(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115174231 A
(43)申请公布日 2022.10.11

(21)申请号 202210799167.3

(22)申请日 2022.07.08

(71)申请人 哈尔滨悦道科技开发有限公司
地址 150000 黑龙江省哈尔滨市南岗区宣化街240-2号

(72)发明人 关显峰

(51)Int.Cl.
H04L 9/40(2022.01)
G06N 20/00(2019.01)

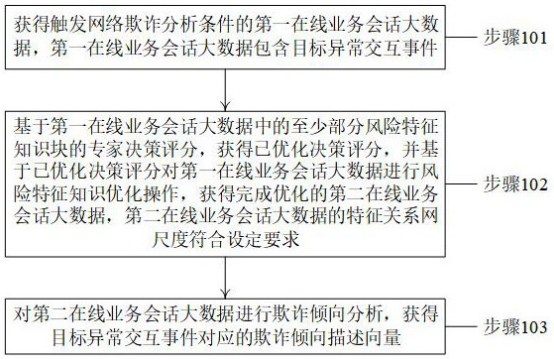
权利要求书3页 说明书19页 附图1页

(54)发明名称

一种基于AI Knowledge Base的网络欺诈分析方法及服务器

(57)摘要

本发明提供一种基于AI Knowledge Base的网络欺诈分析方法及服务器，鉴于第一在线业务会话大数据对应的已优化决策评分与第一在线业务会话大数据自身的专家决策评分存在关系，能够提高风险特征知识优化的智能化程度；已优化决策评分与第一在线业务会话大数据自身的专家决策评分存在关系，优化获得的第二在线业务会话大数据中的各个风险特征知识块之间联动贡献更佳，第二在线业务会话大数据中的已优化风险特征知识块对应的会话大数据活动描述与之前的风险特征知识块对应的会话大数据活动描述的相似度更高，对第二在线业务会话大数据进行欺诈倾向分析，不仅能够减少会话大数据定向捕捉处理的复杂性，还能够确保得到的欺诈倾向描述向量的精度和可信度。



CN 115174231 A

1.一种基于AI Knowledge Base的网络欺诈分析方法,其特征在于,应用于大数据安防服务器,所述方法包括:

获得触发网络欺诈分析条件的第一在线业务会话大数据,所述第一在线业务会话大数据包含目标异常交互事件;

结合所述第一在线业务会话大数据中的至少部分风险特征知识块的专家决策评分,获得已优化决策评分,并结合所述已优化决策评分对所述第一在线业务会话大数据进行风险特征知识优化操作,获得完成优化的第二在线业务会话大数据,所述第二在线业务会话大数据的特征关系网尺度符合设定要求;

对所述第二在线业务会话大数据进行欺诈倾向分析,获得所述目标异常交互事件对应的欺诈倾向描述向量。

2.根据权利要求1所述的方法,其特征在于,所述结合所述已优化决策评分对所述第一在线业务会话大数据进行风险特征知识优化操作,获得完成优化的第二在线业务会话大数据,包括:

依据设定数据信息量和所述第一在线业务会话大数据的信息量占比对所述第一在线业务会话大数据进行知识密度调整,获得第三在线业务会话大数据;以及在确定所述第三在线业务会话大数据的会话数据格式与设定数据格式不配对的基础上,通过所述已优化决策评分对所述第三在线业务会话大数据进行风险特征知识优化操作,获得会话数据格式与所述设定数据格式相配对的、完成优化的所述第二在线业务会话大数据;

或者,

通过所述已优化决策评分对所述第一在线业务会话大数据进行风险特征知识优化操作,获得会话数据格式与所述设定数据格式相配对的、完成优化的第四在线业务会话大数据;以及在确定所述第四在线业务会话大数据的会话数据信息量与所述设定数据信息量不配对的基础上,结合所述设定数据信息量和所述第四在线业务会话大数据的信息量占比对所述第一在线业务会话大数据进行知识密度调整,获得所述第二在线业务会话大数据。

3.根据权利要求1所述的方法,其特征在于,所述设定要求包含以下一项或以上:所述第二在线业务会话大数据的会话数据格式与设定数据格式配对;所述第二在线业务会话大数据的会话数据信息量与设定数据信息量配对。

4.根据权利要求1所述的方法,其特征在于,所述获得触发网络欺诈分析条件的第一在线业务会话大数据,包括:

获得触发网络欺诈分析条件的基础在线业务会话大数据,所述基础在线业务会话大数据中包括所述目标异常交互事件;

对所述基础在线业务会话大数据进行会话大数据定向捕捉,确定所述目标异常交互事件所对应的局部业务会话大数据为所述第一在线业务会话大数据。

5.根据权利要求4所述的方法,其特征在于,所述对所述基础在线业务会话大数据进行会话大数据定向捕捉,确定所述目标异常交互事件所对应的局部业务会话大数据为所述第一在线业务会话大数据,包括:

对所述基础在线业务会话大数据进行事件欺诈行为偏好挖掘,确定所述目标异常交互事件对应的若干个事件欺诈行为偏好,并结合所述若干个事件欺诈行为偏好中的每个所述事件欺诈行为偏好的第一分布标签,从所述基础在线业务会话大数据中捕捉所述目标异常

交互事件对应的所述第一在线业务会话大数据；

对所述基础在线业务会话大数据进行异常交互事件捕捉，确定所述目标异常交互事件对应的窗口化事件捕捉结果，并将所述窗口化事件捕捉结果对应的局部业务会话大数据视为所述第一在线业务会话大数据。

6.根据权利要求1所述的方法，其特征在于，所述基于AI Knowledge Base的网络欺诈分析方法通过已完成调试的AI专家系统模型实现；所述AI专家系统模型为通过携带相同先验注释的不同已认证在线业务会话大数据之间的欺诈倾向挖掘误差确定的欺诈倾向挖掘代价调试获得的。

7.根据权利要求6所述的方法，其特征在于，所述AI专家系统模型的调试包括：

获得若干组已认证在线业务会话大数据；其中，每组已认证在线业务会话大数据中的不同已认证在线业务会话大数据对应的先验注释一致，同一组中不同个已认证在线业务会话大数据中的已认证异常交互事件对应的已认证欺诈倾向描述向量不同；

对于每组已认证在线业务会话大数据，将该组已认证在线业务会话大数据加载到待调试的AI专家系统模型，通过所述待调试的AI专家系统模型对该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据进行处理，确定该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据分别对应的欺诈倾向分析数据；其中，所述欺诈倾向分析数据与欺诈倾向预测向量相对应；

依据每两个已认证在线业务会话大数据对应的欺诈倾向分析数据，确定欺诈倾向挖掘代价；

通过所述每组已认证在线业务会话大数据对应的欺诈倾向挖掘代价，对所述待调试的AI专家系统模型进行循环调试，直到符合调试结束要求，获得调试好的AI专家系统模型。

8.根据权利要求7所述的方法，其特征在于，所述依据每两个已认证在线业务会话大数据对应的欺诈倾向分析数据，确定欺诈倾向挖掘代价，包括：

依据每两个已认证在线业务会话大数据对应的欺诈倾向分析数据，确定每两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差；

结合所述每两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差，确定每两个已认证在线业务会话大数据对应的交叉熵模型代价；

依据每两个已认证在线业务会话大数据对应的交叉熵模型代价，确定第一模型代价指标；

利用每组已认证在线业务会话大数据对应的所述第一模型代价指标，确定所述欺诈倾向挖掘代价；

其中，所述利用每组已认证在线业务会话大数据对应的所述第一模型代价指标，确定所述欺诈倾向挖掘代价，包括：基于每个所述已认证在线业务会话大数据对应的欺诈倾向分析数据和每个所述已认证在线业务会话大数据对应的欺诈倾向参考，确定第二模型代价指标；利用每组已认证在线业务会话大数据对应的所述第一模型代价指标和所述第二模型代价指标，确定所述欺诈倾向挖掘代价。

9.根据权利要求7所述的方法，其特征在于，所述获得若干组已认证在线业务会话大数据，包括：

获得已认证基础业务会话大数据；以及对所述已认证基础业务会话大数据分别进行多

轮存在差异的特征强化操作，获得多个已认证目标业务会话大数据，将所述已认证基础业务会话大数据和所述多个已认证目标业务会话大数据视为所述一组已认证在线业务会话大数据所包含的多个已认证在线业务会话大数据；所述特征强化操作包括更新所述已认证基础业务会话大数据中已认证异常交互事件的全局分布、更新所述已认证基础业务会话大数据中的已认证异常交互事件的设定事件节点分布中的至少一种；所述设定事件节点包括至少一个；

或者，获得已认证异常交互事件对应的目标会话数据流；以及从所述目标会话数据流中确定若干组已认证在线业务会话大数据，其中，每组已认证在线业务会话大数据包括设定数目的在线业务会话信息，对应于相同已认证在线业务会话大数据簇的各个在线业务会话信息中的已认证异常交互事件对应的先验注释一致；且对应于相同已认证在线业务会话大数据簇的各个在线业务会话信息中的已认证异常交互事件对应的已认证欺诈倾向描述向量不同。

10.一种大数据安防服务器，其特征在于，包括：存储器和处理器；所述存储器和所述处理器耦合；所述存储器用于存储计算机程序代码，所述计算机程序代码包括计算机指令；当所述处理器执行所述计算机指令时，使得所述大数据安防服务器执行如权利要求1-9中任意一项所述的方法。

