(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 117544420 B
(45)授权公告日 2024.03.29

(21)申请号 202410021364.1
(22)申请日 2024.01.08
(65)同一申请的已公布的文献号
申请公布号 CN 117544420 A
(43)申请公布日 2024.02.09
(73)专利权人 山东省标准化研究院(WTO/TBT山东咨询工作站)
地址 250013 山东省济南市历下区历山路146-6号
(72)发明人 孙玉亭 王璐 刘春霞 孙阳阳 张静珠 张旭 张岩
(74)专利代理机构 山东鼎骏知识产权代理有限公司 37469
专利代理师 刘玉玲
(51)Int.Cl.
H04L 9/40(2022.01)
G06F 18/213(2023.01)
G06F 18/23(2023.01)
G06F 18/243(2023.01)
G06N 5/022(2023.01)

(56)对比文件
CN 112613664 A,2021.04.06
CN 116821750 A,2023.09.29
CN 117095506 A,2023.11.21
US 2019305589 A1,2019.10.03
CN 116800536 A,2023.09.22
CN 113159482 A,2021.07.23
CN 114997607 A,2022.09.02
CN 115691044 A,2023.02.03
CN 116248489 A,2023.06.09
CN 117235743 A,2023.12.15
EP 4115252 A1,2023.01.11
YuQing Yu;Qingying Hao;Ping Hao.The research and application of enterprises' dynamic risk monitoring and assessment model based on related time series.《2017 Chinese Automation Congress (CAC)》.2018,全文.
(续)

审查员 李华

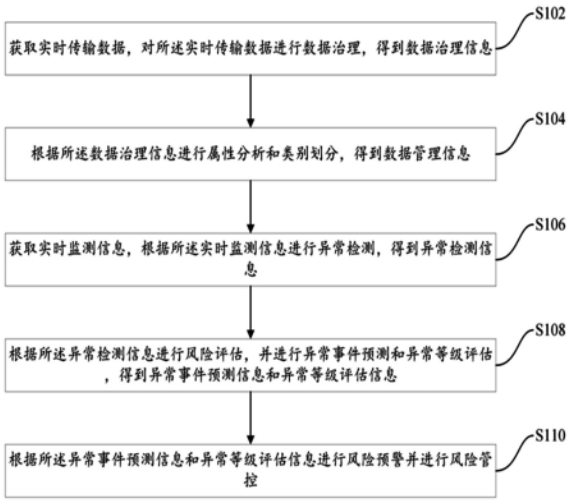
权利要求书5页 说明书11页 附图3页

(54)发明名称

一种基于数据分析的融合系统安全管理方法及系统

(57)摘要

本发明公开了一种基于数据分析的融合系统安全管理方法及系统,包括:获取实时传输数据,对所述实时传输数据进行数据治理,得到数据治理信息;根据所述数据治理信息进行属性分析和类别划分,得到数据管理信息;获取实时监测信息,根据所述实时监测信息进行异常检测,得到异常检测信息;根据所述异常检测信息进行风险评估,并进行异常事件预测和异常等级评估,得到异常事件预测信息和异常等级评估信息;根据所述异常事件预测信息和异常等级评估信息进行风险预警并进行风险管控。本发明在提高系统整体安全性的同时,降低误报率,实现更加智能和高效的安全管理,及对网络安全的全方位监测、分析和响应。



CN 117544420 B

[转续页]

[接上页]

(56)对比文件

王静;高昆仑;卞超轶;梁潇.基于大数据的能源集团统一运行监测与安全预警平台.电信科学.2018,(第05期),全文.

钟志琛.基于网络流量异常检测的电网工控系统安全监测技术.电力信息与通信技术.2017,(第01期),全文.

1.一种基于数据分析的融合系统安全管理方法,其特征在于,包括:

获取实时传输数据,对所述实时传输数据进行数据治理,得到数据治理信息;

根据所述数据治理信息进行属性分析和类别划分,得到数据管理信息;

获取实时监测信息,根据所述实时监测信息进行异常检测,得到异常检测信息;

根据所述异常检测信息进行风险评估,并进行异常事件预测和异常等级评估,得到异常事件预测信息和异常等级评估信息;

根据所述异常事件预测信息和异常等级评估信息进行风险预警并进行风险管控;

所述获取实时监测信息,根据所述实时监测信息进行异常检测,得到异常检测信息,具体包括:

获取实时监测信息,所述实时监测信息包括数据监测信息和运行监测信息;

基于孤立森林算法构建数据异常检测模型,将数据监测信息输入至所述数据异常检测模型中进行数据异常检测;

引入RANSAC算法,根据数据监测信息随机选取若干样本数据,通过选取的若干样本数据进行线性拟合,并根据线性拟合计算实际观测值与拟合预测值的差异,生成残差特征;

对数据监测信息进行特征提取,结合残差特征构建新的特征矩阵,输入至所述数据异常检测模型中,根据新的特征矩阵确定孤立森林中树的总数并构建特征空间;

构建随机二叉搜索树检测特征空间中分布低密度和孤立的数据点,定义为孤立点,计算各孤立点的在对应的树的路径长度,作为异常分数,与预设阈值进行判断,得到异常数据检测信息;

构建数据异常管控规则,结合所述异常数据检测信息对异常数据进行修正和拦截;

对运行监测信息进行时序化处理,构建运行异常检测模型,包括特征提取模块和异常识别模块;

基于梯度提升决策树结合极端梯度提升算法搭建特征提取模块,对所述运行监测信息进行特征提取;

提取时序特征和数据类型特征,并计算各特征之间的皮尔逊相关系数作为相关性特征,得到第二特征信息,并构建特征矩阵;

将构建的特征矩阵输入至异常检测模块,检测异常数据的频率和规模,并根据相关性特征检测潜在异常数据,得到异常运行检测信息;

结合异常数据检测信息和异常运行检测信息构成异常检测信息;

所述根据所述异常检测信息进行风险评估,并进行异常事件预测和异常等级评估,具体包括:

基于大数据检索获取风险因素数据集,利用平行坐标方法将风险因素数据集映射至平行坐标中,每个数据轴特定的维度范围和类型,得到风险因素图;

引入主成分分析法对风险因素图进行降维处理,剔除相关性小的风险因素,得到主要风险因素信息;

根据主要风险因素信息结合专家评价法获取各主要风险因素的风险影响度,构建影响度矩阵,结合谱聚类算法进行风险因素类别划分,并根据各类型风险因素的风险影响度进行风险等级划分,得到风险因素划分信息;

基于熵值法结合风险因素划分信息计算各风险因素的熵值,结合各风险因素的风险等

级设定风险评估权重,得到风险评估权重信息;

获取异常检测信息,基于风险评估权重信息构建风险评估模型,将所述异常检测信息输入至风险评估模型中进行风险评估,得到风险评估信息;

所述风险评估信息包括数据风险评估信息、运行风险评估信息和综合风险评估信息;

基于大数据检索获取各种异常事件的特征信息,并按照时间序列将各特征信息进行时序处理,并构建异常事件特征图谱;

将所述异常检测信息与所述异常事件特征图谱进行相似度计算,并与预设阈值进行判断,根据判断结果确定特征节点,并选取对应的特征路径和异常事件,得到异常事件预测信息;

根据所述异常事件特征图谱构建异常等级评估规则,划分各特征节点的节点范围设定不同的异常等级;

通过异常等级评估规则结合所述异常事件预测信息进行异常等级评估,得到异常等级评估信息。

2.根据权利要求1所述的一种基于数据分析的融合系统安全管理方法,其特征在于,所述获取实时传输数据,对所述实时传输数据进行数据治理,得到数据治理信息,具体包括:

