(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114726654 B
(45)授权公告日 2022.12.06

(21)申请号 202210572275.7
(22)申请日 2022.05.25
(65)同一申请的已公布的文献号
申请公布号 CN 114726654 A
(43)申请公布日 2022.07.08
(73)专利权人 北京徽享科技有限公司
地址 100000 北京市海淀区西北旺东路10号院东区12号楼B座四层406室
(72)发明人 龚良
(74)专利代理机构 北京华仁联合知识产权代理有限公司 11588
专利代理师 王小芳
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/10(2022.01)

(56)对比文件
US 2020186548 A1,2020.06.11
US 2020186548 A1,2020.06.11
WO 2021196911 A1,2021.10.07
CN 111565205 A,2020.08.21
CN 111565205 A,2020.08.21
CN 110839033 A,2020.02.25
CN 106899435 A,2017.06.27
WO 2021169293 A1,2021.09.02

审查员 孙志玲

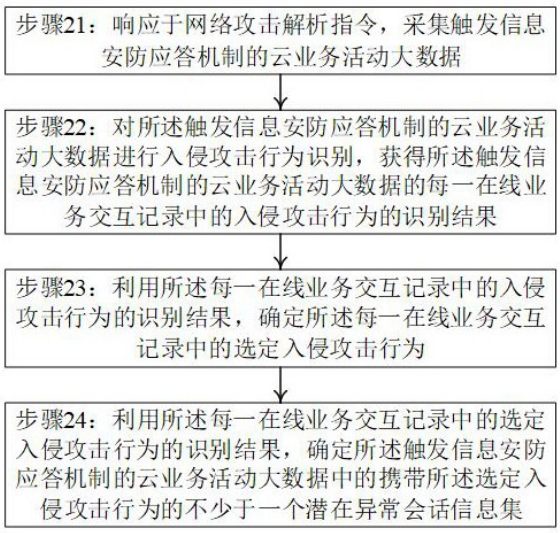
权利要求书3页 说明书16页 附图1页

(54)发明名称

应对云计算网络攻击的数据分析方法及服务器

(57)摘要

本发明提供一种应对云计算网络攻击的数据分析方法及服务器，可智能化地响应于网络攻击解析指令，采集触发信息安防应答机制的云业务活动大数据中的潜在异常会话信息集，继而能够用于引导大数据攻击分析网络基于潜在异常会话信息集对触发信息安防应答机制的云业务活动大数据进行识别，减少大数据攻击分析网络的攻击识别运算量，提高针对选定入侵攻击行为的潜在异常会话信息集的识别精度和时效性，相较于传统的手动为大数据攻击分析网络进行潜在异常会话信息集定位的思路，能够提高针对云业务活动大数据的网络攻击识别的智能化程度，并减少不必要的资源开销。



CN 114726654 B

1.一种应对云计算网络攻击的数据分析方法,其特征在于,应用于大数据分析服务器,所述方法至少包括:

响应于网络攻击解析指令,采集触发信息安防应答机制的云业务活动大数据;

对所述触发信息安防应答机制的云业务活动大数据进行入侵攻击行为识别,获得所述触发信息安防应答机制的云业务活动大数据的每一在线业务交互记录中的入侵攻击行为的识别结果;

利用所述每一在线业务交互记录中的入侵攻击行为的识别结果,确定所述每一在线业务交互记录中的选定入侵攻击行为;

利用所述每一在线业务交互记录中的选定入侵攻击行为的识别结果,确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集;

其中,所述识别结果包含交互记录时序标签和识别单元分布标签;所述利用所述每一在线业务交互记录中的选定入侵攻击行为的识别结果,确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集,包括:利用所述每一在线业务交互记录中的选定入侵攻击行为的交互记录时序标签,确定不少于一个待进行分析的在线业务交互日志,所述待进行分析的在线业务交互日志包括不少于两个存在先后关系的在线业务交互记录,并且所述待进行分析的在线业务交互日志中的每一在线业务交互记录皆携带所述选定入侵攻击行为;利用所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签,确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集的分布标签。

2.如权利要求1所述的方法,其特征在于,所述利用所述每一在线业务交互记录中的选定入侵攻击行为的交互记录时序标签,确定不少于一个待进行分析的在线业务交互日志之后,利用所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签,确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集的分布标签之前,还包括:定位所述待进行分析的在线业务交互日志中有效会话时段达到时段判定值的待进行分析的在线业务交互日志。

3.如权利要求2所述的方法,其特征在于,所述方法还包括:事先利用大数据攻击分析网络的状态触发时刻确定所述时段判定值。

4.如权利要求1所述的方法,其特征在于,所述利用所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签,确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集的分布标签,包括:

利用所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签,整合所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元,获得所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集的分布标签。

5.如权利要求4所述的方法,其特征在于,所述利用所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签,整合所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元,获得所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集的分布标签,包括:

依据指定分布标签指数降序的规则对所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元进行整理,获得已整理识别单元集;

从所述已整理识别单元集中逐一定位识别单元作为第一识别单元,直到完成对所有识别单元的定位;

针对每次定位的一个第一识别单元,逐一从所述已整理识别单元集定位顺序优先级低于所述第一识别单元的第二识别单元,确定所述第一识别单元与所述第二识别单元的分布关联指数;

确定所述第一识别单元与所述第二识别单元的分布关联指数达到设定判定值的基础上,优化所述第一识别单元,完成优化的所述第一识别单元包含优化前的所述第一识别单元和所述第二识别单元,从所述已整理识别单元集过滤所述第二识别单元;

确定所述第一识别单元与每一保留的第二识别单元的分布关联指数均低于所述设定判定值的基础上,从所述已整理识别单元集中定位下一识别单元作为第一识别单元;

确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集,所述潜在异常会话信息集包括所述已整理识别单元集中的识别单元。

6.如权利要求1所述的方法,其特征在于,所述利用所述每一在线业务交互记录中的选定入侵攻击行为的识别结果,确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集之后,所述方法还包括:

利用所述不少于一个潜在异常会话信息集的会话特征,创建原料配对指示;所述潜在异常会话信息集的会话特征包括潜在异常会话信息集的分布标签;所述原料配对指示用于引导大数据攻击分析网络评估时所需的数据原料;

利用所述原料配对指示和所述触发信息安防应答机制的云业务活动大数据,对大数据攻击分析网络进行评估。

7.如权利要求6所述的方法,其特征在于,所述潜在异常会话信息集的会话特征还包括:所述选定入侵攻击行为活跃于所述潜在异常会话信息集的时段范围;

所述利用所述不少于一个潜在异常会话信息集的会话特征,创建原料配对指示之前,所述方法还包括:利用所述选定入侵攻击行为的交互记录时序标签,确定所述选定入侵攻击行为活跃于所述潜在异常会话信息集的时段范围;

其中,所述利用所述不少于一个潜在异常会话信息集的会话特征,创建原料配对指示,包括:获取所述大数据攻击分析网络的会话特征;利用所述大数据攻击分析网络的会话特征,确定在先部署的所述大数据攻击分析网络对应的指示样例;利用所述指示样例和所述不少于一个潜在异常会话信息集的会话特征,创建所述原料配对指示。

8.一种大数据分析服务器,其特征在于,包括:存储器和处理器;所述存储器和所述处

理器耦合;所述存储器用于存储计算机程序代码,所述计算机程序代码包括计算机指令;其中,当所述处理器执行所述计算机指令时,使得所述大数据分析服务器执行如权利要求1-7中任意一项所述的方法。

