内容特征、检索安防路径图以及目标样本的摘要、自聚焦内容特征和安防路径图,计算参考样本与检索信息之间的样本关联度。关联度的计算可能基于文本相似度、特征匹配度、图结构相似度等多种指标的综合评估。

[0198] 示例性地,在以下是一个可能的计算公式,用于计算参考样本与检索信息之间的样本关联度:

[0199] 假设有以下变量:

[0200] (T_s) 表示检索摘要(Text Summary)

[0201] (F_s) 表示检索自聚焦内容特征(Focused Content Feature)

[0202] (G_s) 表示检索安防路径图(Security Path Graph)

[0203] (T_t) 表示目标样本摘要(Target Sample Summary)

[0204] (F_t) 表示目标样本自聚焦内容特征(Target Sample Focused Content Feature)

[0205] (G_t) 表示目标样本安防路径图(Target Sample Security Path Graph)

[0206] 样本关联度 (R) 的计算公式可以定义如下:

[0207] [R = w_1 \cdot \text{Sim}(T_s, T_t) + w_2 \cdot \text{Sim}(F_s, F_t) + w_3 \cdot \text{Sim}(G_s, G_t)]

[0208] 其中：

[0209] (w_1, w_2, w_3) 是权重因子,用于调整不同相似度度量在总关联度中的贡献,这些权重可以根据具体应用场景和需求进行设定。

[0210] (\text{Sim}(T_s, T_t)) 是检索摘要与目标样本摘要之间的文本相似度。可以使用基于词袋模型、TF-IDF、余弦相似度等方法来计算。

[0211] (\text{Sim}(F_s, F_t)) 是检索自聚焦内容特征与目标样本自聚焦内容特征之间的特征相似度。由于这些特征通常是矢量形式,可以使用欧氏距离、余弦相似度等方法来计算。

[0212] (\text{Sim}(G_s, G_t)) 是检索安防路径图与目标样本安防路径图之间的图结构相似度。图结构相似度的计算相对复杂,可以使用图嵌入技术(如Graph2Vec、Node2Vec等)将图转换为矢量表示,然后计算矢量之间的相似度;或者定义特定的图匹配算法来计算图之间的相似度。

[0213] 以下是一个简单的示例计算过程：

[0214] 文本相似度计算：

[0215] 使用TF-IDF方法将检索摘要 (T_s) 和目标样本摘要 (T_t) 转换为特征矢量。

[0216] 计算两个特征矢量之间的余弦相似度作为 (\text{Sim}(T_s, T_t))。

[0217] 特征相似度计算：

[0218] 检索自聚焦内容特征 (F_s) 和目标样本自聚焦内容特征 (F_t) 已经是矢量形式。

[0219] 直接计算两个矢量之间的余弦相似度作为 (\text{Sim}(F_s, F_t))。

[0220] 图结构相似度计算(假设使用图嵌入方法)：

[0221] 使用图嵌入技术(如Graph2Vec)将检索安防路径图 (G_s) 和目标样本安防路径图 (G_t) 转换为矢量表示。

[0222] 计算两个矢量之间的余弦相似度作为 (\text{Sim}(G_s, G_t))。

[0223] 关联度计算：

[0224] 设定权重因子 (w_1, w_2, w_3) 的值(例如 (w_1 = 0.3, w_2 = 0.4, w_3 = 0.3))。

[0225] 根据上述公式计算样本关联度 (R)。

[0226] 这个计算公式可以根据具体的应用场景和需求进行调整和优化。例如,可以根据不同特征的重要性调整权重因子,或者引入更复杂的相似度度量方法来提高计算的准确性。

[0227] 然后,服务器根据样本关联度对参考样本进行降序排列,关联度越高的样本排在越前面,这样,用户就能够优先看到与检索信息最相关的样本数据。

[0228] 最后,服务器将降序排列后的参考样本返回给用户作为目标样本检索结果。用户可以根据这些结果进一步分析和处理相关的安防事件数据。

[0229] 通过这个过程,服务器能够快速地根据用户的检索请求找到相关的物联网安防事件数据,并提供了详细的样本信息和关联度评估,帮助用户更有效地利用这些数据进行分

