(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108881265 A
(43)申请公布日 2018.11.23

(21)申请号 201810714155.X

(22)申请日 2018.06.29

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)

(72)发明人 蒋劭捷 张鑫

(74)专利代理机构 北京华沛德权律师事务所 11302
代理人 房德权

(51)Int.Cl.
H04L 29/06(2006.01)

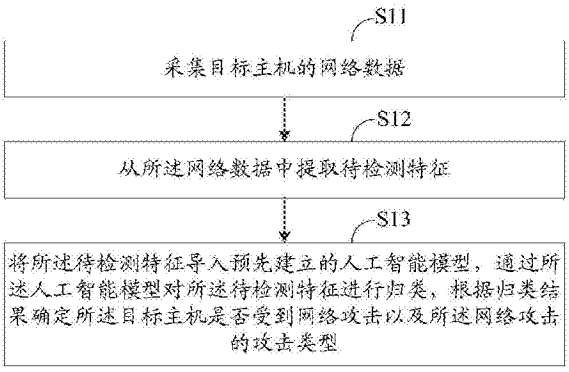
权利要求书2页 说明书22页 附图4页

(54)发明名称

一种基于人工智能的网络攻击检测方法及系统

(57)摘要

本发明公开了一种基于人工智能的网络攻击检测方法及系统，所述基于人工智能的网络攻击检测方法包括：采集目标主机的网络数据；从所述网络数据中提取待检测特征；将所述待检测特征导入预先建立的人工智能模型，通过所述人工智能模型对所述待检测特征进行归类，根据归类结果确定所述目标主机是否受到网络攻击以及所述网络攻击的攻击类型。本发明提供的基于人工智能的网络攻击检测方法及系统，利用人工智能技术进行网络攻击行为的检测，极大地避免了攻击者进行绕过而检测不到的情况，从而能够发现更多的网络攻击。



CN 108881265 A

1.一种基于人工智能的网络攻击检测方法，其特征在于，包括：

采集目标主机的网络数据；

从所述网络数据中提取待检测特征；

将所述待检测特征导入预先建立的人工智能模型，通过所述人工智能模型对所述待检测特征进行归类，根据归类结果确定所述目标主机是否受到网络攻击以及所述网络攻击的攻击类型。

2.根据权利要求1所述的一种基于人工智能的网络攻击检测方法，其特征在于，所述从所述网络数据中提取待检测特征包括：

从所述网络数据中提取请求数据，其中，所述请求数据用于向所述目标主机发起请求服务；

从所述请求数据中提取所述待检测特征。

3.根据权利要求1所述的一种基于人工智能的网络攻击检测方法，其特征在于，在所述将所述待检测特征导入预先建立的人工智能模型之前，还包括：

建立所述人工智能模型。

4.根据权利要求3所述的一种基于人工智能的网络攻击检测方法，其特征在于，所述建立所述人工智能模型包括：

收集模型训练数据；

从所述模型训练数据中提取已知网络攻击的特征，获得攻击特征数据；

对所述攻击特征数据进行分类，获得训练样本；

根据所述训练样本进行模型训练，获得所述人工智能模型。

5.根据权利要求4所述的一种基于人工智能的网络攻击检测方法，其特征在于，所述收集模型训练数据包括：

收集互联网已公开的攻击数据、互联网已公开的漏洞数据、所述目标主机已采集的攻击数据以及所述目标主机已采集的漏洞数据中的一种或多种组合。

6.根据权利要求4所述的一种基于人工智能的网络攻击检测方法，其特征在于，所述根据所述训练样本进行模型训练包括：

根据所述训练样本，采用朴素贝叶斯算法进行模型训练。

7.根据权利要求1至6任一项所述的一种基于人工智能的网络攻击检测方法，其特征在于，在根据归类结果确定所述目标主机受到所述网络攻击以及所述网络攻击的攻击类型之后，还包括：

检测所述网络攻击是否成功；

若所述网络攻击成功，则获得成功的网络攻击的攻击动作。

8.一种基于人工智能的网络攻击检测系统，其特征在于，包括：

采集模块，用于采集目标主机的网络数据；

第一提取模块，用于从所述网络数据中提取待检测特征；

导入模块，用于将所述待检测特征导入预先建立的人工智能模型，通过所述人工智能模型对所述待检测特征进行归类，根据归类结果确定所述目标主机是否受到网络攻击以及所述网络攻击的攻击类型。

9.一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，该程序被处理器执

行时实现权利要求1至7任一项所述的一种基于人工智能的网络攻击检测方法。

10.一种计算机设备，包括存储器、处理器及存储在存储器上并可在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程序时实现权利要求1至7任一项所述的一种基于人工智能的网络攻击检测方法。

一种基于人工智能的网络攻击检测方法及系统

技术领域

[0001] 本发明涉及网络安全技术领域，具体涉及一种基于人工智能的网络攻击检测方法及系统。

背景技术

[0002] 随着计算机技术的不断发展和互联网的不断普及，网络攻击形式层出不穷，网络安全问题日益突出，造成的社会影响和经济损失越来越大，对网络威胁检测与防御提出了新的需求和挑战。网络流量异常是目前主要的网络安全威胁之一，也是网络安全监测的关键对象。快速、准确地发现网络异常流量，对恶意代码及时准确捕获、分析、跟踪与监测，可以为网络安全态势指标评估和免疫决策提供知识支撑，从而提高网络安全应急组织的整体响应能力。

[0003] 传统的网络攻击检测方法主要是通过对已知网络攻击的特征做出确定性的描述，形成相应的规则并汇总成一个特征库，然后将采集的网络数据与特征库中的规则进行一一比对。如果在一一比对的过程中，采集的网络数据与特征库中的规则相匹配，那么就表明这是一个入侵行为。传统的网络攻击检测方法能准确检测已知的网络攻击，但该方法依赖于规则的编写，因而灵活性差、漏报率高。

发明内容

[0004] 本发明所要解决的是传统的网络攻击检测方法灵活性差、漏报率高的问题。

[0005] 本发明通过下述技术方案实现：

[0006] 一种基于人工智能的网络攻击检测方法，包括：

[0007] 采集目标主机的网络数据；

[0008] 从所述网络数据中提取待检测特征；

[0009] 将所述待检测特征导入预先建立的人工智能模型，通过所述人工智能模型对所述待检测特征进行归类，根据归类结果确定所述目标主机是否受到网络攻击以及所述网络攻击的攻击类型。

[0010] 可选的，所述从所述网络数据中提取待检测特征包括：

[0011] 从所述网络数据中提取请求数据，其中，所述请求数据用于向所述目标主机发起请求服务；

[0012] 从所述请求数据中提取所述待检测特征。

[0013] 可选的，在所述将所述待检测特征导入预先建立的人工智能模型之前，还包括：

[0014] 建立所述人工智能模型。

[0015] 可选的，所述建立所述人工智能模型包括：

[0016] 收集模型训练数据；

[0017] 从所述模型训练数据中提取已知网络攻击的特征，获得攻击特征数据；

[0018] 对所述攻击特征数据进行分类，获得训练样本；

[0019] 根据所述训练样本进行模型训练，获得所述人工智能模型。

[0020] 可选的，所述收集模型训练数据包括：

[0021] 收集互联网已公开的攻击数据、互联网已公开的漏洞数据、所述目标主机已采集的攻击数据以及所述目标主机已采集的漏洞数据中的一种或多种组合。

[0022] 可选的，所述根据所述训练样本进行模型训练包括：

[0023] 根据所述训练样本，采用朴素贝叶斯算法进行模型训练。

[0024] 可选的，在根据归类结果确定所述目标主机受到所述网络攻击以及所述网络攻击的攻击类型之后，还包括：

[0025] 检测所述网络攻击是否成功；

[0026] 若所述网络攻击成功，则获得成功的网络攻击的攻击动作。

[0027] 可选的，所述检测所述网络攻击是否成功包括：

[0028] 从所述网络数据中提取待比对特征；

[0029] 将所述待比对特征与预先建立的特征库中的一个以上攻击响应规则进行一一比对，其中，所述攻击响应规则根据第一响应数据形成，所述第一响应数据用于受攻击主机对成功攻击请求的应答；

[0030] 若所述待比对特征与所述攻击响应规则相匹配，则判定所述网络攻击成功。

[0031] 可选的，所述从所述网络数据中提取待比对特征包括：

[0032] 从所述网络数据中提取第二响应数据，其中，所述第二响应数据用于所述目标主机应答请求服务；

[0033] 从所述第二响应数据中提取所述待比对特征。

[0034] 可选的，所述从所述网络数据中提取待比对特征包括：

[0035] 从所述网络数据中提取请求数据和第二响应数据，其中，所述请求数据用于向所述目标主机发起请求服务，所述第二响应数据用于所述目标主机应答请求服务；

[0036] 从所述请求数据和所述第二响应数据中提取所述待比对特征。

[0037] 可选的，在所述将所述待比对特征与预先建立的特征库中的一个以上攻击响应规则进行一一比对之前，还包括：

[0038] 建立所述特征库。

[0039] 可选的，所述建立所述特征库包括：

[0040] 创建数据库；

[0041] 从一个以上第一响应数据中对应提取一个以上攻击响应特征；

[0042] 对每个攻击响应特征进行确定性描述，形成一个以上攻击响应规则；

[0043] 将所述一个以上攻击响应规则存储到所述数据库中，获得所述特征库。

[0044] 可选的，所述特征库包括N个子特征库，N为不小于2的整数，所述建立所述特征库包括：

[0045] 创建N个数据库；

[0046] 从两个以上第一响应数据中对应提取两个以上攻击响应特征；

[0047] 对每个攻击响应特征进行确定性描述，形成两个以上攻击响应规则；

[0048] 将所述两个以上攻击响应规则中属于同种攻击类型的攻击响应规则存储到相同的数据库中，获得所述子特征库。

[0049] 可选的，所述将所述待比对特征与预先建立的特征库中的一个以上攻击响应规则进行一一比对包括：

[0050] 将所述待比对特征与和所述网络攻击的攻击类型对应的子特征库中一个以上攻击响应规则进行一一比对。

[0051] 可选的，所述对每个攻击响应特征进行确定性描述包括：

[0052] 采用正则表达式对每个攻击响应特征进行确定性描述。

[0053] 可选的，所述获得成功的网络攻击的攻击动作包括：

[0054] 建立特征库中每个所述攻击响应规则与攻击动作之间的关联关系；

[0055] 根据特征库中每个所述攻击响应规则与攻击动作之间的关联关系，将与所述待比对特征匹配的攻击响应规则所对应的攻击动作，确定为所述成功的网络攻击的攻击动作。