应对云计算网络攻击的数据分析方法及服务器

技术领域

[0001] 本发明涉及云计算技术领域，尤其涉及一种应对云计算网络攻击的数据分析方法及服务器。

背景技术

[0002] 云计算服务的规模和应用领域的不断扩增在一定程度上增加了云计算服务遭受网络攻击的可能性，这容易导致云计算服务中的重要数据资产的丢失，还可能引发一系列负面的连锁反应。因此，针对云计算的网络攻击防护至关重要。相关的网络攻击防护处理通常基于网络攻击的检测结果实现，但是在实际应用时，由于云计算服务的复杂度通常会对大部分检测技术造成限制，使得这类检测技术很难有效施展拳脚，这样难以准确高效地实现网络攻击检测定位。

发明内容

[0003] 本发明提供一种应对云计算网络攻击的数据分析方法及服务器，为实现上述技术目的，本发明采用如下技术方案。

[0004] 第一方面是一种应对云计算网络攻击的数据分析方法，应用于大数据分析服务器，所述方法至少包括：

[0005] 响应于网络攻击解析指令，采集触发信息安防应答机制的云业务活动大数据；

[0006] 对所述触发信息安防应答机制的云业务活动大数据进行入侵攻击行为识别，获得所述触发信息安防应答机制的云业务活动大数据的每一在线业务交互记录中的入侵攻击行为的识别结果；

[0007] 利用所述每一在线业务交互记录中的入侵攻击行为的识别结果，确定所述每一在线业务交互记录中的选定入侵攻击行为；

[0008] 利用所述每一在线业务交互记录中的选定入侵攻击行为的识别结果，确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集。

[0009] 在一些可选的实施例中，所述识别结果包含入侵攻击行为分类标签；所述利用所述每一在线业务交互记录中的入侵攻击行为的识别结果，确定所述每一在线业务交互记录中的选定入侵攻击行为，包括：

[0010] 利用所述每一在线业务交互记录中的入侵攻击行为的入侵攻击行为分类标签，确定所述每一在线业务交互记录中的入侵攻击行为分类标签指向于目标分类标签的选定入侵攻击行为。

[0011] 在一些可选的实施例中，所述识别结果包含交互记录时序标签和识别单元分布标签；所述利用所述每一在线业务交互记录中的选定入侵攻击行为的识别结果，确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集，包括：

[0012] 利用所述每一在线业务交互记录中的选定入侵攻击行为的交互记录时序标签，确定不少于一个待进行分析的在线业务交互日志，所述待进行分析的在线业务交互日志包括不少于两个存在先后关系的在线业务交互记录，并且所述待进行分析的在线业务交互日志中的每一在线业务交互记录皆携带所述选定入侵攻击行为；

[0013] 利用所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签，确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集的分布标签。

[0014] 在一些可选的实施例中，所述利用所述每一在线业务交互记录中的选定入侵攻击行为的交互记录时序标签，确定不少于一个待进行分析的在线业务交互日志之后，利用所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签，确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集的分布标签之前，还包括：定位所述待进行分析的在线业务交互日志中有效会话时段达到时段判定值的待进行分析的在线业务交互日志。

[0015] 在一些可选的实施例中，所述方法还包括：事先利用大数据攻击分析网络的状态触发时刻确定所述时段判定值。

[0016] 在一些可选的实施例中，所述利用所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签，确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集的分布标签，包括：

[0017] 利用所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签，整合所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元，获得所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集的分布标签。

[0018] 在一些可选的实施例中，所述利用所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签，整合所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元，获得所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集的分布标签，包括：

[0019] 依据指定分布标签指数降序的规则对所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元进行整理，获得已整理识别单元集；

[0020] 从所述已整理识别单元集中逐一定位识别单元作为第一识别单元，直到完成对所有识别单元的定位；

[0021] 针对每次定位的一个第一识别单元，逐一从所述已整理识别单元集定位顺序优先级低于所述第一识别单元的第二识别单元，确定所述第一识别单元与所述第二识别单元的分布关联指数；

[0022] 确定所述第一识别单元与所述第二识别单元的分布关联指数达到设定判定值的

基础上，优化所述第一识别单元，完成优化的所述第一识别单元包含优化前的所述第一识别单元和所述第二识别单元，从所述已整理识别单元集过滤所述第二识别单元；

[0023] 确定所述第一识别单元与每一保留的第二识别单元的分布关联指数均低于所述设定判定值的基础上，从所述已整理识别单元集中定位下一识别单元作为第一识别单元；

[0024] 确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集，所述潜在异常会话信息集包括所述已整理识别单元集中的识别单元。

[0025] 在一些可选的实施例中，所述利用所述每一在线业务交互记录中的选定入侵攻击行为的识别结果，确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集之后，所述方法还包括：

[0026] 利用所述不少于一个潜在异常会话信息集的会话特征，创建原料配对指示；所述潜在异常会话信息集的会话特征包括潜在异常会话信息集的分布标签；所述原料配对指示用于引导大数据攻击分析网络评估时所需的数据原料；

[0027] 利用所述原料配对指示和所述触发信息安防应答机制的云业务活动大数据，对大数据攻击分析网络进行评估。

[0028] 在一些可选的实施例中，所述潜在异常会话信息集的会话特征还包括：所述选定入侵攻击行为活跃于所述潜在异常会话信息集的时段范围；

[0029] 所述利用所述不少于一个潜在异常会话信息集的会话特征，创建原料配对指示之前，所述方法还包括：利用所述选定入侵攻击行为的交互记录时序标签，确定所述选定入侵攻击行为活跃于所述潜在异常会话信息集的时段范围。

[0030] 在一些可选的实施例中，所述利用所述不少于一个潜在异常会话信息集的会话特征，创建原料配对指示，包括：

[0031] 获取所述大数据攻击分析网络的会话特征；

[0032] 利用所述大数据攻击分析网络的会话特征，确定在先部署的所述大数据攻击分析网络对应的指示样例；

[0033] 利用所述指示样例和所述不少于一个潜在异常会话信息集的会话特征，创建所述原料配对指示。

[0034] 第二方面是一种大数据分析服务器，包括存储器和处理器；所述存储器和所述处理器耦合；所述存储器用于存储计算机程序代码，所述计算机程序代码包括计算机指令；其中，当所述处理器执行所述计算机指令时，使得所述大数据分析服务器执行第一方面的方法。

[0035] 第三方面是一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序在运行时执行第一方面的方法。

[0036] 本发明中，触发信息安防应答机制的云业务活动大数据的大数据分析服务器通过对触发信息安防应答机制的云业务活动大数据进行入侵攻击行为识别，获得触发信息安防应答机制的云业务活动大数据的每一在线业务交互记录中的入侵攻击行为的识别结果。结合入侵攻击行为的识别结果，确定每一在线业务交互记录中的选定入侵攻击行为。结合每一在线业务交互记录中的选定入侵攻击行为的识别结果，从触发信息安防应答机制的云业务活动大数据中确定不少于一个潜在异常会话信息集。可智能化地响应于网络攻击解析指

令，采集触发信息安防应答机制的云业务活动大数据中的潜在异常会话信息集，继而能够用于引导大数据攻击分析网络基于潜在异常会话信息集对触发信息安防应答机制的云业务活动大数据进行识别，减少大数据攻击分析网络的攻击识别运算量，提高针对选定入侵攻击行为的潜在异常会话信息集的识别精度和时效性，相较于传统的手动为大数据攻击分析网络进行潜在异常会话信息集定位的思路，能够提高针对云业务活动大数据的网络攻击识别的智能化程度，并减少不必要的资源开销。

附图说明

[0037] 图1为本发明实施例提供的应对云计算网络攻击的数据分析方法的流程示意图。

[0038] 图2为本发明实施例提供的应对云计算网络攻击的数据分析装置的模块框图。

具体实施方式

[0039] 以下，术语“第一”、“第二”和“第三”等仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”或“第三”等的特征可以明示或者隐含地包括一个或者更多个该特征。