一种基于AI Knowledge Base的网络欺诈分析方法及服务器

技术领域

[0001] 本发明涉及人工智能技术领域，尤其涉及一种基于AI Knowledge Base的网络欺诈分析方法及服务器。

背景技术

[0002] 人工智能(Artificial Intelligence,AI)是计算机科学的一个分支，它企图了解智能的实质，并生产出一种新的能以人类智能相似的方式做出反应的智能机器，该领域的研究包括机器人、语言识别、图像识别、自然语言处理和专家系统等。

[0003] 以专家系统为例，专家系统包括知识挖掘等大数据分析功能，能够实现知识特征分析和信息推荐，但是在涉足网络欺诈分析时，相关技术却难以高效、准确且可靠地实现欺诈倾向分析处理。

发明内容

[0004] 本发明提供一种基于AI Knowledge Base的网络欺诈分析方法及服务器，为实现上述技术目的，本发明采用如下技术方案。

[0005] 第一方面是一种基于AI Knowledge Base的网络欺诈分析方法，应用于大数据安防服务器，所述方法包括：获得触发网络欺诈分析条件的第一在线业务会话大数据，所述第一在线业务会话大数据包含目标异常交互事件；结合所述第一在线业务会话大数据中的至少部分风险特征知识块的专家决策评分，获得已优化决策评分，并结合所述已优化决策评分对所述第一在线业务会话大数据进行风险特征知识优化操作，获得完成优化的第二在线业务会话大数据，所述第二在线业务会话大数据的特征关系网尺度符合设定要求；对所述第二在线业务会话大数据进行欺诈倾向分析，获得所述目标异常交互事件对应的欺诈倾向描述向量。

[0006] 应用于该实施例，设定要求可以反映能够进行欺诈倾向分析的在线业务会话大数据需符合的特征关系网尺度标准。依据由第一在线业务会话大数据中的至少部分风险特征知识块的专家决策评分确定的已优化决策评分进行风险特征知识智能优化，获得特征关系网尺度符合设定要求的第二在线业务会话大数据，从而获得了可以直接进行欺诈倾向分析的第二在线业务会话大数据。且鉴于第一在线业务会话大数据对应的已优化决策评分与第一在线业务会话大数据自身的专家决策评分存在关系，相较于仅通过原始专家决策评分进行风险特征知识优化而言，一方面能够提高风险特征知识优化的智能化程度；并且，已优化决策评分与第一在线业务会话大数据自身的专家决策评分存在关系，优化获得的第二在线业务会话大数据中的各个风险特征知识块之间联动贡献更佳，第二在线业务会话大数据中的已优化风险特征知识块对应的会话大数据活动描述与之前的风险特征知识块对应的会话大数据活动描述的相似度更高；进而对通过所述已优化风险特征知识块优化获得的第二在线业务会话大数据进行欺诈倾向分析，不仅能够减少会话大数据定向捕捉处理的复杂性，还能够确保得到的欺诈倾向描述向量的精度和可信度。

[0007] 在一些示例性实施例下,所述设定要求包含以下一项或以上:所述第二在线业务会话大数据的会话数据格式与设定数据格式配对;所述第二在线业务会话大数据的会话数据信息量与设定数据信息量配对。

[0008] 应用于该实施例,设定数据格式为AI专家系统模型能够处理的在线业务会话大数据对应的会话数据格式,设定数据信息量为AI专家系统模型能够处理的在线业务会话大数据对应的会话数据信息量,通过配置以上设定要求,可以获得AI专家系统模型能够快速处理的第二在线业务会话大数据。

[0009] 在一些示例性实施例下,所述结合所述已优化决策评分对所述第一在线业务会话大数据进行风险特征知识优化操作,获得完成优化的第二在线业务会话大数据,包括:依据设定数据信息量和所述第一在线业务会话大数据的信息量占比对所述第一在线业务会话大数据进行知识密度调整,获得第三在线业务会话大数据;以及在确定所述第三在线业务会话大数据的会话数据格式与设定数据格式不配对的基础上,通过所述已优化决策评分对所述第三在线业务会话大数据进行风险特征知识优化操作,获得会话数据格式与所述设定数据格式相配对的、完成优化的所述第二在线业务会话大数据;或者,通过所述已优化决策评分对所述第一在线业务会话大数据进行风险特征知识优化操作,获得会话数据格式与所述设定数据格式相配对的、完成优化的第四在线业务会话大数据;以及在确定所述第四在线业务会话大数据的会话数据信息量与所述设定数据信息量不配对的基础上,结合所述设定数据信息量和所述第四在线业务会话大数据的信息量占比对所述第一在线业务会话大数据进行知识密度调整,获得所述第二在线业务会话大数据。

[0010] 应用于该实施例,依据第一在线业务会话大数据的信息量占比对第一在线业务会话大数据进行知识密度调整,能够确保知识密度调整后的第三在线业务会话大数据不出现信息丢失。通过提供先对第一在线业务会话大数据进行知识密度调整再对知识密度调整后的第三在线业务会话大数据进行风险特征知识优化操作,或者,先对第一在线业务会话大数据进行风险特征知识优化操作,再对完成优化的第四在线业务会话大数据进行知识密度调整两种思路,能够灵活通过所述其中一种思路进行操作,提高了获得第二在线业务会话大数据的智能化程度。

[0011] 在一些示例性实施例下,所述获得触发网络欺诈分析条件的第一在线业务会话大数据,包括:获得触发网络欺诈分析条件的基础在线业务会话大数据,所述基础在线业务会话大数据中包括所述目标异常交互事件;对所述基础在线业务会话大数据进行会话大数据定向捕捉,确定所述目标异常交互事件所对应的局部业务会话大数据为所述第一在线业务会话大数据。

[0012] 应用于该实施例,将目标异常交互事件所对应的局部业务会话大数据视为第一在线业务会话大数据,再对第一在线业务会话大数据进行处理,相较于立刻对基础在线业务会话大数据进行全局处理,鉴于第一在线业务会话大数据的会话数据信息量更小、信噪比更高,对第一在线业务会话大数据进行处理能够减少资源开销,提高处理效率。

[0013] 在一些示例性实施例下,所述对所述基础在线业务会话大数据进行会话大数据定向捕捉,确定所述目标异常交互事件所对应的局部业务会话大数据为所述第一在线业务会话大数据,包括如下一项:对所述基础在线业务会话大数据进行事件欺诈行为偏好挖掘,确定所述目标异常交互事件对应的若干个事件欺诈行为偏好,并结合所述若干个事件欺诈行

为偏好中的每个所述事件欺诈行为偏好的第一分布标签,从所述基础在线业务会话大数据中捕捉所述目标异常交互事件对应的所述第一在线业务会话大数据;对所述基础在线业务会话大数据进行异常交互事件捕捉,确定所述目标异常交互事件对应的窗口化事件捕捉结果,并将所述窗口化事件捕捉结果对应的局部业务会话大数据视为所述第一在线业务会话大数据。

[0014] 应用于该实施例,通过对基础在线业务会话大数据进行事件欺诈行为偏好挖掘,可以精准确定出目标异常交互事件对应的若干个事件欺诈行为偏好,事件欺诈行为偏好可以精准反映目标异常交互事件对应的分布情况和欺诈倾向,由此,通过事件欺诈行为偏好的第一分布标签,能够获得目标异常交互事件对应的准确的第一在线业务会话大数据。通过对基础在线业务会话大数据进行异常交互事件捕捉,可以精准确定出可以反映目标异常交互事件的窗口化事件捕捉结果,进而基于窗口化事件捕捉结果能够获得准确的第一在线业务会话大数据。

[0015] 在一些示例性实施例下,所述基于AI Knowledge Base的网络欺诈分析方法通过已完成调试的AI专家系统模型实现;所述AI专家系统模型为通过携带相同先验注释的不同已认证在线业务会话大数据之间的欺诈倾向挖掘误差确定的欺诈倾向挖掘代价调试获得的。

[0016] 应用于该实施例,鉴于调试好的AI专家系统模型的分析准确性和可靠性较高,通过所述调试好的AI专家系统模型进行欺诈倾向分析,能够确保最终确定的欺诈倾向的精度和可信度。欺诈倾向挖掘误差可以反映AI专家系统模型在对存在相同先验注释的不同已认证在线业务会话大数据进行分析时,生成的欺诈倾向分析数据之间的差异,再通过所述基于该差异确定的欺诈倾向挖掘代价对AI专家系统模型进行调试,能够提高AI专家系统模型对存在相同先验注释的不同已认证在线业务会话大数据进行欺诈倾向分析时的精度和可信度,进而可以减少已认证在线业务会话大数据中的已认证异常交互事件之间的欺诈倾向差异对AI专家系统模型的分析精度和可信度的干扰,提高AI专家系统模型的分析准确性。

[0017] 在一些示例性实施例下,所述AI专家系统模型的调试包括:获得若干组已认证在线业务会话大数据;每组已认证在线业务会话大数据中的不同已认证在线业务会话大数据对应的先验注释一致,同一组中不同个已认证在线业务会话大数据中的已认证异常交互事件对应的已认证欺诈倾向描述向量不同;对于每组已认证在线业务会话大数据,将该组已认证在线业务会话大数据加载到待调试的AI专家系统模型,通过所述待调试的AI专家系统模型对该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据进行处理,确定该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据分别对应的欺诈倾向分析数据;其中,所述欺诈倾向分析数据与欺诈倾向预测向量相对应;依据每两个已认证在线业务会话大数据对应的欺诈倾向分析数据,确定欺诈倾向挖掘代价;通过所述每组已认证在线业务会话大数据对应的欺诈倾向挖掘代价,对所述待调试的AI专家系统模型进行循环调试,直到符合调试结束要求,获得调试好的AI专家系统模型。