析和决策。

[0230] 在一种可能的实施方式中,步骤C120包括:

[0231] 步骤C121,将所述检索物联网安防事件加载到安防事件分析网络,利用所述安防事件分析网络生成所述检索物联网安防事件的目标安全风险分布图。

[0232] 本实施例中,假设服务器收到一个用户提交的检索请求,用户想要查询与“智能仓库夜间非法入侵”相关的物联网安防事件数据。服务器已经预先训练了多个网络模型,包括安防事件分析网络、自聚焦内容编码网络和安防路径图生成网络,用于处理和分析安防事件数据。

[0233] 服务器首先将检索物联网安防事件(即用户想要查询的“智能仓库夜间非法入侵”事件)加载到安防事件分析网络中。安防事件分析网络是一个复杂的神经网络模型,其能够对输入的事件数据进行分析和处理,生成与该事件相关的目标安全风险分布图。

[0234] 在这个场景中,安防事件分析网络对“智能仓库夜间非法入侵”事件进行分析,识别出事件中的关键节点、异常行为和潜在的安全风险点,并生成一个目标安全风险分布图,该目标安全风险分布图直观地展示了事件中的安全风险分布情况,为后续的特征提取和路径图生成提供了基础。

[0235] 步骤C122,获取与所述目标安全风险分布图所对应的自聚焦内容编码网络,以及与所述目标安全风险分布图所对应的安防路径图生成网络。

[0236] 本实施例中,生成目标安全风险分布图后,服务器需要找到与该目标安全风险分布图对应的自聚焦内容编码网络和安防路径图生成网络,这些网络模型是专门设计用于处理和分析具有特定安全风险分布图的事件数据的。

[0237] 在这个场景中,服务器根据目标安全风险分布图的特点和标识信息,从预先训练好的网络模型库中找到与之对应的自聚焦内容编码网络和安防路径图生成网络,这些网络模型已经过充分的训练和优化,能够准确地提取事件数据中的关键特征并生成相应的安防路径图。

[0238] 步骤C123,将所述检索物联网安防事件加载到所述自聚焦内容编码网络,利用所述自聚焦内容编码网络生成所述检索物联网安防事件对应的所述检索自聚焦内容特征。

[0239] 本实施例中,服务器将检索物联网安防事件加载到自聚焦内容编码网络中。自聚焦内容编码网络是一个专门用于提取事件数据中关键自聚焦内容特征的网络模型,通过深度学习算法对输入的事件数据进行分析和处理,自动提取出与事件核心内容相关的特征矢量。

[0240] 在这个场景中,自聚焦内容编码网络对“智能仓库夜间非法入侵”事件进行分析,提取出与非法入侵行为、异常轨迹等关键内容相关的特征矢量,生成检索自聚焦内容特征,这些特征矢量准确地描述了事件中的核心内容,为后续的检索和分析提供了重要的数据支持。

[0241] 步骤C124,将所述检索物联网安防事件加载到所述安防路径图生成网络,利用所述安防路径图生成网络的图卷积单元,提取所述检索物联网安防事件的图卷积矢量序列,基于所述图卷积矢量序列生成所述检索安防路径图。

[0242] 接下来,服务器将检索物联网安防事件加载到安防路径图生成网络中。安防路径图生成网络是一个基于图卷积神经网络(GCN)的模型,其能够根据事件数据中的关键节点

和流转路径生成安防路径图。安防路径图直观地展示了事件中各关键节点之间的联系和流转路径,有助于用户快速理解事件的流程和逻辑。

[0243] 在这个场景中,安防路径图生成网络首先利用图卷积单元对“智能仓库夜间非法入侵”事件中的关键节点和流转路径进行编码,生成图卷积矢量序列。然后,基于这些矢量序列,安防路径图生成网络生成检索安防路径图,该路径图清晰地展示了非法入侵者在智能仓库中的行进路线、触发警报的位置以及安保人员的响应路径等信息,为用户提供了直观的事件可视化展示。

