(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116680098 A
(43)申请公布日 2023.09.01

(21)申请号 202210167170.3

(22)申请日 2022.02.23

(71)申请人 中国软件评测中心(工业和信息化部软件与集成电路促进中心)
地址 100000 北京市海淀区紫竹院路66号

(72)发明人 巩潇 李梦玮 崔登祺 赵郑斌 万彬彬

(74)专利代理机构 深圳中一联合知识产权代理有限公司 44414
专利代理师 甘莹

(51)Int.Cl.
*G06F 11/07*(2006.01)
*H04L 9/40*(2022.01)
*H04L 41/0631*(2022.01)
*H04L 41/0677*(2022.01)

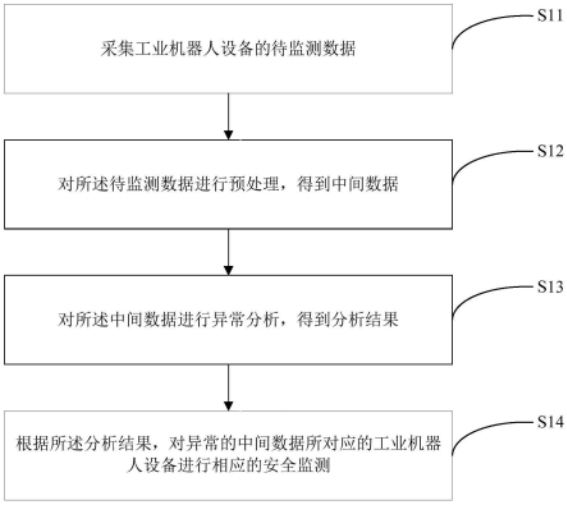
权利要求书2页 说明书11页 附图2页

(54)发明名称

工业机器人安全监测方法、装置及电子设备

(57)摘要

本申请适用于机器人安全监测技术领域,提供了工业机器人安全监测方法、装置及电子设备,包括:采集工业机器人设备的待监测数据,所述待监测数据包括工业机器人的系统数据、运行数据、日志数据和工艺数据,对所述待监测数据进行预处理,得到中间数据,对所述中间数据进行异常分析,得到分析结果,所述异常分析包括以下至少一种:脆弱性分析、异常检测分析、统计分析和故障分析,所述分析结果用于指示所述中间数据是否异常,根据所述分析结果,对异常的中间数据所对应的工业机器人设备进行相应的安全监测。本申请可以为工业机器人提供全面的安全监测。




CN 116680098 A

1.一种工业机器人安全监测方法,其特征在于,包括:

采集工业机器人设备的待监测数据,所述待监测数据包括工业机器人的系统数据、运行数据、日志数据和工艺数据;

对所述待监测数据进行预处理,得到中间数据;

对所述中间数据进行异常分析,得到分析结果,所述异常分析包括以下至少一种:脆弱性分析、异常检测分析、统计分析和故障分析,所述分析结果用于指示所述中间数据是否异常;

根据所述分析结果,对异常的中间数据所对应的工业机器人设备进行相应的安全监测。

2.如权利要求1所述的工业机器人安全监测方法,其特征在于,所述采集工业机器人设备的待监测数据,包括:

根据所述工业机器人设备所采用的工业协议和通信协议,通过对应的方式采集所述待监测数据。

3.如权利要求1所述的工业机器人安全监测方法,其特征在于,所述对所述待监测数据进行预处理,得到中间数据,包括:

按照预设的统一的数据标准对所述待监测数据进行标准化处理,得到标准数据,所述标准化处理包括清洗、打标和关联;

对所述标准数据进行基础数据分析,得到中间数据,所述基础数据分析包括以下至少一种:聚类分析、分类分析、回归分析、时序分析、模式匹配和相似匹配。

4.如权利要求3所述的工业机器人安全监测方法,其特征在于,所述标准数据包括半结构化数据和非结构化数据,在所述得到标准数据之后,还包括:

对所述半结构化数据和非结构化数据进行结构化处理,并分类存储结构化处理后的标准数据。

5.如权利要求1所述的工业机器人安全监测方法,其特征在于,还包括:

若接收到针对所述待监测数据的查询请求,则响应所述查询请求,得到查询结果;

将所述查询结果和热数据存入数据缓存区,所述热数据是指访问频次超出预设访问频次阈值的待监测数据。

6.如权利要求1所述的工业机器人安全监测方法,其特征在于,所述对所述中间数据进行异常分析,包括:

通过建立的脆弱性检测器,对所述运行数据、系统数据所对应的中间数据进行工业机器人的网络脆弱性和设备脆弱性的分析;

和/或,

根据所述运行数据的网络流量数据对应的中间数据,提取所述网络流量的基本数据特征;

根据所述基本数据特征、预先获取的正常网络流量数据特征和攻击行为特征,分析所述网络流量是否存在异常流量或异常行为;

和/或,

根据所述运行数据的网络流量数据对应的中间数据,统计指定时间范围内的网络流量并进行分析,并根据所述网络流量和所述日志数据对应的中间数据进行行为和事件统计分

析；

和/或，

通过建立的故障检测模型，对所述运行数据和日志数据所对应的中间数据，进行故障诊断、故障告警以及故障定位分析。

7.如权利要求1至6任一项所述的工业机器人安全监测方法，其特征在于，所述根据所述分析结果，对异常的中间数据所对应的工业机器人设备进行相应的安全监测，包括：

若所述分析结果指示所述工业机器人设备存在硬件设备异常，则对异常的中间数据所对应的工业机器人设备进行包括以下至少一项安全监测：设备异常监测、设备运行监测、健康度评估；

