(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 113949577 A
(43)申请公布日 2022.01.18

(21)申请号 202111217358.6

(22)申请日 2021.10.19

(71)申请人 广州酷风技术开发有限公司
地址 523000 广东省广州市白云区棠景街机场路585号8楼1021

(72)发明人 闫传红 覃麟凯 许胜楠 陈伟宗

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/10(2022.01)
G06K 9/62(2022.01)
G06N 3/04(2006.01)
G06N 3/08(2006.01)

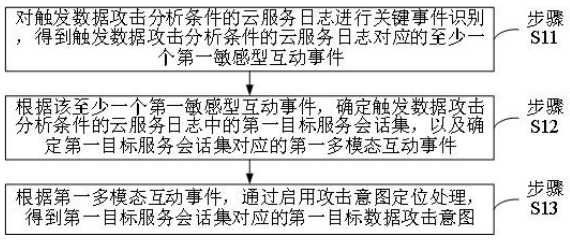
权利要求书3页 说明书24页 附图1页

(54)发明名称

一种应用于云服务的数据攻击分析方法及服务器

(57)摘要

本申请涉及云服务和数据攻击分析技术领域，具体而言，涉及应用于云服务的数据攻击分析方法及服务器，由于在攻击意图分析进程中，服务事件定位处理可以对随机多变的服务环境进行分析，因此，根据该至少一个第一敏感型互动事件，确定触发数据攻击分析条件的云服务日志中的第一目标服务会话集，以及确定第一目标服务会话集对应的第一多模态互动事件，也即得到了在攻击意图分析进程中的意图分析结果，进而根据第一多模态互动事件，通过启用攻击意图定位处理，使得可以得到第一目标服务会话集在服务场景中对应的第一目标数据攻击意图，从而可以实现高效精准地对触发数据攻击分析条件的云服务日志中不同状态的服务会话集的意图分析。



CN 113949577 A

1.一种应用于云服务的数据攻击分析方法,其特征在于,应用于数据攻击分析服务器,所述方法至少包括:

对触发数据攻击分析条件的云服务日志进行关键事件识别,得到所述触发数据攻击分析条件的云服务日志对应的至少一个第一敏感型互动事件;

基于所述至少一个第一敏感型互动事件,确定所述触发数据攻击分析条件的云服务日志中的第一目标服务会话集,以及确定所述第一目标服务会话集对应的第一多模态互动事件;

基于所述第一多模态互动事件,通过启用攻击意图定位处理,得到所述第一目标服务会话集对应的第一目标数据攻击意图。

2.如权利要求1所述的方法,其特征在于,所述第一敏感型互动事件包括第一敏感型互动事件描述;所述基于所述至少一个第一敏感型互动事件,确定所述触发数据攻击分析条件的云服务日志中的第一目标服务会话集,包括:

利用至少一个第一敏感型互动事件描述,对所述触发数据攻击分析条件的云服务日志中的业务会话消息进行第一差异化处理,得到所述触发数据攻击分析条件的云服务日志中的第一原始服务会话集;

基于所述至少一个第一敏感型互动事件描述,对所述触发数据攻击分析条件的云服务日志中的业务会话消息进行第二差异化处理,得到所述触发数据攻击分析条件的云服务日志中的第一热点会话集,所述第一热点会话集对应于所述第一原始服务会话集的热点会话时段;

基于所述第一原始服务会话集和所述第一热点会话集,确定所述第一目标服务会话集。

3.如权利要求1或2所述的方法,其特征在于,所述第一敏感型互动事件包括第一敏感型互动事件描述,所述第一多模态互动事件包括第一多模态互动事件表达;所述基于所述至少一个第一敏感型互动事件,确定所述第一目标服务会话集对应的第一多模态互动事件,包括:

利用至少一个第一敏感型互动事件描述,确定所述触发数据攻击分析条件的云服务日志中各业务会话消息对应的多模态互动事件表达;

基于所述各业务会话消息对应的多模态互动事件表达和所述第一目标服务会话集的分布情况,确定所述第一多模态互动事件表达。

4.如权利要求3所述的方法,其特征在于,所述基于所述第一多模态互动事件,通过启用攻击意图定位处理,得到所述第一目标服务会话集对应的第一目标数据攻击意图,包括:

依据对所述第一多模态互动事件表达启用攻击意图定位处理,得到所述第一目标服务会话集对应的多个数据攻击意图;

依据对所述多个数据攻击意图启用迭代优化处理,得到所述第一目标数据攻击意图。

5.如权利要求1所述的方法,其特征在于,所述应用于云服务的数据攻击分析方法通过意图分析学习模型实施;所述意图分析学习模型的训练范例包括:范例云服务日志、所述范例云服务日志中的参考服务会话集、所述参考服务会话集对应的参考多模态互动事件;

所述方法还包括:

通过原始学习模型对所述范例云服务日志进行关键事件识别,得到所述范例云服务日

志对应的至少一个第二敏感型互动事件；

基于所述至少一个第二敏感型互动事件，确定所述范例云服务日志中的第二目标服务会话集，以及确定所述第二目标服务会话集对应的第二多模态互动事件；

基于所述第二多模态互动事件，通过启用攻击意图定位处理，得到所述第二目标服务会话集对应的第二目标数据攻击意图；

基于所述第二目标服务会话集和所述参考服务会话集确定第一意图解析评价，以及基于所述第二目标数据攻击意图和所述参考多模态互动事件，确定第二意图解析评价；

基于所述第一意图解析评价和所述第二意图解析评价，改进所述原始学习模型的模型变量，得到完成训练的所述意图分析学习模型；

其中，所述训练范例中还包括所述参考服务会话集对应的多个参考服务主题；

所述方法还包括：

基于所述多个参考服务主题，对所述参考服务会话集进行服务主题筛选处理，得到多个已筛选服务主题，存在关联的所述已筛选服务主题之间的关键词一致；

依据对所述多个已筛选服务主题启用事件解析处理，得到所述参考多模态互动事件；

其中，所述参考多模态互动事件包括参考多模态互动事件表达；所述依据对所述多个已筛选服务主题启用事件解析处理，得到所述参考多模态互动事件，包括：

通过确定所述多个已筛选服务主题中的原始已筛选服务主题和各所述已筛选服务主题之间的先后关系，得到所述多个已筛选服务主题对应的服务主题集；

依据对所述服务主题集启用事件解析处理，得到所述参考多模态互动事件表达。

6.如权利要求5所述的方法，其特征在于，所述基于所述第二目标数据攻击意图和所述参考多模态互动事件，确定第二意图解析评价，包括：

依据对所述参考多模态互动事件表达启用攻击意图定位处理，得到所述参考服务会话集对应的第三目标数据攻击意图；

基于所述第二目标数据攻击意图和所述第三目标数据攻击意图之间的比较结果，确定所述第二意图解析评价。

7.如权利要求6所述的方法，其特征在于，所述第二敏感型互动事件包括第二敏感型互动事件描述；所述基于所述至少一个第二敏感型互动事件，确定所述范例云服务日志中的第二目标服务会话集，包括：

利用至少一个第二敏感型互动事件描述，对所述范例云服务日志中的业务会话消息进行第三差异化处理，得到所述范例云服务日志中的第二原始服务会话集；

基于所述至少一个第二敏感型互动事件描述，对所述范例云服务日志中的业务会话消息进行第四差异化处理，得到所述范例云服务日志中的第二热点会话集，所述第二热点会话集对应于所述第二原始服务会话集的热点会话时段；

基于所述第二原始服务会话集和所述第二热点会话集，确定所述第二目标服务会话集。

8.如权利要求7所述的方法，其特征在于，所述基于所述第二目标服务会话集和所述参考服务会话集确定第一意图解析评价，包括：

基于所述参考服务会话集和设定调整指示，确定参考热点会话集，所述参考热点会话集对应于所述参考服务会话集的热点会话时段；

基于所述第二目标服务会话集和所述参考服务会话集之间的比较结果，确定第三意图解析评价；

基于所述第二热点会话集和所述参考热点会话集之间的比较结果，确定第四意图解析评价；

基于所述第三意图解析评价和所述第四意图解析评价，确定所述第一意图解析评价。

9.一种数据攻击分析服务器，其特征在于，包括处理器、通信总线和存储器；所述处理器和所述存储器通过所述通信总线通信，所述处理器从所述存储器中读取计算机程序并运行，以执行权利要求1-8任一项所述的方法。

10.一种计算机存储介质，其特征在于，所述计算机存储介质存储有计算机程序，所述计算机程序在运行时实现权利要求1-8任一项所述的方法。

一种应用于云服务的数据攻击分析方法及服务器

技术领域

[0001] 本申请实施例涉及云服务和数据攻击分析技术领域，具体涉及一种应用于云服务的数据攻击分析方法及服务器。

背景技术

[0002] 云服务(Cloud Serving)是基于互联网的相关服务的增加、使用和交互模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源，也可以理解为通过网络以按需、易扩展的方式获得所需服务，该服务可以是IT和软件、互联网相关，也可是其他服务。云服务的不断发展给提高了各类业务服务的处理效率，但随之而来的数据信息安全问题却不容忽视。近年来，网络攻击所造成的数据信息安全事件层出不穷，给个人或企业造成了或大或小的损失。然而针对网络攻击的分析定位技术却表现出精度低下的缺陷，这样难以实现对网络攻击的准确定位分析。

发明内容

[0003] 有鉴于此，本申请实施例提供了一种应用于云服务的数据攻击分析方法及服务器。

[0004] 本申请实施例提供了一种应用于云服务的数据攻击分析方法，应用于数据攻击分析服务器，所述方法至少包括：对触发数据攻击分析条件的云服务日志进行关键事件识别，得到所述触发数据攻击分析条件的云服务日志对应的至少一个第一敏感型互动事件；基于所述至少一个第一敏感型互动事件，确定所述触发数据攻击分析条件的云服务日志中的第一目标服务会话集，以及确定所述第一目标服务会话集对应的第一多模态互动事件；基于所述第一多模态互动事件，通过启用攻击意图定位处理，得到所述第一目标服务会话集对应的第一目标数据攻击意图。

[0005] 在一些可独立实施的设计思路下，所述第一敏感型互动事件包括第一敏感型互动事件描述；所述基于所述至少一个第一敏感型互动事件，确定所述触发数据攻击分析条件的云服务日志中的第一目标服务会话集，包括：利用至少一个第一敏感型互动事件描述，对所述触发数据攻击分析条件的云服务日志中的业务会话消息进行第一差异化处理，得到所述触发数据攻击分析条件的云服务日志中的第一原始服务会话集；基于所述至少一个第一敏感型互动事件描述，对所述触发数据攻击分析条件的云服务日志中的业务会话消息进行第二差异化处理，得到所述触发数据攻击分析条件的云服务日志中的第一热点会话集，所述第一热点会话集对应于所述第一原始服务会话集的热点会话时段；基于所述第一原始服务会话集和所述第一热点会话集，确定所述第一目标服务会话集。