[0040] 图1示出了本发明实施例提供的应对云计算网络攻击的数据分析方法的流程示意图，应对云计算网络攻击的数据分析方法可以通过大数据分析服务器实现，大数据分析服务器可以包括存储器和处理器；所述存储器和所述处理器耦合；所述存储器用于存储计算机程序代码，所述计算机程序代码包括计算机指令；其中，当所述处理器执行所述计算机指令时，使得所述大数据分析服务器执行如下步骤所描述的技术方案。

[0041] 步骤21：响应于网络攻击解析指令，采集触发信息安防应答机制的云业务活动大数据。

[0042] 对于本发明实施例而言，触发信息安防应答机制的云业务活动大数据可为异地业务活动大数据，也可为本地业务活动大数据。其中，异地业务活动大数据可为通过数据采集线程或数据共享线程采集获得的业务活动大数据。本地业务活动大数据可为数据采集线程实时获得的业务活动大数据，比如，触发信息安防应答机制的云业务活动大数据的大数据分析服务器可与不少于一个数据采集线程之间通信，触发信息安防应答机制的云业务活动大数据的大数据分析服务器可将从数据采集线程获取的实时的业务活动大数据作为触发信息安防应答机制的云业务活动大数据。进一步地，触发信息安防应答机制的方式可以是基于活动时段机制触发、基于业务类型机制触发、基于活动参与者机制触发等，在此不作限定。业务活动大数据可以是跨境电商业务大数据、数字办公业务大数据、虚拟现实业务大数据等。

[0043] 在一些可能的实施例下，触发信息安防应答机制的云业务活动大数据的大数据分析服务器将外部输入的业务活动大数据作为触发信息安防应答机制的云业务活动大数据。在另一些可能的实施例下，触发信息安防应答机制的云业务活动大数据的大数据分析服务器接收协作服务器发送的业务活动大数据作为触发信息安防应答机制的云业务活动大数据。

[0044] 步骤22：对所述触发信息安防应答机制的云业务活动大数据进行入侵攻击行为识别，获得所述触发信息安防应答机制的云业务活动大数据的每一在线业务交互记录中的入

侵攻击行为的识别结果。

[0045] 对于本发明实施例而言，入侵攻击行为识别用于按序地识别触发信息安防应答机制的云业务活动大数据的在线业务交互记录中的入侵攻击行为。比如，入侵攻击行为为DDOS攻击事项，那么入侵攻击行为识别用于识别各组在线业务交互记录中的DDOS攻击事项，以及DDOS攻击事项在在线业务交互记录中的分布情况。

[0046] 对于本发明实施例而言，识别结果包含入侵攻击行为在每一在线业务交互记录中的分布情况。示例性的，识别结果包含入侵攻击行为的识别单元在各在线业务交互记录中的分布情况。识别单元的视觉呈现方式可为任意的视觉呈现方式。示例性的，识别单元的视觉呈现方式可以为表格或者知识图谱。

[0047] 以一些示例性技术方案来看待，对在线业务交互记录进行入侵攻击行为识别可通过AI机器学习模型实现。通过将携带先验知识的在线业务交互记录作为配置依据，对AI机器学习模型进行配置，使配置后的AI机器学习模型可完成对在线业务交互记录的入侵攻击行为识别，其中，先验知识包括识别单元的分布情况信息，该识别单元包含入侵攻击行为。

[0048] 以另一些示例性技术方案来看待，入侵攻击行为识别可通过以下中的一种模型实现：CNN模型、GCN模型、RNN模型等。

[0049] 以另一些示例性技术方案来看待，入侵攻击行为识别可以通过多个AI机器学习模型实现，每一AI机器学习模型分别用于从在线业务交互记录中依次识别出相异的入侵攻击行为。

[0050] 步骤23：利用所述每一在线业务交互记录中的入侵攻击行为的识别结果，确定所述每一在线业务交互记录中的选定入侵攻击行为。

[0051] 以一些示例性技术方案来看待，识别结果包含入侵攻击行为分类标签。比如，通过对在线业务交互记录进行入侵攻击行为识别，确定在线业务交互记录包括入侵攻击行为attack behavior_a和入侵攻击行为attack behavior_b，其中，入侵攻击行为attack behavior_a的入侵攻击行为分类标签为DDOS攻击事项，入侵攻击行为attack behavior_b的入侵攻击行为分类标签为木马攻击事项。

[0052] 触发信息安防应答机制的云业务活动大数据的大数据分析服务器利用每一在线业务交互记录中的入侵攻击行为的入侵攻击行为分类标签，确定每一在线业务交互记录中的入侵攻击行为分类标签指向于目标分类标签的选定入侵攻击行为。

[0053] 比如，在线业务交互记录包括入侵攻击行为attack behavior_a和入侵攻击行为attack behavior_b，其中，入侵攻击行为attack behavior_a的入侵攻击行为分类标签为DDOS攻击事项，入侵攻击行为attack behavior_b的入侵攻击行为分类标签为木马攻击事项。若目标分类标签为DDOS攻击事项，则触发信息安防应答机制的云业务活动大数据的大数据分析服务器确定入侵攻击行为attack behavior_a为选定入侵攻击行为。又比如，在线业务交互记录包括入侵攻击行为attack behavior_a和入侵攻击行为attack behavior_b，其中，入侵攻击行为attack behavior_a的入侵攻击行为分类标签为DDOS攻击事项，入侵攻击行为attack behavior_b的入侵攻击行为分类标签为木马攻击事项，大数据攻击分析网络识别的选定入侵攻击行为为木马攻击事项，那么，从每一在线业务交互记录中确定出包含入侵攻击行为attack behavior_b的所有选定入侵攻击行为。

[0054] 步骤24：利用所述每一在线业务交互记录中的选定入侵攻击行为的识别结果，确

定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集。

[0055] 对于本发明实施例而言，潜在异常会话信息集为会话风险警示报告的活跃数据集，其中，会话风险警示报告的执行方包括选定入侵攻击行为。基于此，触发信息安防应答机制的云业务活动大数据的大数据分析服务器可通过包括选定入侵攻击行为的数据信息集确定会话风险警示报告的活跃数据集(比如潜在异常会话信息集)。

[0056] 对于本发明实施例而言，潜在异常会话信息集的数目可为一个，也可以超过一个。比如，触发信息安防应答机制的云业务活动大数据的大数据分析服务器通过执行步骤24获得潜在异常会话信息集session_a、潜在异常会话信息集session_b和潜在异常会话信息集session_c。潜在异常会话信息集session_a和潜在异常会话信息集session_b均为入侵攻击行为case_A的活跃数据集，其中，潜在异常会话信息集session_a为入侵攻击行为case_A在T1~T2时段活跃时的活跃数据集，潜在异常会话信息集session_b为入侵攻击行为case_A在T3~T4时段活跃时的活跃数据集，潜在异常会话信息集session_c为入侵攻击行为case_B的活跃数据集。

[0057] 以一些示例性技术方案来看待，触发信息安防应答机制的云业务活动大数据的大数据分析服务器依据识别结果，确定触发信息安防应答机制的云业务活动大数据的各在线业务交互记录中的识别单元。整合所有识别单元所涵盖的数据信息集获得潜在异常会话信息集。

[0058] 以另一些示例性技术方案来看待，触发信息安防应答机制的云业务活动大数据的大数据分析服务器依据识别结果，确定各在线业务交互记录中的识别单元。将文本捕捉规模最大的识别单元所涵盖的数据信息集作为潜在异常会话信息集。

[0059] 比如，触发信息安防应答机制的云业务活动大数据包括在线业务交互记录record_a、在线业务交互记录record_b，其中，在线业务交互记录record_a和在线业务交互记录record_b皆携带选定入侵攻击行为，在线业务交互记录record_a中包含选定入侵攻击行为的识别单元为识别单元window unit_A，在线业务交互记录record_b中包含选定入侵攻击行为的识别单元为识别单元window unit_B。如果识别单元window unit_A所涵盖的数据信息集的内容规模大于识别单元window unit_B所涵盖的数据信息集的内容规模，则将识别单元window unit_A所涵盖的数据信息集作为潜在异常会话信息集。