建立数据治理机制,获取实时传输数据,通过数据治理机制对实时传输数据进行数据治理;

预设数据来源识别规则,提取所述实时传输数据的来源标识符结合数据来源识别规则进行来源识别,判断是否为未知数据,得到来源识别结果信息;

提取所述实时传输数据的行为指令特征,根据提取的行为指令特征进行行为识别,识别实时传输数据的行为请求,得到行为识别信息;

根据所述行为识别信息和来源识别结果信息判断是否接收传输数据,若接收,则对所述实时传输数据进行预处理,将所述实时传输数据进行数据拼接、数据合并和数据修正,得到预处理信息;

对所述预处理信息进行标准化处理,提取实时传输信息的传输权限特征,结合数据加密算法判断是否需要进行数据加密,并构建元数据目录,记录数据来源,得到数据治理信息。

3.根据权利要求1所述的一种基于数据分析的融合系统安全管理方法,其特征在于,所述根据所述数据治理信息进行属性分析和类别划分,得到数据管理信息,具体包括:

获取数据治理信息,对所述数据治理信息进行特征提取,提取实时传输数据的技术特征和业务特征,得到第一特征信息;

根据所述第一特征信息对实时传输数据进行技术属性分析,分析目标数据的数据类型、数据格式、存储特点和数据规模,得到技术属性分析信息;

基于专家分析法获取业务属性分析要素,结合主成分分析法进行权重设定,将各业务属性分析要素按照相关性合并成主成分分析要素,计算各主成分的方差解释度,作为业务属性分析权重;

根据业务属性分析权重结合所述第一特征信息进行业务属性分析,得到业务属性分析信息;

结合所述技术属性分析信息和业务属性分析信息构成属性分析信息;

预设若干类别标签,所述类别标签包括技术属性类别标签和业务属性类别标签,计算所述属性分析信息与各类别标签的马氏距离,得到马氏距离信息;

将所述马氏距离信息与预设阈值进行判断,根据判断结果对实时传输数据进行类别划分,得到类别划分信息;

结合属性分析信息和类别划分信息构成数据管理信息。

4.根据权利要求1所述的一种基于数据分析的融合系统安全管理方法,其特征在于,所述根据所述异常事件预测信息和异常等级评估信息进行风险预警并进行风险管控,具体包括:

基于大数据检索获取各种不同异常程度的异常事件处理实例,基于聚类算法结合异常等级评估规则进行处理实例类型划分,得到处理实例数据集;

基于遗传算法构建管控策略制定模型,通过处理实例数据集构建训练数据集对所述管控策略制定模型进行深度学习和训练;

获取异常等级评估信息、异常事件预测信息和风险评估信息,构建风险预警规则,结合异常等级评估信息和风险评估信息进行风险预警判断,根据判断结果进行风险预警;

获取数据治理信息和数据管理信息,结合异常事件预测信息进行异常溯源,分析异常数据的来源、路径和作用,得到异常溯源信息;

将异常溯源信息、异常等级评估信息、异常事件预测信息和风险评估信息输入至所述管控策略制定模型中进行管控策略制定,得到管控策略信息,根据所述管控策略信息进行风险管控。

5.一种基于数据分析的融合系统安全管理系统,其特征在于,该系统包括:存储器、处理器,所述存储器中包含基于数据分析的融合系统安全管理方法程序,所述基于数据分析的融合系统安全管理方法程序被所述处理器执行时实现如下步骤:

获取实时传输数据,对所述实时传输数据进行数据治理,得到数据治理信息;

根据所述数据治理信息进行属性分析和类别划分,得到数据管理信息;

获取实时监测信息,根据所述实时监测信息进行异常检测,得到异常检测信息;

根据所述异常检测信息进行风险评估,并进行异常事件预测和异常等级评估,得到异常事件预测信息和异常等级评估信息;

根据所述异常事件预测信息和异常等级评估信息进行风险预警并进行风险管控;

所述获取实时监测信息,根据所述实时监测信息进行异常检测,得到异常检测信息,具体包括:

获取实时监测信息,所述实时监测信息包括数据监测信息和运行监测信息;

基于孤立森林算法构建数据异常检测模型,将数据监测信息输入至所述数据异常检测模型中进行数据异常检测;

引入RANSAC算法,根据数据监测信息随机选取若干样本数据,通过选取的若干样本数据进行线性拟合,并根据线性拟合计算实际观测值与拟合预测值的差异,生成残差特征;

对数据监测信息进行特征提取,结合残差特征构建新的特征矩阵,输入至所述数据异常检测模型中,根据新的特征矩阵确定孤立森林中树的总数并构建特征空间;

构建随机二叉搜索树检测特征空间中分布低密度和孤立的数据点,定义为孤立点,计算各孤立点的在对应的树的路径长度,作为异常分数,与预设阈值进行判断,得到异常数据

检测信息；

构建数据异常管控规则，结合所述异常数据检测信息对异常数据进行修正和拦截；

对运行监测信息进行时序化处理，构建运行异常检测模型，包括特征提取模块和异常识别模块；

基于梯度提升决策树结合极端梯度提升算法搭建特征提取模块，对所述运行监测信息进行特征提取；

提取时序特征和数据类型特征，并计算各特征之间的皮尔逊相关系数作为相关性特征，得到第二特征信息，并构建特征矩阵；

将构建的特征矩阵输入至异常检测模块，检测异常数据的频率和规模，并根据相关性特征检测潜在异常数据，得到异常运行检测信息；

结合异常数据检测信息和异常运行检测信息构成异常检测信息；

所述根据所述异常检测信息进行风险评估，并进行异常事件预测和异常等级评估，具体包括：

基于大数据检索获取风险因素数据集，利用平行坐标方法将风险因素数据集映射至平行坐标中，每个数据轴特定的维度范围和类型，得到风险因素图；

引入主成分分析法对风险因素图进行降维处理，剔除相关性小的风险因素，得到主要风险因素信息；

根据主要风险因素信息结合专家评价法获取各主要风险因素的风险影响度，构建影响度矩阵，结合谱聚类算法进行风险因素类别划分，并根据各类型风险因素的风险影响度进行风险等级划分，得到风险因素划分信息；

基于熵值法结合风险因素划分信息计算各风险因素的熵值，结合各风险因素的风险等级设定风险评估权重，得到风险评估权重信息；

获取异常检测信息，基于风险评估权重信息构建风险评估模型，将所述异常检测信息输入至风险评估模型中进行风险评估，得到风险评估信息；

所述风险评估信息包括数据风险评估信息、运行风险评估信息和综合风险评估信息；

基于大数据检索获取各种异常事件的特征信息，并按照时间序列将各特征信息进行时序处理，并构建异常事件特征图谱；

将所述异常检测信息与所述异常事件特征图谱进行相似度计算，并与预设阈值进行判断，根据判断结果确定特征节点，并选取对应的特征路径和异常事件，得到异常事件预测信息；

根据所述异常事件特征图谱构建异常等级评估规则，划分各特征节点的节点范围设定不同的异常等级；

通过异常等级评估规则结合所述异常事件预测信息进行异常等级评估，得到异常等级评估信息。

6.根据权利要求5所述的一种基于数据分析的融合系统安全管理系统，其特征在于，所述获取实时传输数据，对所述实时传输数据进行数据治理，得到数据治理信息，具体包括：

建立数据治理机制，获取实时传输数据，通过数据治理机制对实时传输数据进行数据治理；

预设数据来源识别规则，提取所述实时传输数据的来源标识符结合数据来源识别规则

进行来源识别,判断是否为未知数据,得到来源识别结果信息;