[0006] 在一些可独立实施的设计思路下，所述第一敏感型互动事件包括第一敏感型互动事件描述，所述第一多模态互动事件包括第一多模态互动事件表达；所述基于所述至少一个第一敏感型互动事件，确定所述第一目标服务会话集对应的第一多模态互动事件，包括：利用至少一个第一敏感型互动事件描述，确定所述触发数据攻击分析条件的云服务日志中

各业务会话消息对应的多模态互动事件表达;基于所述各业务会话消息对应的多模态互动事件表达和所述第一目标服务会话集的分布情况,确定所述第一多模态互动事件表达。

[0007] 在一些可独立实施的设计思路下,所述基于所述第一多模态互动事件,通过启用攻击意图定位处理,得到所述第一目标服务会话集对应的第一目标数据攻击意图,包括:依据对所述第一多模态互动事件表达启用攻击意图定位处理,得到所述第一目标服务会话集对应的多个数据攻击意图;依据对所述多个数据攻击意图启用迭代优化处理,得到所述第一目标数据攻击意图。

[0008] 在一些可独立实施的设计思路下,所述应用于云服务的数据攻击分析方法通过意图分析学习模型实施;所述意图分析学习模型的训练范例包括:范例云服务日志、所述范例云服务日志中的参考服务会话集、所述参考服务会话集对应的参考多模态互动事件;所述方法还包括:通过原始学习模型对所述范例云服务日志进行关键事件识别,得到所述范例云服务日志对应的至少一个第二敏感型互动事件;基于所述至少一个第二敏感型互动事件,确定所述范例云服务日志中的第二目标服务会话集,以及确定所述第二目标服务会话集对应的第二多模态互动事件;基于所述第二多模态互动事件,通过启用攻击意图定位处理,得到所述第二目标服务会话集对应的第二目标数据攻击意图;基于所述第二目标服务会话集和所述参考服务会话集确定第一意图解析评价,以及基于所述第二目标数据攻击意图和所述参考多模态互动事件,确定第二意图解析评价;基于所述第一意图解析评价和所述第二意图解析评价,改进所述原始学习模型的模型变量,得到完成训练的所述意图分析学习模型;

在一些可独立实施的设计思路下,所述训练范例中还包括所述参考服务会话集对应的多个参考服务主题;所述方法还包括:基于所述多个参考服务主题,对所述参考服务会话集进行服务主题筛选处理,得到多个已筛选服务主题,存在关联的所述已筛选服务主题之间的关键词一致;依据对所述多个已筛选服务主题启用事件解析处理,得到所述参考多模态互动事件。

[0009] 在一些可独立实施的设计思路下,所述参考多模态互动事件包括参考多模态互动事件表达;所述依据对所述多个已筛选服务主题启用事件解析处理,得到所述参考多模态互动事件,包括:通过确定所述多个已筛选服务主题中的原始已筛选服务主题和各所述已筛选服务主题之间的先后关系,得到所述多个已筛选服务主题对应的服务主题集;依据对所述服务主题集启用事件解析处理,得到所述参考多模态互动事件表达。

[0010] 在一些可独立实施的设计思路下,所述基于所述第二目标数据攻击意图和所述参考多模态互动事件,确定第二意图解析评价,包括:依据对所述参考多模态互动事件表达启用攻击意图定位处理,得到所述参考服务会话集对应的第三目标数据攻击意图;基于所述第二目标数据攻击意图和所述第三目标数据攻击意图之间的比较结果,确定所述第二意图解析评价。

[0011] 在一些可独立实施的设计思路下,所述第二敏感型互动事件包括第二敏感型互动事件描述;所述基于所述至少一个第二敏感型互动事件,确定所述范例云服务日志中的第二目标服务会话集,包括:利用至少一个第二敏感型互动事件描述,对所述范例云服务日志中的业务会话消息进行第三差异化处理,得到所述范例云服务日志中的第二原始服务会话集;基于所述至少一个第二敏感型互动事件描述,对所述范例云服务日志中的业务会话消

息进行第四差异化处理，得到所述范例云服务日志中的第二热点会话集，所述第二热点会话集对应于所述第二原始服务会话集的热点会话时段；基于所述第二原始服务会话集和所述第二热点会话集，确定所述第二目标服务会话集。

[0012] 在一些可独立实施的设计思路下，所述基于所述第二目标服务会话集和所述参考服务会话集确定第一意图解析评价，包括：基于所述参考服务会话集和设定调整指示，确定参考热点会话集，所述参考热点会话集对应于所述参考服务会话集的热点会话时段；基于所述第二目标服务会话集和所述参考服务会话集之间的比较结果，确定第三意图解析评价；基于所述第二热点会话集和所述参考热点会话集之间的比较结果，确定第四意图解析评价；基于所述第三意图解析评价和所述第四意图解析评价，确定所述第一意图解析评价。

[0013] 本申请实施例还提供了一种数据攻击分析服务器，包括处理器、通信总线和存储器；所述处理器和所述存储器通过所述通信总线通信，所述处理器从所述存储器中读取计算机程序并运行，以执行上述的方法。

[0014] 本申请实施例还提供了一种计算机存储介质，所述计算机存储介质存储有计算机程序，所述计算机程序在运行时实现上述的方法。

[0015] 在本申请实施例中，对触发数据攻击分析条件的云服务日志进行关键事件识别，得到触发数据攻击分析条件的云服务日志对应的至少一个第一敏感型互动事件，由于在攻击意图分析进程中，服务事件定位处理可以对随机多变的服务环境进行分析，因此，根据该至少一个第一敏感型互动事件，确定触发数据攻击分析条件的云服务日志中的第一目标服务会话集，以及确定第一目标服务会话集对应的第一多模态互动事件，也即得到了在攻击意图分析进程中的意图分析结果，进而根据第一多模态互动事件，通过启用攻击意图定位处理，使得可以得到第一目标服务会话集在服务场景中对应的第一目标数据攻击意图，从而可以实现高效精准地对触发数据攻击分析条件的云服务日志中不同状态的服务会话集的意图分析。

附图说明

[0016] 图1为本申请实施例所提供的一种数据攻击分析服务器的方框示意图。

[0017] 图2为本申请实施例所提供的一种应用于云服务的数据攻击分析方法的流程图。

[0018] 图3为本申请实施例所提供的一种应用于云服务的数据攻击分析装置的框图。

具体实施方式

[0019] 图1示出了本申请实施例所提供的一种数据攻击分析服务器10的方框示意图。本申请实施例中的数据攻击分析服务器10可以为具有数据存储、传输、处理功能的服务端，如图1所示，数据攻击分析服务器10包括：存储器11、处理器12、通信总线13和应用于云服务的数据攻击分析装置20。

[0020] 存储器11、处理器12和通信总线13之间直接或间接地电性连接，以实现数据的传输或交互。例如，这些元件互相之间可以通过一条或多条通讯总线或信号线实现电性连接。存储器11中存储有应用于云服务的数据攻击分析装置20，所述应用于云服务的数据攻击分析装置20包括至少一个可以软件或固件(firmware)的形式储存于所述存储器11中的软件功能模块，所述处理器12通过运行存储在存储器11内的软件程序以及模块，例如本申请实

施例中的应用于云服务的数据攻击分析装置20，从而执行各种功能应用以及数据处理，即实现本申请实施例中的应用于云服务的数据攻击分析方法。

[0021] 可以理解，图1所示的结构仅为示意，数据攻击分析服务器10还可包括比图1中所示更多或者更少的组件，或者具有与图1所示不同的配置。图1中所示的各组件可以采用硬件、软件或其组合实现。

[0022] 本申请实施例还提供了一种计算机存储介质，所述计算机存储介质存储有计算机程序，所述计算机程序在运行时实现上述的方法。

[0023] 图2示出了本申请实施例所提供的一种应用于云服务的数据攻击分析的流程图。所述方法有关的流程所定义的方法步骤应用于数据攻击分析服务器10，可以由所述处理器12实现，所述方法包括如下内容。

[0024] 对于步骤S11而言，对触发数据攻击分析条件的云服务日志进行关键事件识别，得到触发数据攻击分析条件的云服务日志对应的至少一个第一敏感型互动事件。

[0025] 对于步骤S12而言，根据该至少一个第一敏感型互动事件，确定触发数据攻击分析条件的云服务日志中的第一目标服务会话集，以及确定第一目标服务会话集对应的第一多模态互动事件。

[0026] 对于步骤S13而言，根据第一多模态互动事件，通过启用攻击意图定位处理，得到第一目标服务会话集对应的第一目标数据攻击意图。

[0027] 示例性的，在步骤S11中，触发数据攻击分析条件的云服务日志可以理解为待检测的云服务日志，云服务所涉及的领域包括但不限于支付领域、办公领域、医疗领域、企业服务领域、游戏领域、智慧城市领域和物流订单领域等。进一步地，数据攻击分析条件可以是针对设定时段设置的，也可以是针对设定服务场景设置的，还可以是针对设定操作行为设置的，本申请实施例不作限制。进一步地，关键事件识别可以理解为特征提取或者特征挖掘，相应的，敏感型互动事件可以是存在异常的或者需要重点关注的互动事件，互动事件对应于不同的业务领域可以作不同的理解，本申请实施例不进行穷举。

[0028] 示例性的，在步骤S12中，目标服务会话集可以理解为云服务日志的一部分，从某种意义上可以视为局部日志或者日志片段，当然也可以理解为多个会话消息的汇总结果，本申请实施例不作限制。此外，多模态互动事件可以从多个层面或者多个维度反应对应互动事件的相关特征和特性，以尽可能涵盖完整的、能够用于数据攻击分析的相关依据，从而确保数据攻击分析能够适用于不同的服务场景，这样可以保障后续数据攻击分析的准确性和可靠性。

[0029] 示例性的，在步骤S13中，攻击意图定位处理可以理解为针对多模态互动事件进行攻击意图定位和解析，从而确定出第一目标服务会话集对应的第一目标数据攻击意图，第一目标数据攻击意图包括但不限于数据窃取、信息篡改、延迟攻击、碎片攻击等不同的数据信息攻击意图。此外，第一目标数据攻击意图可以通过特征集或者其他形式进行表示本申请实施例不作限制。

[0030] 可以理解的是，上述示例应视为其中一种参考，并不是对本申请实施例的限制，以下给出的相关示例与上述示例可以结合起来理解，也可以单独理解，都应视作对本申请技术方案的合理解释。

[0031] 在本申请实施例中，对触发数据攻击分析条件的云服务日志进行关键事件识别，

得到触发数据攻击分析条件的云服务日志对应的至少一个第一敏感型互动事件，由于在攻击意图分析进程中，服务事件定位处理可以对随机多变的服务环境进行分析，因此，根据该至少一个第一敏感型互动事件，确定触发数据攻击分析条件的云服务日志中的第一目标服务会话集，以及确定第一目标服务会话集对应的第一多模态互动事件，也即得到了在攻击意图分析进程中的意图分析结果，进而根据第一多模态互动事件，通过启用攻击意图定位处理，使得可以得到第一目标服务会话集在服务场景中对应的第一目标数据攻击意图，从而可以实现高效精准地对触发数据攻击分析条件的云服务日志中不同状态的服务会话集的意图分析。