[0056] 可选的，在所述检测所述网络攻击是否成功之后，还包括：

[0057] 生成告警信息，其中，所述告警信息包括所述网络攻击的攻击类型、所述网络攻击是否成功以及成功的网络攻击的攻击动作。

[0058] 可选的，在所述生成告警信息之后，还包括：

[0059] 通过邮件、短信、对话框以及即时通信中的一种或多种组合将所述告警信息发送给网络管理人员。

[0060] 可选的，在所述生成告警信息之后，还包括：

[0061] 根据所述告警信息的告警内容为所述告警信息添加对应的攻击链标签，其中，所述攻击链标签用于表征所述网络攻击在攻击链中所处的攻击阶段；

[0062] 统计同一攻击事件的各个攻击链标签，获得处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作；

[0063] 根据处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作生成攻击路线信息，其中，所述攻击路线信息包括处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作。

[0064] 可选的，所述根据所述告警信息的告警内容为所述告警信息添加对应的攻击链标签包括：

[0065] 根据所述告警信息的告警内容，从预先建立的标签库中确定与所述告警信息对应的攻击链标签。

[0066] 可选的，所述攻击链标签包括两级以上，所述根据所述告警信息的告警内容为所述告警信息添加对应的攻击链标签包括：

[0067] 根据所述告警信息的告警内容，从预先建立的标签库中确定与所述告警信息对应的各级标签，其中，所述标签库存储有M个攻击链标签，所述M个攻击链标签被划分为两级以上，M为大于4的整数。

[0068] 可选的，所述攻击路线信息还包括各个攻击阶段的起止时间，在所述根据处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作生成攻击路线信息之后，还包括：

[0069] 按照各个攻击阶段的起始时间的先后顺序显示所述攻击路线信息。

[0070] 基于同样的发明构思，本发明还提供一种基于人工智能的网络攻击检测系统，包

括：

[0071] 采集模块，用于采集目标主机的网络数据；

[0072] 第一提取模块，用于从所述网络数据中提取待检测特征；

[0073] 导入模块，用于将所述待检测特征导入预先建立的人工智能模型，通过所述人工智能模型对所述待检测特征进行归类，根据归类结果确定所述目标主机是否受到网络攻击以及所述网络攻击的攻击类型。

[0074] 可选的，所述第一提取模块包括：

[0075] 第一提取单元，用于从所述网络数据中提取请求数据，其中，所述请求数据用于向所述目标主机发起请求服务；

[0076] 第二提取单元，用于从所述请求数据中提取所述待检测特征。

[0077] 可选的，所述基于人工智能的网络攻击检测系统，还包括：

[0078] 模型创建模块，用于建立所述人工智能模型。

[0079] 可选的，所述模型创建模块包括：

[0080] 收集模块，用于收集模型训练数据；

[0081] 第二提取模块，用于从所述模型训练数据中提取已知网络攻击的特征，获得攻击特征数据；

[0082] 分类模块，用于对所述攻击特征数据进行分类，获得训练样本；

[0083] 训练模块，用于根据所述训练样本进行模型训练，获得所述人工智能模型。

[0084] 可选的，所述模型训练数据包括互联网已公开的攻击数据、互联网已公开的漏洞数据、所述目标主机已采集的攻击数据以及所述目标主机已采集的漏洞数据中的一种或多种组合。

[0085] 可选的，所述训练模块为朴素贝叶斯算法模块。

[0086] 可选的，所述基于人工智能的网络攻击检测系统，还包括：

[0087] 检测模块，用于检测所述网络攻击是否成功；

[0088] 攻击动作获得模块，用于在所述网络攻击成功时，获得成功的网络攻击的攻击动作。

[0089] 可选的，所述检测模块包括：

[0090] 第三提取模块，用于从所述网络数据中提取待比对特征；

[0091] 比对模块，用于将所述待比对特征与预先建立的特征库中的一个以上攻击响应规则进行一一比对，其中，所述攻击响应规则根据第一响应数据形成，所述第一响应数据用于受攻击主机对成功攻击请求的应答；

[0092] 判定模块，用于在所述待比对特征与所述攻击响应规则相匹配时，判定所述网络攻击成功。

[0093] 可选的，所述第三提取模块包括：

[0094] 第三提取单元，用于从所述网络数据中提取第二响应数据，其中，所述第二响应数据用于所述目标主机应答请求服务；

[0095] 第四提取单元，用于从所述第二响应数据中提取所述待比对特征。

[0096] 可选的，所述第三提取模块包括：

[0097] 第五提取单元，用于从所述网络数据中提取请求数据和第二响应数据，其中，所述

请求数据用于向所述目标主机发起请求服务，所述第二响应数据用于所述目标主机应答请求服务；

[0098] 第六提取单元，用于从所述请求数据和所述第二响应数据中提取所述待比对特征。

[0099] 可选的，所述基于人工智能的网络攻击检测系统，还包括：

[0100] 特征库创建模块，用于建立所述特征库。

[0101] 可选的，所述特征库创建模块包括：

[0102] 数据库创建模块，用于创建数据库；

[0103] 第四提取模块，用于从一个以上第一响应数据中对应提取一个以上攻击响应特征；

[0104] 规则形成模块，用于对每个攻击响应特征进行确定性描述，形成一个以上攻击响应规则；

[0105] 存储模块，用于将所述一个以上攻击响应规则存储到所述数据库中，获得所述特征库。

[0106] 可选的，所述特征库包括N个子特征库，N为不小于2的整数，所述特征库创建模块包括：

[0107] 数据库创建模块，用于创建N个数据库；

[0108] 第四提取模块，用于从两个以上第一响应数据中对应提取两个以上攻击响应特征；

[0109] 规则形成模块，用于对每个攻击响应特征进行确定性描述，形成两个以上攻击响应规则；

[0110] 存储模块，用于将所述两个以上攻击响应规则中属于同种攻击类型的攻击响应规则存储到相同的数据库中，获得所述子特征库。

[0111] 可选的，所述比对模块用于将所述待比对特征与和所述网络攻击的攻击类型对应的子特征库中一个以上攻击响应规则进行一一比对。

[0112] 可选的，所述规则形成模块为正则表达式编写模块。

[0113] 可选的，所述攻击动作获得模块包括：

[0114] 关联关系创建模块，用于建立特征库中每个所述攻击响应规则与攻击动作之间的关联关系；

[0115] 攻击动作确定模块，用于根据特征库中每个所述攻击响应规则与攻击动作之间的关联关系，将与所述待比对特征匹配的攻击响应规则所对应的攻击动作，确定为所述成功的网络攻击的攻击动作。

[0116] 可选的，所述基于人工智能的网络攻击检测系统，还包括：

[0117] 告警信息生成模块，用于生成告警信息，其中，所述告警信息包括所述网络攻击的攻击类型、所述网络攻击是否成功以及成功的网络攻击的攻击动作。

[0118] 可选的，所述基于人工智能的网络攻击检测系统，还包括：

[0119] 发送模块，用于通过邮件、短信、对话框以及即时通信中的一种或多种组合将所述告警信息发送给网络管理人员。

[0120] 可选的，所述基于人工智能的网络攻击检测系统，还包括：

[0121] 标签添加模块，用于根据所述告警信息的告警内容为所述告警信息添加对应的攻击链标签，其中，所述攻击链标签用于表征所述网络攻击在攻击链中所处的攻击阶段；

[0122] 统计模块，用于统计同一攻击事件的各个攻击链标签，获得处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作；

[0123] 路线信息生成模块，用于根据处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作生成攻击路线信息，其中，所述攻击路线信息包括处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作。

[0124] 可选的，所述标签添加模块用于根据所述告警信息的告警内容，从预先建立的标签库中确定与所述告警信息对应的攻击链标签。

[0125] 可选的，所述攻击链标签包括两级以上，所述标签添加模块用于根据所述告警信息的告警内容，从预先建立的标签库中确定与所述告警信息对应的各级标签，其中，所述标签库存储有M个攻击链标签，所述M个攻击链标签被划分为两级以上，M为大于4的整数。

[0126] 可选的，所述攻击路线信息还包括各个攻击阶段的起止时间，所述基于人工智能的网络攻击检测系统，还包括：

[0127] 显示模块，用于按照各个攻击阶段的起始时间的先后顺序显示所述攻击路线信息。

[0128] 基于同样的发明构思，本发明还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现上述基于人工智能的网络攻击检测方法。

[0129] 基于同样的发明构思，本发明还提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述基于人工智能的网络攻击检测方法。

[0130] 本发明与现有技术相比，具有如下的优点和有益效果：

[0131] 本发明提供的基于人工智能的网络攻击检测方法及系统，通过采集目标主机的网络数据，从所述网络数据中提取待检测特征，并将所述待检测特征导入预先建立的人工智能模型，通过所述人工智能模型自动对所述待检测特征进行归类，根据归类结果确定所述目标主机是否受到网络攻击以及受到网络攻击的攻击类型。由于本发明是通过所述人工智能模型对所述待检测特征进行归类来检测所述目标主机是否受到网络攻击，即是利用人工智能技术进行网络攻击行为的检测，不依赖于特征库中的规则，因而实现了对于网络攻击请求的无规则化检测，极大地避免了攻击者进行绕过而检测不到的情况，从而能够发现更多的网络攻击。

附图说明

[0132] 此处所说明的附图用来提供对本发明实施例的进一步理解，构成本申请的一部分，并不构成对本发明实施例的限定。在附图中：

[0133] 图1是本发明实施例的基于人工智能的网络攻击检测方法的流程示意图；

[0134] 图2是本发明实施例的建立人工智能模型的流程示意图；

[0135] 图3是本发明实施例的检测网络攻击是否成功的流程示意图；

[0136] 图4是本发明一种实施例的建立特征库的流程示意图；

[0137] 图5是本发明另一种实施例的建立特征库的流程示意图；

[0138] 图6是本发明实施例的攻击路线信息的示意图；

[0139] 图7是本发明实施例的标签库的示意图。

具体实施方式

[0140] 本发明提供一种基于人工智能的网络攻击检测方法及系统，通过采集目标主机的网络数据，从所述网络数据中提取待检测特征，并将所述待检测特征导入预先建立的人工智能模型，由所述人工智能模型自动对所述待检测特征进行归类，根据归类结果确定所述目标主机是否受到网络攻击以及所述网络攻击的攻击类型。本发明提供的基于人工智能的网络攻击检测方法及系统，利用人工智能技术进行网络攻击行为的检测，不依赖于特征库中的规则，极大地避免了攻击者进行绕过而检测不到网络攻击的情况，因而能够发现更多的网络攻击，降低网络攻击检测的漏报率。

[0141] 为使本发明的目的、技术方案和优点更加清楚明白，下面结合实施例和附图，对本发明作进一步的详细说明，本发明的示意性实施方式及其说明仅用于解释本发明，并不作为对本发明的限定。

