(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116599749 A
(43)申请公布日 2023.08.15

(21)申请号 202310659814.5

(22)申请日 2023.06.05

(71)申请人 白里落
地址 615000 四川省凉山彝族自治州雷波县帕哈乡八合村6组22号

(72)发明人 白里落 任飞 杨庆虎 陈笑蓉

(74)专利代理机构 成都顶峰专利事务所(普通合伙) 51224
专利代理师 曹源

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 41/14(2022.01)
H04L 41/16(2022.01)

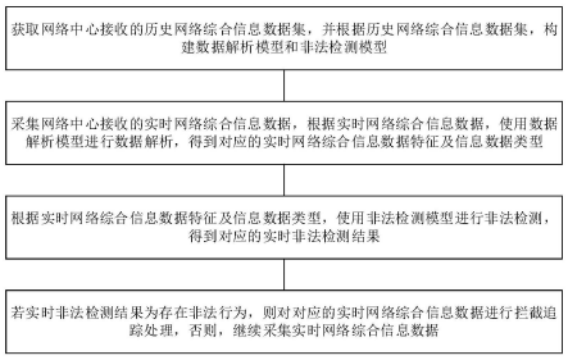
权利要求书3页 说明书8页 附图1页

(54)发明名称

一种网络综合信息监控方法、装置、设备及可读存储介质

(57)摘要

本发明属于网络信息监控技术领域。公开了一种网络综合信息监控方法、装置、设备及可读存储介质。所述的方法包括如下步骤:构建数据解析模型和非法检测模型;根据实时网络综合信息数据,使用数据解析模型进行数据解析;根据实时网络综合信息数据特征及信息数据类型,使用非法检测模型进行非法检测;若实时非法检测结果为存在非法行为,则对对应的实时网络综合信息数据进行拦截追踪处理。所述的装置包括数据获取单元、模型构建单元、数据采集单元、数据解析单元以及非法检测单元。本发明解决了现有技术存在的监测判断能力不足、检测不够准确、检测效率较低以及无法做出有针对性的防御措施的问题。



CN 116599749 A

1.一种网络综合信息监控方法,其特征在于:包括如下步骤:

获取网络中心接收的历史网络综合信息数据集,并根据历史网络综合信息数据集,构建数据解析模型和非法检测模型;

采集网络中心接收的实时网络综合信息数据,根据实时网络综合信息数据,使用数据解析模型进行数据解析,得到对应的实时网络综合信息数据特征及信息数据类型;

根据实时网络综合信息数据特征及信息数据类型,使用非法检测模型进行非法检测,得到对应的实时非法检测结果;

若实时非法检测结果为存在非法行为,则对对应的实时网络综合信息数据进行拦截追踪处理,否则,继续采集实时网络综合信息数据。

2.根据权利要求1所述的一种网络综合信息监控方法,其特征在于:所述的历史/实时网络综合信息数据的信息数据类型包括网络安全运维信息数据、网络访问轨迹信息数据以及网络流量信息数据;

所述的网络安全运维信息数据的信息数据类型包括非法行为拦截信息数据、防火墙开启关闭信息数据以及网络通道开启关闭信息数据;

所述的网络访问轨迹信息数据的信息数据类型包括访问时间信息数据、访问网站域名信息数据、访问网站IP信息数据、访问事件信息数据、访问轨迹信息数据以及访问用户信息数据;

所述的网络流量信息数据的信息数据类型包括网络流量地域时间信息数据、网络流量领域信息数据、网络流量应用信息数据、网络流量层级信息数据以及网络流量日志信息数据。

3.根据权利要求2所述的一种网络综合信息监控方法,其特征在于:获取网络中心接收的历史网络综合信息数据集,并根据历史网络综合信息数据集,构建数据解析模型和非法检测模型,包括如下步骤:

获取网络中心接收的历史网络综合信息数据集;

为历史网络综合信息数据集中每条历史网络综合信息数据分别设置对应的信息数据类型标签,得到设置信息数据类型标签后的历史网络综合信息数据集;

将设置信息数据类型标签后的历史网络综合信息数据集划分为数据解析模型训练样本数据集和数据解析模型测试样本数据集;

根据数据解析模型训练样本数据集,进行训练建模,构建初始的数据解析模型;

根据数据解析模型测试样本数据集,对初始的数据解析模型进行训练优化,若测试准确率大于阈值,则输出最优的数据解析模型,以及历史网络综合信息数据特征集及信息数据类型,否则,继续进行数据解析模型的训练优化;

为历史网络综合信息数据特征集中每条历史网络综合信息数据特征分别设置对应的非法行为标签,得到设置非法行为标签后的历史网络综合信息数据特征集;