[0032] 在一种可独立实施的实施例中，应用于云服务的数据攻击分析方法通过意图分析学习模型实现。比如，可以将触发数据攻击分析条件的云服务日志传入意图分析学习模型，可以高效精准地对触发数据攻击分析条件的云服务日志中不同状态的服务会话集进行意图分析，得到服务会话集对应的数据攻击意图。

[0033] 在一种可独立实施的实施例中，意图分析学习模型可以包括关键事件识别子模型和预测子模型。将触发数据攻击分析条件的云服务日志传入上述意图分析学习模型，关键事件识别子模型对触发数据攻击分析条件的云服务日志进行关键事件识别，得到触发数据攻击分析条件的云服务日志对应的至少一个第一敏感型互动事件。

[0034] 在一种可独立实施的的实施例中，关键事件识别子模型可以包括卷积层和多维度变换层(特征金字塔层)。可以理解的是，将触发数据攻击分析条件的云服务日志传入意图分析学习模型后，卷积层和多维度变换层对触发数据攻击分析条件的云服务日志进行关键事件识别，得到多个不同维度的第一敏感型互动事件，选取至少一个第一敏感型互动事件传入预测子模型进行预测确定。传入预测子模型的第一敏感型互动事件的数目和维度可以根据实际期望确定，本申请对此不作进一步限制。关键事件识别子模型的相关结构除了可以包括卷积层和多维度变换层，还可以包括其它的模型网络层，本申请对此不作进一步限制。

[0035] 在一种可独立实施的实施例中，预测子模型可以包括差异化处理单元(分类单元)和定量关系分析单元(回归分析单元)。结合上述内容，将至少一个第一敏感型互动事件传入预测子模型之后，差异化处理单元利用至少一个第一敏感型互动事件，确定触发数据攻击分析条件的云服务日志中的第一目标服务会话集，定量关系分析单元利用至少一个第一敏感型互动事件，确定第一目标服务会话集对应的第一多模态互动事件表达。

[0036] 在一种可独立实施的实施例中，差异化处理单元和定量关系分析单元可以分别包括6个6*6滑动平均核和一个2*2滑动平均核，在每个滑动平均核之后连接一个触发单元(比如可以是ReevaluationU)。差异化处理单元和定量关系分析单元的相关模型网络层还可以根据实际期望包括其它类型，本申请对此不作进一步限制。

[0037] 在一种可独立实施的实施例中，第一敏感型互动事件包括第一敏感型互动事件描述；利用至少一个第一敏感型互动事件，确定触发数据攻击分析条件的云服务日志中的第一目标服务会话集，包括：利用至少一个第一敏感型互动事件描述，对触发数据攻击分析条件的云服务日志中的业务会话消息进行第一差异化处理，得到触发数据攻击分析条件的云服务日志中的第一原始服务会话集；利用至少一个第一敏感型互动事件描述，对触发数据攻击分析条件的云服务日志中的业务会话消息进行第二差异化处理，得到触发数据攻击分

析条件的云服务日志中的第一热点会话集，第一热点会话集对应于第一原始服务会话集的热点会话时段；根据第一原始服务会话集和第一热点会话集，确定第一目标服务会话集。

[0038] 可以理解的是，通过分别确定第一原始服务会话集和第一热点会话集，可以有效地清洗掉相关的噪声服务会话，从而可以提高最后预测确定得到的第一目标服务会话集的预测精度。

[0039] 请继续结合上述相关内容，差异化处理单元利用至少一个第一敏感型互动事件描述，得到触发数据攻击分析条件的云服务日志中的第一原始服务会话集和第一热点会话集，进而根据第一原始服务会话集和第一热点会话集，确定触发数据攻击分析条件的云服务日志中的第一目标服务会话集。下面对差异化处理单元的相关确定过程进行进一步阐述。

[0040] 差异化处理单元利用至少一个第一敏感型互动事件描述，对触发数据攻击分析条件的云服务日志中的业务会话消息进行第一差异化处理，确定触发数据攻击分析条件的云服务日志中各业务会话消息对应的第一预测可能性，第一预测可能性用于指示各业务会话消息位于服务会话集的可能性，进而根据触发数据攻击分析条件的云服务日志中各业务会话消息对应的第一预测可能性，确定第一原始服务会话集，第一原始服务会话集中各业务会话消息对应的第一预测可能性大于第一判定值。第一判定值的示例性取值可以根据实际期望确定，本申请对此不作进一步限制。

[0041] 差异化处理单元利用至少一个第一敏感型互动事件描述，对触发数据攻击分析条件的云服务日志中的业务会话消息进行第二差异化处理，确定触发数据攻击分析条件的云服务日志中各业务会话消息对应的第二预测可能性，第二预测可能性用于指示各业务会话消息位于热点会话集的可能性，进而根据触发数据攻击分析条件的云服务日志中各业务会话消息对应的第二预测可能性，确定第一热点会话集，第一热点会话集中各业务会话消息对应的第二预测可能性大于第二判定值。第二判定值的示例性取值可以根据实际期望确定，本申请对此不作进一步限制。

[0042] 将第一原始服务会话集中各业务会话消息对应的第一预测可能性，以及第一热点会话集中各业务会话消息对应的第二预测可能性，按照对应业务会话消息进行加权，得到各业务会话消息对应的第三预测可能性，进而根据各业务会话消息对应的第三预测可能性，确定第一目标服务会话集，第一目标服务会话集中各业务会话消息的第三预测可能性大于第三判定值。第三判定值的示例性取值可以根据实际期望确定，本申请对此不作进一步限制。

[0043] 在一种可独立实施的实施例中，第一敏感型互动事件包括第一敏感型互动事件描述，第一多模态互动事件包括第一多模态互动事件表达；利用至少一个第一敏感型互动事件，确定第一目标服务会话集对应的第一多模态互动事件，包括：利用至少一个第一敏感型互动事件描述，确定触发数据攻击分析条件的云服务日志中各业务会话消息对应的多模态互动事件表达；根据各业务会话消息对应的多模态互动事件表达和第一目标服务会话集的分布情况，确定第一多模态互动事件表达。

[0044] 意图分析学习模型可以利用至少一个敏感型互动事件描述可以快速确定触发数据攻击分析条件的云服务日志中各业务会话消息对应的多模态互动事件表达，由于确定了第一目标服务会话集在触发数据攻击分析条件的云服务日志中的分布情况，从而可以快速

确定得到第一目标服务会话集对应的第一多模态互动事件表达。第一敏感型互动事件除了可以包括第一敏感型互动事件描述之外，还可以根据实际期望包括其它形式的敏感型互动事件，例如，敏感型互动事件变量、敏感型互动事件列表等，第一多模态互动事件除了可以包括第一多模态互动事件表达之外，还可以根据实际期望包括其它形式的多模态互动事件，例如，多模态互动事件列表、多模态互动事件变量等，本申请对此不作进一步限制。

[0045] 请继续结合上述相关内容，定量关系分析单元利用至少一个第一敏感型互动事件描述，确定得到触发数据攻击分析条件的云服务日志中各业务会话消息的多模态互动事件表达。针对任一业务会话消息，该业务会话消息的多模态互动事件表达包括该业务会话消息对应的多个阶段的意图分析权重。例如，针对任一业务会话消息，定量关系分析单元确定得到该业务会话消息对应的多个阶段的意图分析权重[...,weight-2,weight-1,weight0,weight1,weight2,...]，根据该业务会话消息对应的多个阶段的意图分析权重，得到该业务会话消息对应的多模态互动事件表达。其中，weightN为第N个阶段的意图分析权重。

[0046] 在本申请实施例中，N的数值区间越大，意图分析学习模型基于多个阶段的意图分析权重形成的多模态互动事件表达对服务会话集进行分析得到的数据攻击意图的精度越高，即意图分析学习模型的意图分析精度越高，但是也会导致意图分析学习模型的运算开销激增，因为，可以全方位考虑意图分析过程中对意图分析精度和运算开销的期望来确定N的示例性取值，以实现在达到意图分析精度期望的前提下尽可能节省运算开销，确保意图分析学习模型的使用效率。例如，将N的数值区间确定从-3到+3，即多个阶段的意图分析权重为[weight-3,weight-2,weight-1,weight0,weight1,weight2,weight3]，此时意图分析学习模型既可以实现对不同状态的服务会话集进行精度较高的意图分析，又可以确保意图分析学习模型的运算开销满足期望。

[0047] 鉴于差异化处理单元已经确定了第一目标服务会话集，由此可以基于定量关系分析单元确定得到的触发数据攻击分析条件的云服务日志中各业务会话消息对应的多模态互动事件表达，确定第一目标服务会话集中各业务会话消息对应的第一多模态互动事件表达。

[0048] 鉴于第一目标服务会话集中各业务会话消息对应的第一多模态互动事件表达皆用于描述第一目标服务会话集的约束，由此除了第一目标服务会话集的热点会话时段业务会话消息之外，第一目标服务会话集中其它各业务会话消息对应的第一多模态互动事件表达是相同的。热点会话时段业务会话消息可以根据第一多模态互动事件表达中包括的初始阶段的意图分析权重确定。

[0049] 例如，根据第一多模态互动事件表达中包括的初始阶段的意图分析权重weight0，在第一目标服务会话集中确定热点会话时段业务会话消息(characteristic_0，description_0)。热点会话时段业务会话消息除了可以通过上述技术方案确定之外，还可以通过其它技术方案确定，本申请对此不作进一步限制。

[0050] 在一种可独立实施的实施例中，根据第一多模态互动事件，通过启用攻击意图定位处理，得到第一目标服务会话集对应的第一目标数据攻击意图，包括：依据对第一多模态互动事件表达启用攻击意图定位处理，得到第一目标服务会话集对应的多个数据攻击意图；依据对多个数据攻击意图启用迭代优化处理，得到第一目标数据攻击意图。

[0051] 由于第一目标服务会话集中各业务会话消息对应的第一多模态互动事件表达皆

用于描述第一目标服务会话集的约束，因此，依据对第一目标服务会话集中各业务会话消息对应的第一多模态互动事件表达启用攻击意图定位处理，可以得到第一目标服务会话集对应的多个数据攻击意图，为了清洗掉多余数据攻击意图，对多个数据攻击意图启用迭代优化处理(比如利用迭代-遍历-清洗的操作步骤实现)，最后得到第一目标服务会话集对应的第一目标数据攻击意图，实现对触发数据攻击分析条件的云服务日志的意图分析。

[0052] 请继续结合参阅上述的相关内容，基于意图分析学习模型，可以将触发数据攻击分析条件的云服务日志中不同状态的第一目标服务会话集通过服务事件定位处理迁移到攻击意图分析进程，在触发数据攻击分析条件的云服务日志中包括多个第一目标服务会话集的前提下，可以利用不同的第一多模态互动事件表达(不同的意图分析权重)来表示不同的第一目标服务会话集，进而依据对各第一目标服务会话集对应的第一多模态互动事件表达启用攻击意图定位处理和迭代优化处理，意图分析学习模型最后输出触发数据攻击分析条件的云服务日志中各第一目标服务会话集对应的第一目标数据攻击意图，使得意图分析学习模型具有灵活适配性，可以实现对触发数据攻击分析条件的云服务日志中不同状态的服务会话集进行灵活分析和定位。

