(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114218568 B
(45)授权公告日 2022.08.23

(21)申请号 202111502860.1
(22)申请日 2021.12.10
(65)同一申请的已公布的文献号
申请公布号 CN 114218568 A
(43)申请公布日 2022.03.22
(73)专利权人 厦门吉快科技有限公司
地址 361000 福建省厦门市火炬高新区软件园三期诚毅北大街65号701室
(72)发明人 徐志全 张红艳
(74)专利代理机构 北京高航知识产权代理有限公司 11530
专利代理师 乔浩刚
(51)Int.Cl.
G06F 21/55(2013.01)
G06F 16/36(2019.01)
G06F 21/56(2013.01)
G06N 20/10(2019.01)

(56)对比文件
CN 112953918 A,2021.06.11
CN 113608882 A,2021.11.05
US 2021357508 A1,2021.11.18
高见等.基于本体的网络威胁情报分析技术研究.《计算机工程与应用》.(第11期),

审查员 刘琪

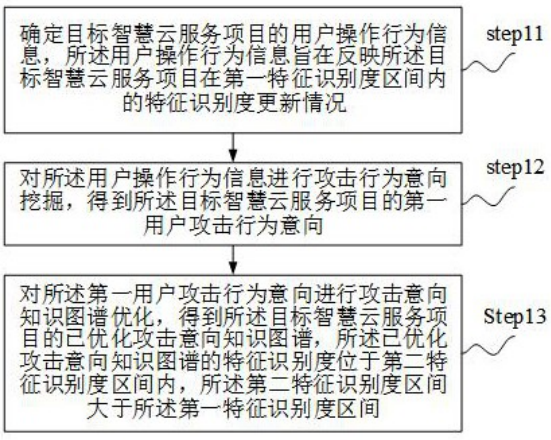
权利要求书3页 说明书20页 附图2页

(54)发明名称

一种应用于云服务的大数据攻击处理方法及系统

(57)摘要

本申请涉及云服务及大数据技术领域,具体而言,涉及一种应用于云服务的大数据攻击处理方法及系统,能够确定目标智慧云服务项目在相对低的第一特征识别度区间内的用户操作行为信息;对用户操作行为信息进行攻击行为意向挖掘,得到用户攻击行为意向;对用户攻击行为意向进行攻击意向知识图谱优化,得到已优化攻击意向知识图谱,从而通过低特征识别度情况下的用户操作行为优化得到高特征识别度情况下的尽可能丰富完整的攻击意向知识图谱,在一定程度上保障攻击意向知识图谱优化的质量,这样能够通过已优化攻击意向知识图谱实现准确可靠的大数据攻击分析和识别,以实现为后续的攻击防护提供准确可信的分析依据。



CN 114218568 B

1.一种应用于云服务的大数据攻击处理方法,其特征在于,应用于大数据攻击处理系统,所述方法至少包括:

确定目标智慧云服务项目的用户操作行为信息,所述用户操作行为信息反映所述目标智慧云服务项目在第一特征识别度区间内的特征识别度更新情况;

对所述用户操作行为信息进行攻击行为意向挖掘,得到所述目标智慧云服务项目的第一用户攻击行为意向,以及对所述第一用户攻击行为意向进行攻击意向知识图谱优化,得到所述目标智慧云服务项目的已优化攻击意向知识图谱,所述已优化攻击意向知识图谱的特征识别度位于第二特征识别度区间内,所述第二特征识别度区间高于所述第一特征识别度区间;

其中,对所述第一用户攻击行为意向进行攻击意向知识图谱优化,得到所述目标智慧云服务项目的已优化攻击意向知识图谱,包括:

依据第一用户行为扰动数据及所述第一用户攻击行为意向,对所述第一用户攻击行为意向进行局部显著性处理,得到第二用户攻击行为意向;

将所述第一用户攻击行为意向与所述第二用户攻击行为意向拼接,得到攻击行为意向拼接结果;

对所述攻击行为意向拼接结果进行攻击意向知识图谱优化,得到所述目标智慧云服务项目的已优化攻击意向知识图谱;

其中,所述方法通过知识库分析模型实现,所述知识库分析模型包括第一攻击行为意向挖掘子模型及攻击意向知识图谱优化子模型,所述第一攻击行为意向挖掘子模型用于对所述用户操作行为信息进行攻击行为意向挖掘,所述攻击意向知识图谱优化子模型用于对所述第一用户攻击行为意向进行攻击意向知识图谱优化,所述方法还包括:

依据指定的模型调试集调试所述知识库分析模型,所述模型调试集包括多个第一范例智慧云服务项目的第一范例用户操作行为信息,多个第二范例智慧云服务项目的第二范例用户操作行为信息及范例智慧云服务项目对应的范例攻击意向知识图谱;

其中,所述第一范例用户操作行为信息是经第三特征识别度区间确定的,所述第二范例用户操作行为信息是经第四特征识别度区间确定的,所述范例智慧云服务项目对应的范例攻击意向知识图谱是经所述第四特征识别度区间确定的,所述第四特征识别度区间高于所述第三特征识别度区间;

其中,所述知识库分析模型还包括支持向量机,所述依据指定的模型调试集调试所述知识库分析模型,包括:

将所述第一范例智慧云服务项目的第一范例用户操作行为信息和所述第二范例智慧云服务项目的第二范例用户操作行为信息分别导入所述第一攻击行为意向挖掘子模型,得到第一范例用户攻击行为意向和第二范例用户攻击行为意向;

将所述第一范例用户攻击行为意向和所述第二范例用户攻击行为意向分别导入所述支持向量机,得到第一类别分析情况和第二类别分析情况;

依据所述第一类别分析情况及所述第二类别分析情况,采用鲁棒性增强策略调试所述知识库分析模型。

2.如权利要求1所述的方法,其特征在于,所述依据指定的模型调试集调试所述知识库分析模型,还包括:

将所述第二范例用户攻击行为意向导入所述攻击意向知识图谱优化子模型，得到所述第二范例智慧云服务项目的第一已优化攻击意向知识图谱；

依据所述第二范例智慧云服务项目的第一已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱，调试所述知识库分析模型。

3.如权利要求2所述的方法，其特征在于，所述知识库分析模型还包括局部显著性处理子模型，所述依据指定的模型调试集调试所述知识库分析模型，还包括：

将所述第二范例用户攻击行为意向及第三用户行为扰动数据导入所述局部显著性处理子模型，得到第四范例用户攻击行为意向；

将所述第二范例用户攻击行为意向与所述第四范例用户攻击行为意向拼接，得到第二范例攻击行为意向拼接结果；

将所述第二范例攻击行为意向拼接结果导入所述攻击意向知识图谱优化子模型，得到所述第二范例智慧云服务项目的第三已优化攻击意向知识图谱；

依据所述第二范例智慧云服务项目的第一已优化攻击意向知识图谱、所述第三已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱，调试所述知识库分析模型。

4.如权利要求1所述的方法，其特征在于，所述知识库分析模型还包括第二攻击行为意向挖掘子模型，所述依据指定的模型调试集调试所述知识库分析模型，还包括：

将所述第二范例智慧云服务项目的第二范例用户操作行为信息及第二用户行为扰动数据导入所述第二攻击行为意向挖掘子模型，得到第三范例用户攻击行为意向；

将所述第二范例用户攻击行为意向与所述第三范例用户攻击行为意向拼接，得到第一范例攻击行为意向拼接结果；

将所述第一范例攻击行为意向拼接结果导入所述支持向量机，得到第三类别分析情况；

依据所述第一类别分析情况及所述第三类别分析情况，采用鲁棒性增强策略调试所述知识库分析模型。

5.如权利要求4所述的方法，其特征在于，所述依据指定的模型调试集调试所述知识库分析模型，还包括：

将所述第一范例攻击行为意向拼接结果导入所述攻击意向知识图谱优化子模型，得到所述第二范例智慧云服务项目的第二已优化攻击意向知识图谱；

依据所述第二范例智慧云服务项目的第二已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱，调试所述知识库分析模型。

6.如权利要求5所述的方法，其特征在于，所述知识库分析模型还包括局部显著性处理子模型，所述依据指定的模型调试集调试所述知识库分析模型，还包括：

将所述第一范例攻击行为意向拼接结果及第四用户行为扰动数据导入所述局部显著性处理子模型，得到第五范例用户攻击行为意向；

将所述第一范例攻击行为意向拼接结果与所述第五范例用户攻击行为意向拼接，得到第三范例攻击行为意向拼接结果；

将所述第三范例攻击行为意向拼接结果导入所述攻击意向知识图谱优化子模型，得到所述第二范例智慧云服务项目的第四已优化攻击意向知识图谱；

依据所述第二范例智慧云服务项目的第二已优化攻击意向知识图谱、所述第四已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱，调试所述知识库分析模型；

相应地，所述依据所述第二范例智慧云服务项目的第二已优化攻击意向知识图谱、所述第四已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱，调试所述知识库分析模型，包括：

依据所述第二范例智慧云服务项目的第二已优化攻击意向知识图谱、所述第四已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱，确定所述知识库分析模型的全局模型性能评价；

依据所述全局模型性能评价，确定所述知识库分析模型的性能变化数据；

依据所述性能变化数据，改进所述第一攻击行为意向挖掘子模型、所述第二攻击行为意向挖掘子模型、所述局部显著性处理子模型及所述攻击意向知识图谱优化子模型的模型变量，其中，所述局部显著性处理子模型的性能变化数据未传输给所述第二攻击行为意向挖掘子模型。

7.一种大数据攻击处理系统，其特征在于，包括处理器、网络模块和存储器；所述处理器和所述存储器通过所述网络模块通信，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1-6任一项所述的方法。

