(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116506206 A
(43)申请公布日 2023.07.28

(21)申请号 202310542761.9

(22)申请日 2023.05.15

(71)申请人 东南大学
地址 210096 江苏省南京市玄武区四牌楼2号

(72)发明人 陈亮 宋宇波

(74)专利代理机构 南京众联专利代理有限公司 32206
专利代理师 叶倩

(51)Int.Cl.
H04L 9/40(2022.01)
G06F 21/62(2013.01)
G06F 21/60(2013.01)
G06F 21/31(2013.01)
G06F 21/32(2013.01)
G06F 21/44(2013.01)
G06F 18/243(2023.01)

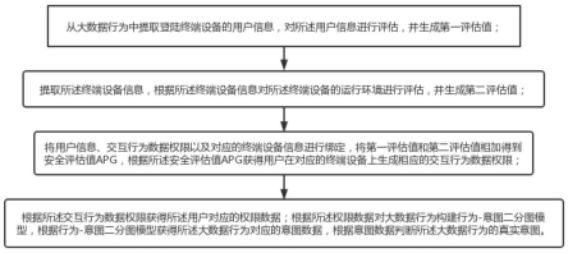
权利要求书3页 说明书12页 附图2页

(54)发明名称

基于零信任网络用户的大数据行为分析方法及系统

(57)摘要

本发明公开了一种基于零信任网络用户的大数据行为分析方法及系统，应用于服务器中，包括：从大数据行为中提取登录终端设备的用户信息，对所述用户信息进行评估，并生成第一评估值；根据所述终端设备信息对所述终端设备的运行环境进行评估，并生成第二评估值；将第一评估值和第二评估值相加得到安全评估值APG，根据所述安全评估值APG获得用户在对应的终端设备上生成相应的交互行为数据权限；根据所述交互行为数据权限获得所述用户对应的权限数据构建行为-意图二分图模型，根据行为-意图二分图模型获得所述大数据行为对应的意图数据，根据意图数据判断所述大数据行为的真实意图。



CN 116506206 A

1.基于零信任网络用户的大数据行为分析方法,应用于服务器中,其特征在于,包括如下步骤:

S1:从大数据行为中提取登录终端设备的用户信息,对所述用户信息进行评估,并生成第一评估值;

S2:提取终端设备信息,根据所述终端设备信息对所述终端设备的运行环境进行评估,并生成第二评估值;

S3:将用户信息以及用户信息对应的终端设备信息进行绑定,将步骤S1获得的第一评估值和步骤S2获得的第二评估值相加得到安全评估值APG,根据所述安全评估值APG获得用户在对应终端设备上生成相应的交互行为数据权限;

S4:根据步骤S3获得的交互行为数据权限获得所述用户对应的权限数据;根据所述权限数据对大数据行为构建行为-意图二分图模型,根据行为-意图二分图模型获得所述大数据行为对应的意图数据,根据意图数据判断所述大数据行为的真实意图。

2.根据权利要求1所述的基于零信任网络用户的大数据行为分析方法,其特征在于:所述步骤S1中的用户信息包括账号身份认证信息、图像身份认证信息、音频身份认证信息、指纹身份认证信息中任意一种或至少两种组合身份认证信息。

3.根据权利要求2所述的基于零信任网络用户的大数据行为分析方法,其特征在于:所述步骤S1中生成第一评估值具体包括:

获取登录终端设备的账号身份认证信息,根据所述账号身份认证信息与预设的用户信息进行身份识别,判断账号身份认证信息是否通过验证;

若所述账号身份认证信息通过验证,则获取对应的用户在当前所述终端设备下的安全等级;将所述用户在当前所述终端设备下的安全等级标记为用户安全等级,对所述用户安全等级赋予相应数值,将所述用户安全等级赋予相应数值标记为AQ;

根据所述预设的用户信息,获得所述预设的用户信息对应的预设用户安全等级,根据所述预设用户安全等级获得所述预设用户安全等级赋予相应数值标记YQ,其中YQ≥AQ;

接收终端设备发起的再次身份认证的请求,将身份认证的请求对应的身份认证条件发送至终端设备,根据终端设备反馈本次身份认证条件对应的用户信息与预设的用户信息进行身份识别分析,若终端设备反馈本次身份认证条件对应的用户信息与预设的用户信息一致,则通过本次认证,更新用户在当前所述终端设备下的安全等级以及对应的安全赋予相应数值加1,并更新安全等级赋予相应数值AQ;

其中,所述身份认证的请求包括图像身份认证、音频身份认证、指纹身份认证中一种或多种组合身份认证的请求;