将设置非法行为标签后的历史网络综合信息数据特征集按照信息数据类型,划分为不同信息数据类型的非法检测模型训练样本数据集和非法检测模型测试样本数据集;

根据不同信息数据类型的非法检测模型训练样本数据集,进行训练建模,构建不同信息数据类型的初始的非法检测模型;

根据不同信息数据类型的非法检测模型测试样本数据集,对对应的初始的非法检测模

型进行训练优化，若测试准确率大于阈值，则输出该信息数据类型的最优的非法检测模型，并结束模型构建，否则，继续进行该信息数据类型的非法检测模型的训练优化，直至输出所有信息数据类型的最优的非法检测模型。

4.根据权利要求3所述的一种网络综合信息监控方法，其特征在于：所述的非法检测模型包括网络安全运维信息数据非法检测模型、网络访问轨迹信息数据非法检测模型以及网络流量信息数据非法检测模型，所述的网络安全运维信息数据非法检测模型、网络访问轨迹信息数据非法检测模型以及网络流量信息数据非法检测模型的模型结构相同；

所述的历史/实时网络综合信息数据包括历史/实时网络安全运维信息数据、历史/实时网络访问轨迹信息数据以及历史/实时网络流量信息数据；

所述的历史/实时网络综合信息数据特征包括历史/实时网络安全运维信息数据特征、历史/实时网络访问轨迹信息数据特征以及历史/实时网络流量信息数据特征。

5.根据权利要求3所述的一种网络综合信息监控方法，其特征在于：根据实时网络综合信息数据特征及信息数据类型，使用非法检测模型进行非法检测，得到对应的实时非法检测结果，包括如下步骤：

根据实时网络综合信息数据特征对应的信息数据类型，匹配对应的非法检测模型；

将实时网络综合信息数据特征输入匹配的非法检测模型，进行非法检测，得到对应的实时非法检测结果。

6.根据权利要求3所述的一种网络综合信息监控方法，其特征在于：所述的数据解析模型基于DBN-Elman算法构建，且数据解析模型包括依次连接的第一输入层、基于DBN网络构建的第一特征提取模块、基于Elman神经网络构建的第一分类层以及第一输出层，所述的基于DBN网络构建的第一特征提取模块包括依次连接的若干隐含层；

所述的非法检测模型基于Dropout-BiLSTM算法构建，且非法检测模型包括依次连的第二输入层、基于Dropout-BiLSTM网络构建的第二特征提取模块、第二分类层以及第二输出层，所述的基于Dropout-BiLSTM网络构建的第二特征提取模块包括依次间隔连接的若干BiLSTM层和若干Dropout层。

7.根据权利要求4所述的一种网络综合信息监控方法，其特征在于：若实时非法检测结果为存在非法行为，则对对应的实时网络综合信息数据进行拦截追踪处理，否则，继续采集实时网络综合信息数据，包括如下步骤：

若网络安全运维信息数据非法检测模型输出的实时非法检测结果为存在非法行为，则对对应的实时网络安全运维信息数据进行防御拦截；

若网络访问轨迹信息数据非法检测模型输出的实时非法检测结果为存在非法行为，则对对应的实时网络访问轨迹信息数据进行防御拦截和数据追踪，并禁止该访问用户的下一次访问；

若网络流量信息数据非法检测模型输出的实时非法检测结果为存在非法行为，则对对应的实时网络流量信息数据进行防御拦截和流量限速；

若实时非法检测结果不存在非法行为，则继续采集实时网络综合信息数据。

8.一种网络综合信息监控装置，用于实现如权利要求1-7任一所述的网络综合信息监控方法，其特征在于：所述的装置包括数据获取单元、模型构建单元、数据采集单元、数据解析单元以及非法检测单元，所述的数据获取单元分别与模型构建单元和网络中心的数据服

务器连接，所述的模型构建单元分别与数据解析单元和非法检测单元连接，所述的数据采集单元、数据解析单元以及非法检测单元依次连接，且数据采集单元与网络中心的数据服务器连接，所述的非法检测单元与网络中心的网络安全系统连接。

9.一种网络综合信息监控设备，其特征在于：所述的设备包括存储器和处理器；

所述的存储器，用于存储网络综合信息监控程序；

所述的处理器，用于执行所述的网络综合信息监控程序，实现如权利要求1-7任一所述的网络综合信息监控方法的步骤。

10.一种计算机可读存储介质，其上存储有网络综合信息监控程序，其特征在于，所述的网络综合信息监控程序被处理器执行时，实现如权利要求1-7任一所述的网络综合信息监控方法的步骤。

