(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 113706177 B
(45)授权公告日 2022.04.29

(21)申请号 202111028016.X
(22)申请日 2021.09.02
(65)同一申请的已公布的文献号
申请公布号 CN 113706177 A
(43)申请公布日 2021.11.26
(73)专利权人 广东奥飞数据科技股份有限公司
地址 510000 广东省广州市南沙区南沙街进港大道8号1508房
(72)发明人 赵琦 林楠
(74)专利代理机构 东莞市神州众达专利商标事务所(普通合伙) 44251
代理人 周松强
(51)Int.Cl.
G06Q 30/00(2012.01)
G06F 11/34(2006.01)
G06F 16/35(2019.01)
G06F 40/205(2020.01)
G06F 40/279(2020.01)
G06F 40/30(2020.01)
G06N 20/00(2019.01)

(56)对比文件
CN 113114637 A,2021.07.13
CN 113051543 A,2021.06.29
US 2017353483 A1,2017.12.07
WO 2021008028 A1,2021.01.21
CN 113312671 A,2021.08.27

审查员 谢艳花

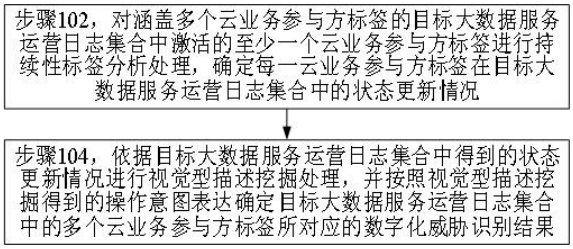
权利要求书3页 说明书24页 附图1页

(54)发明名称

一种基于大数据安防的威胁识别方法及数据安防服务器

(57)摘要

本申请涉及大数据和信息威胁防护技术领域，具体而言，涉及基于大数据安防的威胁识别方法及数据安防服务器，可以通过视觉型描述挖掘思想，从目标大数据服务运营日志集合确定出对数字化威胁识别结果的检测精度和可信度具有正向作用的操作意图表达，进而实现对目标大数据服务运营日志的威胁识别，尽可能保障数字化威胁识别结果的准确性和可靠性，减少除操作意图表达之外的噪声对数字化威胁识别结果的影响和干扰。



CN 113706177 B

1.一种基于大数据安防的威胁识别方法,其特征在于,应用于数据安防服务器,所述方法包括:

对涵盖多个云业务参与方标签的目标大数据服务运营日志集合中激活的至少一个云业务参与方标签进行持续性标签分析处理,确定每一云业务参与方标签在所述目标大数据服务运营日志集合中的状态更新情况;

其中,所述持续性标签分析处理是指对出现在各组大数据服务运营日志中的同一云业务参与方标签进行不间断的分析,在进行持续性标签分析处理时,确定各组大数据服务运营日志中激活的同一云业务参与方标签为所述持续性标签分析处理;所述状态更新情况为云业务参与方标签在目标大数据服务运营日志集合中的业务互动变化信息,所述状态更新情况表征云业务参与方标签在各大数据服务运营日志中的云业务参与方标签的互动操作状态数据,以及时间层面的特征信息,云业务参与方标签的互动操作状态数据表征云业务参与方标签关键词,时间层面的特征信息表征云业务参与方标签的在各状态时所对应的时序描述;

依据所述目标大数据服务运营日志集合中得到的所述状态更新情况进行视觉型描述挖掘处理,并依据所述视觉型描述挖掘得到的操作意图表达确定所述目标大数据服务运营日志集合中的多个所述云业务参与方标签所对应的数字化威胁识别结果;

其中,所述依据所述目标大数据服务运营日志集合中得到的所述状态更新情况进行视觉型描述挖掘处理,获得所述目标大数据服务运营日志集合中的多个所述云业务参与方标签所对应的数字化威胁识别结果,包括:依据所述状态更新情况表示的所述目标大数据服务运营日志集合包括的各大数据服务运营日志中的云业务参与方标签的互动操作状态数据以及所述各大数据服务运营日志中云业务参与方标签之间的视觉关联情况,对所述各大数据服务运营日志依次执行场景视觉型描述挖掘处理,得到各大数据服务运营日志分别所对应的服务场景显著性内容;对所述各大数据服务运营日志分别所对应的服务场景显著性内容进行基于设定优先级次序的识别处理,并依据所述基于设定优先级次序的识别处理得到的操作意图表达确定所述目标大数据服务运营日志集合中的多个所述云业务参与方标签所对应的数字化威胁识别结果;

其中,所述数字化威胁识别结果至少包括如下的其中一种:流量攻击;信息窃取;数据篡改;身份伪造;

其中,所述依据所述状态更新情况表示的所述目标大数据服务运营日志集合包括的各大数据服务运营日志中的云业务参与方标签的互动操作状态数据以及所述各大数据服务运营日志中云业务参与方标签之间的视觉关联情况,对所述各大数据服务运营日志依次执行场景视觉型描述挖掘处理,得到各大数据服务运营日志分别所对应的服务场景显著性内容,包括:依据所述各大数据服务运营日志中云业务参与方标签之间的视觉关联情况,确定所述各大数据服务运营日志分别所对应的共性关键描述集;依据所述云业务参与方标签的互动操作状态数据,确定所述各大数据服务运营日志分别所对应的显著性描述集;依据所述共性关键描述集与所述显著性描述集完成所述场景视觉型描述挖掘处理,获得每一大数据服务运营日志分别所对应的服务场景显著性内容;

其中,所述依据所述目标大数据服务运营日志集合中得到的所述状态更新情况进行视觉型描述挖掘处理,得到与所述目标大数据服务运营日志集合所对应的操作意图表达的步

骤之前，还包括：确定所述目标大数据服务运营日志集合包括的各大数据服务运营日志携带的其中两个云业务参与方标签之间的交互传递情况；依据所述各大数据服务运营日志携带的云业务参与方标签，以及确定的所述交互传递情况，分别确定所述各大数据服务运营日志中云业务参与方标签之间的视觉关联情况；

其中，所述确定所述目标大数据服务运营日志集合包括的各大数据服务运营日志携带的其中两个云业务参与方标签之间的交互传递情况，包括：抽取所述各大数据服务运营日志携带的各云业务参与方标签所对应的约束型描述向量；所述约束型描述向量表征各云业务参与方标签所对应的操作环境描述向量；通过各云业务参与方标签所对应的约束型描述向量，确定各云业务参与方标签中其中两个云业务参与方标签之间的量化比较结果；将没有达到第一设定判定值的量化比较结果所对应的两个云业务参与方标签确定为存在交互传递情况的两个云业务参与方标签；

其中，所述确定所述目标大数据服务运营日志集合包括的各大数据服务运营日志携带的其中两个云业务参与方标签之间的交互传递情况，包括：对所述各大数据服务运营日志依次执行运营日志解析处理，确定所述云业务参与方标签在各大数据服务运营日志中的互动操作状态数据；通过各云业务参与方标签所对应的互动操作状态数据，确定各云业务参与方标签中其中两个云业务参与方标签之间的差异数据；依据所述差异数据确定各大数据服务运营日志携带的其中两个云业务参与方标签之间的交互传递情况；

其中，所述依据所述差异数据确定各大数据服务运营日志携带的其中两个云业务参与方标签之间的交互传递情况，包括：将确定的其中两个云业务参与方标签之间的差异数据迁移变换至通过第三设定判定值与第四设定判定值所确定的约束约束内；将完成迁移变换的其中两个云业务参与方标签之间的差异数据确定为所述其中两个云业务参与方标签之间的关联重要性评价；按照所述其中两个云业务参与方标签之间的关联重要性评价指示所述其中两个云业务参与方标签之间的交互传递情况。

2.如权利要求1所述的方法，其特征在于，所述对涵盖多个云业务参与方标签的目标大数据服务运营日志集合中激活的至少一个云业务参与方标签进行持续性标签分析处理，确定每一云业务参与方标签在所述目标大数据服务运营日志集合中的状态更新情况，包括：

对所述目标大数据服务运营日志集合包括的每一大数据服务运营日志依次执行运营日志解析处理，确定所述每一云业务参与方标签依次在各大数据服务运营日志中的互动操作状态数据；

针对所述每一云业务参与方标签进行持续性标签分析处理，以根据持续性分析结果以及所述互动操作状态数据，确定所述每一云业务参与方标签在所述目标大数据服务运营日志集合中的状态更新情况。

3.如权利要求2所述的方法，其特征在于，所述针对所述每一云业务参与方标签进行持续性标签分析处理，以根据持续性分析结果以及所述互动操作状态数据，确定所述每一云业务参与方标签在所述目标大数据服务运营日志集合中的状态更新情况，包括：

利用时序迭代处理策略或者参与方标签定位线程，针对所述每一云业务参与方标签进行持续性标签分析处理；

基于持续性捕捉到的同一云业务参与方标签在各大数据服务运营日志中的互动操作状态数据，确定所述每一云业务参与方标签的状态更新情况。

4.如权利要求1所述的方法,其特征在于,通过视觉型描述挖掘检测线程执行所述视觉型描述挖掘处理;其中,所述视觉型描述挖掘检测线程的调试方法包括:

生成调试示例,其中,所述调试示例具有涵盖多个云业务参与方标签的状态更新情况,以及具有依据所述多个云业务参与方标签的状态更新情况的数字化威胁识别结果的真实性引导信息;

依据所述状态更新情况和所述数字化威胁识别结果的真实性引导信息对设定的视觉型描述挖掘网络进行调试,获得所述视觉型描述挖掘检测线程;

其中,所述生成调试示例,包括:基于大数据业务分析系统,配置多个参考云业务参与方标签所对应的业务交互类别;依据所述业务交互类别,确定各参考云业务参与方标签所对应的状态更新情况;确定所述各参考云业务参与方标签所对应的状态更新情况表示的数字化威胁识别结果;依据所述状态更新情况,以及所述状态更新情况表示的数字化威胁识别结果,生成所述调试示例。

5.一种数据安防服务器,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1-4任一项所述的方法。

6.一种计算机存储介质,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1-4任一项所述的方法。

一种基于大数据安防的威胁识别方法及数据安防服务器

技术领域

[0001] 本申请实施例涉及大数据和信息威胁防护技术领域，具体涉及一种基于大数据安防的威胁识别方法及数据安防服务器。

背景技术

[0002] 随着大数据的发展，大数据安防已由传统的平安城市、智能交通管理、环境保护、危化品运输监控、食品安全监控等领域延伸到云业务处理领域。现如今的大数据安防更多地侧重于数据信息层面的安全防护处理，以保障用户的数据信息免受各类网络攻击的威胁。在实际应用过程中，针对各类业务进行数据信息安全的威胁识别至关重要，然而发明人在研究和分析过程中发现，相关的信息安全威胁识别技术容易受到干扰和影响，从而难以确保信息安全威胁识别的准确性和可靠性。

发明内容

[0003] 有鉴于此，本申请实施例提供了一种基于大数据安防的威胁识别方法及数据安防服务器。

[0004] 本申请实施例提供了一种基于大数据安防的威胁识别方法，应用于数据安防服务器，所述方法包括：对涵盖多个云业务参与方标签的目标大数据服务运营日志集合中激活的至少一个云业务参与方标签进行持续性标签分析处理，确定每一云业务参与方标签在所述目标大数据服务运营日志集合中的状态更新情况；依据所述目标大数据服务运营日志集合中得到的所述状态更新情况进行视觉型描述挖掘处理，并依据所述视觉型描述挖掘得到的操作意图表达确定所述目标大数据服务运营日志集合中的多个所述云业务参与方标签所对应的数字化威胁识别结果。

[0005] 本申请实施例还提供了一种数据安防服务器，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。