提取所述实时传输数据的行为指令特征,根据提取的行为指令特征进行行为识别,识别实时传输数据的行为请求,得到行为识别信息;

根据所述行为识别信息和来源识别结果信息判断是否接收传输数据,若接收,则对所述实时传输数据进行预处理,将所述实时传输数据进行数据拼接、数据合并和数据修正,得到预处理信息;

对所述预处理信息进行标准化处理,提取实时传输信息的传输权限特征,结合数据加密算法判断是否需要进行数据加密,并构建元数据目录,记录数据来源,得到数据治理信息。

7.根据权利要求5所述的一种基于数据分析的融合系统安全管理系统,其特征在于,所述根据所述数据治理信息进行属性分析和类别划分,得到数据管理信息,具体包括:

获取数据治理信息,对所述数据治理信息进行特征提取,提取实时传输数据的技术特征和业务特征,得到第一特征信息;

根据所述第一特征信息对实时传输数据进行技术属性分析,分析目标数据的数据类型、数据格式、存储特点和数据规模,得到技术属性分析信息;

基于专家分析法获取业务属性分析要素,结合主成分分析法进行权重设定,将各业务属性分析要素按照相关性合并成主成分分析要素,计算各主成分的方差解释度,作为业务属性分析权重;

根据业务属性分析权重结合所述第一特征信息进行业务属性分析,得到业务属性分析信息;

结合所述技术属性分析信息和业务属性分析信息构成属性分析信息;

预设若干类别标签,所述类别标签包括技术属性类别标签和业务属性类别标签,计算所述属性分析信息与各类别标签的马氏距离,得到马氏距离信息;

将所述马氏距离信息与预设阈值进行判断,根据判断结果对实时传输数据进行类别划分,得到类别划分信息;

结合属性分析信息和类别划分信息构成数据管理信息。

一种基于数据分析的融合系统安全管理方法及系统

技术领域

[0001] 本发明涉及数据安全管理技术领域,尤其涉及一种基于数据分析的融合系统安全管理方法及系统。

背景技术

[0002] 在搭建智能化系统的过程中,需重点考虑系统的安全性,信息系统安全规划在满足自身业务需求的同时,必须要满足信息技术安全规范的要求。随着信息技术的迅猛发展,网络攻击手段也日益翻新。传统的系统安全管理方法往往侧重于单一安全防御手段,如防火墙、入侵检测系统、访问控制等,但这些方法存在无法全面覆盖各类安全威胁、难以识别新型攻击手段等问题,并且难以满足复杂多变的威胁环境和系统结构。

[0003] 目前,传统的网络安全手段难以全面应对多样化的攻击形式。网络黑客采用的技术手段日益复杂,包括但不限于恶意软件、社交工程和零日漏洞利用,传统手段在面对这些新型攻击时显得力不从心。同时,网络内部的威胁也日益引起关注。恶意内部人员、未经授权的访问以及内部系统漏洞可能导致敏感信息泄露和系统遭受损害,而传统方法对于这些内部威胁的识别和防范能力相对较弱。

[0004] 因此,迫切需要一种更加综合、智能化的系统安全管理方法,以更好地适应网络安全威胁的多样性和复杂性,提高专利标准融合系统的安全性。同时,在提高网络系统整体安全性的基础上,进一步降低误报率,实现更加智能和高效的安全管理,实现对网络安全的全方位监测、分析和响应。

发明内容

[0005] 本发明克服了现有技术的缺陷,提供了一种基于数据分析的融合系统安全管理方法及系统,其重要目的在于提高网络系统整体安全性,降低误报率,实现更加智能和高效的安全管理。

[0006] 为实现上述目的本发明第一方面提供了一种基于数据分析的融合系统安全管理方法,包括:

[0007] 获取实时传输数据,对所述实时传输数据进行数据治理,得到数据治理信息;

[0008] 根据所述数据治理信息进行属性分析和类别划分,得到数据管理信息;

[0009] 获取实时监测信息,根据所述实时监测信息进行异常检测,得到异常检测信息;

[0010] 根据所述异常检测信息进行风险评估,并进行异常事件预测和异常等级评估,得到异常事件预测信息和异常等级评估信息;

[0011] 根据所述异常事件预测信息和异常等级评估信息进行风险预警并进行风险管控。

[0012] 本方案中,所述获取实时传输数据,对所述实时传输数据进行数据治理,得到数据治理信息,具体为:

[0013] 建立数据治理机制,获取实时传输数据,通过数据治理机制对实时传输数据进行数据治理;

[0014] 预设数据来源识别规则,提取所述实时传输数据的来源标识符结合数据来源识别规则进行来源识别,判断是否为未知数据,得到来源识别结果信息;

[0015] 提取所述实时传输数据的行为指令特征,根据提取的行为指令特征进行行为识别,识别实时传输数据的行为请求,得到行为识别信息;

[0016] 根据所述行为识别信息和来源识别结果信息判断是否接收传输数据,若接收,则对所述实时传输数据进行预处理,将所述实时传输数据进行数据拼接、数据合并和数据修正,得到预处理信息;

[0017] 对所述预处理信息进行标准化处理,提取实时传输信息的传输权限特征,结合数据加密算法判断是否需要进行数据加密,并构建元数据目录,记录数据来源,得到数据治理信息。

[0018] 本方案中,所述根据所述数据治理信息进行属性分析和类别划分,得到数据管理信息,具体为:

[0019] 获取数据治理信息,对所述数据治理信息进行特征提取,提取实时传输数据的技术特征和业务特征,得到第一特征信息;

[0020] 根据所述第一特征信息对实时传输数据进行技术属性分析,分析目标数据的数据类型、数据格式、存储特点和数据规模,得到技术属性分析信息;

[0021] 基于专家分析法获取业务属性分析要素,结合主成分分析法进行权重设定,将各业务属性分析要素按照相关性合并成主成分分析要素,计算各主成分的方差解释度,作为业务属性分析权重;

[0022] 根据业务属性分析权重结合所述第一特征信息进行业务属性分析,得到业务属性分析信息;

[0023] 结合所述技术属性分析信息和业务属性分析信息构成属性分析信息;

[0024] 预设若干类别标签,所述类别标签包括技术属性类别标签和业务属性类别标签,计算所述属性分析信息与各类别标签的马氏距离,得到马氏距离信息;

[0025] 将所述马氏距离信息与预设阈值进行判断,根据判断结果对实时传输数据进行类别划分,得到类别划分信息;

[0026] 结合属性分析信息和类别划分信息构成数据管理信息。

[0027] 本方案中,所述获取实时监测信息,根据所述实时监测信息进行异常检测,得到异常检测信息,具体为:

[0028] 获取实时监测信息,所述实时监测信息包括数据监测信息和运行监测信息;

[0029] 基于孤立森林算法构建数据异常检测模型,将数据监测信息输入至所述数据异常检测模型中进行数据异常检测;

[0030] 引入RANSAC算法,根据数据监测信息随机选取若干样本数据,通过选取的若干样本数据进行线性拟合,并根据线性拟合计算实际观测值与拟合预测值的差异,生成残差特征;

[0031] 对数据监测信息进行特征提取,结合残差特征构建新的特征矩阵,输入至所述数据异常检测模型中,根据新的特征矩阵确定孤立森林中树的总数并构建特征空间;