一种应用于云服务的大数据攻击处理方法及系统

技术领域

[0001] 本申请实施例涉及云服务及大数据技术领域，具体涉及一种应用于云服务的大数据攻击处理方法及系统。

背景技术

[0002] 在云服务及大数据环境下，各行业和领域的数据业务需求正在发生改变，从数据采集、数据整合、数据提炼、数据挖掘到数据发布，这一流程已经形成新的完整链条。随着大数据的进一步集中和数据量的爆发式增长，对产业链中的数据进行安全防护变得更加困难。同时，数据的分布式、协作式、开放式处理也加大了数据泄露和被攻击的风险，在大数据的应用过程中，鲜有技术能够实现准确可靠的大数据攻击分析和识别。

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大数据攻击处理方法及系统。

[0004] 第一方面，本申请实施例提供了一种应用于云服务的大数据攻击处理方法，应用于大数据攻击处理系统，所述方法至少包括：确定目标智慧云服务项目的用户操作行为信息，所述用户操作行为信息旨在反映所述目标智慧云服务项目在第一特征识别度区间内的特征识别度更新情况；对所述用户操作行为信息进行攻击行为意向挖掘，得到所述目标智慧云服务项目的第一用户攻击行为意向，以及对所述第一用户攻击行为意向进行攻击意向知识图谱优化，得到所述目标智慧云服务项目的已优化攻击意向知识图谱，所述已优化攻击意向知识图谱的特征识别度位于第二特征识别度区间内，所述第二特征识别度区间大于所述第一特征识别度区间。

[0005] 第二方面，本申请实施例还提供了一种大数据攻击处理系统，包括处理器、网络模块和存储器；所述处理器和所述存储器通过所述网络模块通信，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。

[0006] 相较于现有技术，本申请实施例提供的一种应用于云服务的大数据攻击处理方法及系统具有以下技术效果：在本申请实施例中，能够确定目标智慧云服务项目在相对低的第一特征识别度区间内的用户操作行为信息；对用户操作行为信息进行攻击行为意向挖掘，得到用户攻击行为意向；对用户攻击行为意向进行攻击意向知识图谱优化，得到目标智慧云服务项目在相对高的第二特征识别度区间内的已优化攻击意向知识图谱，从而通过低特征识别度情况下的用户操作行为优化得到高特征识别度情况下的尽可能丰富完整的攻击意向知识图谱，在一定程度上保障攻击意向知识图谱优化的质量，这样能够通过已优化攻击意向知识图谱实现准确可靠的大数据攻击分析和识别，以实现为后续的攻击防护提供准确可信的分析依据。

附图说明

[0007] 图1为本申请实施例所提供的一种大数据攻击处理系统的方框示意图。图2为本申请实施例所提供的一种应用于云服务的大数据攻击处理方法的流程图。图3为本申请实施例所提供的一种应用于云服务的大数据攻击处理装置的框图。

具体实施方式

[0008] 图1示出了本申请实施例所提供的一种大数据攻击处理系统10的方框示意图。本申请实施例中的大数据攻击处理系统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，大数据攻击处理系统10包括：存储器11、处理器12、网络模块13和应用于云服务的大数据攻击处理装置20。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。图2示出了本申请实施例所提供的一种应用于云服务的大数据攻击处理方法的流程图。所述方法有关的流程所定义的方法步骤应用于大数据攻击处理系统10，可以由所述处理器12实现，所述方法包括以下step11-step13所记录的技术方案。

[0009] step11，确定目标智慧云服务项目的用户操作行为信息，所述用户操作行为信息旨在反映所述目标智慧云服务项目在第一特征识别度区间内的特征识别度更新情况。

[0010] step12，对所述用户操作行为信息进行攻击行为意向挖掘，得到所述目标智慧云服务项目的第一用户攻击行为意向。

[0011] step13，对所述第一用户攻击行为意向进行攻击意向知识图谱优化，得到所述目标智慧云服务项目的已优化攻击意向知识图谱，所述已优化攻击意向知识图谱的特征识别度位于第二特征识别度区间内，所述第二特征识别度区间大于所述第一特征识别度区间。

[0012] 在一种可独立实施的实施例中，目标智慧云服务项目可以是包括在线支付、团购业务、政企业务等智慧云服务项目的业务场景。该目标智慧云服务项目可能位于低特征识别度情况下，通过项目操作终端(例如：项目识别模块或信息采集线程等)获取的该目标智慧云服务项目的攻击意向知识图谱识别度不够，攻击意向知识图谱的完整性相对较差。在上述情况下，对于step11而言，通过用户操作行为获取终端(例如：用户操作行为采集线程)，在与低特征识别度情况相对应的第一特征识别度区间内，确定目标智慧云服务项目的用户操作行为信息，该用户操作行为信息旨在反映目标智慧云服务项目在第一特征识别度区间内的特征识别度更新情况。本申请对第一特征识别度区间的真实取值不作过多限定。

[0013] 可以理解的是，对于step12所描述对所述用户操作行为信息进行攻击行为意向挖掘(比如可以理解为特征提取)，得到目标智慧云服务项目的第一用户攻击行为意向而言，可以通过以下相关内容进行说明。在本申请实施例中，该第一用户攻击行为意向至少涵盖表示该目标智慧云服务项目的事项分布的信息。例如：通过大数据攻击分析模型(比如：卷积神经网络)提取用户操作行为信息的攻击行为意向，该大数据攻击分析模型可包括多个信息提取单元(比如：卷积层)、多个信息优化单元(比如：残差层)等，本申请对大数据攻击分析模型的模型架构不进行限定。

[0014] 可以理解的是，对于step13所描述对第一用户攻击行为意向进行攻击意向知识图谱优化，得到该目标智慧云服务项目的已优化攻击意向知识图谱而言，可以通过以下相关内容进行说明。在本申请实施例中，该已优化攻击意向知识图谱可以例如为视觉型知识库，

该已优化攻击意向知识图谱的特征识别度位于与高特征识别度情况对应的第二特征识别度区间内，该第二特征识别度区间大于第一特征识别度区间。

[0015] 在本申请实施例中，可以通过转置攻击分析模型(比如：反卷积神经网络)对第一用户攻击行为意向进行攻击意向知识图谱优化。进一步地，该转置攻击分析模型可包括多个转置信息提取单元(比如：反卷积层)、多个信息优化单元以及信息提取单元等，本申请对第二特征识别度区间的真实取值以及转置攻击分析模型的模型架构不进行限定。

[0016] 综上所述，能够确定目标智慧云服务项目在相对低的第一特征识别度区间内的用户操作行为信息；对用户操作行为信息进行攻击行为意向挖掘，得到用户攻击行为意向；对用户攻击行为意向进行攻击意向知识图谱优化，得到目标智慧云服务项目在相对高的第二特征识别度区间内的已优化攻击意向知识图谱，从而通过低特征识别度情况下的用户操作行为优化得到高特征识别度情况下的尽可能丰富完整的攻击意向知识图谱，在一定程度上保障攻击意向知识图谱优化的质量，这样能够通过已优化攻击意向知识图谱实现准确可靠的大数据攻击分析和识别，以实现为后续的攻击防护提供准确可信的分析依据。

[0017] 在一种可独立实施的实施例中，step13所记录的对所述第一用户攻击行为意向进行攻击意向知识图谱优化，得到所述目标智慧云服务项目的已优化攻击意向知识图谱，示例性地可以包括step131-step133所记录的技术方案。

[0018] step131，依据第一用户行为扰动数据及所述第一用户攻击行为意向，对所述第一用户攻击行为意向进行局部显著性处理，得到第二用户攻击行为意向。

[0019] step132，将所述第一用户攻击行为意向与所述第二用户攻击行为意向拼接，得到攻击行为意向拼接结果。

[0020] step133，对所述攻击行为意向拼接结果进行攻击意向知识图谱优化，得到所述目标智慧云服务项目的已优化攻击意向知识图谱。

[0021] 举例而言，在低特征识别度情况下确定到的用户操作行为信息可能存在较多的用户行为扰动影响及部分的事项分布信息匮乏。在上述情况下，可对第一用户攻击行为意向进行优化，进而便于还原更多的关注度较高的信息。

[0022] 在本申请实施例中，可以设置有任意的第一用户行为扰动数据(比如：噪声数据)，依据该第一用户行为扰动数据为第一用户攻击行为意向增添多余的扰动线程。将增添扰动线程后的第一用户攻击行为意向导入局部显著性处理子模型中进行局部显著性处理，得到第二用户攻击行为意向。该局部显著性处理子模型可以为resnet，包括信息提取单元及多个信息优化单元。本申请对第一用户行为扰动数据的确定方式及局部显著性处理子模型的实际模型架构不进行限定。

[0023] 可以理解，可以将第一用户攻击行为意向与第二用户攻击行为意向进行拼接(比如：融合)，得到攻击行为意向拼接结果(比如：融合特征)；将攻击行为意向拼接结果导入转置攻击分析模型中进行攻击意向知识图谱优化，得到该目标智慧云服务项目的已优化攻击意向知识图谱。如此，可以显著性提高第一用户攻击行为意向中的局部信息，进一步提高已优化攻击意向知识图谱的质量。

[0024] 在一种可独立实施的实施例中，依据本申请实施例的应用于云服务的大数据攻击处理方法可通过知识库分析模型实现，该知识库分析模型至少包括第一攻击行为意向挖掘子模型及攻击意向知识图谱优化子模型，第一攻击行为意向挖掘子模型用于对所述用户操

作行为信息进行攻击行为意向挖掘，例如为大数据攻击分析模型；攻击意向知识图谱优化子模型用于对所述第一用户攻击行为意向进行攻击意向知识图谱优化，例如为转置攻击分析模型。知识库分析模型可以采用其他类型的网络或模型，在实际实施时可依据真实需求进行设置，本申请对此不进行限定。在应用该知识库分析模型之前，可对该知识库分析模型进行调试。

[0025] 在上述内容的基础上，依据本申请实施例的应用于云服务的大数据攻击处理方法示例性地还可以包括：依据指定的模型调试集调试所述知识库分析模型，所述模型调试集包括多个第一范例智慧云服务项目的第一范例用户操作行为信息，多个第二范例智慧云服务项目的第二范例用户操作行为信息及范例智慧云服务项目对应的范例攻击意向知识图谱。

