(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 116384370 B
(45)授权公告日 2024.10.22

(21)申请号 202310371622.4

(22)申请日 2023.04.10

(65)同一申请的已公布的文献号
申请公布号 CN 116384370 A

(43)申请公布日 2023.07.04

(73)专利权人 沈鹏
地址 755000 宁夏回族自治区中卫市沙坡头区文昌南街159号

(72)发明人 沈鹏

(51)Int.Cl.
G06F 40/205(2020.01)
G06F 16/35(2019.01)
G06F 18/2433(2023.01)
G06F 18/24(2023.01)
G06N 3/0455(2023.01)

(56)对比文件
CN 115174231 A,2022.10.11
US 2019266325 A1,2019.08.29

审查员 谢萍

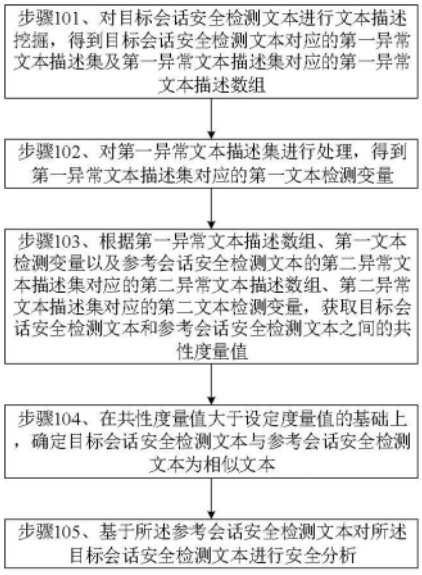
权利要求书3页 说明书19页 附图1页

(54)发明名称

一种用于在线业务会话交互的大数据安全分析方法及系统

(57)摘要

本发明提供一种用于在线业务会话交互的大数据安全分析方法及系统,在获取目标会话安全检测文本和参考会话安全检测文本的共性度量值时,还引入了异常文本描述集的检测偏移指数对共性度量值的贡献,而不是只分析异常文本描述集对应的异常文本描述数组,从而规避由于会话安全检测文本中存在扰动造成异常文本描述数组难以精准输出风险主题的词向量的问题,以便提高风险主题判别的精度,减少文本分析时所产生的偏差。在确定出目标会话安全检测文本与参考会话安全检测文本为相似文本之后,能够以参考会话安全检测文本的相关安全分析策略为基准,对目标会话安全检测文本进行一系列的安全分析,从而提高目标会话安全检测文本的安全分析精度和效率。



CN 116384370 B

1.一种用于在线业务会话交互的大数据安全分析方法,其特征在于,应用于人工智能服务系统,所述方法包括:

对目标会话安全检测文本进行文本描述挖掘,得到所述目标会话安全检测文本对应的第一异常文本描述集及所述第一异常文本描述集对应的第一异常文本描述数组;

对所述第一异常文本描述集进行处理,得到所述第一异常文本描述集对应的第一文本检测变量,所述第一文本检测变量用于表征所述第一异常文本描述集反映所述目标会话安全检测文本中风险主题词向量的检测偏移指数;

依据所述第一异常文本描述数组、所述第一文本检测变量以及参考会话安全检测文本的第二异常文本描述集对应的第二异常文本描述数组、所述第二异常文本描述集对应的第二文本检测变量,获取所述目标会话安全检测文本和所述参考会话安全检测文本之间的共性度量值,所述第二文本检测变量用于表征所述第二异常文本描述集反映所述参考会话安全检测文本中风险主题词向量的检测偏移指数;

在所述共性度量值大于设定度量值的基础上,确定所述目标会话安全检测文本与所述参考会话安全检测文本为相似文本,并基于所述参考会话安全检测文本对所述目标会话安全检测文本进行安全分析;

所述基于所述参考会话安全检测文本对所述目标会话安全检测文本进行安全分析的步骤,包括:

将所述目标会话安全检测文本传入至所述参考会话安全检测文本对应的决策树模型中,得到所述决策树模型生成的针对所述目标会话安全检测文本的会话文本分块池,所述会话文本分块池包括不少于两个会话文本分块;

获得所述会话文本分块池中的各个会话文本分块相对于所述目标会话安全检测文本的贡献权重;

根据所述各个会话文本分块对应的贡献权重,以及所述各个会话文本分块的异常决策向量,对所述各个会话文本分块进行文本分块整理,得到相应的会话文本分块队列;

基于所述会话文本分块队列确定关于所述目标会话安全检测文本的安全分析决策结果集,所述安全分析决策结果集包括至少两个异常事件概率;

利用所述异常事件概率,从所述目标会话安全检测文本中确定出异常事件文本块。

2.根据权利要求1所述的方法,其特征在于,所述对目标会话安全检测文本进行文本描述挖掘,得到所述目标会话安全检测文本对应的第一异常文本描述集及所述第一异常文本描述集对应的第一异常文本描述数组,包括:

通过Transformer网络中的文本描述挖掘子网,对目标会话安全检测文本进行文本描述挖掘,得到所述目标会话安全检测文本对应的第一异常文本描述集及所述第一异常文本描述集对应的第一异常文本描述数组。

3.根据权利要求2所述的方法,其特征在于,所述对所述第一异常文本描述集进行处理,得到所述第一异常文本描述集对应的第一文本检测变量,包括:

通过所述Transformer网络中的描述特征解析子网,对所述第一异常文本描述集进行处理,得到所述第一异常文本描述集对应的第一文本检测变量。

4.根据权利要求2所述的方法,其特征在于,所述文本描述挖掘子网包括文本描述挖掘单元和文本描述投影单元,所述通过Transformer网络中的文本描述挖掘子网,对目标会话

安全检测文本进行文本描述挖掘,得到所述目标会话安全检测文本对应的第一异常文本描述集及所述第一异常文本描述集对应的第一异常文本描述数组,包括:

通过所述文本描述挖掘单元,对所述目标会话安全检测文本进行文本描述挖掘,得到所述目标会话安全检测文本对应的第一异常文本描述集;

通过所述文本描述投影单元,对所述第一异常文本描述集进行文本描述投影,得到所述第一异常文本描述集对应的第一异常文本描述数组。

5.根据权利要求3所述的方法,其特征在于,所述通过所述Transformer网络中的描述特征解析子网,对所述第一异常文本描述集进行处理,得到所述第一异常文本描述集对应的第一文本检测变量之前,所述方法还包括:

根据会话安全检测文本样例和所述会话安全检测文本样例对应的异常文本描述数组样例,调校所述文本描述挖掘子网;

在维持调校后的文本描述挖掘子网不变的基础上,依据所述异常文本描述数组样例和所述会话安全检测文本样例所对应风险主题标签的关键文本描述数组,调校所述描述特征解析子网;

其中,所述根据会话安全检测文本样例和所述会话安全检测文本样例对应的异常文本描述数组样例,调校所述文本描述挖掘子网,包括:

获取所述会话安全检测文本样例和所述会话安全检测文本样例对应的异常文本描述数组样例;

通过所述文本描述挖掘子网,对所述会话安全检测文本样例进行文本描述挖掘,得到所述会话安全检测文本样例对应的异常文本解析描述集及所述异常文本解析描述集对应的异常文本解析数组;

依据所述异常文本解析数组和所述异常文本描述数组样例之间的比较结果,调校所述文本描述挖掘子网;

其中,所述文本描述挖掘子网包括文本描述挖掘单元和文本描述投影单元,所述通过所述文本描述挖掘子网,对所述会话安全检测文本样例进行文本描述挖掘,得到所述会话安全检测文本样例对应的异常文本解析描述集及所述异常文本解析描述集对应的异常文本解析数组,包括:通过所述文本描述挖掘单元,对所述会话安全检测文本样例进行文本描述挖掘,得到所述会话安全检测文本样例对应的异常文本解析描述集;通过所述文本描述投影单元,对所述异常文本解析描述集进行文本描述投影,得到所述异常文本解析描述集对应的异常文本解析数组;

其中,所述Transformer网络还包括网络代价生成子网,所述网络代价生成子网包括每个风险主题标签对应的置信度描述数组,所述依据所述异常文本解析数组和所述异常文本描述数组样例之间的比较结果,调校所述文本描述挖掘子网,包括:通过所述网络代价生成子网,按照所述会话安全检测文本样例所对应风险主题标签对应的置信度描述数组对所述异常文本解析数组进行强化操作,得到所述异常文本解析数组对应的异常文本描述强化数组;获取所述异常文本描述强化数组和所述异常文本描述数组样例之间的第二调校代价指标,所述第二调校代价指标表示所述异常文本描述强化数组和所述异常文本描述数组样例之间的比较结果;依据所述第二调校代价指标,调校所述文本描述挖掘子网和所述网络代价生成子网;

其中,所述在维持调校后的文本描述挖掘子网不变的基础上,依据所述异常文本描述数组样例和所述会话安全检测文本样例所对应风险主题标签的关键文本描述数组,调校所述描述特征解析子网,包括:获取所述会话安全检测文本样例所对应风险主题标签的关键文本描述数组,所述关键文本描述数组表示所述风险主题标签对应的风险主题词向量;通过所述描述特征解析子网,对所述异常文本解析描述集进行处理,得到所述异常文本解析描述集对应的文本检测变量解析结果,所述文本检测变量解析结果用于表征所述异常文本解析描述集反映所述会话安全检测文本样例中风险主题词向量的检测偏移指数;依据所述异常文本解析数组、所述关键文本描述数组和所述文本检测变量解析结果,获取第三调校代价指标,所述第三调校代价指标表示所述异常文本解析描述集对应的文本检测变量解析结果的训练代价;依据所述第三调校代价指标,调校所述描述特征解析子网。