[0006] 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。

[0007] 在本申请中，通过对目标大数据服务运营日志集合中激活的云业务参与方标签进行持续性标签分析处理，确定云业务参与方标签在目标大数据服务运营日志集合中的状态更新情况。然后再根据状态更新情况进行视觉型描述挖掘处理，得到与目标大数据服务运营日志集合所对应的操作意图表达，并根据操作意图表达确定目标大数据服务运营日志集合中的多个云业务参与方标签所对应的数字化威胁识别结果。这样可以通过视觉型描述挖掘思想，从目标大数据服务运营日志集合确定出对数字化威胁识别结果的检测精度和可信度具有正向作用的操作意图表达，进而实现对目标大数据服务运营日志的威胁识别，尽可能保障数字化威胁识别结果的准确性和可靠性，减少除操作意图表达之外的噪声对数字化威胁识别结果的影响和干扰。

附图说明

[0008] 图1为本申请实施例所提供的一种数据安防服务器的方框示意图。

[0009] 图2为本申请实施例所提供的一种基于大数据安防的威胁识别方法的流程图。

[0010] 图3为本申请实施例所提供的一种基于大数据安防的威胁识别装置的框图。

具体实施方式

[0011] 图1示出了本申请实施例所提供的一种数据安防服务器10的方框示意图。本申请实施例中的数据安防服务器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，数据安防服务器10包括：存储器11、处理器12、通信总线13和基于大数据安防的威胁识别装置20。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。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。

[0012] 图2示出了本申请实施例所提供的一种基于大数据安防的威胁识别的流程图。所述方法有关的流程所定义的方法步骤应用于数据安防服务器10，可以由所述处理器12实现，所述方法包括以下内容。

[0013] 步骤102，对涵盖多个云业务参与方标签的目标大数据服务运营日志集合中激活的至少一个云业务参与方标签进行持续性标签分析处理，确定每一云业务参与方标签在目标大数据服务运营日志集合中的状态更新情况。

[0014] 步骤104，依据目标大数据服务运营日志集合中得到的状态更新情况进行视觉型描述挖掘处理，并按照视觉型描述挖掘得到的操作意图表达确定目标大数据服务运营日志集合中的多个云业务参与方标签所对应的数字化威胁识别结果。

[0015] 以上基于大数据安防的威胁识别方法可以应用于数据安防服务器中。其中，以上数据安防服务器可以通过安装与基于大数据安防的威胁识别方法所对应的功能线程执行以上基于大数据安防的威胁识别方法。以上数据安防服务器的类别可以是手提电脑，大型计算机，云服务器等。本申请不对以上数据安防服务器的实际类别进行进一步限定。可以理解的是，以上基于大数据安防的威胁识别方法既可以仅通过业务侧或服务器侧独立实现，也可以通过业务侧与服务器侧互相协作实现。

[0016] 以上基于大数据安防的威胁识别方法可以分为获取目标大数据服务运营日志集合与对目标大数据服务运营日志集合进行数字化威胁识别两个进程。其中，获取进程可以部署于业务用户设备并分布在业务侧。数字化威胁识别进程可以部署于数据安防服务器并分布在服务器侧。以上业务侧可以在获取到目标大数据服务运营日志集合后向以上服务器侧发起数字化威胁识别申请。以上服务器侧在接收到以上数字化威胁识别申请后，可以基于以上数字化威胁识别申请对以上目标大数据服务运营日志集合执行以上基于大数据安防的威胁识别方法。

[0017] 可以理解的是，在实际实施过程中，可以先获取目标大数据服务运营日志集合。该目标大数据服务运营日志集合可以理解为涵盖多个数字化云业务参与方标签、需要进行数字化威胁识别结果检测的大数据服务运营日志集合。该目标大数据服务运营日志集合中可以包括多组大数据服务运营日志。此外，大数据服务运营日志所涉及的领域可以包括区块链支付、智慧医疗、远程办公、在线教育、智慧城市、自动化工厂、云游戏、政企云服务等。

[0018] 以一些可能的实施例来看待，本申请实施例中的目标大数据服务运营日志集合可以包括流式日志集合或多组不存在时间先后联系的大数据服务运营日志集合。以上流式日志集合包括F组存在时间先后联系的涵盖多个云业务参与方标签的大数据服务运营日志，F为正整数。可以理解的是，获取目标大数据服务运营日志集合可以有多种，本申请实施例不作限制。

[0019] 在获取目标大数据服务运营日志集合后，可以继续实施步骤102，对涵盖多个云业务参与方标签的目标大数据服务运营日志集合中激活的至少一个云业务参与方标签进行持续性标签分析处理，确定每一云业务参与方标签在目标大数据服务运营日志集合中的状态更新情况。

[0020] 在本申请实施例中，持续性标签分析处理，可以是指对出现在各组大数据服务运营日志中的同一云业务参与方标签进行不间断的分析。在进行持续性标签分析处理时，确定各组大数据服务运营日志中激活的同一云业务参与方标签可以部分理解为持续性标签分析处理。

[0021] 在本申请实施例中，以上状态更新情况，可以理解为云业务参与方标签在目标大数据服务运营日志集合中的业务互动变化信息。比如，在数字办公环境下，可以对数字化云业务参与方进行持续性标签分析，可以确定出同一数字化云业务参与方在各组大数据服务运营日志中的互动操作状态数据，从而确定该数字化云业务参与方在目标大数据服务运营日志集合中的业务互动变化。可以理解的是，以上状态更新情况可以表征云业务参与方标签在各大数据服务运营日志中的云业务参与方标签的互动操作状态数据，以及时间层面的特征信息。其中，以上云业务参与方标签的互动操作状态数据可以表征云业务参与方标签关键词。以上时间层面的特征信息可以表征云业务参与方标签的在各状态时所对应的时序描述。

[0022] 示例性地，在本申请中可以将获取的目标大数据服务运营日志集合输入持续性标签分析处理节点执行以上步骤102。

[0023] 其中，持续性标签分析处理节点，进一步可以通过数据安防服务器部署的功能模块，实施步骤1022，利用云业务参与方标签状态识别网络，对以上每一大数据服务运营日志依次执行状态识别操作，确定以上每一云业务参与方标签在各大数据服务运营日志中的互动操作状态数据。

[0024] 对于该步骤而言，可以利用云业务参与方标签状态识别网络，对各大数据服务运营日志依次执行状态识别操作，确定云业务参与方标签在各大数据服务运营日志中的互动操作状态数据。其中，云业务参与方标签状态识别网络包括基于多个携带了云业务参与方标签的互动操作状态数据的调试示例所调试得到的识别网络，其中，调试可以理解为训练。

[0025] 进一步的，以上云业务参与方标签状态识别网络可以是AI神经网络。在使用前，可以使用携带了云业务参与方标签的互动操作状态数据的调试示例对该状态识别网络进行调试，直到该网络符合设定条件。

[0026] 在确定以上互动操作状态数据后，以上持续性标签分析处理节点中可以实施步骤1024，基于以上互动操作状态数据，对以上云业务参与方标签进行持续性标签分析处理，确定以上云业务参与方标签在以上目标大数据服务运营日志集合中的状态更新情况。

[0027] 在本申请中不对持续性标签分析处理的方法进行进一步限定，以下示意性的给出

两种持续性标签分析处理方法。

[0028] 对于第一种持续性标签分析处理方法而言，在实施步骤1024时，可以利用时序迭代处理策略(比如相关的滤波算法)，对以上每一云业务参与方标签进行持续性标签分析处理，确定以上每一云业务参与方标签的状态更新情况。以一些可能的实施例来看待，可以按照以上各大数据服务运营日志的获取时间先后，从首组大数据服务运营日志开始，逐一将连续两组大数据服务运营日志确定为当前两组大数据服务运营日志并实施如下步骤：利用时序迭代处理策略确定当前两组大数据服务运营日志中携带的各云业务参与方标签所对应的互动操作状态数据；将当前两组大数据服务运营日志中的第一大数据服务运营日志携带的各云业务参与方标签所对应的互动操作状态数据，分别与以上当前两组大数据服务运营日志中的第二大数据服务运营日志携带的各云业务参与方标签所对应的互动操作状态数据进行配对。

[0029] 进一步地，在实施以上配对操作时，可以确定以上第一大数据服务运营日志携带的各云业务参与方标签所对应的互动操作状态数据，分别与以上第二大数据服务运营日志携带的各云业务参与方标签所对应的互动操作状态数据之间的差异数据。若确定的差异数据小于设定的差异判定值，即可确定该差异数据所对应的两个互动操作状态数据为配对中的两个互动操作状态数据。

[0030] 在执行完以上配对操作后，可以将配对中的两个互动操作状态数据所对应的两个云业务参与方标签确定为在以上当前两组大数据服务运营日志中激活的同一云业务参与方标签，以实现对以上云业务参与方标签进行持续性标签分析处理。当针对所有连续的大数据服务运营日志执行完以上步骤后，基于持续性捕捉到的同一云业务参与方标签在各大数据服务运营日志中的互动操作状态数据，确定以上云业务参与方标签的状态更新情况。

[0031] 在以上方法中可以确定以上各大数据服务运营日志中激活的同一云业务参与方标签，从而实现在各大数据服务运营日志中对该同一云业务参与方标签进行持续性分析处理。在实现对该云业务参与方标签的持续性标签分析处理后，既可基于该云业务参与方标签在各大数据服务运营日志中的互动操作状态数据，确定该云业务参与方标签在以上目标大数据服务运营日志集合中的状态更新情况。

[0032] 对于第一种持续性标签分析处理方法而言，在实施步骤1024时，可以根据参与方标签定位线程确定以上各大数据服务运营日志中激活的同一云业务参与方标签，以实现对以上每一云业务参与方标签进行持续性标签分析处理。

[0033] 以上参与方标签定位线程包括基于AI人工智能生成的网络。通过该参与方标签定位线程可以检测出大数据服务运营日志包括的数字化云业务参与方标签所对应的云业务参与方描述。以一些可能的实施例来看待，以上云业务参与方描述可以行为描述表达。在检测出各大数据服务运营日志包括的云业务参与方描述后，可以对不同的两组大数据服务运营日志携带的云业务参与方描述进行量化比较结果确定，并将量化比较结果达到第二差异判定值的云业务参与方标签确定为同一云业务参与方标签。

[0034] 比如，在数字办公环境下，以上云业务参与方标签目标可以是数字化云业务参与方。此时可以通过以上参与方标签定位线程检测各大数据服务运营日志携带的办公行为描述表达。在检测出各大数据服务运营日志包括的办公行为描述表达后，可以对不同的两组大数据服务运营日志携带的行为描述表达进行量化比较结果确定，并将量化比较结果达到

第二差异判定值的办公行为描述表达确定为同一办公行为描述表达。确定同一办公行为描述表达后即可确定以上两组大数据服务运营日志激活了同一数字化云业务参与方。

[0035] 在确定各组大数据服务运营日志中激活的同一云业务参与方标签后，可以根据持续性捕捉到的同一云业务参与方标签在各大数据服务运营日志中的互动操作状态数据，确定以上每一云业务参与方标签的状态更新情况。

[0036] 以一些可能的实施例来看待，在确定云业务参与方标签所对应的状态更新情况后，可以通过设定形式保存各云业务参与方标签所对应的以上状态更新情况。其中，比如可以通过多维数组对状态更新情况进行存储。可以理解的是，以上多维数组可以被确定为以上目标大数据服务运营日志集合所对应的显著性描述集。

[0037] 可以理解的是，以上状态更新情况具有时间层面的特征，可以指示出云业务参与方标签在以上目标大数据服务运营日志集合示出的时间层面的特征约束内变化的过程中状态关键词的更新情况。基于目标大数据服务运营日志集合中激活的各云业务参与方标签所对应的以上状态更新情况即可确定出各云业务参与方标签的变化情况，即各云业务参与方标签是处于正常业务互动状态还是异常业务互动状态。因此，基于该状态更新情况进行进行数字化威胁识别结果检测是可行的。

[0038] 在另外的一些可独立实施的技术方案中，在确定以上状态更新情况后，可以继续实施步骤104，基于以上目标大数据服务运营日志集合中得到的以上状态更新情况进行视觉型描述挖掘处理，并基于以上视觉型描述挖掘得到的操作意图表达确定以上目标大数据服务运营日志集合中的多个以上云业务参与方标签所对应的数字化威胁识别结果。