[0142] 实施例1

[0143] 本实施例提供一种基于人工智能的网络攻击检测方法，图1是所述基于人工智能的网络攻击检测方法的流程示意图，所述基于人工智能的网络攻击检测方法包括：

[0144] 步骤S11，采集目标主机的网络数据；

[0145] 步骤S12，从所述网络数据中提取待检测特征；

[0146] 步骤S13，将所述待检测特征导入预先建立的人工智能模型，通过所述人工智能模型对所述待检测特征进行归类，根据归类结果确定所述目标主机是否受到网络攻击以及所述网络攻击的攻击类型。

[0147] 具体地，所述目标主机可以是提供各种服务的服务器，也可以是能够实现特定功能的个人计算机，还可以是其他能够提供网络服务的网络设备。所述目标主机可以接收终端设备发送过来的用于向所述目标主机发起请求服务的请求数据，根据所述请求数据进行相应的数据处理以获得第二响应数据，即所述第二响应数据用于所述目标主机应答请求服务，并将所述第二响应数据反馈给所述终端设备。所述终端设备可以是具有显示功能并且支持交互功能的各种电子设备，包括但不限于智能手机、平板电脑、个人计算机以及台式计算机等。在本发明检测网络攻击这一具体的应用场景中，发起网络攻击的攻击者通常为恶意发送大量数据请求的用户。攻击者所利用的终端设备可以是具有强大计算功能的电子设备，甚至还可以是服务器。

[0148] 对于所述目标主机的网络数据的采集，可以采用网络嗅探方式获取，也可以通过网络端口镜像方式获取。所述网络嗅探方式是指将所述目标主机的网卡设置为混杂模式，通过调用网络截包工具来捕获所述目标主机的网路数据。所述网络端口镜像方式是指将所述目标主机的采集端口映射到另一端口，对数据进行实时拷贝，从而获得所述目标主机的网络数据。当然，采集所述目标主机的网络数据的具体实现方式并不限于上述两种方式，本实施例对此不作限定。

[0149] 采集到所述网络数据之后，从所述网络数据中提取所述待检测特征。所述网络数

据包括所述请求数据和所述第二响应数据，如前所述，所述请求数据用于向所述目标主机发起请求服务，是由终端设备发送给所述目标主机的数据；所述第二响应数据用于所述目标主机应答请求服务，是由所述目标主机发送给终端设备的数据。所述待检测特征的提取，可以是直接从所述网络数据中提取所述请求数据的特征来获得所述待检测特征，也可以是先从所述网络数据中提取所述请求数据，再从所述请求数据中提取所述待检测特征，本实施例对此不作限定。所述待检测特征可以包括请求时间、IP信息、端口信息、协议类型、发包频度、邮件地址、文件名称以及目标URL地址中的一项或多项组合。需要说明的是，所述待检测特征可根据实际情况进行灵活设定，本实施例对此不作限制。

[0150] 根据所述目标主机与终端设备之间采用的传输协议的不同，例如包括但不限于超文本传输协议(HTTP，Hyper Text Transfer Protocol)、文件传输协议(FTP，File Transfer Protocol)、简单邮件传输协议(SMTP，Simple Mail Transfer Protocol)，所述请求数据的结构也不相同。以HTTP类型的网络请求为例，所述请求数据包括以下三个部分：请求行，由方法(例如，POST)、统一资源标识符(URI，Uniform Resource Identifier)以及协议版本(例如，HTTP 1.1)三个部分构成；请求头部，用于通知所述目标主机有关终端设备请求的信息，包括但不限于产生请求的浏览器类型、终端设备可识别的内容类型列表以及请求的主机名；请求主体。在采集到所述网络数据后，进行HTTP请求头部中各个字段的解析，查找出需要进行检测的字段内容，即提取到所述待检测特征。

[0151] 获得所述待检测特征之后，将所述待检测特征导入预先建立的人工智能模型，通过所述人工智能模型对所述待检测特征进行归类，获得归类结果。所述人工智能模型可以为机器学习分类模型，例如朴素贝叶斯分类模型，还可以为深度学习分类模型。若所述归类结果为所述待检测特征不属于任何一种已知攻击类型的网络攻击，也不属于未知攻击类型的网络攻击，则确定所述目标主机未受到网络攻击；若所述归类结果为所述待检测特征属于某种已知攻击类型的网络攻击，则确定所述目标主机受到该种攻击类型的网络攻击；若所述归类结果为所述待检测特征属于某种未知攻击类型的网络攻击，则确定所述目标主机受到未知攻击类型的网络攻击。

[0152] 本实施例提供的基于人工智能的网络攻击检测方法，通过将所述待检测特征导入预先建立的人工智能模型，由所述人工智能模型自动对所述待检测特征进行归类，从而检测出所述目标主机是否受到网络攻击以及受到网络攻击的攻击类型。由于所述人工智能模型是利用人工智能技术的分类模型，具有自学习、自组织、自适应等能力，所以可有效地发现新型或变种的网络攻击，有效地弥补传统的网络攻击检测方法不能检测未知网络攻击的缺点，提高整体网络攻击检测能力，能够降低漏报率。

[0153] 进一步，在将所述待检测特征导入预先建立的人工智能模型之前，还需要建立所述人工智能模型。图2是建立所述人工智能模型的流程示意图，所述建立所述人工智能模型包括：

[0154] 步骤S21，收集模型训练数据；

[0155] 步骤S22，从所述模型训练数据中提取已知网络攻击的特征，获得攻击特征数据；

[0156] 步骤S23，对所述攻击特征数据进行分类，获得训练样本；

[0157] 步骤S24，根据所述训练样本进行模型训练，获得所述人工智能模型。

[0158] 具体地，所述模型训练数据包括互联网已公开的攻击数据、互联网已公开的漏洞

数据、所述目标主机已采集的攻击数据以及所述目标主机已采集的漏洞数据中的一种或多种组合。所述攻击数据为从已有的网络攻击案例中提取出的数据，所述漏洞数据为从已有的漏洞案例中提取出的数据。所述攻击数据和所述漏洞数据可以是互联网公开的，也可以是所述目标主机根据以往遭受的网络攻击事件进行分析和提炼而来。

[0159] 获得所述模型训练数据之后，从所述模型训练数据中提取已知网络攻击的特征，获得攻击特征数据。进一步，提取的攻击特征数据可以包括请求时间、IP信息、端口信息、协议类型、发包频度、邮件地址、文件名称以及目标URL地址中的一项或多项组合。需要说明的是，所述攻击特征数据可根据实际情况进行灵活设定，本实施例对此不作限制。获得所述攻击特征数据之后，按照其所属网络攻击的攻击类型进行分类以形成训练样本，所述网络攻击的攻击类型包括但不限于SQL注入攻击和XSS攻击。

[0160] 根据所述训练样本进行模型训练，即计算每种攻击类型的网络攻击在所述训练样本中的出现频率以及每个攻击特征数据划分对每种攻击类型的网络攻击的条件概率估计，并将计算结果进行记录就获得所述人工智能模型。在本实施例中，进行模型训练采用的算法为朴素贝叶斯算法。朴素贝叶斯算法对小规模的数据表现很好，适合多分类任务，适合增量式训练。当然，也可以采用其他机器学习分类算法或者深度学习分类算法进行模型训练，例如，还可以采用决策树算法进行模型训练，本实施例对此不作限定。

[0161] 实施例2

[0162] 本实施例提供另一种基于人工智能的网络攻击检测方法，与实施例1提供的基于人工智能的网络攻击检测方法相比，在根据归类结果确定所述目标主机受到所述网络攻击以及所述网络攻击的攻击类型之后，还包括：检测所述网络攻击是否成功；若所述网络攻击成功，则获得成功的网络攻击的攻击动作。

[0163] 在本实施例中，采用规则匹配的方式检测所述网络攻击是否成功。图3是本实施例的检测所述网络攻击是否成功的流程示意图，所述检测所述网络攻击是否成功包括：

[0164] 步骤S31，从所述网络数据中提取待比对特征；

[0165] 步骤S32，将所述待比对特征与预先建立的特征库中的一个以上攻击响应规则进行一一比对，其中，所述攻击响应规则根据第一响应数据形成，所述第一响应数据用于受攻击主机对成功攻击请求的应答；

[0166] 步骤S33，若所述待比对特征与所述攻击响应规则相匹配，则判定所述网络攻击成功。

[0167] 具体地，每种成功的网络攻击都有其独特性，这种独特性主要通过受攻击主机对成功攻击请求的应答体现。因此，所述待比对特征的提取即是提取所述第二响应数据的特征。提取所述待比对特征可以是直接从所述网络数据中提取所述第二响应数据的特征，也可以是先从所述网络数据中提取所述第二响应数据，再从所述第二响应数据中提取所述待比对特征，本实施例对此不作限定。

[0168] 以HTTP类型的网络响应为例，所述第二响应数据包括以下三个部分：状态行，由协议版本(例如，HTTP 1.1)、状态码以及状态码描述三个部分组成；响应头部，包括但不限于应用程序的名称、应用程序的版本、响应正文类型、响应正文长度以及响应正文所采用的编码；响应主体。在采集到所述网络数据后，进行HTTP响应头部中各个字段的解析，查找出需要进行比对的字段内容，即提取到所述待比对特征。

[0169] 进一步，要判断一个网络攻击是否成功，还可以从攻击者的角度进行逆向推导，通过响应内容反推攻击请求应具备的特征，以提高识别网络攻击是否成功的准确性。因此，所述待比对特征的提取还可以是从所述第二响应数据和所述请求数据中共同提取。具体地，可以从所述网络数据中提取所述请求数据和所述第二响应数据，再从所述请求数据和所述第二响应数据中提取所述待比对特征。仍以HTTP类型的网络请求和HTTP类型的网络响应为例，在采集到所述网络数据后，进行HTTP请求头部和HTTP响应头部中各个字段的解析，查找出需要进行比对的字段内容，即提取到所述待比对特征。

[0170] 获得所述待比对特征之后，将所述待比对特征与所述特征库中的一个以上攻击响应规则进行一一比对。仍以HTTP类型的传输协议为例，若所述待比对特征与所述特征库中的某个攻击响应规则相匹配，则判定HTTP请求为恶意攻击，所述目标主机受到的网络攻击成功；若所述待比对特征不能与所述特征库中的任意一个攻击响应规则相匹配，则判定HTTP请求为无效网络攻击，可以直接忽略该HTTP请求。

[0171] 所述特征库是预先建立的，其存储的攻击响应规则是根据所述第一响应数据形成，所述第一响应数据用于受攻击主机对成功攻击请求的应答，即所述攻击响应规则是根据已经存在的成功攻击请求对应的攻击响应的响应特性预先生成的。图4是本实施例提供的一种建立所述特征库的流程示意图，所述建立所述特征库包括：