[0053] 在一种可独立实施的实施例中，在利用意图分析学习模型对触发数据攻击分析条件的云服务日志中不同状态的服务会话集进行意图分析之前，还需要对意图分析学习模型进行训练。对意图分析学习模型进行训练，即对意图分析学习模型中的关键事件识别子模型和预测子模型皆进行训练。

[0054] 下面对意图分析学习模型的训练过程进行进一步阐述。

[0055] 在一种可独立实施的实施例中，意图分析学习模型的训练范例包括：范例云服务日志、范例云服务日志中的参考服务会话集、参考服务会话集对应的参考多模态互动事件；该应用于云服务的数据攻击分析方法还包括：通过原始学习模型对范例云服务日志进行关键事件识别，得到范例云服务日志对应的至少一个第二敏感型互动事件；利用至少一个第二敏感型互动事件，确定范例云服务日志中的第二目标服务会话集，以及确定第二目标服务会话集对应的第二多模态互动事件；根据第二多模态互动事件，通过启用攻击意图定位处理，得到第二目标服务会话集对应的第二目标数据攻击意图；根据第二目标服务会话集和参考服务会话集确定第一意图解析评价，以及根据第二目标数据攻击意图和参考多模态互动事件，确定第二意图解析评价；根据第一意图解析评价和第二意图解析评价，改进原始学习模型的模型变量，得到完成训练的意图分析学习模型。

[0056] 可以理解的是，上述的参考内容可以理解为标注内容，意图解析评价可以理解为模型损失或者模型损失函数。通过事先创建意图分析学习模型的训练范例，利用训练范例中的范例云服务日志、范例云服务日志中的参考服务会话集、参考服务会话集对应的参考多模态互动事件表达对原始学习模型进行训练，使得训练后得到的意图分析学习模型可以实现对不同状态的服务会话集进行意图分析。原始学习模型可以是与意图分析学习模型具有相同模型网络层，但是模型变量不同，且具有意图分析功能的学习模型(比如AI智能模型)。

[0057] 在一种可独立实施的实施例中，训练范例中可以包括至少一个范例云服务日志，且各范例云服务日志中包括至少一个参考服务会话集。训练范例中包括的范例云服务日志的数目、以及任一范例云服务日志中包括的参考服务会话集的数目，可以根据实际获取的

范例云服务日志来确定，本申请对此不作进一步限制。

[0058] 请继续参阅上述的相关内容，将训练范例中的范例云服务日志传入意图分析学习模型，关键事件识别子模型对范例云服务日志进行关键事件识别，得到范例云服务日志对应的至少一个第二敏感型互动事件。关键事件识别子模型对范例云服务日志进行关键事件识别的相关过程，与上述关键事件识别子模型对触发数据攻击分析条件的云服务日志进行关键事件识别的相关过程类似，在此不再进行说明。

[0059] 将关键事件识别子模型提取得到的至少一个第二敏感型互动事件传入预测子模型，预测子模型中的差异化处理单元利用至少一个第二敏感型互动事件，确定范例云服务日志中的第二目标服务会话集，定量关系分析单元利用至少一个第二敏感型互动事件，确定第二目标服务会话集对应的第二多模态互动事件。

[0060] 在一种可独立实施的实施例中，第二敏感型互动事件包括第二敏感型互动事件描述；利用至少一个第二敏感型互动事件，确定范例云服务日志中的第二目标服务会话集，包括：利用至少一个第二敏感型互动事件描述，对范例云服务日志中的业务会话消息进行第三差异化处理，得到范例云服务日志中的第二原始服务会话集；利用至少一个第二敏感型互动事件描述，对范例云服务日志中的业务会话消息进行第四差异化处理，得到范例云服务日志中的第二热点会话集，第二热点会话集对应于第二原始服务会话集的热点会话时段；根据第二原始服务会话集和第二热点会话集，确定第二目标服务会话集。

[0061] 差异化处理单元对范例云服务日志中第二目标服务会话集的进一步确定过程，与差异化处理单元对触发数据攻击分析条件的云服务日志中第一目标服务会话集的进一步确定过程类似，在此不再进行说明。第二多模态互动事件包括第二多模态互动事件表达，定量关系分析单元对第二目标服务会话集对应的第二多模态互动事件表达的进一步确定过程，与定量关系分析单元对第一目标服务会话集对应的第一多模态互动事件表达的进一步确定过程类似，在此不再进行说明。第二敏感型互动事件除了可以包括第二敏感型互动事件描述之外，还可以根据实际期望包括其它形式的敏感型互动事件，例如，敏感型互动事件变量、敏感型互动事件列表等，第二多模态互动事件除了可以包括第二多模态互动事件表达之外，还可以根据实际期望包括其它形式的多模态互动事件，例如，多模态互动事件列表、多模态互动事件变量等，本申请对此不作进一步限制。

[0062] 可以理解的是，在确定第二目标服务会话集对应的第二多模态互动事件表达之后，由于第二目标服务会话集对应的第二多模态互动事件表达皆用于描述第二目标服务会话集的约束，因此，依据对第二多模态互动事件表达启用攻击意图定位处理，可以得到第二目标服务会话集对应的多个数据攻击意图，为了清洗掉多余数据攻击意图，对多个数据攻击意图启用迭代优化处理，最后得到第二目标服务会话集对应的第二目标数据攻击意图，实现意图分析学习模型对范例云服务日志的意图分析。

[0063] 通过分析意图解析评价，以使得可以根据意图解析评价改进原始学习模型的模型变量，进而实现对意图分析学习模型的训练。在分析意图解析评价时，全方位考虑差异化处理单元和定量关系分析单元的损失。例如，可以通过以下算法确定意图分析学习模型的意图解析评价evaluation:evaluation＝evaluation_classification+Q*evaluation_R。

[0064] 在上述算法中，evaluation_classification为差异化处理单元对应的第一意图解析评价，evaluation_R为定量关系分析单元对应的第二意图解析评价。进一步地，Q可以

理解为为用于调节第一意图解析评价evaluation_classification和第二意图解析评价evaluation_R的变量。Q的示例性取值可以根据实际期望确定，本申请对此不作进一步限制。

[0065] 在一种可独立实施的实施例中，根据第二目标服务会话集和参考服务会话集确定第一意图解析评价，包括：根据参考服务会话集和设定调整指示，确定参考热点会话集，参考热点会话集对应于参考服务会话集的热点会话时段；根据第二目标服务会话集和参考服务会话集之间的比较结果，确定第三意图解析评价；根据第二热点会话集和参考热点会话集之间的比较结果，确定第四意图解析评价；根据第三意图解析评价和第四意图解析评价，确定第一意图解析评价。

[0066] 由于差异化处理单元在对第二目标服务会话集进行确定的过程中，确定了第二热点会话集，因此，在确定差异化处理单元对应的第一意图解析评价时，全方位考虑对第二目标服务会话集和第二热点会话集的意图解析评价。

[0067] 在实际应用过程中，为了确定差异化处理单元对第二热点会话集的意图解析评价，可以通过设定调整指示对参考服务会话集进行信息压缩或者信息扩增处理，从而在参考服务会话集的热点会话时段确定得到参考热点会话集。设定调整指示的示例性取值可以根据实际期望确定，本申请实施例不作进一步限制，例如，设定调整指示可以为0.6。

[0068] 在另外的一些实施例中，可以通过以下算法确定差异化处理单元对应的第一意图解析评价evaluation_classification。

[0069] evaluation_classification＝evaluation_A+evaluation_B。

[0070] 在上述算法中，evaluation_A为根据第二目标服务会话集和参考服务会话集之间的比较结果确定的第三意图解析评价，evaluation_B为根据第二热点会话集和参考热点会话集之间的比较结果确定的第四意图解析评价。第三意图解析评价和第四意图解析评价皆可以为代价函数，本申请对此不作进一步限制。

[0071] 在对意图分析学习模型进行模型训练的过程中，范例云服务日志中包括积极范例(比如正样本)和消极范例(比如负样本)，其中，积极范例为服务会话集，消极范例为非服务会话集。当范例云服务日志中积极范例和消极范例数量差异不平衡时，例如，当消极范例数量差异明显高于积极范例，即非服务会话集相对于服务会话集较大时，不利于对意图分析学习模型的训练，会导致完成训练的意图分析学习模型的意图分析精度较低，因此，为了解决范例调节性的问题，对范例云服务日志中积极范例和消极范例的数量差异进行平衡化设置，例如，消极范例与积极范例之比为4:1。积极范例和消极范例数量差异的示例性取值可以根据实际期望进行设置，本申请对此不作进一步限制。

[0072] 由于第二目标服务会话集对应的第二目标数据攻击意图，是基于定量关系分析单元确定的第二目标服务会话集对应的第二多模态互动事件进行攻击意图定位确定的，为了确定定量关系分析单元对应的第二意图解析评价，需要利用参考服务会话集对应的参考多模态互动事件，依据对参考多模态互动事件进行攻击意图定位得到参考服务会话集对应的参考数据攻击意图，进而通过第二目标数据攻击意图和参考数据攻击意图之间的比较结果，确定定量关系分析单元对应的第二意图解析评价。

[0073] 下面对训练范例中包括的参考服务会话集对应的参考多模态互动事件的确定过程进行进一步阐述。

[0074] 在一种可独立实施的实施例中，训练范例中还包括参考服务会话集对应的多个参考服务主题；该方法还包括：根据多个参考服务主题，对参考服务会话集进行服务主题筛选处理，得到多个已筛选服务主题，存在关联的已筛选服务主题之间的关键词一致；依据对多个已筛选服务主题启用事件解析处理，得到参考多模态互动事件。

[0075] 由于在范例云服务日志中包括多个参考服务会话集时，不同参考服务会话集对应的参考服务主题的数目可能不完全相同，且各参考服务会话集对应的参考服务主题的分布情况可能并不平衡，为了提高训练质量以及实现对不同样本的处理能力，针对任一参考服务会话集，根据参考服务会话集对应的多个参考服务主题，对参考服务会话集进行服务主题筛选处理，得到参考服务会话集对应的分布平衡的多个已筛选服务主题，进而依据对多个已筛选服务主题启用事件解析处理，得到准确性较高的参考服务会话集对应的参考特征描述。

[0076] 参考服务会话集对应的多个参考服务主题的形式可以是关联性较差的多个参考服务主题，可以是关联性较强的多个参考服务主题形成的参考数据攻击意图，还可以是分布于参考服务会话集约束上的其它形式的多个参考服务主题，本申请对此不做进一步限制。

[0077] 请继续参阅以上相关的内容，参考服务会话集中包括具有第一服务场景状态的多个参考服务主题，基于多个参考服务主题，对参考服务会话集进行服务主题筛选处理，得到具有第二服务场景状态的分布平衡的多个已筛选服务主题。

[0078] 在一种可独立实施的实施例中，参考多模态互动事件包括参考多模态互动事件表达；依据对多个已筛选服务主题启用事件解析处理，得到参考多模态互动事件，包括：通过确定多个已筛选服务主题中的原始已筛选服务主题和各已筛选服务主题之间的先后关系，得到多个已筛选服务主题对应的服务主题集；依据对服务主题集启用事件解析处理，得到参考多模态互动事件表达。