[0018] 应用于该实施例,依据每两个已认证在线业务会话大数据对应的欺诈倾向分析数据,能够确定出每两个已认证在线业务会话大数据之间的欺诈倾向差别,该欺诈倾向差别是鉴于已认证在线业务会话大数据中的已认证异常交互事件对应的已认证欺诈倾向描述向量之间的欺诈倾向差异造成的,由此,依据每两个已认证在线业务会话大数据对应的欺

诈倾向分析数据，可以确定出可以反映欺诈倾向差别的欺诈倾向挖掘代价，再通过所述基于该欺诈倾向挖掘代价确定的欺诈倾向挖掘代价对待调试的AI专家系统模型进行循环调试，可以减少已认证在线业务会话大数据中的已认证异常交互事件之间的欺诈倾向差异对AI专家系统模型的分析精度和可信度的干扰，从而提高AI专家系统模型的适用性以及分析准确性。

[0019] 在一些示例性实施例下，所述依据每两个已认证在线业务会话大数据对应的欺诈倾向分析数据，确定欺诈倾向挖掘代价，包括：依据每两个已认证在线业务会话大数据对应的欺诈倾向分析数据，确定每两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差；结合所述每两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差，确定每两个已认证在线业务会话大数据对应的交叉熵模型代价；依据每两个已认证在线业务会话大数据对应的交叉熵模型代价，确定第一模型代价指标；利用每组已认证在线业务会话大数据对应的所述第一模型代价指标，确定所述欺诈倾向挖掘代价。

[0020] 应用于该实施例，交叉熵模型代价能够反映两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差，基于若干个交叉熵模型代价可以确定出可以反映任意两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差的第一模型代价指标；通过所述第一模型代价指标对应的欺诈倾向挖掘代价对待调试的AI专家系统模型进行循环调试，可以显著减少已认证在线业务会话大数据中的已认证异常交互事件之间的欺诈倾向差异对AI专家系统模型的分析精度和可信度的干扰。

[0021] 在一些示例性实施例下，所述利用每组已认证在线业务会话大数据对应的所述第一模型代价指标，确定所述欺诈倾向挖掘代价，包括：基于每个所述已认证在线业务会话大数据对应的欺诈倾向分析数据和每个所述已认证在线业务会话大数据对应的欺诈倾向参考，确定第二模型代价指标；利用每组已认证在线业务会话大数据对应的所述第一模型代价指标和所述第二模型代价指标，确定所述欺诈倾向挖掘代价。

[0022] 应用于该实施例，基于每个已认证在线业务会话大数据对应的欺诈倾向分析数据和每个已认证在线业务会话大数据对应的欺诈倾向参考，可以精准确定出对待调试的AI专家系统模型生成的欺诈倾向分析数据和欺诈倾向参考之间的第二模型代价指标，通过所述第二模型代价指标对待调试的AI专家系统模型进行调试，能够使得待调试的AI专家系统模型生成的欺诈倾向分析数据贴近欺诈倾向参考，从而，能显著提高待调试的AI专家系统模型的分析准确性。

[0023] 在一些示例性实施例下，所述获得若干组已认证在线业务会话大数据，包括如下一项：获得已认证基础业务会话大数据；以及对所述已认证基础业务会话大数据分别进行多轮存在差异的特征强化操作，获得多个已认证目标业务会话大数据，将所述已认证基础业务会话大数据和所述多个已认证目标业务会话大数据视为所述一组已认证在线业务会话大数据所包含的多个已认证在线业务会话大数据；所述特征强化操作包括更新所述已认证基础业务会话大数据中已认证异常交互事件的全局分布、更新所述已认证基础业务会话大数据中的已认证异常交互事件的设定事件节点分布中的至少一种；所述设定事件节点包括至少一个；获得已认证异常交互事件对应的目标会话数据流；以及从所述目标会话数据流中确定若干组已认证在线业务会话大数据，其中，每组已认证在线业务会话大数据包括设定数目的在线业务会话信息，对应于相同已认证在线业务会话大数据簇的各个在线业务

会话信息中的已认证异常交互事件对应的先验注释一致;且对应于相同已认证在线业务会话大数据簇的各个在线业务会话信息中的已认证异常交互事件对应的已认证欺诈倾向描述向量不同。

[0024] 应用于该实施例,通过特征强化操作,可以在获得少部分已认证基础业务会话大数据的基础上,获得更多数目的已认证在线业务会话大数据,显著减少了数据集(已认证基础业务会话大数据)的获取开销。通过特征强化操作后获得的已认证目标业务会话大数据中的已认证异常交互事件的欺诈倾向,和已认证基础业务会话大数据中的已认证异常交互事件的欺诈倾向存在欺诈倾向差异,将存在欺诈倾向差异的已认证目标业务会话大数据和已认证基础业务会话大数据视为已认证在线业务会话大数据,能够提高待调试的AI专家系统模型对欺诈倾向差异的吸收性能,继而有助于提高AI专家系统模型的分析准确性。

[0025] 第二方面是一种大数据安防服务器,包括存储器和处理器;所述存储器和所述处理器耦合;所述存储器用于存储计算机程序代码,所述计算机程序代码包括计算机指令;其中,当所述处理器执行所述计算机指令时,使得所述大数据安防服务器执行第一方面的方法。

[0026] 第三方面是一种计算机可读存储介质,其上存储有计算机程序,所述计算机程序在运行时执行第一方面的方法。

附图说明

[0027] 图1为本发明实施例提供的基于AI Knowledge Base的网络欺诈分析方法的流程示意图。

[0028] 图2为本发明实施例提供的基于AI Knowledge Base的网络欺诈分析装置的模块框图。

具体实施方式

[0029] 以下,术语“第一”、“第二”和“第三”等仅用于描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”或“第三”等的特征可以明示或者隐含地包括一个或者更多个该特征。

[0030] 图1示出了本发明实施例提供的基于AI Knowledge Base的网络欺诈分析方法的流程示意图,基于AI Knowledge Base的网络欺诈分析方法可以通过大数据安防服务器实现,大数据安防服务器可以包括存储器和处理器;所述存储器和所述处理器耦合;所述存储器用于存储计算机程序代码,所述计算机程序代码包括计算机指令;其中,当所述处理器执行所述计算机指令时,使得所述大数据安防服务器执行如下步骤所描述的技术方案。

[0031] 步骤101、获得触发网络欺诈分析条件的第一在线业务会话大数据,第一在线业务会话大数据包含目标异常交互事件。

[0032] 对于本发明实施例而言,第一在线业务会话大数据可以为获得的需要对其中所包含的目标异常交互事件进行欺诈倾向分析的在线业务会话大数据,第一在线业务会话大数据中的目标异常交互事件对应有待分析欺诈倾向。目标异常交互事件可以包括但不限于目标业务咨询事件、目标链接推荐事件,举例而言,目标异常交互事件可以为任一存在欺诈倾向分析价值的异常交互事件。待分析欺诈倾向比如可以包括资金盗取、信息窃取、隐私访

问、流氓推送等，举例而言，待分析欺诈倾向可以为目标异常交互事件匹配的任一欺诈倾向。

[0033] 在实际实施过程中，可以将大数据采集线程采集包括蕴藏待分析欺诈倾向的目标异常交互事件的在线业务会话大数据视为触发网络欺诈分析条件的第一在线业务会话大数据，或者，也可以从通过所述大数据采集线程采集的目标异常交互事件的会话数据流中确定任意一组在线业务会话信息视为触发网络欺诈分析条件的第一在线业务会话大数据。

[0034] 进一步地，网络欺诈分析条件可以基于业务类型设置，比如可以将跨境电商业务类型的会话大数据作为触发网络欺诈分析条件的在线业务会话大数据，网络欺诈分析条件还可以根据业务时段设置，在此不作限定。在线业务会话大数据记录了不同用户之间的交互情况，比如行为记录、聊天记录、操作记录等。

[0035] 对于一些可能的设计思路而言，还可以通过如下方式获得第一在线业务会话大数据。

[0036] 步骤1011、获得触发网络欺诈分析条件的基础在线业务会话大数据；基础在线业务会话大数据中包含目标异常交互事件。

[0037] 对于本发明实施例而言，基础在线业务会话大数据可以为获得的需要对其中所包含的目标异常交互事件进行欺诈倾向分析的原始在线业务会话大数据，第一在线业务会话大数据可以为从基础在线业务会话大数据中拆解出来的只包含目标异常交互事件对应的数据集的在线业务会话大数据。

[0038] 举例而言，可以将大数据采集线程采集包括蕴藏待分析欺诈倾向的目标异常交互事件的在线业务会话大数据视为基础在线业务会话大数据。

[0039] 步骤1012、对基础在线业务会话大数据进行会话大数据定向捕捉，确定目标异常交互事件所对应的局部业务会话大数据为第一在线业务会话大数据。

[0040] 对于本发明实施例而言，对基础在线业务会话大数据进行的会话大数据定向捕捉可以为捕捉到基础在线业务会话大数据中的目标异常交互事件所对应的数据集的操作，会话大数据定向捕捉后获得的结果可以与目标异常交互事件在基础在线业务会话大数据中的分布情况以及目标异常交互事件实施的待分析欺诈倾向有关，从而第一在线业务会话大数据与目标异常交互事件在基础在线业务会话大数据中的分布情况以及目标异常交互事件实施的待分析欺诈倾向相关。