[0060] 对于另外的一些示例而言，触发信息安防应答机制的云业务活动大数据的大数据分析服务器确定包括选定入侵攻击行为的数据信息集为潜在异常会话信息集。

[0061] 比如，触发信息安防应答机制的云业务活动大数据包括在线业务交互记录record_a、在线业务交互记录record_b和在线业务交互记录record_c，其中，在线业务交互记录record_a不包含选定入侵攻击行为，在线业务交互记录record_b和在线业务交互记录record_c皆携带选定入侵攻击行为。触发信息安防应答机制的云业务活动大数据的大数据分析服务器可从在线业务交互记录record_b中确定包括选定入侵攻击行为的数据信息集作为潜在异常会话信息集，触发信息安防应答机制的云业务活动大数据的大数据分析服务器也可从在线业务交互记录record_c中确定包括选定入侵攻击行为的数据信息集作为潜在异常会话信息集。

[0062] 应用于上述技术方案，触发信息安防应答机制的云业务活动大数据的大数据分析

服务器通过对触发信息安防应答机制的云业务活动大数据进行入侵攻击行为识别，获得触发信息安防应答机制的云业务活动大数据的每一在线业务交互记录中的入侵攻击行为的识别结果。结合入侵攻击行为的识别结果，确定每一在线业务交互记录中的选定入侵攻击行为。结合每一在线业务交互记录中的选定入侵攻击行为的识别结果，从触发信息安防应答机制的云业务活动大数据中确定不少于一个潜在异常会话信息集，可削减手动注释触发信息安防应答机制的云业务活动大数据用于评估时的潜在异常会话信息集的开销，且能够在一定程度上提高攻击识别的精度。

[0063] 在一些可独立的设计思路下，所述识别结果包含交互记录时序标签和识别单元分布标签。触发信息安防应答机制的云业务活动大数据的大数据分析服务器在实施步骤23时，可以参考如下相关的技术方案。

[0064] 步骤31：利用所述每一在线业务交互记录中的选定入侵攻击行为的交互记录时序标签，确定不少于一个待进行分析的在线业务交互日志。

[0065] 对于本发明实施例而言，待进行分析的在线业务交互日志包括不少于两个存在先后关系的在线业务交互记录，且待进行分析的在线业务交互日志中的每一在线业务交互记录皆携带选定入侵攻击行为。比如，选定入侵攻击行为的交互记录时序标签(比如时序先后顺序)包括标签1、标签2、标签3、标签7、标签8、标签15，可以理解，触发信息安防应答机制的云业务活动大数据中的第一组在线业务交互记录、第二组在线业务交互记录、第三组在线业务交互记录、第七组在线业务交互记录、第八组在线业务交互记录和第十五组在线业务交互记录都包括选定入侵攻击行为。这时，第一组在线业务交互记录、第二组在线业务交互记录和第三组在线业务交互记录为一个待进行分析的在线业务交互日志，第七组在线业务交互记录和第八组在线业务交互记录为一个待进行分析的在线业务交互日志。

[0066] 步骤32：利用所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签，确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集的分布标签。

[0067] 以一些示例性技术方案来看待，触发信息安防应答机制的云业务活动大数据的大数据分析服务器根据选定入侵攻击行为在一个待进行分析的在线业务交互记录的每一在线业务交互记录中的识别单元分布标签(比如识别窗口的位置信息)，确定各在线业务交互记录中的识别单元。将文本捕捉规模最大的识别单元所涵盖的数据信息集作为一个潜在异常会话信息集，进而确定一个潜在异常会话信息集的分布标签。触发信息安防应答机制的云业务活动大数据的大数据分析服务器依据不少于一个待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签，可确定不少于一个潜在异常会话信息集的分布标签。

[0068] 鉴于会话风险警示报告并不是突然产生的，而是需要保持一定时段，触发信息安防应答机制的云业务活动大数据的大数据分析服务器通过从待进行分析的在线业务交互日志中确定包含选定入侵攻击行为的数据信息集获得不少于一个潜在异常会话信息集，可提高潜在异常会话信息集的精确度及可信度。

[0069] 比如，会话风险警示报告为木马攻击事项异动。评判木马攻击事项是否异动的根据是，木马攻击事项处于异动信息集中的持续时段满足时序值(比如：4S)。

[0070] 如果触发信息安防应答机制的云业务活动大数据包括在线业务交互记录record_

a,在线业务交互记录record_b,在线业务交互记录record_c和在线业务交互记录record_d,其中,在线业务交互记录record_a为第一组在线业务交互记录,在线业务交互记录record_b为第二组在线业务交互记录,在线业务交互记录record_c为第三组在线业务交互记录,在线业务交互记录record_d为第四帧在线业务交互记录。在在线业务交互记录record_a中,木马攻击事项处于异动信息集内。在在线业务交互记录record_b和在线业务交互记录record_c中,木马攻击事项没有处于异动信息集内。在在线业务交互记录record_d中,木马攻击事项处于异动信息集内。显而易见,只通过在线业务交互记录record_a或在线业务交互记录record_d都无法评判木马攻击事项已异动,若依据在线业务交互记录record_a中包含木马攻击事项的数据信息集或在线业务交互记录record_d中包含木马攻击事项的数据信息集获得不少于一个潜在异常会话信息集,会在一定程度上造成极大的偏差。

[0071] 在一些可独立的设计思路下,触发信息安防应答机制的云业务活动大数据的大数据分析服务器在实施步骤32之前,实施步骤31之后,还可以参考如下相关的技术方案。

[0072] 步骤33:定位所述待进行分析的在线业务交互日志中有效会话时段达到时段判定值的待进行分析的在线业务交互日志。

[0073] 对于本发明实施例而言,待进行分析的在线业务交互日志的有效会话时段应当达到确认会话风险警示报告产生所需要的维持时段。触发信息安防应答机制的云业务活动大数据的大数据分析服务器在依据待进行分析的在线业务交互日志确定潜在异常会话信息集的分布标签之前,清洗掉有效会话时段低于时段判定值的待进行分析的在线业务交互日志,存储有效会话时段达到时段判定值的待进行分析的在线业务交互日志,可为降低从触发信息安防应答机制的云业务活动大数据中确定不少于一个潜在异常会话信息集的分布标签的资源浪费量,规避在大数据攻击分析时,大数据攻击分析网络对不符合会话风险警示报告产生所需要的维持时段的信息集进行识别,从而提高了触发信息安防应答机制的云业务活动大数据的分析质量。

[0074] 比如,若入侵攻击行为为异动。确定木马攻击事项异动的根据是,木马攻击事项处于异动信息集内的维持时段大于10seconds。这时,时段判定值为10seconds。若触发信息安防应答机制的云业务活动大数据为25组/second的业务活动大数据,那么待进行分析的在线业务交互日志的有效会话时段低于时段判定值可以指,待进行分析的在线业务交互日志中在线业务交互记录的数目低于125组。

[0075] 在一些可独立的设计思路下,触发信息安防应答机制的云业务活动大数据的大数据分析服务器事先利用大数据攻击分析网络的状态触发时刻确定时段判定值。对于本发明实施例而言,会话风险警示报告的产生包括风险触发方和维持时段,大数据攻击分析网络的状态触发时刻可以为产生会话风险警示报告的最小维持时段。比如,会话风险警示报告为异动,评判木马攻击事项是否异动的根据是木马攻击事项处于异动信息集内维持时段是否大于2seconds。这时,维持时段为2seconds,可以理解为大数据攻击分析网络的状态触发时刻为2seconds。