[0079] 对于相同的参考服务会话集，多个已筛选服务主题形成的不同队列可能会产生不同的多模态互动事件表达，因此，为了确保一个参考服务会话集对应的参考多模态互动事件表达具有独立性，以更高效地进行模型训练，通过确定多个已筛选服务主题中的原始已筛选服务主题和各已筛选服务主题之间的先后关系，得到多个已筛选服务主题对应的具有独立性的服务主题集，进而使得依据对服务主题集启用事件解析处理后，得到的参考多模态互动事件表达也具有独立性。在一种可可独立实施的实施例中，将通过参考服务会话集的热点会话时段业务会话消息的消息标签，与参考服务会话集之间最边缘的匹配结果，确定为原始已筛选服务主题。例如，业务会话消息information为参考服务会话集的原始已筛选服务主题。原始已筛选服务主题除了可以采用上述确定方式确定之外，还可以采用其它确定方式进行确定，本申请对此不作进一步限制。

[0080] 在一种可独立实施的实施例中，将各已筛选服务主题之间的先后关系确定为从原始已筛选服务主题起始的顺序。各已筛选服务主题之间的先后关系还可以采用其它确定方式，本申请对此不作进一步限制。依据对服务主题集启用事件解析处理，得到参考多模态互动事件表达，参考多模态互动事件表达包括多个阶段的意图分析权重。例如，服务主题集为[theme1,theme2,...,themen,...,themeM]，其中，themeM为服务主题集中的第M个已筛选服务主题。进而可以对服务主题集进行服务事件定位处理，得到多个阶段的意图分析权重，

进而得到由多个阶段的意图分析权重形成的参考多模态互动事件表达。

[0081] 在一种可独立实施的实施例中，根据第二目标数据攻击意图和参考多模态互动事件，确定第二意图解析评价，包括：依据对参考多模态互动事件表达启用攻击意图定位处理，得到参考服务会话集对应的第三目标数据攻击意图；根据第二目标数据攻击意图和第三目标数据攻击意图之间的比较结果，确定第二意图解析评价。

[0082] 由于意图分析学习模型最后输出的是服务场景中的第二目标数据攻击意图，也即最后的攻击意图定位结果仍然是服务场景中的模糊表达，因此，为了提高完成训练的意图分析学习模型的意图分析精度，需要在服务场景中对意图分析学习模型中的定量关系分析单元进行持续性跟踪训练，由于第二目标数据攻击意图是依据对第二多模态互动事件表达进行攻击意图定位得到的，因此，依据对参考多模态互动事件表达启用攻击意图定位处理，得到参考服务会话集在服务场景中对应的第三目标数据攻击意图，进而根据第二目标数据攻击意图和第三目标数据攻击意图之间的比较结果，即服务场景中的比较结果，确定定量关系分析单元对应的第二意图解析评价。

[0083] 在一种可能的示例中，攻击意图定位处理与事件解析处理互逆，在确定差异化处理单元对应的第一意图解析评价，以及定量关系分析单元对应的第二意图解析评价之后，根据第一意图解析评价和第二意图解析评价，改进原始学习模型的模型变量，通过反复执行上述模型训练过程，可以得到完成训练的意图分析学习模型，完成训练的意图分析学习模型可以实现高效精准地对不同状态的服务会话集进行意图分析。

[0084] 在一种可独立实施的实施例中，在得到所述第一目标服务会话集对应的第一目标数据攻击意图之后，所述方法还包括以下内容：确定所述第一目标数据攻击意图的待处理风险意图大数据，并根据所述待处理风险意图大数据更新风险意图数据库；响应于用户行为分析请求，通过所述风险意图数据集对待分析用户行为事件的业务互动大数据进行处理得到目标风险意图大数据；根据所述目标风险意图大数据对所述待分析用户行为事件进行大数据防护分析，得到大数据防护分析结果；基于所述大数据防护分析结果启用目标数据安防策略。

[0085] 在本申请实施例中，可以根据预先设置的映射关系查询第一目标数据攻击意图对应的待处理风险意图大数据，进一步地，可以根据待处理风险意图大数据对风险意图数据库中的风险意图大数据的关联关系和时效性特征进行更新，以便于后续进行风险意图大数据的定位。

[0086] 在一种可独立实施的实施例中，通过所述风险意图数据集对待分析用户行为事件的业务互动大数据进行处理得到目标风险意图大数据，可以包括以下内容：采集待分析用户行为事件的业务互动大数据；通过所述待分析用户行为事件的业务互动大数据，访问行为需求信息集，获得与所述待分析用户行为事件的业务互动大数据存在关联关系的第一行为需求信息，其中，所述行为需求信息集涵盖若干行为需求信息；基于所述第一行为需求信息和风险意图数据集，获得与所述待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据，其中，所述风险意图数据集涵盖若干风险意图大数据。

[0087] 在一种可独立实施的实施例中，通过所述风险意图数据集对待分析用户行为事件的业务互动大数据进行处理得到目标风险意图大数据的示例性技术方案可以包括如下相关内容。

[0088] 步骤100、采集待分析用户行为事件的业务互动大数据。

[0089] 本申请实施例中，待分析用户行为事件的业务互动大数据可以指包含有待分析用户行为事件的行为需求的业务互动大数据，可以包括行为需求的在线业务互动大数据或服务会话中包括行为需求的服务会话大数据。例如，待分析用户行为事件的业务互动大数据可以为服务会话大数据，可以是来自于业务用户互动终端的服务会话日志中的业务互动会话消息，也可以为独立的一条业务互动大数据或者一组业务互动大数据，还可以来自于另外的互动终端，本申请实施例对待分析用户行为事件的业务互动大数据的状态、传输方和获取方式等进一步实现不作限制。

[0090] 示例性地，待分析用户行为事件可以是存在安全分析需求的行为事件，比如支付业务的身份验证事件和支付行为事件，又比如办公业务的文件传输事件，再比如智慧医疗业务的用户信息匿名处理行为事件等。此外，业务互动大数据可以包括多个维度的信息或者多个层面的信息，能够作为安全分析的原料，但是直接针对业务互动大数据进行数据安全分析，可能存在较大的噪声，因此需要进行后续的行为需求和风险意图挖掘和分析，从而提高数据信息安防处理和分析的精度和可信度。

[0091] 步骤102、利用待分析用户行为事件的业务互动大数据，访问行为需求信息集，获得与待分析用户行为事件的业务互动大数据存在关联关系的第一行为需求信息。

[0092] 本申请实施例中，行为需求信息集可以是事先搭建的用于存储行为需求信息的关系型数据库(例如MySQL)。行为需求信息集中可以包含一个或多个用户行为事件的多个行为需求信息，每个用户行为事件可以对应一个或多个行为需求信息。

[0093] 可以理解的是，该行为需求信息集中包括的行为需求信息可以是通过对一个或多个服务会话中的服务会话大数据进行行为需求挖掘处理得到的，或者，行为需求信息集包括的行为需求信息也可以是通过对在线业务互动大数据进行行为需求挖掘处理得到的，本申请实施例对行为需求信息集中包括的行为需求信息的提供方不作限定。

[0094] 可以理解的是，该第一行为需求信息的个数可以为一个或多个，换言之，可以利用待分析用户行为事件的业务互动大数据访问行为需求信息集，获得与待分析用户行为事件的业务互动大数据存在关联关系的至少一个第一行为需求信息。

[0095] 例如，行为需求信息集requirement_collection中包含有多个用户行为事件的行为需求信息，每个用户行为事件的行为需求信息可以为一个或多个，基于行为需求信息集requirement_collection访问与待分析用户行为事件的业务互动大数据ser_DATA存在关联关系的如下行为需求信息：第一行为需求信息req_information_1、req_information_2和req_information_3。其中，第一行为需求信息req_information_1、req_information_2和req_information_3为与待分析用户行为事件的业务互动大数据ser_DATA配对于同一个用户行为事件的行为需求信息。

[0096] 示例性的，行为需求信息可以用于表征对应用户行为事件的互动需求或者交互需求，从而能够为后续的意图挖掘提供更为针对性的分析原料。

[0097] 步骤104、根据第一行为需求信息和风险意图数据集，获得与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据。

[0098] 本申请实施例中，风险意图数据集可以是事先搭建的用于记录风险意图大数据的关系型数据库。风险意图数据集中可以包含一个或多个用户行为事件的多个风险意图大数

据,每个用户行为事件可以对应一个或多个风险意图大数据。

[0099] 可以理解的是,风险意图数据集中包括的风险意图大数据可以是通过对一个或多个服务会话中的服务会话大数据进行风险意图挖掘处理得到的,其中,风险意图数据集中的风险意图大数据的服务会话提供方可以与行为需求信息集中的行为需求信息的服务会话提供方完全相同、部分相同或完全不同。亦或者,风险意图数据集中的风险意图大数据可以是通过对在线业务互动大数据进行风险意图挖掘处理得到的,本申请实施例对风险意图数据集中包括的风险意图大数据的提供方不作限定。

[0100] 在上述内容的基础上,可以根据每个第一行为需求信息和风险意图数据集,得到至少一个目标风险意图大数据。该目标风险意图大数据可以是通过访问风险意图数据集得到的,但本申请实施例对此不作限定。

[0101] 例如,风险意图数据集risk_intention_collection中可以包含有一个或多个用户行为事件的风险意图大数据,每个用户行为事件的风险意图大数据可以为多个,根据风险意图数据集risk_intention_collection和第一行为需求信息req_information_1可以采集与待分析用户行为事件的业务互动大数据ser_DATA存在关联关系的风险意图大数据risk_intention_DATA1和风险意图大数据risk_intention_DATA2,根据风险意图数据集risk_intention_collection和第一行为需求信息req_information_2可以采集与待分析用户行为事件的业务互动大数据ser_DATA存在关联关系的风险意图大数据risk_intention_DATA3,根据风险意图数据集risk_intention_collection和第一行为需求信息req_information_3可以采集与待分析用户行为事件的业务互动大数据ser_DATA存在关联关系的风险意图大数据risk_intention_DATA4和风险意图大数据risk_intention_DATA5。这样,可以获得与待分析用户行为事件的业务互动大数据存在关联关系的5个目标风险意图大数据risk_intention_DATA1-风险意图大数据risk_intention_DATA5。

[0102] 本申请实施例中,上述步骤102可以认为是行为需求分析过程,步骤104可以认为是风险意图分析过程。此外,风险意图大数据可以包括各类存在异常的行为意图或者行为倾向,比如异常登录意图、异常互动意图、非常用地身份验证意图等,这些风险意图大数据可以作为大数据信息安防处理的依据,由于风险意图大数据精度高、针对性强,因而能够保障大数据信息安防检测和分析的精度和可信度,且由于风险意图大数据是经过简化处理的,在一定程度上还能够确保大数据信息安防检测和分析的效率,提高信息防护的时效性。

