



(12)发明专利申请

(10)申请公布号 CN 110188198 A

(43)申请公布日 2019.08.30

(21)申请号 201910415531.X

(22)申请日 2019.05.13

(71)申请人 北京一览群智数据科技有限责任公司

地址 100080 北京市海淀区苏州街79号金
洲大厦5层

(72)发明人 窦志成 姜涛 韩维思 黄真

(74)专利代理机构 北京中创阳光知识产权代理
有限责任公司 11003

代理人 尹振启

(51)Int.Cl.

G06F 16/35(2019.01)

G06F 16/36(2019.01)

G06Q 40/02(2012.01)

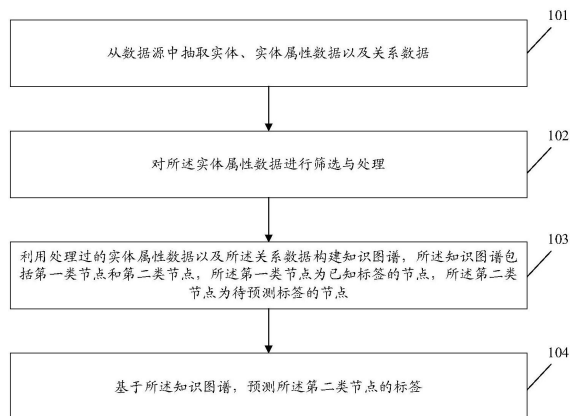
权利要求书3页 说明书12页 附图2页

(54)发明名称

一种基于知识图谱的反欺诈方法及装置

(57)摘要

本申请公开了一种基于知识图谱的反欺诈方法及装置,所述方法包括:从数据源中抽取实体、实体属性数据以及关系数据;对所述实体属性数据进行筛选与处理,并利用处理过的实体属性数据以及所述关系数据构建知识图谱,所述知识图谱包括第一类节点和第二类节点,所述第一类节点为已知标签的节点,所述第二类节点为待预测标签的节点;基于所述知识图谱,预测所述第二类节点的标签。



1. 一种基于知识图谱的反欺诈方法,其特征在于,所述方法包括:
从数据源中抽取实体、实体属性数据以及关系数据;
对所述实体属性数据进行筛选与处理,并利用处理过的实体属性数据以及所述关系数据构建知识图谱,所述知识图谱包括第一类节点和第二类节点,所述第一类节点为已知标签的节点,所述第二类节点为待预测标签的节点;
基于所述知识图谱,预测所述第二类节点的标签。
2. 根据权利要求1所述的方法,其特征在于,所述实体为企业;相应地,
所述实体属性数据包括企业信息和个人客户信息;
所述关系数据包括以下至少之一:企业与个人的对应关系、个人与个人的对应关系、企业与相关属性的对应关系、个人与相关属性的对应关系、企业与企业之间的对应关系。
3. 根据权利要求2所述的方法,其特征在于,所述个人客户信息包括企业实控人信息与多个企业干系人信息;
所述对所述实体属性数据进行筛选与处理,包括:
将所述多个企业干系人信息进行聚合后,得到干系人聚合特征;
将实控人特征与干系人聚合特征关联到企业上,得到企业样本数据;
对所述企业样本数据进行以下至少一种处理:异常值处理、缺失值处理、变量之间相关性的分析、类别变量的编码。
4. 根据权利要求1或3所述的方法,其特征在于,所述利用处理过的实体属性数据以及所述关系数据构建知识图谱,包括:
以企业作为知识图谱的节点;
将处理过的企业信息、企业实控人信息以及企业干系人信息的聚合共同作为节点的属性;
将企业之间的归约关系作为知识图谱的关系;
删除掉知识图谱中存在的孤立节点。
5. 根据权利要求1所述的方法,其特征在于,所述基于所述知识图谱,预测所述第二类节点的标签,包括:
S1:使用真实标签已知的企业属性特征进行训练,得到欺诈预估模型local_classifier;
S2:从知识图谱中抽取真实标签已知的企业属性特征矩阵,并根据知识图谱中的节点关联计算训练数据集中的每个企业节点的一度邻居中的正样本的比例,将该值拼接到企业属性特征后,再次进行训练,得到加入邻居标签信息的欺诈预估模型relation_classifier;
S3:将标签未知的企业的属性特征输入S1中训练的模型,获得初步的欺诈风险概率pos_probability,将该概率值同样作为知识图谱中待预测企业节点的属性进行存储;
S4:设置预定义的最大迭代轮数N,迭代次数i初始化为1,待预估企业节点个数为M;N,i,M为正整数;
S5:计算每个待预测企业节点的不欺诈概率neg_probability=1-pos_probabiliy,并将pos_probabiliy和neg_probability做差值,得到信心度confidence,并将confidence的绝对值进行排序;

S6:选择前 $i \times M/N$ 个企业进行预分类,如果confidence大于0,则将该预测样本的预估标签置为正,如果confidence小于等于0,则将该预测样本的预估标签置为负,并写回知识图谱中的pred属性存储;

S7:对于每一个待预测的企业节点,计算其周围一度邻居的正样本比例,如果周围邻居节点在训练样本或者在上一轮确定了该测试节点的标签,则可加入计算,将计算结果拼接到该企业的属性数据;

S8:使用S2中relation_classifier进行分类,得到本轮的该节点的欺诈风险概率pos_probability,写回知识图谱中更新该属性值;

S9:迭代次数 $i+1$,重复迭代S5、S6、S7、S8;其中,迭代结束标志为 $i > N$ 或本轮预测结果与上一轮预测结果相同。

6. 一种基于知识图谱的反欺诈装置,其特征在于,所述装置包括:

抽取单元,用于从数据源中抽取实体、实体属性数据以及关系数据;

处理单元,用于对所述实体属性数据进行筛选与处理;