若所述分析结果指示所述工业机器人设备存在网络异常，则对异常的中间数据所对应的工业机器人设备进行包括以下至少一项安全监测：入侵监测、行为监测、威胁监测和漏洞监测。

8.一种工业机器人安全监测装置，其特征在于，包括：

数据采集模块，用于采集工业机器人设备的待监测数据，所述待监测数据包括工业机器人的系统数据、运行数据、日志数据和工艺数据；

数据预处理模块，用于对所述待监测数据进行预处理，得到中间数据；

异常分析模块，用于对所述中间数据进行异常分析，得到分析结果，所述异常分析包括以下至少一种：脆弱性分析、异常检测分析、统计分析和故障分析，所述分析结果用于指示所述中间数据是否异常；

安全监测模块，用于根据所述分析结果，对异常的中间数据所对应的工业机器人设备进行相应的安全监测。

9.一种电子设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求1至7任一项所述的方法。

10.一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至7任一项所述的方法。

# 工业机器人安全监测方法、装置及电子设备

## 技术领域

[0001] 本申请属于工业机器人安全技术领域，尤其涉及一种工业机器人安全监测方法、装置、电子设备及计算机可读存储介质。

## 背景技术

[0002] 随着工业自动化和智能化的快速发展，工业机器人技术在各行业中的应用越来越广泛，工业机器人投放到市场上的数量也越来越多。

[0003] 工业机器人的推广和普及，在对提高生产效率、增强生产安全、解放生产力带来巨大便利的同时，也带来了新的安全问题和巨大挑战。这是因为，工业机器人本身就是一个高度融合机械、驱动、控制等于一体的复杂系统，且其控制系统也是一台功能强大的高端计算机，此外，工业机器人的实际应用场景会涉及工业机器人生产线，即其实际应用场景需要增加很多感知、定位等设备，所以，工业机器人的安全问题通常会涉及到机械安全、控制安全、计算机系统的软硬件安全、应用软件安全和数据安全等安全问题。在一些复杂应用场景中，若需要多工业机器人、多设备协同工作，即应用场景除了工业机器人外还包括许多的IT设备和工控设备，此时，工业机器人的安全还涉及网络安全和工控安全等安全问题。

[0004] 现有方法中，通过采用被动检测的方式采集和解析网络数据包，从而生成相关的异常检测规则对网络进行异常监测，但上述方法只针对工控网络安全，不能提供面向工业机器人的多方面的安全监测，因此，一旦发生上述的安全问题，很可能会造成严重的生产事故。

## 发明内容

[0005] 本申请实施例提供了工业机器人安全监测方法及装置，可以解决不能为工业机器人提供多方面安全监测的问题。

[0006] 第一方面，本申请实施例提供了一种工业机器人安全监测方法，包括：

[0007] 采集工业机器人设备的待监测数据，所述待监测数据包括工业机器人的系统数据、运行数据、日志数据和工艺数据；

[0008] 对所述待监测数据进行预处理，得到中间数据；

[0009] 对所述中间数据进行异常分析，得到分析结果，所述异常分析包括以下至少一种：脆弱性分析、异常检测分析、统计分析和故障分析，所述分析结果用于指示所述中间数据是否异常；

[0010] 根据所述分析结果，对异常的中间数据所对应的工业机器人设备进行相应的安全监测。

[0011] 第二方面，本申请实施例提供了一种工业机器人安全监测装置，包括：

[0012] 数据采集模块，用于采集工业机器人设备的待监测数据，所述待监测数据包括工业机器人的系统数据、运行数据、日志数据和工艺数据；

[0013] 数据预处理模块，用于对所述待监测数据进行预处理，得到中间数据；

[0014] 异常分析模块，用于对所述中间数据进行异常分析，得到分析结果，所述异常分析包括以下至少一种：脆弱性分析、异常检测分析、统计分析和故障分析，所述分析结果用于指示所述中间数据是否异常；

[0015] 安全监测模块，用于根据所述分析结果，对异常的中间数据所对应的工业机器人设备进行相应的安全监测。

[0016] 第三方面，本申请实施例提供了一种电子设备，包括：存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现上述第一方面中所述的工业机器人安全监测方法的步骤。

[0017] 第四方面，本申请实施例提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述第一方面中所述的工业机器人安全监测方法的步骤。

[0018] 第五方面，本申请实施例提供了一种计算机程序产品，当计算机程序产品在电子设备上运行时，使得电子设备执行上述第一方面所述的工业机器人安全监测方法。

[0019] 本申请实施例与现有技术相比存在的有益效果是：通过对采集的工业机器人的待监测数据进行预处理，得到标准的中间数据，再对中间数据异常分析，得到分析结果，最后根据分析结果中存在异常的中间数据所对应的工业机器人设备进行相应的安全监测。由于工业机器人的待监测数据包括了工业机器人的系统数据、运行数据、日志数据和工艺数据，因此，保证了根据待检测数据得到的中间数据的全面性，进而保证了工业机器人安全监测的全面性。并且，由于分析结果能够指示中间数据是否异常，因此，能够根据分析结果确定出存在异常的中间数据，进而只需针对存在异常的中间数据所对应的工业机器人设备进行安全监测，从而减少不必要的工业机器人设备的安全监测，提高了安全监测效率。