[0103] 本申请实施例基于行为需求分析结合风险意图分析的综合解析方式,一方面根据行为需求信息集访问获得与待分析用户行为事件的业务互动大数据存在关联关系的第一行为需求信息,另一方面根据风险意图数据集和第一行为需求信息采集与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据,既具有行为需求分析的时序持续性强、准确性高的优点,又具有风险意图分析的检测灵敏性高的优点,提高了针对待分析用户行为事件进行风险意图挖掘和分析的准确性和可靠性,此外,通过考虑行为需求和风险意图,能够实现风险意图挖掘分析的层次性以保障风险意图大数据的完整性,这样一来,在以目标风险意图大数据作为数据信息防护分析依据时,能够保障数据信息防护的可信度。

[0104] 在一些可独立实施的实施例中,以下为根据本申请实施例的基于用户行为的大数据防护方法另一实施方式。

[0105] 步骤200、生成行为需求信息集和风险意图数据集。

[0106] 本申请实施例中，行为需求信息集和风险意图数据集的生成过程可以互相隔离、互相不存在影响，可以同时实施或以随机顺序实施，本申请实施例对此不作限制。下面将分别介绍行为需求信息集和风险意图数据集的生成过程。

[0107] STEP1生成行为需求信息集

STEP1-1行为需求挖掘处理

可以对至少一个服务会话中的每个服务会话包括的服务会话大数据进行行为需求挖掘处理，得到多个行为需求信息，并将多个行为需求信息以及多个行为需求信息中每个行为需求信息的信息添加到行为需求信息集。

[0108] 以一些示例性的角度来看待，行为需求信息的信息可以包括以下内容中的一种或多种：行为需求信息所绑定的服务会话信息、行为需求信息的分布信息(先后关系信息或者序号信息)、行为需求信息在服务会话大数据中的业务互动大数据描述信息(行为需求信息在服务会话大数据相对位置信息)等。

[0109] 行为需求信息的分布信息可以指示行为需求信息所绑定的服务会话大数据，或者，行为需求信息所绑定的服务会话大数据也可以通过其他参量指示。可以理解的是，行为需求信息在服务会话大数据中的业务互动大数据描述信息可以指示行为需求信息在服务会话大数据中的描述，例如，行为需求信息在服务会话大数据中的业务互动大数据描述信息可以包括行为需求信息的约束标签描述信息(比如标识集的位置)。可以理解的是，行为需求信息的信息还可以包括其他信息，本申请实施例对此不作限定。

[0110] 例如，可以将服务会话conversation_1进行拆解处理，得到两组服务会话大数据conversation_DATA1和conversation_DATA2。然后，可以对服务会话大数据conversation_DATA1和conversation_DATA2进行行为需求挖掘处理，从服务会话大数据conversation_DATA1中得到如下的行为需求信息，它们分别是：

行为需求信息conversation_req_information1；

行为需求信息conversation_req_information2，以及

行为需求信息conversation_req_information3。

[0111] 从服务会话大数据conversation_DATA2中得到如下的行为需求信息，它们分别是：

行为需求信息conversation_req_information4，以及

行为需求信息conversation_req_information5。

[0112] 在上述基础上，并采集各个行为需求信息的特征。其中，行为需求信息conversation_req_information1的特征包括：范例业务互动大数据conversation_DATA1的特征，如范例业务互动大数据conversation_DATA1的标签、序号、数据量、时序特征等，服务会话大数据conversation_DATA1的对应的分布distribution_1，行为需求信息conversation_req_information1在范例业务互动大数据conversation_DATA1中的描述信息，等等。

[0113] 其中：

行为需求信息conversation_req_information2、

行为需求信息conversation_req_information3、

行为需求信息conversation_req_information4,以及

行为需求信息conversation_req_information5的特征与行为需求信息conversation_req_information1的特征类似,在此不再赘述。

[0114] 在上述内容的基础上,可以将行为需求信息conversation_req_information1、

行为需求信息conversation_req_information2、

行为需求信息conversation_req_information3、

行为需求信息conversation_req_information4和行为需求信息conversation_req_information5及各自的特征添加到行为需求信息集requirement_collection。

[0115] STEP1-2行为需求持续性分析处理

对上述行为需求挖掘处理得到的多个行为需求信息进行行为需求持续性分析处理,得到至少一个行为需求视觉记录,其中,每个行为需求视觉记录涵盖若干行为需求信息中的至少两个行为需求信息。行为需求视觉记录包括的至少两个行为需求信息可以配对于同一用户行为事件。可以理解的是,可以将用于指示该多个行为需求信息与该至少一个行为需求视觉记录之间的对应关系的信息添加到行为需求信息集。作为一个可能的实施例,可以将该至少一个行为需求视觉记录中每个行为需求视觉记录的信息添加到行为需求信息集。可以理解的是,行为需求视觉记录的信息可以包括行为需求视觉记录包括的行为需求信息的标识信息。

[0116] 可以理解的是,可以根据至少一个行为需求视觉记录中每个行为需求视觉记录包括的至少两个行为需求信息,确定每个行为需求视觉记录的去极性显著性表达,并将至少一个行为需求视觉记录中每个行为需求视觉记录的去极性显著性表达添加到行为需求信息集。

[0117] 例如,可以对行为需求信息conversation_req_information1、

行为需求信息conversation_req_information2、

行为需求信息conversation_req_information3、

行为需求信息conversation_req_information4和行为需求信息conversation_req_information5进行行为需求持续性分析处理,得到行为需求视觉记录visual_record_1和visual_record_2。

[0118] 其中,行为需求视觉记录visual_record_1包括行为需求信息conversation_req_information1、conversation_req_information3和行为需求信息conversation_req_information5,行为需求视觉记录visual_record_2包括行为需求信息conversation_req_information2和conversation_req_information4。

[0119] 进一步地,在上述内容的基础上可以分别确定以下的行为需求信息conversation_req_information1、conversation_req_information3和行为需求信息conversation_req_information5的显著性表达,并将行为需求信息conversation_req_information1、conversation_req_information3和行为需求信息conversation_req_information5的显著性表达的去极性处理结果(平均化处理结果)作为行为需求视觉记录visual_record_1的去极性显著性表达characteristic_ave_1,分别确定行为需求信息conversation_req_information2和conversation_req_information4的显著性表达,并将行为需求信息conversation_req_information2和conversation_req_information4的显

著性表达的去极性处理结果作为行为需求视觉记录visual_record_2的去极性显著性表达characteristic_ave_2。最后，将行为需求视觉记录visual_record_1的去极性显著性表达characteristic_ave_1和行为需求视觉记录visual_record_2的去极性显著性表达characteristic_ave_2添加到行为需求信息集requirement_collection。

[0120] 可以理解的是，在上述例子中以行为需求视觉记录包括的多个行为需求信息的显著性表达的去极性处理结果作为行为需求视觉记录的去极性显著性表达，在本申请实施例中，行为需求视觉记录的去极性显著性表达可以是通过对行为需求视觉记录包括的至少两个行为需求信息的显著性表达进行处理得到的，本申请实施例对处理的进一步实现不作限定。

[0121] 在另外的一些可能的示例中，可以将行为需求信息所绑定的行为需求视觉记录的信息作为行为需求信息的信息添加到行为需求信息集，例如行为需求信息的信息包括行为需求信息所绑定的行为需求视觉记录的标识信息和/或去极性显著性表达，本申请实施例对此不作限定。

[0122] 可以理解的是，在生成行为需求信息集的过程中，可以采用AI智能模型等进行行为需求挖掘处理和行为需求持续性分析处理，本申请实施例对行为需求挖掘处理和行为需求持续性分析处理所采用的技术手段不作限制。

[0123] STEP2生成风险意图数据集

STEP2-1风险意图挖掘处理

对至少一个服务会话中的每个服务会话中的服务会话大数据进行风险意图挖掘处理，得到多个风险意图大数据，并将多个风险意图大数据以及多个风险意图大数据中每个风险意图大数据的信息添加到风险意图数据集。以一些示例性的角度来看待，风险意图大数据的信息可以包括以下内容中的一种或多种：风险意图大数据所绑定的服务会话信息、风险意图大数据的分布信息、风险意图大数据在服务会话大数据中的业务互动大数据描述信息。

[0124] 风险意图大数据的分布信息可以指示风险意图大数据所绑定的服务会话大数据，或者，风险意图大数据所绑定的服务会话大数据也可以通过其他参量指示。可以理解的是，风险意图大数据在服务会话大数据中的业务互动大数据描述信息可以指示风险意图大数据在服务会话大数据中的描述，例如，风险意图大数据在服务会话大数据中的业务互动大数据描述信息可以包括风险意图大数据的约束标签描述信息。可以理解的是，风险意图大数据的信息还可以包括其他信息，本申请实施例对此不作限定。风险意图挖掘处理的实施方式可以参照上述行为需求挖掘处理的实施方式，在此不再赘述。

[0125] STEP2-2风险意图持续性分析处理

对多个风险意图大数据进行风险意图持续性分析处理，得到至少一个风险意图视觉记录，其中，每个风险意图视觉记录涵盖若干风险意图大数据中的至少两个风险意图大数据。风险意图视觉记录包括的至少两个风险意图大数据可以配对于同一用户行为事件。可以理解的是，可以将用于指示该多个风险意图大数据与该至少一个风险意图视觉记录之间的对应关系的信息添加到行为需求信息集。以一些示例性的角度来看待，可以将该至少一个风险意图视觉记录中每个风险意图视觉记录的信息添加到行为需求信息集。可以理解的是，风险意图视觉记录的信息可以包括风险意图视觉记录包括的风险意图大数据的标识

信息。

[0126] 可以理解的是，可以确定风险意图视觉记录中包括的至少两个风险意图大数据中每个风险意图大数据的显著性表达，并根据风险意图视觉记录包括的每个风险意图大数据的显著性表达，确定风险意图视觉记录的去极性显著性表达。其中，风险意图视觉记录的去极性显著性表达可以是通过对该风险意图视觉记录包括的至少两个风险意图大数据中每个风险意图大数据的显著性表达进行处理得到的，例如去极性处理处理，等等，本申请实施例对风险意图视觉记录的去极性显著性表达的进一步实现不做限定。

[0127] 以一些示例性的角度来看待，可以根据至少一个风险意图视觉记录中每个风险意图视觉记录包括的至少两个风险意图大数据，确定每个风险意图视觉记录的去极性显著性表达，并将至少一个风险意图视觉记录中每个风险意图视觉记录的去极性显著性表达添加到行为需求信息集。

[0128] 在另外的一些可能的示例中，可以将风险意图大数据所绑定的风险意图视觉记录的信息作为风险意图大数据的信息添加到行为需求信息集，例如风险意图大数据的信息包括风险意图大数据所绑定的风险意图视觉记录的标识信息和/或去极性显著性表达，本申请实施例对此不作限定。风险意图持续性分析处理的实施方式可以参照上述行为需求持续性分析处理的实施方式，在此不再赘述。

[0129] 对于一种可独立实施的实施方式而言，对服务会话中的服务会话大数据进行行为需求/风险意图挖掘处理可以指利用行为需求/风险意图挖掘算法对服务会话中的每一条业务互动大数据进行分析，得到每一条业务互动大数据中的行为需求/风险意图数据集。对服务会话中的服务会话大数据进行行为需求/风险意图持续性分析处理可以指利用行为需求/风险意图持续性分析算法挖掘服务会话中配对于同一用户行为事件的行为需求/风险意图大数据，但本申请实施例对此不做限定。