将所述用户安全等级赋予相应数值和所述预设用户安全等级赋予相应数值的比值标记为第一评估值PG1,所述第一评估值PG1为小于等于1的值;

重复操作身份认证的请求,更新第一评估值PG1。

4.根据权利要求3所述的基于零信任网络用户的大数据行为分析方法,其特征在于:所述第一评估值PG1的分析具体为:

将所述第一评估值PG1代入安全梯度参考值Ph1和Ph2进行比对分析,其中Ph1＜Ph2;

若第一评估值PG1大于或等于安全梯度参考值Ph2时,则将用户信息对应的交互行为数据权限标记为高级交互权限;

若第一评估值PG1小于安全梯度参考值Ph2,且安全评估值APG大于或等于安全梯度参考值Ph1时,则将用户信息对应的交互行为数据权限标记为中级交互权限;

若第一评估值PG1小于安全梯度参考值Ph1时,则将用户信息对应的交互行为数据权限标记为低级交互权限。

5.根据权利要求4所述的基于零信任网络用户的大数据行为分析方法,其特征在于:所述步骤S2中终端设备信息包括第一终端设备的设备ID、设备登录时间和设备登录位置;

将所述设备ID、设备登录时间和设备登录位置的安全等级分别赋予相应数值,分别标记为R1、R2和R3;其中R1＞R2＞R3;

若所述设备ID、设备登录时间和设备登录位置未发生变化,则对所述设备ID、设备登录时间和设备登录位置的安全等级赋值分别为R1、R2、R3;

将所述设备ID、设备登录时间和设备登录位置对应的安全等级赋值相加累计为第二评估值PG2,PG2＝R1+R2+R3;

若所述设备ID、设备登录时间和设备登录位置发生变化,则对改变的所述设备ID、设备登录时间或设备登录位置的安全等级赋值分别为a1R1、a2R2、a3R3;

其中,a1+a2+a3＝1,a1、a2以及a3为大于0且小于1的权重;a1为所述设备ID的安全等级赋值R1的权重;a2为设备登录时间的安全等级赋值R2的权重;a3为设备登录位置发生变化的安全等级赋值R3的权重;

将所述设备ID、设备登录时间和设备登录位置对应的安全等级赋值相加累计为第二评估值PG2,PG2＝a1R1+a2R2+a3R3。

6.根据权利要求5所述的基于零信任网络用户的大数据行为分析方法,其特征在于:根据第一评估值和第二评估值相乘得到安全评估值APG,将所述安全评估值APG代入安全梯度参考值Ph1和Ph2进行比对分析,其中Ph1＜Ph2;

将所述第一评估值PG1代入安全梯度参考值Ph1和Ph2进行比对分析,其中Ph1＜Ph2;

若安全评估值APG大于或等于安全梯度参考值Ph2时,则将用户信息对应的交互行为数据权限标记为高级交互权限;

若安全评估值APG小于安全梯度参考值Ph2,且安全评估值APG大于或等于安全梯度参考值Ph1时,则将用户信息对应的交互行为数据权限标记为中级交互权限;

若安全评估值APG小于安全梯度参考值Ph1时,则将用户信息对应的交互行为数据权限标记为低级交互权限。

7.根据权利要求6所述的基于零信任网络用户的大数据行为分析方法,其特征在于:所述步骤S4中,根据所述交互行为数据权限获得所述用户对应的权限数据集;所述权限数据集包括n个意图数据,所述意图数据为所述大数据行为的关联数据。

8.根据权利要求7所述的基于零信任网络用户的大数据行为分析方法,其特征在于:所述步骤S4中,根据行为-意图二分图模型获得所述大数据行为对应的意图数据具体为:

行为-意图二分图模型表示为G＝(V,S,E),其中V表示数据交互系统中请求接入的大数据行为集合,S表示大数据行为对应的意图数据集合,共有m个大数据行为和n个意图数据,E表示大数据行为和意图数据之间可选链路的集合,可选链路是二分图中的边e＝(v,s),e∈E,v∈V,s∈S,每条可选链路均具有权值$l_{m,n}$,权值$l_{m,n}$为可选链路的匹配数据,通过匹配数据将大数据行为与意图数据之间进行数字关联。

9.根据权利要求8所述的基于零信任网络用户的大数据行为分析方法，其特征在于：所述步骤S4中，在交互行为数据权限下，根据意图数据判断所述大数据行为的真实意图具体为：

意图数据包括b个数据包x，以及每个所述数据包x相对应的浏览时间t，将与数据包x相对应的浏览时间t之和标记为表现系数z；统计b个数据包x的表现系数z_b，将表现系数z_b中最大的表现系数z1对应的数据包x作为意图数据的意图信号z；根据行为-意图二分图模型获得所述意图数据对应的匹配数据$l_{m,n}$；意图信号z与对应的匹配数据$l_{m,n}$的乘积标记为意图预测值；