6.根据权利要求5所述的方法,其特征在于,所述依据所述异常文本解析数组、所述关键文本描述数组和所述文本检测变量解析结果,获取第三调校代价指标,包括:

依据所述异常文本解析数组和所述关键文本描述数组之间的差异特征,获取目标文本检测变量;

依据所述目标文本检测变量和所述文本检测变量解析结果之间的比较结果,获取所述第三调校代价指标。

7.根据权利要求5所述的方法,其特征在于,所述获取所述会话安全检测文本样例所对应风险主题标签的关键文本描述数组,包括:

获取所述会话安全检测文本样例所对应风险主题标签的多个会话安全检测文本对应的异常文本描述数组;

根据获取到的多个异常文本描述数组,确定所述关键文本描述数组。

8.根据权利要求5所述的方法,其特征在于,所述获取所述会话安全检测文本样例所对应风险主题标签的关键文本描述数组,包括:

获取所述会话安全检测文本样例所对应风险主题标签对应的置信度描述数组;

将所述会话安全检测文本样例对应的置信度描述数组确定为所述关键文本描述数组。

9.一种人工智能服务系统,其特征在于,包括:存储器和处理器;所述存储器和所述处理器耦合;所述存储器用于存储计算机程序代码,所述计算机程序代码包括计算机指令;其中,当所述处理器执行所述计算机指令时,使得所述人工智能服务系统执行如权利要求1-8中任意一项所述的方法。

10.一种计算机可读存储介质,其特征在于,其上存储有计算机程序,所述计算机程序在运行时如权利要求1-8中任意一项所述的方法。

一种用于在线业务会话交互的大数据安全分析方法及系统

技术领域

[0001] 本发明涉及大数据安全技术领域,尤其涉及一种用于在线业务会话交互的大数据安全分析方法及系统。

背景技术

[0002] 大数据时代来临,各行业数据规模呈TB级增长,高价值数据源在大数据产业链中占据至关重要的核心地位。随着各行业的线上业务升级,业务交互大多通过在线会话实现,由此所产生的会话大数据的信息量也不容忽视,如何确保会话大数据安全性是现目前亟需重视的问题。传统的数据安全分析技术大多通过对检测文本进行分析实现,但是这种方式存在效率和精度低下的问题。

发明内容

[0003] 本发明提供一种用于在线业务会话交互的大数据安全分析方法及系统,为实现上述技术目的,本发明采用如下技术方案。

[0004] 第一方面是一种用于在线业务会话交互的大数据安全分析方法,应用于人工智能服务系统,所述方法包括:

[0005] 对目标会话安全检测文本进行文本描述挖掘,得到所述目标会话安全检测文本对应的第一异常文本描述集及所述第一异常文本描述集对应的第一异常文本描述数组;

[0006] 对所述第一异常文本描述集进行处理,得到所述第一异常文本描述集对应的第一文本检测变量,所述第一文本检测变量用于表征所述第一异常文本描述集反映所述目标会话安全检测文本中风险主题词向量的检测偏移指数;

[0007] 依据所述第一异常文本描述数组、所述第一文本检测变量以及参考会话安全检测文本的第二异常文本描述集对应的第二异常文本描述数组、所述第二异常文本描述集对应的第二文本检测变量,获取所述目标会话安全检测文本和所述参考会话安全检测文本之间的共性度量值,所述第二文本检测变量用于表征所述第二异常文本描述集反映所述参考会话安全检测文本中风险主题词向量的检测偏移指数;

[0008] 在所述共性度量值大于设定度量值的基础上,确定所述目标会话安全检测文本与所述参考会话安全检测文本为相似文本,并基于所述参考会话安全检测文本对所述目标会话安全检测文本进行安全分析。

[0009] 在一些可选的实施例中,所述对目标会话安全检测文本进行文本描述挖掘,得到所述目标会话安全检测文本对应的第一异常文本描述集及所述第一异常文本描述集对应的第一异常文本描述数组,包括:

[0010] 通过Transformer网络中的文本描述挖掘子网,对目标会话安全检测文本进行文本描述挖掘,得到所述目标会话安全检测文本对应的第一异常文本描述集及所述第一异常文本描述集对应的第一异常文本描述数组。

[0011] 在一些可选的实施例中,所述对所述第一异常文本描述集进行处理,得到所述第

一异常文本描述集对应的第一文本检测变量,包括:

[0012] 通过所述Transformer网络中的描述特征解析子网,对所述第一异常文本描述集进行处理,得到所述第一异常文本描述集对应的第一文本检测变量。

[0013] 在一些可选的实施例中,所述文本描述挖掘子网包括文本描述挖掘单元和文本描述投影单元,所述通过Transformer网络中的文本描述挖掘子网,对目标会话安全检测文本进行文本描述挖掘,得到所述目标会话安全检测文本对应的第一异常文本描述集及所述第一异常文本描述集对应的第一异常文本描述数组,包括:

[0014] 通过所述文本描述挖掘单元,对所述目标会话安全检测文本进行文本描述挖掘,得到所述目标会话安全检测文本对应的第一异常文本描述集;

[0015] 通过所述文本描述投影单元,对所述第一异常文本描述集进行文本描述投影,得到所述第一异常文本描述集对应的第一异常文本描述数组。

[0016] 在一些可选的实施例中,所述通过所述Transformer网络中的描述特征解析子网,对所述第一异常文本描述集进行处理,得到所述第一异常文本描述集对应的第一文本检测变量之前,所述方法还包括:

[0017] 根据会话安全检测文本样例和所述会话安全检测文本样例对应的异常文本描述数组样例,调校所述文本描述挖掘子网;

[0018] 在维持调校后的文本描述挖掘子网不变的基础上,依据所述异常文本描述数组样例和所述会话安全检测文本样例所对应风险主题标签的关键文本描述数组,调校所述描述特征解析子网。

[0019] 在一些可选的实施例中,所述根据会话安全检测文本样例和所述会话安全检测文本样例对应的异常文本描述数组样例,调校所述文本描述挖掘子网,包括:

[0020] 获取所述会话安全检测文本样例和所述会话安全检测文本样例对应的异常文本描述数组样例;

[0021] 通过所述文本描述挖掘子网,对所述会话安全检测文本样例进行文本描述挖掘,得到所述会话安全检测文本样例对应的异常文本解析描述集及所述异常文本解析描述集对应的异常文本解析数组;

[0022] 依据所述异常文本解析数组和所述异常文本描述数组样例之间的比较结果,调校所述文本描述挖掘子网。

[0023] 在一些可选的实施例中,所述文本描述挖掘子网包括文本描述挖掘单元和文本描述投影单元,所述通过所述文本描述挖掘子网,对所述会话安全检测文本样例进行文本描述挖掘,得到所述会话安全检测文本样例对应的异常文本解析描述集及所述异常文本解析描述集对应的异常文本解析数组,包括:

[0024] 通过所述文本描述挖掘单元,对所述会话安全检测文本样例进行文本描述挖掘,得到所述会话安全检测文本样例对应的异常文本解析描述集;

[0025] 通过所述文本描述投影单元,对所述异常文本解析描述集进行文本描述投影,得到所述异常文本解析描述集对应的异常文本解析数组。

[0026] 在一些可选的实施例中,所述Transformer网络还包括网络代价生成子网,所述网络代价生成子网包括每个风险主题标签对应的置信度描述数组,所述依据所述异常文本解析数组和所述异常文本描述数组样例之间的比较结果,调校所述文本描述挖掘子网,包括:

[0027] 通过所述网络代价生成子网,按照所述会话安全检测文本样例所对应风险主题标签对应的置信度描述数组对所述异常文本解析数组进行强化操作,得到所述异常文本解析数组对应的异常文本描述强化数组;

[0028] 获取所述异常文本描述强化数组和所述异常文本描述数组样例之间的第二调校代价指标,所述第二调校代价指标表示所述异常文本描述强化数组和所述异常文本描述数组样例之间的比较结果;

[0029] 依据所述第二调校代价指标,调校所述文本描述挖掘子网和所述网络代价生成子网。

[0030] 在一些可选的实施例中,所述在维持调校后的文本描述挖掘子网不变的基础上,依据所述异常文本描述数组样例和所述会话安全检测文本样例所对应风险主题标签的关键文本描述数组,调校所述描述特征解析子网,包括:

[0031] 获取所述会话安全检测文本样例所对应风险主题标签的关键文本描述数组,所述关键文本描述数组表示所述风险主题标签对应的风险主题词向量;

[0032] 通过所述描述特征解析子网,对所述异常文本解析描述集进行处理,得到所述异常文本解析描述集对应的文本检测变量解析结果,所述文本检测变量解析结果用于表征所述异常文本解析描述集反映所述会话安全检测文本样例中风险主题词向量的检测偏移指数;

[0033] 依据所述异常文本解析数组、所述关键文本描述数组和所述文本检测变量解析结果,获取第三调校代价指标,所述第三调校代价指标表示所述异常文本解析描述集对应的文本检测变量解析结果的训练代价;

[0034] 依据所述第三调校代价指标,调校所述描述特征解析子网。

[0035] 在一些可选的实施例中,所述依据所述异常文本解析数组、所述关键文本描述数组和所述文本检测变量解析结果,获取第三调校代价指标,包括:

[0036] 依据所述异常文本解析数组和所述关键文本描述数组之间的差异特征,获取目标文本检测变量;

[0037] 依据所述目标文本检测变量和所述文本检测变量解析结果之间的比较结果,获取所述第三调校代价指标。

[0038] 在一些可选的实施例中,所述获取所述会话安全检测文本样例所对应风险主题标签的关键文本描述数组,包括:

[0039] 获取所述会话安全检测文本样例所对应风险主题标签的多个会话安全检测文本对应的异常文本描述数组;