一种网络综合信息监控方法、装置、设备及可读存储介质

技术领域

[0001] 本发明属于网络信息监控技术领域，具体涉及一种网络综合信息监控方法、装置、设备及可读存储介质。

背景技术

[0002] 随着互联网技术的发展，信息网络已经成为社会发展的重要保证，有很多是敏感信息，所以难免会吸引来自世界各地的各种人为攻击，例如信息泄露、信息窃取、数据篡改、密码破解、木马病毒等，网络中心作为网络信息的传输终端或中继点，在每时每刻都面临着海量的网络信息接收与传输，为了防止恶意网络访问给网络中心的数据带来的破坏、更改和泄露，保证网络中心安全可靠的运行，需要对网络访问的网络信息进行非法检测和行为管理。

[0003] 现有的网络信息监控方法大多借助入侵检测技术、网络行为审计技术、异常流量分析技术以及病毒检测技术等实现对网络访问流量数据的监控，而实际情况下网络传输通道中不仅仅包括网络访问流量数据，还包括网络安全运维信息数据和网络访问轨迹信息数据，非法攻击数据可以通过模拟网络中心或网络安全运维人员发送的网络安全运维信息数据等躲过监控，导致网络中心受到非法攻击发生重大数据安全事故，因此，现有技术存在对用户网络访问和相关行为的监测判断能力不足，对网络信息安全状态的检测不够准确，并且检测效率较低，无法确保网络信息安全系统做出有针对性的防御措施的问题。

发明内容

[0004] 为了解决现有技术存在的监测判断能力不足、检测不够准确、检测效率较低以及无法做出有针对性的防御措施的问题，本发明目的在于提供一种网络综合信息监控方法、装置、设备及可读存储介质。

[0005] 本发明所采用的技术方案为：

[0006] 一种网络综合信息监控方法，包括如下步骤：

[0007] 获取网络中心接收的历史网络综合信息数据集，并根据历史网络综合信息数据集，构建数据解析模型和非法检测模型；

[0008] 采集网络中心接收的实时网络综合信息数据，根据实时网络综合信息数据，使用数据解析模型进行数据解析，得到对应的实时网络综合信息数据特征及信息数据类型；

[0009] 根据实时网络综合信息数据特征及信息数据类型，使用非法检测模型进行非法检测，得到对应的实时非法检测结果；

[0010] 若实时非法检测结果为存在非法行为，则对对应的实时网络综合信息数据进行拦截追踪处理，否则，继续采集实时网络综合信息数据。

[0011] 进一步地，历史/实时网络综合信息数据的信息数据类型包括网络安全运维信息数据、网络访问轨迹信息数据以及网络流量信息数据；

[0012] 网络安全运维信息数据的信息数据类型包括非法行为拦截信息数据、防火墙开启

关闭信息数据以及网络通道开启关闭信息数据；

[0013] 网络访问轨迹信息数据的信息数据类型包括访问时间信息数据、访问网站域名信息数据、访问网站IP信息数据、访问事件信息数据、访问轨迹信息数据以及访问用户信息数据；

[0014] 网络流量信息数据的信息数据类型包括网络流量地域时间信息数据、网络流量领域信息数据、网络流量应用信息数据、网络流量层级信息数据以及网络流量日志信息数据。

[0015] 进一步地，获取网络中心接收的历史网络综合信息数据集，并根据历史网络综合信息数据集，构建数据解析模型和非法检测模型，包括如下步骤：

[0016] 获取网络中心接收的历史网络综合信息数据集；

[0017] 为历史网络综合信息数据集中每条历史网络综合信息数据分别设置对应的信息数据类型标签，得到设置信息数据类型标签后的历史网络综合信息数据集；

[0018] 将设置信息数据类型标签后的历史网络综合信息数据集划分为数据解析模型训练样本数据集和数据解析模型测试样本数据集；

[0019] 根据数据解析模型训练样本数据集，进行训练建模，构建初始的数据解析模型；

[0020] 根据数据解析模型测试样本数据集，对初始的数据解析模型进行训练优化，若测试准确率大于阈值，则输出最优的数据解析模型，以及历史网络综合信息数据特征集及信息数据类型，否则，继续进行数据解析模型的训练优化；

[0021] 为历史网络综合信息数据特征集中每条历史网络综合信息数据特征分别设置对应的非法行为标签，得到设置非法行为标签后的历史网络综合信息数据特征集；

[0022] 将设置非法行为标签后的历史网络综合信息数据特征集按照信息数据类型，划分为不同信息数据类型的非法检测模型训练样本数据集和非法检测模型测试样本数据集；

[0023] 根据不同信息数据类型的非法检测模型训练样本数据集，进行训练建模，构建不同信息数据类型的初始的非法检测模型；

[0024] 根据不同信息数据类型的非法检测模型测试样本数据集，对对应的初始的非法检测模型进行训练优化，若测试准确率大于阈值，则输出该信息数据类型的最优的非法检测模型，并结束模型构建，否则，继续进行该信息数据类型的非法检测模型的训练优化，直至输出所有信息数据类型的最优的非法检测模型。