[0041] 在实际实施过程中，在获得基础在线业务会话大数据然后可以对基础在线业务会话大数据进行会话大数据定向捕捉(也可以理解为进行会话大数据分析/识别)，确定出基础在线业务会话大数据中的目标异常交互事件所对应的数据集。在确定出目标异常交互事件所对应的数据集然后可以立即将基础在线业务会话大数据中的该数据集对应的局部在线业务会话大数据捕捉出来视为第一在线业务会话大数据；或者，在确定出基础在线业务会话大数据中的目标异常交互事件对应的数据集然后可以依据设定的扩展比值对该数据集进行数据集扩展操作，将完成扩展操作的数据集对应的局部在线业务会话大数据视为第一在线业务会话大数据，扩展操作后的获得的第一在线业务会话大数据的会话数据信息量少于基础在线业务会话大数据的会话数据信息量。

[0042] 如此一来，相较于基础在线业务会话大数据，拆解下来的第一在线业务会话大数据的会话数据信息量更小、信噪比更高，通过对从基础在线业务会话大数据中拆解下来的

第一在线业务会话大数据进行欺诈倾向分析处理，能够减少资源开销，提高处理效率。

[0043] 对于本发明实施例而言，鉴于目标异常交互事件在基础在线业务会话大数据中的分布情况以及目标异常交互事件对应的待分析欺诈倾向不同，因此确定出的基础在线业务会话大数据中的目标异常交互事件对应的数据集的数据格式也不确定，比如，确定出的目标异常交互事件对应的数据集可以为列表式数据集、图节点式数据集等。由此，根据相异的基础在线业务会话大数据获得的第一在线业务会话大数据对应的会话数据格式也可以存在差异，在会话数据格式存在差异的基础上，根据相异的基础在线业务会话大数据获得的第一在线业务会话大数据对应的会话数据信息量也将不一致。

[0044] 此外，即便对于同一组基础在线业务会话大数据，在通过相异的捕捉思路进行会话大数据定向捕捉时，确定出的基础在线业务会话大数据中的目标异常交互事件对应的数据集的数据格式也可能存在差异，进而获得的第一在线业务会话大数据对应的会话数据格式和会话数据信息量也可能存在差异。

[0045] 进一步地，对于任一基础在线业务会话大数据，对其进行会话大数据定向捕捉后获得的第一在线业务会话大数据的对应会话数据格式。

[0046] 对于一些可能的设计思路而言，对于步骤1012，可以通过如下两种思路(思路一和思路二)从基础在线业务会话大数据中确定出第一在线业务会话大数据。

[0047] 思路一、对基础在线业务会话大数据进行事件欺诈行为偏好挖掘，确定目标异常交互事件对应的若干个事件欺诈行为偏好，并基于若干个事件欺诈行为偏好中的每个事件欺诈行为偏好的第一分布标签，从基础在线业务会话大数据中捕捉目标异常交互事件对应的第一在线业务会话大数据。

[0048] 对于本发明实施例而言，事件欺诈行为偏好可以为可以反映目标异常交互事件实施的欺诈倾向的若干个行为偏好。比如，在目标异常交互事件为目标业务咨询事件的基础上，可以在目标业务咨询事件的不同事件环节确定一定数目的行为偏好，将这些行为偏好视为目标业务咨询事件对应的事件欺诈行为偏好。关于事件欺诈行为偏好的数目的配置可以灵活实现。

[0049] 第一分布标签可以为分析出的事件欺诈行为偏好在基础在线业务会话大数据中的分布情况，举例而言，该分布情况可以为风险特征知识块位置分布。

[0050] 在本发明实施例所提供的基于AI Knowledge Base的网络欺诈分析方法通过所述已完成调试的AI专家系统模型实现的基础上，AI专家系统模型中还可以包括行为偏好挖掘单元。在实际实施过程中，在将基础在线业务会话大数据加载到AI专家系统模型然后可以通过所述行为偏好挖掘单元，对基础在线业务会话大数据进行事件欺诈行为偏好挖掘，确定出目标异常交互事件对应的各个事件欺诈行为偏好；进而可以确定出各个事件欺诈行为偏好在基础在线业务会话大数据中对应的风险特征知识块位置分布；然后，可以基于各个事件欺诈行为偏好对应的风险特征知识块位置分布，确定出捕捉窗口，将该捕捉窗口对应的在线业务会话数据集从基础在线业务会话大数据中捕捉出，获得第一在线业务会话大数据。

[0051] 思路二、对基础在线业务会话大数据进行异常交互事件捕捉，确定目标异常交互事件对应的窗口化事件捕捉结果，并将窗口化事件捕捉结果对应的局部业务会话大数据视为第一在线业务会话大数据。

[0052] 对于本发明实施例而言，窗口化事件捕捉结果可以为目标异常交互事件对应在基础在线业务会话大数据中的分布情况。此外，窗口化事件捕捉结果还可以理解为事件捕捉框/事件识别框。

[0053] 在实际实施过程中，在本发明实施例所提供的基于AI Knowledge Base的网络欺诈分析方法通过所述已完成调试的AI专家系统模型实现的基础上，AI专家系统模型中可以包括已完成调试的、用于捕捉在线业务会话大数据中包含的目标异常交互事件的异常交互事件捕捉单元。在实际实施过程中，在将基础在线业务会话大数据加载到AI专家系统模型然后可以通过所述异常交互事件捕捉单元，对基础在线业务会话大数据进行欺诈倾向分析处理，确定出目标异常交互事件对应的窗口化事件捕捉结果，然后可以将窗口化事件捕捉结果对应的局部业务会话大数据视为第一在线业务会话大数据。

[0054] 步骤102、基于第一在线业务会话大数据中的至少部分风险特征知识块的专家决策评分，获得已优化决策评分，并基于已优化决策评分对第一在线业务会话大数据进行风险特征知识优化操作，获得完成优化的第二在线业务会话大数据，第二在线业务会话大数据的特征关系网尺度符合设定要求。

[0055] 对于本发明实施例而言，第一在线业务会话大数据中的至少部分风险特征知识块(风险特征向量、风险特征字段、风险特征数组等，比如电子商务会话中的异常信息请求行为特征，第三方链接发送行为特征等)可以为第一在线业务会话大数据中的所有风险特征知识块、第一在线业务会话大数据中的部分风险特征知识块，已优化决策评分可以为需要优化在第一在线业务会话大数据中的已优化风险特征知识块对应的专家决策评分。进一步地，专家决策评分可以理解为已优化风险特征知识块的知识值、描述值和特征值。

[0056] 第二在线业务会话大数据可以为对第一在线业务会话大数据进行风险特征知识优化后获得的、会话大数据活动描述关系网尺度符合设定要求的在线业务会话大数据。设定要求可以反映能够进行欺诈倾向分析的在线业务会话大数据需符合的特征关系网尺度标准。鉴于AI专家系统模型要求加载的在线业务会话大数据需要存在指定数据信息量和指定数据格式，所以在实际实施过程中，设定要求可以包含以下一项或以上：第二在线业务会话大数据的会话数据格式与设定数据格式配对；第二在线业务会话大数据的会话数据信息量与设定数据信息量配对。

[0057] 对于本发明实施例而言，设定数据格式可以为AI专家系统模型要求加载的在线业务会话大数据需具备的指定数据信息量，设定数据信息量可以为AI专家系统模型要求加载的在线业务会话大数据需具备的指定数据信息量。示例性的设定数据格式和设定数据信息量可以基于实际应用场景中的模型变量进行配置。

[0058] 鉴于在实际应用场景中获得的第一在线业务会话大数据的会话数据格式和会话数据信息量都不确定，因此在获得第一在线业务会话大数据之后，需要对其进行优化，将其优化为特征关系网尺度符合设定要求的第二在线业务会话大数据。

[0059] 在实际实施过程中，在获得第一在线业务会话大数据然后可以将第一在线业务会话大数据中的至少部分风险特征知识块的专家决策评分的评分均值视为已优化决策评分；或者，也可以将先验的若干个专家决策评分对应的均值(示例性为专家决策评分127)视为已优化决策评分；或者，也可以基于第一在线业务会话大数据中的至少部分风险特征知识块中的每个风险特征知识块的专家决策评分，确定至少部分风险特征知识块对应的专家决

策评分的均值、中位数等，将其视为已优化决策评分。

[0060] 以已优化决策评分为评分均值为例，在确定已优化决策评分之后，还可以确定第一在线业务会话大数据对应的会话大数据活动描述关系网尺度是否符合设定要求。如果不符合设定要求，则可以通过所述已优化决策评分对第一在线业务会话大数据进行特征识别度智能优化，将第一在线业务会话大数据的会话数据信息量优化为设定数据信息量，且将第一在线业务会话大数据的会话数据格式优化为设定数据格式，从而，在第一在线业务会话大数据的标志性数据区域增设一定数目的风险特征知识特征值为已优化决策评分的已优化风险特征知识块。进而优化完成后可以获得会话大数据活动描述关系网尺度符合设定要求的第二在线业务会话大数据。

[0061] 进一步地，第一在线业务会话大数据对应的会话大数据活动描述关系网尺度不符合设定要求的情况比如可以包括如下两种：第一种、第一在线业务会话大数据对应的会话数据信息量不是设定数据信息量，且第一在线业务会话大数据对应的会话数据格式不是设定数据格式；第二种、第一在线业务会话大数据对应的会话数据格式为设定数据格式，但第一在线业务会话大数据对应的会话数据信息量不是设定数据信息量。

[0062] 在一些示例中，如果从基础在线业务会话大数据中拆解获得的第一在线业务会话大数据的会话大数据活动描述关系网尺度符合设定要求，则可以不对第一在线业务会话大数据做任何调整，立刻将第一在线业务会话大数据视为第二在线业务会话大数据。