将权限数据集内最大的意图预测值对应的意图数据作为大数据行为的真实意图；若意图预测值数量为至少两个时，则任意确定一个意图预测值，将意图预测值对应的意图数据作为大数据行为的真实意图。

10.基于零信任网络用户的大数据行为分析系统，应用于服务器中，其特征在于：所述服务器包括数据采集模块、数据分析模块、安全评估确定模块、交互权限确定模块、数据存储模块，模块间信号相互传递；

所述数据采集模块：获取登录终端设备的用户信息和终端设备信息，并将所述用户信息和终端设备信息发送至数据分析模块；

所述数据分析模块，对所述用户信息进行评估，并生成第一评估值，并将用户信息和对应的第一评估值存储在数据存储模块；

所述用户信息包括账号身份认证信息、图像身份认证信息、音频身份认证信息、指纹身份认证信息中任意一种或至少两种组合身份认证信息；

所述数据分析模块，提取所述终端设备信息，根据所述终端设备信息对所述终端设备的运行环境进行评估，并生成第二评估值，并终端设备信息和对应的第二评估值存储在数据存储模块；

所述安全评估确定模块，将用户信息以及对应的终端设备信息进行绑定，将第一评估值和第二评估值相加得到安全评估值APG；

所述交互权限确定模块，根据所述安全评估值APG获得用户在对应的终端设备上生成相应的交互行为数据权限，并将安全评估值APG和对应的交互行为数据权限存储在数据存储模块。

基于零信任网络用户的大数据行为分析方法及系统

技术领域

[0001] 本发明属于零信任网络领域，涉及用户大数据分析技术，具体涉及一种基于零信任网络用户的大数据行为分析方法及系统。

背景技术

[0002] 零信任安全核心思想是默认情况下不应该信任网络内部和外部的任何人/设备/系统，需要基于认证和授权机制，重构网络安全的信任基础。零信任安全模型假设攻击者可能出现在企业内部网络，企业内部网络基础设施与其它外部网络一样，面临同样的安全威胁，也容易受到攻击破坏，并不具有更高的可信度。在这种情况下，企业必须不断地分析和评估其内部网络和业务功能面临的安全风险，提升网络安全防护能力来降低风险。

[0003] 在零信任中，通常涉及将数据、计算和应用程序等网资源的访问权限最小化，只对那些必须用户和资产开启访问权限进行授权访问，并持续对每个访问请求者的身份和安全状态进行身份验证和授权，才能访问网络资源。

[0004] 在这种情况下，任何异常的行为都将被视为潜在的攻击，并受到相应的处理。但是其存在的问题就是，缺少对用户行为的风险评定，进而缺乏对风险等级高的用户行为进行合理阻断的方法。

[0005] 鉴于此，本发明提出一种基于零信任网络用户的大数据行为分析方法及系统。

发明内容

[0006] 本发明正是针对现有技术中存在的问题，提供一种基于零信任网络用户的大数据行为分析方法及系统，应用于服务器中，包括：从大数据行为中提取登录终端设备的用户信息，对所述用户信息进行评估，并生成第一评估值；根据所述终端设备信息对所述终端设备的运行环境进行评估，并生成第二评估值；将第一评估值和第二评估值相加得到安全评估值APG，根据所述安全评估值APG获得用户在对应的终端设备上生成相应的交互行为数据权限；根据所述交互行为数据权限获得所述用户对应的权限数据构建行为-意图二分图模型，根据行为-意图二分图模型获得所述大数据行为对应的意图数据，根据意图数据判断所述大数据行为的真实意图。

[0007] 为了实现上述目的，本发明采取的技术方案是：基于零信任网络用户的大数据行为分析方法，应用于服务器中，包括如下步骤：

[0008] S1：从大数据行为中提取登录终端设备的用户信息，对所述用户信息进行评估，并生成第一评估值；

[0009] S2：提取终端设备信息，根据所述终端设备信息对所述终端设备的运行环境进行评估，并生成第二评估值；

[0010] S3：将用户信息以及用户信息对应的终端设备信息进行绑定，将步骤S1获得的第一评估值和步骤S2获得的第二评估值相加得到安全评估值APG，根据所述安全评估值APG获得用户在对应终端设备上生成相应的交互行为数据权限；

[0011] S4:根据步骤S3获得的交互行为数据权限获得所述用户对应的权限数据;根据所述权限数据对大数据行为构建行为-意图二分图模型,根据行为-意图二分图模型获得所述大数据行为对应的意图数据,根据意图数据判断所述大数据行为的真实意图。