[0032] 构建随机二叉搜索树检测特征空间中分布低密度和孤立的数据点,定义为孤立点,计算各孤立点的在对应的树的路径长度,作为异常分数,与预设阈值进行判断,得到异

常数据检测信息；

[0033] 构建数据异常管控规则，结合所述异常数据检测信息对异常数据进行修正和拦截；

[0034] 对运行监测信息进行时序化处理，构建运行异常检测模型，包括特征提取模块和异常识别模块；

[0035] 基于梯度提升决策树结合极端梯度提升算法搭建特征提取模块，对所述运行监测信息进行特征提取；

[0036] 提取时序特征和数据类型特征，并计算各特征之间的皮尔逊相关系数作为相关性特征，得到第二特征信息，并构建特征矩阵；

[0037] 将构建的特征矩阵输入至异常检测模块，检测异常数据的频率和规模，并根据相关性特征检测潜在异常数据，得到异常运行检测信息；

[0038] 结合异常数据检测信息和异常运行检测信息构成异常检测信息。

[0039] 本方案中，所述根据所述异常检测信息进行风险评估，并进行异常事件预测和异常等级评估，具体为：

[0040] 基于大数据检索获取风险因素数据集，利用平行坐标方法将风险因素数据集映射至平行坐标中，每个数据轴特定的维度范围和类型，得到风险因素图；

[0041] 引入主成分分析法对风险因素图进行降维处理，剔除相关性小的风险因素，得到主要风险因素信息；

[0042] 根据主要风险因素信息结合专家评价法获取各主要风险因素的风险影响度，构建影响度矩阵，结合谱聚类算法进行风险因素类别划分，并根据各类型风险因素的风险影响度进行风险等级划分，得到风险因素划分信息；

[0043] 基于熵值法结合风险因素划分信息计算各风险因素的熵值，结合各风险因素的风险等级设定风险评估权重，得到风险评估权重信息；

[0044] 获取异常检测信息，基于风险评估权重信息构建风险评估模型，将所述异常检测信息输入至风险评估模型中进行风险评估，得到风险评估信息；

[0045] 所述风险评估结果信息包括数据风险评估信息、运行风险评估信息和综合风险评估信息；

[0046] 基于大数据检索获取各种异常事件的特征信息，并按照时间序列将各特征信息进行时序处理，并构建异常事件特征图谱；

[0047] 将所述异常检测信息与所述异常事件特征图谱进行相似度计算，并与预设阈值进行判断，根据判断结果确定特征节点，并选取对应的特征路径和异常事件，得到异常事件预测信息；

[0048] 根据所述异常事件特征图谱构建异常等级评估规则，划分各特征节点的节点范围设定不同的异常等级；

[0049] 通过异常等级评估规则结合所述异常事件预测信息进行异常等级评估，得到异常等级评估信息。

[0050] 本方案中，所述根据所述异常事件预测信息和异常等级评估信息进行风险预警并进行风险管控，具体为：

[0051] 基于大数据检索获取各种不同异常程度的异常事件处理实例，基于聚类算法结合

异常等级评估规则进行处理实例类型划分,得到处理实例数据集;

[0052] 基于遗传算法构建管控策略制定模型,通过处理实例数据集构建训练数据集对所述管控策略制定模型进行深度学习和训练;

[0053] 获取异常等级评估信息、异常事件预测信息和风险评估信息,构建风险预警规则,结合异常等级评估信息和风险评估信息进行风险预警判断,根据判断结果进行风险预警;

[0054] 获取数据治理信息和数据管理信息,结合异常事件预测信息进行异常溯源,分析异常数据的来源、路径和作用,得到异常溯源信息;

[0055] 将异常溯源信息、异常等级评估信息、异常事件预测信息和风险评估信息输入至所述管控策略制定模型中进行管控策略制定,得到管控策略信息,根据所述管控策略信息进行风险管控。

[0056] 本发明第二方面提供了一种基于数据分析的融合系统安全管理系统,该系统包括:存储器、处理器,所述存储器中包含基于数据分析的融合系统安全管理方法程序,所述基于数据分析的融合系统安全管理方法程序被所述处理器执行时实现如下步骤:

[0057] 获取实时传输数据,对所述实时传输数据进行数据治理,得到数据治理信息;

[0058] 根据所述数据治理信息进行属性分析和类别划分,得到数据管理信息;

[0059] 获取实时监测信息,根据所述实时监测信息进行异常检测,得到异常检测信息;

[0060] 根据所述异常检测信息进行风险评估,并进行异常事件预测和异常等级评估,得到异常事件预测信息和异常等级评估信息;

[0061] 根据所述异常事件预测信息和异常等级评估信息进行风险预警并进行风险管控。

[0062] 本发明公开了一种基于数据分析的融合系统安全管理方法及系统,包括:获取实时传输数据,对所述实时传输数据进行数据治理,得到数据治理信息;根据所述数据治理信息进行属性分析和类别划分,得到数据管理信息;获取实时监测信息,根据所述实时监测信息进行异常检测,得到异常检测信息;根据所述异常检测信息进行风险评估,并进行异常事件预测和异常等级评估,得到异常事件预测信息和异常等级评估信息;根据所述异常事件预测信息和异常等级评估信息进行风险预警并进行风险管控。提高系统整体安全性的同时,降低误报率,实现更加智能和高效的安全管理,及对网络安全的全方位监测、分析和响应。

附图说明

[0063] 为了更清楚地说明本发明实施例或示例性中的技术方案,下面将对实施例或示例性描述中所需要使用的附图作简单地介绍,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,还可以按照这些附图示出的获得其他的附图。

[0064] 图1为本发明一实施例提供的一种基于数据分析的融合系统安全管理方法流程图;

[0065] 图2为本发明一实施例提供的安全管理流程图;

[0066] 图3为本发明一实施例提供的一种基于数据分析的融合系统安全管理系统框图;

[0067] 本发明目的的实现、功能特点及优点将结合实施例,参照附图做进一步说明。

具体实施方式

[0068] 为了能够更清楚地理解本发明的上述目的、特征和优点,下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是,在不冲突的情况下,本申请的实施例及实施例中的特征可以相互组合。

[0069] 在下面的描述中阐述了很多具体细节以便于充分理解本发明,但是,本发明还可以采用其他不同于在此描述的其他方式来实施,因此,本发明的保护范围并不受下面公开的具体实施例的限制。

[0070] 图1为本发明一实施例提供的一种基于数据分析的融合系统安全管理方法流程图;

[0071] 如图1所示,本发明提供了一种基于数据分析的融合系统安全管理方法流程图,包括:

[0072] S102,获取实时传输数据,对所述实时传输数据进行数据治理,得到数据治理信息;

[0073] 建立数据治理机制,获取实时传输数据,通过数据治理机制对实时传输数据进行数据治理;

[0074] 预设数据来源识别规则,提取所述实时传输数据的来源标识符结合数据来源识别规则进行来源识别,判断是否为未知数据,得到来源识别结果信息;

[0075] 提取所述实时传输数据的行为指令特征,根据提取的行为指令特征进行行为识别,识别实时传输数据的行为请求,得到行为识别信息;

[0076] 根据所述行为识别信息和来源识别结果信息判断是否接收传输数据,若接收,则对所述实时传输数据进行预处理,将所述实时传输数据进行数据拼接、数据合并和数据修正,得到预处理信息;

[0077] 对所述预处理信息进行标准化处理,提取实时传输信息的传输权限特征,结合数据加密算法判断是否需要进行数据加密,并构建元数据目录,记录数据来源,得到数据治理信息。