[0130] 步骤202、采集待分析用户行为事件的业务互动大数据。

[0131] 步骤204、利用待分析用户行为事件的业务互动大数据，访问行为需求信息集，获得与待分析用户行为事件的业务互动大数据存在关联关系的第一行为需求信息。

[0132] 可以理解的是，步骤204可以包括如下步骤。

[0133] 步骤2040、确定待分析用户行为事件的业务互动大数据的第一行为需求显著性表达。

[0134] 本申请实施例中，将待分析用户行为事件的业务互动大数据的显著性表达(特征向量或者描述向量)称为第一行为需求显著性表达。可以理解的是，可以基于行为需求识别网络确定待分析用户行为事件的业务互动大数据的第一行为需求显著性表达，其中，行为需求识别网络用于确定行为需求显著性表达。

[0135] 在一种可能的实施方式中，行为需求识别网络可以为AI智能模型。例如，基于行为需求识别网络采集待分析用户行为事件的业务互动大数据的第一行为需求显著性表达，第一行为需求显著性表达可以是多维向量，具体的维度与行为需求识别网络相关，第一行为需求显著性表达的每一位特征值的取值进行归一化处理，以保障每一位的取值的区间为[-1,1]，但本申请实施例不限于此。

[0136] 步骤2041、根据第一行为需求显著性表达，从行为需求信息集所包括的多个行为需求信息中确定第一行为需求信息。

[0137] 以一些示例性的角度来看待，可以分别确定第一行为需求显著性表达与多个行为需求信息对应的多个第二行为需求显著性表达中每个第二行为需求显著性表达之间的差异分析结果(如欧式距离)；将多个第二行为需求显著性表达中与第一行为需求显著性表达之间的差异分析结果最小或者差异分析结果不超过第一判定值的第二行为需求显著性表达所对应的至少一个行为需求信息确定为第一行为需求信息。

[0138] 本申请实施例将行为需求信息集中的行为需求信息的显著性表达称为第二行为需求显著性表达。可以理解的是，多个行为需求信息中的每个行为需求信息可以配对于一个第二行为需求显著性表达，而该多个行为需求信息中的不同行为需求信息对应的第二行为需求显著性表达可以相同或不同。可以理解的是，该多个行为需求信息中配对于同一行为需求视觉记录的至少两个行为需求信息具有相同的第二行为需求显著性表达。例如，该至少两个行为需求信息的第二行为需求显著性表达可以为该至少两个行为需求信息所属行为需求视觉记录的去极性显著性表达，但本申请实施例不限于此。

[0139] 行为需求信息conversation_req_information1、

行为需求信息conversation_req_information2、

行为需求信息conversation_req_information3、

行为需求信息conversation_req_information4和行为需求信息conversation_req_information5中的

行为需求信息conversation_req_information1、

conversation_req_information3和

行为需求信息conversation_req_information5

属于行为需求视觉记录visual_record_1。

[0140] 行为需求信息conversation_req_information2

和conversation_req_information4不属于任何行为需求视觉记录，则行为需求信息conversation_req_information1对应的第二行为需求显著性表达、行为需求信息conversation_req_information3对应的第二行为需求显著性表达和行为需求信息conversation_req_information5对应的第二行为需求显著性表达均为行为需求视觉记录visual_record_1的去极性显著性表达characteristic_ave_1，行为需求信息conversation_req_information2的第二行为需求显著性表达可以为行为需求信息conversation_req_information2的显著性表达。

[0141] 可以理解的是，可以将多个第二行为需求显著性表达中最小的第二行为需求显著性表达所对应的至少一个行为需求信息确定为第一行为需求信息，或者可以将多个第二行为需求显著性表达中不超过第一判定值的至少一个第二行为需求显著性表达所对应的至少一个行为需求信息确定为第一行为需求信息，其中，第一判定值可以根据不同的要求事先进行设定，本申请对其进一步实现不做限定。

[0142] 步骤206、根据第一行为需求信息和风险意图数据集，获得与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据。

[0143] 可以理解的是，步骤206可以包括如下步骤。

[0144] 步骤2060、采集与第一行为需求信息对应的第一风险意图大数据。

[0145] 本申请实施例中，可以从行为需求信息集中采集第一行为需求信息的特征，并根

据采集的特征，确定与第一行为需求信息对应的第一风险意图大数据。可以理解的是，第一行为需求信息的特征可以包括第一行为需求信息所绑定的服务会话的特征和/或第一行为需求信息的分布特征，或者还可以进一步包括第一行为需求信息的业务互动大数据描述特征。以一些示例性的角度来看待，可以确定第一行为需求信息所绑定的第一服务会话以及第一行为需求信息的分布特征和业务互动大数据描述特征，并根据第一行为需求信息的分布特征和业务互动大数据描述特征，采集第一服务会话中与第一行为需求信息对应的第一风险意图大数据。

[0146] 在一些可能的示例中，第一行为需求信息的分布特征可以指示第一行为需求信息在第一服务会话中所在的位置，可以根据第一行为需求信息的分布特征采集第一服务会话中包括第一行为需求信息的第一服务会话大数据，其中，第一服务会话大数据在第一服务会话中所绑定的位置配对于该第一行为需求信息的分布特征。第一行为需求信息的业务互动大数据描述特征可以指示第一行为需求信息在所绑定的服务会话大数据中的描述，例如，第一行为需求信息的约束标签在第一服务会话大数据中的相对位置特征，但本申请实施例不限于此。

[0147] 可以理解的是，在采集第一风险意图大数据的过程中，具体可以依照如下两种方式实现。

[0148] 第一种方式、如果第一服务会话中存在分布与第一行为需求信息的分布信息匹配且携带第一行为需求信息的风险意图大数据，将包含第一行为需求信息的风险意图大数据确定为与第一行为需求信息对应的第一风险意图大数据。

[0149] 例如，第一行为需求信息req_information_1在第一服务会话service_1的第20组服务会话大数据中，在第一服务会话service_1的第20组服务会话大数据中存在完全包含第一行为需求信息req_information_1的风险意图大数据risk_intention_DATA1，则将风险意图大数据risk_intention_DATA1确定为与第一行为需求信息req_information_1对应的第一风险意图大数据。

[0150] 第二种方式、若第一服务会话中不存在分布与第一行为需求信息的分布信息匹配且携带第一行为需求信息的风险意图大数据，将第一行为需求信息在第一服务会话大数据中依照设定指示进行上采样，获得与第一行为需求信息对应的第一风险意图大数据，其中，第一服务会话大数据在第一服务会话中的分布配对于第一行为需求信息的分布信息。

[0151] 例如，第一行为需求信息req_information_2在第一服务会话service_2的第13组服务会话大数据中，在第一服务会话service_2的第13组服务会话大数据中不存在完全包含第一行为需求信息req_information_2的风险意图大数据，则可以将第一行为需求信息req_information_2在第一服务会话大数据即第13组服务会话大数据中依照设定指示进行上采样，并将上采样后的数据集确定为与第一行为需求信息req_information_2对应的第一风险意图大数据。

[0152] 步骤2061、通过第一风险意图大数据访问风险意图数据集，获得与第一风险意图大数据存在关联关系的至少一个风险意图大数据。

[0153] 本申请实施例中，可以理解的是，可以确定第一风险意图大数据的第一风险意图显著性表达，并根据第一风险意图显著性表达，从风险意图数据集所包括的多个风险意图大数据中确定与第一风险意图大数据存在关联关系的至少一个风险意图大数据。

[0154] 本申请实施例将第一风险意图大数据的显著性表达称为第一风险意图显著性表达。可以理解的是，在从风险意图数据集所包括的多个风险意图大数据中确定与第一风险意图大数据存在关联关系的至少一个风险意图大数据时，可以确定第一风险意图显著性表达与多个风险意图大数据对应的多个第二风险意图显著性表达中每个第二风险意图显著性表达之间的差异分析结果，并将多个第二风险意图显著性表达中与第一风险意图显著性表达之间的差异分析结果最小或者不超过第二判定值的第二风险意图显著性表达所对应的至少一个风险意图大数据确定为与第一风险意图大数据存在关联关系的至少一个风险意图大数据。

[0155] 可以理解的是，多个风险意图大数据中的每个风险意图大数据可以配对于一个第二风险意图显著性表达，而该多个风险意图大数据中的不同风险意图大数据对应的第二风险意图显著性表达可以相同或不同。可以理解的是，该多个风险意图大数据中配对于同一风险意图视觉记录的至少两个风险意图大数据具有相同的第二风险意图显著性表达。例如，该至少两个风险意图大数据的第二风险意图显著性表达可以为该至少两个风险意图大数据所属风险意图视觉记录的去极性显著性表达，但本申请实施例不限于此。

[0156] 可以理解的是，可以将多个第二风险意图显著性表达中最小的第二风险意图显著性表达所对应的至少一个风险意图大数据确定为与第一风险意图大数据存在关联关系的风险意图大数据，或者可以将多个第二风险意图显著性表达中不超过第二判定值的至少一个第二风险意图显著性表达所对应的至少一个风险意图大数据确定为与第一风险意图大数据存在关联关系的风险意图大数据，其中，第二判定值可以根据不同的要求事先进行设定，本申请对其进一步实现不做限定。

[0157] 以一些示例性的角度来看待，可以将与第一风险意图大数据存在关联关系的至少一个风险意图大数据确定为与待分析用户行为事件的业务互动大数据存在关联关系的目标风险意图大数据。

[0158] 在另外的一些可能的示例中，步骤206还可以进一步包括：对与第一风险意图大数据存在关联关系的至少一个风险意图大数据进行过滤，获得与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据。

[0159] 在另外的一些可能的示例中，在本申请实施例中，可以将与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据确定为待分析用户行为事件的访问结果。也可以首先确定与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据，然后对与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据进行过滤，得到待分析用户行为事件的访问结果，本申请实施例对此不做限定。

[0160] 步骤208、对与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据进行过滤，得到待分析用户行为事件的访问结果。

[0161] 可以理解的是，步骤208可以依照如下两种方式中的至少一种方式实现。

[0162] 方式一、根据时序过滤指标和服务会话过滤指标中的至少一种对与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据进行过滤。

[0163] 在一种可独立实施的实施方式中，可以根据实际情况调整过滤指标，例如，根据时序过滤指标(如从某一天的某个时段内)、服务会话过滤指标(如来自于哪个业务端)对待分

析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据进行过滤。本申请实施例中，过滤指标包括但不限于时序过滤指标和服务会话过滤指标，还可以包括用户行为事件过滤指标，如事件类别、事件参与方的数目等等，本申请实施例对此不做限定。

[0164] 方式二、对与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据的显著性表达对该至少一个目标风险意图大数据进行特征分析(聚类)，并根据特征分析结果进行过滤。