[0172] 步骤S41，创建数据库；

[0173] 步骤S42，从一个以上第一响应数据中对应提取一个以上攻击响应特征；

[0174] 步骤S43，对每个攻击响应特征进行确定性描述，形成一个以上攻击响应规则；

[0175] 步骤S44，将所述一个以上攻击响应规则存储到所述数据库中，获得所述特征库。

[0176] 具体地，所述创建数据库即是创建空白的存储空间。所述第一响应数据用于受攻击主机对成功攻击请求的应答，可以从互联网已公开的攻击数据和/或所述目标主机已采集的攻击数据中进行收集。例如，攻击者向被攻击主机发送了floor()函数报错注入攻击请求，且所述floor()函数报错注入攻击请求获得了成功，所述被攻击主机对所述floor()函数报错注入攻击请求的应答即为所述第一响应数据。对于同一种攻击类型的网络攻击，根据具体攻击动作的不同还可以进行划分。例如，对于SQL注入攻击，还包括count()函数报错注入、rand()函数报错注入以及floor()函数报错注入等。对于每种攻击动作的网络攻击，对应可以收集一个第一响应数据，因而从一个以上第一响应数据中可以对应提取一个以上攻击响应特征，即每个第一响应数据可以对应提取到一个攻击响应特征。与所述攻击特征数据类似，所述攻击响应特征可以包括请求时间、IP信息、端口信息、协议类型、发包频度、邮件地址、文件名称以及目标URL地址中的一项或多项组合。需要说明的是，所述攻击响应特征也可根据实际情况进行灵活设定，本实施例对此不作限制。

[0177] 获得所述攻击响应特征之后，对每个攻击响应特征进行确定性描述，所述确定性描述是按照预设的规则进行描述。在本实施例中，可以采用传统的正则表达式对每个攻击响应特征进行确定性描述，也可以在所述正则表达式中加入运算逻辑、匹配逻辑等复杂逻辑，以提高匹配结果的准确性。获得所述攻击响应规则之后，将所有攻击响应规则存储到所述数据库中，即在所述空白的存储空间中写入相应的数据，就获得所述特征库。

[0178] 进一步，所述特征库还可以包括N个子特征库，每个子特征库对应存储同一种攻击类型的所有攻击响应规则，其中，N为不小于2的整数。基于此，图5是本实施例提供的另一种

建立所述特征库的流程示意图，所述建立所述特征库包括：

[0179] 步骤S51，创建N个数据库；

[0180] 步骤S52，从两个以上第一响应数据中对应提取两个以上攻击响应特征；

[0181] 步骤S53，对每个攻击响应特征进行确定性描述，形成两个以上攻击响应规则；

[0182] 步骤S54，将所述两个以上攻击响应规则中属于同种攻击类型的攻击响应规则存储到相同的数据库中，获得所述子特征库。

[0183] 具体地，步骤S51～步骤S53可参考前述对步骤S41～步骤S43的描述，在此不再赘述。在获得两个以上攻击响应规则之后，按照每个攻击响应规则所属的攻击类型，将属于同种攻击类型的攻击响应规则存储到相同的数据库中，获得所述子特征库。在本实施例中，所述子特征库可以为基础特征库、SQL注入特征库、XSS动态特征库以及工具指纹库，其中，所述基础特征库存储的是命令特征和文件特征，所述SQL注入特征库存储的是SQL注入攻击的特征，所述XSS动态特征库存储的是XSS动态攻击的特征，所述工具指纹库存储的是大马连接指纹和菜刀指纹。需要说明的是，所述子特征库可根据实际情况进行灵活设定，本实施例对此不作限制。

[0184] 针对采用图5所示流程建立的特征库，所述将所述待比对特征与预先建立的特征库中的一个以上攻击响应规则进行一一比对具体包括：将所述待比对特征与和所述网络攻击的攻击类型对应的子特征库中的一个以上攻击响应规则进行一一比对。例如，若所述网络攻击的攻击类型为SQL注入攻击，则将所述待比对特征与SQL注入特征库中的一个以上攻击响应规则进行一一比对；若所述网络攻击的攻击类型为XSS动态攻击，则将所述待比对特征与XSS动态特征库中的一个以上攻击响应规则进行一一比对。通过将所述特征库设置为多个子特征库，可以减少与所述待比对特征进行比对的攻击响应规则数量，只需与某个子特征库中的攻击响应规则进行匹配即可，因而能够提高所述待比对特征与所述攻击响应规则的比对效率。

[0185] 对于每种攻击动作的网络攻击，对应得到一个攻击响应规则，因而可以通过建立所述特征库中每个攻击响应规则与攻击动作之间的关联关系，根据所述特征库中每个攻击响应规则与攻击动作之间的关联关系，将与所述待比对特征匹配的攻击响应规则所对应的攻击动作，确定为所述成功的网络攻击的攻击动作。例如，与所述待比对特征相匹配的攻击响应规则对应的攻击动作为floor()函数报错注入，则成功的网络攻击的攻击动作为floor()函数报错注入。

[0186] 本实施例提供的基于人工智能的网络攻击检测方法，在确定所述目标主机受到所述网络攻击以及所述网络攻击的攻击类型之后，还检测所述网络攻击是否成功，并获得成功的网络攻击的攻击动作。因此，本实施例能够有效地识别成功的网络攻击，从而能够提高运维效率，发现真实漏洞。

[0187] 实施例3

[0188] 本实施例提供另一种基于人工智能的网络攻击检测方法，与实施例2提供的基于人工智能的网络攻击检测方法相比，在检测所述网络攻击是否成功之后，还可以生成告警信息，其中，所述告警信息包括所述网络攻击的攻击类型、所述网络攻击是否成功以及成功的网络攻击的攻击动作。例如，当所述目标主机受到SQL注入攻击但攻击不成功时，所述告警信息可以为“受到SQL注入攻击，攻击无效”；当所述目标主机受到SQL注入攻击并且攻击

成功，具体的攻击动作是利用floor()函数报错注入，所述告警信息可以为“受到SQL注入攻击，攻击成功，floor()函数报错注入”。

[0189] 进一步，在生成所述告警信息之后，还可以将所述告警信息发送给网络管理人员。例如，可以通过邮件的方式将所述告警信息发送至指定的邮箱地址，还可以通过短信的方式将所述告警信息发送至指定的移动终端，还可以通过对话框的形式直接在所述目标主机显示所述告警信息，还可以通过即时通信的方式将所述告警信息发送给网络管理人员。当然，可以采用上述任意一种方式将所述告警信息发送给网络管理人员，也可以采用任意几种方式的组合将所述告警信息发送给网络管理人员。

[0190] 通过生成所述告警信息，并将所述告警信息发送给网络管理人员，可以使网络管理人员直观地掌握所述目标主机受到的网络攻击情况。

[0191] 实施例4

[0192] 实施例3采取的是一个网络攻击对应一个告警信息的告警方式，即检测到一个网络攻击，对应就会产生一个告警信息。然而，孤立的告警信息不能准确地反映所述目标主机的安全状态，此种攻击展现不能从整体上把握攻击过程。因此，本实施例提供另一种基于人工智能的网络攻击检测方法。与实施例3提供的基于人工智能的网络攻击检测方法相比，本实施例在生成所述告警信息之后，还包括：

[0193] 根据所述告警信息的告警内容为所述告警信息添加对应的攻击链标签，其中，所述攻击链标签用于表征所述网络攻击在攻击链中所处的攻击阶段；

[0194] 统计同一攻击事件的各个攻击链标签，获得处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作；

[0195] 根据处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作生成攻击路线信息，其中，所述攻击路线信息包括处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作。

[0196] 根据所述目标主机受到的网络攻击的攻击阶段不同，所述告警信息的告警内容也不一样，即所述告警信息的告警内容揭示了所述告警信息对应的网络攻击想要实现的攻击目的，不同告警内容的告警信息对应不同攻击阶段。因此，根据目标主机遭受的网络攻击对应的告警信息的告警内容可以确定攻击阶段。具体地，根据所述告警信息的告警内容，从预先建立的标签库中确定与所述告警信息对应的攻击链标签。所述标签库存储有M个攻击链标签，每个攻击链标签对应表征攻击链中的一个攻击阶段。所述攻击链是指攻击者对目标主机从探测到破坏的一系列循环处理过程，通常由几个不同攻击阶段构成。例如，所述攻击链可以由侦察阶段、入侵阶段、命令控制阶段、横向渗透阶段、数据外泄阶段以及痕迹清理阶段六个攻击阶段构成，即M的值为6。相应地，所述M个攻击链标签为侦察标签、入侵标签、命令控制标签、横向渗透标签、数据外泄标签以及痕迹清理标签。当然，所述攻击链的划分并不限于此种方式，具体可根据实际情况进行灵活设置。

[0197] 如前所述，不同告警内容的告警信息对应不同攻击阶段，而每个攻击链标签对应表征一个攻击阶段，因而可以根据已公开的网络攻击事件，预先建立不同告警内容的告警信息与不同攻击链标签之间的关联关系。根据所述告警信息的告警内容，可以从预先建立的标签库中确定与所述告警信息对应的攻击链标签。以所述告警信息中所述网络攻击的攻

击类型为PHP代码执行攻击为例，对于PHP代码执行攻击，其在攻击链中处于命令控制阶段，因此为所述告警信息添加的攻击链标签为“命令控制”标签。进一步，所述攻击链标签可以作为所述告警信息的属性进行添加。

[0198] 在为一个攻击事件的所有告警信息添加对应的攻击链标签之后，通过统计相同攻击链标签的数量，即可获得处于所述攻击事件各个攻击阶段的网络攻击总次数。例如，通过统计侦察标签的数量，可以获得处于所述攻击事件侦察阶段的网络攻击总次数；通过统计入侵标签的数量，可以获得处于所述攻击事件入侵阶段的网络攻击总次数。以所述攻击事件中所述目标主机受到10次网络攻击为例，对应产生了10个告警信息，所述10个告警信息对应的攻击链标签分别为：侦察标签、侦察标签、入侵标签、入侵标签、入侵标签、侦察标签、入侵标签、命令控制标签、命令控制标签以及命令控制标签。通过对10个攻击链标签进行统计，可知所述目标主机受到侦察阶段的网络攻击3次，受到入侵阶段的网络攻击4次，受到命令控制阶段的网络攻击3次。

[0199] 对于处于所述攻击事件各个攻击阶段的成功的网络攻击次数的获得，可以将成功的网络攻击对应的告警信息筛选出来，再分别统计这些被筛选出来的告警信息对应的攻击链标签中相同攻击链标签的数量，即可获得处于所述攻击事件各个攻击阶段的成功的网络攻击次数。结合被筛选出来的告警信息内容，即可获得处于所述攻击事件各个攻击阶段的成功的网络攻击的攻击动作。