[0026] 在本申请实施例中，所述第一范例用户操作行为信息是经第三特征识别度区间内确定的，所述第二范例用户操作行为信息是经第四特征识别度区间内确定的，所述范例智慧云服务项目对应的范例攻击意向知识图谱是经所述第四特征识别度区间内确定的，所述第四特征识别度区间大于所述第三特征识别度区间。

[0027] 举例而言，可以事先设定有模型调试集，模型调试集中包括多个范例智慧云服务项目，例如：在线支付、团购业务、政企业务等智慧云服务项目。范例智慧云服务项目可分为低特征识别度对应的智慧云服务项目（可称为第一范例智慧云服务项目）和正常特征识别度对应的智慧云服务项目（可称为第二范例智慧云服务项目）。每个第一范例智慧云服务项目包括第一范例用户操作行为信息；每个第二范例智慧云服务项目包括第二范例用户操作行为信息及范例智慧云服务项目对应的范例攻击意向知识图谱。第一范例智慧云服务项目和第二范例智慧云服务项目可以为相同或不同的智慧云服务项目，本申请对此不进行限定。

[0028] 在一种可独立实施的实施例中，在第一范例智慧云服务项目位于与低特征识别度情况相对应的第三特征识别度区间时，可通过用户操作行为获取终端（例如：用户操作行为采集线程）确定第一范例智慧云服务项目的特征识别度更新情况，得到第一范例用户操作行为信息，以便作为知识库分析模型的导入。该第一范例用户操作行为信息涵盖反映该第一范例智慧云服务项目的全局事项分布的信息。第三特征识别度区间可与前述的第一特征识别度区间相同或不同，本申请对此不进行限定。

[0029] 可以理解，低特征识别度情况下的该第一范例用户操作行为信息涵盖反映该第一范例智慧云服务项目的全局事项分布的信息，但不具备显著性信息（比如：攻击意向知识图谱的特征识别度信息）。在上述情况下，可导入高特征识别度情况下的第二范例智慧云服务项目的用户操作行为信息（可称为第二范例用户操作行为信息），以便通过知识库分析模型学习该第二范例用户操作行为信息中的显著性信息。

[0030] 可以理解，在第二范例智慧云服务项目位于与高特征识别度情况相对应的第四特征识别度区间时，可通过用户操作行为获取终端确定第二范例智慧云服务项目的特征识别度更新情况，得到第二范例用户操作行为信息。第四特征识别度区间大于第三特征识别度区间。其中，第四特征识别度区间可与前述的第二特征识别度区间相同或不同，本申请对此不进行限定。其中，第一范例智慧云服务项目的第一范例用户操作行为信息和第二范例智慧云服务项目的第二范例用户操作行为信息的确定方式可与目标智慧云服务项目的用户

操作行为信息的确定思路类似,在此不再进行更多说明。

[0031] 另外,对于位于低特征识别度情况下的第一范例智慧云服务项目,通过项目操作终端获取的目标智慧云服务项目的攻击意向知识图谱的完整性相对较差,无法当作标注信息。在上述情况下,可导入高特征识别度情况下的第二范例智慧云服务项目的范例智慧云服务项目对应的范例攻击意向知识图谱,作为知识库分析模型的标注信息。可通过项目操作终端(例如信息采集线程)在与高特征识别度情况相对应第四特征识别度区间内确定该范例智慧云服务项目对应的范例攻击意向知识图谱。如此,可以提高知识库分析模型的调试效果。

[0032] 在一种可独立实施的实施例中,所述知识库分析模型还包括支持向量机,所述依据指定的模型调试集调试所述知识库分析模型的步骤,示例性地可以包括step201-step203所记录的内容。

[0033] step201,将所述第一范例智慧云服务项目的第一范例用户操作行为信息和所述第二范例智慧云服务项目的第二范例用户操作行为信息分别导入所述第一攻击行为意向挖掘子模型,得到第一范例用户攻击行为意向和第二范例用户攻击行为意向。

[0034] step202,将所述第一范例用户攻击行为意向和所述第二范例用户攻击行为意向分别导入所述支持向量机,得到第一类别分析情况和第二类别分析情况。

[0035] step203,依据所述第一类别分析情况及所述第二类别分析情况,采用鲁棒性增强策略调试所述知识库分析模型。

[0036] 举例而言,知识库分析模型中的支持向量机(比如:鉴别网络)用于对第一攻击行为意向挖掘子模型导出内容进行分类。简单的理解,可通过采用鲁棒性增强策略(比如:对抗策略)调试第一攻击行为意向挖掘子模型(比如:特征提取网络),以使第一攻击行为意向挖掘子模型学习到低特征识别度情况下的第一范例用户操作行为信息和高特征识别度情况下的第二范例用户操作行为信息之间共性描述信息。

[0037] 在本申请实施例中,可以将第一范例智慧云服务项目(比如:样本项目)的第一范例用户操作行为信息和第二范例智慧云服务项目的第二范例用户操作行为信息分别导入到第一攻击行为意向挖掘子模型中处理,导出第一范例用户攻击行为意向和第二范例用户攻击行为意向;将第一范例用户攻击行为意向和第二范例用户攻击行为意向分别导入支持向量机,得到第一类别分析情况(比如:鉴别结果)和第二类别分析情况;依据第一类别分析情况和第二类别分析情况,采用鲁棒性增强策略调试所述知识库分析模型。

[0038] 可以理解,在采用鲁棒性增强策略调试过程中,第一攻击行为意向挖掘子模型倾向模糊第一范例用户攻击行为意向和第二范例用户攻击行为意向,支持向量机倾向识别第一范例用户攻击行为意向和第二范例用户攻击行为意向,通过上述对抗训练,可促使第一攻击行为意向挖掘子模型提取出高特征识别度情况下的行为意向描述与低特征识别度情况下的行为意向描述之间的共性意向描述,使得低特征识别度情况下的第一范例用户攻击行为意向具有高特征识别度情况下的用户操作行为信息的全局性特点,高特征识别度情况下的第二范例用户攻击行为意向具有低特征识别度情况下的用户操作行为信息的全局性特点。换言之,通过迁移学习的思路,使得第一攻击行为意向挖掘子模型同时适用于两种不同状态的数据的攻击行为意向挖掘。本申请对采用鲁棒性增强策略调试的代价函数的选取不进行限定。

[0039] 如此设计，可以使得第一攻击行为意向挖掘子模型能够更加全面完整地挖掘出低特征识别度情况下的用户攻击行为意向，进而提高第一攻击行为意向挖掘子模型的精度和抗干扰程度，以便利用低特征识别度情况下的用户操作行为信息实现高效的攻击意向知识图谱优化。

[0040] 在一种可独立实施的实施例中，所述依据指定的模型调试集调试所述知识库分析模型的步骤，示例性地还可以包括step301和step302所记录的内容。

[0041] step301，将所述第二范例用户攻击行为意向导入所述攻击意向知识图谱优化子模型，得到所述第二范例智慧云服务项目的第一已优化攻击意向知识图谱。

[0042] step302，依据所述第二范例智慧云服务项目的第一已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱，调试所述知识库分析模型。

[0043] 举例而言，在采用鲁棒性增强策略调试后，第一攻击行为意向挖掘子模型挖掘出的第二范例用户攻击行为意向，具有低特征识别度情况下的用户操作行为信息的全局性特点，并且相应的第二范例用户操作行为信息具有标注信息(换言之，高特征识别度情况下的范例智慧云服务项目对应的范例攻击意向知识图谱)。

[0044] 在本申请实施例中，可以将该第二范例用户攻击行为意向导入攻击意向知识图谱优化子模型中处理，导出第二范例智慧云服务项目的第一已优化攻击意向知识图谱；依据第二范例智慧云服务项目的第一已优化攻击意向知识图谱及范例智慧云服务项目对应的范例攻击意向知识图谱之间的对比信息(比如：差异信息)，可确定第一攻击行为意向挖掘子模型及攻击意向知识图谱优化子模型的模型差异(可以理解为网络损失)，进而可以依据该模型差异反馈改进第一攻击行为意向挖掘子模型及攻击意向知识图谱优化子模型的模型变量，实现第一攻击行为意向挖掘子模型及攻击意向知识图谱优化子模型的调试。

[0045] 在实际调试过程中，可进行循环调试。换言之，在每次循环处理的过程中，依据对抗模型差异(对抗网络损失)，反馈改进支持向量机的模型变量。再依据第一攻击行为意向挖掘子模型及攻击意向知识图谱优化子模型的模型差异，反馈改进第一攻击行为意向挖掘子模型及攻击意向知识图谱优化子模型的模型变量，本轮调试中依然会得到支持向量机的输出作为引导，但不优化支持向量机的变量。这样，经过多次循环处理，在符合调试指标(比如：设定指标)的基础上，可得到调试后的知识库分析模型。如此一来，可以实现整个知识库分析模型的调试过程，得到相对完整地知识库分析模型。

[0046] 在一种可独立实施的实施例中，所述知识库分析模型还包括第二攻击行为意向挖掘子模型，所述依据指定的模型调试集调试所述知识库分析模型的步骤，示例性地还可以包括step401-step404所记录的内容。

[0047] step401，将所述第二范例智慧云服务项目的第二范例用户操作行为信息及第二用户行为扰动数据导入所述第二攻击行为意向挖掘子模型，得到第三范例用户攻击行为意向。

[0048] step402，将所述第二范例用户攻击行为意向与所述第三范例用户攻击行为意向拼接，得到第一范例攻击行为意向拼接结果。

[0049] step403，将所述第一范例攻击行为意向拼接结果导入所述支持向量机，得到第三类别分析情况。

[0050] step404，依据所述第一类别分析情况及所述第三类别分析情况，采用鲁棒性增强

策略调试所述知识库分析模型。

[0051] 举例而言，低特征识别度情况下的第一范例用户操作行为信息可能存在一定的用户行为扰动影响，而高特征识别度情况下的第二范例用户操作行为信息中用户行为扰动低下。在上述情况下，可为第二范例用户操作行为信息导入多余的扰动线程，以便提高模型的鲁棒性。