[0012] 作为本发明的一种改进,所述步骤S1中的用户信息包括账号身份认证信息、图像身份认证信息、音频身份认证信息、指纹身份认证信息中任意一种或至少两种组合身份认证信息。

[0013] 作为本发明的一种改进,所述步骤S1中生成第一评估值具体包括:

[0014] 获取登录终端设备的账号身份认证信息,根据所述账号身份认证信息与预设的用户信息进行身份识别,判断账号身份认证信息是否通过验证;

[0015] 若所述账号身份认证信息通过验证,则获取对应的用户在当前所述终端设备下的安全等级;将所述用户在当前所述终端设备下的安全等级标记为用户安全等级,对所述用户安全等级赋予相应数值,将所述用户安全等级赋予相应数值标记为AQ;

[0016] 根据所述预设的用户信息,获得所述预设的用户信息对应的预设用户安全等级,根据所述预设用户安全等级获得所述预设用户安全等级赋予相应数值标记YQ,其中YQ≥AQ;

[0017] 接收终端设备发起的再次身份认证的请求,将身份认证的请求对应的身份认证条件发送至终端设备,根据终端设备反馈本次身份认证条件对应的用户信息与预设的用户信息进行身份识别分析,若终端设备反馈本次身份认证条件对应的用户信息与预设的用户信息一致,则通过本次认证,更新用户在当前所述终端设备下的安全等级以及对应的安全赋予相应数值加1,并更新安全等级赋予相应数值AQ;

[0018] 其中,所述身份认证的请求包括图像身份认证、音频身份认证、指纹身份认证中一种或多种组合身份认证的请求;

[0019] 将所述用户安全等级赋予相应数值和所述预设用户安全等级赋予相应数值的比值标记为第一评估值PG1,所述第一评估值PG1为小于等于1的值;

[0020] 重复操作身份认证的请求,更新第一评估值PG1。

[0021] 作为本发明的另一种改进,所述第一评估值PG1的分析具体为:

[0022] 将所述第一评估值PG1代入安全梯度参考值Ph1和Ph2进行比对分析,其中Ph1＜Ph2;

[0023] 若第一评估值PG1大于或等于安全梯度参考值Ph2时,则将用户信息对应的交互行为数据权限标记为高级交互权限;

[0024] 若第一评估值PG1小于安全梯度参考值Ph2,且安全评估值APG大于或等于安全梯度参考值Ph1时,则将用户信息对应的交互行为数据权限标记为中级交互权限;

[0025] 若第一评估值PG1小于安全梯度参考值Ph1时,则将用户信息对应的交互行为数据权限标记为低级交互权限。

[0026] 作为本发明的另一种改进,所述步骤S2中终端设备信息包括第一终端设备的设备I D、设备登录时间和设备登录位置;

[0027] 将所述设备I D、设备登录时间和设备登录位置的安全等级分别赋予相应数值,分别标记为R1、R2和R3;其中R1＞R2＞R3;

[0028] 若所述设备I D、设备登录时间和设备登录位置未发生变化,则对所述设备I D、设

备登录时间和设备登录位置的安全等级赋值分别为R1、R2、R3；

[0029] 将所述设备I D、设备登录时间和设备登录位置对应的安全等级赋值相加累计为第二评估值PG2，PG2＝R1+R2+R3；

[0030] 若所述设备I D、设备登录时间和设备登录位置发生变化，则对改变的所述设备I D、设备登录时间或设备登录位置的安全等级赋值分别为a1 R1、a2R2、a3R3；

[0031] 其中，a1+a2+a3＝1，a1、a2以及a3为大于0且小于1的权重；a1为所述设备I D的安全等级赋值R1的权重；a2为设备登录时间的安全等级赋值R2的权重；a3为设备登录位置发生变化的安全等级赋值R3的权重；

[0032] 将所述设备I D、设备登录时间和设备登录位置对应的安全等级赋值相加累计为第二评估值PG2，PG2＝a1 R1+a2R2+a3R3。

[0033] 作为本发明的又一种改进，根据第一评估值和第二评估值相乘得到安全评估值APG，将所述安全评估值APG代入安全梯度参考值Ph1和Ph2进行比对分析，其中Ph1＜Ph2；

[0034] 将所述第一评估值PG1代入安全梯度参考值Ph1和Ph2进行比对分析，其中Ph1＜Ph2；

[0035] 若安全评估值APG大于或等于安全梯度参考值Ph2时，则将用户信息对应的交互行为数据权限标记为高级交互权限；

[0036] 若安全评估值APG小于安全梯度参考值Ph2，且安全评估值APG大于或等于安全梯度参考值Ph1时，则将用户信息对应的交互行为数据权限标记为中级交互权限；