[0200] 在获得处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作之后，生成所述攻击路线信息。进一步，所述攻击路线信息还可以包括各个攻击阶段的起止时间，在所述生成攻击路线信息之后，还可以按照各个攻击阶段的起始时间的先后顺序显示所述攻击路线信息。各个攻击阶段的起始时间为处于该攻击阶段的首个网络攻击时间，各个攻击阶段的终止时间为处于该攻击阶段的末个网络攻击时间。还是以上述所述目标主机受到10次网络攻击为例，若侦察阶段的起止时间为2018-3-15 03:20～2018-3-19 15:12，入侵阶段的起止时间为2018-3-17 07:38～2018-3-21 05:21，命令控制阶段的起止时间为2018-3-20 14:47～2018-3-20 18:21，则根据统计结果生成的网络攻击路线信息可以显示为“2018-3-15 03:20～2018-3-19 15:12，侦查阶段:3次；2018-3-17 07:38～2018-3-21 05:21，入侵阶段，4次；2018-3-20 14:47～2018-3-20 18:21，命令控制阶段，4次”。当然，所述攻击路线信息还可以包括所述目标主机的IP地址和整个攻击事件的持续时间等信息，如图6所示，本实施例对此不作限定。

[0201] 进一步，由于所述攻击链中的各个攻击阶段还可以被划分为若干个更小的攻击阶段，每个更小的攻击阶段也由攻击链标签表征。相应地，所述攻击链标签可以包括两级以上，所述根据所述告警信息的告警内容为所述告警信息添加对应的攻击链标签包括：根据所述告警信息的告警内容，从预先建立的标签库中确定与所述告警信息对应的各级标签，其中，所述标签库存储有M个攻击链标签，所述M个攻击链标签被划分为两级以上，M为大于4的整数。

[0202] 图7是本实施例提供的一种标签库的示意图，所述标签库中的攻击链标签分为三个等级。一级标签包括侦察标签、入侵标签、命令控制标签、横向渗透标签、数据外泄标签以及痕迹清理标签。侦察标签对应的二级标签包括端口扫描标签、信息泄露标签、IP扫描标签以及子域名收集标签；入侵标签对应的二级标签包括漏洞探测标签、漏洞利用标签、拒绝服

务标签、暴力破解标签以及高危操作标签；命令控制标签对应的二级标签包括主机受控标签、黑客工具上传标签、服务器中转行为标签、提权标签、关闭杀毒软件标签以及主机信息获取标签；横向渗透标签包括内网侦查标签、嗅探攻击标签、内网漏洞探测标签以及内网漏洞利用标签；数据外泄标签对应的二级标签包括文件下载标签和拖库行为标签；痕迹清理标签对应的二级标签包括后门删除标签、关闭攻击服务标签以及清除日志标签。高危操作标签对应的三级标签包括数据库操作标签和弱口令成功登录标签。

[0203] 通过将攻击链标签设置为多个等级，可以更详细地描述攻击链中的攻击阶段，从而更详细地给网络管理人员呈现出攻击事件的整个过程。需要说明的是，所述标签库可以由所述目标主机创建，也可以由其他主机创建，所述目标主机需要添加对应的攻击链标签时直接从其他主机调用所述标签库即可。进一步，也可以直接为所述告警信息添加对应的攻击链标签，而不需要创建所述标签库。

[0204] 在生成所述攻击路线信息之后，可以通过邮件、短信、对话框以及即时通信中的一种或多种组合方式将所述攻击路线信息发送给网络管理人员。通过为所述告警信息添加对应的攻击链标签，根据所述攻击链标签统计处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作，可以对攻击事件重新按照事件的攻击链划分，能够从大数据分析的角度分攻击阶段地给网络管理人员呈现出攻击事件的整个过程，避免攻击线路混乱。

[0205] 实施例5

[0206] 本实施例提供一种基于人工智能的网络攻击检测系统，所述基于人工智能的网络攻击检测系统包括采集模块、第一提取模块以及导入模块。

[0207] 具体地，所述采集模块用于采集目标主机的网络数据；所述第一提取模块用于从所述网络数据中提取待检测特征；所述导入模块用于将所述待检测特征导入预先建立的人工智能模型，通过所述人工智能模型对所述待检测特征进行归类，根据归类结果确定所述目标主机是否受到网络攻击以及所述网络攻击的攻击类型。

[0208] 进一步，所述第一提取模块包括：第一提取单元，用于从所述网络数据中提取请求数据，其中，所述请求数据用于向所述目标主机发起请求服务；第二提取单元，用于从所述请求数据中提取所述待检测特征。

[0209] 进一步，所述基于人工智能的网络攻击检测系统还包括模型创建模块，所述模型创建模块用于建立所述人工智能模型。具体地，所述模型创建模块包括：收集模块，用于收集模型训练数据；第二提取模块，用于从所述模型训练数据中提取已知网络攻击的特征，获得攻击特征数据；分类模块，用于对所述攻击特征数据进行分类，获得训练样本；训练模块，用于根据所述训练样本进行模型训练，获得所述人工智能模型。

[0210] 所述基于人工智能的网络攻击检测系统的具体工作原理可参考实施例1中对于步骤S11至步骤S13的描述，本实施例在此不再赘述。

[0211] 实施例6

[0212] 本实施例提供另一种基于人工智能的网络攻击检测系统，与实施例5提供的基于人工智能的网络攻击检测系统相比，所述基于人工智能的网络攻击检测系统还包括：检测模块，用于检测所述网络攻击是否成功；攻击动作获得模块，用于在所述网络攻击成功时，获得成功的网络攻击的攻击动作。

[0213] 具体地，所述检测模块包括：第三提取模块，用于从所述网络数据中提取待比对特征；比对模块，用于将所述待比对特征与预先建立的特征库中的一个以上攻击响应规则进行一一比对，其中，所述攻击响应规则根据第一响应数据形成，所述第一响应数据用于受攻击主机对成功攻击请求的应答；判定模块，用于在所述待比对特征与所述攻击响应规则相匹配时，判定所述网络攻击成功。

[0214] 进一步，所述第三提取模块可以包括：第三提取单元，用于从所述网络数据中提取第二响应数据，其中，所述第二响应数据用于所述目标主机应答请求服务；第四提取单元，用于从所述第二响应数据中提取所述待比对特征。

[0215] 进一步，所述第三提取模块也可以包括：第五提取单元，用于从所述网络数据中提取请求数据和第二响应数据，其中，所述请求数据用于向所述目标主机发起请求服务，所述第二响应数据用于所述目标主机应答请求服务；第六提取单元，用于从所述请求数据和所述第二响应数据中提取所述待比对特征。

[0216] 进一步，所述基于人工智能的网络攻击检测系统还包括：特征库创建模块，用于建立所述特征库。具体地，所述特征库创建模块可以包括：数据库创建模块，用于创建数据库；第四提取模块，用于从一个以上第一响应数据中对应提取一个以上攻击响应特征；规则形成模块，用于对每个攻击响应特征进行确定性描述，形成一个以上攻击响应规则；存储模块，用于将所述一个以上攻击响应规则存储到所述数据库中，获得所述特征库。所述特征库可以包括N个子特征库，N为不小于2的整数。基于此，所述特征库创建模块也可以包括：数据库创建模块，用于创建N个数据库；第四提取模块，用于从两个以上第一响应数据中对应提取两个以上攻击响应特征；规则形成模块，用于对每个攻击响应特征进行确定性描述，形成两个以上攻击响应规则；存储模块，用于将所述两个以上攻击响应规则中属于同种攻击类型的攻击响应规则存储到相同的数据库中，获得所述子特征库。

[0217] 进一步，所述攻击动作获得模块包括：关联关系创建模块，用于建立特征库中每个所述攻击响应规则与攻击动作之间的关联关系；攻击动作确定模块，用于根据特征库中每个所述攻击响应规则与攻击动作之间的关联关系，将与所述待比对特征匹配的攻击响应规则所对应的攻击动作，确定为所述成功的网络攻击的攻击动作。

[0218] 所述基于人工智能的网络攻击检测系统的具体工作原理可参考实施例2中对于步骤S31至步骤S33的描述，本实施例在此不再赘述。

[0219] 实施例7

[0220] 本实施例提供另一种基于人工智能的网络攻击检测系统，与实施例6提供的基于人工智能的网络攻击检测系统相比，所述基于人工智能的网络攻击检测系统还包括：告警信息生成模块，用于生成告警信息，其中，所述告警信息包括所述网络攻击的攻击类型、所述网络攻击是否成功以及成功的网络攻击的攻击动作。进一步，所述基于人工智能的网络攻击检测系统，还包括：发送模块，用于通过邮件、短信、对话框以及即时通信中的一种或多种组合将所述告警信息发送给网络管理人员。

[0221] 所述基于人工智能的网络攻击检测系统的具体工作原理可参考实施例3中对各个步骤的描述，本实施例在此不再赘述。

[0222] 实施例8

[0223] 本实施例提供另一种基于人工智能的网络攻击检测系统，与实施例8提供的基于

人工智能的网络攻击检测系统相比，所述基于人工智能的网络攻击检测系统还包括：

[0224] 标签添加模块，用于根据所述告警信息的告警内容为所述告警信息添加对应的攻击链标签，其中，所述攻击链标签用于表征所述网络攻击在攻击链中所处的攻击阶段；

[0225] 统计模块，用于统计同一攻击事件的各个攻击链标签，获得处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作；

[0226] 路线信息生成模块，用于根据处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作生成攻击路线信息，其中，所述攻击路线信息包括处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作。

[0227] 进一步，所述攻击链标签包括两级以上，所述标签添加模块用于根据所述告警信息的告警内容，从预先建立的标签库中确定与所述告警信息对应的各级标签，其中，所述标签库存储有M个攻击链标签，所述M个攻击链标签被划分为两级以上，M为大于4的整数。

[0228] 进一步，所述攻击路线信息还包括各个攻击阶段的起止时间，所述基于人工智能的网络攻击检测系统还包括：显示模块，用于按照各个攻击阶段的起始时间的先后顺序显示所述攻击路线信息。

[0229] 所述基于人工智能的网络攻击检测系统的具体工作原理可参考实施例4中对各个步骤的描述，本实施例在此不再赘述。

[0230] 实施例9

[0231] 本实施例提供一种计算机可读存储介质，其上存储有计算机程序，本发明实施例1至实施例4提供的任一种基于人工智能的网络攻击检测方法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，本发明实现实施例1至实施例4提供的任一种基于人工智能的网络攻击检测方法中的全部或部分流程，也可以通过计算机程序来指令相关的硬件来完成。所述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。