[0078] 需要说明的是,在进行实时数据传输时,传输的数据包括行为请求、数据上传、数据下载等信息,通过构建数据治理机制,包括数据采集、清洗、预处理和加密等多个环节。首先,在进行数据传输时,对目标数据进行来源识别,设定来源识别规则,提取传输数据的来源标识符,通过来源标识符判断是否为正规来源,从而避免非常规信息的侵入。接着,对传输的数据进行分析,判断传输的数据的行为,如请求数据交互、请求查阅或者修改等,了解传输数据的目的。然后,根据行为识别信息和来源识别结果信息判断是否接收数据,若接收,则对目标数据进行预处理,若不接收,则将截断目标传输节点,并删除传输数据。最后,对于可接收的数据,对其进行标准化处理,并根据传输时的权限特征,判断是否需要加密,通过加密算法进行内容加密,同时,构建元数据目录,记录数据来源、时间和处理操作等,便于数据丢失或者数据异常时进行数据恢复和异常检测,确保数据的完整性、可靠性,并为后续的安全管理提供了高质量的数据基础。

[0079] S104,根据所述数据治理信息进行属性分析和类别划分,得到数据管理信息;

[0080] 获取数据治理信息,对所述数据治理信息进行特征提取,提取实时传输数据的技术特征和业务特征,得到第一特征信息;

[0081] 根据所述第一特征信息对实时传输数据进行技术属性分析,分析目标数据的数据类型、数据格式、存储特点和数据规模,得到技术属性分析信息;

[0082] 基于专家分析法获取业务属性分析要素,结合主成分分析法进行权重设定,将各业务属性分析要素按照相关性合并成主成分分析要素,计算各主成分的方差解释度,作为业务属性分析权重;

[0083] 根据业务属性分析权重结合所述第一特征信息进行业务属性分析,得到业务属性分析信息;

[0084] 结合所述技术属性分析信息和业务属性分析信息构成属性分析信息;

[0085] 预设若干类别标签,所述类别标签包括技术属性类别标签和业务属性类别标签,计算所述属性分析信息与各类别标签的马氏距离,得到马氏距离信息;

[0086] 将所述马氏距离信息与预设阈值进行判断,根据判断结果对实时传输数据进行类别划分,得到类别划分信息;

[0087] 结合属性分析信息和类别划分信息构成数据管理信息。

[0088] 需要说明的是,对于接收的数据,需要对其进行数据管理,从技术属性和业务属性来对接受的数据进行定义,技术属性包括目标数据的数据类型、数据格式、存储特点和数据规模等,业务属性包括领域、类型、指标等,比如某接受数据的业务属性为金融领域的某部门的业绩数据。首先,通过数据治理的步骤,得到了处理好的接收数据,对处理好的接收数据进行特征提取,根据提取的特征分析接收数据的技术属性。然后,采用专家分析法,获取业务属性分析要素,然后结合主成分分析法进行权重设定,将多个相关性较高的业务要素合并为少数几个主成分,并计算各主成分的方差解释度,作为业务属性分析的权重,通过设定的权重进行业务属性分析。同时,预设若干类别标签,包括技术属性类别标签和业务属性类别标签。通过计算属性分析信息与各类别标签的马氏距离,与预设阈值进行比较判断,以此对实时传输数据进行类别划分。进一步的对实时传输的数据进行详细的理解,便于进行安全管理。

[0089] S106,获取实时监测信息,根据所述实时监测信息进行异常检测,得到异常检测信息;

[0090] 获取实时监测信息,所述实时监测信息包括数据监测信息和运行监测信息;

[0091] 基于孤立森林算法构建数据异常检测模型,将数据监测信息输入至所述数据异常检测模型中进行数据异常检测;

[0092] 引入RANSAC算法,根据数据监测信息随机选取若干样本数据,通过选取的若干样本数据进行线性拟合,并根据线性拟合计算实际观测值与拟合预测值的差异,生成残差特征;

[0093] 对数据监测信息进行特征提取,结合残差特征构建新的特征矩阵,输入至所述数据异常检测模型中,根据新的特征矩阵确定孤立森林中树的总数并构建特征空间;

[0094] 构建随机二叉搜索树检测特征空间中分布低密度和孤立的数据点,定义为孤立点,计算各孤立点的在对应的树的路径长度,作为异常分数,与预设阈值进行判断,得到异常数据检测信息;

[0095] 构建数据异常管控规则,结合所述异常数据检测信息对异常数据进行修正和拦截;

[0096] 对运行监测信息进行时序化处理,构建运行异常检测模型,包括特征提取模块和异常识别模块;

[0097] 基于梯度提升决策树结合极端梯度提升算法搭建特征提取模块,对所述运行监测信息进行特征提取;

[0098] 提取时序特征和数据类型特征,并计算各特征之间的皮尔逊相关系数作为相关性特征,得到第二特征信息,并构建特征矩阵;

[0099] 将构建的特征矩阵输入至异常检测模块,检测异常数据的频率和规模,并根据相关性特征检测潜在异常数据,得到异常运行检测信息;

[0100] 结合异常数据检测信息和异常运行检测信息构成异常检测信息。

[0101] 需要说明的是,对于实时数据交换和数据传输等网络操作,需要进行实时的异常检测,包括数据层面的异常检测和运行层面的异常检测,数据异常检测包括对于数据传输质量检测和异常数据检测,运行异常检测是对于系统运行状态的异常检测,判断某部分模块出现异常运行数据。

[0102] 需要说明的是,首先,采用孤立森林算法构建数据异常检测模型,此算法适用于检测数据中的异常点,通过将数据点随机分割,构建随机二叉搜索树,然后根据路径长度来评估数据点的异常度。为了增强对数据异常的检测,引入RANSAC算法。该算法通过随机选择一小部分样本数据,进行线性拟合,计算实际观测值与拟合预测值的差异,生成残差特征,从而提供新的维度特征来检测和捕获数据中的异常。根据残差特征构建新的特征矩阵,形成更全面的特征矩阵,以提高异常检测的准确性。接着,将新特征矩阵输入至孤立森林中,确定孤立森林中树的总数并构建特征空间。通过随机二叉搜索树检测特征空间中分布低密度和孤立的数据点,定义为孤立点,计算各孤立点的在对应的树的路径长度,作为异常分数。随后,将计算得到的异常分数与预设阈值进行判断,得到异常数据检测信息。最后,构建数据异常管控规则,结合异常数据检测信息对异常数据进行修正和拦截。从而保证数据传输和储存的质量,同时避免接受异常数据。

[0103] 需要说明的是,对于运行异常检测,首先,对获取的运行监测信息进行时序化处理,将监测的信息按照时间进行排列、整合和拼接,以便能够更好的捕捉运行状态的变化。然后,构建运行异常检测模型,按照功能来设定模块,包括特征提取模块和异常识别模块,使用梯度提升决策树算法作为基础框架,引入计算梯度提升算法进行优化,从而搭建特征提取模块,加速特征提取的收敛过程,并提升特征提取的准确性和鲁棒性。通过特征提取模块对运行监测信息进行特征提取,提取时序特征和数据类型特征。时序特征涵盖了时间序列数据的模式和趋势,而数据类型特征则关注运行监测信息的种类,计算各特征之间的皮尔逊相关系数,作为相关性特征,理解特征之间的关联关系,得到第二特征信息,并构建特征矩阵输入至异常检测模块,检测异常数据的频率和规模,通过对相关性特征的分析,能够检测潜在的异常数据,从而映射潜在运行异常,提高系统的安全性和稳定性。