[0037] 若安全评估值APG小于安全梯度参考值Ph1时，则将用户信息对应的交互行为数据权限标记为低级交互权限。

[0038] 作为本发明的又一种改进，所述步骤S4中，根据所述交互行为数据权限获得所述用户对应的权限数据集；所述权限数据集包括n个意图数据，所述意图数据为所述大数据行为的关联数据。

[0039] 作为本发明的更进一步改进，所述步骤S4中，根据行为-意图二分图模型获得所述大数据行为对应的意图数据具体为：

[0040] 行为-意图二分图模型表示为G＝(V,S,E)，其中V表示数据交互系统中请求接入的大数据行为集合，S表示大数据行为对应的意图数据集合，共有m个大数据行为和n个意图数据，E表示大数据行为和意图数据之间可选链路的集合，可选链路是二分图中的边e＝(v,s)，e∈E，v∈V，s∈S，每条可选链路均具有权值$l_{m,n}$，权值$l_{m,n}$为可选链路的匹配数据，通过匹配数据将大数据行为与意图数据之间进行数字关联。

[0041] 作为本发明的更进一步改进，所述步骤S4中，在交互行为数据权限下，根据意图数据判断所述大数据行为的真实意图具体为：

[0042] 意图数据包括b个数据包x，以及每个所述数据包x相对应的浏览时间t，将与数据包x相对应的浏览时间t之和标记为表现系数z；统计b个数据包x的表现系数z_b，将表现系数z_b中最大的表现系数z1对应的数据包x作为意图数据的意图信号z；根据行为-意图二分图模型获得所述意图数据对应的匹配数据$l_{m,n}$；意图信号z与对应的匹配数据$l_{m,n}$的乘积标记为意图预测值；

[0043] 将权限数据集内最大的意图预测值对应的意图数据作为大数据行为的真实意图；若意图预测值数量为至少两个时，则任意确定一个意图预测值，将意图预测值对应的意图

数据作为大数据行为的真实意图。

[0044] 为了实现上述目的，本发明还采取的技术方案是：基于零信任网络用户的大数据行为分析系统，应用于服务器中，其特征在于：所述服务器包括数据采集模块、数据分析模块、安全评估确定模块、交互权限确定模块、数据存储模块，模块间信号相互传递；

[0045] 所述数据采集模块：获取登录终端设备的用户信息和终端设备信息，并将所述用户信息和终端设备信息发送至数据分析模块；

[0046] 所述数据分析模块，对所述用户信息进行评估，并生成第一评估值，并将用户信息和对应的第一评估值存储在数据存储模块；

[0047] 所述用户信息包括账号身份认证信息、图像身份认证信息、音频身份认证信息、指纹身份认证信息中任意一种或至少两种组合身份认证信息；

[0048] 所述数据分析模块，提取所述终端设备信息，根据所述终端设备信息对所述终端设备的运行环境进行评估，并生成第二评估值，并终端设备信息和对应的第二评估值存储在数据存储模块；

[0049] 所述安全评估确定模块，将用户信息以及对应的终端设备信息进行绑定，将第一评估值和第二评估值相加得到安全评估值APG；

[0050] 所述交互权限确定模块，根据所述安全评估值APG获得用户在对应的终端设备上生成相应的交互行为数据权限，并将安全评估值APG和对应的交互行为数据权限存储在数据存储模块。

[0051] 与现有技术相比，本发明具有的有益效果：本发明用于零信任网络用户的安全评估，首先从大数据行为中提取用户信息和终端设备信息，并将其绑定到交互行为数据权限中，生成安全评估值APG，并根据APG获得用户在对应终端设备上的交互行为数据权限，使用该权限数据构建行为-意图二分图模型来判断大数据行为的真实意图。

附图说明

[0052] 图1为本发明的零信任网络用户的大数据行为分析系统示意图；

[0053] 图2为本发明的零信任网络用户的大数据行为分析方法流程图；

[0054] 图3为本发明的二分图匹配模型示意图。

[0055] 图中：1、数据采集模块；2、数据分析模块；3、安全评估确定模块；4、交互权限确定模块；5、数据存储模块。

具体实施方式

[0056] 下面结合附图和具体实施方式，进一步阐明本发明，应理解下述具体实施方式仅用于说明本发明而不用于限制本发明的范围。

[0057] 实施例1

[0058] 本发明实施例的零信任服务器应用的终端设备和用户实时安全等级评估方法是贯穿整个访问过程的，实现对终端设备和用户的当前安全等级的实时计算更新。

[0059] 如图1所示，一种基于零信任网络用户的大数据行为分析系统，应用于服务器中，所述服务器包括数据采集模块1、数据分析模块2、安全评估确定模块3、交互权限确定模块4、数据存储模块5，模块间通过电气和/或无线网络方式连接，实现数据相互传递。