[0039] 进一步地，可以先实施步骤1042，基于以上目标大数据服务运营日志集合中得到的以上状态更新情况进行视觉型描述挖掘处理，得到与以上目标大数据服务运营日志集合所对应的操作意图表达。

[0040] 以上操作意图表达，可以包括进行视觉型描述挖掘处理(包括场景视觉型描述挖掘与时间层面的特征的视觉型描述挖掘)确定出的显著性描述集或描述内容(比如特征向量)。可以理解的是，以上操作意图表达为基于目标大数据服务运营日志集合中的多个数字化云业务参与方标签的状态更新情况确定的，因此以上操作意图表达对确定数字化威胁识别结果的准确性和可靠性是保障的。

[0041] 以一些可能的实施例来看待，在实施步骤1042前，可以确定以上目标大数据服务运营日志集合包括的各大数据服务运营日志中云业务参与方标签之间的视觉关联情况。以一些可能的实施例来看待，可以通过大数据服务运营日志所对应的关系表达表征以上视觉关联情况。以下为本申请示出的一种大数据服务运营日志中云业务参与方标签视觉关联情况的确定方法。

[0042] 步骤302，确定以上目标大数据服务运营日志集合包括的各大数据服务运营日志携带的其中两个云业务参与方标签之间的交互传递情况。

[0043] 在本申请实施例中，通过不同的交互传递情况定位策略确定的交互传递情况(比如连接关系)对应不同的理解。比如，通过两个云业务参与方标签之间的量化比较结果大小确定的交互传递情况可以从共性层面(比如相似性角度)表征两个云业务参与方标签之间的相关性评估情况。再比如，通过两个云业务参与方标签之间的差异数据大小确定的交互传递情况可以从差异数据角度实际性引导两个云业务参与方标签之间的相关性评估情况。

[0044] 以一些可能的实施例来看待，在执行步骤302时，可以抽取以上各大数据服务运营日志携带的各云业务参与方标签所对应的约束型描述向量。以上约束型描述向量表征与各云业务参与方标签所对应的操作环境描述向量。以上约束型描述向量可以包括各云业务参与方标签所处状态的业务流程层面的信息，通过比较各云业务参与方标签所处状态的业务流程层面的信息可以确定云业务参与方标签之间的交互传递情况。

[0045] 在确定各云业务参与方标签所对应的云业务参与方描述后，可以根据各云业务参与方标签所对应的约束型描述向量，确定各云业务参与方标签中其中两个云业务参与方标签之间的量化比较结果。将没有达到第一设定判定值的量化比较结果所对应的两个云业务参与方标签确定为存在交互传递情况的两个云业务参与方标签。进一步地，以上第一设定判定值包括根据实际需求设置的阈值。在本申请中不对以上第一设定判定值进行进一步限定。

[0046] 可以理解的是，本申请不对确定量化比较结果的方法进行进一步限定。比如，以上确定量化比较结果的方法可以根据实际的差异比较情况确定。

[0047] 以一些可能的实施例来看待，为了提升对目标大数据服务运营日志集合的威胁识别精度，在执行步骤302时，可以根据云业务参与方标签之间的差异数据确定云业务参与方标签之间的交互传递情况。

[0048] 进一步地，可以对以上各大数据服务运营日志依次执行运营日志解析处理，确定以上云业务参与方标签在各大数据服务运营日志中的互动操作状态数据。在确定各大数据服务运营日志中的互动操作状态数据后，可以根据各云业务参与方标签所对应的互动操作状态数据，确定各云业务参与方标签中其中两个云业务参与方标签之间的差异数据。在确定其中两个云业务参与方标签之间的差异数据后，可以根据以上差异数据确定各大数据服务运营日志携带的其中两个云业务参与方标签之间的交互传递情况。

[0049] 以一些可能的实施例来看待，在基于以上差异数据确定各大数据服务运营日志携带的其中两个云业务参与方标签之间的交互传递情况时，可以将没有达到第二设定判定值的差异数据所对应的两个云业务参与方标签确定为存在交互传递情况的两个云业务参与方标签。可以理解的，以上第二设定判定值包括根据实际需求配置的阈值。在本申请中不对以上第二设定判定值进行进一步限定。

[0050] 以一些可能的实施例来看待，若确定两个云业务参与方标签之间具有交互传递情况，则该两个云业务参与方标签之间的关联重要性评价配置为“Y”，否则将该两个云业务参与方标签之间的关联重要性评价配置为“N”。

[0051] 由于以上交互传递情况是通过云业务参与方标签之间的差异数据确定的，因此，基于该交互传递情况确定的多模态特征可以指示各云业务参与方标签之间的差异数据关系，对多模态特征进行视觉型描述挖掘操作后确定的操作意图表达也可以包含云业务参与方标签之间的差异数据信息。因此在基于该操作意图表达进行以上目标大数据服务运营日志集合中数字化威胁识别结果检测时，可以提升比如流量攻击，信息窃取或数据篡改的威胁识别精度。

[0052] 以一些可能的实施例来看待，为了进一步提升威胁识别精度，可以根据两个云业务参与方标签之间的实际差异数据，确定两个云业务参与方标签之间的关联重要性评价。

[0053] 进一步地，可以将确定的其中两个云业务参与方标签之间的差异数据迁移变换至

通过第三设定判定值与第四设定判定值所确定的约束约束内。其中，以上第三设定判定值与以上第四设定判定值为基于实际需求设置的阈值。以一些可能的实施例来看待，以上第三设定判定值为“num1”，以上第四设定判定值为“num2”。

[0054] 在完成以上迁移变换(映射)后，可以将完成迁移变换的其中两个云业务参与方标签之间的差异数据确定为以上其中两个云业务参与方标签之间的关联重要性评价，并通过以上其中两个云业务参与方标签之间的关联重要性评价指示以上其中两个云业务参与方标签之间的交互传递情况。

[0055] 由于以上示例中通过两个云业务参与方标签的实际差异数据确定两个云业务参与方标签之间的交互传递情况，因此以上多模态特征可以指示出更加适配于真实的差异数据信息，从而进一步提升威胁识别精度。

[0056] 在确定以上目标大数据服务运营日志集合包括的各大数据服务运营日志携带的其中两个云业务参与方标签之间的交互传递情况后，可以继续执行步骤304，基于以上各大数据服务运营日志携带的云业务参与方标签，以及确定的以上交互传递情况，分别确定以上各大数据服务运营日志中云业务参与方标签之间的视觉关联情况。

[0057] 对于该步骤而言，可以将大数据服务运营日志包括的云业务参与方标签作为关系表达内容的中心C_label，以及将确定的两个云业务参与方标签之间的交互传递情况确定为有向联系R，从而确定大数据服务运营日志所对应的关系表达DES(C_label，R)。以一些可能的实施例来看待可以通过共性关键描述集表示以上关系表达。

[0058] 在确定以上目标大数据服务运营日志集合中各大数据服务运营日志中云业务参与方标签之间的视觉关联情况后，可以继续实施步骤104。

[0059] 此外，可以通过视觉型描述挖掘网络实现以上步骤1042。以上视觉型描述挖掘网络，可以是基于多维视觉型描述挖掘处理网络生成的模型。其中以上多维视觉型描述挖掘网络至少包括用于对各组大数据服务运营日志进行场景视觉型描述挖掘处理的场景视觉型描述挖掘网络，以及用于对各组大数据服务运营日志所对应的服务场景显著性内容进行基于设定优先级次序的识别的基于设定优先级次序的识别网络。

[0060] 进一步地，在实施以上步骤1042时，可以将以上状态更新情况输入视觉型描述挖掘网络包括的场景视觉型描述挖掘网络中执行步骤402，基于以上状态更新情况表示的以上目标大数据服务运营日志集合包括的各大数据服务运营日志中的云业务参与方标签的互动操作状态数据以及以上各大数据服务运营日志中云业务参与方标签之间的视觉关联情况，对以上各大数据服务运营日志依次执行场景视觉型描述挖掘处理，得到各大数据服务运营日志分别所对应的服务场景显著性内容。对于该步骤而言，可以根据以上各大数据服务运营日志分别所对应的关系表达，确定以上各大数据服务运营日志分别所对应的共性关键描述集ch_A。以及基于以上云业务参与方标签的互动操作状态数据，确定以上各大数据服务运营日志分别所对应的显著性描述集remarkable_DES_x0。

[0061] 在确定以上共性关键描述集与以上显著性描述集后，可以根据以上共性关键描述集与以上显著性描述集完成以上场景视觉型描述挖掘处理，得到以上每一大数据服务运营日志分别所对应的服务场景显著性内容。

[0062] 可以理解的是，在本申请中不对以上视觉型描述挖掘策略进行进一步限定。在得到以上各大数据服务运营日志分别所对应的服务场景显著性内容后，可以将以上服务场景

显著性内容输入视觉型描述挖掘网络包括的基于设定优先级次序的识别网络中执行步骤404，对以上各大数据服务运营日志分别所对应的服务场景显著性内容进行基于设定优先级次序的识别处理，得到与以上目标大数据服务运营日志集合所对应的操作意图表达。

[0063] 对于该步骤而言，可以对以上各大数据服务运营日志分别所对应的服务场景显著性内容按照以上状态更新情况表示的时间层面的特征信息进行整理。然后基于设定的线性滑动平均处理单元，对整理后的各大数据服务运营日志分别所对应的服务场景显著性内容进行线性滑动平均处理，得到与以上目标大数据服务运营日志集合所对应的操作意图表达。

[0064] 在上述内容的基础上，在得到与以上目标大数据服务运营日志集合所对应的操作意图表达后，可以继续实施步骤1044，基于以上操作意图表达确定以上目标大数据服务运营日志集合中的多个以上云业务参与方标签所对应的数字化威胁识别结果。

[0065] 对于该步骤而言，可以将以上操作意图表达输入预先调试的多分类线程中进行数字化威胁识别，从而得到以上数字化威胁识别结果。

[0066] 以下为本申请示出的一种数字化威胁识别流程的相关内容。其中，以上多分类线程包括特征精简模块以及分类识别模块。其中，以上特征精简模块可以用于对操作意图表达进行处理得到所对应的描述内容。比如，以上特征精简模块可以是下采样节点。以上分类识别模块用于基于以上描述内容进行数字化威胁识别，得到与各设定威胁类型所对应的可信系数。

[0067] 在实施步骤1044时，可以将以上操作意图表达输入特征精简模块执行步骤502，对以上操作意图表达进行平均池化得到所对应的描述内容。在得到以上描述内容后可以将该描述内容输入分类识别模块执行步骤504，对该描述内容进行分类识别处理，得到与各设定威胁类型所对应的可信系数。

[0068] 在得到各可信系数后，即可将最大可信系数所对应的数字化威胁识别结果类型确定为以上目标大数据服务运营日志集合中的多个以上云业务参与方标签所对应的数字化威胁识别结果。其中，以上数字化威胁识别结果至少包括如下的其中一种：流量攻击；信息窃取；数据篡改；身份伪造。

[0069] 在以上方法中，通过对目标大数据服务运营日志集合中激活的云业务参与方标签进行持续性标签分析处理，确定以上云业务参与方标签在以上目标大数据服务运营日志集合中的状态更新情况。然后再基于以上状态更新情况进行视觉型描述挖掘处理，得到与以上目标大数据服务运营日志集合所对应的操作意图表达，并基于以上操作意图表达确定以上目标大数据服务运营日志集合中的多个以上云业务参与方标签所对应的数字化威胁识别结果。这样可以通过视觉型描述挖掘思想，从目标大数据服务运营日志集合确定出对数字化威胁识别结果的检测精度和可信度具有正向作用的操作意图表达，进而实现以上目标大数据服务运营日志集合表示的数字化威胁识别结果的精准可靠检测。

[0070] 以下结合数字办公环境进行实施例说明。以上数字办公环境通常会设置办公信息安防软件。该办公信息安防软件通常可以采集流式日志集合。可以理解的是，在数字办公环境下实际是对办公信息安防软件采集的流式日志集合进行数字化威胁识别。