[0040] 根据获取到的多个异常文本描述数组,确定所述关键文本描述数组。

[0041] 在一些可选的实施例中,所述获取所述会话安全检测文本样例所对应风险主题标签的关键文本描述数组,包括:

[0042] 获取所述会话安全检测文本样例所对应风险主题标签对应的置信度描述数组;

[0043] 将所述会话安全检测文本样例对应的置信度描述数组确定为所述关键文本描述数组。

[0044] 第二方面是一种人工智能服务系统,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,使得所述人工智能服务系统执行第一方面的方法。

[0045] 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。

[0046] 本发明实施例提供的技术方案,获取目标会话安全检测文本对应的第一异常文本描述集以及第一异常文本描述集对应的第一异常文本描述数组和第一文本检测变量,根据第一异常文本描述数组、第一文本检测变量以及参考会话安全检测文本的第二异常文本描述集对应的第二异常文本描述数组和第二文本检测变量,获取目标会话安全检测文本和参考会话安全检测文本之间的共性度量值,在共性度量值大于设定度量值的基础上确定目标会话安全检测文本与参考会话安全检测文本为相似文本。鉴于第一文本检测变量表示第一异常文本描述集反映目标会话安全检测文本中风险主题词向量的检测偏移指数,第二文本检测变量表示第二异常文本描述集反映参考会话安全检测文本中风险主题词向量的检测偏移指数,这样在获取目标会话安全检测文本和参考会话安全检测文本的共性度量值时,还引入了异常文本描述集的检测偏移指数对共性度量值的贡献,而不是只分析异常文本描述集对应的异常文本描述数组,从而规避由于会话安全检测文本中存在扰动造成异常文本描述数组难以精准输出风险主题的词向量的问题,以便提高风险主题判别的精度,减少文本分析时所产生的偏差。在确定出目标会话安全检测文本与参考会话安全检测文本为相似文本之后,能够以参考会话安全检测文本的相关安全分析策略为基准,对目标会话安全检测文本进行一系列的安全分析,从而提高目标会话安全检测文本的安全分析精度和效率。

[0047] 此外,本发明实施例中,将目标会话安全检测文本的文本描述投影到文本场景向量关系网中,得到该目标会话安全检测文本对应的第一异常文本描述集。鉴于相较于传统的文本向量关系网,文本场景向量关系网更匹配风险主题的向量关系网,这样在文本场景向量关系网中对风险主题进行文本描述挖掘可以使提取到的风险主题词向量尽可能精准和完整,以保障风险主题分析的精度和可信度。

[0048] 此外,获取会话安全检测文本样例和会话安全检测文本样例对应的异常文本描述数组样例,通过文本描述挖掘子网提取会话安全检测文本样例的异常文本解析描述集和异常文本解析数组,根据异常文本解析数组和异常文本描述数组样例之间的比较结果,调校文本描述挖掘子网。获取会话安全检测文本样例所对应风险主题标签的关键文本描述数组,通过描述特征解析子网获取异常文本解析描述集对应的文本检测变量解析结果,根据异常文本解析数组、关键文本描述数组和文本检测变量解析结果获取第三调校代价指标,根据第三调校代价指标调校描述特征解析子网。之后便能够通过包括该文本描述挖掘子网和描述特征解析子网的Transformer网络进行风险主题解析,鉴于引入描述特征解析子网,这样在获取目标会话安全检测文本和参考会话安全检测文本之间的共性度量值时,还引入了描述特征解析子网生成的文本检测变量对共性度量值的贡献,也即是引入了异常文本描述集的检测偏移指数对共性度量值的贡献,而不是只分析异常文本描述集对应的异常文本描述数组,从而规避由于会话安全检测文本中存在扰动造成异常文本描述数组难以精准输出风险主题的词向量的问题,以便提高风险主题判别的精度,减少文本分析时所产生的偏差。

[0049] 此外,根据会话安全检测文本样例和会话安全检测文本样例对应的异常文本描述

数组样例,调校文本描述挖掘子网,在维持调校后的文本描述挖掘子网不变的基础上,根据异常文本描述数组样例和会话安全检测文本样例所对应风险主题标签的关键文本描述数组,调校描述特征解析子网。以此对Transformer网络的调校过程可以分为文本描述挖掘子网的调校环节和描述特征解析子网的调校环节,则在文本描述挖掘子网调校好的基础上,仅需获取调校该文本描述挖掘子网的会话安全检测文本样例,对描述特征解析子网进行调校便可,不用再次调校新的文本描述挖掘子网,也不用再次获取会话安全检测文本样例。

附图说明

[0050] 图1为本发明实施例提供的用于在线业务会话交互的大数据安全分析方法的流程示意图。

具体实施方式

[0051] 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。

[0052] 图1示出了本发明实施例提供的用于在线业务会话交互的大数据安全分析方法的流程示意图,用于在线业务会话交互的大数据安全分析方法可以通过人工智能服务系统实现,人工智能服务系统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,使得所述人工智能服务系统执行步骤101-步骤105。

[0053] 步骤101、对目标会话安全检测文本进行文本描述挖掘,得到目标会话安全检测文本对应的第一异常文本描述集及第一异常文本描述集对应的第一异常文本描述数组。

[0054] 人工智能服务系统获取到目标会话安全检测文本时,对该目标会话安全检测文本进行文本描述挖掘,得到该目标会话安全检测文本对应的第一异常文本描述集,以及该第一异常文本描述集对应的第一异常文本描述数组。

[0055] 其中,第一异常文本描述集为表示目标会话安全检测文本的文本特征的记录,比如会话安全检测文本的文本特征可以包括会话安全检测文本的检测规则文本特征、会话行为文本特征、潜在风险文本特征等。第一异常文本描述数组为表示目标会话安全检测文本的文本特征的线性字段,比如该第一异常文本描述数组可以为多维度的线性字段。在人工智能领域,本领域技术人员可知晓,文本特征可以通过特征向量、描述数组、线性字段等作为载体来记载。

[0056] 步骤102、对第一异常文本描述集进行处理,得到第一异常文本描述集对应的第一文本检测变量。

[0057] 当人工智能服务系统获取到目标会话安全检测文本对应的第一异常文本描述集,对该第一异常文本描述集进行处理,得到该第一异常文本描述集对应的第一文本检测变量。其中,第一文本检测变量用于表征第一异常文本描述集反映目标会话安全检测文本中风险主题词向量的检测偏移指数。

[0058] 检测偏移指数可以理解为在处理过程中由于存在偏差,对得到的结果的质疑程度,可以反映第一异常文本描述集能精准表征风险主题词向量的可能性,因此检测偏移指

数还可以理解为质疑系数或者不确定系数。进一步地,文本检测变量可以理解为特征变量,该第一文本检测变量越小,表示该第一异常文本描述集反映目标会话安全检测文本中风险主题词向量的精准性越佳,该第一文本检测变量越大,表示该第一异常文本描述集反映该目标会话安全检测文本中风险主题词向量的精准性越差。此外,风险主题词向量可以用于表征不同会话风险的类别特征,比如风险主题词向量1可以表征数据泄露风险、风险主题词向量2可以表征钓鱼陷阱、风险主题词向量3可以表征电信诈骗等。

[0059] 步骤103、根据第一异常文本描述数组、第一文本检测变量以及参考会话安全检测文本的第二异常文本描述集对应的第二异常文本描述数组、第二异常文本描述集对应的第二文本检测变量,获取目标会话安全检测文本和参考会话安全检测文本之间的共性度量值。

[0060] 本发明实施例的风险主题解析任务,为对目标会话安全检测文本和参考会话安全检测文本进行解析,以确定该目标会话安全检测文本是否与参考会话安全检测文本为相似文本,其中参考会话安全检测文本为事先记录的会话安全检测文本,目标会话安全检测文本为当前获取的、需要进行风险主题解析的文本数据。为了将目标会话安全检测文本与参考会话安全检测文本进行相似性分析,人工智能服务系统获取参考会话安全检测文本的第二异常文本描述集对应的第二异常文本描述数组以及该第二异常文本描述集对应的第二文本检测变量,根据第一异常文本描述数组、第一文本检测变量、第二异常文本描述数组和第二文本检测变量,获取目标会话安全检测文本和参考会话安全检测文本之间的共性度量值。

[0061] 其中,第二异常文本描述集为表示参考会话安全检测文本的文本特征的记录,第二异常文本描述数组为表示参考会话安全检测文本的文本特征的线性字段。第二文本检测变量用于表征第二异常文本描述集反映参考会话安全检测文本中风险主题词向量的检测偏移指数。

[0062] 其中,目标会话安全检测文本和参考会话安全检测文本之间的共性度量值越大,表示目标会话安全检测文本与参考会话安全检测文本为相似文本的可能性越高,目标会话安全检测文本和参考会话安全检测文本之间的共性度量值越小,表示目标会话安全检测文本与参考会话安全检测文本为相似文本的可能性越低。因此,共性度量值还可以理解为文本相似度。

[0063] 步骤104、在共性度量值大于设定度量值的基础上,确定目标会话安全检测文本与参考会话安全检测文本为相似文本。

[0064] 当人工智能服务系统获取到目标会话安全检测文本和参考会话安全检测文本之间的共性度量值,将该共性度量值与设定度量值进行比较,若共性度量值大于该设定度量值,则确定目标会话安全检测文本与参考会话安全检测文本为相似文本,则可以对目标会话安全检测文本进行间接、高效的安全分析。若共性度量值不大于该设定度量值,则确定目标会话安全检测文本与参考会话安全检测文本不是相似文本,此时可以继续将目标会话安全检测文本与下一个参考会话安全检测文本进行相似性分析,直到确定目标会话安全检测文本与某一参考会话安全检测文本为相似文本,则可以对目标会话安全检测文本进行间接、高效的安全分析,或者直至确定目标会话安全检测文本与记录的每个参考会话安全检测文本均不是相似文本,则直接对目标会话安全检测文本进行安全分析。其中,本领域技术