[0060] 数据采集模块1:获取登录终端设备的用户信息和终端设备信息,并将所述用户信息和终端设备信息发送至数据分析模块2。

[0061] 数据分析模块2,对所述用户信息进行评估,并生成第一评估值,并将用户信息和用户信息对应的第一评估值存储在数据存储模块5;

[0062] 生成第一评估结果的逻辑为:

[0063] 获取登录终端设备的账号身份认证信息,根据所述账号身份认证信息与预设的用户信息进行身份识别,判断账号身份认证信息是否通过验证;

[0064] 若所述账号身份认证信息通过验证,则获取对应的用户在当前所述终端设备下的安全等级;将所述用户在当前所述终端设备下的安全等级标记为用户安全等级,对所述用户安全等级进行赋予相应数值,将所述用户安全等级赋予相应数值标记为AQ;

[0065] 根据所述预设的用户信息,获得所述预设的用户信息对应的预设用户安全等级,根据所述预设用户安全等级获得所述预设用户安全等级赋予相应数值标记YQ,其中YQ≥AQ;

[0066] 接收终端设备发起的再次身份认证的请求,将身份认证的请求对应的身份认证条件发送至终端设备,根据终端设备反馈本次身份认证条件对应的用户信息与预设的用户信息进行身份识别分析,若终端设备反馈本次身份认证条件对应的用户信息与预设的用户信息一致,则通过本次认证,更新用户在当前所述终端设备下的安全等级以及对应的安全赋予相应数值加1,并更新安全等级赋予相应数值AQ;

[0067] 其中,所述身份认证的请求包括图像身份认证、音频身份认证、指纹身份认证中一种或多种组合身份认证的请求;

[0068] 将所述用户安全等级赋予相应数值和所述预设用户安全等级赋予相应数值的比值标记为第一评估值PG1,所述第一评估值PG1为小于等于1的值;

[0069] 重复发起身份认证的请求,更新第一评估值PG1。

[0070] 零信任网络中对于用户是零信任的,因此在每个操作步骤之后都需要对其进行身份认证,其中,具体的身份认证过程可以在电子设备中实现,也可以是电子设备通过与身份认证平台的交互时实现身份认证;

[0071] 所述用户信息包括账号身份认证信息、图像身份认证信息、音频身份认证信息、指纹身份认证信息中任意一种或至少两种组合身份认证信息;也就是说,可以从终端设备中获取所述用户信息,获取的所述用户信息并不局限于某一种身份信息,基于现在大数据中对用户身份的认证方式的多样化,这里可以选择普遍的账号身份认证信息,抑或是对图像身份认证信息、音频身份认证信息或指纹身份认证信息,以及其他数据库中可以用于身份认证的手段,如果一个用户同时通过多重身份认证,可以更好的表明当前使用零信任网络的用户信息就是用户本人,避免其他人盗取账号,一定程度上阻碍恶意交互行为。

[0072] 数据分析模块2,提取所述终端设备信息,根据所述终端设备信息对所述终端设备的运行环境进行评估,并生成第二评估值,并终端设备信息和对应的第二评估值存储在数据存储模块5;

[0073] 所述终端设备信息包括第一终端设备的设备I D、设备登录时间和设备登录位置;

[0074] 将所述设备I D、设备登录时间和设备登录位置的安全等级分别赋予相应数值,并将赋予相应数值分别标记为R1、R2和R3;其中R1＞R2＞R3;

[0075] 若所述设备I D、设备登录时间和设备登录位置未发生变化,则对所述设备I D、设备登录时间和设备登录位置的安全等级赋值分别为R1、R2、R3;

[0076] 将所述设备I D、设备登录时间和设备登录位置对应的安全等级赋值相加累计为第二评估值PG2,即PG2＝R1+R2+R3;

[0077] 若所述设备I D、设备登录时间和设备登录位置发生变化,则对改变的所述设备I D、设备登录时间或设备登录位置的安全等级赋值分别为a1 R1、a2R2、a3R3;

[0078] 其中,a1+a2+a3＝1,a1、a2以及a3为大于0且小于1的权重;a1为所述设备I D的安全等级赋值R1的权重;a2为设备登录时间的安全等级赋值R2的权重;a3为设备登录位置发生变化的安全等级赋值R3的权重;