[0071] 以下为一种数字化威胁识别流程的相关内容。

[0072] 在获取目标流式日志集合后，可以根据关键词确定节点执行步骤602，对以上目标

流式日志集合包括的各大数据服务运营日志依次执行运营日志解析处理，确定流式日志中激活的数字化云业务参与方在各大数据服务运营日志中的互动操作状态数据。

[0073] 在确定以上互动操作状态数据后，可以根据持续性标签分析单元执行步骤604，基于以上互动操作状态数据，对以上数字化云业务参与方进行持续性标签分析处理，确定以上数字化云业务参与方在以上目标大数据服务运营日志集合中的状态更新情况。

[0074] 在确定以上状态更新情况后，可以根据视觉型描述挖掘检测线程包括的日志挖掘子线程执行步骤606，基于以上状态更新情况进行视觉型描述挖掘处理，得到与以上目标大数据服务运营日志集合所对应的操作意图表达。

[0075] 以上视觉型描述挖掘检测线程，进一步可以是基于视觉型描述挖掘网络与多检测线程生成的检测线程。通过该视觉型描述挖掘检测线程，一方面，可以对多模态特征进行视觉型描述挖掘操作，确定以上多模态特征所对应的操作意图表达；另一方面，可以根据以上操作意图表达对以上目标大数据服务运营日志集合进行数字化威胁识别处理，确定该集合的威胁类别。

[0076] 在确定以上操作意图表达后，可以根据以上视觉型描述挖掘检测线程包括的多检测线程执行步骤608基于以上操作意图表达确定以上目标大数据服务运营日志集合中的多个以上云业务参与方标签所对应的数字化威胁识别结果。

[0077] 在以上方案中，先利用视觉型描述挖掘原理，基于数字化云业务参与方在流式日志中的状态更新情况确定出可以反映各数字化云业务参与方在流式日志集合中的差异数据更新情况的操作意图表达。然后再基于以上操作意图表达确定以上流式日志集合的威胁类别，从而提高威胁识别和检测的精度。

[0078] 以上是对本申请示出的大数据服务运营日志集合的威胁识别方案的说明，以下对使用的视觉型描述挖掘检测线程的调试方法进行说明。以上视觉型描述挖掘检测线程可以用于实现以上视觉型描述挖掘处理。

[0079] 以一些可能的实施例来看待，以上视觉型描述挖掘检测线程可以包括视觉型描述挖掘网络以及多检测线程。其中，以上视觉型描述挖掘网络，可以将目标大数据服务运营日志集合中各云业务参与方标签的状态更新情况作为输入进行视觉型描述挖掘处理，得到与以上目标大数据服务运营日志集合所对应的操作意图表达。以上多检测线程，可以将以上操作意图表达作为输入，对以上操作意图表达进行数字化威胁识别处理，得到以上目标大数据服务运营日志集合表示的数字化威胁识别结果。

[0080] 可以理解的是，对视觉型描述挖掘检测线程的调试实际是确定以上视觉型描述挖掘网络以及以上多检测线程包括的线程变量的过程。

[0081] 在本申请中提出了一种线程调试方法。该方法通过生成参考的调试示例对视觉型描述挖掘检测线程进行调试，从而在缺乏实际示例的情形下，也可实现线程调试。相应的，以上调试方法包括如下内容。

[0082] 步骤702，生成调试示例，其中，以上调试示例具有涵盖多个云业务参与方标签的状态更新情况，以及具有基于以上多个云业务参与方标签的状态更新情况的数字化威胁识别结果的真实性引导信息。对于该步骤而言，可以先执行步骤7022，基于大数据业务分析系统，设置流式日志中激活的云业务参与方标签所对应的业务交互类别。以上大数据业务分析系统，进一步是可以进行变化分析的任一系统。以一些可能的实施例来看待，以上大数据

业务分析系统可以是企业服务开发平台。以上业务交互类别，可以包括交互热度与偏好变化。通过以上业务交互类别，一方面可以确定云业务参与方标签在以上流式日志包括的各组大数据服务运营日志中的关键词，从而确定各云业务参与方标签在以上流式日志中的状态更新情况。另一方面，可以得到以上流式日志表示的数字化威胁识别结果。比如，在数字办公环境下，当各数字化云业务参与方的业务交互类别为集中型类别时，即可确定流式日志表示的数字化威胁识别结果为流量攻击；反之则可以确定流式日志表示的数字化威胁识别结果为信息窃取。当然，数字化威胁识别结果的判定不限于上述内容，本申请实施例不作一一列举。

[0083] 在确定各云业务参与方标签的业务交互类别后，可以执行步骤7024，基于以上业务交互类别，确定各云业务参与方标签所对应的状态更新情况，以及确定以上各云业务参与方标签所对应的状态更新情况表示的数字化威胁识别结果。其中以上数字化威胁识别结果可以包括流量攻击，信息窃取与数据篡改等。

[0084] 在确定以上状态更新情况以及以上流式日志表示的数字化威胁识别结果后，可以执行步骤7026，基于以上状态更新情况，以及以上状态更新情况表示的数字化威胁识别结果，生成以上调试示例。

[0085] 在得到以上调试示例后，可以继续执行步骤704，基于预设线程评估指标，以及以上调试示例对以上视觉型描述挖掘检测线程进行调试，直至该线程满足设定条件(比如线程趋于稳定)。以上预设线程评估指标可以是根据经验设定的线程评估指标。

[0086] 在以上调试方法中，由于使用了调试示例对视觉型描述挖掘检测线程进行调试，从而实现调试过程中不用依赖实际调试示例。

[0087] 以一些可能的实施例来看待，还可以对用于确定云业务参与方标签状态的云业务参与方标签状态识别网络、进行持续性标签分析处理的持续性标签分析处理模型以及用于进行视觉型描述挖掘处理和分类的视觉型描述挖掘检测线程进行联动调试。

[0088] 以一些可能的实施例来看待，可以通过大数据业务分析系统生成表征流量攻击、信息窃取等流式日志，并对生成的流式日志进行数字化威胁识别结果实际性引导，得到调试示例。

[0089] 在得到调试示例后，可以将调试示例输入至以上云业务参与方标签状态识别网络，得到第一处理结果。然后再将以上第一处理结果输入以上持续性标签分析处理模型，得到第二处理结果。之后再将以上第二处理结果输入以上视觉型描述挖掘检测线程得到针对流式日志表示的数字化威胁识别结果的检测结果。在得到相关结果后，可以根据与以上参考识别所对应的真实性引导信息，反馈完成各线程的变量更新。在以上示例中，可以实现对各线程的联动调试，确保高效的调试。

[0090] 在一些可独立实施的技术方案下，所述方法还包括：在所述目标大数据服务运营日志集合中的多个所述云业务参与方标签所对应的数字化威胁识别结果为身份伪造的前提下，根据所述数字化威胁识别结果确定业务会话流式记录，基于所述业务会话流式记录进行反欺诈检测处理得到反欺诈检测结果，根据所述反欺诈检测结果进行信息防护处理。

[0091] 如此，通过二次检测(反欺诈检测)，能够实现对数字化威胁的应对处理，从而保障用户信息的安全。

[0092] 在一些可独立实施的技术方案下，基于所述业务会话流式记录进行反欺诈检测处

理得到反欺诈检测结果，可以包括以下内容：针对接收到的业务会话流式记录进行解析，以获得用户会话事件描述；以及，针对接收到的反欺诈检测授权信息记录进行解析，以获得待进行反欺诈检测的会话事件描述；在所述待进行反欺诈检测的会话事件描述符合第一反欺诈检测条件且所述用户会话事件描述符合第二反欺诈检测条件的前提下，确定与所述反欺诈检测授权信息记录存在联系的检测约束特征；通过所述检测约束特征，对所述用户会话事件描述中的至少部分会话事件描述进行反欺诈检测处理。

[0093] 在一些可独立实施的技术方案下，基于所述业务会话流式记录进行反欺诈检测处理得到反欺诈检测结果可以通过以下技术方案实现。

[0094] STEP101，针对接收到的业务会话流式记录进行解析，以获得用户会话事件描述。在一些可能的实施例中，业务会话流式记录为视觉特征信息包括待解析会话事项的流式记录，例如可以是按照时间先后顺序整理而成的日志记录，其中，待解析会话事项的数目可以是一个、两个或者两个以上等。

[0095] 对于一些可能的实现方式而言，通过对业务会话流式记录中的每一个待解析会话事项，采用与该会话事项存在配对关系的业务会话样本，进行各个事件属性记录的事件属性（例如事件特征）解析，并同时结合该待解析会话事项中关联事件属性记录之间的联系情况，对事件属性解析结果进行优化处理，从而得到具备显著可视化的用户会话事件描述（例如可以理解为用户会话事件数据）。待解析会话事项中关联事件属性记录之间的联系情况可以理解为，一组会话事项中静态事件属性（固定不变的事件特征）与会话事项中的动态事件属性（动态可变的事件特征）之间的对应关系。如此，针对一组待解析会话事项中关联事件属性记录之间的对应关系，对该会话事项的事件属性解析结果中的事件属性进行关联后输出，即可得到具备显著可视化的用户会话事件描述。在业务会话流式记录中包括多组待解析会话事项的前提下，每一组待解析会话事项均具备显著可视化的事件属性解析结果，这样可以得到完整丰富的用户会话事件描述。

[0096] 在本申请实施例中，用户会话事件涉及各类数字化业务，包括但不限于支付业务、办公业务、车联网业务、自动化生产业务、智慧教育业务、云游戏业务等。

[0097] STEP102，针对接收到的反欺诈检测授权信息记录进行解析，以获得待进行反欺诈检测的会话事件描述。在一些可能的实施例中，反欺诈检测授权信息记录为视觉特征信息包括待解析反欺诈检测授权信息的流式记录；其中，反欺诈检测授权信息用于进行反欺诈检测的验证结果。反欺诈检测授权信息能够作为反欺诈检测的风向标。例如，反欺诈检测授权信息m1表征所采用的反欺诈检测方式为F1，反欺诈检测授权信息m2表征反欺诈检测的对象为支付业务行为数据等。

[0098] 对于一些可能的实现方式而言，通过对反欺诈检测授权信息记录中的待解析反欺诈检测授权信息进行事件属性解析，并结合该反欺诈检测授权信息中不同事件属性记录之间的显著性区分关系（例如可以理解为语义关系），对事件属性解析结果进行显著可视化处理，从而使得事件属性解析结果中的事件属性是存在配对关系的，即得到的待进行反欺诈检测的会话事件描述具备显著可视化。

[0099] 在一个可能的示例中，按照反欺诈检测授权信息记录中的视觉型限制信息将该反欺诈检测授权信息拆解为多个事件属性记录；通过对这多个事件属性记录之间的联系情况进行分析，确定事件属性解析结果中事件属性的输出结果联系，即哪些事件属性与哪些事

件属性是关联数据。如此，以获得并输出具备显著可视化的待进行反欺诈检测的会话事件描述，从而提高待进行反欺诈检测的会话事件描述的使用效率。

[0100] STEP103，在待进行反欺诈检测的会话事件描述符合第一反欺诈检测条件，且用户会话事件描述符合第二反欺诈检测条件的前提下，确定与反欺诈检测授权信息记录存在联系的检测约束特征。

[0101] 在一些可能的实施例中，第一反欺诈检测条件为待进行反欺诈检测的会话事件描述包括的核验成功消息的数目等于设定判定值；通过确定所述待进行反欺诈检测的会话事件描述包括的核验成功消息的数目，在响应于所述数目等于设定判定值的前提下，确定所述待进行反欺诈检测的会话事件描述符合所述第一反欺诈检测条件。该设定判定值可以是基于重要的核验角度(不同的验证层面)的数目进行确定的，例如，核验角度中关注点有5个，那么可以将设定判定值设定为5。