图谱构建单元,用于利用处理过的实体属性数据以及所述关系数据构建知识图谱,所述知识图谱包括第一类节点和第二类节点,所述第一类节点为已知标签的节点,所述第二类节点为待预测标签的节点;

预测单元,用于基于所述知识图谱,预测所述第二类节点的标签。

7. 根据权利要求6所述的装置,其中,所述实体为企业;相应地,

所述实体属性数据包括企业信息和个人客户信息;

所述关系数据包括以下至少之一:企业与个人的对应关系、个人与个人的对应关系、企业与相关属性的对应关系、个人与相关属性的对应关系、企业与企业之间的对应关系。

8. 根据权利要求7所述的装置,其中,所述个人客户信息包括企业实控人信息与多个企业干系人信息;

所述处理单元,用于将所述多个企业干系人信息进行聚合后,得到干系人聚合特征;将实控人特征与干系人聚合特征关联到企业上,得到企业样本数据;对所述企业样本数据进行以下至少一种处理:异常值处理、缺失值处理、变量之间相关性的分析、类别变量的编码。

9. 根据权利要求6或8所述的装置,其中,所述图谱构建单元,用于:

以企业作为知识图谱的节点;

将处理过的企业信息、企业实控人信息以及企业干系人信息的聚合共同作为节点的属性;

将企业之间的归约关系作为知识图谱的关系;

删除掉知识图谱中存在的孤立节点。

10. 根据权利要求6所述的装置,其中,所述预测单元,用于执行以下步骤:

S1:使用真实标签已知的企业属性特征进行训练,得到欺诈预估模型local_classifier;

S2:从知识图谱中抽取真实标签已知的企业属性特征矩阵,并根据知识图谱中的节点关联计算训练数据集中的每个企业节点的一度邻居中的正样本的比例,将该值拼接到企业属性特征后,再次进行训练,得到加入邻居标签信息的欺诈预估模型relation_classifier;

S3:将标签未知的企业的属性特征输入S1中训练的模型,获得初步的欺诈风险概率pos_probability,将该概率值同样作为知识图谱中待预测企业节点的属性进行存储;

S4:设置预定义的最大迭代轮数N,迭代次数i初始化为1,待预估企业节点个数为M;N,i,M为正整数;

S5:计算每个待预测企业节点的不欺诈概率neg_probability=1-pos_probabiliy,并将pos_probabiliy和neg_probability做差值,得到信心度confidence,并将confidence的绝对值进行排序;

S6:选择前i*M/N个企业进行预分类,如果confidence大于0,则将该预测样本的预估标签置为正,如果confidence小于等于0,则将该预测样本的预估标签置为负,并写回知识图谱中的pred属性存储;

S7:对于每一个待预测的企业节点,计算其周围一度邻居的正样本比例,如果周围邻居节点在训练样本或者在上一轮确定了该测试节点的标签,则可加入计算,将计算结果拼接 to 该企业的属性数据;

S8:使用S2中relation_classifier进行分类,得到本轮的该节点的欺诈风险概率pos_probability,写回知识图谱中更新该属性值;

S9:迭代次数i+1,重复迭代S5、S6、S7、S8;其中,迭代结束标志为i>N或本轮预测结果与上一轮预测结果相同。

一种基于知识图谱的反欺诈方法及装置

技术领域

[0001] 本申请涉及反欺诈技术,尤其涉及一种基于知识图谱的反欺诈方法及装置。

背景技术

[0002] 传统银行业等放贷机构在评估调查申贷企业时需要耗费大量的人力和时间成本,导致企业融资周期长、融资成本高。许多小型企业在申请贷款时主动申报的资料中含有大量虚假信息,导致机构无法正确评估放贷风险。

发明内容

[0003] 为解决上述技术问题,本申请实施例提供了一种基于知识图谱的反欺诈方法及装置。

[0004] 本申请实施例提供的基于知识图谱的反欺诈方法,包括:

[0005] 从数据源中抽取实体、实体属性数据以及关系数据;

[0006] 对所述实体属性数据进行筛选与处理,并利用处理过的实体属性数据以及所述关系数据构建知识图谱,所述知识图谱包括第一类节点和第二类节点,所述第一类节点为已知标签的节点,所述第二类节点为待预测标签的节点;

[0007] 基于所述知识图谱,预测所述第二类节点的标签。

[0008] 在一实施方式中,所述实体为企业;相应地,

[0009] 所述实体属性数据包括企业信息和个人客户信息;

[0010] 所述关系数据包括以下至少之一:企业与个人的对应关系、个人与个人的对应关系、企业与相关属性的对应关系、个人与相关属性的对应关系、企业与企业的对应关系。

[0011] 在一实施方式中,构建知识图谱之前,所述方法还包括:

[0012] 对所述关系数据进行归约,使得每条关系对应到企业。

[0013] 在一实施方式中,所述个人客户信息包括企业实控人信息与多个企业干系人信息;

[0014] 所述对所述实体属性数据进行筛选与处理,包括:

[0015] 将所述多个企业干系人信息进行聚合后,得到干系人聚合特征;

[0016] 将实控人特征与干系人聚合特征关联到企业上,得到企业样本数据;

[0017] 对所述企业样本数据进行以下至少一种处理:异常值处理、缺失值处理、变量之间相关性的分析、类别变量的编码。

[0018] 在一实施方式中,所述利用处理过的实体属性数据以及所述关系数据构建知识图谱,包括:

[0019] 以企业作为知识图谱的节点;

[0020] 将处理过的企业信息、企业实控人信息以及企业干系人信息的聚合共同作为节点的属性;

[0021] 将企业之间的归约关系作为知识图谱的关系;