[0165] 可以理解的是，根据与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据中每个目标风险意图大数据的显著性表达，将至少一个目标风险意图大数据拆解成至少一组风险意图大数据，每组风险意图大数据可以包括至少一个风险意图大数据；根据该至少一组风险意图大数据中每组风险意图大数据包括的至少一个风险意图大数据的显著性表达，确定该每组风险意图大数据的过滤汇总结果；根据该至少一组风险意图大数据中每组风险意图大数据的过滤汇总结果，将该至少一组风险意图大数据中的一组或多组风险意图大数据包括的风险意图大数据确定为待分析用户行为事件的访问结果。

[0166] 以一些示例性的角度来看待，一组风险意图大数据的过滤汇总结果可以包括该组风险意图大数据包括的至少一个风险意图大数据的显著性表达的去极性处理结果，但本申请实施例不限于此。

[0167] 以一些示例性的角度来看待，可以根据每组风险意图大数据的过滤汇总结果，对至少一组风险意图大数据进行整理，并将排序在端点的一组或多组风险意图大数据剔除，得到待分析用户行为事件的访问结果。

[0168] 对于一种可独立实施的实施方式而言，可以采用多均值聚类特征分析算法对与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据的显著性表达进行特征分析，得到多个分组的显著性表达，对于每个分组中的显著性表达，确定其对应的视觉记录的数目、显著性表达的偏移等过滤汇总结果，并根据过滤汇总结果确定哪些分组是干扰(如偏移最大的组为干扰组)。例如，假设与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据具体为200个风险意图视觉记录，每个风险意图视觉记录包括若干个风险意图大数据，则可以通过多均值聚类特征分析算法将200个风险意图视觉记录的显著性表达拆解为20个分组，具体地，可以对200个风险意图视觉记录的200个显著性表达进行多轮迭代多均值聚类特征分析运算，分成20个组，其中每组中包括的风险意图视觉记录的数目可以相同或不同，其中，第20组中只有10个风险意图视觉记录，且显著性表达的偏移最大，则可以确定第20组中的10个风险意图视觉记录为干扰，并从结果中去除第20组中的10个风险意图视觉记录中包括的风险意图大数据，剩余结果即为访问结果。

[0169] 基于本申请实施例的上述介绍，本申请实施例的基于用户行为的大数据防护方法事先对大量的服务会话(如支付服务会话)进行服务会话优化操作(主要包括行为需求/风险意图挖掘处理和行为需求/风险意图持续性分析处理)，生成行为需求信息集和风险意图数据集。在对包含行为需求的待分析用户行为事件的业务互动大数据进行访问时，一方面根据行为需求信息集进行行为需求分析，得到第一行为需求信息，另一方面根据风险意图

数据集对第一行为需求信息进行风险意图分析，得到若干风险意图大数据，然后对若干风险意图大数据进行过滤处理，最终得到待分析用户行为事件的访问结果(该访问结果可以理解为针对于大数据防护的访问结果和定位结果)。

[0170] 本申请实施例基于行为需求分析结合风险意图分析的综合解析方式，一方面根据行为需求信息集访问获得与待分析用户行为事件的业务互动大数据存在关联关系的第一行为需求信息，另一方面根据风险意图数据集和第一行为需求信息采集与待分析用户行为事件的业务互动大数据存在关联关系的至少一个目标风险意图大数据。本申请实施例既具有行为需求分析的时序持续性强、准确性高的优点，又具有风险意图分析的检测灵敏性高的优点，提高了针对待分析用户行为事件进行风险意图挖掘和分析的准确性和可靠性，此外，通过考虑行为需求和风险意图，能够实现风险意图挖掘分析的层次性以保障风险意图大数据的完整性，这样一来，在以目标风险意图大数据作为数据信息防护分析依据时，能够保障数据信息防护的可信度。

[0171] 在本申请实施例中，可以通过大数据防护分析结果从预设的数据安防策略库中匹配对应的目标数据安防策略并启用，以实现对相关数据信息的防护处理，比如数据信息访问的权限验证处理，又比如指定访问对象的拦截处理，再比如相关重要信息的匿名化处理等，在此不作限定。可以理解的是，由于大数据防护分析结果是基于目标风险意图大数据得到的，因而能够确保大数据防护分析结果的针对性和可靠性。

[0172] 在一些可独立实施的实施例中，根据所述目标风险意图大数据对所述待分析用户行为事件进行大数据防护分析，得到大数据防护分析结果，可以包括以下步骤所描述的内容。

[0173] 步骤300、根据所述目标风险意图大数据以及所述待分析用户行为事件的关联事件，确定待进行防护分析的事件特征簇，所述待进行防护分析的事件特征簇中包括多条待进行防护分析的事件特征。

[0174] 在本申请实施例中，关联事件可以是与待分析用户行为事件存在时序关联或者场景关联的事件，事件特征可以是连续的特征轨迹。

[0175] 步骤302、在根据所述待进行防护分析的事件特征簇进行威胁分析处理的过程中，在识别到第一待进行防护分析的事件特征中存在热度关键词的前提下，对所述第一待进行防护分析的事件特征再次进行事件特征调整，得到至少一条第二待进行防护分析的事件特征，所述第一待进行防护分析的事件特征包括位于所述大数据防护服务器的识别区间内的待进行防护分析的事件特征。

[0176] 在本申请实施例中，热度关键词可以表征相关的特征信息处于使用状态，在这种情况下，需要跳过这类特征信息的威胁分析/防护分析，从而保障特征信息的正常使用。进一步地，大数据防护服务器的识别区间可以理解为大数据防护服务器的识别条件或者捕捉条件。

[0177] 步骤304、根据所述第二待进行防护分析的事件特征对所述待进行防护分析的事件特征簇进行优化，得到优化后的待进行防护分析的事件特征簇；根据所述优化后的待进行防护分析的事件特征簇进行威胁分析处理，得到大数据防护分析结果。

[0178] 可以理解的是，通过更新待进行防护分析的事件特征簇并进行威胁分析处理，能够在保障特征信息正常使用的前提下实现准确可靠的大数据防护分析。可以理解的是，热

度关键词对应的特征信息通常是在先经过防护分析的，因而通过上述方式还能够在一定程度上节省大数据防护分析的资源开销。

[0179] 在一些可独立实施的实施例中，任一待进行防护分析的事件特征包括第一特征成员和第二特征成员，所述在识别到第一待进行防护分析的事件特征中存在热度关键词的前提下，对所述第一待进行防护分析的事件特征再次进行事件特征调整，得到至少一条第二待进行防护分析的事件特征，包括：在识别到所述第一待进行防护分析的事件特征中存在热度关键词的前提下，根据所述第一待进行防护分析的事件特征的第一特征成员和第二特征成员及所述热度关键词的分布情况，对所述第一待进行防护分析的事件特征再次进行事件特征调整，得到至少一条第二待进行防护分析的事件特征。

[0180] 在本申请实施例中，特征成员可以是事件特征中的特征节点或者特征图谱单元，如此设计，通过对事件特征进行拆解处理分析，能够确保第二待进行防护分析的事件特征的准确可靠调整。

[0181] 基于上述同样的发明构思，还提供了一种应用于云服务的数据攻击分析装置20，应用于数据攻击分析服务器10，所述装置包括：互动事件识别模块21，用于对触发数据攻击分析条件的云服务日志进行关键事件识别，得到所述触发数据攻击分析条件的云服务日志对应的至少一个第一敏感型互动事件；服务会话确定模块22，用于基于所述至少一个第一敏感型互动事件，确定所述触发数据攻击分析条件的云服务日志中的第一目标服务会话集，以及确定所述第一目标服务会话集对应的第一多模态互动事件；攻击意图定位模块23，用于基于所述第一多模态互动事件，通过启用攻击意图定位处理，得到所述第一目标服务会话集对应的第一目标数据攻击意图。

[0182] 以上所述仅为本申请的优选实施例而已，并不用于限制本申请，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

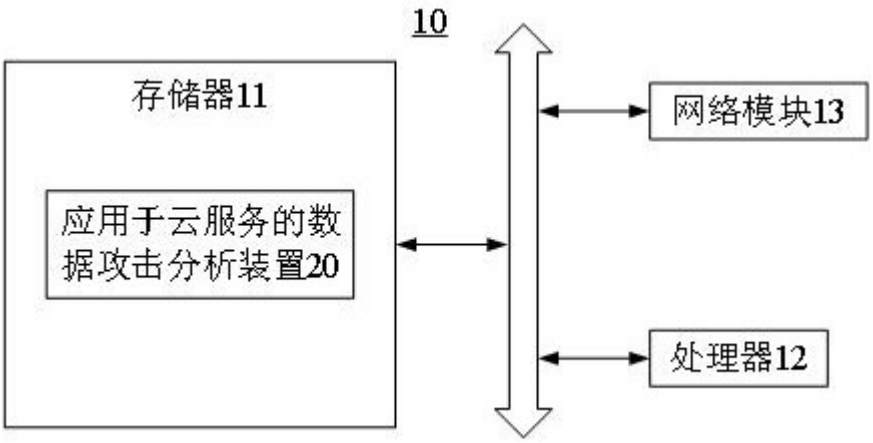

10
存储器11
应用于云服务的数据攻击分析装置20
网络模块13
处理器12

图 1

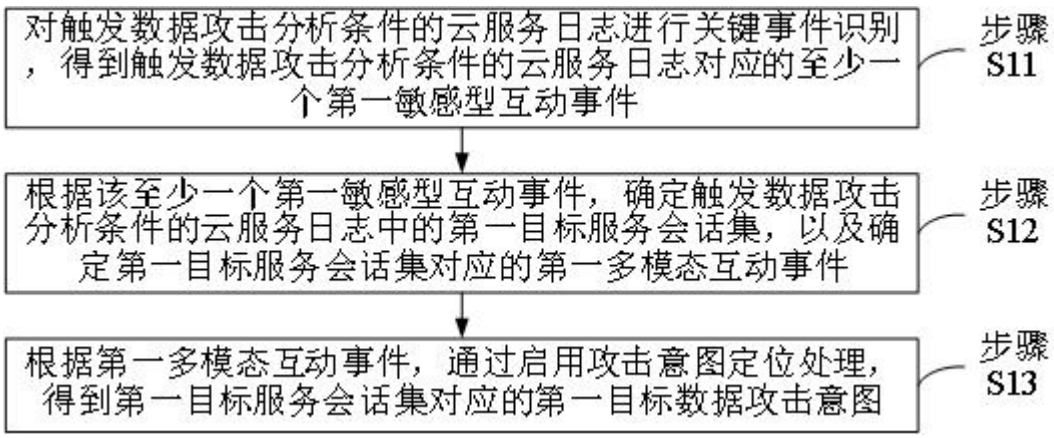

对触发数据攻击分析条件的云服务日志进行关键事件识别，得到触发数据攻击分析条件的云服务日志对应的至少一个第一敏感型互动事件
步骤S11
根据该至少一个第一敏感型互动事件，确定触发数据攻击分析条件的云服务日志中的第一目标服务会话集，以及确定第一目标服务会话集对应的第一多模态互动事件
步骤S12
根据第一多模态互动事件，通过启用攻击意图定位处理，得到第一目标服务会话集对应的第一目标数据攻击意图
步骤S13

图 2


20
互动事件识别模块21
服务会话确定模块22
攻击意图定位模块23

图 3