[0076] 示例性的,触发信息安防应答机制的云业务活动大数据的大数据分析服务器将大数据攻击分析网络的状态触发时刻作为时段判定值。

[0077] 在一些可独立的设计思路下,在线业务交互记录的大数据分析服务器在实施步骤

32的过程中可以参考如下相关的技术方案。

[0078] 步骤41:利用所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签,整合所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元,获得所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集的分布标签。

[0079] 对于本发明实施例而言,触发信息安防应答机制的云业务活动大数据的大数据分析服务器依据选定入侵攻击行为在一个待处理在线业务交互记录的每一在线业务交互记录中的识别单元分布标签,确定各在线业务交互记录中的识别单元。整合所有识别单元所涵盖的数据信息集获得一个潜在异常会话信息集,进而确定一个潜在异常会话信息集的分布标签。触发信息安防应答机制的云业务活动大数据的大数据分析服务器依据不少于一个待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元分布标签,可确定不少于一个潜在异常会话信息集的分布标签。

[0080] 在一些可独立的设计思路下,大数据分析服务器在实施步骤41时,可以使用nonMaximumSuppression算法整合识别单元。进一步地,触发信息安防应答机制的云业务活动大数据的大数据分析服务器在实施步骤41的过程中示例性可以参考如下相关的技术方案。

[0081] 步骤51:依据指定分布标签指数降序的规则对所述选定入侵攻击行为在所述待进行分析的在线业务交互日志的每一在线业务交互记录中的识别单元进行整理(排序),获得已整理识别单元集。

[0082] 对于本发明实施例而言,指定分布标签指数可为识别单元的分布标签中的最大值。比如,识别单元四个局部区域的分布标签分别为(para1,para3)、(para1,para5)、(para4,para3)、(para4,para5),在这种情况下,识别单元的指定分布标签指数为para5。此外,降序的规则可以理解为由大到小的顺序。

[0083] 步骤52:从所述已整理识别单元集中逐一定位识别单元作为第一识别单元,直到完成对所有识别单元的定位。

[0084] 步骤53:针对每次定位的一个第一识别单元,逐一从所述已整理识别单元集定位顺序优先级低于所述第一识别单元的第二识别单元,确定所述第一识别单元与所述第二识别单元的分布关联指数。

[0085] 对于本发明实施例而言,两个识别单元的分布关联指数表示两个识别单元的重叠部分的内容规模与两个识别单元的结合部分的内容规模的比值。比如,识别单元Identification unit_a与识别单元Identification unit_b的重叠部分的内容规模为20unit,识别单元Identification unit_a与识别单元Identification unit_b的结合部分的内容规模为50unit。此时,识别单元Identification unit_a与识别单元Identification unit_b的分布关联指数为20unit/50unit=0.4。

[0086] 步骤54:确定所述第一识别单元与所述第二识别单元的分布关联指数达到设定判定值的基础上,优化所述第一识别单元,完成优化的所述第一识别单元包含优化前的所述第一识别单元和所述第二识别单元,从所述已整理识别单元集过滤所述第二识别单元。

[0087] 示例性的,触发信息安防应答机制的云业务活动大数据的大数据分析服务器在确

定第一识别单元与第二识别单元的分布关联指数达到设定判定值的基础上，通过整合第一识别单元和第二识别单元，优化已整理识别单元集中的第一识别单元，并将第二识别单元从已整理识别单元集中过滤。

[0088] 比如，已整理识别单元集为识别单元Identification unit_a、识别单元Identification unit_b、识别单元Identification unit_c、识别单元Identification unit_d。触发信息安防应答机制的云业务活动大数据的大数据分析服务器将识别单元Identification unit_a作为第一识别单元，将识别单元Identification unit_b作为第二识别单元。若第一识别单元与第二识别单元的分布关联指数达到设定判定值，则通过整合识别单元Identification unit_a和识别单元Identification unit_b优化识别单元Identification unit_a，这时，完成优化的识别单元Identification unit_a所囊括的数据信息集为识别单元Identification unit_a所包含的数据信息集和识别单元Identification unit_b所包含的数据信息集的结合部分。触发信息安防应答机制的云业务活动大数据的大数据分析服务器还将识别单元Identification unit_b从已整理识别单元集中过滤，于是已整理识别单元集中的识别单元为识别单元Identification unit_a、识别单元Identification unit_c、识别单元Identification unit_d。

[0089] 第一识别单元与第二识别单元的分布关联指数达到设定判定值说明，第一识别单元与第二识别单元的重叠度相对较高，即第一识别单元所涵盖的选定入侵攻击行为和第二识别单元所涵盖的选定入侵攻击行为为同一个选定入侵攻击行为。比如，选定入侵攻击行为为DDOS攻击事项。如果在第一识别单元与第二识别单元的分布关联指数达到设定判定值，表明第一识别单元内的DDOS攻击事项与第二识别单元内的DDOS攻击事项为同一个DDOS攻击事项。

[0090] 由此，在第一识别单元所囊括的数据信息集和第二识别单元所囊括的数据信息集都反映选定入侵攻击行为所包含的数据信息集的基础上，触发信息安防应答机制的云业务活动大数据的大数据分析服务器在第一识别单元与第二识别单元的分布关联指数达到设定判定值的基础上，通过整合第一识别单元和第二识别单元优化第一识别单元，可提高选定入侵攻击行为所包含的数据信息集的精准度。

[0091] 步骤55:确定所述第一识别单元与每一保留的第二识别单元的分布关联指数均低于所述设定判定值的基础上，从所述已整理识别单元集中定位下一识别单元作为第一识别单元。

[0092] 比如，已整理识别单元集为识别单元Identification unit_a、识别单元Identification unit_b、识别单元Identification unit_c。触发信息安防应答机制的云业务活动大数据的大数据分析服务器将识别单元Identification unit_a作为第一识别单元，将识别单元Identification unit_b作为第二识别单元。若第一识别单元与第二识别单元的分布关联指数低于设定判定值，则触发信息安防应答机制的云业务活动大数据的大数据分析服务器确定识别单元Identification unit_a与识别单元Identification unit_c的分布关联指数(比如交集和/或并集)。

[0093] 如果识别单元Identification unit_a与识别单元Identification unit_c的分布关联指数达到设定判定值，则通过整合识别单元Identification unit_a和识别单元Identification unit_c优化识别单元Identification unit_a，此时，完成优化的识别单

元Identification unit_a所囊括的数据信息集为识别单元Identification unit_a所包含的数据信息集和识别单元Identification unit_c所包含的数据信息集的结合部分。触发信息安防应答机制的云业务活动大数据的大数据分析服务器还将识别单元Identification unit_c从已整理识别单元集中过滤，于是已整理识别单元集中的识别单元为识别单元Identification unit_a、识别单元Identification unit_b。

[0094] 如果识别单元Identification unit_a与识别单元Identification unit_c的分布关联指数低于设定判定值，则将识别单元Identification unit_b作为第一识别单元，并确定识别单元Identification unit_b与识别单元Identification unit_c的分布关联指数。

[0095] 如果识别单元Identification unit_b与识别单元Identification unit_c的分布关联指数达到设定判定值，则通过整合识别单元Identification unit_b和识别单元Identification unit_c优化识别单元Identification unit_b，此时，完成优化的识别单元Identification unit_b所囊括的数据信息集为识别单元Identification unit_b所包含的数据信息集和识别单元Identification unit_c所包含的数据信息集的结合部分。触发信息安防应答机制的云业务活动大数据的大数据分析服务器还将识别单元Identification unit_c从已整理识别单元集中过滤，于是已整理识别单元集中的识别单元为识别单元Identification unit_a、识别单元Identification unit_b。