- [0022] 删除掉知识图谱中存在的孤立节点。
- [0023] 在一实施方式中,所述基于所述知识图谱,预测所述第二类节点的标签,包括:
- [0024] S1:使用真实标签已知的企业属性特征进行训练,得到欺诈预估模型local_classifier;
- [0025] S2:从知识图谱中抽取真实标签已知的企业属性特征矩阵,并根据知识图谱中的节点关联计算训练数据集中的每个企业节点的一度邻居中的正样本的比例,将该值拼接到企业属性特征后,再次进行训练,得到加入邻居标签信息的欺诈预估模型relation_classifier;
- [0026] S3:将标签未知的企业的属性特征输入S1中训练的模型,获得初步的欺诈风险概率pos_probability,将该概率值同样作为知识图谱中待预测企业节点的属性进行存储;
- [0027] S4:设置预定义的最大迭代轮数N,迭代次数i初始化为1,待预估企业节点个数为M;N,i,M为正整数;
- [0028] S5:计算每个待预测企业节点的不欺诈概率neg_probability=1-pos_probability,并将pos_probability和neg_probability做差值,得到信心度confidence,并将confidence的绝对值进行排序;
- [0029] S6:选择前i*M/N个企业进行预分类,如果confidence大于0,则将该预测样本的预估标签置为正,如果confidence小于等于0,则将该预测样本的预估标签置为负,并写回知识图谱中的pred属性存储;
- [0030] S7:对于每一个待预测的企业节点,计算其周围一度邻居的正样本比例,如果周围邻居节点在训练样本或者在上一轮确定了该测试节点的标签,则可加入计算,将计算结果拼接到该企业的属性数据;
- [0031] S8:使用S2中relation_classifier进行分类,得到本轮的该节点的欺诈风险概率pos_probability,写回知识图谱中更新该属性值;
- [0032] S9:迭代次数i+1,重复迭代S5、S6、S7、S8;其中,迭代结束标志为i>N或本轮预测结果与上一轮预测结果相同。
- [0033] 本申请实施例提供的基于知识图谱的反欺诈装置,包括:
- [0034] 抽取单元,用于从数据源中抽取实体、实体属性数据以及关系数据;
- [0035] 处理单元,用于对所述实体属性数据进行筛选与处理;
- [0036] 图谱构建单元,用于利用处理过的实体属性数据以及所述关系数据构建知识图谱,所述知识图谱包括第一类节点和第二类节点,所述第一类节点为已知标签的节点,所述第二类节点为待预测标签的节点;
- [0037] 预测单元,用于基于所述知识图谱,预测所述第二类节点的标签。
- [0038] 在一实施方式中,所述实体为企业;相应地,
- [0039] 所述实体属性数据包括企业信息和个人客户信息;
- [0040] 所述关系数据包括以下至少之一:企业与个人的对应关系、个人与个人的对应关系、企业与相关属性的对应关系、个人与相关属性的对应关系、企业与企业之间的对应关系。
- [0041] 在一实施方式中,所述装置还包括:
- [0042] 规约单元,用于对所述关系数据进行归约,使得每条关系对应到企业。
- [0043] 在一实施方式中,所述个人客户信息包括企业实控人信息与多个企业干系人信

息;

[0044] 所述处理单元,用于将所述多个企业干系人信息进行聚合后,得到干系人聚合特征;将实控人特征与干系人聚合特征关联到企业上,得到企业样本数据;对所述企业样本数据进行以下至少一种处理:异常值处理、缺失值处理、变量之间相关性的分析、类别变量的编码。

[0045] 在一实施方式中,所述图谱构建单元,用于:

[0046] 以企业作为知识图谱的节点;

[0047] 将处理过的企业信息、企业实控人信息以及企业干系人信息的聚合共同作为节点的属性;

[0048] 将企业之间的归约关系作为知识图谱的关系;

[0049] 删除掉知识图谱中存在的孤立节点。

[0050] 在一实施方式中,所述预测单元,用于执行以下步骤:

[0051] S1:使用真实标签已知的企业属性特征进行训练,得到欺诈预估模型`local_classifier`;

[0052] S2:从知识图谱中抽取真实标签已知的企业属性特征矩阵,并根据知识图谱中的节点关联计算训练数据集中的每个企业节点的一度邻居中的正样本的比例,将该值拼接到企业属性特征后,再次进行训练,得到加入邻居标签信息的欺诈预估模型`relation_classifier`;

[0053] S3:将标签未知的企业的属性特征输入S1中训练的模型,获得初步的欺诈风险概率`pos_probability`,将该概率值同样作为知识图谱中待预测企业节点的属性进行存储;

[0054] S4:设置预定义的最大迭代轮数 N ,迭代次数 i 初始化为1,待预估企业节点个数为 M ; N, i, M 为正整数;

[0055] S5:计算每个待预测企业节点的不欺诈概率`neg_probability` $=1-\text{pos_probability}$,并将`pos_probability`和`neg_probability`做差值,得到信心度`confidence`,并将`confidence`的绝对值进行排序;

[0056] S6:选择前 $i*M/N$ 个企业进行预分类,如果`confidence`大于0,则将该预测样本的预估标签置为正,如果`confidence`小于等于0,则将该预测样本的预估标签置为负,并写回知识图谱中的`pred`属性存储;

[0057] S7:对于每一个待预测的企业节点,计算其周围一度邻居的正样本比例,如果周围邻居节点在训练样本或者在上一轮确定了该测试节点的标签,则可加入计算,将计算结果拼接到该企业的属性数据;

[0058] S8:使用S2中`relation_classifier`进行分类,得到本轮的该节点的欺诈风险概率`pos_probability`,写回知识图谱中更新该属性值;