[0232] 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可以包括：能够携带所述计算机程序代码的任何实体或装置、介质、U盘、移动硬盘、磁碟、光盘、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等。需要说明的是，所述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减，例如在某些司法管辖区，根据立法和专利实践，计算机可读介质不包括电载波信号和电信信号。

[0233] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

[0234] 本发明公开A1、一种基于人工智能的网络攻击检测方法，包括：

[0235] 采集目标主机的网络数据；

[0236] 从所述网络数据中提取待检测特征；

[0237] 将所述待检测特征导入预先建立的人工智能模型，通过所述人工智能模型对所述待检测特征进行归类，根据归类结果确定所述目标主机是否受到网络攻击以及所述网络攻击的攻击类型。

[0238] A2、根据A1所述的一种基于人工智能的网络攻击检测方法，所述从所述网络数据中提取待检测特征包括：

[0239] 从所述网络数据中提取请求数据，其中，所述请求数据用于向所述目标主机发起请求服务；

[0240] 从所述请求数据中提取所述待检测特征。

[0241] A3、根据A1所述的一种基于人工智能的网络攻击检测方法，在所述将所述待检测特征导入预先建立的人工智能模型之前，还包括：

[0242] 建立所述人工智能模型。

[0243] A4、根据A3所述的一种基于人工智能的网络攻击检测方法，所述建立所述人工智能模型包括：

[0244] 收集模型训练数据；

[0245] 从所述模型训练数据中提取已知网络攻击的特征，获得攻击特征数据；

[0246] 对所述攻击特征数据进行分类，获得训练样本；

[0247] 根据所述训练样本进行模型训练，获得所述人工智能模型。

[0248] A5、根据A4所述的一种基于人工智能的网络攻击检测方法，所述收集模型训练数据包括：

[0249] 收集互联网已公开的攻击数据、互联网已公开的漏洞数据、所述目标主机已采集的攻击数据以及所述目标主机已采集的漏洞数据中的一种或多种组合。

[0250] A6、根据A4所述的一种基于人工智能的网络攻击检测方法，所述根据所述训练样本进行模型训练包括：

[0251] 根据所述训练样本，采用朴素贝叶斯算法进行模型训练。

[0252] A7、根据A1至A6任一项所述的一种基于人工智能的网络攻击检测方法，在根据归类结果确定所述目标主机受到所述网络攻击以及所述网络攻击的攻击类型之后，还包括：

[0253] 检测所述网络攻击是否成功；

[0254] 若所述网络攻击成功，则获得成功的网络攻击的攻击动作。

[0255] A8、根据A7所述的一种基于人工智能的网络攻击检测方法，所述检测所述网络攻击是否成功包括：

[0256] 从所述网络数据中提取待比对特征；

[0257] 将所述待比对特征与预先建立的特征库中的一个以上攻击响应规则进行一一比对，其中，所述攻击响应规则根据第一响应数据形成，所述第一响应数据用于受攻击主机对成功攻击请求的应答；

[0258] 若所述待比对特征与所述攻击响应规则相匹配，则判定所述网络攻击成功。

[0259] A9、根据A8所述的一种基于人工智能的网络攻击检测方法，所述从所述网络数据中提取待比对特征包括：

[0260] 从所述网络数据中提取第二响应数据，其中，所述第二响应数据用于所述目标主机应答请求服务；

[0261] 从所述第二响应数据中提取所述待比对特征。

[0262] A10、根据A8所述的一种基于人工智能的网络攻击检测方法，A所述从所述网络数据中提取待比对特征包括：

[0263] 从所述网络数据中提取请求数据和第二响应数据，其中，所述请求数据用于向所述目标主机发起请求服务，所述第二响应数据用于所述目标主机应答请求服务；

[0264] 从所述请求数据和所述第二响应数据中提取所述待比对特征。

[0265] A11、根据A8所述的一种基于人工智能的网络攻击检测方法，在所述将所述待比对特征与预先建立的特征库中的一个以上攻击响应规则进行一一比对之前，还包括：

[0266] 建立所述特征库。

[0267] A12、根据A11所述的一种基于人工智能的网络攻击检测方法，所述建立所述特征库包括：

[0268] 创建数据库；

[0269] 从一个以上第一响应数据中对应提取一个以上攻击响应特征；

[0270] 对每个攻击响应特征进行确定性描述，形成一个以上攻击响应规则；

[0271] 将所述一个以上攻击响应规则存储到所述数据库中，获得所述特征库。

[0272] A13、根据A11所述的一种基于人工智能的网络攻击检测方法，所述特征库包括N个子特征库，N为不小于2的整数，所述建立所述特征库包括：

[0273] 创建N个数据库；

[0274] 从两个以上第一响应数据中对应提取两个以上攻击响应特征；

[0275] 对每个攻击响应特征进行确定性描述，形成两个以上攻击响应规则；

[0276] 将所述两个以上攻击响应规则中属于同种攻击类型的攻击响应规则存储到相同的数据库中，获得所述子特征库。

[0277] A14、根据A13所述的一种基于人工智能的网络攻击检测方法，所述将所述待比对特征与预先建立的特征库中的一个以上攻击响应规则进行一一比对包括：

[0278] 将所述待比对特征与和所述网络攻击的攻击类型对应的子特征库中一个以上攻击响应规则进行一一比对。

[0279] A15、根据A12或A13所述的一种基于人工智能的网络攻击检测方法，所述对每个攻击响应特征进行确定性描述包括：

[0280] 采用正则表达式对每个攻击响应特征进行确定性描述。

[0281] A16、根据A12或A13所述的一种基于人工智能的网络攻击检测方法，所述获得成功的网络攻击的攻击动作包括：

[0282] 建立特征库中每个所述攻击响应规则与攻击动作之间的关联关系；

[0283] 根据特征库中每个所述攻击响应规则与攻击动作之间的关联关系，将与所述待比对特征匹配的攻击响应规则所对应的攻击动作，确定为所述成功的网络攻击的攻击动作。

[0284] A17、根据A7所述的一种基于人工智能的网络攻击检测方法，在所述检测所述网络攻击是否成功之后，还包括：

[0285] 生成告警信息，其中，所述告警信息包括所述网络攻击的攻击类型、所述网络攻击是否成功以及成功的网络攻击的攻击动作。

[0286] A18、根据A17所述的一种基于人工智能的网络攻击检测方法，在所述生成告警信

息之后，还包括：

[0287] 通过邮件、短信、对话框以及即时通信中的一种或多种组合将所述告警信息发送给网络管理人员。

[0288] A19、根据A17所述的一种基于人工智能的网络攻击检测方法，在所述生成告警信息之后，还包括：

[0289] 根据所述告警信息的告警内容为所述告警信息添加对应的攻击链标签，其中，所述攻击链标签用于表征所述网络攻击在攻击链中所处的攻击阶段；

[0290] 统计同一攻击事件的各个攻击链标签，获得处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作；

[0291] 根据处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作生成攻击路线信息，其中，所述攻击路线信息包括处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作。

[0292] A20、根据A19所述的一种基于人工智能的网络攻击检测方法，所述根据所述告警信息的告警内容为所述告警信息添加对应的攻击链标签包括：

[0293] 根据所述告警信息的告警内容，从预先建立的标签库中确定与所述告警信息对应的攻击链标签。

[0294] A21、根据A19所述的一种基于人工智能的网络攻击检测方法，所述攻击链标签包括两级以上，所述根据所述告警信息的告警内容为所述告警信息添加对应的攻击链标签包括：

[0295] 根据所述告警信息的告警内容，从预先建立的标签库中确定与所述告警信息对应的各级标签，其中，所述标签库存储有M个攻击链标签，所述M个攻击链标签被划分为两级以上，M为大于4的整数。

[0296] A22、根据A19所述的一种基于人工智能的网络攻击检测方法，所述攻击路线信息还包括各个攻击阶段的起止时间，在所述根据处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作生成攻击路线信息之后，还包括：

[0297] 按照各个攻击阶段的起始时间的先后顺序显示所述攻击路线信息。

[0298] 本发明还公开了B23、一种基于人工智能的网络攻击检测系统，包括：

[0299] 采集模块，用于采集目标主机的网络数据；

[0300] 第一提取模块，用于从所述网络数据中提取待检测特征；

[0301] 导入模块，用于将所述待检测特征导入预先建立的人工智能模型，通过所述人工智能模型对所述待检测特征进行归类，根据归类结果确定所述目标主机是否受到网络攻击以及所述网络攻击的攻击类型。

[0302] B24、根据B23所述的一种基于人工智能的网络攻击检测系统，B所述第一提取模块包括：

[0303] 第一提取单元，用于从所述网络数据中提取请求数据，其中，所述请求数据用于向所述目标主机发起请求服务；

[0304] 第二提取单元，用于从所述请求数据中提取所述待检测特征。

[0305] B25、根据B23所述的一种基于人工智能的网络攻击检测系统，还包括：

[0306] 模型创建模块，用于建立所述人工智能模型。

[0307] B26、根据B25所述的一种基于人工智能的网络攻击检测系统，所述模型创建模块包括：

[0308] 收集模块，用于收集模型训练数据；

[0309] 第二提取模块，用于从所述模型训练数据中提取已知网络攻击的特征，获得攻击特征数据；

[0310] 分类模块，用于对所述攻击特征数据进行分类，获得训练样本；

[0311] 训练模块，用于根据所述训练样本进行模型训练，获得所述人工智能模型。

[0312] B27、根据B26所述的一种基于人工智能的网络攻击检测系统，所述模型训练数据包括互联网已公开的攻击数据、互联网已公开的漏洞数据、所述目标主机已采集的攻击数据以及所述目标主机已采集的漏洞数据中的一种或多种组合。

[0313] B28、根据B26所述的一种基于人工智能的网络攻击检测系统，所述训练模块为朴素贝叶斯算法模块。

[0314] B29、根据B23至B28任一项所述的一种基于人工智能的网络攻击检测系统，还包括：

[0315] 检测模块，用于检测所述网络攻击是否成功；

[0316] 攻击动作获得模块，用于在所述网络攻击成功时，获得成功的网络攻击的攻击动作。

[0317] B30、根据B29所述的一种基于人工智能的网络攻击检测系统，所述检测模块包括：

[0318] 第三提取模块，用于从所述网络数据中提取待比对特征；

[0319] 比对模块，用于将所述待比对特征与预先建立的特征库中的一个以上攻击响应规则进行一一比对，其中，所述攻击响应规则根据第一响应数据形成，所述第一响应数据用于受攻击主机对成功攻击请求的应答；