人员可以自行调整该设定度量值。

[0065] 步骤105、基于所述参考会话安全检测文本对所述目标会话安全检测文本进行安全分析。

[0066] 在本发明实施例中,可以将参考会话安全检测文本对应的参考安全分析策略沿用进行,比如可以通过参考安全分析策略对目标会话安全检测文本进行安全分析。示例性的,参考安全分析策略同样可以是神经网络模型,比如可以是决策树模型。在实际实施时,由于参考会话安全检测文本和目标会话安全检测文本是相似文本,因此将目标会话安全检测文本输入到决策树模型进行异常事件文本块的判别处理是合理的,这样一来,由于决策树模型之前已经投入使用,因而免去了对决策树模型的再次调试训练,又由于参考会话安全检测文本和目标会话安全检测文本是相似文本,因而决策树模型对目标会话安全检测文本的处理不会出现太大偏差,这样可以确保得到的异常事件文本块的精度和可信度。

[0067] 基于上述相关内容,在一些可独立的实施例中,步骤105中的基于所述参考会话安全检测文本对所述目标会话安全检测文本进行安全分析,包括步骤1051-步骤1054。

[0068] 步骤1051、将所述目标会话安全检测文本传入至所述参考会话安全检测文本对应的决策树模型中,得到所述决策树模型生成的针对所述目标会话安全检测文本的会话文本分块池,所述会话文本分块池包括不少于两个会话文本分块。

[0069] 步骤1052、获得所述会话文本分块池中的各个会话文本分块相对于所述目标会话安全检测文本的贡献权重。

[0070] 步骤1053、根据所述各个会话文本分块对应的贡献权重,以及所述各个会话文本分块的异常决策向量,对所述各个会话文本分块进行文本分块整理,得到相应的会话文本分块队列。

[0071] 步骤1054、基于所述会话文本分块队列确定关于所述目标会话安全检测文本的安全分析决策结果集,所述安全分析决策结果集包括至少两个异常事件概率。

[0072] 步骤1055、利用所述异常事件概率,从所述目标会话安全检测文本中确定出异常事件文本块。

[0073] 其中,贡献权重可以理解为会话文本分块相对于所述目标会话安全检测文本的相关度,异常事件概率用于指示对应会话文本分块为异常事件文本块的可能性,基于此,在确定异常事件文本块时,可以基于设定事件概率阈值实现,比如设定事件概率阈值为0.6,则将高于0.6的异常事件概率所对应的会话文本分块确定为异常事件文本块,以便针对这些异常事件文本块进行针对性的安全防护策略和风险应对策略的定制。可见,基于异常事件概率确定异常事件文本块,可以提高异常事件文本块确定的灵活性,在异常事件文本块确定标准较为严格时,可以将异常事件概率调低,在异常事件文本块确定标准较为宽松时,可以将异常事件概率调高。

[0074] 基于上述相关内容,在一些可独立的实施例中,所述根据所述各个会话文本分块对应的贡献权重,以及所述各个会话文本分块的异常决策向量,对所述各个会话文本分块进行文本分块整理,得到相应的会话文本分块队列,包括:根据所述各个会话文本分块对应的贡献权重,以及所述各个会话文本分块的异常决策向量,对所述各个会话文本分块进行拆解,得到至少两个会话文本分块簇;对各个会话文本分块簇进行文本分块整理,并分别对所述各个会话文本分块簇中的各个会话文本分块进行文本分块整理,得到所述会话文本分

块队列。

[0075] 基于上述相关内容,在一些可独立的实施例中,所述根据所述各个会话文本分块对应的贡献权重,以及所述各个会话文本分块的异常决策向量,对所述各个会话文本分块进行拆解,得到至少两个会话文本分块簇,包括:分别根据所述各个会话文本分块对应的贡献权重,对所述各个会话文本分块的异常决策向量进行强化,得到所述各个会话文本分块的强化异常决策向量;根据所述各个会话文本分块的强化异常决策向量对所述各个会话文本分块进行分簇,得到至少两个会话文本分块簇。

[0076] 基于上述相关内容,在一些可独立的实施例中,所述对各个会话文本分块簇之间进行文本分块整理,并分别对所述各个会话文本分块簇中的各个会话文本分块进行文本分块整理,得到所述会话文本分块队列,包括:根据各个会话文本分块簇所包含的会话文本分块的个数,对所述各个会话文本分块簇进行文本分块整理;以及,针对所述各个会话文本分块簇,分别执行以下操作:根据所述会话文本分块簇中各个会话文本分块的异常决策向量与所述会话文本分块簇的联系性,对所述会话文本分块簇中的各个会话文本分块进行文本分块整理;基于所述各个会话文本分块簇之间的文本分块整理结果,以及所述各个会话文本分块簇中各个会话文本分块的文本分块整理结果,生成所述会话文本分块队列。

[0077] 本发明实施例提供的方法,获取目标会话安全检测文本对应的第一异常文本描述集以及第一异常文本描述集对应的第一异常文本描述数组和第一文本检测变量,根据第一异常文本描述数组、第一文本检测变量以及参考会话安全检测文本的第二异常文本描述集对应的第二异常文本描述数组和第二文本检测变量,获取目标会话安全检测文本和参考会话安全检测文本之间的共性度量值,在共性度量值大于设定度量值的基础上确定目标会话安全检测文本与参考会话安全检测文本为相似文本。鉴于第一文本检测变量表示第一异常文本描述集反映目标会话安全检测文本中风险主题词向量的检测偏移指数,第二文本检测变量表示第二异常文本描述集反映参考会话安全检测文本中风险主题词向量的检测偏移指数,这样在获取目标会话安全检测文本和参考会话安全检测文本之间的共性度量值时,还引入了异常文本描述集的检测偏移指数对共性度量值的贡献,而不是只分析异常文本描述集对应的异常文本描述数组,从而规避由于会话安全检测文本中存在扰动造成异常文本描述数组难以精准输出风险主题的词向量的问题,以便提高风险主题判别的精度,减少文本分析时所产生的偏差。

[0078] 在确定出目标会话安全检测文本与参考会话安全检测文本为相似文本之后,能够以参考会话安全检测文本的相关安全分析策略为基准,对目标会话安全检测文本进行一系列的安全分析,从而提高目标会话安全检测文本的安全分析精度和效率。

[0079] 本发明实施例提供的另一种用于在线业务会话交互的大数据安全分析方法包括以下步骤。

[0080] 步骤201、人工智能服务系统通过Transformer网络中的文本描述挖掘单元,对目标会话安全检测文本进行文本描述挖掘,得到目标会话安全检测文本对应的第一异常文本描述集。

[0081] 在本发明实施例中,该Transformer网络可以为该人工智能服务系统事先完成调校的神经网络,或者由其他系统调校好之后加载到该人工智能服务系统中的模型。Transformer网络是用于进行风险主题解析(也可以理解为相似文本分析)的神经网络,该

Transformer网络包括文本描述挖掘子网(特征提取网络)和描述特征解析子网(预测网络),文本描述挖掘子网和描述特征解析子网连接,文本描述挖掘子网用于提取会话安全检测文本的异常文本描述集和异常文本描述数组,描述特征解析子网用于根据异常文本描述集获取文本检测变量。该文本描述挖掘子网包括文本描述挖掘单元和文本描述投影单元(特征映射层),文本描述挖掘单元与文本描述投影单元连接,文本描述挖掘单元用于根据会话安全检测文本提取对应的异常文本描述集,文本描述投影单元用于根据异常文本描述集获取对应的异常文本描述数组。

[0082] 当人工智能服务系统获取到待进行相似性分析的目标会话安全检测文本时,通过该Transformer网络中的文本描述挖掘单元,对该目标会话安全检测文本进行文本描述挖掘,得到该目标会话安全检测文本对应的第一异常文本描述集。其中,本发明实施例中的文本描述挖掘单元,可以将目标会话安全检测文本的文本描述投影到文本场景向量关系网中,得到该目标会话安全检测文本对应的第一异常文本描述集,使得该第一异常文本描述集中所记载的细节符合文本场景向量关系网(维度更高的特征空间)的分布。鉴于相较于传统的文本向量关系网,文本场景向量关系网更匹配风险主题的向量关系网,这样在文本场景向量关系网中对会话安全检测文本进行文本描述挖掘可以使提取到的风险主题词向量尽可能精准和完整。

[0083] 在一些示例中,该文本描述挖掘单元可以为CNN、RNN等AI网络,本领域技术人员也可以根据实际需求自行选择。

[0084] 其中,第一异常文本描述集为表示目标会话安全检测文本的文本特征的记录,比如会话安全检测文本的文本特征可以包括会话安全检测文本的检测规则文本特征、会话行为文本特征、潜在风险文本特征等。

[0085] 又比如,对于获取目标会话安全检测文本的方式,本领域技术人员可以根据实际需求自行选择。

[0086] 步骤202、人工智能服务系统通过Transformer网络中的文本描述投影单元,对第一异常文本描述集进行文本描述投影,得到第一异常文本描述集对应的第一异常文本描述数组。

[0087] Transformer网络中的文本描述投影单元和文本描述挖掘单元连接,该文本描述投影单元用于根据异常文本描述集获取对应的异常文本描述数组。示例性地,该文本描述投影单元可以为全连接层,本领域技术人员也可以根据实际需求自行选择。