[0052] 可以理解，知识库分析模型还包括第二攻击行为意向挖掘子模型，包括多个信息提取单元及多个信息优化单元，本申请对第二攻击行为意向挖掘子模型的模型架构不进行限定。

[0053] 在本申请实施例中，可以设置有任意的第二用户行为扰动数据，依据该第二用户行为扰动数据为第二范例用户操作行为信息增添扰动线程。将增添扰动线程后的第二范例用户操作行为信息导入第二攻击行为意向挖掘子模型中进行攻击行为意向挖掘，导出第三范例用户攻击行为意向；将所述第二范例用户攻击行为意向与所述第三范例用户攻击行为意向拼接，得到第一范例攻击行为意向拼接结果。如此，可以实现第二范例用户攻击行为意向的行为意向增强处理。

[0054] 在本申请实施例中，将第一范例攻击行为意向拼接结果导入支持向量机，可得到第三类别分析情况；依据第一类别分析情况及所述第三类别分析情况，采用鲁棒性增强策略调试所述知识库分析模型。采用鲁棒性增强策略调试的实际流程不再作过多描述。如此，可进一步提高第一攻击行为意向挖掘子模型的精度。

[0055] 在一种可独立实施的实施例中，所述知识库分析模型还包括第二攻击行为意向挖掘子模型，所述依据指定的模型调试集调试所述知识库分析模型的步骤，示例性地还可以包括step501和step502所记录的内容。

[0056] step501，将所述第一范例攻击行为意向拼接结果导入所述攻击意向知识图谱优化子模型，得到所述第二范例智慧云服务项目的第二已优化攻击意向知识图谱。

[0057] step502，依据所述第二范例智慧云服务项目的第二已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱，调试所述知识库分析模型。

[0058] 举例而言，在采用鲁棒性增强策略调试后，第一攻击行为意向挖掘子模型及第二攻击行为意向挖掘子模型挖掘出的第一范例攻击行为意向拼接结果，具有低特征识别度情况下的用户操作行为信息的全局性特点，并且相应的第二范例用户操作行为信息具有标注信息(换言之，高特征识别度情况下的范例智慧云服务项目对应的范例攻击意向知识图谱)。

[0059] 在本申请实施例中，可将该第一范例攻击行为意向拼接结果导入攻击意向知识图谱优化子模型中处理，导出第二范例智慧云服务项目的第二已优化攻击意向知识图谱；依据第二范例智慧云服务项目的第二已优化攻击意向知识图谱及范例智慧云服务项目对应的范例攻击意向知识图谱之间的对比内容(差异)，可确定第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型及攻击意向知识图谱优化子模型的模型差异；进而可依据该模型差异反馈改进第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型及攻击意向知识图谱优化子模型的模型变量，实现第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型及攻击意向知识图谱优化子模型的调试。

[0060] 在实际调试过程中，同样可进行循环调试。换言之，在每次循环处理的过程中，依

据对抗模型差异，反馈改进支持向量机的模型变量；再依据第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型及攻击意向知识图谱优化子模型的模型差异，反馈改进第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型及攻击意向知识图谱优化子模型的模型变量，本轮调试中依然会得到支持向量机的导出信息作为引导，但不优化支持向量机的变量。如此，通过多次循环处理，在符合调试指标(例如设定指标)的基础上，可得到调试后的知识库分析模型。如此，可以实现整个知识库分析模型的调试过程，得到相对完整地知识库分析模型。

[0061] 在一种可独立实施的实施例中，所述知识库分析模型还包括局部显著性处理子模型，所述依据指定的模型调试集调试所述知识库分析模型的步骤，示例性地还可以包括step601-step604所记录的内容。

[0062] step601，将所述第二范例用户攻击行为意向及第三用户行为扰动数据导入所述局部显著性处理子模型，得到第四范例用户攻击行为意向。

[0063] step602，将所述第二范例用户攻击行为意向与所述第四范例用户攻击行为意向拼接，得到第二范例攻击行为意向拼接结果。

[0064] step603，将所述第二范例攻击行为意向拼接结果导入所述攻击意向知识图谱优化子模型，得到所述第二范例智慧云服务项目的第三已优化攻击意向知识图谱。

[0065] step604，依据所述第二范例智慧云服务项目的第一已优化攻击意向知识图谱、所述第三已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱，调试所述知识库分析模型。

[0066] 举例而言，可以导入局部显著性处理子模型对用户攻击行为意向进行局部显著性处理，以便还原更多的攻击意向知识图谱对应的局部信息(例如局部的事项分布信息)。局部显著性处理子模型可例如为resnet，包括信息提取单元及多个信息优化单元，本申请对局部显著性处理子模型的模型架构不进行限定。

[0067] 在一种可独立实施的实施例中，在没有导入第二攻击行为意向挖掘子模型的基础上，可以直接使用第二范例用户攻击行为意向进行局部显著性处理。可以将设置有任意的第三用户行为扰动数据，依据该第三用户行为扰动数据为第二范例用户攻击行为意向增添扰动线程(比如扰动通道)。将增添扰动线程后的第二范例用户攻击行为意向导入局部显著性处理子模型中处理，得到第四范例用户攻击行为意向；将第二范例用户攻击行为意向与第四范例用户攻击行为意向拼接，得到第二范例攻击行为意向拼接结果；将所述第二范例攻击行为意向拼接结果导入所述攻击意向知识图谱优化子模型，得到所述第二范例智慧云服务项目的第三已优化攻击意向知识图谱。

[0068] 在本申请实施例中，依据所述范例智慧云服务项目的第一已优化攻击意向知识图谱、所述第三已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱，调试所述知识库分析模型。

[0069] 其中，依据第三已优化攻击意向知识图谱与范例智慧云服务项目对应的范例攻击意向知识图谱之间的对比内容(差异)，可确定第一攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型的第一代价；依据第三已优化攻击意向知识图谱与范例智慧云服务项目对应的范例攻击意向知识图谱之间的对比内容(差异)，以及第一已优化攻击意向知识图谱与范例智慧云服务项目对应的范例攻击意向知识图谱之间的对

比内容(差异),可确定第一攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型的第二代价。该第二代价可以确保导入局部显著性处理后的第三已优化攻击意向知识图谱的质量高于没有导入局部显著性处理时的第一已优化攻击意向知识图谱的质量,保证局部显著性处理子模型能够满足实际需求。

[0070] 举例而言,可依据第一代价和第二代价确定第一攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型的全局模型性能评价,例如:将第一代价与第二代价的全局处理结果确定为全局模型性能评价(比如:总体损失);进而可以依据该全局模型性能评价反馈改进第一攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型的模型变量,实现第一攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型的调试。

[0071] 在实际调试过程中,同样可进行循环调试。换言之在每次循环处理的过程中,采用鲁棒性增强策略调试支持向量机;再调试第一攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型,支持向量机的导出信息作为引导,但不优化支持向量机的变量。经过多次循环处理,在符合调试指标(例如设定指标)的基础上,可得到调试后的知识库分析模型。如此,可以实现已优化攻击意向知识图谱的局部显著性处理,进一步提高调试后的知识库分析模型得到的已优化攻击意向知识图谱的质量。

[0072] 在一种可独立实施的实施例中,所述依据指定的模型调试集调试所述知识库分析模型的步骤,示例性地还可以包括step701-step704所记录的内容。

[0073] step701,将所述第一范例攻击行为意向拼接结果及第四用户行为扰动数据导入所述局部显著性处理子模型,得到第五范例用户攻击行为意向。

[0074] step702,将所述第一范例攻击行为意向拼接结果与所述第五范例用户攻击行为意向拼接,得到第三范例攻击行为意向拼接结果。

[0075] step703,将所述第三范例攻击行为意向拼接结果导入所述攻击意向知识图谱优化子模型,得到所述第二范例智慧云服务项目的第四已优化攻击意向知识图谱。

[0076] step704,依据所述第二范例智慧云服务项目的第二已优化攻击意向知识图谱、所述第四已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱,调试所述知识库分析模型。

[0077] 举例而言,在已导入第二攻击行为意向挖掘子模型的基础上,可以通过第一范例攻击行为意向拼接结果进行局部显著性处理。可以将设置有任意的第四用户行为扰动数据,依据该第四用户行为扰动数据为第一范例攻击行为意向拼接结果增添扰动线程。将增添扰动线程后的第一范例攻击行为意向拼接结果导入局部显著性处理子模型中处理,得到第五范例用户攻击行为意向;将第一范例攻击行为意向拼接结果与第五范例用户攻击行为意向拼接,得到第三范例攻击行为意向拼接结果;将所述第三范例攻击行为意向拼接结果导入所述攻击意向知识图谱优化子模型,得到所述第二范例智慧云服务项目的第四已优化攻击意向知识图谱。

[0078] 在一种可独立实施的实施例中,依据所述第二范例智慧云服务项目的第二已优化攻击意向知识图谱、所述第四已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱,调试知识库分析模型。该步骤可以包括step801-step803所记录的内容。

[0079] step801，依据所述第二范例智慧云服务项目的第二已优化攻击意向知识图谱、所述第四已优化攻击意向知识图谱及所述范例智慧云服务项目对应的范例攻击意向知识图谱，确定所述知识库分析模型的全局模型性能评价。

[0080] step802，依据所述全局模型性能评价，确定所述知识库分析模型的性能变化数据。

[0081] step803，依据所述性能变化数据，改进所述第一攻击行为意向挖掘子模型、所述第二攻击行为意向挖掘子模型、所述局部显著性处理子模型及所述攻击意向知识图谱优化子模型的模型变量，其中，所述局部显著性处理子模型的性能变化数据未传输给所述第二攻击行为意向挖掘子模型。