[0059] S9:迭代次数 $i+1$,重复迭代S5、S6、S7、S8;其中,迭代结束标志为 $i>N$ 或本轮预测结果与上一轮预测结果相同。

[0060] 本申请实施例的技术方案,能够利用企业关系图谱对高风险企业进行识别过滤。通过整合企业工商、企业干系人数据,同时考虑与目标企业发生关联的企业,最终将企业以及企业间关联关系描述出来。本申请实施例的技术方案有助于识别组团欺诈、团伙涉黑、骗贷等欺诈案件,能够全面评估申贷企业的风险状况,提前预防隐蔽的欺诈行为并阻断贷款

路径。除了能够识别企业欺诈风险外,构建的多种关系图谱还可对股东持股结构、涉诉案件、高管关系、亲属关系等方面进行可视化分析和挖掘。

附图说明

- [0061] 图1为本申请实施例提供的基于知识图谱的反欺诈方法的流程示意图;
[0062] 图2为本申请实施例提供的风险概率预测算法的逻辑图;
[0063] 图3为本申请实施例提供的基于知识图谱的反欺诈装置的结构组成示意图。

具体实施方式

[0064] 为便于理解本申请实施例的技术方案,以下对本申请实施例的相关技术进行说明。

[0065] 目前的信贷反欺诈实现路线可概括为以下四大技术手段:基于黑白名单、基于规则引擎、有监督的学习以及无监督的学习。

[0066] • 黑白名单是最简单原始的反欺诈手段,新申请客户和历史黑名单数据进行查询匹配,达到过滤筛查欺诈用户的目的。

[0067] • 规则引擎起源于基于规则的专家系统,用来模拟人的行为以实现计算机自动决策,是一种建立在对欺诈行为的特点与模式充分认知的基础上,针对单一或组合欺诈行为设计的启动和触发机制。

[0068] • 有监督学习是当下反欺诈检测中应用最为广泛的机器学习方法。该方法需要收集已知欺诈数据和正常数据用作训练集,训练出的机器学习模型通过对用户特征的抽象理解,分析特征间隐层关系,来填补并增强规则引擎无法覆盖的复杂欺诈行为。

[0069] • 无监督学习是近年来逐渐兴起的反欺诈策略。该种检测算法无需依赖任何标签来进行模型训练,通过关联分析和相似性分析,发现欺诈用户行为间的共性异常,创建聚类群组,并在一个或多个群组中发掘未知的欺诈行为。

[0070] 上述四种技术手段分别存在如下问题:1.黑白名单虽然简单易用,但积累用时较长,购买成本高昂。识别欺诈者的效果受制于黑名单规模和来源,且在时间维度上具有天然的滞后性,难以提前遏制欺诈案件。2.基于专家经验的规则引擎有着配置简单的优点,但规则的制定与更新基于业务经验性,存在一定误判的风险。尽管规则引擎能够识别新的欺诈者却无法检测新的欺诈模式。由于规则的作用时间有限,规则引擎需要花费大量运营资源、时间和费用来维护。3.当前广泛使用的有监督学习虽然避免了人为经验的干扰,但收集足够的训练数据和准确的标记数据却为有监督机器学习增加了一定局限性。大部分的机器学习模型,特别是金融行业普遍应用的逻辑回归模型需要较长的训练时间,因此难于应对变化多端的欺诈行为。除此以外,传统意义上的有监督机器学习模式多适用于独立分布的数据,即样本与样本间的特征不存在相互关联、相互依赖的情况。而反欺诈场景中,企业间的隐藏关联往往包含着未知的潜在信息,利用关联企业的信息去预测企业本身对传统有监督学习来说是一个挑战。4.无监督学习虽然不需要大量人工确定标签过程,但聚类结果仍然需要业务专家结合领域知识进行甄别,对于聚类的好坏没有明确的标准和评价。

[0071] 为解决上述问题,提出了本申请实施例的以下技术方案,本申请实施例的技术方案旨在结合已披露的企业欺诈记录,整合多个权威数据来源,主动构建企业间关系图谱,全

面评估未知目标企业经营状况,量化企业欺诈风险,帮助放贷机构快速制定风控策略。

[0072] 为了能够更加详尽地了解本申请实施例的特点与技术内容,下面结合附图对本申请实施例的实现进行详细阐述,所附附图仅供参考说明之用,并非用来限定本申请实施例。以下先对本申请实施例中涉及到的相关概念进行说明:

[0073] 实体:具有可区别性且独立存在的事物。本申请中构建的反欺诈图谱只包含一种实体,即企业。

[0074] 关系:实体之间的联系。如:“同实控人”、“同联系电话”。

[0075] 属性:属性是对实体和关系的描述。实体一般具有属性,比如企业的工商数据等。关系也可以有属性,比如关系上的权重。

[0076] 一度关联(一度邻居):与目标节点直接相连的节点。

[0077] 企业干系人:实控人、法人、高管、股东。

[0078] AUM:银行对客户的一种考量,衡量客户对银行的贡献度。

[0079] LightGBM(Light Gradient Boosting Machine),一个开源的实现GBDT(Gradient Boosting Decision Tree)算法的框架,支持高效率的并行训练。

[0080] 图1为本申请实施例提供的基于知识图谱的反欺诈方法的流程示意图,如图1所示,所述基于知识图谱的反欺诈方法包括以下步骤:

[0081] 步骤101:从数据源中抽取实体、实体属性数据以及关系数据。

[0082] 本申请中用到的所有数据源来自于机构提供的企业数据、个人客户数据以及外部三方数据。数据的抽取可分为实体、属性的抽取以及关系的抽取。在一可选实施方式中,数据的抽取时间范围确定在企业贷款申请时间处于t1时间到t2时间且有还款表现的企业中,例如:数据的抽取时间范围确定在企业贷款申请时间处于2018年1月到2018年12月且有还款表现的企业中。