[0063] 步骤103、对第二在线业务会话大数据进行欺诈倾向分析，获得目标异常交互事件对应的欺诈倾向描述向量。

[0064] 对于本发明实施例而言，欺诈倾向描述向量可以为分析出的目标异常交互事件在第一在线业务会话大数据中对应的欺诈倾向，比如，欺诈倾向描述向量可以为隐私窃取、数据篡改等。

[0065] 在实际实施过程中，可以通过所述已完成调试的AI专家系统模型对第二在线业务会话大数据进行异常交互事件欺诈倾向分析，以确定目标异常交互事件在第二在线业务会话大数据中实施的欺诈倾向，从而确定了目标异常交互事件在基础在线业务会话大数据中实施的欺诈倾向，进而可以将确定的该欺诈倾向视为目标异常交互事件对应的欺诈倾向描述向量。

[0066] 应用以上步骤101-步骤103所记录的技术方案，依据由第一在线业务会话大数据中的至少部分风险特征知识块的专家决策评分确定的已优化决策评分进行风险特征知识智能优化，获得特征关系网尺度符合设定要求的第二在线业务会话大数据，从而获得了可以直接进行欺诈倾向分析的第二在线业务会话大数据。且鉴于第一在线业务会话大数据对应的已优化决策评分与第一在线业务会话大数据自身的专家决策评分存在关系，相较于仅通过原始专家决策评分进行风险特征知识优化而言，一方面能够提高风险特征知识优化的智能化程度；并且，已优化决策评分与第一在线业务会话大数据自身的专家决策评分存在关系，优化获得的第二在线业务会话大数据中的各个风险特征知识块之间联动贡献更佳，第二在线业务会话大数据中的已优化风险特征知识块对应的会话大数据活动描述与之前的风险特征知识块对应的会话大数据活动描述的相似度更高；进而对通过所述已优化风险特征知识块优化获得的第二在线业务会话大数据进行欺诈倾向分析，不仅能够减少会话大数据定向捕捉处理的复杂性，还能够确保得到的欺诈倾向描述向量的精度和可信度。

[0067] 对于一些可能的设计思路而言，对于步骤102中基于已优化决策评分对第一在线业务会话大数据进行风险特征知识优化操作，获得完成优化的第二在线业务会话大数据的步骤，还可以按照以下两种思路(思路a和思路b)中的任一种实施。

[0068] 思路a、依据设定数据信息量和第一在线业务会话大数据的信息量占比对第一在线业务会话大数据进行知识密度调整，获得第三在线业务会话大数据；以及在确定第三在线业务会话大数据的会话数据格式与设定数据格式不配对的基础上，通过所述已优化决策评分对第三在线业务会话大数据进行风险特征知识优化操作，获得会话数据格式与设定数据格式相配对的、完成优化的第二在线业务会话大数据。

[0069] 对于本发明实施例而言，信息量占比可以为第一在线业务会话大数据对应的窗口化覆盖规模数据，或者，信息量占比也可以为第一在线业务会话大数据中的目标异常交互事件对应的窗口化覆盖规模数据。第三在线业务会话大数据可以为只对第一在线业务会话大数据进行知识密度调整后获得的在线业务会话大数据。进一步地，知识密度调整可以理解为知识精简处理。

[0070] 在实际实施过程中，在确定第一在线业务会话大数据的会话数据信息量与设定数据信息量不符的基础上，则可以确定第一在线业务会话大数据不可供AI专家系统模型直接捕捉。进而可以以设定数据信息量视为调整参考，以维持第一在线业务会话大数据的信息量占比不发生改变为调整思路，对第一在线业务会话大数据进行知识密度调整(窗口规模变更，压缩或者扩展数据窗口)，获得第三在线业务会话大数据。

[0071] 进一步地，在获得第三在线业务会话大数据之后，还可以确定第三在线业务会话大数据的会话数据格式是否与设定数据格式相配对，如果配对，则可以确定第三在线业务会话大数据对应的会话大数据活动描述关系网尺度符合设定要求，第三在线业务会话大数据可供AI专家系统模型直接处理，进而将第三在线业务会话大数据视为最终确定的第二在线业务会话大数据。

[0072] 如果不配对，则表明第三在线业务会话大数据不可供AI专家系统模型直接识别，进而可以通过所述确定的已优化决策评分对第三在线业务会话大数据进行风险特征知识优化操作，将第三在线业务会话大数据的会话数据格式优化为设定数据格式，从而获得会话数据格式与设定数据格式相配对的、完成优化的第二在线业务会话大数据。

[0073] 举例而言，在通过所述已优化决策评分对第三在线业务会话大数据进行风险特征知识优化操作时，可以根据第三在线业务会话大数据的会话数据格式和设定数据格式，确定需要优化的已优化风险特征知识块的数目和各个已优化风险特征知识块的分布情况。对于本发明实施例而言，在在实际实施过程中，在确定需要优化的已优化风险特征知识块的数目和分布情况时，可以以需要优化的已优化风险特征知识块的数目最小即可将第三在线业务会话大数据的会话数据格式变为设定数据格式为目的，确定已优化风险特征知识块的数目和分布情况。进一步的，可以基于确定的已优化风险特征知识块的数目和分布情况，对第三在线业务会话大数据进行特征识别度智能优化，获得第二在线业务会话大数据。

[0074] 思路b、通过所述已优化决策评分对第一在线业务会话大数据进行风险特征知识优化操作，获得会话数据格式与设定数据格式相配对的、完成优化的第四在线业务会话大数据；以及在确定第四在线业务会话大数据的会话数据信息量与设定数据信息量不配对的基础上，依据设定数据信息量和所述第四在线业务会话大数据的信息量占比对第一在线业

务会话大数据进行知识密度调整，获得第二在线业务会话大数据。

[0075] 对于本发明实施例而言，第四在线业务会话大数据可以为只对第一在线业务会话大数据进行风险特征知识优化操作后获得的在线业务会话大数据。

[0076] 在实际实施过程中，在获得第一在线业务会话大数据之后，若确定第一在线业务会话大数据对应的会话数据格式与设定数据格式不配对，则可以确定第一在线业务会话大数据不可供AI专家系统模型直接识别。进而可以根据第一在线业务会话大数据的会话数据格式和设定数据格式，确定需要优化的已优化风险特征知识块的数目和各个已优化风险特征知识块的分布情况。对于本发明实施例而言，在在实际实施过程中，在确定需要优化的已优化风险特征知识块的数目和分布情况时，可以以需要优化的已优化风险特征知识块的数目最小即可将第一在线业务会话大数据的会话数据格式变为设定数据格式为目的，确定已优化风险特征知识块的数目和分布情况。进一步的，可以基于确定的已优化风险特征知识块的数目和分布情况，对第一在线业务会话大数据进行特征识别度智能优化，获得第四在线业务会话大数据。

[0077] 进一步的，在获得第四在线业务会话大数据然后可以确定第四在线业务会话大数据对应的会话数据信息量是否与设定数据信息量相配对，如果是，则表明第四在线业务会话大数据对应的会话大数据活动描述关系网尺度符合设定要求，第四在线业务会话大数据可供AI专家系统模型直接识别，进而将第四在线业务会话大数据视为最终确定的第二在线业务会话大数据。如果否，则说明第四在线业务会话大数据不可供AI专家系统模型直接处理，进而可以以设定数据信息量视为调整参考，以维持第四在线业务会话大数据对应的信息量占比不发生改变为调整思路，对第四在线业务会话大数据进行知识密度调整，获得会话数据信息量为设定数据信息量的第二在线业务会话大数据。

[0078] 对于一些可能的设计思路而言，本发明实施例所提供的基于AI Knowledge Base的网络欺诈分析方法可以为已完成调试的AI专家系统模型实现的；AI专家系统模型可以为通过携带相同先验注释的不同已认证在线业务会话大数据之间的欺诈倾向挖掘误差确定的欺诈倾向挖掘代价调试获得的。

[0079] 对于本发明实施例而言，欺诈倾向挖掘误差可以为AI专家系统模型在对已认证在线业务会话大数据进行欺诈倾向分析时，生成的各个已认证在线业务会话大数据对应的欺诈倾向分析数据之间的偏差。欺诈倾向分析数据用于表征AI专家系统模型生成的已认证在线业务会话大数据对应于各种设定的挖掘欺诈倾向的可能性矩阵，基于欺诈倾向分析数据，可以直接确定已认证在线业务会话大数据对应的欺诈倾向预测向量。比如，可以确定欺诈倾向分析数据对应的可能性矩阵中的最大可能性值，将该最大可能性值对应的设定的挖掘欺诈倾向视为已认证在线业务会话大数据对应的欺诈倾向预测向量。

[0080] 进一步地，不同的已认证在线业务会话大数据对应的先验注释一致，从而不同的已认证在线业务会话大数据对应的实际的欺诈倾向描述向量一致，但不同的已认证在线业务会话大数据中的已认证异常交互事件对应的已认证欺诈倾向描述向量存在一定的差别。

[0081] 在实际实施过程中，可以将不同的已认证在线业务会话大数据加载到待调试的AI专家系统模型，通过所述待调试的AI专家系统模型对不同的已认证在线业务会话大数据分别进行处理，分别确定出每个已认证在线业务会话大数据对应的欺诈倾向分析数据。其次，依据每两个已认证在线业务会话大数据对应的欺诈倾向分析数据，确定出每两个已认证在