[0082] 举例而言，依据第四已优化攻击意向知识图谱与范例智慧云服务项目对应的范例攻击意向知识图谱之间的对比内容(差异)，可确定第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型的第三代价；依据第四已优化攻击意向知识图谱与范例智慧云服务项目对应的范例攻击意向知识图谱之间的对比内容(差异)，以及第二已优化攻击意向知识图谱与范例智慧云服务项目对应的范例攻击意向知识图谱之间的对比内容(差异)，可确定第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型的第四代价。该第四代价可保证导入局部显著性处理后的第四已优化攻击意向知识图谱的质量优于没有导入局部显著性处理时的第二已优化攻击意向知识图谱的质量，保证局部显著性处理子模型能够满足实际需求。

[0083] 在本申请实施例中，可以依据第三代价和第四代价确定第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型的全局模型性能评价，例如将第三代价与第四代价的全局处理结果确定为全局模型性能评价；依据该全局模型性能评价，可确定第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型的性能变化数据，进而，可在第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型中反馈传递该性能变化数据，从而改进第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型的模型变量，实现第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型的调试。

[0084] 在本申请实施例中，由于第二攻击行为意向挖掘子模型与局部显著性处理子模型的导入均增添了扰动线程，因此，为了规避在前期调试阶段干扰调试结果，在反馈传递性能变化数据(比如：梯度信息)时，局部显著性处理子模型与第二攻击行为意向挖掘子模型之间终止变化特征传输(比如梯度传递)，从而避免局部显著性处理子模型与第二攻击行为意向挖掘子模型之间的相互干扰，保障模型稳定性。

[0085] 在实际调试过程中，同样可进行循环调试。换言之在每次循环处理的过程中，采用鲁棒性增强策略调试支持向量机。再调试第一攻击行为意向挖掘子模型、第二攻击行为意向挖掘子模型、局部显著性处理子模型及攻击意向知识图谱优化子模型，支持向量机的输出作为引导，但不优化支持向量机的变量。经过多次循环处理，在符合调试指标(例如设定指标)的基础上，可得到调试后的知识库分析模型。如此，可以实现已优化攻击意向知识图

谱的局部显著性处理，进一步提高调试后的知识库分析模型得到的已优化攻击意向知识图谱的质量。

[0086] 可以理解的是，依据本申请实施例的应用于云服务的大数据攻击处理方法，通过将迁移学习方法与用户操作行为采集线程结合，利用低特征识别度情况下的用户操作行为信息进行攻击意向知识图谱优化，得到高特征识别度情况下的尽可能丰富完整的攻击意向知识图谱，在一定程度上保障攻击意向知识图谱优化的质量，这样能够通过已优化攻击意向知识图谱实现准确可靠的大数据攻击分析和识别，以实现为后续的攻击防护提供准确可信的分析依据。

[0087] 在上述内容的基础上，在一些可独立实施的设计思路下，在得到所述目标智慧云服务项目的已优化攻击意向知识图谱之后，该方法还可以包括以下内容：根据所述已优化攻击意向知识图谱确定存在隐私信息窃取风险的智慧业务会话日志；借助会话活动兴趣挖掘处理确定所述存在隐私信息窃取风险的智慧业务会话日志中的隐私威胁信息。

[0088] 在本申请实施例中，可以通过已优化攻击意向知识图中的关键图谱节点对应的属性标签确定对应的存在隐私信息窃取风险的智慧业务会话日志。基于此，借助会话活动兴趣挖掘处理确定所述存在隐私信息窃取风险的智慧业务会话日志中的隐私威胁信息，可以通过以下实施方式实现。

[0089] 步骤101，对存在隐私信息窃取风险的智慧业务会话日志执行会话活动兴趣挖掘，得到多个业务状态下的异常活动兴趣描述feature1。

[0090] 步骤102，基于对异常活动兴趣描述feature1执行兴趣描述属性更新，得到每个业务状态下的异常活动兴趣描述feature1对应的异常活动兴趣描述feature2；其中，不同业务状态下的异常活动兴趣描述feature1对应的异常活动兴趣描述feature2的兴趣描述属性一致。

[0091] 步骤103，逐一更新每个业务状态下的异常活动兴趣描述feature2的兴趣描述属性，得到每个业务状态下的异常活动兴趣描述feature2对应的异常活动兴趣描述feature3，其中，每个业务状态下的异常活动兴趣描述feature3的阶段性层面指标的量化分析结果与设定量化分析结果相匹配。

[0092] 步骤104，基于异常活动兴趣描述feature3，确定存在隐私信息窃取风险的智慧业务会话日志中的隐私威胁信息。

[0093] 实施步骤101-步骤104所记录的技术方案，基于对异常活动兴趣描述feature1执行兴趣描述属性更新，得到每个业务状态下的异常活动兴趣描述feature1对应的异常活动兴趣描述feature2，并对每个业务状态下的异常活动兴趣描述feature2的阶段性层面指标进行更新，使得所得的每个业务状态下的异常活动兴趣描述feature2对应的异常活动兴趣描述feature3的阶段性层面指标存在量化相关性，进而可以基于阶段性层面不同的异常活动兴趣描述feature3(通过不同的阶段性层面来反映隐私威胁的不同关注点，进而得到不同关注点下的隐私威胁特征)，确定存在隐私信息窃取风险的智慧业务会话日志中的隐私威胁信息，实现了基于初始会话分布的存在隐私信息窃取风险的智慧业务会话日志，确定存在隐私信息窃取风险的智慧业务会话日志的隐私威胁信息，鉴于无需修改存在隐私信息窃取风险的智慧业务会话日志的会话分布结构，在保证隐私威胁信息检测精度的同时，减少了隐私威胁信息检测的软硬件资源开销，在一定程度上提升了隐私威胁检测的效率。

[0094] 对于步骤101-步骤104所描述的技术方案,具体可以通过如下描述内容进行说明。

[0095] 可以理解的是,对于步骤101所描述的对存在隐私信息窃取风险的智慧业务会话日志执行会话活动兴趣挖掘,得到多个业务状态下的异常活动兴趣描述feature1。

[0096] 在本申请实施例中,第一个业务状态下的异常活动兴趣描述feature1是对存在隐私信息窃取风险的智慧业务会话日志执行会话活动兴趣挖掘所得的,存在关联的两个业务状态下的异常活动兴趣描述feature1中的后一个业务状态下的异常活动兴趣描述feature1是对存在关联的两个业务状态下的异常活动兴趣描述feature1中的前一个业务状态下的异常活动兴趣描述feature1执行会话活动兴趣挖掘所得的。

[0097] 可以理解的是,隐私信息窃取风险的存在性判定可以根据预先设置的规则实现,比如通过时段条件或者业务类型条件进行判断。因此,存在隐私信息窃取风险的智慧业务会话日志可以理解为待处理的智慧业务会话日志,该会话日志可以是流式记录的日志文本或者图文信息。进一步地,会话互动兴趣挖掘可以理解为特征提取(对应于异常活动兴趣描述的提取)。

[0098] 本申请实施例中,对存在隐私信息窃取风险的智慧业务会话日志执行会话活动兴趣挖掘,得到多个业务状态下的异常活动兴趣描述feature1时,可以通过多个业务状态下的第一AI机器学习模型(比如CNN)对存在隐私信息窃取风险的智慧业务会话日志执行会话活动兴趣挖掘,得到每一个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1。进一步地,多个业务状态下的第一AI机器学习模型形成的机器学习模型可以理解为对存在隐私信息窃取风险的智慧业务会话日志中涵盖的隐私威胁信息进行检测的其中一个机器学习模型,在实际实施时,对待检测智慧业务会话日志中涵盖的隐私威胁信息进行检测的机器学习模型可以分割(拆分或者划分)为多个进程(多个阶段)的AI机器学习模型,每一进程的AI机器学习模型对应一个业务状态下的第一AI机器学习模型。其中,多个业务状态下的第一AI机器学习模型的结构可以根据真实业务需求进行设置,本申请实施例在此不作更多说明。

[0099] 举例而言,若多个业务状态下的第一AI机器学习模型包括第一个业务状态下的第一AI机器学习模型、第二个业务状态下的第一AI机器学习模型、第三个业务状态下的第一AI机器学习模型,则第一个业务状态下的第一AI机器学习模型可以对存在隐私信息窃取风险的智慧业务会话日志进行兴趣特征分析,得到第一个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1;并将第一个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1传输至第二个业务状态下的第一AI机器学习模型,第二个业务状态下的第一AI机器学习模型对获取到的异常活动兴趣描述feature1进行兴趣特征分析,得到第二个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1;再将第二个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1传输至第三个业务状态下的第一AI机器学习模型,第三个业务状态下的第一AI机器学习模型对获取到的异常活动兴趣描述feature1进行兴趣特征分析,得到第三个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1,进而得到了每一个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1。其中,由于第一个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1经过的兴趣特征分析的次数较少,因此第一个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1的局部描述较丰富、全局

描述较匮乏;而第三个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1经过的兴趣特征分析的次数较多,故第三个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1的全局描述较多(即异常活动兴趣描述feature1中涵盖的与隐私威胁信息相关的描述内容较丰富)、局部描述较匮乏。

[0100] 在本申请实施例中,存在隐私信息窃取风险的智慧业务会话日志可以为涵盖隐私威胁信息的任一智慧业务会话日志。其中,存在隐私信息窃取风险的智慧业务会话日志的持续时段可以为随机持续时段,例如:存在隐私信息窃取风险的智慧业务会话日志的持续时段可以为15min、25min等。在实际实施时,可以基于多个业务状态下的第一AI机器学习模型确定智慧业务会话日志检测持续时段,在存在隐私信息窃取风险的智慧业务会话日志的持续时段超过智慧业务会话日志检测持续时段时,可以将存在隐私信息窃取风险的智慧业务会话日志分割为多个智慧业务会话日志,使得分割后的每个智慧业务会话日志的持续时段与智慧业务会话日志检测持续时段一致。比如:若存在隐私信息窃取风险的智慧业务会话日志的持续时段为1.5小时时,确定的智慧业务会话日志检测持续时段为15min,则可以将存在隐私信息窃取风险的智慧业务会话日志分割为6个持续时段为15min的智慧业务会话日志,多个业务状态下的第一AI机器学习模型分别对每个15min的智慧业务会话日志执行会话活动兴趣挖掘,确定每个15min智慧业务会话日志对应的隐私威胁信息,进而得到该存在隐私信息窃取风险的智慧业务会话日志的隐私威胁信息。