[0025] 进一步地，非法检测模型包括网络安全运维信息数据非法检测模型、网络访问轨迹信息数据非法检测模型以及网络流量信息数据非法检测模型，网络安全运维信息数据非法检测模型、网络访问轨迹信息数据非法检测模型以及网络流量信息数据非法检测模型的模型结构相同；

[0026] 历史/实时网络综合信息数据包括历史/实时网络安全运维信息数据、历史/实时网络访问轨迹信息数据以及历史/实时网络流量信息数据；

[0027] 历史/实时网络综合信息数据特征包括历史/实时网络安全运维信息数据特征、历史/实时网络访问轨迹信息数据特征以及历史/实时网络流量信息数据特征。

[0028] 进一步地，根据实时网络综合信息数据特征及信息数据类型，使用非法检测模型进行非法检测，得到对应的实时非法检测结果，包括如下步骤：

[0029] 根据实时网络综合信息数据特征对应的信息数据类型，匹配对应的非法检测模型；

[0030] 将实时网络综合信息数据特征输入匹配的非法检测模型，进行非法检测，得到对应的实时非法检测结果。

[0031] 进一步地，数据解析模型基于DBN-Elman算法构建，且数据解析模型包括依次连接的第一输入层、基于DBN网络构建的第一特征提取模块、基于Elman神经网络构建的第一分类层以及第一输出层，基于DBN网络构建的第一特征提取模块包括依次连接的若干隐含层；

[0032] 非法检测模型基于Dropout-BiLSTM算法构建，且非法检测模型包括依次连的第二输入层、基于Dropout-BiLSTM网络构建的第二特征提取模块、第二分类层以及第二输出层，基于Dropout-BiLSTM网络构建的第二特征提取模块包括依次间隔连接的若干BiLSTM层和若干Dropout层。

[0033] 进一步地，若实时非法检测结果为存在非法行为，则对对应的实时网络综合信息数据进行拦截追踪处理，否则，继续采集实时网络综合信息数据，包括如下步骤：

[0034] 若网络安全运维信息数据非法检测模型输出的实时非法检测结果为存在非法行为，则对对应的实时网络安全运维信息数据进行防御拦截；

[0035] 若网络访问轨迹信息数据非法检测模型输出的实时非法检测结果为存在非法行为，则对对应的实时网络访问轨迹信息数据进行防御拦截和数据追踪，并禁止该访问用户的下一次访问；

[0036] 若网络流量信息数据非法检测模型输出的实时非法检测结果为存在非法行为，则对对应的实时网络流量信息数据进行防御拦截和流量限速；

[0037] 若实时非法检测结果不存在非法行为，则继续采集实时网络综合信息数据。

[0038] 一种网络综合信息监控装置，用于实现网络综合信息监控方法，装置包括数据获取单元、模型构建单元、数据采集单元、数据解析单元以及非法检测单元，数据获取单元分别与模型构建单元和网络中心的数据服务器连接，模型构建单元分别与数据解析单元和非法检测单元连接，数据采集单元、数据解析单元以及非法检测单元依次连接，且数据采集单元与网络中心的数据服务器连接，非法检测单元与网络中心的网络安全系统连接。

[0039] 一种网络综合信息监控设备，设备包括存储器和处理器；

[0040] 存储器，用于存储网络综合信息监控程序；

[0041] 处理器，用于执行网络综合信息监控程序，实现网络综合信息监控方法的步骤。

[0042] 一种计算机可读存储介质，其上存储有网络综合信息监控程序，网络综合信息监控程序被处理器执行时，实现网络综合信息监控方法的步骤。

[0043] 本发明的有益效果为：

[0044] 本发明提供的一种网络综合信息监控方法、装置、设备及可读存储介质，综合考虑网络传输通道中存在的网络综合信息数据，对网络中心进行网络综合信息监控，避免了非法攻击数据模拟合法数据躲过监控的问题，提高了网络中心的数据安全性，并且采用人工智能技术，通过大量的历史网络综合信息数据构建数据解析模型和非法检测模型，实现了数据解析和非法检测的自动化监控，提高了监测判断能力、检测准确性以及检测效率，最后根据实时非法检测结果对访问网络中心的含有非法攻击数据的实时网络综合信息数据进行拦截追踪处理，在数据源头上进行设防，有效的减少网络中心被木马文件、异常登录、密码破解行为恶意破坏，造成不必要的经济损失。