[0088] 当人工智能服务系统获取到目标会话安全检测文本对应的第一异常文本描述集,则通过Transformer网络中的文本描述投影单元,对该第一异常文本描述集进行文本描述投影,得到该第一异常文本描述集对应的第一异常文本描述数组。其中,该第一异常文本描述数组由该第一异常文本描述集投影得到,该第一异常文本描述数组为用于表征目标会话安全检测文本的文本特征的线性字段,可以为多维度的线性字段,比如该第一异常文本描述数组为1*h维的线性字段,则第一异常文本描述数组中包括h个维度的描述变量,h为正整数。

[0089] 本发明实施例中,Transformer网络中的文本描述挖掘子网包括文本描述挖掘单元和文本描述投影单元,因此上述步骤201和步骤202,以文本描述挖掘单元对目标会话安全检测文本进行处理和文本描述投影单元对第一异常文本描述集进行处理为例,介绍得到

目标会话安全检测文本对应的第一异常文本描述集及第一异常文本描述集对应的第一异常文本描述数组的过程。在其他设计思路下,文本描述挖掘子网还可以为其他结构的子网,只要保障通过通过该文本描述挖掘子网对目标会话安全检测文本进行文本描述挖掘,可以得到第一异常文本描述集以及第一异常文本描述数组便可。

[0090] 步骤203、人工智能服务系统通过Transformer网络中的描述特征解析子网,对第一异常文本描述集进行处理,得到第一异常文本描述集对应的第一文本检测变量。

[0091] 其中,Transformer网络中的描述特征解析子网与文本描述挖掘子网连接,该描述特征解析子网用于对异常文本描述集进行处理得到对应的文本检测变量。本发明实施例中,文本描述挖掘子网包括文本描述挖掘单元和文本描述投影单元,则该描述特征解析子网与该文本描述挖掘子网中的文本描述挖掘单元连接。示例性地,该描述特征解析子网可以为残差模型等,本领域技术人员也可以根据实际需求自行选择。

[0092] 当人工智能服务系统获取到目标会话安全检测文本对应的第一异常文本描述集,则通过该描述特征解析子网对第一异常文本描述集进行处理,得到该第一异常文本描述集对应的第一文本检测变量。其中,第一文本检测变量用于表征第一异常文本描述集反映目标会话安全检测文本中风险主题词向量的检测偏移指数,检测偏移指数可以理解为在处理过程中由于存在偏差,对得到的结果的质疑程度,可以反映第一异常文本描述集能精准表征风险主题词向量的程度。该第一文本检测变量越小,表示该第一异常文本描述集反映目标会话安全检测文本中风险主题词向量的精准性越佳,该第一文本检测变量越大,表示该第一异常文本描述集反映该第一会话安全检测文本中风险主题词向量的精准性越差。示例性地,该第一异常文本描述集为会话安全检测文本映射在文本场景向量关系网的异常文本描述集,该第一异常文本描述集中所记载的细节符合文本场景向量关系网的分布,则该第一文本检测变量也为符合文本场景向量关系网的分布的第一文本检测变量,用于表征文本场景向量关系网的第一异常文本描述集反映目标会话安全检测文本中风险主题词向量的检测偏移指数。

[0093] 步骤204、人工智能服务系统通过文本描述挖掘单元,对参考会话安全检测文本进行文本描述挖掘,得到参考会话安全检测文本对应的第二异常文本描述集。

[0094] 本发明实施例的风险主题解析任务,为对目标会话安全检测文本和参考会话安全检测文本进行解析,以确定该目标会话安全检测文本是否与参考会话安全检测文本为相似文本。其中参考会话安全检测文本为人工智能服务系统事先记录的会话安全检测文本,目标会话安全检测文本为人工智能服务系统当前获取的需要进行风险主题解析的文本数据。目标会话安全检测文本与参考会话安全检测文本为相似文本为目标会话安全检测文本中的风险主题与参考会话安全检测文本中的风险主题相同或者类似。

[0095] 基于此,人工智能服务系统获取事先记录的参考会话安全检测文本,通过该Transformer网络中的文本描述挖掘单元,对该参考会话安全检测文本进行文本描述挖掘,得到该参考会话安全检测文本对应的第二异常文本描述集,其中,第二异常文本描述集为表示参考会话安全检测文本的文本特征的记录。其中,本发明实施例中的文本描述挖掘单元,可以将参考会话安全检测文本的文本描述投影到文本场景向量关系网中,得到该参考会话安全检测文本对应的第二异常文本描述集。步骤204中的文本场景向量关系网与步骤201中的文本场景向量关系网相同。

[0096] 步骤205、人工智能服务系统通过文本描述投影单元,对第二异常文本描述集进行文本描述投影,得到第二异常文本描述集对应的第二异常文本描述数组。

[0097] 当人工智能服务系统获取到参考会话安全检测文本对应的第二异常文本描述集,则通过Transformer网络中的文本描述投影单元,对该第二异常文本描述集进行文本描述投影,得到该第二异常文本描述集对应的第二异常文本描述数组。其中,该第二异常文本描述数组为用于表征参考会话安全检测文本的文本特征的线性字段,可以为多维度的线性字段,比如该第二异常文本描述数组为1*h维的线性字段,则第二异常文本描述数组中包括h个维度的描述变量。该第二异常文本描述数组由该第二异常文本描述集投影所得。

[0098] 本发明实施例中Transformer网络中的文本描述挖掘子网包括文本描述挖掘单元和文本描述投影单元,因此步骤204步骤205以文本描述挖掘单元对参考会话安全检测文本进行处理和文本描述投影单元对第二异常文本描述集进行处理为例,介绍得到参考会话安全检测文本对应的第二异常文本描述集及第二异常文本描述集对应的第二异常文本描述数组的过程,在其他设计思路下,文本描述挖掘子网还可以为其他结构的子网,只要保障通过该文本描述挖掘子网对参考会话安全检测文本进行文本描述挖掘,可以得到第二异常文本描述集以及第二异常文本描述数组便可。

[0099] 步骤206、人工智能服务系统通过描述特征解析子网,对第二异常文本描述集进行处理,得到第二异常文本描述集对应的第二文本检测变量。

[0100] 第二文本检测变量用于表征第二异常文本描述集反映参考会话安全检测文本中风险主题词向量的检测偏移指数。

[0101] 示例性的,人工智能服务系统在本轮风险主题解析之前,可以预先对参考会话安全检测文本进行处理,得到参考会话安全检测文本对应的第二异常文本描述数组和第二文本检测变量,将该第二异常文本描述数组和第二文本检测变量进行记录,则无需再实施步骤204-步骤206,直接获取记录的第二异常文本描述数组和第二文本检测变量便可。或者,人工智能服务系统获取到待进行相似性分析的目标会话安全检测文本后,获取事先记录的参考会话安全检测文本,将该目标会话安全检测文本和参考会话安全检测文本以文本二元组的方式一并加载到Transformer网络中,由该Transformer网络中分别对目标会话安全检测文本和参考会话安全检测文本进行处理,得到第一异常文本描述数组、第一文本检测变量、第二异常文本描述数组和第二文本检测变量。其中,该Transformer网络的各个子网可以对目标会话安全检测文本和参考会话安全检测文本进行同步操作,比如在Transformer网络中的文本描述挖掘模型对目标会话安全检测文本进行处理的同时,该Transformer网络中的描述特征解析子网可以对参考会话安全检测文本进行处理,进而达到对目标会话安全检测文本和参考会话安全检测文本同步处理,提升整体方案的时效性。

[0102] 步骤207、人工智能服务系统根据第一异常文本描述数组、第一文本检测变量以及参考会话安全检测文本的第二异常文本描述集对应的第二异常文本描述数组、第二异常文本描述集对应的第二文本检测变量,获取目标会话安全检测文本和参考会话安全检测文本之间的共性度量值。

[0103] 当人工智能服务系统获取到第一异常文本描述数组、第一文本检测变量、第二异常文本描述数组和第二文本检测变量,则根据该第一异常文本描述数组、第一文本检测变量、第二异常文本描述数组和第二文本检测变量,获取目标会话安全检测文本和参考会话

安全检测文本之间的共性度量值。其中,目标会话安全检测文本和参考会话安全检测文本之间的共性度量值越大,表示目标会话安全检测文本中的风险主题和参考会话安全检测文本中的风险主题相同或者类似的可能性越高,也即是目标会话安全检测文本与参考会话安全检测文本为相似文本的可能性越高;目标会话安全检测文本和参考会话安全检测文本之间的共性度量值越小,表示目标会话安全检测文本中的风险主题和参考会话安全检测文本中的风险主题相同或者类似的可能性越低,也即是目标会话安全检测文本与参考会话安全检测文本为相似文本的可能性越低。

[0104] 在一些示例中,人工智能服务系统采用余弦相似度的运算思路对第一异常文本描述数组、第一文本检测变量、第二异常文本描述数组和第二文本检测变量进行处理,得到目标会话安全检测文本和参考会话安全检测文本之间的共性度量值。

[0105] 步骤208、人工智能服务系统在共性度量值大于设定度量值的基础上,确定目标会话安全检测文本与参考会话安全检测文本为相似文本。

[0106] 当人工智能服务系统获取到目标会话安全检测文本和参考会话安全检测文本之间的共性度量值,将该共性度量值与设定度量值进行比较,若共性度量值大于该设定度量值,则确定目标会话安全检测文本中的风险主题和参考会话安全检测文本中的风险主题相同或者类似,也即是目标会话安全检测文本与参考会话安全检测文本为相似文本。若共性度量值不大于该设定度量值,则确定目标会话安全检测文本中的风险主题和参考会话安全检测文本中的风险主题不相同或者类似,也即是目标会话安全检测文本与参考会话安全检测文本不是相似文本。