## 附图说明

[0020] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍。

[0021] 图1是本申请一实施例提供的一种工业机器人安全监测方法的流程示意图；

[0022] 图2是本申请实施例提供的工业机器人安全监测装置的结构示意图；

[0023] 图3是本申请实施例提供的电子设备的结构示意图。

## 具体实施方式

[0024] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本申请实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本申请。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

[0025] 应当理解，当在本申请说明书和所附权利要求书中使用时，术语“包括”指示所描述特征、整体、步骤、操作、元素和/或组件的存在，但并不排除一个或多个其它特征、整体、步骤、操作、元素、组件和/或其集合的存在或添加。

[0026] 还应当理解，在本申请说明书和所附权利要求书中使用的术语“和/或”是指相关联列出的项中的一个或多个的任何组合以及所有可能组合，并且包括这些组合。

[0027] 在本申请说明书中描述的参考“一个实施例”或“一些实施例”等意味着在本申请的一个或多个实施例中包括结合该实施例描述的特定特征、结构或特点。由此，在本说明书中的不同之处出现的语句“在一个实施例中”、“在一些实施例中”、“在其他一些实施例中”、“在另外一些实施例中”等不是必然都参考相同的实施例，而是意味着“一个或多个但不是所有的实施例”，除非是以其他方式另外特别强调。

[0028] 实施例一：

[0029] 图1示出了本发明实施例提供的一种工业机器人安全监测方法的流程示意图，详述如下：

[0030] 步骤S11，采集工业机器人设备的待监测数据。

[0031] 其中，工业机器人为面向工业领域的多关节机械手或多自由度的机器装置，在工业生产加工过程中通过自动控制来执行作业。

[0032] 上述工业机器人设备包括工业机器人、工业机器人的控制系统、工业机器人的辅助设备、网络设备、工业生产控制系统。其中，该工业机器人的控制系统包括计算机硬件、操作系统、应用软件、数据库；该工业机器人的辅助设备是指工业机器人生产线上辅助工业机器人进行作业的设备，包括以下至少一项：感知设备、识别设备、跟踪设备、定位设备；该工业机器人的网络设备包括服务器、中间件、交换机、路由器等。

[0033] 上述待监测数据包括工业机器人的系统数据、运行数据、日志数据和工艺数据。

[0034] 本申请实施例中，该系统数据包括工业机器人设备的基本信息、硬件信息、协议信息；该运行数据包括以下至少一项：工业机器人设备的网络流量、硬件状态信息、软件状态信息；该日志数据包括工业机器人设备的运行日志，该运行日志包括以下至少一项：操作、系统、硬件、程序、通信、用户、配置信息；该工艺数据包括以下至少一项：工业机器人的逻辑程序、逻辑程序备份、位置点位、工作范围、工作速度。

[0035] 本申请实施例中，采集工业机器人各类设备所对应的系统数据、运行数据、日志数据和工艺数据，保证了采集的待监测数据的全面性，即，保证了后续进行异常分析和安全监测的全面性。

[0036] 步骤S12，对该待监测数据进行预处理，得到中间数据。

[0037] 本申请实施例中，考虑到待监测数据是从多个数据源采集得到，因此，需要对待监测数据进行预处理，比如，统一待监测数据的格式、过滤掉错误的待监测数据等等，以提高后续异常分析的便利性。

[0038] 步骤S13，对该中间数据进行异常分析，得到分析结果。

[0039] 上述异常分析包括以下至少一种：脆弱性分析、异常检测分析、故障分析和统计分析。

[0040] 其中，脆弱性分析是指通过中间数据，分析工业机器人设备是否存在脆弱性；异常检测分析是指通过中间数据检测和分析工业机器人设备存在的异常信息；统计分析是指通过中间数据统计和分析工业机器人设备的事件和行为信息；故障分析是指通过中间数据分析工业机器人设备存在的故障信息。

[0041] 上述分析结果用于指示该中间数据是否存在异常。

[0042] 本申请实施例中，通过中间数据进行异常分析，得到分析结果，该分析结果可指示该中间数据是否存在异常，以得到存在异常的中间数据相应的工业机器人设备，从而进行

相应的工业机器人安全监测。

[0043] 步骤S14,根据所述分析结果,对异常的中间数据所对应的工业机器人设备进行相应的安全监测。

[0044] 本申请实施例中,根据分析结果中存在异常的中间数据所对应的工业机器人设备进行安全监测,能够减少不必要的工业机器人安全监测,从而提高了工业机器人安全监测效率。

[0045] 本申请实施例中,通过对采集的工业机器人的待监测数据进行预处理,得到标准的中间数据,以便后续进行异常分析。对中间数据异常分析,得到分析结果,该分析结果可指示中间数据是否异常,并根据分析结果中存在异常的中间数据所对应的工业机器人设备进行相应的安全监测。由于工业机器人的待监测数据包括了工业机器人的系统数据、运行数据、日志数据和工艺数据,因此,通过对中间数据进行异常分析从而对存在异常的中间数据对应的工业机器人设备进行安全监测,保证了工业机器人安全监测的全面性,且只针对存在异常的中间数据所对应的工业机器人设备进行安全监测,减少不必要的工业机器人设备的安全监测,提高了安全监测效率。

[0046] 在一些实施例中,上述步骤S11包括:

[0047] 根据所述工业机器人设备所采用的工业协议和通信协议,通过对应的方式采集该待监测数据。

[0048] 具体地,根据工业机器人、工业机器人的控制系统、工业机器人辅助设备、网络设备、工业生产控制系统所采用的协议,以及待采集数据的数据类型,采用相应的方式采集该待监测数据。其中,工业机器人使用的协议繁多,如Profinet(Profinet,是新一代基于工业以太网技术的自动化总线标准)、以太网(Ethernet)/工业协议(Industrial Protocol,IP),不同型号、品牌的工业机器人采用的工业协议、通信协议可能都不相同,需要针对工业机器人采用的具体协议采用对应的连接方法采集数据。例如,对于工业机器人的网络设备,采用简单网络管理协议(Simple Network Management Protocol,SNMP)采集网络设备的网口信息、路由信息、丢包率等数据。

[0049] 本申请实施例中,通过根据工业机器人设备所采用的工业协议、通信协议,采用相应的方式采集待监测数据,能够降低采集不同工业机器人设备的数据的难度,即降低待监测数据的不同数据源的采集难度,保证了采集的待监测数据的全面性。

[0050] 在一些实施例中,上述对待监测数据进行预处理包括标准化处理和基础数据分析,通过对待监测数据进行标准化处理和基础数据分析的预处理操作,得到标准的中间数据,以便于后续根据中间数据进行异常分析,提高异常分析效率。对应地,上述步骤S12包括:

[0051] A1、对该待监测数据按照预设的统一的数据标准,进行标准化处理,得到标准数据,该标准化处理包括清洗、打标和关联;

[0052] 具体地,对待监测数据按照预设的统一的数据标准,进行数据的过滤、去重、和补全;按照预设的标签规则对清洗后的数据进行打标,生成各种标签数据。例如,根据工业机器人的硬件状态信息和软件状态信息的属性和数据内容,将其设定为状态数据,将硬件状态信息和软件状态信息标记为状态标签。通过关联挖掘,将表面没有相关性但具有潜在内关联的标签数据进行关联操作,得到标准数据。例如,根据数据的属性值,将不同数据源的

待监测数据关联起来，比如，将网络流量和日志数据的通信数据关联起来。

[0053] A2、对该标准数据进行基础数据分析，得到中间数据。该基础数据分析包括以下至少一种：聚类分析、分类分析、回归分析、时序分析、模式匹配和相似匹配。

[0054] 具体地，该聚类分析是指根据该标准数据中相似数据的相似性进行分类，聚类分析可根据标准数据自动进行分类。

[0055] 该分类分析是指从标准数据中选出已分好类的训练集来建立分类模型，对没有进行分类的标准数据进行分类。

[0056] 该回归分析是指通过建立因变量与影响它的自变量之间的回归模型，来预测因变量的发展趋势，例如，根据工业机器人硬件设备的基本信息及其状态信息、日志信息，获取影响工业机器人硬件设备状态的影响因子，进行回归分析，预测工业机器人硬件设备的发展趋势，如故障预测。

[0057] 该时序分析是指寻找数据的当前值与其过去值的关系，分析该标准数据的发展过程、方向和趋势。

[0058] 该模式匹配是指根据给定的数据在某一标准数据中找出与该给定的数据相同的所有数据，例如，根据给定的IP地址(Internet Protocol Address，网际协议地址)找出网络流量中该IP地址的所有数据。

[0059] 该相似匹配是指根据标准数据的特征部分，匹配找出具有相同特征的数据。

[0060] 本申请实施例中，按照预设的统一的数据标准，对待监测数据进行清洗、打标和关联，得到标准数据，对该标准数据进行基础数据分析，得到中间数据，以便于后续根据中间数据进行异常分析。

[0061] 在一些实施例中，该标准数据包括半结构化数据和非结构化数据，在上述步骤A1得到标准数据之后，还包括：

[0062] 对所述半结构化数据和非结构化数据进行结构化处理，并分类存储结构化处理后的标准数据。

[0063] 其中，根据标准数据的数据类型和数据内容将标准数据进行分类存储。例如，将工业机器人设备的硬件状态信息和软件状态信息，归类为状态信息进行存储，将工业机器人设备的硬件状态信息、软件状态信息、网络流量、协议信息归类为运行信息进行存储。

[0064] 本申请实施例中，通过对半结构化和非结构化数据进行结构化处理，得到结构化的标准数据，便于后续进行基础数据分析，同时将标准数据进行分类存储，以便查询进行基础数据分析时所需的标准数据。

[0065] 在一些实施例中，在上述步骤S12对该待监测数据进行预处理，得到中间数据之后，还包括：

[0066] B1：若接收到针对该待监测数据的查询请求，则响应该查询请求，得到查询结果。

[0067] 其中，上述针对该待监测数据的查询请求是指进行异常分析针对该待监测数据的查询请求。

[0068] B2：将该查询结果和热数据存入数据缓存区。

[0069] 其中，上述热数据是指访问频次超出预设访问频次阈值的待监测数据。

[0070] 本申请实施例中，通过将查询结果存入缓存区中，可解决数据积压的问题，同时将热数据，即访问频次超出预设阈值的待监测数据也存入缓存区中以减轻数据查询压力。