[0083] A) 实体和属性的抽取

[0084] 本申请以企业粒度进行建模,每一个实体即是企业。实体属性由企业自身的属性信息以及企业相关个人客户的属性信息共同构成。其中,企业自身的属性信息(简称为企业数据,或者企业信息)包括但不限于企业的技术编号、工商数据、联系电话、注册地址、所属行业门类、成立日期等基础信息以及企业存款数据、转账数据、贷款数据。企业相关个人客户的属性信息(简称为个人客户数据,或者个人客户信息)包括但不限于个人技术编号、性别、年龄、学历、居住状况、职业、职务、职称、婚姻状况、子女状况等基础信息以及个人存款数据、贷款数据。



[0085] B) 关系的抽取

[0086] 抽取关系所涉及的数据表可汇总为以下五类:1.企业与个人的对应关系(实控关系表、高管关系表、法人关系表、投资控股关系表)。2.个人与个人的对应关系(直系亲属关系表、配偶关系表)。3.企业与相关属性的对应关系(企业地址关系表、企业电话号码关系表)。4.个人与相关属性的对应关系(个人地址关系表、个人电话号码关系表、个人设备使用关系表)。5.企业与企业的对应关系(企业担保关系表)。

[0087] 本申请实施例中,需要对所述关系数据进行归约,使得每条关系对应到企业。具体地,原始的企业关系信息来源多、数据异构、碎片化。为保证整体企业关系网络同构,即知识图谱实体统一,本申请将关系按照如下表1的方式进行归约,保证每条关系对应到企业本

身。

[0088]

关系	具体关系	表示及说明
企业干系人相同 (干系人包括实控人、法人、股东、高管)	C1、C2 两企业具有相同实控人	
	C1、C2 两企业具有相同法人	
	C1、C2 两企业具有相同股东	
	C1、C2 两企业具有相同高管	C1, C2 ∈ (企业), C1 ≠ C2, P ∈ (个人), r ∈ (实控人, 法人, 股东, 高管关系)
	C1 企业实控人在 C2 企业担任法人	

[0089]

	C1 企业实控人在 C2 企业担任股东	$C1, C2 \in (\text{企业}), C1 \neq C2,$ $P \in (\text{个人}),$ $r1,$ $r2 \in (\text{实控人, 法人, 股东, 高管关系}),$ $r1 \neq r2$
	C1 企业实控人在 C2 企业担任高管	
	C1 企业法人在 C2 企业担任股东	
	C1 企业法人在 C2 企业担任高管	
	C1 企业股东在 C2 企业担任高管	
企业干系人存在配偶或亲属关系	C1 企业任意干系人与 C2 企业任意干系人存在配偶关系	$C1 \xrightarrow{r1} (P1) \xrightarrow{r3} (P2) \xrightarrow{r2} C2$
	C1 企业任意干系人与 C2 企业任意干系人存在亲属关系	$C1, C2 \in (\text{企业}), C1 \neq C2,$ $P1, P2 \in (\text{个人}), P1 \neq P2,$ $r1,$ $r2 \in (\text{实控人, 法人, 股东, 高管关系})$ $r3 \in (\text{配偶, 亲属关系})$
企业相同联系方式	C1 企业与 C2 企业联系方式相同	$C1 \xrightarrow{r} (Attr) \xrightarrow{r} C2$
企业相同注册地址	C1 企业与 C2 企业注册地址相同	$C1, C2 \in (\text{企业}), C1 \neq C2,$ $Attr \in (\text{地址, 电话})$ $r \in (\text{拥有地址, 电话关系})$
企业干系人相同联系方式	C1 企业任意干系人与 C2 企业任意干系人使用相同手机号	$C1 \xrightarrow{r1} (P1) \xrightarrow{r3} (Attr) \xrightarrow{r4} (P2) \xrightarrow{r2} C2$
企业干系人相同通讯地址	C1 企业任意干系人与 C2 企业任意干系人使用相同通讯地址	$C1, C2 \in (\text{企业}), C1 \neq C2,$ $P1,$ $P2 \in (\text{个人}), P1 \neq P2,$ $Attr \in$ (地址, 电话) $r1, r2 \in$ $(\text{实控人, 法人, 股东, 高管关系})$ $r3, r4 \in (\text{拥有地址, 电话, 设备关系})$
企业干系人相同登录设备	C1 企业任意干系人与 C2 企业任意干系人使用相同登录设备	
企业相同担保	C1 企业与 C2 企业的担保公司相同	$C1 \xrightarrow{r} (C3) \xrightarrow{r} C2$ $C1, C2, C3 \in (\text{企业}), C1 \neq C2 \neq C3,$ $r \in$ (担保关系)

[0090] 表1

[0091] 步骤102:对所述实体属性数据进行筛选与处理。

[0092] A) 企业数据

[0093] 企业的属性数据来自于上述从数据源中抽取的企业信息。具体包括企业技术编号、工商数据、注册地址、所属行业门类、成立日期、注册日期等基础信息,以及企业存款数据、转账数据与贷款数据。其中,企业工商数据包括企业的注册资金金额、年检资产总额、客户利润总额、销售或营业收入、净资产总额五项。企业存款数据包括数据截取时刻企业存款余额和存款月、季、年积数。企业转账数据包括其一年内的总转账(转入、转出)次数与总转

账金额。企业贷款数据包括其一年内申贷次数、申贷被拒次数以及逾期情况(逾期本金、利息、天数)。

[0094] B) 企业干系人数据

[0095] 单纯使用企业相关数据对欺诈案件的预测不足,因此,本申请在使用企业属性数据的同时为每个企业匹配实控人及其他干系人的相关信息建立基于企业的多维特征数据,增强总体数据的表征能力。每个企业具有唯一实控人和多个其他干系人,而实控人与企业的关联程度较其他干系人相比更为密切。因此,单独将企业实控人的信息与企业信息拼接,并将企业其他实控人(即干系人)的信息进行聚合后对企业特征进行进一步的扩展。实控人的信息与其他干系人信息均来自于上述抽取的个人客户数据,具体包括个人技术编号、性别、年龄、学历、居住状况、职业、职务、职称、婚姻状况、子女状况以及个人存款数据、贷款数据。个人客户存款数据包括数据截取时刻个人存款余额和存款月、季、年积数,个人时点、月均以及年均AUM值。贷款数据包括其一年内申贷次数以及逾期情况(连续拖欠期数、逾期本金、利息、最大拖欠天数)。