[0102] 基于此，待进行反欺诈检测的会话事件描述符合第一反欺诈检测条件，说明该待进行反欺诈检测的会话事件描述已通过多级核验。通过对业务会话流式记录进行事件属性检测、事件属性解析和对事件属性解析结果进行内容显著可视化之后，输出用户会话事件描述。通过对反欺诈检测授权信息记录进行事件属性检测、事件属性解析和对事件属性解析结果进行内容显著可视化之后，输出待进行反欺诈检测的会话事件描述。判断用户会话事件描述与待进行反欺诈检测的会话事件描述之间的量化适配程度，如果用户会话事件描述与待进行反欺诈检测的会话事件描述相对应，进一步判断用户会话事件描述是否符合目标反欺诈检测指标，例如，是否符合反欺诈检测线程关于反欺诈检测需求的指示。

[0103] 对于一些可能的实现方式而言，第二反欺诈检测条件为用户会话事件描述与待进行反欺诈检测的会话事件描述相对应，且用户会话事件描述符合目标反欺诈检测指标，可以通过以下过程验证用户会话事件描述是否符合第二反欺诈检测条件，相关内容如下。

[0104] 第1步，确定用户会话事件描述与待进行反欺诈检测的会话事件描述之间的第一量化适配程度。

[0105] 在一些可能的实施例中，首先，对待进行反欺诈检测的会话事件描述中的待反欺诈检测事项进行差异化分析(分类)；然后，针对分出的每一差异化分析结果，在用户会话事件描述中，寻觅属于该类(例如分类关键词)的数据，最后，判断用户会话事件描述中该关键词的数据是否与待进行反欺诈检测的会话事件描述中该关键词的数据匹配。因此，量化适配程度可以理解为匹配度。

[0106] 第2步，响应于第一量化适配程度不小于设定量化适配程度阈值，确定用户会话事件描述与所述待进行反欺诈检测的会话事件描述相对应，并确定用户会话事件描述是否符合目标反欺诈检测指标。在一些可能的实施例中，针对待进行反欺诈检测的会话事件描述中的每一关键词，皆进行关联度判断，如果每一关键词的用户会话事件描述与待进行反欺诈检测的会话事件描述皆匹配，确定用户会话事件描述与待进行反欺诈检测的会话事件描述相对应。例如，待进行反欺诈检测的会话事件描述中支付类反欺诈检测维度为20，那么在用户会话事件描述中，寻觅属于该支付类的会话事项维度，并确定出支付类会话事项的全局维度；如果支付类会话事项的全局维度不大于20，说明支付类的待进行反欺诈检测的会话事件描述与用户会话事件描述匹配；如果支付类会话事项的全局维度大于20，说明支付类的待进行反欺诈检测的会话事件描述与用户会话事件描述部分匹配。如果在用户会话事

件描述中，未寻觅属于该支付类的会话事项，那么则表明待进行反欺诈检测的会话事件描述与用户会话事件描述不匹配。

[0107] 第3步，响应于用户会话事件描述符合目标反欺诈检测指标，确定用户会话事件描述符合第二反欺诈检测条件。在一些可能的实施例中，如果用户会话事件描述既与待进行反欺诈检测的会话事件描述匹配，也符合目标限定，确定用户会话事件描述符合第二反欺诈检测条件。如此，通过上述第1步至第3步可以智能化地实现对待解析会话事项的验证。

[0108] 对于一些可能的实现方式而言，可以通过以下过程实现对待进行反欺诈检测的会话事件描述的验证，即验证待进行反欺诈检测的会话事件描述中是否包括符合一定数据的核验成功消息，即验证该反欺诈检测授权信息是否通过多级核验。如果待进行反欺诈检测的会话事件描述包括设定数目的核验成功消息，确定待进行反欺诈检测的会话事件描述符合第一反欺诈检测条件，即表明该反欺诈检测授权信息通过多级核验。最后，在确定待进行反欺诈检测的会话事件描述符合第一反欺诈检测条件，且所述用户会话事件描述符合第二反欺诈检测条件情况下，确定检测约束特征。与反欺诈检测授权信息记录存在联系的检测约束特征包括，基于该反欺诈检测授权信息记录确定的反欺诈检测请求端信息、该反欺诈检测请求端所指向的业务交互端以及身份安全校验端等用于实现对用户会话事件描述进行反欺诈检测的检测约束信息。目标反欺诈检测指标可以理解为是反欺诈检测线程针对需要反欺诈检测的会话事项设定的条件；例如，单组业务会话的维度、会话事项种类和会话事项时段等；判断待解析会话事项是否符合这些设定的条件，以实现对待解析会话事项的验证。

[0109] STEP104，基于检测约束特征，对用户会话事件描述中的至少部分会话事件描述进行反欺诈检测处理。在一些可能的实施例中，对于一种关键词(一种类别)的反欺诈检测任务，如果用户会话事件描述中属于该关键词的会话事项的全局维度小于等于反欺诈检测授权信息记录中包括的该关键词的待反欺诈检测维度，说明用户会话事件描述中该关键词的会话事项的全局维度未超出反欺诈检测授权信息中的该关键词的维度。例如，如果反欺诈检测授权信息中的支付类的待反欺诈检测维度为20，用户会话事件描述中属于该支付类的会话事项的全局维度为18，那么对用户会话事件描述中的全部待解析会话事项进行反欺诈检测处理。如果反欺诈检测授权信息中的支付类的待反欺诈检测维度为20，用户会话事件描述中属于该支付类的会话事项的全局维度为24，那么在用户会话事件描述中，确定出全局维度为20的支付类会话事项，对这全局维度为20的支付类会话事项进行反欺诈检测，剩余4的支付类会话事项是不进行反欺诈检测的。对于一些可能的实现方式而言，如果是对用户会话事件描述的部分描述信息进行反欺诈检测，那么可以基于剩余描述信息，确定该剩余描述信息的待解析会话事项；并将剩余描述信息的待解析会话事项反馈至反欺诈检测请求侧，以使反欺诈检测请求端取消剩余描述信息的待解析会话事项。

[0110] 在本申请实施例中，对于接收到的业务会话流式记录和反欺诈检测授权信息记录，首先智能化地对业务会话流式记录和反欺诈检测授权信息记录进行解析，以获得用户会话事件描述与待进行反欺诈检测的会话事件描述；如此，可以自适应进行业务会话流式记录及反欺诈检测授权信息记录解析，以及分析业务会话之间的联系；然后对待进行反欺诈检测的会话事件描述以及用户会话事件描述进行验证完成之后，针对性地确定与反欺诈检测授权信息记录存在联系的检测约束特征，这样能够实现对用户会话事件描述的针对性

识别;最后利用对应的检测约束特征,对用户会话事件描述进行反欺诈检测处理,这样,基于完成校验的检测约束特征对用户会话事件描述进行反欺诈检测处理,能够实现针对性和自适应的反欺诈检测,确保应对不同的反欺诈检测需求,提高反欺诈检测的准确性和可靠性。

[0111] 在一些可能的实施例中,通过将业务会话与业务会话数据集中的业务会话样本进行关联,以得到业务会话的可信指数,从而将高可信指数的业务会话样本确定为待使用的业务会话样本,智能化地实现业务会话解析,提高会话处理效率,即上述STEP101可以通过如下的相关步骤进行说明。

[0112] STEP201,在业务会话流式记录中,对待解析会话事项所在的流式记录内容进行分割,以获得至少一个局部记录描述。在一些可能的实施例中,一组待解析会话事项对应一个局部记录描述。该业务会话流式记录中的待解析会话事项可以是一组或者多组;对包括一组或者多组待解析会话事项的会话信息进行流式记录处理,即可得到该业务会话流式记录;或者,对多个待解析会话事项进行流式记录处理,将整理到的流式记录进行组合得到包括多个待解析会话事项的业务会话流式记录。

[0113] 在业务会话流式记录中,确定出每一待解析会话事项所在的流式记录内容,对这些流式记录内容进行局部拆分处理,这样,可以得到视觉特征信息包括一个待解析会话事项的多个局部记录描述。对于一些可能的实现方式而言,如果业务会话流式记录中包括6组待解析会话事项,那么针对这6组待解析会话事项所在的流式记录内容分别进行分割,以获得每一组待解析会话事项所对应的局部记录描述。

[0114] 对于一些可能的实现方式而言,对于业务会话流式记录中待解析会话事项所在的流式记录内容进行局部拆分处理之后,以获得多个流式记录内容,响应于局部记录描述处于特征识别度异常状态,对该局部记录描述中的视觉特征信息进行特征识别度优化操作,并将经特征识别度优化操作后得到的流式记录作为局部记录描述。如此,对每一流式记录内容的流式记录内容进行特征识别度优化处理,以使流式记录内容的特征识别度回归正常,可以通过以下过程实现。

[0115] 第1步,在业务会话流式记录中,对每一待解析会话事项所在的流式记录内容进行局部拆分处理,以获得至少两个局部拆分处理流式记录。第2步,响应于所述局部拆分处理流式记录处于特征识别度异常状态,对所述局部拆分处理流式记录中的视觉特征信息进行特征识别度优化操作,并将经所述特征识别度优化操作后得到的流式记录作为局部记录描述。例如,特征识别度优化操作可以理解为特征识别度校正或者修正,以确保视觉特征信息的特征识别度尽可能趋于正常。

[0116] STEP202,对所述局部记录描述进行解析,以获得所述用户会话事件描述。在一些可能的实施例中,对每一组局部记录描述进行范围性解析,从设定业务会话集中调用可信指数较高的业务会话样本进行事件属性检测和事件属性解析,并结合该局部记录描述中不同事件属性记录之间的联系情况对事件属性解析结果进行显著可视化处理,以获得具备显著可视化的用户会话事件描述。

[0117] 对于一些可能的实现方式而言,通过在业务会话数据集中寻觅与局部记录描述量化适配程度较高的业务会话样本,实现对局部记录描述的解析,即上述STEP202可以通过以下过程实现。

[0118] STEP231，获取所述局部记录描述所对应的会话事项关键词。在一些可能的实施例中，对于得到的多个局部记录描述，通过对该局部记录描述中包括的待解析会话事项进行差异化分析，以获得局部记录描述所对应的会话事项关键词。

[0119] STEP232，在设定业务会话数据集中寻觅与所述会话事项关键词存在配对关系的目标业务会话样本。在一些可能的实施例中，按照会话事项关键词，在设定业务会话数据集中，确定属于该关键词的业务会话样本与该局部记录描述的可信指数，将可信指数大于或等于设定可信指数阈值的业务会话样本作为该局部记录描述的目标业务会话样本。

[0120] STEP233，在寻觅到所述目标业务会话样本的前提下，通过所述目标业务会话样本，对所述局部记录描述中的事件属性记录进行事件属性解析，以获得事件属性解析结果。在一些可能的实施例中，在设定业务会话数据集中寻觅到目标业务会话样本，即说明设定业务会话数据集中存在与局部记录描述的可信指数大于设定可信指数阈值的业务会话样本，调用该目标业务会话样本对该局部记录描述中的各个事件属性记录进行事件属性检测和事件属性解析，以获得事件属性解析结果。例如，业务会话流式记录中包括3个待解析会话事项，对于待解析会话事项case_1，该待解析会话事项case_1的会话事项关键词为企业服务会话事项，那么在设定业务会话样本的相关业务会话样本中，寻觅与该待解析会话事项case_1的局部记录描述可信指数较高的目标业务会话样本。通过调用目标业务会话样本，对该待解析会话事项case_1的局部记录描述进行事件属性检测，以获得局部记录描述中包括事件属性的各个事件属性记录。其中，事件属性解析结果包括局部记录描述中任意事件属性记录中的事件属性。

[0121] STEP234，基于事件属性解析结果，以及不同事件属性记录之间的联系情况，以获得用户会话事件描述。在一些可能的实施例中，对于业务会话流式记录中包括一组局部记录描述的前提下，即独立的局部记录描述，按照该局部记录描述的目标业务会话样本，确定该局部记录描述的待解析会话事项中关联事件属性记录之间的联系情况。基于关联事件属性记录之间的联系情况，对事件属性解析结果进行显著可视化处理，以实现事件属性匹配，从而得到具备显著可视化的事件属性输出结果。