[0107] 本发明实施例是以人工智能服务系统对目标会话安全检测文本与一个参考会话安全检测文本进行解析为例,介绍风险主题解析的过程。在其他设计思路下,人工智能服务系统存储有多个参考会话安全检测文本,则人工智能服务系统获取到待进行相似性分析的目标会话安全检测文本后,对多个参考会话安全检测文本进行依次处理,对依次处理的每一个参考会话安全检测文本实施上述相关技术方案,直到确定目标会话安全检测文本与多个参考会话安全检测文本中的某一参考会话安全检测文本为相似文本,或者直到确定目标会话安全检测文本与多个参考会话安全检测文本中的任一参考会话安全检测文本均不是相似文本。

[0108] 可以理解,本发明实施例是以人工智能服务系统通过Transformer网络中的文本描述挖掘子网和描述特征解析子网对文本进行处理为例进行介绍。在其他设计思路下,人工智能服务系统可通过另外的思路,实现对目标会话安全检测文本进行文本描述挖掘,得到目标会话安全检测文本对应的第一异常文本描述集及第一异常文本描述集对应的第一异常文本描述数组,对第一异常文本描述集进行处理,得到第一异常文本描述集对应的第一文本检测变量。

[0109] 本发明实施例提供的方法,通过Transformer网络中的文本描述挖掘子网和描述特征解析子网,获取第一异常文本描述集对应的第一异常文本描述数组和第一文本检测变量,根据第一异常文本描述数组、第一文本检测变量以及参考会话安全检测文本对应的第二异常文本描述数组和第二文本检测变量,获取目标会话安全检测文本和参考会话安全检测文本之间的共性度量值,在共性度量值大于设定度量值的基础上,确定目标会话安全检测文本与参考会话安全检测文本为相似文本。鉴于第一文本检测变量表示第一异常文本描

述集反映目标会话安全检测文本中风险主题词向量的检测偏移指数,第二文本检测变量表示第二异常文本描述集反映参考会话安全检测文本中风险主题词向量的检测偏移指数,这样在获取目标会话安全检测文本和参考会话安全检测文本之间的共性度量值时,还引入了异常文本描述集的检测偏移指数对共性度量值的贡献,而不是只分析异常文本描述集对应的异常文本描述数组,从而规避由于会话安全检测文本中存在扰动造成异常文本描述数组难以精准输出风险主题的词向量的问题,以便提高风险主题判别的精度,减少文本分析时所产生的偏差。

[0110] 本发明实施例中,将目标会话安全检测文本的文本描述投影到文本场景向量关系网中,得到该目标会话安全检测文本对应的第一异常文本描述集。鉴于相较于传统的文本向量关系网,文本场景向量关系网更匹配风险主题的向量关系网,这样在文本场景向量关系网中对风险主题进行文本描述挖掘可以使提取到的风险主题词向量尽可能精准和完整,以保障风险主题分析的精度和可信度。

[0111] 在通过Transformer网络进行风险主题解析(相似文本分析)之前,需要先对Transformer网络进行调校训练,相关的调校训练方法包括以下步骤。

[0112] 步骤301、人工智能服务系统获取会话安全检测文本样例和会话安全检测文本样例对应的异常文本描述数组样例。

[0113] 人工智能服务系统获取用于调校Transformer网络的会话安全检测文本样例和会话安全检测文本样例对应的异常文本描述数组样例。其中,会话安全检测文本样例为包括风险主题的文本数据,会话安全检测文本样例对应的异常文本描述数组样例为用于表征会话安全检测文本样例的文本特征的线性字段。比如,该异常文本描述数组样例可用于表征会话安全检测文本样例所对应的风险主题标签,以安全风险1和安全风险2为例,包括安全风险1的风险主题的任一会话安全检测文本样例对应的异常文本描述数组样例均为异常文本描述数组样例sample1,包括安全风险2的风险主题的任一会话安全检测文本样例对应的异常文本描述数组样例均为异常文本描述数组样例sample2。

[0114] 其中,会话安全检测文本样例可以为人工智能服务系统中事先记录的会话安全检测文本样例,或者由人工智能服务系统从其他系统中调用的会话安全检测文本样例,还可以为其他系统上传至该人工智能服务系统中的会话安全检测文本样例。其中会话安全检测文本样例对应的异常文本描述数组样例可以是为会话安全检测文本样例所注释的异常文本描述数组样例,或者由另外的思路得到的异常文本描述数组样例,本领域技术人员也可以根据实际需求自行选择。上述样例可以理解为用于进行网络训练的样本信息,通常还可以理解为文本示例、示例性文本或者已认证文本。

[0115] 步骤302、人工智能服务系统通过Transformer网络中的文本描述挖掘单元,对会话安全检测文本样例进行文本描述挖掘,得到会话安全检测文本样例对应的异常文本解析描述集。

[0116] Transformer网络是用于进行风险主题解析(文本相似性分析)的网络,该Transformer网络包括文本描述挖掘子网和描述特征解析子网。其中,文本描述挖掘子网与描述特征解析子网连接,文本描述挖掘子网用于提取会话安全检测文本对应的异常文本描述集和异常文本描述数组,描述特征解析子网用于根据异常文本描述集获取对应的文本检测变量。其中,该文本描述挖掘子网包括文本描述挖掘单元和文本描述投影单元,文本描述

挖掘单元与文本描述投影单元连接,文本描述挖掘单元用于根据会话安全检测文本提取对应的异常文本描述集,文本描述投影单元用于根据异常文本描述集获取对应的异常文本描述数组。

[0117] 当人工智能服务系统获取到会话安全检测文本样例,则通过Transformer网络中的文本描述挖掘单元,对该会话安全检测文本样例进行文本描述挖掘,得到该会话安全检测文本样例对应的异常文本解析描述集。该异常文本解析描述集为表示会话安全检测文本样例的特征的文本数据。

[0118] 其中,本发明实施例中的文本描述挖掘单元,将会话安全检测文本样例的文本描述投影到文本场景向量关系网中,得到该会话安全检测文本样例对应的异常文本解析描述集。相较于传统的文本向量关系网,文本场景向量关系网更匹配风险主题的向量关系网,在文本场景向量关系网中对风险主题进行文本描述挖掘可以使提取到的风险主题词向量尽可能精准和完整。

[0119] 步骤303、人工智能服务系统通过Transformer网络中的文本描述投影单元,对异常文本解析描述集进行文本描述投影,得到异常文本解析描述集对应的异常文本解析数组。

[0120] Transformer网络中的文本描述投影单元和文本描述挖掘单元连接,该文本描述投影单元用于根据异常文本描述集获取对应的异常文本描述数组。示例性地,该文本描述投影单元可以为全连接层,或者该文本描述投影单元还可以为其他结构的网络,本领域技术人员也可以根据实际需求自行选择。

[0121] 当人工智能服务系统获取到会话安全检测文本样例对应的异常文本解析描述集,则通过Transformer网络中的文本描述投影单元,对该异常文本解析描述集进行文本描述投影,得到该异常文本解析描述集对应的异常文本解析数组。其中,该异常文本解析数组为用于表征会话安全检测文本样例的特征的线性字段,该异常文本解析数组由该异常文本解析描述集投影所得。

[0122] 本发明实施例中,Transformer网络中的文本描述挖掘子网包括文本描述挖掘单元和文本描述投影单元,因此上述步骤302和步骤03,以文本描述挖掘单元对会话安全检测文本样例进行处理和文本描述投影单元对异常文本解析描述集进行处理为例,介绍得到会话安全检测文本样例对应的异常文本解析描述集及异常文本解析描述集对应的异常文本解析数组的过程。在其他设计思路下,文本描述挖掘子网还可以为其他结构的子网,只要保障通过该文本描述挖掘子网对会话安全检测文本样例进行文本描述挖掘,可以得到异常文本解析描述集以及异常文本解析数组便可。

[0123] 步骤304、人工智能服务系统根据异常文本解析数组和异常文本描述数组样例之间的比较结果,调校文本描述挖掘子网。

[0124] 其中,异常文本解析数组为通过Transformer网络推测的表示会话安全检测文本样例的特征的线性字段,异常文本描述数组样例为真实的表示会话安全检测文本样例的特征的线性字段。因此,当人工智能服务系统获取到异常文本解析数组和异常文本描述数组样例,则根据异常文本解析数组和异常文本描述数组样例之间的比较结果,来调校Transformer网络中的文本描述挖掘子网,也即是调校文本描述挖掘单元和文本描述投影单元,以使通过文本描述挖掘单元和文本描述投影单元得到的异常文本解析数组与异常文

本描述数组样例的比较结果(差异)越来越小。

[0125] 在一些示例中,人工智能服务系统获取异常文本解析数组和异常文本描述数组样例之间的第一调校代价指标,根据该第一调校代价指标,调校文本描述挖掘子网。其中,第一调校代价指标表示异常文本解析数组和异常文本描述数组样例之间的比较结果。

[0126] 示例性地,人工智能服务系统获取第一代价函数,根据第一代价函数对异常文本解析数组和异常文本描述数组样例进行确定,得到第一调校代价指标。其中,第一代价函数为用于获取异常文本解析数组和异常文本描述数组样例之间的训练代价的评估算法。

[0127] 在一些示例下,Transformer网络还包括网络代价生成子网,网络代价生成子网与文本描述挖掘子网连接。该网络代价生成子网包括每个风险主题标签对应的置信度描述数组。人工智能服务系统通过网络代价生成子网,按照会话安全检测文本样例所对应风险主题标签对应的置信度描述数组对异常文本解析数组进行强化操作(加权操作),得到异常文本解析数组对应的异常文本描述强化数组,获取异常文本描述强化数组和异常文本描述数组样例之间的第二调校代价指标,根据第二调校代价指标,调校文本描述挖掘子网和网络代价生成子网。其中,第二调校代价指标表示异常文本描述强化数组和异常文本描述数组样例之间的比较结果。