[0096] 在对企业其他干系人进行聚合时,对不同变量选用的聚合函数包括:

[0097] -数值型变量:分别选取最大值,加和,中位数,均值

[0098] -类别型变量:选取众数

[0099] 最终,处理过的实控人特征与干系人聚合特征被关联到企业上,使得一个样本数据(企业)对应一条记录。之后对上述的企业样本数据以下至少一种处理:异常值处理、缺失值处理、变量之间相关性的分析、类别变量的编码。例如:将缺失率高达80%以上,或皮尔逊系数高于0.98的特征删除后,将剩余特征共同作为模型训练的企业属性特征。

[0100] 步骤103:利用处理过的实体属性数据以及所述关系数据构建知识图谱,所述知识图谱包括第一类节点和第二类节点,所述第一类节点为已知标签的节点,所述第二类节点为待预测标签的节点。

[0101] 本申请实施例中的知识图谱也称为反欺诈企业知识图谱,知识图谱的具体构建过程如下:

[0102] A) 以企业作为知识图谱的节点。

[0103] 具体地,以提交信贷申请的企业作为图谱的节点实体,其中用于建立关系的人或物在关系构建过程中被归约掉;

[0104] B) 将处理过的企业信息、企业实控人信息以及企业干系人信息的聚合共同作为节点的属性。

[0105] 具体地,将步骤102中处理过的企业的基本信息、实控人基本信息以及干系人基本信息的聚合共同作为实体的属性。

[0106] C) 将企业之间的归约关系作为知识图谱的关系。

[0107] 具体地,将步骤101中企业之间的各种归约关系作为图谱的关系。

[0108] D) 删除掉知识图谱中存在的孤立节点。

[0109] 本申请实施例中,由于历史数据中缺少对企业欺诈的准确定义,选择根据机构内部或相关部门披露的企业及企业干系人在一段时间内的严重违规记录建立企业欺诈标签,并将该标签作为目标变量。相关企业和个人严重违规数据包括但不限于:1.机构内部欺诈系统中的欺诈名单;2.企业和个人的行政违法记录及犯罪嫌疑人黑名单;3.跨平台数借贷

数大于N笔,N例如为4。

[0110] 步骤104:基于所述知识图谱,预测所述第二类节点的标签。

[0111] 本申请实施例中,基于所述知识图谱,预测所述第二类节点的标签可以定义成如下问题:基于步骤103构建的企业关系图谱记为G,在G上所有的节点记为V,X为步骤1中企业的自身属性向量,V_k为G中已知标签节点,V_u为企业图谱G中待预测的节点。已知图谱结构G、所有节点(企业)所携带的属性X和部分已知标签节点V_k,利用以上信息预测V_u的标签类型。相应的伪代码如下所示:

[0112]

classify (*V,E,X,VK*)=

//local_classifier = uses attributes and relations, *relation_classifier* = classifier that uses only attributes

// n = number of iterations,

for each node *vi* \in *Vu* **do**

(yi, confi) \leftarrow *local_classifier*(*xi*)

for *h* = 1 **to** *n* **do**

m \leftarrow |*Vu*|·(*h/n*)

[0113] *Y'* \leftarrow *VK* \cup {*yi*|*vi* \in *Vu* \wedge *sort*(|*confi*|) \leq *m*}

for each node *vi* \in *Vu* **do**

fi \leftarrow *neighbor_pos_probability*(*V,E,Y'*)

for each node *vi* \in *Vu* **do**

(yi, confi) \leftarrow *relation_classifier*(*xi, fi*)

return {*yi*|*vi* \in *Vu*}

[0114] 参照图2,上述伪代码可以实现如下步骤:

[0115] S1:使用真实标签已知的企业属性特征进行训练,通过微软开源的LightGBM框架进行训练,得到一个只依赖于企业自身属性的欺诈预估模型*local_classifier*;

[0116] S2:从知识图谱中抽取真实标签已知的企业属性特征矩阵,并根据知识图谱中的节点关联计算训练数据集中的每个企业节点的一度邻居中的正样本的比例,将该值拼接企业属性特征后,再次通过LightGBM框架进行训练,得到加入邻居标签信息的欺诈预估模型*relation_classifier*;

[0117] S3:将标签未知的企业的属性特征输入S1中训练的模型,获得初步的欺诈风险概率*pos_probability*,将该概率值同样作为知识图谱中待预测企业节点的属性进行存储;

[0118] S4:设置预定义的最大迭代轮数N,迭代次数*i*初始化为1,待预估企业节点个数为M;N,*i*,M为正整数;

[0119] S5:计算每个待预测企业节点的不欺诈概率*neg_probability*=1-*pos_*

probabiliy,并将pos_probabiliy和neg_probability做差值,得到信心度confidence,并将confidence的绝对值进行排序;

[0120] S6:选择前 $i \times M/N$ 个企业进行预分类,如果confidence大于0,则将该预测样本的预估标签置为正,如果confidence小于等于0,则将该预测样本的预估标签置为负,并写回知识图谱中的pred属性存储;

[0121] S7:对于每一个待预测的企业节点,计算其周围一度邻居的正样本比例,如果周围邻居节点在训练样本或者在上一轮确定了该测试节点的标签,则可加入计算,将计算结果拼接到该企业的属性数据;