[0320] 判定模块，用于在所述待比对特征与所述攻击响应规则相匹配时，判定所述网络攻击成功。

[0321] B31、根据B30所述的一种基于人工智能的网络攻击检测系统，所述第三提取模块包括：

[0322] 第三提取单元，用于从所述网络数据中提取第二响应数据，其中，所述第二响应数据用于所述目标主机应答请求服务；

[0323] 第四提取单元，用于从所述第二响应数据中提取所述待比对特征。

[0324] B32、根据B30所述的一种基于人工智能的网络攻击检测系统，所述第三提取模块包括：

[0325] 第五提取单元，用于从所述网络数据中提取请求数据和第二响应数据，其中，所述请求数据用于向所述目标主机发起请求服务，所述第二响应数据用于所述目标主机应答请求服务；

[0326] 第六提取单元，用于从所述请求数据和所述第二响应数据中提取所述待比对特征。

[0327] B33、根据B30所述的一种基于人工智能的网络攻击检测系统，还包括：

[0328] 特征库创建模块，用于建立所述特征库。

[0329] B34、根据B33所述的一种基于人工智能的网络攻击检测系统，所述特征库创建模块包括：

[0330] 数据库创建模块，用于创建数据库；

[0331] 第四提取模块，用于从一个以上第一响应数据中对应提取一个以上攻击响应特征；

[0332] 规则形成模块，用于对每个攻击响应特征进行确定性描述，形成一个以上攻击响应规则；

[0333] 存储模块，用于将所述一个以上攻击响应规则存储到所述数据库中，获得所述特征库。

[0334] B35、根据B33所述的一种基于人工智能的网络攻击检测系统，所述特征库包括N个子特征库，N为不小于2的整数，所述特征库创建模块包括：

[0335] 数据库创建模块，用于创建N个数据库；

[0336] 第四提取模块，用于从两个以上第一响应数据中对应提取两个以上攻击响应特征；

[0337] 规则形成模块，用于对每个攻击响应特征进行确定性描述，形成两个以上攻击响应规则；

[0338] 存储模块，用于将所述两个以上攻击响应规则中属于同种攻击类型的攻击响应规则存储到相同的数据库中，获得所述子特征库。

[0339] B36、根据B35所述的一种基于人工智能的网络攻击检测系统，所述比对模块用于将所述待比对特征与和所述网络攻击的攻击类型对应的子特征库中一个以上攻击响应规则进行一一比对。

[0340] B37、根据B34或B35所述的一种基于人工智能的网络攻击检测系统，所述规则形成模块为正则表达式编写模块。

[0341] B38、根据B34或B35所述的一种基于人工智能的网络攻击检测系统，所述攻击动作获得模块包括：

[0342] 关联关系创建模块，用于建立特征库中每个所述攻击响应规则与攻击动作之间的关联关系；

[0343] 攻击动作确定模块，用于根据特征库中每个所述攻击响应规则与攻击动作之间的关联关系，将与所述待比对特征匹配的攻击响应规则所对应的攻击动作，确定为所述成功的网络攻击的攻击动作。

[0344] B39、根据B29所述的一种基于人工智能的网络攻击检测系统，还包括：

[0345] 告警信息生成模块，用于生成告警信息，其中，所述告警信息包括所述网络攻击的攻击类型、所述网络攻击是否成功以及成功的网络攻击的攻击动作。

[0346] B40、根据B39所述的一种基于人工智能的网络攻击检测系统，还包括：

[0347] 发送模块，用于通过邮件、短信、对话框以及即时通信中的一种或多种组合将所述告警信息发送给网络管理人员。

[0348] B41、根据B39所述的一种基于人工智能的网络攻击检测系统，还包括：

[0349] 标签添加模块，用于根据所述告警信息的告警内容为所述告警信息添加对应的攻

击链标签，其中，所述攻击链标签用于表征所述网络攻击在攻击链中所处的攻击阶段；

[0350] 统计模块，用于统计同一攻击事件的各个攻击链标签，获得处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作；

[0351] 路线信息生成模块，用于根据处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作生成攻击路线信息，其中，所述攻击路线信息包括处于所述攻击事件各个攻击阶段的网络攻击总次数、成功的网络攻击次数以及成功的网络攻击的攻击动作。

[0352] B42、根据B41所述的一种基于人工智能的网络攻击检测系统，所述标签添加模块用于根据所述告警信息的告警内容，从预先建立的标签库中确定与所述告警信息对应的攻击链标签。

[0353] B43、根据B41所述的一种基于人工智能的网络攻击检测系统，所述攻击链标签包括两级以上，所述标签添加模块用于根据所述告警信息的告警内容，从预先建立的标签库中确定与所述告警信息对应的各级标签，其中，所述标签库存储有M个攻击链标签，所述M个攻击链标签被划分为两级以上，M为大于4的整数。

[0354] B44、根据B41所述的一种基于人工智能的网络攻击检测系统，所述攻击路线信息还包括各个攻击阶段的起止时间，还包括：

[0355] 显示模块，用于按照各个攻击阶段的起始时间的先后顺序显示所述攻击路线信息。

[0356] 本发明还公开了C45、一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现A1至A22任一项所述的一种基于人工智能的网络攻击检测方法。

[0357] 本发明还公开了D46、一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现A1至A22任一项所述的一种基于人工智能的网络攻击检测方法。

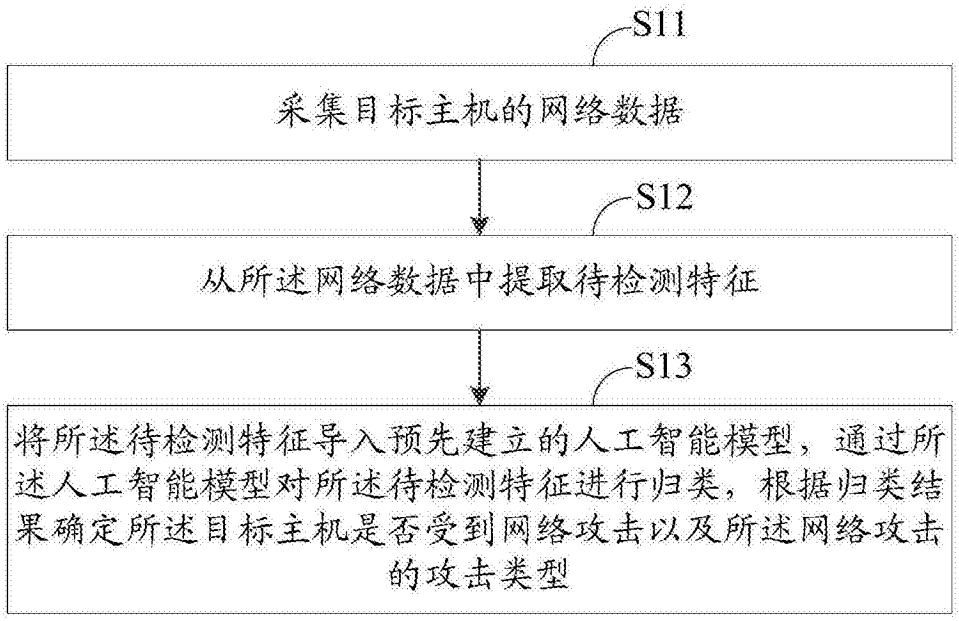

S11
采集目标主机的网络数据
S12
从所述网络数据中提取待检测特征
S13
将所述待检测特征导入预先建立的人工智能模型，通过所述人工智能模型对所述待检测特征进行归类，根据归类结果确定所述目标主机是否受到网络攻击以及所述网络攻击的攻击类型

图1

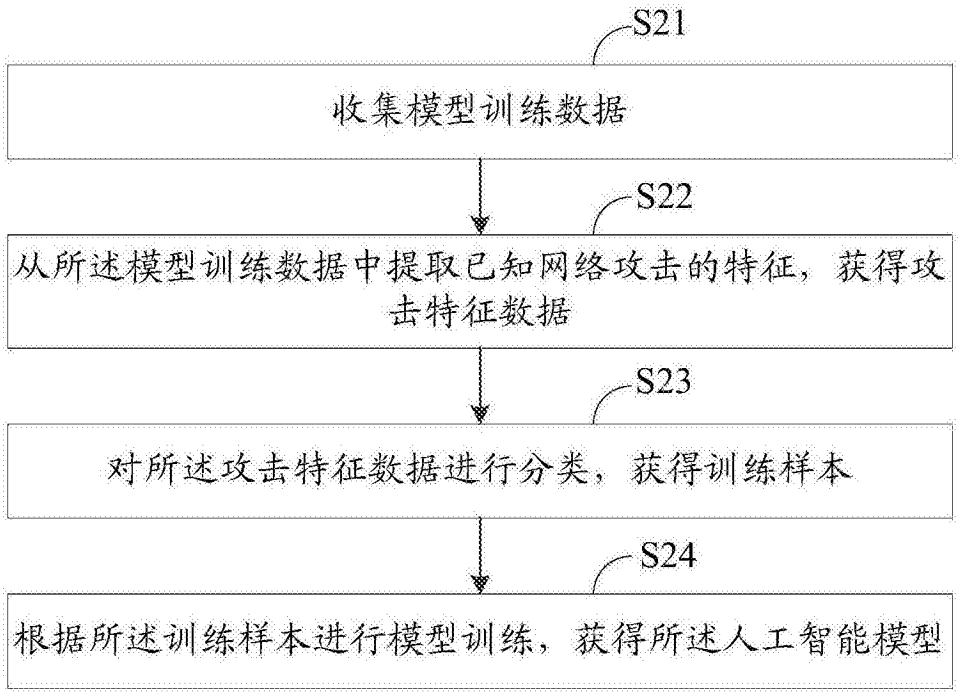

S21
收集模型训练数据
S22
从所述模型训练数据中提取已知网络攻击的特征，获得攻击特征数据
S23
对所述攻击特征数据进行分类，获得训练样本
S24
根据所述训练样本进行模型训练，获得所述人工智能模型