[0096] 如果识别单元Identification unit_b与识别单元Identification unit_c的分布关联指数低于设定判定值，则确定已整理识别单元集中的识别单元为识别单元Identification unit_a、识别单元Identification unit_b和识别单元Identification unit_c。

[0097] 第一识别单元与第二识别单元的分布关联指数低于设定判定值说明，第一识别单元与第二识别单元的重叠度相对较底，即第一识别单元所涵盖的选定入侵攻击行为和第二识别单元所涵盖的选定入侵攻击行为为两个相异的选定入侵攻击行为。比如，选定入侵攻击行为为DDOS攻击事项。如果在第一识别单元与第二识别单元的分布关联指数低于设定判定值，表明第一识别单元内的DDOS攻击事项与第二识别单元内的DDOS攻击事项存在差异。

[0098] 由此一来，在第一识别单元所囊括的数据信息集和第二识别单元所囊括的数据信息集都反映选定入侵攻击行为所包含的数据信息集的基础上，触发信息安防应答机制的云业务活动大数据的大数据分析服务器在第一识别单元与第二识别单元的分布关联指数低于设定判定值的基础上，将第一识别单元和第二识别单元分别保留，可提高选定入侵攻击行为所包含的数据信息集的精准度。

[0099] 步骤56：确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集，所述潜在异常会话信息集包括所述已整理识别单元集中的识别单元。

[0100] 示例性的，触发信息安防应答机制的云业务活动大数据的大数据分析服务器将已整理识别单元集中的一个识别单元所囊括的数据信息集作为一个潜在异常会话信息集。

[0101] 在一些可独立的设计思路下，在线业务交互记录的大数据分析服务器在实施步骤24之后，还可以参考如下相关的技术方案。

[0102] 步骤61：利用所述不少于一个潜在异常会话信息集的会话特征，创建原料配对指

示。

[0103] 对于本发明实施例而言，潜在异常会话信息集的会话特征包括潜在异常会话信息集的分布标签。原料配对指示用于引导大数据攻击分析网络评估时所需的数据原料。

[0104] 对于本发明实施例而言，大数据攻击分析网络为用于识别会话风险警示报告的AI模型。可以理解的是，AI模型可以用于识别至少一种会话风险警示报告。

[0105] 比如，大数据攻击分析网络可以用于识别DDOS攻击事项聚集；又比如，大数据攻击分析网络用于识别隐私窃取；再比如，大数据攻击分析网络既可用于识别隐私窃取，又可用于识别异动。

[0106] 对于本发明实施例而言，大数据攻击分析网络评估时所需的数据原料包括潜在异常会话信息集的分布标签。比如，会话风险警示报告为异动。评判木马攻击事项是否异动的根据，为评判木马攻击事项是否在异动信息集内的异动。这时，潜在异常会话信息集的分布标签为异动信息集的分布标签，大数据攻击分析网络评估时所需的数据原料包括异动信息集的分布标签。

[0107] 示例性的，大数据攻击分析网络评估时所需的数据原料还包括状态触发时刻。比如，会话风险警示报告为异动。评判木马攻击事项是否异动的根据为，评判在异动信息集内的维持时段是否大于2seconds，若大于2seconds，则确定木马攻击事项异动。若木马攻击事项不满足在异动信息集内的维持时段大于2seconds这一要求，则确定木马攻击事项未异动。

[0108] 由此，大数据攻击分析网络评估时所需的数据原料包括：异动信息集的分布标签(可以理解为所述潜在异常会话信息集的分布标签)、状态触发时刻为2seconds。

[0109] 步骤62：利用所述原料配对指示和所述触发信息安防应答机制的云业务活动大数据，对大数据攻击分析网络进行评估。

[0110] 对于本发明实施例而言，触发信息安防应答机制的云业务活动大数据的大数据分析服务器在对大数据攻击分析网络进行处理时，通过加载原料配对指示，确定大数据攻击分析网络评估时所需的数据原料，并以大数据攻击分析网络评估时所需的数据原料为依据，使用触发信息安防应答机制的云业务活动大数据对大数据攻击分析网络进行评估。

[0111] 比如，大数据攻击分析网络评估时所需的数据原料包括：识别异动信息集的分布标签(可以理解为所述潜在异常会话信息集的分布标签)、状态触发时刻以及在线业务交互记录识别度、输出信息的细节等。

[0112] 触发信息安防应答机制的云业务活动大数据的大数据分析服务器在评估大数据攻击分析网络时，使用大数据攻击分析网络对触发信息安防应答机制的云业务活动大数据进行处理，以确定是否有木马攻击事项满足在异动信息集内的维持时段大于2seconds这一指标。若有，则确定存在异动事项，若没有，则确定不存在异动事项。

[0113] 对于本发明实施例而言，触发信息安防应答机制的云业务活动大数据的大数据分析服务器利用创建代码和触发信息安防应答机制的云业务活动大数据，对大数据攻击分析网络进行评估，可在从触发信息安防应答机制的云业务活动大数据中确定不少于一个潜在异常会话信息集的基础上，将触发信息安防应答机制的云业务活动大数据作为大数据攻击分析网络的评估为例，评估大数据攻击分析网络识别入侵攻击行为的质量。而且鉴于通过加载原料配对指示(输入信息配对参考)便可完成对大数据攻击分析网络的评估，可提高评

估大数据攻击分析网络的性能。

[0114] 在一些可独立的设计思路下，所述潜在异常会话信息集的会话特征还包括：所述选定入侵攻击行为活跃于所述潜在异常会话信息集的时段范围。

[0115] 比如，潜在异常会话信息集的时段范围为2seconds到5seconds。会话风险警示报告为异动。评判木马攻击事项是否异动的依据，是评判在异动信息集内的维持时段是否大于2seconds，若大于2seconds，则确定木马攻击事项异动。若木马攻击事项不满足在异动信息集内的维持时段大于2seconds这一要求，则确定木马攻击事项未异动。

[0116] 触发信息安防应答机制的云业务活动大数据的大数据分析服务器在测试大数据攻击分析网络时，使用大数据攻击分析网络对触发信息安防应答机制的云业务活动大数据的2seconds到5seconds内的在线业务交互日志进行处理，以确定是否有木马攻击事项符合在异动信息集内的维持时段大于2seconds这一要求。若有，则确定存在异动事项，若没有，则确定不存在异动事项。

[0117] 在一些可独立的设计思路下，触发信息安防应答机制的云业务活动大数据的大数据分析服务器在实施步骤61之前，还可以参考如下相关的技术方案。

[0118] 步骤63：利用所述选定入侵攻击行为的交互记录时序标签，确定所述选定入侵攻击行为活跃于所述潜在异常会话信息集的时段范围。

[0119] 对于本发明实施例而言，触发信息安防应答机制的云业务活动大数据的大数据分析服务器依据交互记录时序标签，可确定交互记录时序标签所对应的在线业务交互记录的有效会话时段，继而能够依据选定入侵攻击行为的交互记录时序标签，确定潜在异常会话信息集对应的时段范围。

[0120] 如此一来，在对大数据攻击分析网络进行处理时，可以指定大数据攻击分析网络识别触发信息安防应答机制的云业务活动大数据的潜在异常会话信息集和时段范围，在大数据攻击分析网络输出识别结果后，分析识别结果是否准确。或者，在对大数据攻击分析网络进行处理时，指定大数据攻击分析网络识别触发信息安防应答机制的云业务活动大数据的潜在异常会话信息集，在大数据攻击分析网络输出识别结果后，分析识别结果包含的识别到风险事项的时段与所述潜在异常会话信息集的时段范围是否一致。