[0244] 通过这个过程,服务器能够准确地获取检索物联网安防事件对应的检索安防路径图和检索自聚焦内容特征,为后续的事件检索和分析提供了重要的数据支持。同时,这也展示了服务器在处理和分析物联网安防事件方面的强大能力和灵活性。

[0245] 请结合参阅图2,本申请实施例还提供了一种基于人工智能的物联网数据处理系统100,包括处理器111,以及与处理器111连接的存储器112和总线113。其中,处理器111和存储器112通过总线113完成相互间的通信。处理器111用于调用存储器112中的程序指令,以执行上述的基于人工智能的物联网数据处理方法。

[0246] 此外,本申请实施例还提供一种可读存储介质,所述可读存储介质中预设有计算机可执行指令,当处理器执行所述计算机可执行指令时,实现如上基于人工智能的物联网数据处理方法。

[0247] 应当注意的是,为了简化本申请披露的表述,从而帮助对一个或以上发明实施例的理解,前文对本申请实施例的描述中,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。同理,应当注意的是,为了简化本申请披露的表述,从而帮助对一个或以上发明实施例的理解,前文对本申请实施例的描述中,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。

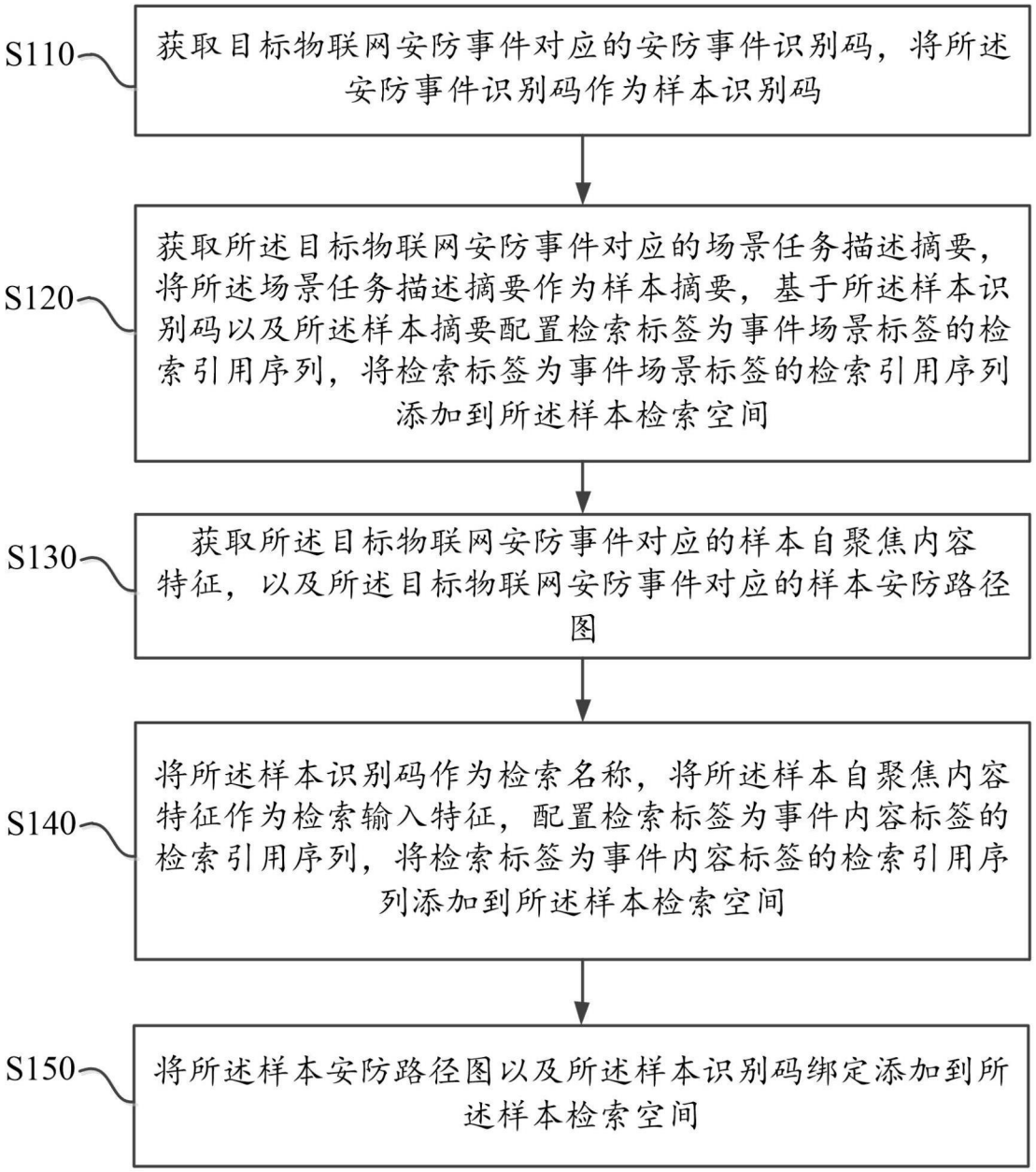

S110
获取目标物联网安防事件对应的安防事件识别码，将所述安防事件识别码作为样本识别码
S120
获取所述目标物联网安防事件对应的场景任务描述摘要，将所述场景任务描述摘要作为样本摘要，基于所述样本识别码以及所述样本摘要配置检索标签为事件场景标签的检索引用序列，将检索标签为事件场景标签的检索引用序列添加到所述样本检索空间
S130
获取所述目标物联网安防事件对应的样本自聚焦内容特征，以及所述目标物联网安防事件对应的样本安防路径图
S140
将所述样本识别码作为检索名称，将所述样本自聚焦内容特征作为检索输入特征，配置检索标签为事件内容标签的检索引用序列，将检索标签为事件内容标签的检索引用序列添加到所述样本检索空间
S150
将所述样本安防路径图以及所述样本识别码绑定添加到所述样本检索空间

图 1

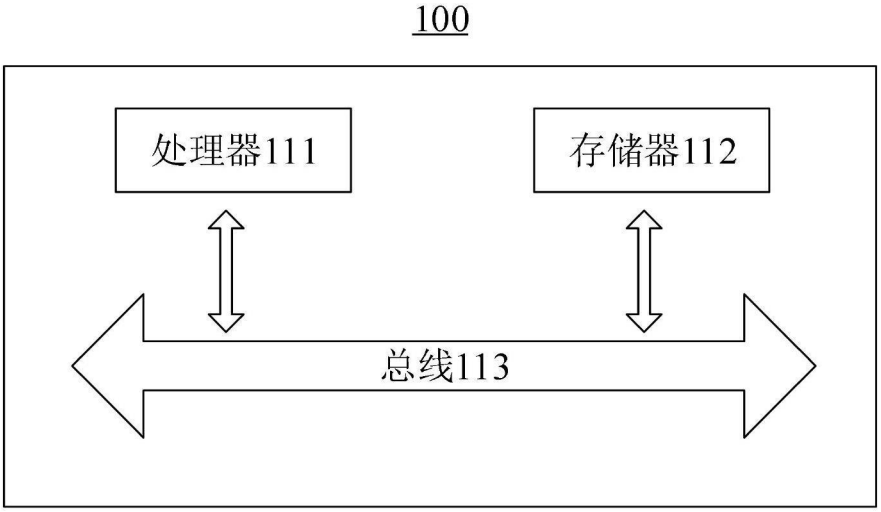


图 2