线业务会话大数据对应的欺诈倾向挖掘误差;之后,基于确定的每个欺诈倾向挖掘误差,确定出最后的欺诈倾向挖掘误差。进而可以通过所述该欺诈倾向挖掘误差确定待调试的AI专家系统模型的欺诈倾向挖掘代价,并通过所述确定该欺诈倾向挖掘代价对待调试的AI专家系统模型进行循环调试,获得调试好的AI专家系统模型。

[0082] 在本发明实施例中,可以仅上述步骤103通过所述已完成调试的AI专家系统模型实现。

[0083] 对于一些可能的设计思路而言,本发明实施例还提供了一种调试AI专家系统模型的思路,示例性的可以包括以下步骤301-步骤304所记录的技术方案。

[0084] 步骤301、获得若干组已认证在线业务会话大数据。

[0085] 进一步地,每组已认证在线业务会话大数据中的不同已认证在线业务会话大数据对应的先验注释一致,同一组中不同个已认证在线业务会话大数据中的已认证异常交互事件对应的已认证欺诈倾向描述向量不同。

[0086] 对于本发明实施例而言,若干组已认证在线业务会话大数据中的每组已认证在线业务会话大数据对应的先验注释不一致,但同一组已认证在线业务会话大数据中的不同已认证在线业务会话大数据对应的先验注释一致,先验注释可以为已认证在线业务会话大数据中已认证异常交互事件对应的已认证欺诈倾向描述向量对应的欺诈倾向。

[0087] 比如,对于已认证在线业务会话大数据簇data set1,该组中的各个已认证在线业务会话大数据对应的先验注释均为已认证异常交互事件对应的已认证倾向为“隐私窃取”,对于已认证在线业务会话大数据簇data set2,该组中的各个已认证在线业务会话大数据对应的先验注释均为已认证异常交互事件对应的已认证倾向为“数据篡改”。

[0088] 但同一个已认证在线业务会话大数据簇中的各个已认证在线业务会话大数据中已认证异常交互事件对应的已认证欺诈倾向描述向量之间存在些许变化,从而同一组中不同个已认证在线业务会话大数据中的已认证异常交互事件对应的已认证欺诈倾向描述向量不同。并且,为了降低调试开销,在确定数据集时,通常一种欺诈倾向对应的已认证在线业务会话大数据的数目有限,进而造成完成调试的AI专家系统模型会出现处理条件过于苛刻。如此,在完成调试的AI专家系统模型应用时,在线业务会话大数据中欺诈倾向的轻微改变,比如,业务咨询事件状态更新,将导致AI专家系统模型生成的欺诈倾向更新,显著干扰了AI专家系统模型的挖掘可信度。

[0089] 对于上述问题,本发明提供了一种获得已认证在线业务会话大数据的思路,基于该思路能显著提高用于调试的已认证在线业务会话大数据的数目。举例而言,对于一些可能的设计思路而言,可以按照以下两种思路(思路M和思路N)中的任一种方式获得若干组已认证在线业务会话大数据。

[0090] 思路M、获得已认证基础业务会话大数据;以及对已认证基础业务会话大数据分别进行多轮存在差异的特征强化操作,获得多个已认证目标业务会话大数据,将已认证基础业务会话大数据和多个已认证目标业务会话大数据视为一组已认证在线业务会话大数据所包含的多个已认证在线业务会话大数据;特征强化操作包括更新已认证基础业务会话大数据中已认证异常交互事件的全局分布、更新已认证基础业务会话大数据中的已认证异常交互事件的设定事件节点分布中的至少一种;设定事件节点包括至少一个。

[0091] 对于本发明实施例而言,已认证基础业务会话大数据可以包括若干个存在不同先

验注释的在线业务会话大数据，每个已认证基础业务会话大数据对应于一个先验注释，不同已认证基础业务会话大数据对应的先验注释不同。在实际实施过程中，获得的已认证基础业务会话大数据的数目可以根据AI专家系统模型能够挖掘的欺诈倾向类别确定。比如，AI专家系统模型能够挖掘的欺诈倾向类别为5种，类别classification1、类别classification2、类别classification3、类别classification4、类别classification5，则可以确定5组已认证基础业务会话大数据，其中，5组已认证基础业务会话大数据中的已认证异常交互事件对应的欺诈倾向类别分类为类别classification1、类别classification2、类别classification3、类别classification4、类别classification5。

[0092] 可以理解的是，特征强化操作可以为能够对已认证基础业务会话大数据进行会话大数据活动描述更新、获得已认证基础业务会话大数据对应的已认证目标业务会话大数据的处理。特征强化操作可以包括更新已认证基础业务会话大数据中已认证异常交互事件的全局分布、更新已认证基础业务会话大数据中的已认证异常交互事件的设定事件节点分布中的至少一种；设定事件节点包括至少一个。其中，设定事件节点比如可以为已认证异常交互事件的不同交互节点。更新已认证基础业务会话大数据中已认证异常交互事件的全局分布比如可以为已认证异常交互事件的整体位置分布。更新已认证基础业务会话大数据中的已认证异常交互事件的设定事件节点分布可以为更新已认证异常交互事件的任一设定事件节点的上下游关联特征。

[0093] 举例而言，特征强化操作还可以包括但不限于如下几种：对已认证基础业务会话大数据进行特征层面的显著性增强，更新已认证基础业务会话大数据中的数据标签，更新已认证基础业务会话大数据中的各个风险特征知识块的标签，更新已认证基础业务会话大数据中的已认证异常交互事件的分布情况、已认证异常交互事件中的某一节点的分布情况，对已认证基础业务会话大数据中的已认证异常交互事件的欺诈倾向进行一定程度的更新等。

[0094] 进一步地，对已认证基础业务会话大数据进行多轮存在差异的特征强化操作的操作为：对于已认证基础业务会话大数据，对其进行以上的至少一种特征强化操作，获得操作后的已认证基础业务会话大数据，将该操作后的已认证基础业务会话大数据视为已认证基础业务会话大数据对应的一组已认证目标业务会话大数据。然后，可以再次对已认证基础业务会话大数据进行以上的至少一种特征强化操作，获得已认证基础业务会话大数据对应的新的一组已认证目标业务会话大数据。每个已认证目标业务会话大数据可以为立刻根据已认证基础业务会话大数据确定的。

[0095] 已认证基础业务会话大数据对应的已认证目标业务会话大数据的先验注释与已认证基础业务会话大数据对应的先验注释一致。每个已认证目标业务会话大数据之间不同，且与已认证基础业务会话大数据不同，举例而言，每个已认证目标业务会话大数据中的已认证异常交互事件对应的已认证欺诈倾向描述向量不同，且与已认证基础业务会话大数据中的已认证异常交互事件对应的已认证欺诈倾向描述向量不同。每个已认证目标业务会话大数据可以为立刻根据已认证基础业务会话大数据确定的。

[0096] 对于同一个已认证基础业务会话大数据对应的已认证目标业务会话大数据的数目，可以根据调试指标进行灵活配置，比如，同一个已认证基础业务会话大数据对应的已认证目标业务会话大数据的数目可以为6个、7个、8个等。已认证基础业务会话大数据与其对

应的各个已认证目标业务会话大数据可以生成一个在线业务会话大数据集,将该在线业务会话大数据集视为一个已认证在线业务会话大数据簇。

[0097] 在实际实施过程中,对于思路M,可以先获得多个已认证基础业务会话大数据,对于每个已认证基础业务会话大数据,可以对该已认证基础业务会话大数据分别进行多轮存在差异的特征强化操作,获得多个已认证目标业务会话大数据,然后,可以将该已认证基础业务会话大数据和其对应的多个已认证目标业务会话大数据视为一组已认证在线业务会话大数据所包含的多个已认证在线业务会话大数据。

[0098] 或者,已认证目标业务会话大数据也可以为对每轮获得的已认证目标业务会话大数据再次进行特征强化操作获得的。举例而言,可以先对获得的已认证基础业务会话大数据进行特征强化操作,获得该已认证基础业务会话大数据对应的已认证目标业务会话大数据,然后可以对该已认证目标业务会话大数据进行下一轮的特征强化操作,获得新的已认证目标业务会话大数据;进而可以对该新的已认证目标业务会话大数据进行下一轮的特征强化操作,获得另一个新的已认证目标业务会话大数据,逐一推算,可以获得多个已认证目标业务会话大数据。最后,可以将获得的多个已认证目标业务会话大数据和该已认证基础业务会话大数据视为一组已认证在线业务会话大数据所包含的多个已认证在线业务会话大数据。

[0099] 基于此,通过上述思路M,可以确定出多个已认证基础业务会话大数据中的每个已认证基础业务会话大数据对应的多个已认证目标业务会话大数据,进而获得多个已认证基础业务会话大数据中的每个已认证基础业务会话大数据对应的已认证在线业务会话大数据簇,一个已认证在线业务会话大数据簇便为一组已认证在线业务会话大数据,已认证在线业务会话大数据簇中的各个在线业务会话大数据均可以为用于对待调试的AI专家系统模型进行调试的已认证在线业务会话大数据。

[0100] 思路N、获得已认证异常交互事件对应的目标会话数据流;以及从目标会话数据流中确定若干组已认证在线业务会话大数据,其中,每组已认证在线业务会话大数据包括设定数目的在线业务会话信息,对应于相同已认证在线业务会话大数据簇的各个在线业务会话信息中的已认证异常交互事件对应的先验注释一致;且对应于相同已认证在线业务会话大数据簇的各个在线业务会话信息中的已认证异常交互事件对应的已认证欺诈倾向描述向量不同。