[0122] 对于业务会话流式记录中包括多组局部记录描述的情况，那么需要对相关信息之间的联系进行处理分析，以实现对事件属性解析结果中的事件属性进行关联。对于一些可能的实现方式而言，通过这多组局部记录描述中的不同时段，把不同的待解析会话事项进行关联。

[0123] 上述STEP231至STEP234提供了一种实现“对局部记录描述进行解析，以获得用户会话事件描述”的技术方案，在该技术方案中，通过在设定业务会话数据集中调用可信指数较高的目标业务会话样本，对局部记录描述进行事件属性检测、事件属性解析和优化处理等操作，从而可以自适应进行业务会话的事件属性解析和关联，提高处理效率，减少不必要的资源开销。

[0124] 在一些可能的实施例中，如果在设定业务会话数据集中未寻觅到目标业务会话目标，可以通过以下两种方式得到用户会话事件描述，其中，第一种方式如STEP235至STEP237所示。

[0125] STEP235，响应于未寻觅到目标业务会话样本，对局部记录描述进行事件属性解析，以获得第一会话场景解析结果。在一些可能的实施例中，按照局部记录描述与业务会话

样本的可信指数，在设定业务会话数据集中寻觅可信指数较高的目标业务会话样本，如果设定业务会话数据集中业务会话样本的可信指数均低于设定可信指数阈值，那么则表明未寻觅到目标业务会话样本。那么在对该局部记录描述进行业务会话样本匹配时，即便是找到最高可信指数业务会话样本，该业务会话样本的可信指数仍然达不到设定可信指数阈值。基于此，对局部记录描述进行范围性事件属性解析，以获得范围性事件属性解析结果，即第一会话场景解析结果；这样，能够基于局部记录描述的显著性区分信息结合第一会话场景解析结果(全局性的解析结果)，进行二次验证，以得到准确的解析结果。

[0126] STEP236，通过所述局部记录描述中的显著性区分信息，对所述第一会话场景解析结果进行改进，以获得过渡型解析结果，并将所述过渡型解析结果作为所述用户会话事件描述。在一些可能的实施例中，局部记录描述中的显著性区分信息用于描述该局部记录描述的视觉特征信息以及表明局部记录描述的视觉特征信息中各个特征的显著性区分。对于一些可能的实现方式而言，对局部记录描述进行范围性事件属性解析之后结合局部记录描述中的显著性区分信息，对第一会话场景解析结果中的事件属性按照显著性区分信息，对事件属性整合结果进行改进，使得到的过渡型解析结果符合显著性区分信息，可以将该过渡型解析结果作为用户会话事件描述。然后进入STEP237。

[0127] STEP237，向校验线程发送所述局部记录描述和所述过渡型解析结果，以从所述校验线程获取所述用户会话事件描述。在一些可能的实施例中，该校验线程可以是基于机器学习的校验线程，将局部记录描述和过渡型解析结果发送至该基于机器学习的校验线程。如此，利用校验线程并基于局部记录描述，能够对得到的过渡型解析结果进行校验和修改，以得到准确的用户会话事件描述。

[0128] 在上述STEP235至STEP237中提供了一种实现“对所述至少两个局部记录描述进行解析，以获得所述用户会话事件描述”的方式，在该方式中如果设定业务会话数据集中不包括目标业务会话样本，通过对局部记录描述进行基于机器学习的验证，以获得准确度较高的用户会话事件描述。

[0129] 第二种方式如STEP238至STEP240所示。

[0130] STEP238，在没有寻觅到所述目标业务会话样本的前提下，呈现设定可视化引导，以获取所述局部记录描述对应的会话事项流式记录。在一些可能的实施例中，在设定业务会话数据集中不包括目标业务会话样本的前提下，还可以将该未匹配到目标业务会话样本的局部记录描述进行反馈，以使反欺诈检测请求端再次进行局部记录描述的导入，即该局部记录描述所对应的高质量的会话事项流式记录。即输出反欺诈检测结果，该反欺诈检测结果可以是提示反欺诈检测请求端有会话事项存在欺诈风险；如果该局部记录描述中待解析会话事项的关键词是可解析的，即能够解析到该待解析会话事项的关键词，那么基于局部记录描述的视觉特征信息生成该反欺诈检测结果，以使反欺诈检测结果可以与局部记录描述相对应。此外，反欺诈检测结果还可以通过不同的等级进行表现，例如等级1表明存在高欺诈风险，等级2表明存在低欺诈风险，等级3表明不存在欺诈风险。STEP239，确定会话事项流式记录的会话事项标签。在一些可能的实施例中，会话事项标签包括会话事项的多个封面的关键信息或者主题信息，例如会话名称、会话时段、会话参与方、会话任务、事项进度情况等，本申请实施例不作限制。STEP240，在所述设定业务会话数据集中寻觅与所述会话事项标签存在配对关系的业务会话样本，作为所述目标业务会话样本，对所述局部记录描

述进行事件属性解析并得到所述用户会话事件描述。在一些可能的实施例中，与会话事项标签存在配对关系的业务会话样本，为业务会话样本中样本反欺诈主题信息与会话事项标签相对应，进一步地，可基于该目标业务会话样本对其中的局部记录描述进行事件属性解析，以获得该用户会话事件描述。

[0131] 上述STEP238至STEP240提供了另一种得到目标业务会话样本的方式，在该方式中，对于在设定业务会话数据集中为匹配到目标业务会话样本的局部记录描述，进行反馈，并提示反欺诈检测请求端再次导入该局部记录描述的会话事项流式记录，从而可以通过再次导入的优质会话事项流式记录为该待解析会话事项匹配目标业务会话样本，以提高业务会话样本的匹配效率，进而能够提高对局部记录描述进行事件属性解析得到的解析结果的准确度和可信度。

[0132] 在其他实施例中，在STEP238将未匹配到目标业务会话样本的局部记录描述反馈之后，可以提示再次导入会话事项流式记录，即提示反欺诈检测请求端导入该局部记录描述对应会话事项的会话事项标签。这样在对局部记录描述进行业务会话样本匹配时，无需对与局部记录描述和业务会话样本之间的可信指数进行判别，可以直接调用该会话事项标签存在配对关系的目标业务会话样本，提高了业务会话样本适配的时效性和准确度。

[0133] 在一些可能的实施例中，对于设定业务会话数据集中不存在目标业务会话样本的前提下，可以基于待解析会话事项的会话事项标签，生成新的业务会话样本，以实现对设定业务会话样本的更换，可以通过以下过程实现。

[0134] 第1步，响应于未寻觅到与会话事项标签存在配对关系的业务会话样本，基于会话事项标签，生成当前业务会话样本。在一些可能的实施例中，设定业务会话数据集中的业务会话样本与会话事项标签的整理情况的可信指数均小于可信指数阈值，或者设定业务会话数据集中业务会话样本的关键词没有该会话事项标签对应的待解析会话事项的关键词，即确定在设定业务会话数据集中未寻觅到与会话事项标签存在配对关系的业务会话样本。在这种情况下，可以通过分析会话事项标签，生成当前业务会话样本。例如，虽然设定业务会话数据集中业务会话样本的关键词包括该会话事项标签对应的待解析会话事项的关键词，但是由于不同场景对于同一关键词的会话事项的整理不同，所以在该设定业务会话数据集中已经存在的该关键词的业务会话样本是与该待解析会话事项不适配的；基于此，可以按照会话事项标签，分析出该会话事项的整理，从而生成新的业务会话样本。或者是，该会话事项是非热点会话事项，那么在设定业务会话数据集中业务会话样本的关键词没有该会话事项的关键词，这样仍然可以按照会话事项标签，分析出该非热点会话事项的整理，从而生成新的业务会话样本，新的业务会话样本可以理解为当前业务会话样本。

[0135] 第2步，将所述当前业务会话样本，加载至所述设定业务会话数据集。在一些可能的实施例中，通过分析会话事项标签，生成当前业务会话样本之后，将该当前业务会话样本加入设定业务会话数据集。对于一些可能的实现方式而言，对于设定业务会话数据集中的业务会话样本可以按照一定步长，对旧整理的业务会话样本进行清洗，以及时更当前业务会话数据集。在本申请实施例中，通过对设定业务会话数据集进行更换，能够使得更换的设定业务会话数据集能够符合会话事项整理的更换迭代，以便于为局部记录描述匹配出高可信指数的业务会话样本。

[0136] 在一些可能的实施例中，对于获取视觉特征信息包括待解析反欺诈检测授权信息

的反欺诈检测授权信息记录，可以通过以下两种方式实现对反欺诈检测授权信息内容的解析，以获得具备显著可视化的待进行反欺诈检测的会话事件描述，即上述STEP102可以通过以下两种方式实现。

[0137] 第一种方式

[0138] STEP121，对所述反欺诈检测授权信息记录中的视觉型限制信息进行解析，以获得视觉型限制信息组合形成的多个授权事件集。在一些可能的实施例中，由于反欺诈检测授权信息记录中包括许多视觉型限制信息，以及不同的视觉型限制信息组合形成的约束范围，对反欺诈检测授权信息记录进行拆解，将一个约束范围拆解为一个授权事件集，从而得到多个授权事件集。其中，授权事件可以理解为允许进行反欺诈检测的相关事件，例如授权事件1可以是允许针对XXX进行反欺诈检测，授权事件2可以是允许采用YYY方式对XXX进行反欺诈检测。

[0139] STEP122，对每一授权事件集中的事件属性进行解析，以获得视觉型解析结果。在一些可能的实施例中，可以通过可视化和图形化的方式进行事件属性解析以得到每一授权事件集中的事件属性。

[0140] STEP123，依据存在差异的授权事件集之间的联系情况，对所述存在差异的授权事件集对应的视觉型解析结果中的事件属性之间进行关联，以获得所述待进行反欺诈检测的会话事件描述。在一些可能的实施例中，通过对多个授权事件集进行显著性区分分析，确定存在差异的授权事件集之间的联系情况。例如，通过对反欺诈检测授权信息记录中的任一授权事件集的关联的关联授权事件集中的内容进行分析，判断与该授权事件集的联系情况。基于此，对视觉型解析结果中的事件属性按照授权事件集之间的联系情况，对事件属性展现的区域进行改进，以使得改进后的事件属性输出结果中事件属性之间的是关联的，即输出具备显著可视化的待进行反欺诈检测的会话事件描述。

[0141] 在上述第一种方式中，通过解析反欺诈检测授权信息记录中的视觉型限制信息，以多组视觉型限制信息组合形成的约束区间为基准，对每个授权事件集中的事件属性进行解析，这样使得后续解析更有针对性，无论是基于显著性区分分析还是关联分析，皆是对一个授权事件集内的事件属性进行分析，能够提高事件属性分析的准确性和可靠性。

[0142] 第二种方式

[0143] STEP124，确定反欺诈检测授权信息记录中的授权信息区分性表达。在一些可能的实施例中，授权信息区分性表达可以理解为授权信息的类别。对于一些可能的实现方式而言，通过对反欺诈检测授权信息记录的主题名称进行解析，确定授权信息区分性表达；例如，主题名称为游戏反欺诈检测授权信息，那么该授权信息区分性表达为游戏类。或者是通过对反欺诈检测授权信息记录中的静态描述进行解析，确定授权信息区分性表达。

[0144] STEP125，在设定反欺诈主题数据集中，寻觅与授权信息区分性表达适配的目标反欺诈主题样本。在一些可能的实施例中，确定反欺诈检测授权信息的种类之后，由于不同的反欺诈检测授权信息通常有静态的反欺诈主题样本，所以可以基于该反欺诈检测授权信息的种类从设定反欺诈主题数据集中，寻觅授权信息区分性表达属于该种类的反欺诈主题样本。例如，反欺诈检测授权信息的种类为游戏类反欺诈检测授权信息，那么在设定反欺诈主题数据集中寻觅属于游戏类的反欺诈主题样本，以获得目标反欺诈主题样本。