[0045] 本发明的其他有益效果将在具体实施方式中进一步进行说明。

附图说明

[0046] 图1是本发明中网络综合信息监控方法的流程框图。

[0047] 图2是本发明中网络综合信息监控装置的结构框图。

具体实施方式

[0048] 下面结合附图及具体实施例对本发明做进一步阐释。

[0049] 实施例1：

[0050] 如图1所示，本实施例提供一种网络综合信息监控方法，包括如下步骤：

[0051] 获取网络中心接收的历史网络综合信息数据集；

[0052] 历史网络综合信息数据的信息数据类型包括网络安全运维信息数据、网络访问轨迹信息数据以及网络流量信息数据；

[0053] 网络安全运维信息数据的信息数据类型包括非法行为拦截信息数据、防火墙开启关闭信息数据以及网络通道开启关闭信息数据；

[0054] 网络访问轨迹信息数据的信息数据类型包括访问时间信息数据、访问网站域名信息数据、访问网站IP信息数据、访问事件信息数据、访问轨迹信息数据以及访问用户信息数据；

[0055] 网络流量信息数据的信息数据类型包括网络流量地域时间信息数据、网络流量领域信息数据、网络流量应用信息数据、网络流量层级信息数据以及网络流量日志信息数据；

[0056] 根据历史网络综合信息数据集，构建数据解析模型和非法检测模型，包括如下步骤：

[0057] 对历史网络综合信息数据集进行数据预处理，包括数据清洗、数据筛选以及归一化处理，得到预处理后的历史网络综合信息数据集；

[0058] 为预处理后的历史网络综合信息数据集中每条预处理后的历史网络综合信息数据分别设置对应的信息数据类型标签，得到设置信息数据类型标签后的历史网络综合信息数据集；

[0059] 历史网络综合信息数据包括历史网络安全运维信息数据、历史网络访问轨迹信息数据以及历史网络流量信息数据；

[0060] 将设置信息数据类型标签后的历史网络综合信息数据集划分为数据解析模型训练样本数据集和数据解析模型测试样本数据集；

[0061] 根据数据解析模型训练样本数据集，进行训练建模，构建初始的数据解析模型；

[0062] 根据数据解析模型测试样本数据集，对初始的数据解析模型进行训练优化，若测试准确率大于阈值，则输出最优的数据解析模型，以及历史网络综合信息数据特征集及信息数据类型，否则，继续进行数据解析模型的训练优化；

[0063] 数据解析模型基于DBN-Elman算法构建，且数据解析模型包括依次连接的第一输入层、基于深度信念(Deep Belief Nets,DBN)网络构建的第一特征提取模块、基于Elman神经网络构建的第一分类层以及第一输出层，基于DBN网络构建的第一特征提取模块包括依次连接的若干隐含层；

[0064] DBN网络是一种使用多个隐含层对数据特征进行提取的深度学习算法，能够学习数据的深层特征，提高了数据学习的效率和数据特征提取的有效性，并且通过分类器进行

分类，本实施例采用预先训练好的Elman神经网络作为分类器，提高了分类的准确性和效率，Elman神经网络是一种典型的局部回归网络，可以看作是一个具有局部记忆单元，能够通过预训练实现对信息数据类型的分类工作；

[0065] 第一输入层，用于接收输入数据解析模型的历史/实时网络综合信息数据，并将历史/实时网络综合信息数据传输至第一特征提取模块；

[0066] 第一特征提取模块，用于接收第一输入层传输的历史/实时网络综合信息数据，根据历史/实时网络综合信息数据，提取对应的历史/实时网络综合信息数据特征，并将历史/实时网络综合信息数据特征传输至第一分类层；

[0067] 第一分类层，用于接收第一特征提取模块传输的历史/实时网络综合信息数据特征，根据历史/实时网络综合信息数据特征进行分类，得到对应的信息数据类型，并将历史/实时网络综合信息数据特征及信息数据类型传输至第一输出层；

[0068] 第一输出层，用于接收第一分类层传输的历史/实时网络综合信息数据特征及信息数据类型，并将历史/实时网络综合信息数据特征及信息数据类型进行输出；

[0069] 为历史网络综合信息数据特征集中每条历史网络综合信息数据特征分别设置对应的非法行为标签，得到设置非法行为标签后的历史网络综合信息数据特征集；

[0070] 历史网络综合信息数据特征包括历史网络安全运维信息数据特征、历史网络访问轨迹信息数据特征以及历史网络流量信息数据特征；

[0071] 将设置非法行为标签后的历史网络综合信息数据特征集按照信息数据类型，划分为不同信息数据类型的非法检测模型训练样本数据集和非法检测模型测试样本数据集；

[0072] 根据不同信息数据类型的非法检测模型训练样本数据集，进行训练建模，构建不同信息数据类型的初始的非法检测模型；

[0073] 根据不同信息数据类型的非法检测模型测试样本数据集，对对应的初始的非法检测模型进行训练优化，若测试准确率大于阈值，则输出该信息数据类型的最优的非法检测模型，并结束模型构建，否则，继续进行该信息数据类型的非法检测模型的训练优化，直至输出所有信息数据类型的最优的非法检测模型；