[0121] 在一些可独立的设计思路下，触发信息安防应答机制的云业务活动大数据的大数据分析服务器在实施步骤61的过程中可以参考如下相关的技术方案。

[0122] 步骤71：获取所述大数据攻击分析网络的会话特征。

[0123] 对于本发明实施例而言，大数据攻击分析网络的会话特征包括大数据攻击分析网络所能识别的会话风险警示报告的决策数据。比如，大数据攻击分析网络可用于识别异动。评判异动的依据是，评判木马攻击事项是否在异动信息集内的木马攻击事项异常时段是否达到状态触发时刻。这时，异动的决策数据包括异动信息集的分布标签和状态触发时刻。

[0124] 步骤72：利用所述大数据攻击分析网络的会话特征，确定在先部署的所述大数据攻击分析网络对应的指示样例。

[0125] 对于本发明实施例而言，指示样例用于创建原料配对指示。相异的指示样例用于创建用于评估不同大数据攻击分析网络的原料配对指示。

[0126] 比如，指示样例example_a用于创建信息为潜在异常会话信息集的分布标签和状态触发时刻的大数据攻击分析网络的原料配对指示。

[0127] 示例性的，触发信息安防应答机制的云业务活动大数据的大数据分析服务器的存储区中包括不少于一个在先部署的指示样例。触发信息安防应答机制的云业务活动大数据的大数据分析服务器利用大数据攻击分析网络的会话特征，确定与大数据攻击分析网络对应的指示样例。

[0128] 步骤73：利用所述指示样例和所述不少于一个潜在异常会话信息集的会话特征，创建所述原料配对指示。

[0129] 基于上述相关内容，可完成对触发信息安防应答机制的云业务活动大数据的注释，获得触发信息安防应答机制的云业务活动大数据的先验知识。

[0130] 比如信息安防平台platform欲确定若干检测异动质量较佳的AI模型。在获得AI模型识别异动的性能之前，需要将数据采集线程采集到的多个触发信息安防应答机制的云业务活动大数据中的潜在异常会话信息集的分布标签进行注释。鉴于触发信息安防应答机制的云业务活动大数据的数目较多，且触发信息安防应答机制的云业务活动大数据的有效会话时段较长，信息安防平台platform采用相关内容对触发信息安防应答机制的云业务活动大数据进行处理，可从触发信息安防应答机制的云业务活动大数据中确定不少于一个潜在异常会话信息集的分布标签。示例性的，信息安防平台platform可对触发信息安防应答机制的云业务活动大数据进行处理，从触发信息安防应答机制的云业务活动大数据中确定不少于一个潜在异常会话信息集的分布标签，并将不少于一个潜在异常会话信息集的分布标签作为先验知识。在获得触发信息安防应答机制的云业务活动大数据的先验知识后，还可基于相关内容完成对AI模型的评估处理。

[0131] 比如，可依据大数据攻击分析网络的会话特征确定在先部署的大数据攻击分析网络对应的指示样例。利用指示样例和不少于一个潜在异常会话信息集的会话特征，创建原料配对指示。进而利用原料配对指示和触发信息安防应答机制的云业务活动大数据，对待触发信息安防应答机制的云业务活动大数据进行评估，获得评估信息。信息安防平台platform继而能够依据该评估信息，确定大数据攻击分析网络识别异动的性能。

[0132] 在一些可能的实施例下，在确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集之后，该方法还可以包括如下内容：基于所述潜在异常会话信息集对所述选定入侵攻击行为进行攻击意向分析，得到所述选定入侵攻击行为的攻击意向特征；利用所述攻击意向特征生成攻击防护策略；激活所述攻击防护策略。

[0133] 在本发明实施例中，攻击意向分析能够挖掘出选定入侵攻击行为的攻击意图或者攻击偏好，通过攻击意向特征记录，能够实现与上述人工智能模型的适配性，这样可以在上述相关人工智能模型的基础上进行网络层添加和部署，从而提高挖掘攻击意向特征的效率和精度，并且在一定程度上提高获取得到的攻击意向特征与整体业务环境的适配性，进而可以确保生成的攻击防护策略的针对性和可信度，从而可以通过激活攻击防护策略进行有效的网络攻击防护。

[0134] 在一些可能的实施例中，基于所述潜在异常会话信息集对所述选定入侵攻击行为进行攻击意向分析，得到所述选定入侵攻击行为的攻击意向特征，可以通过如下技术方案实现：对所述潜在异常会话信息集中的多个潜在异常会话信息分别进行被动攻击意向挖掘和主动攻击意向挖掘，得到被动攻击意向挖掘知识簇和主动攻击意向挖掘知识簇；通过预

设知识处理层layer1，对所述被动攻击意向挖掘知识簇进行第一噪声清洗，得到包括有被动攻击意向的知识关系网knowledge network1；通过预设知识处理层layer2，对所述主动攻击意向挖掘知识簇进行第二噪声清洗，得到包括有主动攻击意向的知识关系网knowledge network2；基于所述知识关系网knowledge network1和所述知识关系网knowledge network2进行组合，得到所述潜在异常会话信息集中与目标攻击意向相匹配的潜在异常会话描述；所述目标攻击意向包括被动攻击意向和主动攻击意向中的至少一种，基于潜在异常会话描述确定所述选定入侵攻击行为的攻击意向特征。

[0135] 在本发明实施例中，预设知识处理层layer1以及预设知识处理层layer2可以在上述相关的人工智能模型的基础上额外增设，这样能够实现对不同类型的攻击意向的挖掘分析，从而确保潜在异常会话描述的完整性，继而准确完整地确定出选定入侵攻击行为的攻击意向特征。

[0136] 在一些可能的实施例中，所述对所述潜在异常会话信息集中的多个潜在异常会话信息分别进行被动攻击意向挖掘和主动攻击意向挖掘，得到被动攻击意向挖掘知识簇和主动攻击意向挖掘知识簇，包括：对所述潜在异常会话信息集中的多个潜在异常会话信息分别进行被动攻击意向挖掘，得到各个潜在异常会话信息中的被动攻击意向挖掘窗口、以及各被动攻击意向挖掘窗口所对应的基于意向类别；基于各潜在异常会话信息中的被动攻击意向挖掘窗口和相应的基于意向类别，确定被动攻击意向挖掘知识簇；对所述潜在异常会话信息集中的多个潜在异常会话信息分别进行主动攻击意向挖掘，得到主动攻击意向挖掘知识簇。

[0137] 在一些可能的实施例中，所述对所述潜在异常会话信息集中的多个潜在异常会话信息分别进行主动攻击意向挖掘，得到主动攻击意向挖掘知识簇，包括：对所述潜在异常会话信息中的多个潜在异常会话信息分别进行入侵节点挖掘，得到各潜在异常会话信息分别对应的入侵节点挖掘信息；对所述潜在异常会话信息中的多个潜在异常会话信息分别进行入侵场景挖掘，得到各潜在异常会话信息分别对应的入侵场景挖掘信息；将对应于相同攻击事项的入侵节点挖掘信息和入侵场景挖掘信息进行关联；基于所述潜在异常会话信息中与目标入侵节点挖掘信息相关联的入侵场景挖掘信息进行主动攻击意向挖掘处理，得到主动攻击意向挖掘知识簇。

[0138] 在一些可能的实施例中，所述通过预设知识处理层layer1，对所述被动攻击意向挖掘知识簇进行第一噪声清洗，得到包括有被动攻击意向的知识关系网knowledge network1，包括：对所述被动攻击意向挖掘知识簇中的每个潜在异常会话信息分别进行意向类别处理，得到每个潜在异常会话信息逐一匹配的独占意向类别；基于每个潜在异常会话信息中与相应独占意向类别对应的被动攻击意向挖掘窗口的规模，分别进行攻击意向挖掘窗口优化处理，得到更新后的被动攻击意向挖掘知识簇；对所述更新后的被动攻击意向挖掘知识簇进行清洗处理，得到多个包括有被动攻击意向的第一待定知识关系网；根据各所述第一待定知识关系网分别所属的被动攻击意向类别，对属于相同被动攻击意向类别的第一待定知识关系网进行关系网调整，得到包括有被动攻击意向的知识关系网knowledge network1。