[0145] STEP126，响应于寻觅到目标反欺诈主题样本，确定包括静态描述的范例样本集和

与包括动态描述的待解析样本集。在一些可能的实施例中，范例样本集为具有静态描述的集合，静态描述可以理解为不变的内容，动态描述可以理解为可变的内容。

[0146] STEP127，基于范例样本集和待解析样本集，对反欺诈检测授权信息记录中的事件属性进行解析，以获得待进行反欺诈检测的会话事件描述。在一些可能的实施例中，确定出目标反欺诈主题样本之后，可以通过分析该目标反欺诈主题样本中标记的范例样本集，以及与该范例样本集关联的待解析样本集。通过按照授权信息区分性表达在设定反欺诈主题数据集中调用相同种类的目标反欺诈主题样本，这样，能够提高对反欺诈检测流式记录进行事件属性解析效率。

[0147] 在一些可能的实施例中，在对反欺诈检测授权信息记录进行反欺诈主题样本适配的过程中，可以通过对范围性流式记录进行事件属性解析，然后在事件属性解析结果中寻觅与该范例样本集的事件属性适配的部分，即可得到该范例样本集的目标待解析样本集，可通过以下步骤实现。

[0148] 第1步，对反欺诈检测授权信息记录中的事件属性进行范围性解析，以获得第二会话场景解析结果。在一些可能的实施例中，在对反欺诈检测授权信息记录进行反欺诈主题样本适配的过程中，采用视觉分析技术对反欺诈检测授权信息记录进行范围性事件属性解析，以获得事件属性解析结果，即第二会话场景解析结果。第2步，在第二会话场景解析结果中，寻觅与每一范例样本集存在配对关系的部分解析结果。在一些可能的实施例中，在第二会话场景解析结果中，寻觅标记出的范例样本集的静态描述，即部分解析结果。第3步，基于部分解析结果，确定与部分解析结果对应的范例样本集存在联系的目标待解析样本集。在一些可能的实施例中，在第二会话场景解析结果中，确定与部分解析结果存在联系的解析结果，存在联系的解析结果所对应的待解析样本集，即为目标待解析样本集。第4步，基于每一范例样本集与目标待解析样本集之间的联系情况，对第二会话场景解析结果中位于范例样本集的静态事件属性和位于目标待解析样本集的动态描述进行关联，以获得待进行反欺诈检测的会话事件描述。

[0149] 在一些可能的实施例中，对于每一范例样本集，均在第二会话场景解析结果中，确定出该范例样本集对应的目标待解析样本集；这样，基于每一范例样本集与目标待解析样本集之间的联系情况，建立第二会话场景解析结果中的静态描述和动态描述之间的匹配关系；并基于该匹配关系，输出待进行反欺诈检测的会话事件描述。这样即可确定范例样本集的静态描述和目标待解析样本集的动态描述的展现区域，从而实现对第二会话场景解析结果的优化处理；使得输出的待进行反欺诈检测的会话事件描述中位于范例样本集的静态事件属性和位于目标待解析样本集的动态描述的展现区域是符合实际需求的。

[0150] 在本申请实施例中，通过将反欺诈检测授权信息记录与各反欺诈主题样本进行关联，以调用相同种类的反欺诈主题样本实现对反欺诈检测授权信息的事件属性解析，以及通过反欺诈主题样本中注释的范例样本集和存在联系的待解析样本集对事件属性解析结果进行显著可视化，从而能够提高得到的待进行反欺诈检测的会话事件描述的准确性和业务适配性。

[0151] 在一些可能的实施例中，如果在设定反欺诈主题数据集中不包括授权信息区分性表达的样本，则不能查到与授权信息区分性表达相同的目标反欺诈主题样本，那么可以基于该授权信息区分性表达结合反欺诈检测授权信息中的范例样本集的静态描述，生成实时

反欺诈主题样本;并将生成的实时反欺诈主题样本存入设定反欺诈主题数据集中,以实现对设定反欺诈主题数据集进行更换,使得更换的设定反欺诈主题数据集能够符合多种种类的反欺诈检测授权信息,从而提高对反欺诈检测授权信息记录进行样本适配的准确度和可信度。

[0152] 在一些可能的实施例中,对业务会话流式记录和反欺诈检测授权信息记录进行事件属性解析之后,需要判断得到的用户会话事件描述与待进行反欺诈检测的会话事件描述之间的量化适配程度,以实现对业务会话流式记录中的待解析会话事项和反欺诈检测授权信息的验证,进而判断该用户会话事件描述是否符合第二反欺诈检测条件,可以通过以下过程实现。

[0153] STEP151,通过所述反欺诈检测授权信息记录的范例样本集中的静态描述,对所述待进行反欺诈检测的会话事件描述进行差异化分析,以获得反欺诈检测关键词集合。在一些可能的实施例中,对于反欺诈检测授权信息记录包括的待进行反欺诈检测的会话事件描述,通过分析反欺诈检测授权信息记录的范例样本集中的静态描述,可以得到该反欺诈检测授权信息记录中包括哪些反欺诈检测关键词。

[0154] STEP152,在所述用户会话事件描述中,确定每一反欺诈检测关键词对应的待解析会话事项的多样化特征。在一些可能的实施例中,由于业务会话流式记录中包括多组待解析会话事项,那么这多组待解析会话事项可以是同一关键词的会话事项,也可以是不同关键词的会话事项。在确定出反欺诈检测授权信息中包括的反欺诈检测关键词之后,在用户会话事件描述中,对待解析会话事项按照该反欺诈检测关键词集合进行差异化分析,以获得每一反欺诈检测关键词的会话事项对应的用户会话事件描述,即多样化特征。例如,反欺诈检测关键词为支付类,那么在用户会话事件描述中,确定为支付类的会话事项对应的用户会话事件描述,即支付类的多样化特征。

[0155] STEP153,对于每一反欺诈检测关键词,确定每一所述反欺诈检测关键词对应的待进行反欺诈检测的会话事件描述与每一所述反欺诈检测关键词的多样化特征之间的量化适配程度。在一些可能的实施例中,按照反欺诈检测授权信息中的反欺诈检测关键词,对待进行反欺诈检测的会话事件描述和用户会话事件描述进行验证,分别验证每一反欺诈检测关键词中,该关键词的会话事项提供的数据是否与反欺诈检测授权信息中的数据相匹配,基于此,实现对反欺诈检测授权信息和会话事项的验证。每一反欺诈检测关键词的多样化特征包括:该反欺诈检测关键词的会话事项全局维度、互动时段等;通过比对多样化特征中每一项数据是否与该反欺诈检测关键词的待进行反欺诈检测的会话事件描述匹配,来确定每一反欺诈检测关键词对应的待进行反欺诈检测的会话事件描述与每一反欺诈检测关键词的多样化特征之间的量化适配程度。

[0156] STEP154,在所述量化适配程度不小于所述设定量化适配程度阈值的前提下,确定所述用户会话事件描述与所述待进行反欺诈检测的会话事件描述相对应。在一些可能的实施例中,如果用户会话事件描述中,该反欺诈检测关键词的多样化特征与反欺诈检测授权信息中的该反欺诈检测关键词的数据一致,那么则表明量化适配程度不小于设定量化适配程度阈值。

[0157] 在本申请实施例中,通过对反欺诈检测流式记录中的内容与待解析会话事项包括的内容进行验证,以确定用户会话事件描述是否与待进行反欺诈检测的会话事件描述一

致，可以自适应进行对反欺诈检测授权信息和会话事项的验证，以提高反欺诈检测过程中验证反欺诈检测授权信息和会话事项的效率。

[0158] 在一些可能的实施例中，通过将待解析会话事项的用户会话事件描述与反欺诈检测条件进行验证，以确定业务会话流式记录中的会话事项是否符合反欺诈检测条件，可以通过以下过程实现。

[0159] STEP161，在用户会话事件描述中，确定属于每一待解析会话事项的独立会话事件描述。在一些可能的实施例中，对于业务会话流式记录中的每一待解析会话事项，确定一组待解析会话事项的独立会话事件描述；例如，单组业务会话的维度、业务互动时段等。

[0160] STEP162，确定所述独立会话事件描述是否符合所述目标反欺诈检测指标，以确定所述用户会话事件描述是否符合所述第二反欺诈检测条件。在一些可能的实施例中，确定独立会话事件描述是否符合目标反欺诈检测指标，响应于独立会话事件描述符合目标反欺诈检测指标，确定用户会话事件描述符合第二反欺诈检测条件。通过对单组会话事项的用户会话事件描述中的每一项进行判断，如果单组业务会话的用户会话事件描述符合目标反欺诈检测指标，说明该业务会话流式记录中的每一待解析会话事项均是符合目标反欺诈检测指标的，所以确定用户会话事件描述符合第二反欺诈检测条件。

[0161] 对于一些可能的实现方式而言，首先，确定所述独立会话事件描述中的独立事件描述维度，和/或，确定携带衍生检测指标的目标会话事项种类，和/或，确定所述独立会话事件描述对应的待解析会话事项的区分性内容；然后，在所述独立事件描述维度不大于设定维度边界，和/或，所述目标会话事项种类的衍生内容与所述衍生指标相对应，和/或，在所述区分性内容属于设定业务会话内容集的前提下，确定所述用户会话事件描述符合目标反欺诈检测指标，以确定所述用户会话事件描述符合所述第二反欺诈检测条件。

[0162] 基于此，可以通过以下多种方式实现对用户会话事件描述是否符合目标反欺诈检测指标的验证。

[0163] 第一种方式

[0164] 第1步，确定独立会话事件描述的独立事件描述维度。在一些可能的实施例中，对于单组待解析会话事项的用户会话事件描述，确定该会话事项的维度，即独立事件描述维度；例如，对于云办公会话事项，确定该会话事项文件交互的维度。

[0165] 第2步，响应于独立事件描述维度不大于设定维度边界，确定用户会话事件描述符合目标反欺诈检测指标。在一些可能的实施例中，如果单组业务会话的维度小于或者等于设定的单组业务会话的设定维度边界，还可以进一步判断，与该会话事项属于同一关键词的所有会话事项的全局维度，判断全局维度是否超出设定的总维度约束，如果全局维度不大于设定的总维度约束，确定用户会话事件描述符合目标反欺诈检测指标。在本申请实施例中，维度用于指示不同的交互层面或者分析层面，例如业务层面、对象层面、网络环境层面等。

[0166] 第二种方式

[0167] 第1步，确定携带衍生检测指标的目标会话事项种类。在一些可能的实施例中，目标会话事项种类可以是在目标反欺诈检测指标中设定的，还可以是基于待解析会话事项的视觉特征信息的细致化程度，确定目标会话事项种类。第2步，响应于目标会话事项种类的衍生内容与衍生指标相对应，确定用户会话事件描述符合目标反欺诈检测指标。在一些可

能的实施例中，首先，在所述用户会话事件描述中，寻觅与所述目标会话事项种类适配的会话事项的衍生内容(例如可以是一些额外的详细内容)；进而判断目标会话事项种类的衍生内容与衍生指标的量化适配程度，如果量化适配程度较高，说明对于具有衍生检测指标的会话事项种类，实际上添加了对应的详细内容，因此，确定用户会话事件描述符合目标反欺诈检测指标。

[0168] 第三种方式

[0169] 第1步，确定独立会话事件描述对应的待解析会话事项的区分性内容。在一些可能的实施例中，待解析会话事项的区分性内容包括：待解析会话事项的会话事项编号和会话事项字段等，能够唯一区分该待解析会话事项的信息。第2步，响应于区分性内容属于设定业务会话内容集，确定用户会话事件描述符合目标反欺诈检测指标。在一些可能的实施例中，设定业务会话标识集为能够在指定平台查到会话事项标识的标识库，如果待解析会话事项的会话事项标识包含在设定业务会话标识集中，说明该待解析会话事项是有效会话事项，进一步，确定用户会话事件描述符合目标反欺诈检测指标。