[0074] 非法检测模型基于设置有Dropout机制的双向长短期记忆网络(Bidirectional Long Short-Term Memory Network，BiLSTM)算法构建，且非法检测模型包括依次连的第二输入层、基于Dropout-BiLSTM网络构建的第二特征提取模块、第二分类层以及第二输出层，基于Dropout-BiLSTM网络构建的第二特征提取模块包括依次间隔连接的若干BiLSTM层和若干Dropout层；

[0075] BiLSTM层由前向LSTM和后向LSTM构成，能够更好的捕捉双向的语义依赖，对历史/实时网络综合信息数据特征进行针对性的特征提取，获取其中包含的非法行为的历史/实时非法行为数据特征，Dropout层作为使用Dropout机制的结构，能够在训练途中，随机丢弃不必要的神经元结构，提高模型的训练和预测效率，减少计算机资源占用；

[0076] 第二输入层，用于接收输入非法检测模型的历史/实时网络综合信息数据特征，并将历史/实时网络综合信息数据特征传输至第二特征提取模块；

[0077] 第二特征提取模块，用于接收第二输入层传输的历史/实时网络综合信息数据特征，根据历史/实时网络综合信息数据特征，提取对应的历史/实时非法行为数据特征，并将历史/实时非法行为数据特征传输至第二分类层；

[0078] 第二分类层，用于接收第二特征提取模块传输的历史/实时非法行为数据特征，根据历史/实时非法行为数据特征进行分类，得到对应的历史/实时非法行为标签，并将历史/实时非法行为标签传输至第二输出层；

[0079] 第二输出层，用于接收第二分类层传输的历史/实时非法行为标签，并将历史/实时非法行为标签作为对应的历史/实时非法检测结果进行输出；

[0080] 非法检测模型包括网络安全运维信息数据非法检测模型、网络访问轨迹信息数据非法检测模型以及网络流量信息数据非法检测模型，网络安全运维信息数据非法检测模型、网络访问轨迹信息数据非法检测模型以及网络流量信息数据非法检测模型的模型结构相同；

[0081] 采集网络中心接收的实时网络综合信息数据，并对实时网络综合信息数据进行数据预处理，包括数据清洗、数据筛选以及归一化处理，得到预处理后的实时网络综合信息数据；

[0082] 根据预处理后的实时网络综合信息数据，使用数据解析模型进行数据解析，得到对应的实时网络综合信息数据特征及信息数据类型；

[0083] 实时网络综合信息数据的信息数据类型包括网络安全运维信息数据、网络访问轨迹信息数据以及网络流量信息数据；

[0084] 实时网络综合信息数据包括实时网络安全运维信息数据、实时网络访问轨迹信息数据以及实时网络流量信息数据；

[0085] 实时网络综合信息数据特征包括实时网络安全运维信息数据特征、实时网络访问轨迹信息数据特征以及实时网络流量信息数据特征；

[0086] 根据实时网络综合信息数据特征及信息数据类型，使用非法检测模型进行非法检测，得到对应的实时非法检测结果，包括如下步骤：

[0087] 根据实时网络综合信息数据特征对应的信息数据类型，匹配对应的非法检测模型；

[0088] 将实时网络综合信息数据特征输入匹配的非法检测模型，进行非法检测，得到对应的实时非法检测结果；

[0089] 若实时非法检测结果为存在非法行为，则对对应的实时网络综合信息数据进行拦截追踪处理，否则，继续采集实时网络综合信息数据，包括如下步骤：

[0090] 若网络安全运维信息数据非法检测模型输出的实时非法检测结果为存在非法行为，则对对应的实时网络安全运维信息数据进行防御拦截；网络安全运维信息数据存在非法行为，则说明非法攻击数据伪装成网络安全运维相关数据，对于这种方式的攻击，数据追踪困难，只需要进行防御拦截；

[0091] 若网络访问轨迹信息数据非法检测模型输出的实时非法检测结果为存在非法行为，则对对应的实时网络访问轨迹信息数据进行防御拦截和数据追踪，并禁止该访问用户的下一次访问；