[0071] 在一些实施例中，上述步骤S13对中间数据进行异常分析时，包括：

[0072] C1：通过建立的脆弱性检测器，对所述运行数据、系统数据所对应的中间数据进行工业机器人的网络脆弱性和设备脆弱性的分析。

[0073] 和/或，

[0074] C2：根据所述运行数据的网络流量数据对应的中间数据，提取所述网络流量的基本数据特征；根据所述基本数据特征、预先获取的正常网络流量数据特征和攻击行为特征，分析所述网络流量是否存在异常流量或异常行为。

[0075] 和/或，

[0076] C3：根据所述运行数据的网络流量数据对应的中间数据，统计指定时间范围内的网络流量并进行分析，并根据所述网络流量和所述日志数据对应的中间数据进行行为和事件统计分析。

[0077] 和/或，

[0078] C4：通过建立的故障检测模型，对所述运行数据和日志数据所对应的中间数据，进行故障诊断、故障告警以及故障定位分析。

[0079] 本申请实施例中，通过对中间数据进行脆弱性分析、异常检测分析、统计分析、故障分析中的一种或几种异常分析，得到相应的异常结果，便于后续针对存在异常的中间数据对应的工业机器人设备进行相应的安全监测。

[0080] 在一些实施例中，上述步骤S14根据该分析结果，对异常的标准数据所对应的工业机器人设备进行相应的安全监测时，包括：

[0081] D1：若该异常的标准数据存在工业机器人硬件设备的异常，则根据异常结果对相应的工业机器人设备进行包括以下至少一项安全监测：设备异常监测、设备运行监测、健康度评估。

[0082] 其中，对存在异常的工业机器人设备进行设备异常监测时，将监测该工业机器人设备的数据是否仍存在异常，若存在异常则根据异常情况采取相应措施，若在设定时间内该工业机器人并无异常，则不再对该工业机器人设备进行异常监测。

[0083] 对存在异常的工业机器人设备或有需求的工业机器人设备进行设备运行监测时，将监测分析该工业机器人设备的运行信息，实时呈现该工业机器人设备的运行状况。

[0084] 对存在异常的工业机器人设备或有需求的工业机器人设备进行健康度评估时，将建立健康度模型，计算和评估工业机器人设备的健康状况，根据工业机器人设备的健康状况进行相应的保护措施和预防措施。

[0085] D2：若该异常的标准数据存在工业机器人网络的异常，则根据该异常结果对相应的工业机器人设备进行包括以下至少一项安全监测：入侵监测、行为监测、威胁监测和漏洞监测。

[0086] 其中，对存在异常的工业机器人设备进行入侵监测时，将对该工业机器人设备的网络流量进行协议解析。对于非加密流量，通过已知特征库匹配入侵行为，而对于加密流量，则通过机器学习判断网络行为。

[0087] 对存在异常的工业机器人设备进行行为监测时，对于已知协议通过协议解析识别网络中发生的行为，对于其他情况，根据已有的行为模型识别网络行为。

[0088] 对存在异常的工业机器人设备进行威胁监测时，实时更新病毒流行情况，结合工

业机器人网络内设备的漏洞、联网情况，分析工业机器人网络面临的威胁，并根据危险程度进行预警。

[0089] 对存在异常的工业机器人设备进行漏洞监测时，根据现有漏洞库，扫描探测网络中的设备存在的漏洞，提醒用户及时打补丁。

[0090] 在一些实施例中，在步骤S14之后，包括：

[0091] 根据该分析结果，结合该标准数据对工业机器人设备进行以下安全监测：主动防御、追踪溯源以及态势感知。

[0092] 其中，主动防御是指：根据工业机器人设备存在的异常，对该异常进行分析，提供针对性的防御策略。

[0093] 追踪溯源是指：通过分析工业机器人设备的日志信息，结合当前工业机器人设备的网络流量、状态信息识别攻击数据流，分析其在工业机器人网络中的行为变化，对网络攻击者进行追踪定位。

[0094] 态势感知是指：通过对工业机器人待监测数据进行综合统计分析，呈现总体运行情况，判断工业机器人的发展态势，发现工业机器人生产线上存在的威胁。

[0095] 本申请实施例中，通过对存在的工业机器人硬件设备或网络的异常，根据分析结果对应的工业机器人设备进行安全监测，用于只针对存在异常的工业机器人设备进行安全监测，减少了不必要的持续的安全监测，提高了安全监测的效率。

[0096] 实施例二：

[0097] 对应于上文实施例所述的一种工业机器人安全监测方法，图2示出了本申请实施例提供的一种工业机器人安全监测装置的结构框图，为了便于说明，仅示出了与本申请实施例相关的部分。

[0098] 参照图2，该工业机器人安全监测装置2包括：数据采集模块21，数据预处理模块22，异常分析模块23，安全监测模块24。其中，

[0099] 数据采集模块21，用于采集工业机器人设备的待监测数据，该待监测数据包括工业机器人的系统数据、运行数据、日志数据和工艺数据。

[0100] 数据预处理模块22，用于对该待监测数据进行预处理，得到中间数据。

[0101] 异常分析模块23，用于对该中间数据进行异常分析，得到分析结果，该异常分析包括以下至少一种：脆弱性分析、异常检测分析、统计分析和故障分析，该分析结果用于指示该中间数据是否异常。