[0128] 网络代价生成子网用于根据异常文本描述数组获取对应的调校代价指标,该网络代价生成子网与文本描述挖掘子网连接,本发明实施例中,文本描述挖掘子网包括文本描述挖掘单元和文本描述投影单元,则该网络代价生成子网与该文本描述挖掘子网中的文本描述投影单元连接。该网络代价生成子网可以为分类模型,本领域技术人员也可以根据实际需求自行选择。

[0129] 其中,每个风险主题标签对应的置信度描述数组用于表征该风险主题标签对应的会话安全检测文本对应的异常文本描述数组的权重,示例性地,会话安全检测文本样例对应的异常文本解析数组为1*h维的线性字段,则异常文本解析数组中包括h个维度的描述变量。则风险主题标签对应的置信度描述数组也为1*h维的线性字段,置信度描述数组中包括h个维度的偏置系数,h个维度的偏置系数分别表示对应的异常文本解析数组中每个维度的描述变量的重要性。

[0130] 人工智能服务系统获取到会话安全检测文本样例对应的异常文本解析描述集后,在网络代价生成子网包括的多个置信度描述数组中,确定该会话安全检测文本样例所对应风险主题标签对应的置信度描述数组,通过网络代价生成子网,按照该会话安全检测文本样例所对应风险主题标签对应的置信度描述数组,对异常文本解析数组进行强化操作,得到异常文本解析数组对应的异常文本描述强化数组。也即是将异常文本解析数组中每个维度的描述变量,分别与置信度描述数组中对应的偏置系数进行乘法运算,得到异常文本描述强化数组。示例性地,网络代价生成子网还包括第二代价函数。人工智能服务系统获取第二代价函数,根据第二代价函数对异常文本描述强化数组和异常文本描述数组样例进行处理,得到第二调校代价指标。其中,第二代价函数为用于获取异常文本描述强化数组和异常文本描述数组样例之间的训练代价的评估算法。

[0131] 在一些示例下,人工智能服务系统基于梯度下降规则,对文本描述挖掘子网和网络代价生成子网进行改进,以达到调校文本描述挖掘子网和网络代价生成子网的目的。其中,本领域技术人员也可以根据实际需求自行选择梯度下降规则。

[0132] 可以理解,步骤301-步骤304只介绍根据会话安全检测文本样例获取异常文本解析数组,根据异常文本解析数组和异常文本描述数组样例之间的比较结果,调校文本描述挖掘子网和网络代价生成子网,以此实现根据会话安全检测文本样例和会话安全检测文本样例对应的异常文本描述数组样例,调校文本描述挖掘子网。在其他设计思路下人工智能服务系统还可以采用另外的思路,实现根据会话安全检测文本样例和会话安全检测文本样例对应的异常文本描述数组样例,调校文本描述挖掘子网。

[0133] 本发明实施例中是以根据一个异常文本描述集样例和该异常文本描述集样例对应的异常文本描述数组样例调校文本描述挖掘子网和网络代价生成子网为例进行调校。在实际调校过程中,人工智能服务系统会根据多个会话安全检测文本样例和该多个会话安全检测文本样例对应的异常文本描述数组样例,调校文本描述挖掘子网和网络代价生成子网。其中,多个会话安全检测文本样例之间的任两个会话安全检测文本样例所对应的风险主题标签可一致也可不一致。

[0134] 在一些示例中,人工智能服务系统获取多个会话安全检测文本样例和该多个会话安全检测文本样例对应的异常文本描述数组样例,将多个会话安全检测文本样例同时加载到Transformer网络中的文本描述挖掘单元,由该Transformer网络中分别对多个会话安全检测文本样例进行处理,根据得到的异常文本解析数组和对应的异常文本描述数组样例,调校文本描述挖掘子网和网络代价生成子网。其中,该Transformer网络中的文本描述挖掘子网和网络代价生成子网可以对多个会话安全检测文本样例进行同步操作。比如多个会话安全检测文本样例中包括第一会话安全检测文本样例和第二会话安全检测文本样例,在Transformer网络中的网络代价生成子网对第一会话安全检测文本样例进行处理的同时,该Transformer网络中的文本描述挖掘子网可以对第二会话安全检测文本样例进行处理,以此达到对多个会话安全检测文本样例同步处理,提升整体方案的时效性。

[0135] 在一些示例下,当调校文本描述挖掘子网和网络代价生成子网的循环次数达到设定次数时,完成对文本描述挖掘子网和网络代价生成子网的调校。或者,当人工智能服务系统获取的第一调校代价指标或者第二调校代价指标小于第一设定指标值时,表示文本描述挖掘子网和网络代价生成子网的调校代价指标趋于稳定,则完成对文本描述挖掘子网和网络代价生成子网的调校。

[0136] 在其他设计思路下,人工智能服务系统中事先具有调校好的文本描述挖掘子网以及调校该文本描述挖掘子网所用到的会话安全检测文本样例,则人工智能服务系统无需执行上述步骤301-步骤304,仅需获取调校该文本描述挖掘子网所用到的会话安全检测文本样例,执行下述步骤305-步骤307,完成对描述特征解析子网的调校便可。

[0137] 步骤305、人工智能服务系统获取会话安全检测文本样例所对应风险主题标签的关键文本描述数组。

[0138] 其中,每个风险主题标签对应一个关键文本描述数组,该关键文本描述数组表示风险主题标签对应的风险主题词向量。当人工智能服务系统完成对Transformer网络中的文本描述挖掘子网和网络代价生成子网的调校之后,人工智能服务系统获取该会话安全检测文本样例所对应风险主题标签的关键文本描述数组,该关键文本描述数组可用于表征该会话安全检测文本样例中的风险主题词向量。

[0139] 在一些示例中,人工智能服务系统获取会话安全检测文本样例所对应风险主题标

签的多个会话安全检测文本对应的异常文本描述数组,根据获取到的多个异常文本描述数组,确定关键文本描述数组。在调校文本描述挖掘子网和网络代价生成子网的过程中,人工智能服务系统得到多个会话安全检测文本对应的异常文本描述数组,则人工智能服务系统确定该异常文本描述集样例所对应风险主题标签的多个会话安全检测文本,获取该多个会话安全检测文本对应的多个异常文本描述数组,对获取到的该多个异常文本描述数组进行平均化处理,得到该会话安全检测文本样例所对应风险主题标签对应的关键文本描述数组。

[0140] 在一些示例下,人工智能服务系统获取会话安全检测文本样例所对应风险主题标签对应的置信度描述数组,将该会话安全检测文本样例对应的置信度描述数组确定为关键文本描述数组。

[0141] 其中,网络代价生成子网包括每个风险主题标签对应的置信度描述数组。在调校文本描述挖掘子网和网络代价生成子网的过程中,会持续调整网络代价生成子网中的每个置信度描述数组,当调校完成时,网络代价生成子网中包括调校后的每个置信度描述数组。则人工智能服务系统可以确定该会话安全检测文本样例所对应的风险主题标签,从网络代价生成子网中的多个置信度描述数组中获取该风险主题标签对应的置信度描述数组,将该置信度描述数组确定为该会话安全检测文本样例所对应风险主题标签对应的关键文本描述数组。

[0142] 步骤306、人工智能服务系统通过描述特征解析子网,对异常文本解析描述集进行处理,得到异常文本解析描述集对应的文本检测变量解析结果。

[0143] 文本检测变量解析结果用于表征异常文本解析描述集反映会话安全检测文本样例中风险主题词向量的检测偏移指数。

[0144] 步骤307、人工智能服务系统根据异常文本解析数组、关键文本描述数组和文本检测变量解析结果,获取第三调校代价指标,根据第三调校代价指标,调校描述特征解析子网。

[0145] 当人工智能服务系统获取到会话安全检测文本样例对应的异常文本解析数组、关键文本描述数组和文本检测变量解析结果,根据异常文本解析数组、关键文本描述数组和文本检测变量解析结果获取第三调校代价指标,根据该第三调校代价指标调校Transformer网络中的描述特征解析子网,以使该描述特征解析子网生成的异常文本解析描述集对应的文本检测变量解析结果尽可能精准和完整。其中,第三调校代价指标表示异常文本解析描述集对应的文本检测变量解析结果(文本检测变量的预测结果)的训练代价。

[0146] 在一些示例中,人工智能服务系统获取第三代价函数,根据第三代价函数对异常文本解析数组、关键文本描述数组和文本检测变量解析结果进行确定,得到第三调校代价指标。

[0147] 在一些示例下,人工智能服务系统根据异常文本解析数组和关键文本描述数组之间的差异特征,获取目标文本检测变量,根据目标文本检测变量和文本检测变量解析结果之间的比较结果,获取第三调校代价指标。

[0148] 鉴于文本检测变量解析结果用于表征异常文本描述集样例反映会话安全检测文本中风险主题词向量的检测偏移指数,在实际应用时,人工智能服务系统会根据异常文本描述集对应的异常文本描述数组和文本检测变量获取会话安全检测文本之间的共性度量

值。因此,文本检测变量解析结果实质是需要表示会话安全检测文本样例对应的异常文本解析数组与会话安全检测文本样例对应的关键文本描述数组相匹配的检测偏移指数,异常文本解析数组与关键文本描述数组之间的差异特征越小,异常文本解析数组与关键文本描述数组越类似,也即是异常文本解析数组与关键文本描述数组越接近。

[0149] 其中,人工智能服务系统可以根据异常文本解析数组和关键文本描述数组之间的差异特征,获取目标文本检测变量,则该目标文本检测变量便可表示异常文本解析数组和关键文本描述数组相匹配的检测偏移指数。异常文本解析数组和关键文本描述数组之间的差异特征越大,异常文本解析数组和关键文本描述数组相匹配的检测偏移指数越大,也即是目标文本检测变量越大;异常文本解析数组和关键文本描述数组之间的差异特征越小,异常文本解析数组和关键文本描述数组相匹配的检测偏移指数越小,也即是目标文本检测变量越小。