[0092] 网络访问轨迹信息数据存在非法行为，可能是非法用户的非法访问行为或合法用户的非法网站访问，需要进行数据追踪并进行网站或用户的访问拦截；

[0093] 若网络流量信息数据非法检测模型输出的实时非法检测结果为存在非法行为，则对对应的实时网络流量信息数据进行防御拦截和流量限速；

[0094] 网络流量信息数据存在非法行为，可能是非法流量攻击，需要进行防御拦截和流量限速，避免网络中心的访问流量超限；

[0095] 若实时非法检测结果不存在非法行为，则继续采集实时网络综合信息数据。

[0096] 实施例2：

[0097] 如图2所示，本实施例提供一种网络综合信息监控装置，用于实现网络综合信息监控方法，装置包括数据获取单元、模型构建单元、数据采集单元、数据解析单元以及非法检测单元，数据获取单元分别与模型构建单元和网络中心的数据服务器连接，模型构建单元分别与数据解析单元和非法检测单元连接，数据采集单元、数据解析单元以及非法检测单元依次连接，且数据采集单元与网络中心的数据服务器连接，非法检测单元与网络中心的网络安全系统连接；

[0098] 数据获取单元，用于获取数据服务器存储的网络中心接收的历史网络综合信息数据集，并将历史网络综合信息数据集传输至模型构建单元；

[0099] 模型构建单元，用于接收数据获取单元传输的历史网络综合信息数据集，根据历史网络综合信息数据集，构建数据解析模型和非法检测模型；将数据解析模型传输至数据解析单元，并将非法检测模型传输至非法检测单元；

[0100] 数据采集单元，用于采集数据服务器存储的网络中心接收的实时网络综合信息数据，并将实时网络综合信息数据传输至数据解析单元；

[0101] 数据解析单元，用于接收模型构建单元传输的数据解析模型，和数据采集单元传输的实时网络综合信息数据；根据实时网络综合信息数据，使用数据解析模型进行数据解析，得到对应的实时网络综合信息数据特征及信息数据类型；将实时网络综合信息数据特征及信息数据类型传输至非法检测单元；

[0102] 非法检测单元，用于接收模型构建单元传输的非法检测模型，和数据解析单元传输的实时网络综合信息数据特征及信息数据类型；根据实时网络综合信息数据特征及信息数据类型，使用非法检测模型进行非法检测，得到对应的实时非法检测结果；若实时非法检测结果为存在非法行为，则生成对应的非法行为报告并发送至网络中心的网络安全系统，网络安全系统根据非法检测单元发送的非法行为报告，对对应的实时网络综合信息数据进行拦截追踪处理。

[0103] 实施例3：

[0104] 本实施例提供一种网络综合信息监控设备，设备包括存储器和处理器；

[0105] 存储器，用于存储网络综合信息监控程序；

[0106] 处理器，用于执行网络综合信息监控程序，实现网络综合信息监控方法的步骤。

[0107] 实施例4：

[0108] 本实施例提供一种计算机可读存储介质，其上存储有网络综合信息监控程序，网络综合信息监控程序被处理器执行时，实现网络综合信息监控方法的步骤。

[0109] 本发明提供的一种网络综合信息监控方法、装置、设备及可读存储介质，综合考虑网络传输通道中存在的网络综合信息数据，对网络中心进行网络综合信息监控，避免了非法攻击数据模拟合法数据躲过监控的问题，提高了网络中心的数据安全性，并且采用人工智能技术，通过大量的历史网络综合信息数据构建数据解析模型和非法检测模型，实现了数据解析和非法检测的自动化监控，提高了监测判断能力、检测准确性以及检测效率，最后

根据实时非法检测结果对访问网络中心的含有非法攻击数据的实时网络综合信息数据进行拦截追踪处理，在数据源头上进行设防，有效的减少网络中心被木马文件、异常登录、密码破解行为恶意破坏，造成不必要的经济损失。

[0110] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明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(如ROM/RAM)中，包括若干指令用以使得一台终端(可以是手机，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的方法。

[0111] 本发明不局限于上述可选的实施方式，任何人在本发明的启示下都可得出其他各种形式的产品。上述具体实施方式不应理解成对本发明的保护范围的限制，本发明的保护范围应当以权利要求书中界定的为准，并且说明书可以用于解释权利要求书。