[0139] 在一些可能的实施例中，所述对所述被动攻击意向挖掘知识簇中的每个潜在异常会话信息分别进行意向类别处理，得到每个潜在异常会话信息逐一匹配的独占意向类别，

包括:针对所述被动攻击意向挖掘知识簇中的每个潜在异常会话信息,当潜在异常会话信息的基于意向类别的数目为不少于两个时,获取每个基于意向类别的意向类别权重;当意向类别权重最大的基于意向类别为一个时,将所述意向类别权重最大的基于意向类别作为相应潜在异常会话信息的独占意向类别;当所述意向类别权重最大的基于意向类别为不少于两个时,针对每个意向类别权重最大的基于意向类别,获取对应的被动攻击意向挖掘窗口的窗口权重;根据最大的窗口权重所对应的基于意向类别,确定相应潜在异常会话信息所对应的独占意向类别。

[0140] 基于同样的发明构思,图2示出了本发明实施例提供的应对云计算网络攻击的数据分析装置的模块框图,应对云计算网络攻击的数据分析装置可以包括实施图1所示的相关方法步骤的攻击行为识别模块21,用于响应于网络攻击解析指令,采集触发信息安防应答机制的云业务活动大数据;对所述触发信息安防应答机制的云业务活动大数据进行入侵攻击行为识别,获得所述触发信息安防应答机制的云业务活动大数据的每一在线业务交互记录中的入侵攻击行为的识别结果;异常会话定位模块22,用于利用所述每一在线业务交互记录中的入侵攻击行为的识别结果,确定所述每一在线业务交互记录中的选定入侵攻击行为;利用所述每一在线业务交互记录中的选定入侵攻击行为的识别结果,确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集。

[0141] 应用于本发明的相关实施例可以达到如下技术效果:触发信息安防应答机制的云业务活动大数据的大数据分析服务器通过对触发信息安防应答机制的云业务活动大数据进行入侵攻击行为识别,获得触发信息安防应答机制的云业务活动大数据的每一在线业务交互记录中的入侵攻击行为的识别结果。结合入侵攻击行为的识别结果,确定每一在线业务交互记录中的选定入侵攻击行为。结合每一在线业务交互记录中的选定入侵攻击行为的识别结果,从触发信息安防应答机制的云业务活动大数据中确定不少于一个潜在异常会话信息集。可智能化地响应于网络攻击解析指令,采集触发信息安防应答机制的云业务活动大数据中的潜在异常会话信息集,继而能够用于引导大数据攻击分析网络基于潜在异常会话信息集对触发信息安防应答机制的云业务活动大数据进行识别,减少大数据攻击分析网络的攻击识别运算量,提高针对选定入侵攻击行为的潜在异常会话信息集的识别精度和时效性,相较于传统的手动为大数据攻击分析网络进行潜在异常会话信息集定位的思路,能够提高针对云业务活动大数据的网络攻击识别的智能化程度,并减少不必要的资源开销。

[0142] 以上所述,仅为本发明的具体实施方式。熟悉本技术领域的技术人员根据本发明提供的具体实施方式,可想到变化或替换,都应涵盖在本发明的保护范围之内。

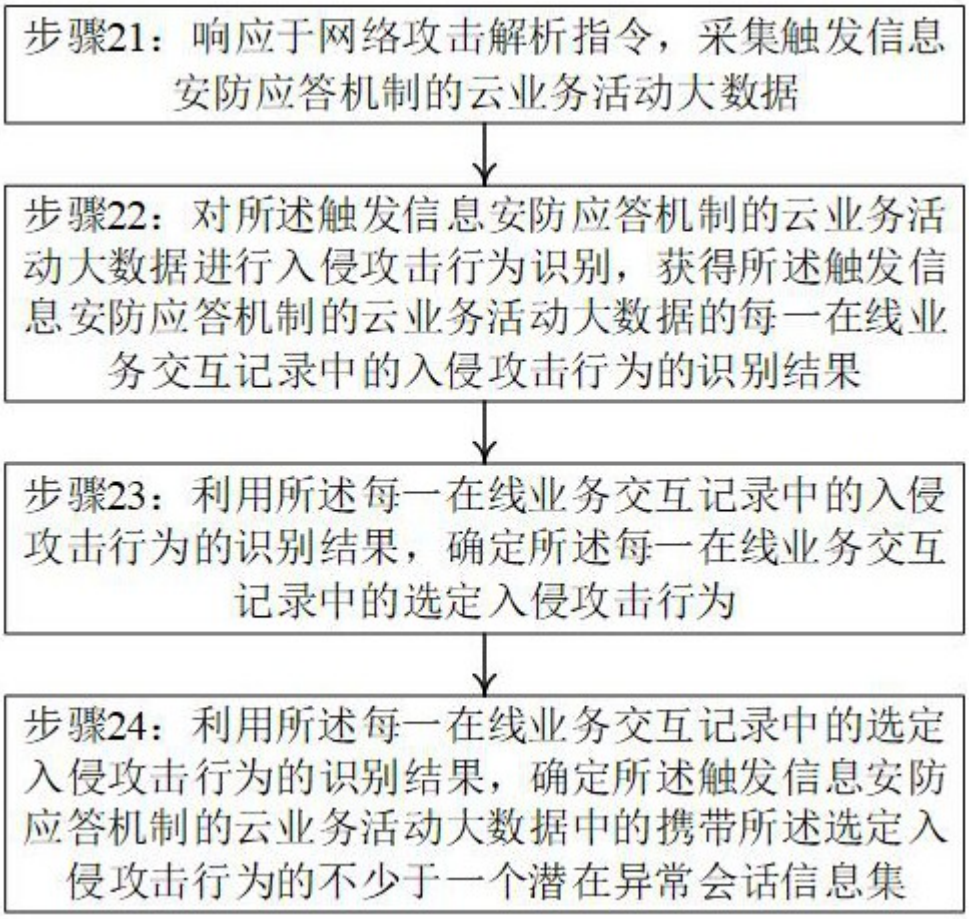

步骤21：响应于网络攻击解析指令，采集触发信息安防应答机制的云业务活动大数据
步骤22：对所述触发信息安防应答机制的云业务活动大数据进行入侵攻击行为识别，获得所述触发信息安防应答机制的云业务活动大数据的每一在线业务交互记录中的入侵攻击行为的识别结果
步骤23：利用所述每一在线业务交互记录中的入侵攻击行为的识别结果，确定所述每一在线业务交互记录中的选定入侵攻击行为
步骤24：利用所述每一在线业务交互记录中的选定入侵攻击行为的识别结果，确定所述触发信息安防应答机制的云业务活动大数据中的携带所述选定入侵攻击行为的不少于一个潜在异常会话信息集

图1

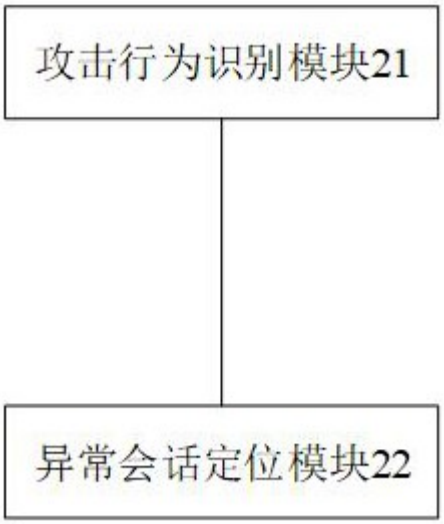

攻击行为识别模块21
异常会话定位模块22

图2