[0150] 而在实际实施过程中难以获得待进行相似性分析的会话安全检测文本所对应的风险主题标签,因此也难以获得会话安全检测文本对应的关键文本描述数组,因此人工智能服务系统根据异常文本描述集来获取文本检测变量。这样在描述特征解析子网的调校过程中,需保障描述特征解析子网得到的文本检测变量解析结果可以表示会话安全检测文本样例对应的异常文本解析数组与会话安全检测文本样例对应的关键文本描述数组相匹配的检测偏移指数,也即是需保障文本检测变量解析结果与目标文本检测变量之间的比较结果较小。因此人工智能服务系统可根据目标文本检测变量和文本检测变量解析结果之间的比较结果获取第三调校代价指标,根据第三调校代价指标调校描述特征解析子网,以使该目标文本检测变量和文本检测变量解析结果之间的比较结果越来越小,使该描述特征解析子网生成的文本检测变量解析结果越来越精准。

[0151] 在一些示例下,人工智能服务系统基于梯度下降规则,对描述特征解析子网进行优化,以达到调校描述特征解析子网的目的。

[0152] 通过实施步骤305-步骤307,实现了在维持调校后的文本描述挖掘子网不变的基础上,根据异常文本描述数组样例和会话安全检测文本样例所对应风险主题标签的关键文本描述数组,调校描述特征解析子网。在其他设计思路下,人工智能服务系统还可以采用另外的思路,根据异常文本描述数组样例和关键文本描述数组,调校描述特征解析子网。

[0153] 本发明实施例提供的方法中,将调校Transformer网络分为文本描述挖掘子网的调校环节和描述特征解析子网的调校环节。在一些示例中,将获取共性度量值的逻辑配置为共性度量确定单元,将比较共性度量值与设定度量值的逻辑配置为度量比对单元,则人工智能服务系统可以将调校好的文本描述挖掘子网、描述特征解析子网以及共性度量确定单元和度量比对单元进行配置,得到Transformer网络。示例性的设计思路包括:(1)调校文本描述挖掘单元与文本描述投影单元;(2)调校描述特征解析子网;(3)将文本描述挖掘单元、文本描述投影单元、描述特征解析子网、共性度量确定单元、度量比对单元进行整合,生成Transformer网络。

[0154] 本发明实施例提供的技术方案,获取会话安全检测文本样例和会话安全检测文本样例对应的异常文本描述数组样例,通过文本描述挖掘子网提取会话安全检测文本样例的异常文本解析描述集和异常文本解析数组,根据异常文本解析数组和异常文本描述数组样例之间的比较结果,调校文本描述挖掘子网。获取会话安全检测文本样例所对应风险主题

标签的关键文本描述数组,通过描述特征解析子网获取异常文本解析描述集对应的文本检测变量解析结果,根据异常文本解析数组、关键文本描述数组和文本检测变量解析结果获取第三调校代价指标, 根据第三调校代价指标调校描述特征解析子网。之后便能够通过包括该文本描述挖掘子网和描述特征解析子网的Transformer网络进行风险主题解析,鉴于引入描述特征解析子网,这样在获取目标会话安全检测文本和参考会话安全检测文本之间的共性度量值时,还引入了描述特征解析子网生成的文本检测变量对共性度量值的贡献,也即是引入了异常文本描述集的检测偏移指数对共性度量值的贡献,而不是只分析异常文本描述集对应的异常文本描述数组,从而规避由于会话安全检测文本中存在扰动造成异常文本描述数组难以精准输出风险主题的词向量的问题,以便提高风险主题判别的精度,减少文本分析时所产生的偏差。

[0155] 此外,根据会话安全检测文本样例和会话安全检测文本样例对应的异常文本描述数组样例,调校文本描述挖掘子网,在维持调校后的文本描述挖掘子网不变的基础上,根据异常文本描述数组样例和会话安全检测文本样例所对应风险主题标签的关键文本描述数组,调校描述特征解析子网。以此对Transformer网络的调校过程可以分为文本描述挖掘子网的调校环节和描述特征解析子网的调校环节,则在文本描述挖掘子网调校好的基础上,仅需获取调校该文本描述挖掘子网的会话安全检测文本样例,对描述特征解析子网进行调校便可,不用再次调校新的文本描述挖掘子网,也不用再次获取会话安全检测文本样例。

[0156] 此外,本发明实施例中,将会话安全检测文本样例的文本描述投影到文本场景向量关系网中,得到该会话安全检测文本样例对应的异常文本解析描述集。鉴于相较于传统的文本向量关系网,文本场景向量关系网更匹配风险主题的向量关系网,这样在文本场景向量关系网中对风险主题进行文本描述挖掘可以使提取到的风险主题词向量尽可能精准和完整,可以提高调校得到的Transformer网络进行风险主题解析时的精度。

[0157] 以上所述,仅为本发明的具体实施方式。熟悉本技术领域的技术人员根据本发明提供的具体实施方式,可想到变化或替换,都应涵盖在本发明的保护范围之内。

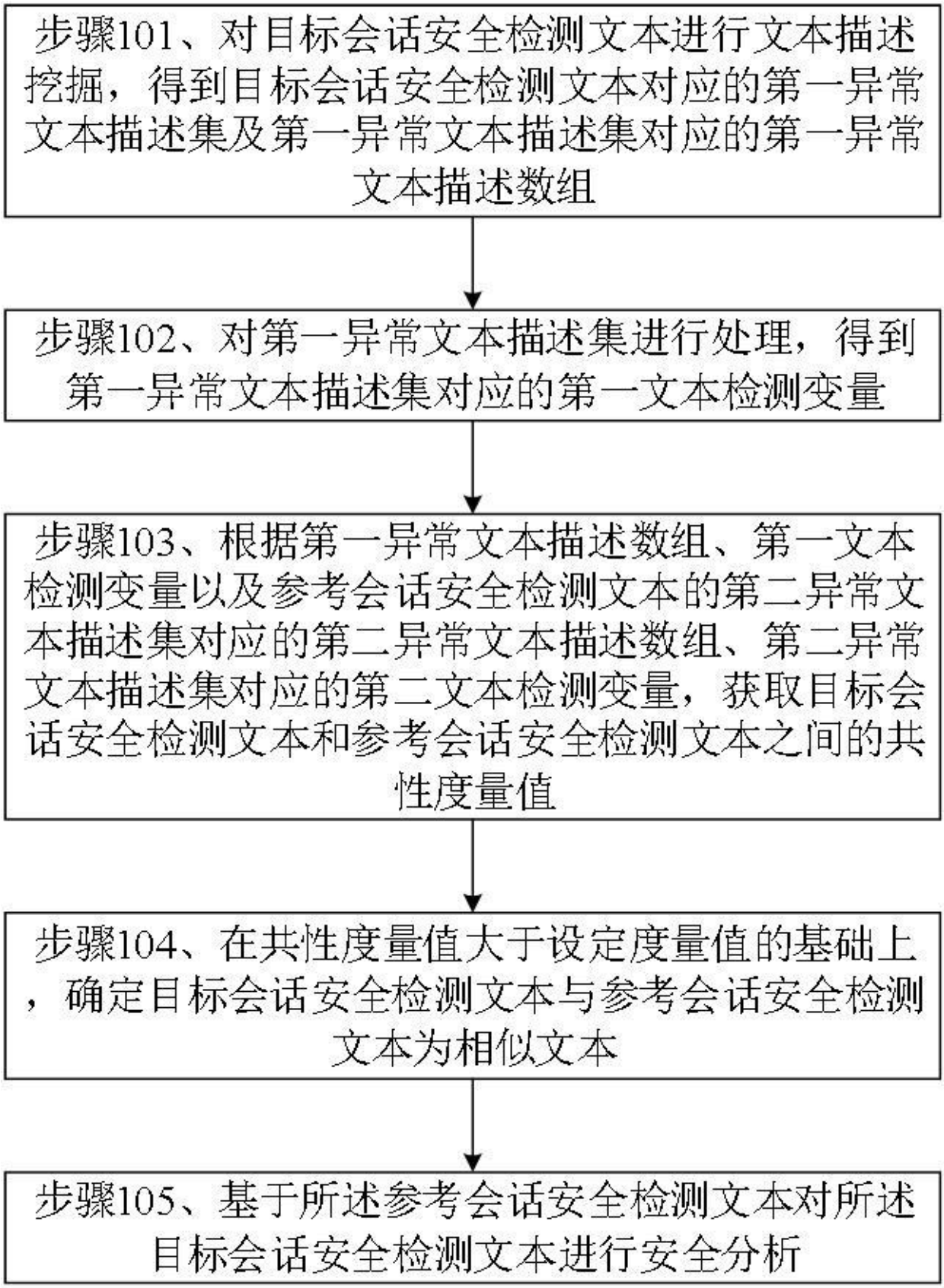

步骤101、对目标会话安全检测文本进行文本描述挖掘，得到目标会话安全检测文本对应的第一异常文本描述集及第一异常文本描述集对应的第一异常文本描述数组
步骤102、对第一异常文本描述集进行处理，得到第一异常文本描述集对应的第一文本检测变量
步骤103、根据第一异常文本描述数组、第一文本检测变量以及参考会话安全检测文本的第二异常文本描述集对应的第二异常文本描述数组、第二异常文本描述集对应的第二文本检测变量，获取目标会话安全检测文本和参考会话安全检测文本之间的共性度量值
步骤104、在共性度量值大于设定度量值的基础上，确定目标会话安全检测文本与参考会话安全检测文本为相似文本
步骤105、基于所述参考会话安全检测文本对所述目标会话安全检测文本进行安全分析

图1