[0102] 安全监测模块24，用于根据该分析结果，对异常的中间数据所对应的工业机器人设备进行相应的安全监测。

[0103] 本申请实施例中，通过对采集的工业机器人的待监测数据进行预处理，得到标准的中间数据，以便后续进行异常分析。对中间数据异常分析，得到分析结果，该分析结果可指示中间数据是否异常，并根据分析结果中存在异常的中间数据所对应的工业机器人设备进行相应的安全监测。由于工业机器人的待监测数据包括了工业机器人的系统数据、运行数据、日志数据和工艺数据，因此，通过对中间数据进行异常分析从而对存在异常的中间数据对应的工业机器人设备进行安全监测，保证了工业机器人安全监测的全面性，且只针对存在异常的中间数据所对应的工业机器人设备进行安全监测，减少不必要的工业机器人设备的安全监测，提高了安全监测效率。

[0104] 在一些实施例中，上述数据采集模块21具体用于：

[0105] 根据工业机器人设备所采用的工业协议和通信协议，通过对应的方式采集待监测数据。

[0106] 在一些实施例中，上述数据预处理模块22包括：

[0107] 标准化处理单元，用于按照预设的统一的数据标准对该待监测数据进行标准化处理，得到标准数据，该标准化处理包括清洗、打标和关联。

[0108] 基础数据分析单元，用于对该标准数据进行基础数据分析，得到中间数据，该基础数据分析包括以下至少一种：聚类分析、分类分析、回归分析、时序分析、模式匹配和相似匹配。

[0109] 在一些实施例中，上述标准数据包括半结构化数据和非结构化数据，上述工业机器人安全监测装置2还包括：

[0110] 分类存储模块，用于对半结构化数据和非结构化数据进行结构化处理，并分类存储结构化处理后的标准数据。

[0111] 在一些实施例中，上述工业机器人安全监测装置2还包括：

[0112] 数据查询模块，用于接收针对该待监测数据的查询请求，响应该查询请求，得到查询结果。

[0113] 缓存模块，用于将上述查询结果和热数据存入数据缓存区，该热数据是指访问频次超出预设访问频次阈值的待监测数据。

[0114] 在一些实施例中，上述异常分析模块23包括：

[0115] 脆弱性分析单元，用于通过建立的脆弱性检测器，对该运行数据、系统数据所对应的中间数据进行工业机器人的网络脆弱性和设备脆弱性的分析。

[0116] 异常检测分析单元，用于根据该运行数据的网络流量数据对应的中间数据，提取该网络流量的基本数据特征；根据该基本数据特征、预先获取的正常网络流量数据特征和攻击行为特征，分析该网络流量是否存在异常流量或异常行为。

[0117] 统计分析单元，用于根据该运行数据的网络流量数据对应的中间数据，统计指定时间范围内的网络流量并进行分析，并根据该网络流量和该日志数据对应的中间数据进行行为和事件统计分析。

[0118] 故障分析单元，用于通过建立的故障检测模型，对该运行数据和日志数据所对应的中间数据，进行故障诊断、故障告警以及故障定位分析。

[0119] 在一些实施例中，上述安全监测模块24包括：

[0120] 设备安全监测单元，用于对异常的中间数据所对应的工业机器人设备进行包括以下至少一项安全监测：设备异常监测、设备运行监测、健康度评估。

[0121] 网络安全监测单元，用于对异常的中间数据所对应的工业机器人设备进行包括以下至少一项安全监测：入侵监测、行为监测、威胁监测和漏洞监测。

[0122] 在一些实施例中，上述工业机器人安全监测装置2还包括：

[0123] 整体应用模块，用于根据该分析结果，结合该标准数据对工业机器人设备进行以下安全监测：主动防御、追踪溯源以及态势感知。

[0124] 需要说明的是，上述装置/单元之间的信息交互、执行过程等内容，由于与本申请方法实施例基于同一构思，其具体功能及带来的技术效果，具体可参见方法实施例部分，此

处不再赘述。

[0125] 实施例三：

[0126] 图3为本申请一实施例提供的电子设备的结构示意图。如图3所示，该实施例的电子设备3包括：至少一个处理器30(图3中仅示出一个处理器)、存储器31以及存储在所述存储器31中并可在所述至少一个处理器30上运行的计算机程序32，所述处理器30执行所述计算机程序32时实现上述任意各个方法实施例中的步骤，例如图1所示的步骤S11至S14。或者，所述处理器30执行所述计算机程序32时实现上述各装置实施例中各模块/单元的功能，如图2所示模块21至24的功能。

[0127] 示例性的，所述计算机程序32可以被分割成一个或多个模块/单元，所述一个或者多个模块/单元被存储在所述存储器31中，并由所述处理器30执行，以完成本申请。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机程序指令段，该指令段用于描述所述计算机程序32在所述电子设备3中的执行过程。例如，所述计算机程序32可以被分割成数据采集模块、数据预处理模块、异常分析模块、安全监测模块，各模块之间具体功能如下：

[0128] 数据采集模块21，用于采集工业机器人设备的待监测数据，该待监测数据包括工业机器人的系统数据、运行数据、日志数据和工艺数据；

[0129] 数据预处理模块22，用于对该待监测数据进行预处理，得到中间数据；

[0130] 异常分析模块23，用于对该中间数据进行异常分析，得到分析结果，该异常分析包括以下至少一种：脆弱性分析、异常检测分析、统计分析和故障分析，该分析结果用于指示该中间数据是否异常；