[0101] 在本申请实施例中,异常活动兴趣描述feature1可以包括四个层面下的兴趣描述属性(比如,参数信息)。举例而言,如果多个业务状态下的第一AI机器学习模型为三个层面下的AI机器学习模型(还可以为卷积神经网络),则可以得到存在隐私信息窃取风险的智慧业务会话日志的异常活动兴趣描述feature1,该异常活动兴趣描述feature1可以包括四个层面下的兴趣描述属性;若多个业务状态下的第一AI机器学习模型为两个层面下的AI机器学习模型,则可以通过多个业务状态下的第一AI机器学习模型执行会话活动兴趣挖掘,得到存在隐私信息窃取风险的智慧业务会话日志中每组会话事件对应的异常活动兴趣描述,将所得的存在隐私信息窃取风险的智慧业务会话日志中每组会话事件关键词的异常活动兴趣描述依据阶段性层面进行整合,得到存在隐私信息窃取风险的智慧业务会话日志对应的异常活动兴趣描述feature1。

[0102] 可以理解的是,对于步骤102而言,基于对异常活动兴趣描述feature1执行兴趣描述属性更新,得到每个业务状态下的异常活动兴趣描述feature1对应的异常活动兴趣描述feature2。

[0103] 举例而言,将第一个业务状态下的异常活动兴趣描述feature1的兴趣描述属性、第二个业务状态下的异常活动兴趣描述feature1的兴趣描述属性、以及第三个业务状态下的异常活动兴趣描述feature1的兴趣描述属性更新为相同。

[0104] 对于一种可独立实施的技术方案而言,步骤102所记录的基于对异常活动兴趣描述feature1执行兴趣描述属性更新,得到每个业务状态下的异常活动兴趣描述feature1对应的异常活动兴趣描述feature2,示例性的可以包括如下内容:确定每个业务状态下的异常活动兴趣描述feature1对应的兴趣描述属性中量化约束最少的异常活动兴趣描述feature1,并将除量化约束最少的异常活动兴趣描述feature1外的剩余异常活动兴趣描述feature1,更新为与该量化约束最少的异常活动兴趣描述feature1相同兴趣描述属性的异

常活动兴趣描述，将量化约束最少的异常活动兴趣描述feature1，以及更新后与该量化约束最少的异常活动兴趣描述feature1相同兴趣描述属性的异常活动兴趣描述作为异常活动兴趣描述feature2；或者，将每个业务状态下的异常活动兴趣描述feature1更新为设定兴趣描述属性下的异常活动兴趣描述，将该设定兴趣描述属性下的异常活动兴趣描述作为异常活动兴趣描述feature2。

[0105] 在本申请实施例中，若多个业务状态下的异常活动兴趣描述feature1包括第一个业务状态下的异常活动兴趣描述feature1、第二个业务状态下的异常活动兴趣描述feature1、第三个业务状态下的异常活动兴趣描述feature1，则确定第一个业务状态下的异常活动兴趣描述feature1、第二个业务状态下的异常活动兴趣描述feature1、第三个业务状态下的异常活动兴趣描述feature1中，量化约束最少的异常活动兴趣描述feature1，则确定第三个业务状态下的异常活动兴趣描述feature1对应的兴趣描述属性中量化约束最少，则分别将第一个业务状态下的异常活动兴趣描述feature1以及第二个业务状态下的异常活动兴趣描述feature1的兴趣描述属性进行更新，使得更新后的每个业务状态下的异常活动兴趣描述feature2的兴趣描述属性互相之间存在一致性。

[0106] 或者，确定一个设定兴趣描述属性，将每个业务状态下的异常活动兴趣描述feature1更新为设定兴趣描述属性下的异常活动兴趣描述，将该设定兴趣描述属性下的异常活动兴趣描述作为异常活动兴趣描述feature2。可以理解，设定兴趣描述属性中的量化约束不大于每个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1对应的兴趣描述属性中量化约束最少的异常活动兴趣描述feature1的兴趣描述属性。

[0107] 如此设计，将每个业务状态下的第一异常活动兴趣描述feature1更新为较少的量化约束，在对存在隐私信息窃取风险的智慧业务会话日志中涵盖的隐私威胁信息进行检测时，可以减少隐私威胁信息检测的软硬件资源开销，进而在一定程度上提升了隐私威胁检测的效率。

[0108] 对于一种可独立实施的技术方案而言，步骤101所记录的对存在隐私信息窃取风险的智慧业务会话日志执行会话活动兴趣挖掘，得到多个业务状态下的异常活动兴趣描述feature1，示例性地可以包括：通过多个业务状态下的第一AI机器学习模型对存在隐私信息窃取风险的智慧业务会话日志执行会话活动兴趣挖掘，得到每一个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1。

[0109] 在上述内容的基础上，步骤102所记录的基于对异常活动兴趣描述feature1执行兴趣描述属性更新，得到每个业务状态下的异常活动兴趣描述feature1对应的异常活动兴趣描述feature2，示例性的可以包括步骤201和步骤202所记录的技术方案。

[0110] 步骤201，根据确定的更新后的兴趣描述属性，以及每一个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1的兴趣描述属性，确定该业务状态下的第一AI机器学习模型对应的第二AI机器学习模型的模型变量数据。

[0111] 步骤202，结合涵盖了确定的模型变量数据的每一个业务状态下的第二AI机器学习模型，对该业务状态下的第二AI机器学习模型对应的第一AI机器学习模型导出的异常活动兴趣描述feature1进行兴趣特征分析，得到该业务状态下的第二AI机器学习模型导出的异常活动兴趣描述feature2。

[0112] 在本申请实施例中，可以根据确定的更新后的兴趣描述属性，以及每一个业务状

态下的第一AI机器学习模型导出的异常活动兴趣描述feature1的兴趣描述属性，分别确定第一个业务状态下的第一AI机器学习模型对应的第二AI机器学习模型的模型变量数据、第二个业务状态下的第一AI机器学习模型对应的第二AI机器学习模型的模型变量数据、第三个业务状态下的第一AI机器学习模型对应的第二AI机器学习模型的模型变量数据。

[0113] 举例而言，第一个业务状态下的第一AI机器学习模型对应的涵盖了模型变量数据(比如，模型参数信息)的第二AI机器学习模型，对第一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature1进行兴趣特征分析，得到该业务状态下的第二AI机器学习模型导出的异常活动兴趣描述feature2。逐一类推，第二个业务状态下的第一AI机器学习模型对应的涵盖了模型变量数据的第二AI机器学习模型，对第二个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature1进行兴趣特征分析，得到该业务状态下的第二AI机器学习模型导出的异常活动兴趣描述feature2。第三个业务状态下的第一AI机器学习模型对应的涵盖了模型变量数据的第二AI机器学习模型，对第三个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature1进行兴趣特征分析，得到该业务状态下的第二AI机器学习模型导出的异常活动兴趣描述feature2。

[0114] 如此设计，通过确定每个业务状态下的第二AI机器学习模型的模型变量数据，并结合涵盖了确定的模型变量数据的每一个业务状态下的第二AI机器学习模型，对对应的异常活动兴趣描述feature1进行兴趣特征分析，实现了将每个业务状态下的第一AI机器学习模型导出的异常活动兴趣描述feature1的兴趣描述属性中的量化约束更新为较少的量化约束，进而使得对存在隐私信息窃取风险的智慧业务会话日志进行分析时，减少了软硬件资源开销，在一定程度上提升了隐私威胁检测的效率。

[0115] 可以理解的是，对于步骤103而言：本申请实施例中，可以对每个业务状态下的异常活动兴趣描述feature2的兴趣描述属性进行更新，得到每个业务状态下的异常活动兴趣描述feature2对应的异常活动兴趣描述feature3，使得所得的每个业务状态下的异常活动兴趣描述feature3的阶段性层面指标的量化分析结果与设定量化分析结果相匹配。其中，每一个业务状态下的异常活动兴趣描述feature3的阶段性层面指标(比如时间维度值)与其覆盖范围相关。在实际实施时，异常活动兴趣描述经过兴趣特征分析的次数越少，覆盖范围越小，则对应的阶段性层面指标设置的较大时，才能相对精确的确定存在隐私信息窃取风险的智慧业务会话日志中的隐私威胁信息；反之，异常活动兴趣描述经过兴趣特征分析的次数越多，覆盖范围越大，则为了减少软硬件资源开销，则可以将对应的阶段性层面指标的较少，实现了在保证存在隐私信息窃取风险的智慧业务会话日志检测的精度的同时，尽量减少软硬件资源开销，提高隐私威胁检测效率。比如，第一个业务状态下的异常活动兴趣描述feature3与第二个业务状态下的异常活动兴趣描述feature3之间的阶段性层面指标的量化分析结果可以设置为2:6或者4:16等。

[0116] 对于一种可独立实施的技术方案而言，103所记录的逐一更新每个业务状态下的异常活动兴趣描述feature2的兴趣描述属性，得到每个业务状态下的异常活动兴趣描述feature2对应的异常活动兴趣描述feature3，示例性地可以包括步骤301-步骤303所记录的技术方案。