[0079] 将所述设备I D、设备登录时间和设备登录位置对应的安全等级赋值相加累计为第二评估值PG2,即PG2＝a1 R1+a2R2+a3R3。

[0080] 提取终端设备信息并生成第二评估值,其中设备I D可以包含终端设备的操作系统,软件版本,网络连接等信息,根据设备I D设备登录时间和设备登录位置来评估终端设备的安全状态。这个步骤可以确保终端设备没有被感染恶意软件或其他威胁。

[0081] 所述设备I D、设备登录时间和设备登录位置的安全等级赋值分别为R1、R2、R3,以及其对应的权重a1、a2、a3;这些数据都是基于大数据通过安全状态检测结果获得,其利用加权求和的方式,确定终端设备信息的第二评估值PG2。

[0082] 其中R1＞R2＞R3,说明设备I D的权重高于设备登录时间和设备登录位置的权重,因为设备I D更难以伪造或更容易检测到,可确保对用户的终端设备信息进行保密,并确保该系统或应用程序符合适用的法律法规和标准。

[0083] 安全评估确定模块3,将用户信息以及对应的终端设备信息进行绑定,将第一评估值和第二评估值相加得到安全评估值APG;

[0084] 交互权限确定模块4,根据所述安全评估值APG获得用户在对应的终端设备上生成相应的交互行为数据权限,并将安全评估值APG和对应的交互行为数据权限存储在数据存储模块5。

[0085] 根据第一评估值和第二评估值相乘得到安全评估值APG,将所述安全评估值APG代入安全梯度参考值Ph1和Ph2进行比对分析,其中Ph1＜Ph2;

[0086] 将所述第一评估值PG1代入安全梯度参考值Ph1和Ph2进行比对分析,其中Ph1＜Ph2;

[0087] 若安全评估值APG大于或等于安全梯度参考值Ph2时,则将用户信息对应的交互行为数据权限标记为高级交互权限;

[0088] 若安全评估值APG小于安全梯度参考值Ph2,且安全评估值APG大于或等于安全梯度参考值Ph1时,则将对应的交互行为数据权限标记为中级交互权限;

[0089] 若安全评估值APG小于安全梯度参考值Ph1时,则将用户信息对应的交互行为数据权限标记为低级交互权限。

[0090] 将用户信息、终端设备信息进行绑定,并计算出安全评估值(APG)。这可以确定用户在特定终端设备上的访问权限。例如,如果第一评估值较低,说明用户的身份验证或安全历史记录存在问题,则可能会限制用户在该设备上的访问权限。同样地,如果第二评估值较低,则说明设备的安全性较差,可能需要采取更严格的访问限制。

[0091] 总的来说，本发明可以评估用户在特定终端设备上的安全性，并确定他们是否有权访问敏感数据。同时，这个系统可以根据评估值自动调整用户的权限，以确保数据的安全性，非常适用零信任网络。

[0092] 根据所述交互行为数据权限获得所述用户对应的权限数据；根据所述权限数据对大数据行为构建行为-意图二分图模型，根据行为-意图二分图模型获得所述大数据行为对应的意图数据，根据意图数据判断所述大数据行为的真实意图。

[0093] 根据交互行为数据权限获得所述用户对应的权限数据，根据权限数据对大数据行为构建行为-意图二分图模型。行为节点表示具体的大数据行为，意图节点表示用户的意图，根据行为-意图二分图模型获得所述大数据行为对应的意图数据，根据意图数据判断所述大数据行为的真实意图。可以使用自然语言处理技术、机器学习算法等方法来完成这个步骤。

[0094] 如图3所示，根据行为-意图二分图模型获得所述大数据行为对应的意图数据的生成逻辑为：

[0095] 行为-意图二分图模型表示为G＝(V,S,E)，其中V表示数据交互系统中请求接入的大数据行为集合，S表示大数据行为对应的意图数据集合，共有m个大数据行为和n个意图数据，E表示大数据行为和意图数据之间可选链路的集合，可选链路是二分图中的边e＝(v,s)，e∈E，v∈V，s∈S，每条可选链路均具有权值$l_{m,n}$，权值$l_{m,n}$为可选链路的匹配数据，通过匹配数据将大数据行为与意图数据之间进行数字关联。

[0096] 在行为-意图二分图模型中，大数据行为和意图数据分别作为二分图的两个独立集合，它们之间的可选链路表示大数据行为和意图数据之间的可能关联。权值$l_{m,n}$表示大数据行为与意图数据之间的相关程度，可以使用各种方法来计算，如基于机器学习的模型、统计模型等。

[0097] 行为-意图二分图模型可以应用于许多领域，如网络安全、广告推荐、搜索引擎优化等。它可以帮助用户更好地理解大数据行为背后的意图，提高数据处理和利用的效率，同时也可以为相关机构提供更好的安全保障和用户服务。