[0170] 在本申请实施例中，上述方式一至三可以是并列的三种验证用户会话事件描述是否符合目标反欺诈检测指标的三种方式，还可以是对方式一至三中的任意两个或者三个设定先后关系或者顺承关系来验证用户会话事件描述是否符合目标反欺诈检测指标；例如，方式3的先后顺序优先于方式1，方式1的先后顺序优先于方式2；即，首先，判断区分性内容是否属于设定业务会话内容集；然后，如果区分性内容属于设定业务会话内容集，判断该有效业务会话的独立事件描述维度，最后，如果有效业务会话的独立事件描述维度小于等于维度边界，判断目标会话事项种类的衍生内容与衍生指标是否相对应，如果目标会话事项种类的衍生内容与衍生指标相对应，确定用户会话事件描述符合目标反欺诈检测指标。

[0171] 在另一实现方式中，还可以是针对方式一和三设定顺承关系，例如，首先，判断区分性内容是否属于设定业务会话内容集；然后，如果区分性内容属于设定业务会话内容集，判断该有效业务会话的独立事件描述维度，最后，如果有效业务会话的独立事件描述维度小于等于维度边界，确定用户会话事件描述符合目标反欺诈检测指标。

[0172] 在本申请实施例中，通过多种方式对待解析会话事项进行验证，以确定待解析会话事项的用户会话事件描述是否符合反欺诈检测条件，从而可以自适应进行对会话事项数据与反欺诈检测需求的验证。

[0173] 在一些可能的实施例中，对待进行反欺诈检测的会话事件描述和用户会话事件描述检测通过之后，对待解析会话事项进行反欺诈检测，即上述STEP103可以通过以下过程实现。

[0174] STEP131，响应于待进行反欺诈检测的会话事件描述符合第一反欺诈检测条件，且用户会话事件描述符合第二反欺诈检测条件，至少确定反欺诈检测授权信息记录所指向的检测约束类别和反欺诈检测对象信息。在一些可能的实施例中，在待进行反欺诈检测的会话事件描述符合第一反欺诈检测条件，且用户会话事件描述符合第二反欺诈检测条件的前提下，确定反欺诈检测授权信息记录中反欺诈检测对象的相关基本信息；通过对反欺诈检测对象信息的分析，确定反欺诈检测授权信息记录所指向的检测约束类别，比如各类反欺诈检测的限定条件。

[0175] STEP132，至少将检测约束类别和反欺诈检测对象信息，作为检测约束特征。在一

些可能的实施例中，基于检测约束特征中的反欺诈检测对象信息，确定用户会话事件描述的注释信息；将检测约束类别、反欺诈检测对象信息和注释信息等这些内容作为检测约束特征，实现对用户会话事件描述的反欺诈检测处理。

[0176] 在本申请实施例中，对反欺诈检测授权信息和会话事项进行验证通过后，通过在反欺诈检测授权信息记录中提取反欺诈检测对象信息，确定出相关等检测约束特征，从而实现智能化的反欺诈检测。

[0177] 在其他实施例中，对用户会话事件描述进行反欺诈检测之后，还可以包括以下内容：确定用户会话事件描述中已完成反欺诈检测的维度；基于已完成反欺诈检测的维度，创建并呈现反欺诈检测结果。

[0178] 在一些可能的实施例中，可以是生成与已完成反欺诈检测的维度存在配对关系的反欺诈检测结果。

[0179] 在一些可独立实施的实施例中，根据所述反欺诈检测结果进行信息防护处理，可以包括以下内容：获取针对反欺诈检测结果的信息风险描述记录，所述信息风险描述记录包括至少两条信息风险描述；获得所述信息风险描述记录中的各条信息风险描述与所述反欺诈检测结果之间的量化适配数据；根据所述各条信息风险描述对应的量化适配数据，以及所述各条信息风险描述的风险倾向表达，对所述各条信息风险描述进行整理，得到相应的信息风险描述整理结果；基于所述信息风险描述整理结果生成针对所述反欺诈检测结果的目标防护策略整理结果，所述目标防护策略整理结果包括至少两个目标防护策略；按照所述目标防护策略整理结果中的目标防护策略的先后顺序依次进行信息防护处理。

[0180] 可以理解的是，在本申请实施例中，通过考虑信息风险描述与反欺诈检测结果之间的量化适配数据，能够实现对信息风险描述的优先级调整，从而确定出有序的目标防护策略整理结果，这样在目标防护策略整理结果中的目标防护策略的先后顺序依次进行信息防护处理时能够尽可能避免前后策略之间的冲突，同时还能够提高信息防护的时效性和可靠性。

[0181] 在一些可独立实施的实施例中，所述根据所述各条信息风险描述对应的量化适配数据，以及所述各条信息风险描述的风险倾向表达，对所述各条信息风险描述进行整理，得到相应的信息风险描述整理结果，具体包括：根据所述各条信息风险描述对应的量化适配数据，以及所述各条信息风险描述的风险倾向表达，对所述各条信息风险描述进行拆解，得到至少两个信息风险描述子记录；对各个信息风险描述子记录进行整理，并分别对所述各个信息风险描述子记录中的各条信息风险描述进行整理，得到所述信息风险描述整理结果。如此，能够完整准确地确定信息风险描述整理结果。

[0182] 在一些可独立实施的实施例中，所述根据所述各条信息风险描述对应的量化适配数据，以及所述各条信息风险描述的风险倾向表达，对所述各条信息风险描述进行拆解，得到至少两个信息风险描述子记录，具体包括：分别根据所述各条信息风险描述对应的量化适配数据，对所述各条信息风险描述的风险倾向表达进行注意力处理，得到所述各条信息风险描述的注意力风险倾向表达；根据所述各条信息风险描述的注意力风险倾向表达对所述各条信息风险描述进行整合，得到至少两个信息风险描述子记录。如此，能够避免信息风险描述子记录之间存在混乱。

[0183] 在一些可独立实施的实施例中，所述对各个信息风险描述子记录之间进行整理，

并分别对所述各个信息风险描述子记录中的各条信息风险描述进行整理，得到所述信息风险描述整理结果，具体包括：根据各个信息风险描述子记录所包含的信息风险描述的数量，对所述各个信息风险描述子记录进行整理；以及，针对所述各个信息风险描述子记录，分别执行以下操作：根据所述信息风险描述子记录中各条信息风险描述的风险倾向表达与所述信息风险描述子记录的共性情况，对所述信息风险描述子记录中的各条信息风险描述进行整理；基于所述各个信息风险描述子记录之间的整理结果，以及所述各个信息风险描述子记录中各条信息风险描述的整理结果，生成所述信息风险描述整理结果。如此，能够确保信息风险描述整理结果的完整性。

[0184] 基于上述同样的发明构思，还提供了一种基于大数据安防的威胁识别装置20，应用于数据安防服务器10，所述装置包括：

[0185] 标签分析模块21，用于对涵盖多个云业务参与方标签的目标大数据服务运营日志集合中激活的至少一个云业务参与方标签进行持续性标签分析处理，确定每一云业务参与方标签在所述目标大数据服务运营日志集合中的状态更新情况；

[0186] 威胁识别模块22，用于依据所述目标大数据服务运营日志集合中得到的所述状态更新情况进行视觉型描述挖掘处理，并依据所述视觉型描述挖掘得到的操作意图表达确定所述目标大数据服务运营日志集合中的多个所述云业务参与方标签所对应的数字化威胁识别结果。

[0187] 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。

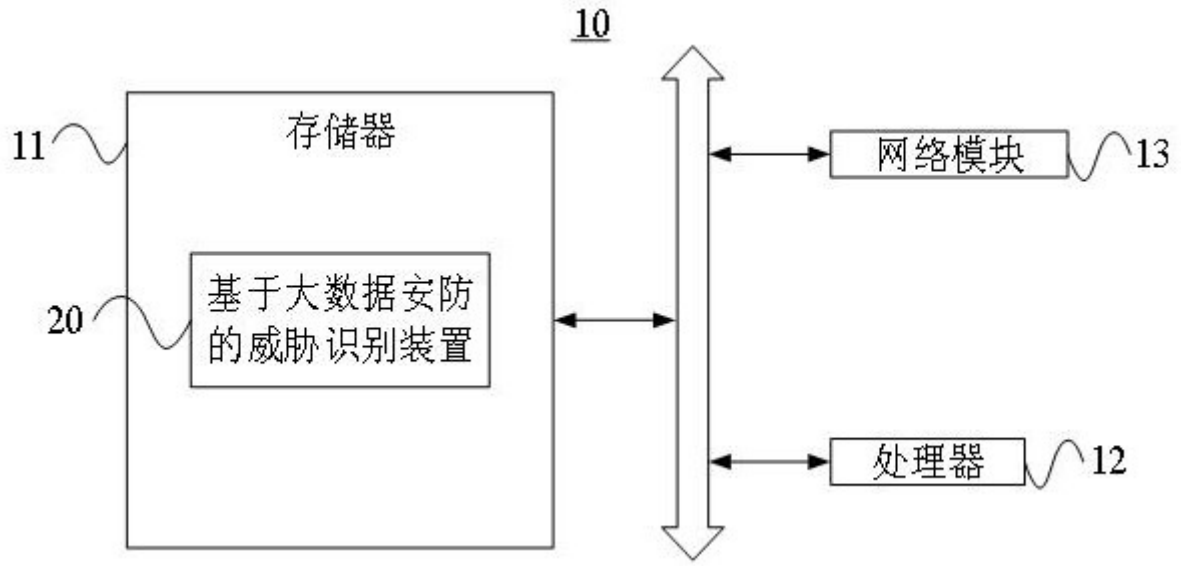

10
11
存储器
20
基于大数据安防的威胁识别装置
网络模块
13
处理器
12

图 1

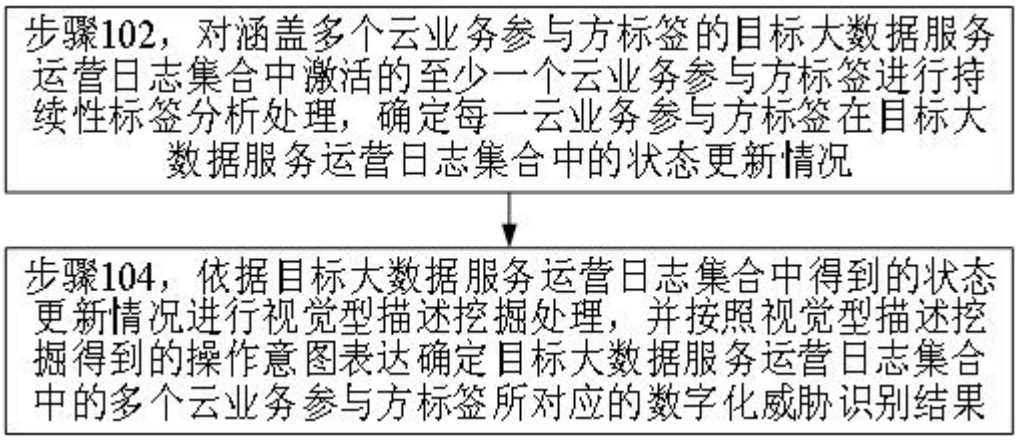

步骤102，对涵盖多个云业务参与方标签的目标大数据服务运营日志集合中激活的至少一个云业务参与方标签进行持续性标签分析处理，确定每一云业务参与方标签在目标大数据服务运营日志集合中的状态更新情况
步骤104，依据目标大数据服务运营日志集合中得到的状态更新情况进行视觉型描述挖掘处理，并按照视觉型描述挖掘得到的操作意图表达确定目标大数据服务运营日志集合中的多个云业务参与方标签所对应的数字化威胁识别结果

图 2

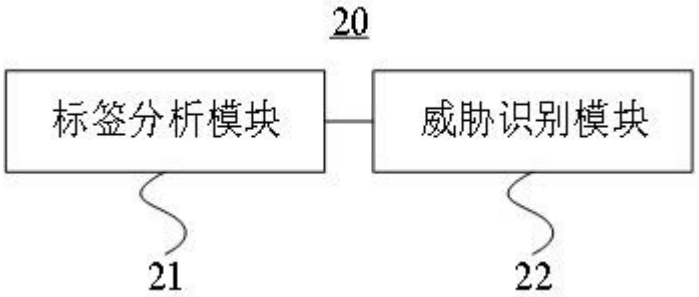

20
标签分析模块
威胁识别模块
21
22

图 3