[0131] 安全监测模块24，用于根据该分析结果，对异常的中间数据所对应的工业机器人设备进行相应的安全监测。

[0132] 所述电子设备3可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。该电子设备可包括，但不仅限于，处理器30、存储器31。本领域技术人员可以理解，图3仅仅是电子设备3的举例，并不构成对电子设备3的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如还可以包括输入输出设备、网络接入设备等。

[0133] 所称处理器30可以是中央处理单元(Central Processing Unit，CPU)，该处理器30还可以是其他通用处理器、数字信号处理器(Digital Signal Processor，DSP)、专用集成电路(Application Specific Integrated Circuit，ASIC)、现场可编程门阵列(Field-Programmable Gate Array，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。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。

[0134] 所述存储器31在一些实施例中可以是所述电子设备3的内部存储单元，例如电子设备3的硬盘或内存。所述存储器31在另一些实施例中也可以是所述电子设备3的外部存储设备，例如所述电子设备3上配备的插接式硬盘，智能存储卡(Smart Media Card，SMC)，安全数字(Secure Digital，SD)卡，闪存卡(Flash Card)等。进一步地，所述存储器31还可以既包括所述电子设备3的内部存储单元也包括外部存储设备。所述存储器31用于存储操作系统、应用程序、引导装载程序(BootLoader)、数据以及其他程序等，例如所述计算机程序的程序代码等。所述存储器31还可以用于暂时地存储已经输出或者将要输出的数据。

[0135] 所属领域的技术人员可以清楚地了解到,为了描述的方便和简洁,仅以上述各功能单元、模块的划分进行举例说明,实际应用中,可以根据需要而将上述功能分配由不同的功能单元、模块完成,即将所述装置的内部结构划分成不同的功能单元或模块,以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中,上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。另外,各功能单元、模块的具体名称也只是为了便于相互区分,并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0136] 本申请实施例还提供了一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,所述计算机程序被处理器执行时实现可实现上述各个方法实施例中的步骤。

[0137] 本申请实施例提供了一种计算机程序产品,当计算机程序产品在电子设备上运行时,使得电子设备执行时实现可实现上述各个方法实施例中的步骤。

[0138] 所述集成的单元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,本申请实现上述实施例方法中的全部或部分流程,可以通过计算机程序来指令相关的硬件来完成,所述的计算机程序可存储于一计算机可读存储介质中,该计算机程序在被处理器执行时,可实现上述各个方法实施例的步骤。其中,所述计算机程序包括计算机程序代码,所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质至少可以包括:能够将计算机程序代码携带到拍照装置/电子设备的任何实体或装置、记录介质、计算机存储器、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、电载波信号、电信信号以及软件分发介质。例如U盘、移动硬盘、磁碟或者光盘等。在某些司法管辖区,根据立法和专利实践,计算机可读介质不可以是电载波信号和电信信号。

[0139] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述或记载的部分,可以参见其它实施例的相关描述。

[0140] 本领域普通技术人员可以意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本申请的范围。

[0141] 在本申请所提供的实施例中,应该理解到,所揭露的装置/网络设备和方法,可以通过其它的方式实现。例如,以上所描述的装置/网络设备实施例仅仅是示意性的,例如,所述模块或单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通讯连接可以是通过一些接口,装置或单元的间接耦合或通讯连接,可以是电性,机械或其它的形式。

[0142] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个

网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0143] 以上所述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，均应包含在本申请的保护范围之内。