[0104] S108,根据所述异常检测信息进行风险评估,并进行异常事件预测和异常等级评估,得到异常事件预测信息和异常等级评估信息;

[0105] 基于大数据检索获取风险因素数据集,利用平行坐标方法将风险因素数据集映射至平行坐标中,每个数据轴特定的维度范围和类型,得到风险因素图;

[0106] 引入主成分分析法对风险因素图进行降维处理,剔除相关性小的风险因素,得到

主要风险因素信息；

[0107] 根据主要风险因素信息结合专家评价法获取各主要风险因素的风险影响度，构建影响度矩阵，结合谱聚类算法进行风险因素类别划分，并根据各类型风险因素的风险影响度进行风险等级划分，得到风险因素划分信息；

[0108] 基于熵值法结合风险因素划分信息计算各风险因素的熵值，结合各风险因素的风险等级设定风险评估权重，得到风险评估权重信息；

[0109] 获取异常检测信息，基于风险评估权重信息构建风险评估模型，将所述异常检测信息输入至风险评估模型中进行风险评估，得到风险评估信息；

[0110] 所述风险评估结果信息包括数据风险评估信息、运行风险评估信息和综合风险评估信息；

[0111] 基于大数据检索获取各种异常事件的特征信息，并按照时间序列将各特征信息进行时序处理，并构建异常事件特征图谱；

[0112] 将所述异常检测信息与所述异常事件特征图谱进行相似度计算，并与预设阈值进行判断，根据判断结果确定特征节点，并选取对应的特征路径和异常事件，得到异常事件预测信息；

[0113] 根据所述异常事件特征图谱构建异常等级评估规则，划分各特征节点的节点范围设定不同的异常等级；

[0114] 通过异常等级评估规则结合所述异常事件预测信息进行异常等级评估，得到异常等级评估信息。

[0115] 需要说明的是，首先，通过大数据检索获得风险因素数据集。随后，采用平行坐标方法，将风险因素数据集映射至平行坐标图。在平行坐标中，每个轴代表着数据的不同维度范围和类型，形成了直观清晰的风险因素图。为了简化数据结构，引入主成分分析(PCA)进行降维处理。通过PCA，剔除相关性较小的风险因素，得到主要风险因素信息。接着，基于主要风险因素信息，采用专家评价法获取各主要风险因素的风险影响度，并构建相应的影响度矩阵。结合谱聚类算法，对风险因素进行分类，并根据影响度划定不同风险等级，形成详实的风险因素划分信息。利用熵值法，计算各风险因素的熵值。综合考虑风险因素的划分信息和风险等级，设定相应的风险评估权重，得到风险评估权重信息。然后，基于先前计算的风险评估权重信息构建了风险评估模型，将异常检测信息输入至风险评估模型中进行风险评估，得到风险评估信息。随后，通过大数据检索，获取各种异常事件的特征信息，按照时间序列对这些特征信息进行处理，通过各异常事件的特征，按照时间节点构建异常事件特征图谱。通过相似度计算将异常检测信息与异常事件特征图谱进行比较，根据预设阈值进行判断，得到异常事件预测信息，通过分析当前时刻的特征与异常事件的特征的相似度，判断当前时刻的异常特征会导致的异常事件。最后，根据异常事件特征图谱构建异常等级评估规则，划分各特征节点的节点范围，为不同异常等级设定对应的标准。结合先前获得的异常事件预测信息，进行异常等级评估，评估当前异常事件的异常程度，从而为后续进行安全管理提供重要依据。

[0116] S110，根据所述异常事件预测信息和异常等级评估信息进行风险预警并进行风险管控；

[0117] 基于大数据检索获取各种不同异常程度的异常事件处理实例，基于聚类算法结合

异常等级评估规则进行处理实例类型划分,得到处理实例数据集;

[0118] 基于遗传算法构建管控策略制定模型,通过处理实例数据集构建训练数据集对所述管控策略制定模型进行深度学习和训练;

[0119] 获取异常等级评估信息、异常事件预测信息和风险评估信息,构建风险预警规则,结合异常等级评估信息和风险评估信息进行风险预警判断,根据判断结果进行风险预警;

[0120] 获取数据治理信息和数据管理信息,结合异常事件预测信息进行异常溯源,分析异常数据的来源、路径和作用,得到异常溯源信息;

[0121] 将异常溯源信息、异常等级评估信息、异常事件预测信息和风险评估信息输入至所述管控策略制定模型中进行管控策略制定,得到管控策略信息,根据所述管控策略信息进行风险管控。

[0122] 需要说明的是,首先利用大数据检索获取各种不同异常程度的异常事件处理实例。通过这些实例,获得多样的异常情境数据。接着,采用聚类算法结合异常等级评估规则,对这些处理实例进行类型划分,形成了一个包含不同异常等级的处理实例数据集。然后,基于遗传算法构建了管控策略制定模型,使用处理实例数据集构建训练数据集,并对管控策略制定模型进行深度学习和训练。接着,获取异常等级评估信息、异常事件预测信息和风险评估信息。基于这些信息,构建风险预警规则。结合异常等级评估信息和风险评估信息,对当前的异常情况进行分析和判断,通过预设的风险预警规则,对异常情况进行预警。获取数据治理信息和数据管理信息,结合异常事件预测信息,系统进行异常溯源,详细分析了异常数据的来源、路径和作用,深入理解异常事件的形成和传播过程。将异常溯源信息、异常等级评估信息、异常事件预测信息和风险评估信息输入至管控策略制定模型中,制定具体的管控策略。最后,根据制定的管控策略进行风险管控,从而能够及时、有效地应对异常情况,最大程度地减轻或防范风险的发生。

[0123] 图2为本发明一实施例提供的安全管理流程图;

[0124] 如图2所示,本发明提供了安全管理流程图,包括:

[0125] S202,获取实时监测信息,根据实时监测信息进行数据异常检测和运行异常检测;

[0126] S204,获取异常检测信息,输入至风险评估模型中进行风险评估,评估异常数据的风险程度;

[0127] S206,根据异常事件特征图谱进行异常事件预测,并结合异常等级评估规则进行异常等级评估;

[0128] S208,根据异常等级评估信息和风险评估信息结合风险预警规则进行风险预警;

[0129] S210,对异常数据进行溯源,得到异常溯源信息,结合异常等级评估信息、异常事件预测信息和风险评估信息进行管控策略制定;

[0130] S212,通过管控策略制定模型中制定管控策略,进行风险管控。

[0131] 进一步的,获取异常溯源信息,根据所述异常溯源信息判断异常事件来源;若为异常数据,则提取异常数据特征,得到异常数据特征信息;根据所述异常数据特征信息识别异常行为,判断异常数据的是传输异常还是入侵异常,得到异常来源判断信息;若异常来源判断信息为传输异常,则获取异常数据的传输节点和传输路径,对目标节点和路径进行状态评估,得到状态评估信息;根据状态评估信息进行传输能力分析,计算数据传输的丢包率、时延、误码率和传输速率,并与预设阈值进行判断,得到传输能力分析信息;预设数据隔离