[0122] S8:使用S2中relation_classifier进行分类,得到本轮的该节点的欺诈风险概率pos_probability,写回知识图谱中更新该属性值;

[0123] S9:迭代次数 $i+1$,重复迭代S5、S6、S7、S8;其中,迭代结束标志为 $i > N$ 或本轮预测结果与上一轮预测结果相同。

[0124] 需要说明的是,本申请实施例中的LightGBM算法可被替换为任意可输出概率的机器学习算法,包括但不限于Logistic Regression,Random Forest,XGBoost,GBDT等算法。

[0125] 图3为本申请实施例提供的基于知识图谱的反欺诈装置的结构组成示意图,如图3所示,所述基于知识图谱的反欺诈装置包括:

[0126] 抽取单元301,用于从数据源中抽取实体、实体属性数据以及关系数据;

[0127] 处理单元302,用于对所述实体属性数据进行筛选与处理;

[0128] 图谱构建单元303,用于利用处理过的实体属性数据以及所述关系数据构建知识图谱,所述知识图谱包括第一类节点和第二类节点,所述第一类节点为已知标签的节点,所述第二类节点为待预测标签的节点;

[0129] 预测单元304,用于基于所述知识图谱,预测所述第二类节点的标签。

[0130] 在一实施方式中,所述实体为企业;相应地,

[0131] 所述实体属性数据包括企业信息和个人客户信息;

[0132] 所述关系数据包括以下至少之一:企业与个人的对应关系、个人与个人的对应关系、企业与相关属性的对应关系、个人与相关属性的对应关系、企业与企业的对应关系。

[0133] 在一实施方式中,所述装置还包括:

[0134] 规约单元(图中未示出),用于对所述关系数据进行归约,使得每条关系对应到企业。

[0135] 在一实施方式中,所述个人客户信息包括企业实控人信息与多个企业干系人信息;

[0136] 所述处理单元302,用于将所述多个企业干系人信息进行聚合后,得到干系人聚合特征;将实控人特征与干系人聚合特征关联到企业上,得到企业样本数据;对所述企业样本数据进行以下至少一种处理:异常值处理、缺失值处理、变量之间相关性的分析、类别变量的编码。

[0137] 在一实施方式中,所述图谱构建单元303,用于:

[0138] 以企业作为知识图谱的节点;

[0139] 将处理过的企业信息、企业实控人信息以及企业干系人信息的聚合共同作为节点的属性;

- [0140] 将企业之间的归约关系作为知识图谱的关系;
- [0141] 删除掉知识图谱中存在的孤立节点。
- [0142] 在一实施方式中,所述预测单元304,用于执行以下步骤:
- [0143] S1:使用真实标签已知的企业属性特征进行训练,得到欺诈预估模型local_classifier;
- [0144] S2:从知识图谱中抽取真实标签已知的企业属性特征矩阵,并根据知识图谱中的节点关联计算训练数据集中的每个企业节点的一度邻居中的正样本的比例,将该值拼接到企业属性特征后,再次进行训练,得到加入邻居标签信息的欺诈预估模型relation_classifier;
- [0145] S3:将标签未知的企业的属性特征输入S1中训练的模型,获得初步的欺诈风险概率pos_probability,将该概率值同样作为知识图谱中待预测企业节点的属性进行存储;
- [0146] S4:设置预定义的最大迭代轮数N,迭代次数i初始化为1,待预估企业节点个数为M;N,i,M为正整数;
- [0147] S5:计算每个待预测企业节点的不欺诈概率neg_probability=1-pos_probability,并将pos_probability和neg_probability做差值,得到信心度confidence,并将confidence的绝对值进行排序;
- [0148] S6:选择前i*M/N个企业进行预分类,如果confidence大于0,则将该预测样本的预估标签置为正,如果confidence小于等于0,则将该预测样本的预估标签置为负,并写回知识图谱中的pred属性存储;
- [0149] S7:对于每一个待预测的企业节点,计算其周围一度邻居的正样本比例,如果周围邻居节点在训练样本或者在上一轮确定了该测试节点的标签,则可加入计算,将计算结果拼接到该企业的属性数据;
- [0150] S8:使用S2中relation_classifier进行分类,得到本轮的该节点的欺诈风险概率pos_probability,写回知识图谱中更新该属性值;
- [0151] S9:迭代次数i+1,重复迭代S5、S6、S7、S8;其中,迭代结束标志为i>N或本轮预测结果与上一轮预测结果相同。
- [0152] 本领域技术人员应当理解,图3所示的基于知识图谱的反欺诈装置中的各单元的实现功能可参照前述基于知识图谱的反欺诈方法的相关描述而理解。图3所示的基于知识图谱的反欺诈装置中的各单元的功能可通过运行于处理器上的程序而实现,也可通过具体的逻辑电路而实现。
- [0153] 本申请实施例所记载的技术方案之间,在不冲突的情况下,可以任意组合。
- [0154] 在本申请所提供的几个实施例中,应该理解到,所揭露的方法和智能设备,可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的,例如,所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,如:多个单元或组件可以结合,或可以集成到另一个系统,或一些特征可以忽略,或不执行。另外,所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口,设备或单元的间接耦合或通信连接,可以是电性的、机械的或其它形式的。
- [0155] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的,作为单元显示的部件可以是、或也可以不是物理单元,即可以位于一个地方,也可以分布到多个网络单

元上;可以根据实际的需要选择其中的部分或全部单元来实现本实施例方案的目的。

[0156] 另外,在本申请各实施例中的各功能单元可以全部集成在一个第二处理单元中,也可以是各单元分别单独作为一个单元,也可以两个或两个以上单元集成在一个单元中;上述集成的单元既可以采用硬件的形式实现,也可以采用硬件加软件功能单元的形式实现。