[0101] 对于本发明实施例而言,目标会话数据流可以为采集的已认证异常交互事件在任意周期的会话数据流,已认证异常交互事件在目标会话数据流中,可以对应有若干个对应于不同先验注释的欺诈倾向,对应于相同个先验注释的欺诈倾向可以对应一连串的在线业务会话信息,该连串中的每个在线业务会话信息中的已认证异常交互事件对应的已认证欺诈倾向描述向量存在欺诈倾向差异,该连串中的每个在线业务会话信息中的已认证异常交互事件对应的先验注释一致,该连串中的各个在线业务会话信息可以对应于一个已认证在线业务会话大数据簇,从而该连串中的各个在线业务会话信息都可以为用于对待调试的AI专家系统模型进行调试的已认证在线业务会话大数据。

[0102] 在实际实施过程中,可以先获得已认证异常交互事件对应的目标会话数据流,其次,对于已认证异常交互事件在目标会话数据流中匹配的对应于相同先验注释的欺诈倾向,可以根据设定的时序间隙,从该连串欺诈倾向对应的在线业务会话信息中确定设定数

目的在线业务会话信息，将确定的设定数目的在线业务会话信息视为一组已认证在线业务会话大数据。

[0103] 进而对于已认证异常交互事件在目标会话数据流中实施的对应于相同先验注释的每个欺诈倾向，如此，确定出该欺诈倾向对应的至少一组已认证在线业务会话大数据，然后，获得若干组已认证在线业务会话大数据。

[0104] 步骤302、对于每组已认证在线业务会话大数据，将该组已认证在线业务会话大数据加载到待调试的AI专家系统模型，通过所述待调试的AI专家系统模型对该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据进行处理，确定该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据分别对应的欺诈倾向分析数据。

[0105] 对于本发明实施例而言，一组已认证在线业务会话大数据便为一个已认证在线业务会话大数据簇，欺诈倾向分析数据与欺诈倾向预测向量相对应，欺诈倾向预测向量可以对应于完成调试的目标AI专家系统模型在对第二在线业务会话大数据进行欺诈倾向分析时，生成的欺诈倾向描述向量。举例而言，欺诈倾向分析数据可以为待调试的AI专家系统模型生成的、已认证在线业务会话大数据中的已认证异常交互事件对应的已认证欺诈倾向描述向量对应于各种设定的挖掘欺诈倾向的可能性矩阵。比如，对应于设定的挖掘欺诈倾向inclination_a的可能性为0.8，对应于设定的挖掘欺诈倾向inclination_b的可能性为0.15，对应于设定的挖掘欺诈倾向inclination_c的可能性为0.05。

[0106] 进而基于欺诈倾向分析数据，可以确定欺诈倾向预测向量。举例而言，可以将可能性矩阵中最大可能性值对应的设定的挖掘欺诈倾向视为欺诈倾向预测向量。

[0107] 在实际实施过程中，对于每组已认证在线业务会话大数据，可以将该组已认证在线业务会话大数据加载到待调试的AI专家系统模型，通过所述待调试的AI专家系统模型对该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据分别进行处理，获得每个已认证在线业务会话大数据分别对应的欺诈倾向分析数据。基于此，可以获得每组已认证在线业务会话大数据中的每个已认证在线业务会话大数据分别对应的欺诈倾向分析数据。

[0108] 步骤303、依据每两个已认证在线业务会话大数据对应的欺诈倾向分析数据，确定欺诈倾向挖掘代价。

[0109] 对于本发明实施例而言，欺诈倾向挖掘代价能够反映两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差，从而，可以反映待调试的AI专家系统模型在对先验注释一致、但其中的已认证异常交互事件对应的已认证欺诈倾向描述向量存在一定的差别的两个已认证在线业务会话大数据，进行欺诈倾向分析时的评估代价。

[0110] 在实际实施过程中，对于每组已认证在线业务会话大数据，可以根据该已认证在线业务会话大数据簇中的每两个已认证在线业务会话大数据对应的欺诈倾向分析数据，确定出这两个已认证在线业务会话大数据对应的欺诈倾向分析数据之间的欺诈倾向挖掘误差，其次，可以根据该已认证在线业务会话大数据簇中的每两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差，确定该已认证在线业务会话大数据簇对应的欺诈倾向挖掘代价；并且，在获得欺诈倾向挖掘代价之后，还可以对该欺诈倾向挖掘代价进行min化处理，将处理后获得的min化的欺诈倾向挖掘代价视为最后的欺诈倾向挖掘代价。

[0111] 步骤304、通过所述每组已认证在线业务会话大数据对应的欺诈倾向挖掘代价，对

待调试的AI专家系统模型进行循环调试，直到符合调试结束要求，获得调试好的AI专家系统模型。

[0112] 对于本发明实施例而言，调试结束要求可以包括对待调试的AI专家系统模型进行循环的次数满足设定次数和/或调试获得的AI专家系统模型的分析准确性符合目标准确度。

[0113] 在根据步骤303获得每组已认证在线业务会话大数据(每个已认证在线业务会话大数据簇)分别对应的欺诈倾向挖掘代价然后可以通过所述每组已认证在线业务会话大数据分别对应的欺诈倾向挖掘代价，分别对待调试的AI专家系统模型进行循环调试;或者，也可以先根据每组已认证在线业务会话大数据分别对应的欺诈倾向挖掘代价，确定待调试的AI专家系统模型对应的全局欺诈倾向挖掘代价，再通过所述该全局欺诈倾向挖掘代价对待调试的AI专家系统模型进行循环调试。

[0114] 在确定符合调试结束要求的基础上，将调试获得的AI专家系统模型视为完成调试的AI专家系统模型。如此，通过所述可以反映AI专家系统模型在对存在相同先验注释的不同已认证在线业务会话大数据进行分析时所生成的欺诈倾向分析数据之间差别的欺诈倾向挖掘代价，对AI专家系统模型进行调试，可以显著减少已认证在线业务会话大数据中的已认证异常交互事件之间的欺诈倾向差异对AI专家系统模型的分析精度和可信度的干扰，从而保证调试好的AI专家系统模型的分析准确性。

[0115] 对于一些可能的设计思路而言，对于步骤303，可以通过如下方式实施，进一步地可以包括步骤3031-步骤3034。

[0116] 步骤3031、依据每两个已认证在线业务会话大数据对应的欺诈倾向分析数据，确定每两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差。

[0117] 对于本发明实施例而言，对于同一组已认证在线业务会话大数据中的每两个已认证在线业务会话大数据，可以对该两个已认证在线业务会话大数据对应的欺诈倾向分析数据进行设定运算(比如:进行差值运算)，将该运算结果视为该两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差。

[0118] 步骤3032、依据每两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差，确定每两个已认证在线业务会话大数据对应的交叉熵模型代价。

[0119] 对于本发明实施例而言，交叉熵模型代价可以为根据欺诈倾向挖掘误差对应的绝对值确定的。

[0120] 在实际实施过程中，对于同一组已认证在线业务会话大数据中的每两个已认证在线业务会话大数据，可以根据确定的该两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差，确定该两个已认证在线业务会话大数据对应的交叉熵模型代价。

[0121] 步骤3033、依据每两个已认证在线业务会话大数据对应的交叉熵模型代价，确定第一模型代价指标。

[0122] 对于本发明实施例而言，第一评估代价可以反映任意两个已认证在线业务会话大数据对应的欺诈倾向挖掘误差。

[0123] 对于同一组已认证在线业务会话大数据，可以先根据该组已认证在线业务会话大数据对应的欺诈倾向挖掘误差的数目，确定该组已认证在线业务会话大数据对应的全局处理结果，然后对该组已认证在线业务会话大数据中的每两个已认证在线业务会话大数据对

应的交叉熵模型代价进行累计处理，在通过所述全局处理结果对累计处理获得的结果进行全局操作，将全局操作后的结果视为该组已认证在线业务会话大数据对应的第一模型代价指标。

[0124] 步骤3034、利用每组已认证在线业务会话大数据对应的第一模型代价指标，确定欺诈倾向挖掘代价。

[0125] 对于本发明实施例而言，对于每组已认证在线业务会话大数据，可以直接将该组已认证在线业务会话大数据对应的第一模型代价指标，视为该组已认证在线业务会话大数据对应的欺诈倾向挖掘代价。

[0126] 对于一些可能的设计思路而言，对于步骤3034，通过如下方式实施，具体可以包括步骤30341和步骤30342。

[0127] 步骤30341、基于每个已认证在线业务会话大数据对应的欺诈倾向分析数据和每个已认证在线业务会话大数据对应的欺诈倾向参考，确定第二模型代价指标。

[0128] 对于本发明实施例而言，每个已认证在线业务会话大数据对应的欺诈倾向参考可以为每个已认证在线业务会话大数据对应的先验注释。第二模型代价指标可以为待调试的AI专家系统模型生成的欺诈倾向分析数据和欺诈倾向参考之间的代价。

[0129] 在实际实施过程中，对于每组已认证在线业务会话大数据中的每个已认证在线业务会话大数据，可以通过所述该组已认证在线业务会话大数据对应的欺诈倾向分析数据和该组已认证在线业务会话大数据对应的欺诈倾向参考，确定该组已认证在线业务会话大数据对应的评估代价，其次，可以根据该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据对应的评估代价，确定该组已认证在线业务会话大数据对应的第二模型代价指标。比如，对该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据对应的评估代价进行全局操作，将全局操作后获得的代价视为该组已认证在线业务会话大数据对应的第二模型代价指标。