区,根据所述传输能力分析信息判断异常数据所在传输节点和路径是否能够继续传输;若不能传输,则将目标数据转移至数据隔离区,进行数据暂存,并评估其他传输通道的传输状态,进行传输调控;提取数据隔离区的等待数据信息和最大容量信息,计算数据隔离区的数据转移速率和数据暂存速率,结合等待数据信息和最大容量信息预测数据隔离区的数据饱和时间,得到饱和时间预测信息;根据饱和时间预测信息进行数据暂存控制,并实时评估数据隔离区的数据量,根据数据量的变化判断是否需要对传输来源进行传输控制;若异常来源判断信息为入侵异常,则获取入侵数据的来源通道并关闭异常传输通道,并将入侵数据转移至数据隔离区;对入侵数据进行特征提取,根据提取的特征进行行为识别和入侵路径识别,得到入侵数据分析信息;根据入侵数据分析信息进行潜在危险分析,通过入侵数据的行为,判断入侵数据的入侵位置,结合其入侵路径,对入侵位置和路劲的数据和模块进行潜在异常检测,得到潜在异常检测信息;根据所述潜在异常检测信息进行风险管控,提高系统的安全性。

[0132] 图3为本发明一实施例提供的一种基于数据分析的融合系统安全管理方法系统框图3,该系统包括:存储器31、处理器32,所述存储器31中包含基于数据分析的融合系统安全管理方法方法程序,所述基于数据分析的融合系统安全管理方法方法程序被所述处理器32执行时实现如下步骤:

[0133] 获取实时传输数据,对所述实时传输数据进行数据治理,得到数据治理信息;

[0134] 根据所述数据治理信息进行属性分析和类别划分,得到数据管理信息;

[0135] 获取实时监测信息,根据所述实时监测信息进行异常检测,得到异常检测信息;

[0136] 根据所述异常检测信息进行风险评估,并进行异常事件预测和异常等级评估,得到异常事件预测信息和异常等级评估信息;

[0137] 根据所述异常事件预测信息和异常等级评估信息进行风险预警并进行风险管控。

[0138] 需要说明的是,本发明提供了一种基于数据分析的融合系统安全管理方法及系统,通过对实时传输数据进行数据治理和数据管理,识别数据的来源,判断是否为安全来源,分析数据的行为请求,判断数据的请求目的,结合来源识别和行为识别,判断是否能够接受数据,做到初步异常拦截。对于接收的数据,判断是否需要进行数据加密,保证数据安全性,并对目标数据进行预处理,保证数据的规范性。同时,对目标数据进行属性分析,分析目标数据的技术属性和业务属性,从而便于更好的理解数据的内在意义,便于进行数据管理。另一方面,提供异常检测和安全管理方法,将异常检测分为数据异常和运行异常,从两个不同的层面进行异常检测和安全管理,不仅检测数据安全和完整,还检测运行状态,判断是否出现异常运行情况,为安全管理提供了全面的异常检测,提高系统整体安全性的同时,降低误报率,实现更加智能和高效的安全管理,及对网络安全的全方位监测、分析和响应。

[0139] 在本申请所提供的几个实施例中,应该理解到,所揭露的设备和方法,可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的,例如,所述单元的划分,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,如:多个单元或组件可以结合,或可以集成到另一个系统,或一些特征可以忽略,或不执行。另外,所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口,设备或单元的间接耦合或通信连接,可以是电性的、机械的或其它形式的。

[0140] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的,作为单元显

示的部件可以是、或也可以不是物理单元;既可以位于一个地方,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全部单元来实现本实施例方案的目的。

[0141] 另外,在本发明各实施例中的各功能单元可以全部集成在一个处理单元中,也可以是各单元分别单独作为一个单元,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,也可以采用硬件加软件功能单元的形式实现。

[0142] 本领域普通技术人员可以理解:实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成,前述的程序可以存储于计算机可读取存储介质中,该程序在执行时,执行包括上述方法实施例的步骤;而前述的存储介质包括:移动存储设备、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0143] 或者,本发明上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时,也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,本发明实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机、服务器、或者网络设备等)执行本发明各个实施例所述方法的全部或部分。而前述的存储介质包括:移动存储设备、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0144] 以上所述,仅为本发明的具体实施方式,但本发明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发明揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应以所述权利要求的保护范围为准。

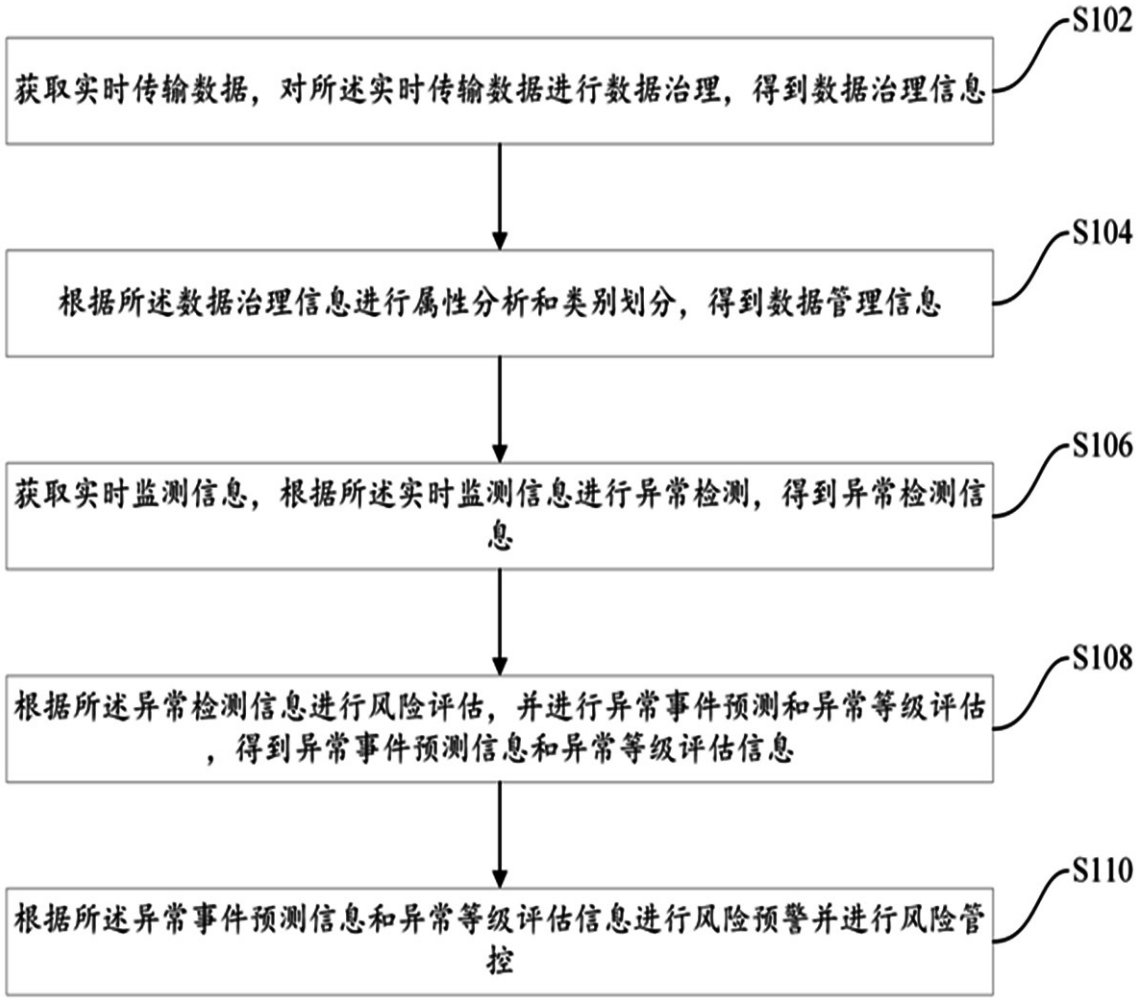

S102
获取实时传输数据，对所述实时传输数据进行数据治理，得到数据治理信息
S104
根据所述数据治理信息进行属性分析和类别划分，得到数据管理信息
S106
获取实时监测信息，根据所述实时监测信息进行异常检测，得到异常检测信息
S108
根据所述异常检测信息进行风险评估，并进行异常事件预测和异常等级评估，得到异常事件预测信息和异常等级评估信息
S110
根据所述异常事件预测信息和异常等级评估信息进行风险预警并进行风险管控