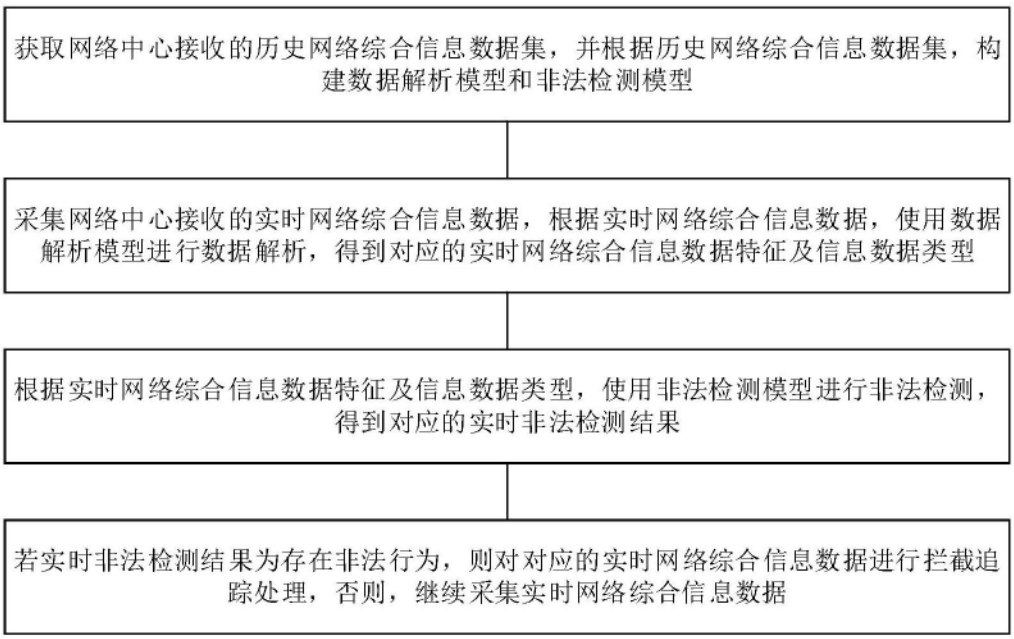

获取网络中心接收的历史网络综合信息数据集，并根据历史网络综合信息数据集，构建数据解析模型和非法检测模型
采集网络中心接收的实时网络综合信息数据，根据实时网络综合信息数据，使用数据解析模型进行数据解析，得到对应的实时网络综合信息数据特征及信息数据类型
根据实时网络综合信息数据特征及信息数据类型，使用非法检测模型进行非法检测，得到对应的实时非法检测结果
若实时非法检测结果为存在非法行为，则对对应的实时网络综合信息数据进行拦截追踪处理，否则，继续采集实时网络综合信息数据

图1

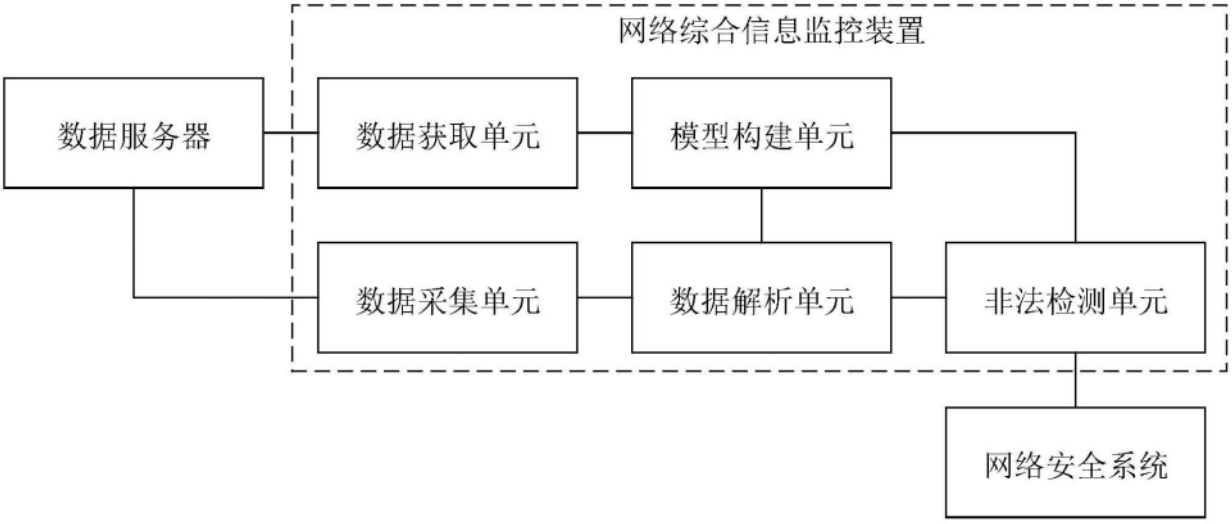

网络综合信息监控装置
数据服务器
数据获取单元
模型构建单元
数据采集单元
数据解析单元
非法检测单元
网络安全系统

图2