[0117] 步骤301，基于不同业务状态下的第一AI机器学习模型之间的阶段性层面指标的量化分析结果，以及每一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述

feature2的阶段性层面指标，确定每个业务状态下的第一AI机器学习模型分别对应的异常活动兴趣描述feature3的阶段性层面指标。

[0118] 步骤302，根据确定的每个业务状态下的第一AI机器学习模型分别对应的异常活动兴趣描述feature3的阶段性层面指标，以及每一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature2的阶段性层面指标，确定该业务状态下的第一AI机器学习模型对应的第三AI机器学习模型的模型变量数据。

[0119] 步骤303，结合涵盖了确定的模型变量数据的每一个业务状态下的第三AI机器学习模型，对该业务状态下的第三AI机器学习模型对应的异常活动兴趣描述feature2进行兴趣特征分析，得到该业务状态下的第三AI机器学习模型导出的异常活动兴趣描述feature3。

[0120] 本申请实施例中，不同业务状态下的第一AI机器学习模型之间的阶段性层面指标的量化分析结果可以根据真实业务需求进行设置，例如：若多个业务状态下的第一AI机器学习模型包括第一个业务状态下的第一AI机器学习模型、第二个业务状态下的第一AI机器学习模型、第三个业务状态下的第一AI机器学习模型，则不同业务状态下的第一AI机器学习模型之间的阶段性层面指标的量化分析结果(比如可以是比例)可以为1:4:6，也可以为1:5:10等。进一步的，若每一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature2的阶段性层面指标(比如，时间维度值)为32，阶段性层面指标的量化分析结果为1:4:6，则可以确定第一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3的阶段性层面指标为8第二个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3的阶段性层面指标为16，第三个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3的阶段性层面指标为32。

[0121] 本申请实施例中，可以根据上述的相关内容确定每一个业务状态下的第一AI机器学习模型对应的第三AI机器学习模型的模型变量数据。比如，可以通过为每一个业务状态下的第三AI机器学习模型设置不同的时维间隔，使得每个业务状态下的第三AI机器学习模型导出的异常活动兴趣描述feature3的阶段性层面指标与设置的量化分析结果相同。

[0122] 示例性的，第一个业务状态下的第一AI机器学习模型对应的涵盖了模型变量数据的第三AI机器学习模型，对该业务状态下的对应的异常活动兴趣描述feature2进行兴趣特征分析，得到该业务状态下的第三AI机器学习模型导出的异常活动兴趣描述feature3。逐一推导，第二个业务状态下的第一AI机器学习模型对应的涵盖了模型变量数据的第三AI机器学习模型，对该业务状态下的对应的异常活动兴趣描述feature2进行兴趣特征分析，得到该业务状态下的第三AI机器学习模型导出的异常活动兴趣描述feature3。第三个业务状态下的第一AI机器学习模型对应的涵盖了模型变量数据的第三AI机器学习模型，对该业务状态下的对应的异常活动兴趣描述feature2进行兴趣特征分析，得到该业务状态下的第三AI机器学习模型导出的异常活动兴趣描述feature3。

[0123] 实施步骤301-步骤303所记录的内容，通过修改每一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature2的阶段性层面指标，使得所得的每一个业务状态下的第三AI机器学习模型导出的异常活动兴趣描述feature3的阶段性层面指标与设置的量化分析结果相匹配(相当于修改了存在隐私信息窃取风险的智慧业务会话日志中包括的隐私威胁信息的关注点)，使得基于更新阶段性层面指标后的异常活动兴趣描述

feature3,能够相对精确的对存在隐私信息窃取风险的智慧业务会话日志中包括的隐私威胁信息进行识别,进而在一定程度上提升了隐私威胁检测的精确性。

[0124] 可以理解的是,对于步骤104而言:本申请实施例中,可以将每个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3进行连接,并将异常活动兴趣描述feature3连接后所得的异常活动兴趣描述导入到测试机器学习模型中,得到存在隐私信息窃取风险的智慧业务会话日志中包括的隐私威胁信息。若存在隐私信息窃取风险的智慧业务会话日志中包括多个隐私威胁信息,则可以得到存在隐私信息窃取风险的智慧业务会话日志中包括的每一隐私威胁信息。

[0125] 对于一种可独立实施的技术方案而言,步骤104所记录的基于异常活动兴趣描述feature3,确定存在隐私信息窃取风险的智慧业务会话日志中的隐私威胁信息,示例性地可以包括步骤401和步骤402所记录的内容。

[0126] 步骤401,将每个业务状态下的异常活动兴趣描述feature2对应的异常活动兴趣描述feature3进行连接处理,得到完成连接的异常活动兴趣描述feature4。

[0127] 步骤402,基于异常活动兴趣描述feature4,确定存在隐私信息窃取风险的智慧业务会话日志中的隐私威胁信息。

[0128] 在本申请实施例中,在得到每个业务状态下的异常活动兴趣描述feature2对应的异常活动兴趣描述feature3之后,可以将每个业务状态下的异常活动兴趣描述feature3进行连接处理,得到完成连接的异常活动兴趣描述feature4,在基于异常活动兴趣描述feature4,确定存在隐私信息窃取风险的智慧业务会话日志中的隐私威胁信息。

[0129] 实施步骤401和步骤402所记录的内容,将所得的每个业务状态下的异常活动兴趣描述feature2对应的异常活动兴趣描述feature3进行连接处理,使得所得的异常活动兴趣描述feature4可以包括阶段性层面指标不同的异常活动兴趣描述feature3的特征,进而基于异常活动兴趣描述feature4确定存在隐私信息窃取风险的智慧业务会话日志中的隐私威胁信息时,能够提升隐私威胁检测的精确性。

[0130] 对于一种可独立实施的技术方案而言,上述步骤401所记录的将每个业务状态下的异常活动兴趣描述feature2对应的异常活动兴趣描述feature3进行连接处理,得到完成连接的异常活动兴趣描述feature4,示例性地可以包括如下内容:依据预设的连接方式,将每个业务状态下的异常活动兴趣描述feature2对应的异常活动兴趣描述feature3逐一进行连接处理,得到每一轮完成连接的过渡异常活动兴趣描述;基于每一轮完成连接的过渡异常活动兴趣描述,得到异常活动兴趣描述feature4。

[0131] 在本申请实施例中,可以设定异常活动兴趣描述feature3的连接方式(可以理解为融合顺序),将每个业务状态下的异常活动兴趣描述feature2对应的异常活动兴趣描述feature3依据预设的连接方式,逐一进行连接处理,得到每一轮完成连接的过渡异常活动兴趣描述。

[0132] 举例而言,若预设的连接方式为:第一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3、第二个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3、第三个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3,则可以先将第一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3与第二个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3

进行连接,得到第一轮完成连接的过渡异常活动兴趣描述;在将所得的完成连接的过渡异常活动兴趣描述与第三个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3进行连接,得到第二轮完成连接的过渡异常活动兴趣描述。在可以基于每一轮完成连接的过渡异常活动兴趣描述,得到异常活动兴趣描述feature4。

[0133] 可以理解,第一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3与第二个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3进行连接时,可以先将第一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3进行上采样操作,在将上采样操作后的第一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3与第二个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3进行连接,得到第一轮完成连接的过渡异常活动兴趣描述。每一轮的连接过程,可以参考第一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3与第二个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3进行连接的过程,本申请实施例在此不作过多描述。

[0134] 举例而言,若第一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3的兴趣描述属性为value1,第二个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3的兴趣描述属性为value2,则可以先将第一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3进行上采样操作,上采样操作后的第一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3的兴趣描述属性为value2;然后将上采样操作后的第一个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3中每一活动兴趣描述事项的描述值,与第二个业务状态下的第一AI机器学习模型对应的异常活动兴趣描述feature3中对应的活动兴趣描述事项的描述值进行整合,得到第一轮完成连接的过渡异常活动兴趣描述,其中,该第一轮完成连接的过渡异常活动兴趣描述的兴趣描述属性为value2。

[0135] 对于一种可独立实施的技术方案而言,将每个业务状态下的异常活动兴趣描述feature2对应的异常活动兴趣描述feature3作为第一个业务状态下的异常活动兴趣描述feature3至第X个业务状态下的异常活动兴趣描述feature3,其中第X个业务状态下的异常活动兴趣描述feature3的阶段性层面指标大于第X-1个业务状态下的异常活动兴趣描述feature3的阶段性层面指标,X为大于1的正整数。则依据预设的连接方式,将每个业务状态下的异常活动兴趣描述feature2对应的异常活动兴趣描述feature3逐一进行连接处理,得到每一轮完成连接的过渡异常活动兴趣描述,包括以下几项设计思路中的其中一种。

[0136] 第一项设计思路:依据从第一个业务状态下的异常活动兴趣描述feature3到第X个业务状态下的异常活动兴趣描述feature3的连接方式,逐一将每个业务状态下的异常活动兴趣描述feature3进行连接处理,分别得到每一轮完成连接的异常活动兴趣描述,将第一个业务状态下的异常活动兴趣描述feature3以及每一轮完成连接的异常活动兴趣描述,作为所得的过渡异常活动兴趣描述。

[0137] 第二项设计思路:依据从第X个业务状态下的异常活动兴趣描述feature3到第一个业务状态下的异常活动兴趣描述feature3的连接方式,逐一将每个业务状态下的异常活动兴趣描述feature3进行连接处理,分别得到每一轮完成连接的异常活动兴趣描述,将第X个业务状态下的异常活动兴趣描述feature3以及每一轮完成连接的异常活动兴趣描述,作