图 1

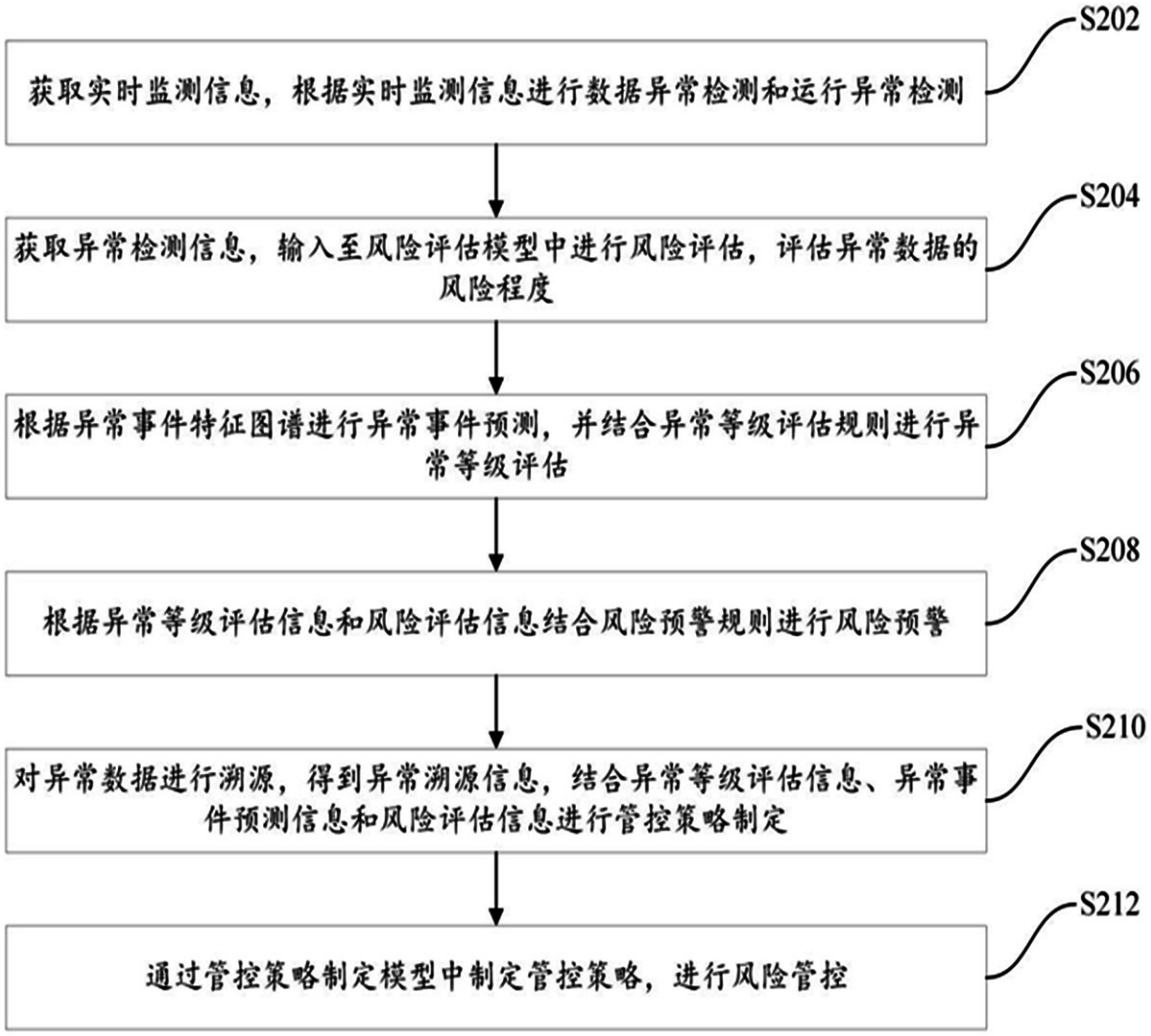

S202
获取实时监测信息，根据实时监测信息进行数据异常检测和运行异常检测
S204
获取异常检测信息，输入至风险评估模型中进行风险评估，评估异常数据的风险程度
S206
根据异常事件特征图谱进行异常事件预测，并结合异常等级评估规则进行异常等级评估
S208
根据异常等级评估信息和风险评估信息结合风险预警规则进行风险预警
S210
对异常数据进行溯源，得到异常溯源信息，结合异常等级评估信息、异常事件预测信息和风险评估信息进行管控策略制定
S212
通过管控策略制定模型中制定管控策略，进行风险管控

图 2

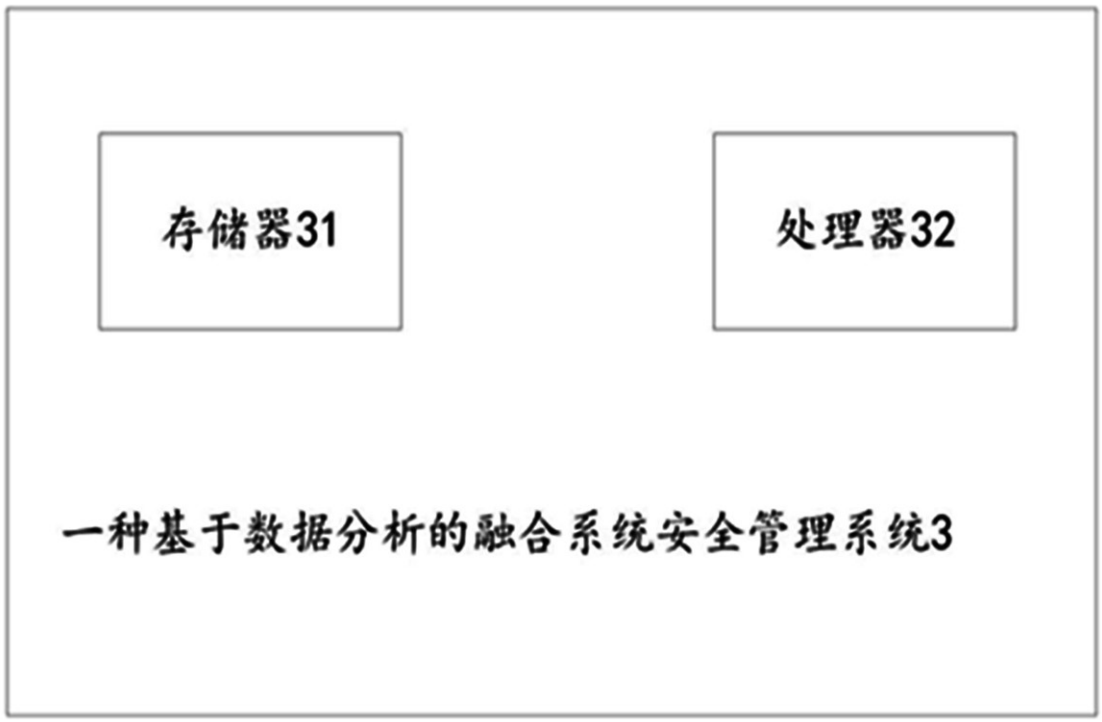


图 3