[0130] 可以理解的是，根据步骤30341，可以确定每组已认证在线业务会话大数据对应的第二模型代价指标。

[0131] 对于另一些可能的设计思路而言，对于每组已认证在线业务会话大数据中的每个已认证在线业务会话大数据，可以通过所述该组已认证在线业务会话大数据对应的欺诈倾向分析数据和该组已认证在线业务会话大数据对应的欺诈倾向参考，确定该组已认证在线业务会话大数据对应的铰链代价。然后，可以根据该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据对应的铰链代价，确定该组已认证在线业务会话大数据对应的第二模型代价指标。

[0132] 或者，还可以根据该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据对应的铰链代价(hinge loss)，确定该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据对应的窗口化代价，进而可以根据该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据对应的窗口化代价(focal loss)，确定该组已认证在线业务会话大数据对应的第二模型代价指标。比如，可以将该组已认证在线业务会话大数据中的每个已认证在线业务会话大数据对应的窗口化代价的累计值视为该组已认证在线业务会话大数据对应的第二模型代价指标。

[0133] 步骤30342、利用每组已认证在线业务会话大数据对应的第一模型代价指标和第

二模型代价指标，确定欺诈倾向挖掘代价。

[0134] 在实际实施过程中，可以基于如下算法确定欺诈倾向挖掘代价：cost0＝q1*cost1+q2*cost2。

[0135] 其中，cost0表示欺诈倾向挖掘代价，q1表示第一设定全局处理结果，q2表示第二设定全局处理结果，cost1表示第一模型代价指标，cost2表示第二模型代价指标。

[0136] 在实际实施过程中，对于每组已认证在线业务会话大数据，可以结合上述内容，通过所述第一设定全局处理结果对该组已认证在线业务会话大数据对应的第一模型代价指标进行全局操作，获得第一全局操作结果；以及通过所述第二设定全局处理结果对该组已认证在线业务会话大数据对应的第二模型代价指标进行全局操作，获得第二全局操作结果；然后，可以对第一全局操作结果和第二全局操作结果进行累计处理，将累计处理获得的结果视为该组已认证在线业务会话大数据对应的欺诈倾向挖掘代价。

[0137] 进一步的，可以通过所述确定的每组已认证在线业务会话大数据对应的欺诈倾向挖掘代价分别对待调试的AI专家系统模型进行循环调试；也可以通过所述确定的每组已认证在线业务会话大数据对应的欺诈倾向挖掘代价，确定待调试的AI专家系统模型对应的一个整体的欺诈倾向挖掘代价，通过所述该整体的欺诈倾向挖掘代价对待调试的AI专家系统模型进行循环调试。

[0138] 在一些可独立的设计思路下，在获得所述目标异常交互事件对应的欺诈倾向描述向量之后，该方法还包括如下内容：基于所述欺诈倾向描述向量确定欺诈防护方案；激活所述欺诈防护方案。

[0139] 其中，可以根据在线业务终端的算力进行欺诈防护方案的适应性激活，如果在线业务终端的算力较大，能够负载欺诈防护方案，则可以在在线业务终端侧部署欺诈防护方案，如果在线业务终端的算力较小，可以在大数据安防服务器侧部署欺诈防护方案以实现间接性地安全监测。

[0140] 在一些可独立的设计思路下，基于所述欺诈倾向描述向量确定欺诈防护方案，可以包括如下内容：对欺诈倾向描述向量的第一入侵攻击细节短语簇进行攻击主题识别，得到所述第一入侵攻击细节短语簇对应的第一攻击主题字段簇；根据所述第一攻击主题字段簇进行趋势分析，得到完成趋势分析的第二攻击主题字段簇；对所述第二攻击主题字段簇进行欺诈防护配对，得到所述第二攻击主题字段簇对应的欺诈防护方案。

[0141] 举例而言，攻击主题识别可以确定出欺诈倾向描述向量的模拟攻击行为特征，也即第一攻击主题字段簇，然后通过前瞻性趋势分析，能够得到第二攻击主题字段簇，进而基于欺诈防护方案的配对处理，以快速准确地得到欺诈防护方案。

[0142] 在一些可独立的设计思路下，所述对欺诈倾向描述向量的第一入侵攻击细节短语簇进行攻击主题识别，得到所述第一入侵攻击细节短语簇对应的第一攻击主题字段簇，包括：对欺诈倾向描述向量的第一入侵攻击细节短语簇进行特征映射，得到所述第一入侵攻击细节短语簇对应的第一模拟攻击向量簇；对所述第一模拟攻击向量簇进行特征下采样，得到所述第一入侵攻击细节短语簇对应的第一攻击主题字段簇。

[0143] 在一些可独立的设计思路下，所述对所述第二攻击主题字段簇进行欺诈防护配对，得到所述第二攻击主题字段簇对应的欺诈防护方案，包括：对所述第二攻击主题字段簇进行欺诈防护配对，得到所述第二攻击主题字段簇对应的第二模拟攻击向量簇；对所述第

二模拟攻击向量簇进行基于关系型数据库的匹配处理，得到所述第二攻击主题字段簇对应的欺诈防护方案。

[0144] 在一些可独立的设计思路下，所述对所述第二攻击主题字段簇进行欺诈防护配对，得到所述第二攻击主题字段簇对应的第二模拟攻击向量簇，包括：采用深度学习网络对所述第二攻击主题字段簇进行迭代处理，得到所述第二攻击主题字段簇对应的第二模拟攻击向量簇。

[0145] 基于同样的发明构思，图2示出了本发明实施例提供的基于AI Knowledge Base的网络欺诈分析装置的模块框图，基于AI Knowledge Base的网络欺诈分析装置可以包括实施图1所示的相关方法步骤的大数据获取模块21，用于获得触发网络欺诈分析条件的第一在线业务会话大数据，所述第一在线业务会话大数据包含目标异常交互事件；知识优化模块22，用于结合所述第一在线业务会话大数据中的至少部分风险特征知识块的专家决策评分，获得已优化决策评分，并结合所述已优化决策评分对所述第一在线业务会话大数据进行风险特征知识优化操作，获得完成优化的第二在线业务会话大数据，所述第二在线业务会话大数据的特征关系网尺度符合设定要求；欺诈分析模块23，用于对所述第二在线业务会话大数据进行欺诈倾向分析，获得所述目标异常交互事件对应的欺诈倾向描述向量。

[0146] 以上所述，仅为本发明的具体实施方式。熟悉本技术领域的技术人员根据本发明提供的具体实施方式，可想到变化或替换，都应涵盖在本发明的保护范围之内。

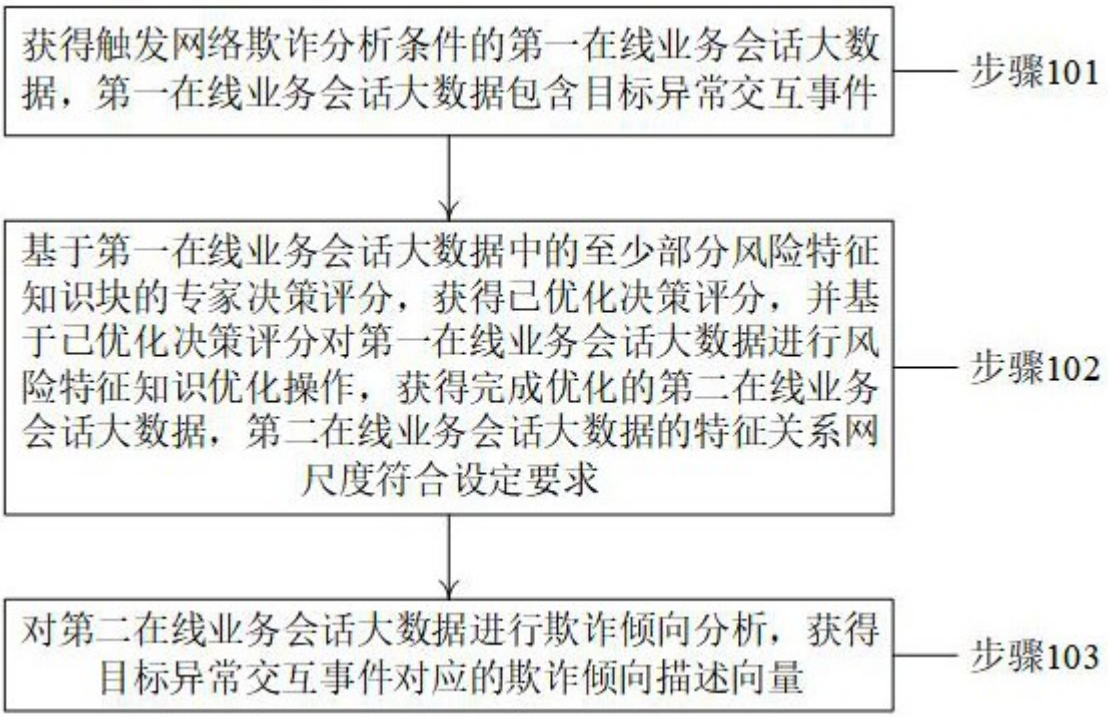

获得触发网络欺诈分析条件的第一在线业务会话大数据，第一在线业务会话大数据包含目标异常交互事件
步骤101
基于第一在线业务会话大数据中的至少部分风险特征知识块的专家决策评分，获得已优化决策评分，并基于已优化决策评分对第一在线业务会话大数据进行风险特征知识优化操作，获得完成优化的第二在线业务会话大数据，第二在线业务会话大数据的特征关系网尺度符合设定要求
步骤102
对第二在线业务会话大数据进行欺诈倾向分析，获得目标异常交互事件对应的欺诈倾向描述向量
步骤103

图1


大数据获取模块21
知识优化模块22
欺诈分析模块23

图2