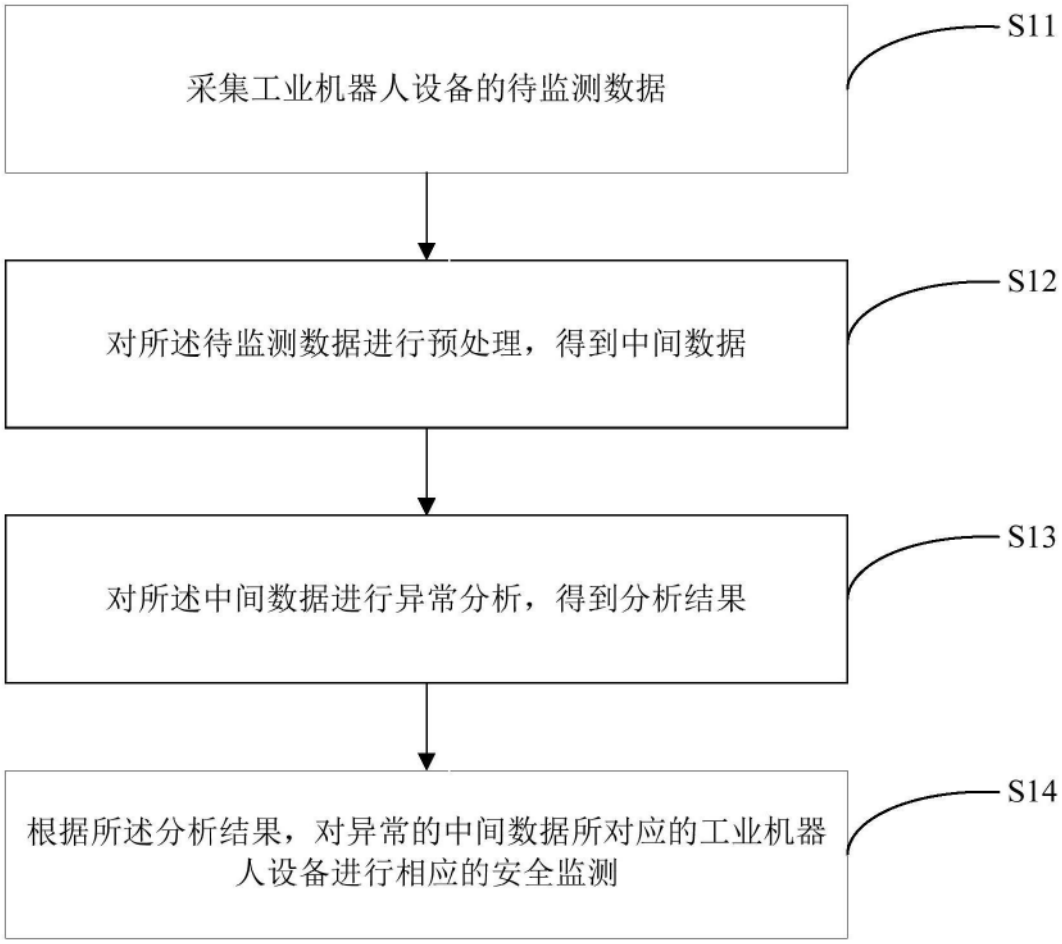

采集工业机器人设备的待监测数据
S11
对所述待监测数据进行预处理，得到中间数据
S12
对所述中间数据进行异常分析，得到分析结果
S13
根据所述分析结果，对异常的中间数据所对应的工业机器人设备进行相应的安全监测
S14

图1

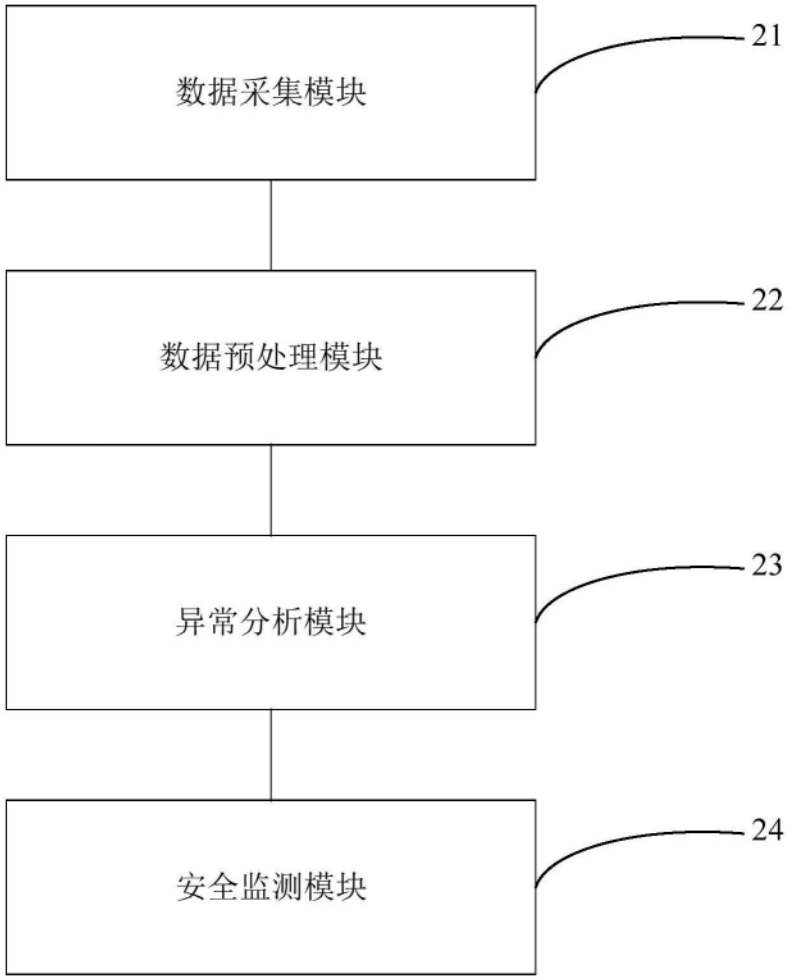

数据采集模块
21
数据预处理模块
22
异常分析模块
23
安全监测模块
24

图2

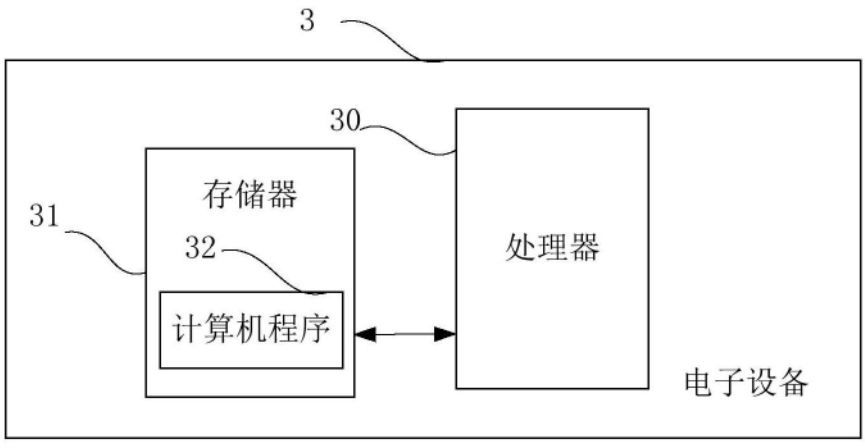

3
30
存储器
31
32
计算机程序
处理器
电子设备

图3