图2

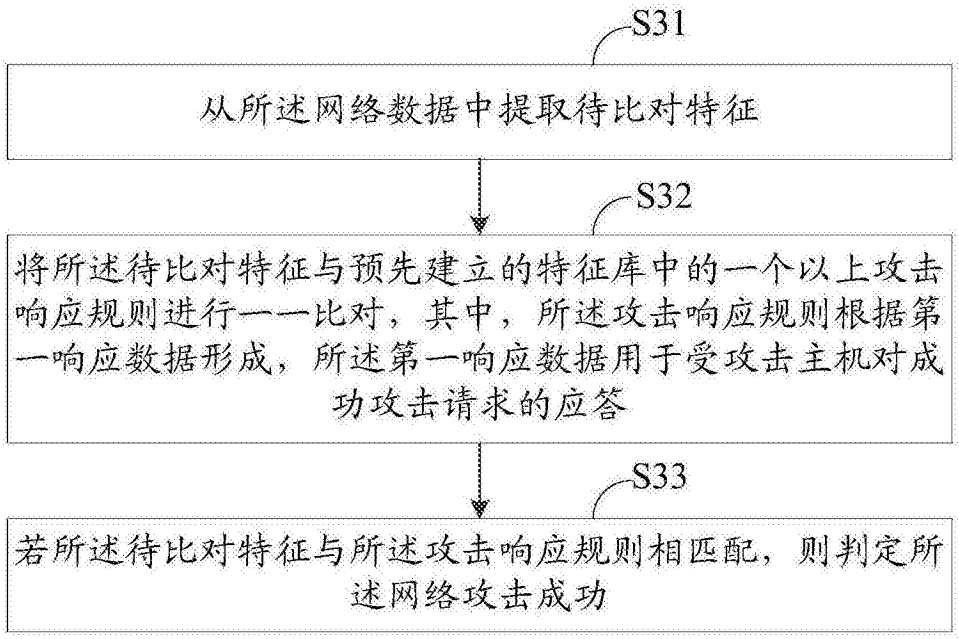

S31
从所述网络数据中提取待比对特征
S32
将所述待比对特征与预先建立的特征库中的一个以上攻击响应规则进行一一比对，其中，所述攻击响应规则根据第一响应数据形成，所述第一响应数据用于受攻击主机对成功攻击请求的应答
S33
若所述待比对特征与所述攻击响应规则相匹配，则判定所述网络攻击成功

图3

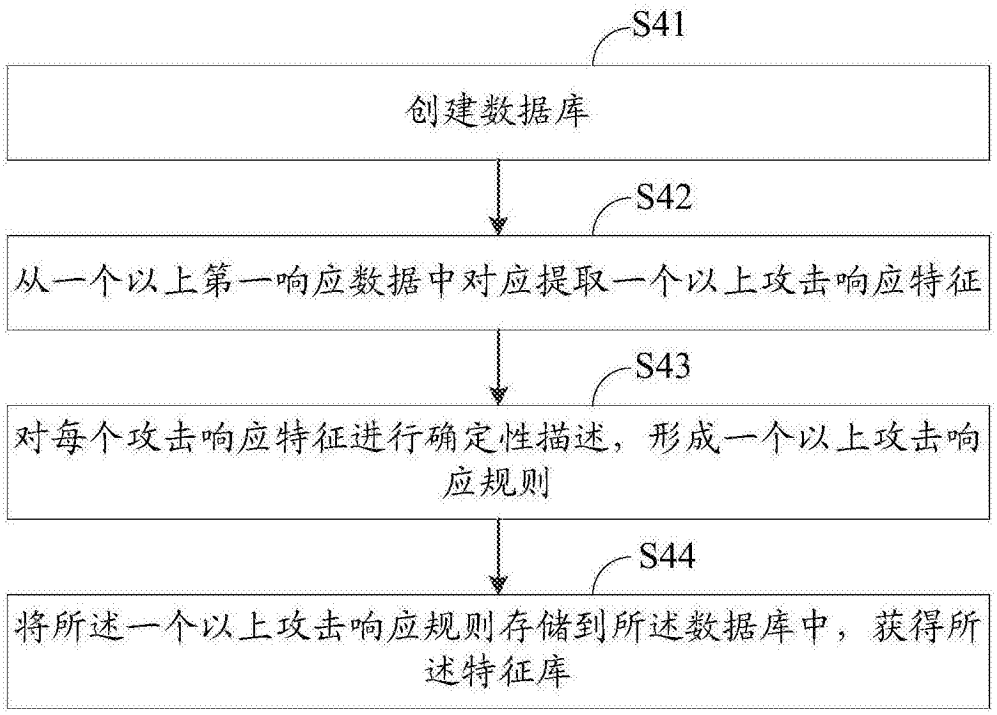

S41
创建数据库
S42
从一个以上第一响应数据中对应提取一个以上攻击响应特征
S43
对每个攻击响应特征进行确定性描述，形成一个以上攻击响应规则
S44
将所述一个以上攻击响应规则存储到所述数据库中，获得所述特征库

图4

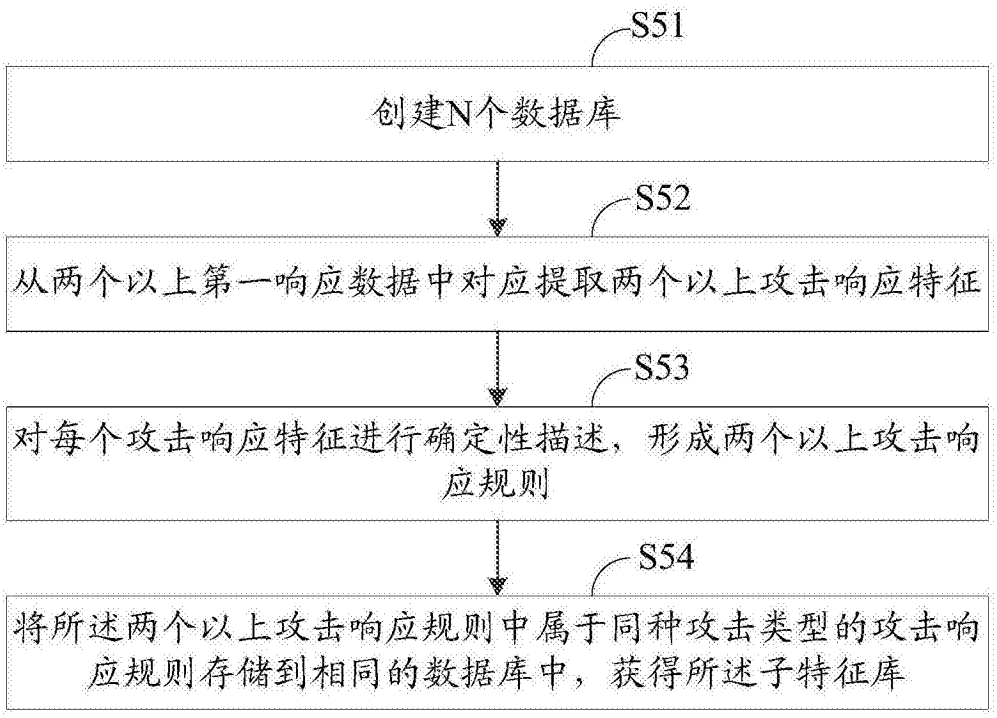

S51
创建N个数据库
S52
从两个以上第一响应数据中对应提取两个以上攻击响应特征
S53
对每个攻击响应特征进行确定性描述，形成两个以上攻击响应规则
S54
将所述两个以上攻击响应规则中属于同种攻击类型的攻击响应规则存储到相同的数据库中，获得所述子特征库

图5

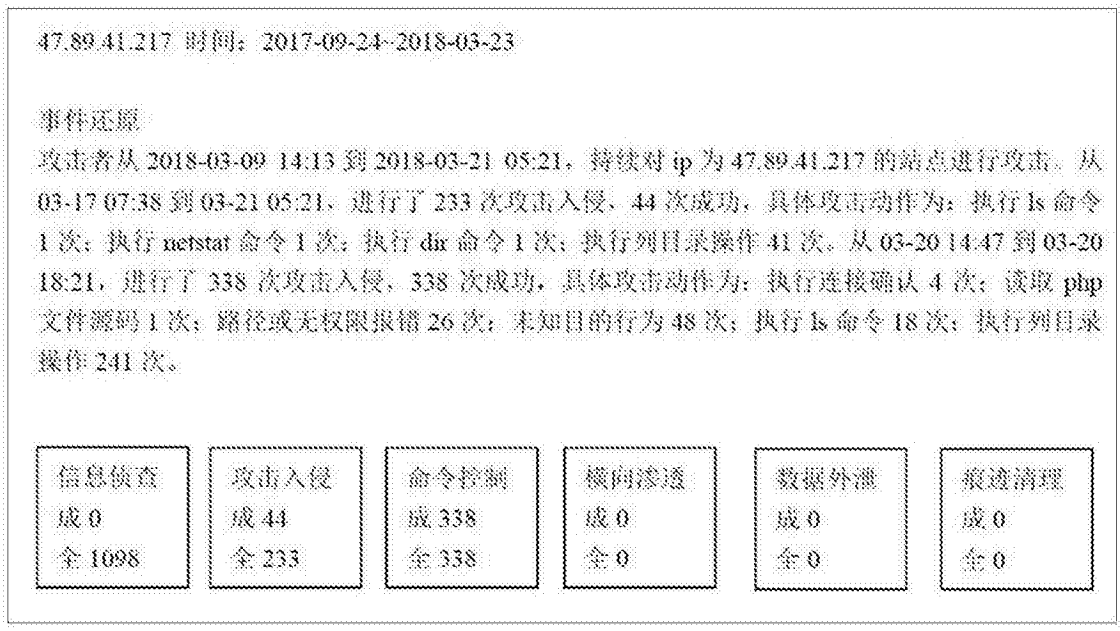

47.89.41.217 时间：2017-09-24~2018-03-23
事件还原
攻击者从 2018-03-09 14:13 到 2018-03-21 05:21，持续对 ip 为 47.89.41.217 的站点进行攻击。从 03-17 07:38 到 03-21 05:21，进行了 233 次攻击入侵，44 次成功，具体攻击动作为：执行 ls 命令 1 次；执行 netstat 命令 1 次；执行 dir 命令 1 次；执行列目录操作 41 次。从 03-20 14:47 到 03-20 18:21，进行了 338 次攻击入侵，338 次成功，具体攻击动作为：执行连接确认 4 次；读取 php 文件源码 1 次；路径或无权限报错 26 次；未知目的行为 48 次；执行 ls 命令 18 次；执行列目录操作 241 次。
信息侦查
成 0
全 1098
攻击入侵
成 44
全 233
命令控制
成 338
全 338
横向渗透
成 0
全 0
数据外泄
成 0
全 0
痕迹清理
成 0
全 0

图6

攻击链标签			
一级标签	二级标签	三级标签	
侦查			
	端口扫描		
	信息泄露		
	IP 扫描		
	子域名收集		
入侵			
	漏洞探测		
	漏洞利用		
	拒绝服务		
	暴力破解		
	高危操作		
		数据库操作	
		弱口令成功登录	
命令控制			
	主机受控		
	黑客工具上传		
	服务器中转行为		
	提权		
	关闭杀毒软件		
	主机信息获取		
横向渗透			
	内网侦查		
	嗅探攻击		
	内网漏洞探测		
	内网漏洞利用		
数据外泄			
	文件下载		
	拖库行为		
痕迹清理			
	后门删除		
	关闭攻击服务		
	清除日志		

图7