[0157] 以上所述,仅为本申请的具体实施方式,但本申请的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本申请揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本申请的保护范围之内。

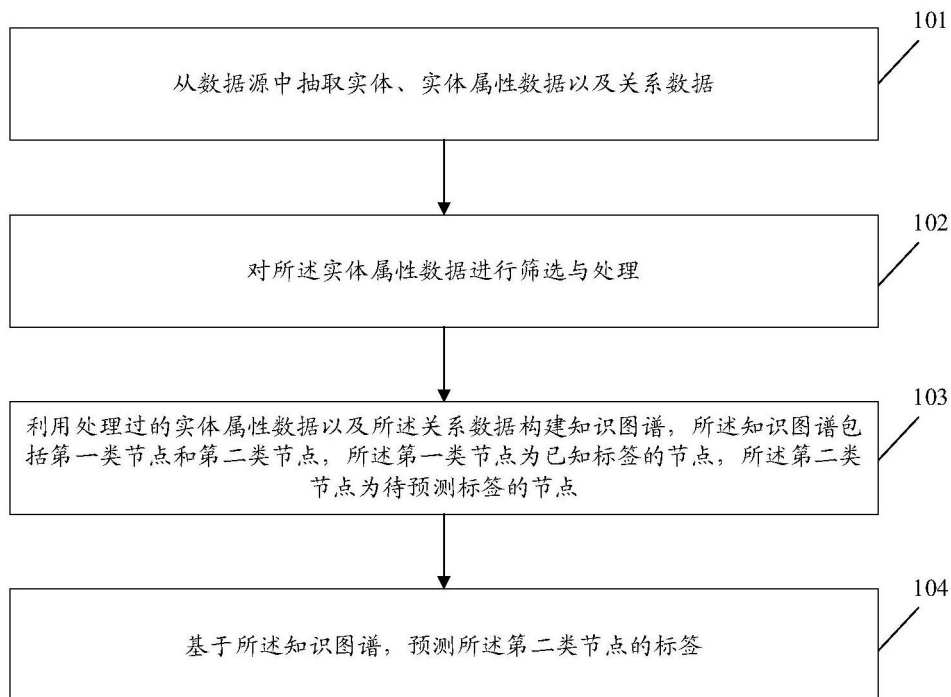


图1

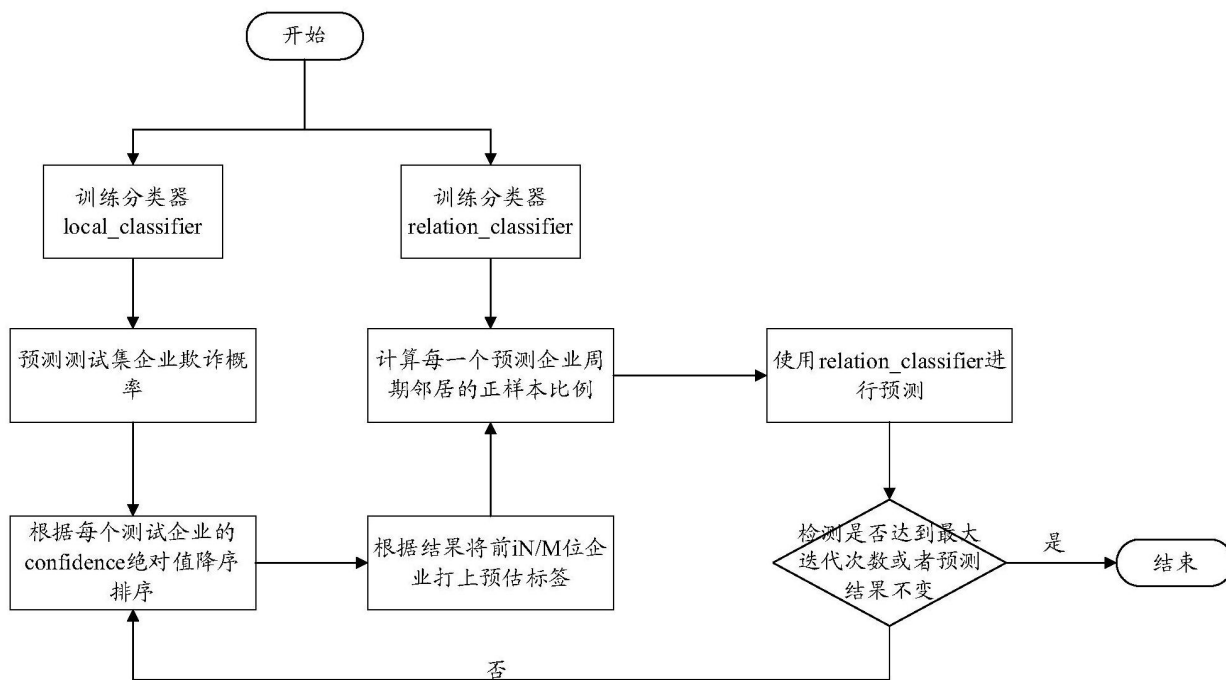


图2

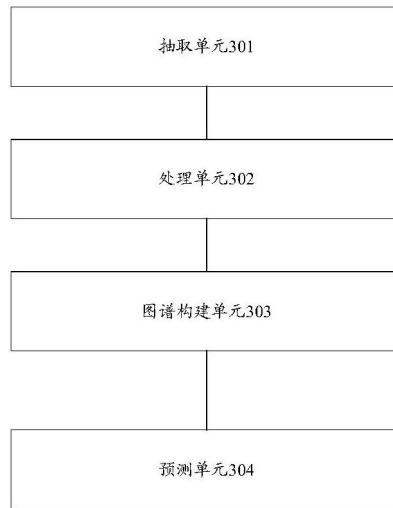


图3