为得到过渡异常活动兴趣描述。

[0138] 第三项设计思路:依据从第一个业务状态下的异常活动兴趣描述feature3到第X个业务状态下的异常活动兴趣描述feature3的连接方式,将每个业务状态下的异常活动兴趣描述feature3进行连接处理,分别得到从第一个业务状态下的异常活动兴趣描述feature3到第X个业务状态下的异常活动兴趣描述feature3进行连接处理时每一轮完成连接的异常活动兴趣描述,分别对第一个业务状态下的异常活动兴趣描述feature3以及每一轮完成连接的异常活动兴趣描述进行兴趣特征分析,得到第一个业务状态下的连接异常活动兴趣描述至第X个业务状态下的连接异常活动兴趣描述,其中,每一个业务状态下的连接异常活动兴趣描述的兴趣描述属性与兴趣特征分析前对应的异常活动兴趣描述的兴趣描述属性一致;依据从第X个业务状态下的连接异常活动兴趣描述到第一个业务状态下的连接异常活动兴趣描述的连接方式,逐一将每个业务状态下的连接异常活动兴趣描述进行连接处理,分别得到从第X个业务状态下的连接异常活动兴趣描述到第一个业务状态下的连接异常活动兴趣描述进行连接处理时每一轮完成连接的异常活动兴趣描述,将每一轮完成连接的异常活动兴趣描述以及第X个业务状态下的连接异常活动兴趣描述,作为所得的过渡异常活动兴趣描述。

[0139] 第四项设计思路:依据从第一个业务状态下的异常活动兴趣描述feature3到第X个业务状态下的异常活动兴趣描述feature3的连接方式,将每个业务状态下的异常活动兴趣描述feature3进行连接处理,分别得到每一轮完成连接的异常活动兴趣描述,将第一个业务状态下的异常活动兴趣描述feature3以及从第一个业务状态下的异常活动兴趣描述feature3到第X个业务状态下的异常活动兴趣描述feature3进行连接处理时每一轮完成连接的异常活动兴趣描述,作为所得的第一过渡异常活动兴趣描述,并依据从第X个业务状态下的异常活动兴趣描述feature3到第一个业务状态下的异常活动兴趣描述feature3的连接方式,将每个业务状态下的异常活动兴趣描述feature3进行连接处理,分别得到每一轮完成连接的异常活动兴趣描述,将第X个业务状态下的异常活动兴趣描述feature3以及从第X个业务状态下的异常活动兴趣描述feature3到第一个业务状态下的异常活动兴趣描述feature3进行连接处理时每一轮完成连接的异常活动兴趣描述,作为所得的第二过渡异常活动兴趣描述;将第一过渡异常活动兴趣描述和第二过渡异常活动兴趣描述作为所得的过渡异常活动兴趣描述。

[0140] 在上述内容的基础上,对于一些可独立实施的设计思路而言,在确定所述存在隐私信息窃取风险的智慧业务会话日志中的隐私威胁信息之后,该方法还可以包括以下内容:根据所述隐私威胁信息执行对应的隐私威胁防护措施。

[0141] 在上述内容的基础上,对于一些可独立实施的设计思路而言,根据所述隐私威胁信息执行对应的隐私威胁防护措施,可以包括以下内容:根据所述隐私威胁信息确定待进行匿名化处理的目标个体用户信息;对所述目标个体用户信息中的多个个体用户信息片段分别进行共享型使用需求解析和独占型使用需求解析,得到共享型使用需求解析结果集和独占型使用需求解析结果集;通过第一指定调整策略,对所述共享型使用需求解析结果集进行第一调整处理,得到包括有共享型使用需求的第一个体用户信息簇;通过第二指定调整策略,对所述独占型使用需求解析结果集进行第二调整处理,得到包括有独占型使用需求的第二个体用户信息簇;基于所述第一个体用户信息簇和所述第二个体用户信息簇进行

下采样处理，得到所述目标个体用户信息中与目标使用需求相匹配的目标个体用户信息簇；所述目标使用需求包括共享型使用需求和独占型使用需求中的至少一种，所述目标个体用户信息簇用于对所述目标个体用户信息进行匿名化处理；基于所述目标个体用户信息簇对所述目标个体用户信息中的至少部分进行匿名化处理。如此设计，能够通过考虑不同的使用需求从而实现针对性的信息匿名化处理，从而实现准确可靠的隐私威胁防护。

[0142] 基于上述同样的发明构思，还提供了一种应用于云服务的大数据攻击处理装置20，应用于大数据攻击处理系统10，所述装置包括：

[0143] 行为信息确定模块21，用于确定目标智慧云服务项目的用户操作行为信息，所述用户操作行为信息旨在反映所述目标智慧云服务项目在第一特征识别度区间内的特征识别度更新情况；

[0144] 行为意向挖掘模块22，用于对所述用户操作行为信息进行攻击行为意向挖掘，得到所述目标智慧云服务项目的第一用户攻击行为意向；

[0145] 知识图谱优化模块23，用于对所述第一用户攻击行为意向进行攻击意向知识图谱优化，得到所述目标智慧云服务项目的已优化攻击意向知识图谱，所述已优化攻击意向知识图谱的特征识别度位于第二特征识别度区间内，所述第二特征识别度区间大于所述第一特征识别度区间。

[0146] 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。

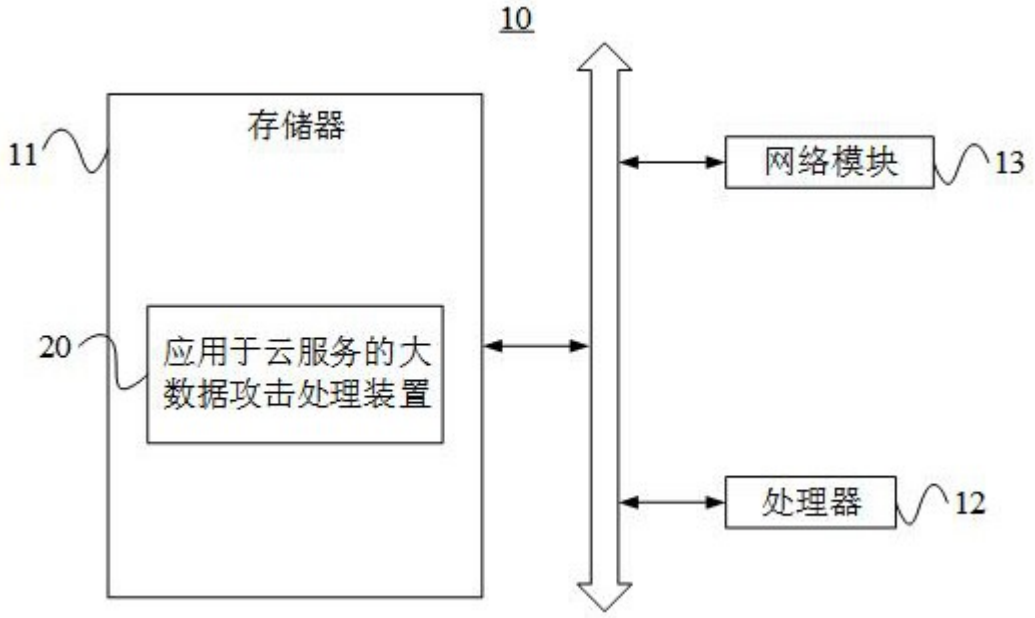

10
存储器
11
网络模块
13
20
应用于云服务的大数据攻击处理装置
处理器
12

图1

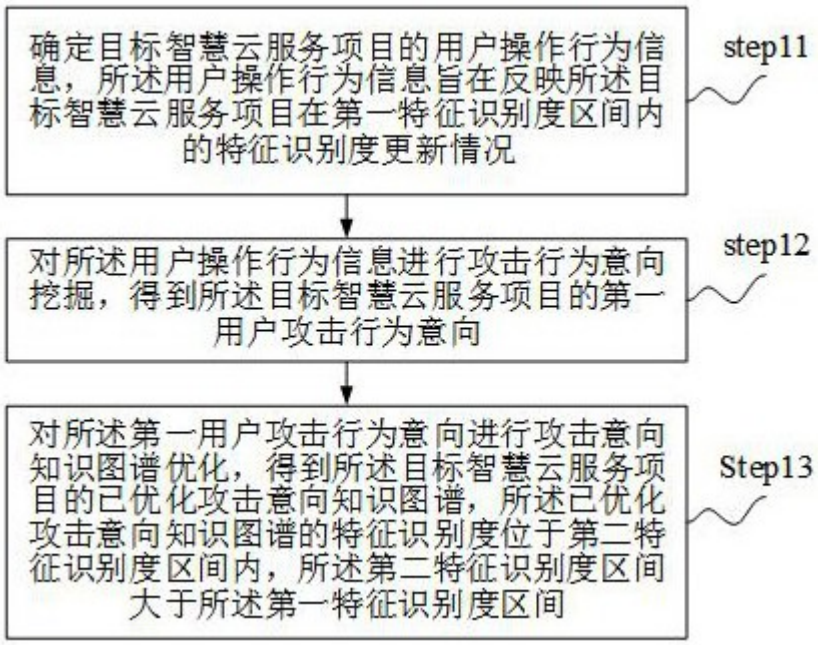

确定目标智慧云服务项目的用户操作行为信息，所述用户操作行为信息旨在反映所述目标智慧云服务项目在第一特征识别度区间内的特征识别度更新情况
step11
对所述用户操作行为信息进行攻击行为意向挖掘，得到所述目标智慧云服务项目的第一用户攻击行为意向
step12
对所述第一用户攻击行为意向进行攻击意向知识图谱优化，得到所述目标智慧云服务项目的已优化攻击意向知识图谱，所述已优化攻击意向知识图谱的特征识别度位于第二特征识别度区间内，所述第二特征识别度区间大于所述第一特征识别度区间
Step13

图2

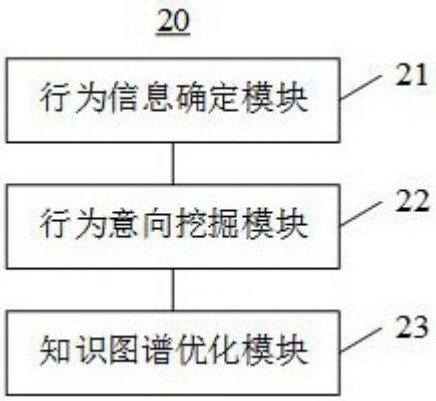


图3