[0098] 在交互行为数据权限下，根据意图数据判断所述大数据行为的真实意图的生成逻辑为：

[0099] 意图数据包括b个数据包x，以及每个所述数据包x相对应的浏览时间t，将数据包x与数据包x相对应的浏览时间t之和标记为表现系数z；统计b个数据包x的表现系数z_b，将表现系数z_b中最大的表现系数z1对应的数据包x作为意图数据的意图信号z；根据行为-意图二分图模型获得所述意图数据对应的匹配数据$l_{m,n}$；意图信号z与对应的匹配数据$l_{m,n}$的乘积标记为意图预测值；

[0100] 将权限数据集内最大的意图预测值对应的意图数据作为大数据行为的真实意图；若意图预测值数量为至少两个时，则任意确定一个意图预测值，将意图预测值对应的意图数据作为大数据行为的真实意图。

[0101] 这里需要说明是：这是一个简化的流程，实际情况可能会更加复杂，需要根据具体应用场景进行调整。

[0102] 实施例2

[0103] 本实施例所述一种基于零信任网络用户的大数据行为分析系统，员工YG在入职

时,已经向公司系统录入个人的用户信息,以及公司分配的终端设备和其他个人常用设备,将其统称为终端设备信息;将用户信息、终端设备信息进行绑定,并计算出安全评估值(APG)。零信任网络用户的大数据行为分析系统会根据员工YG录入的用户信息和终端设备信息进行匹配交互行为数据权限;可以评估用户在特定终端设备上的安全性,并确定他们是否有权访问敏感数据。同时,这个系统可以根据评估值自动调整用户的权限,以确保数据的安全性,非常适用零信任网络。

[0104] 当员工YG在终端设备上录入“公司利润”时,系统会根据员工的交互行为数据权限获得员工YG对应的权限数据;员工YG只能在对应的权限数据中查看相应的“公司利润”相关的数据,在当前权限数据中,关于“公司利润”相关的数据会有很多,例如销售利润数据、销售额数据,因此构建行为-意图二分图模型,并通过构建行为-意图二分图模型获得“公司利润”相关联的意图数据,每个意图数据中都会包含多个数据包x,以及每个所述数据包x相对应的浏览时间t,正常情况下,员工YG都不进行浏览数据包x肯定不是员工YG想要获取的数据,而进行浏览的浏览时间t越大,其关联性越强,浏览时间t越小,其关联性越弱,因此将数据包x与数据包x相对应的浏览时间t之和标记为表现系数z;统计b个数据包x的表现系数z_b,将表现系数z_b中最大的表现系数z1对应的数据包x作为意图数据的意图信号z;这里的意图信号z对应的是员工YG真实想要的数据,

[0105] 根据行为-意图二分图模型获得所述意图数据对应的匹配数据$1_{m,n}$;意图信号z与对应的匹配数据$1_{m,n}$的乘积标记为意图预测值;

[0106] 将权限数据集内最大的意图预测值对应的意图数据作为大数据行为的真实意图;若意图预测值数量为至少两个时,则任意确定一个意图预测值,将意图预测值对应的意图数据作为大数据行为的真实意图。

[0107] 这里的真实意图简而言之就是员工YG在个人权限数据中可以获取的最接近他想法的数据,即为大数据行为交互得到的真实意图,实际上这里的真实意图是一个相对的概念,必须符合员工YG的权限数据。

[0108] 实施例3

[0109] 本实施例所述一种基于零信任网络用户的大数据行为分析系统,其与实施例1不同点在于,当所述终端设备信息不具备安全等级的要求,即终端设备处于高风险的情况下,本实施例仅仅对所述用户信息进行评估,通过将第一评估值PG1代入安全梯度参考值Ph1和Ph2进行比对分析,通过判断第一评估值PG1的大小,获取对应的交互行为数据权限。

[0110] 对所述第一评估值PG1的分析逻辑为:

[0111] 将所述第一评估值PG1代入安全梯度参考值Ph1和Ph2进行比对分析,其中Ph1＜Ph2;

[0112] 若第一评估值PG1大于或等于安全梯度参考值Ph2时,则将用户信息对应的交互行为数据权限标记为高级交互权限;

[0113] 若第一评估值PG1小于安全梯度参考值Ph2,且安全评估值APG大于或等于安全梯度参考值Ph1时,则将对应的交互行为数据权限标记为中级交互权限;

[0114] 若第一评估值PG1小于安全梯度参考值Ph1时,则将用户信息对应的交互行为数据权限标记为低级交互权限。

[0115] 用户信息是指经过用户身份认证后的用户信息,其中用户身份认证可以是账号身

份认证信息(即用户名和密码)以及其他身份验证方法,如生物识别技术。第一评估值可以表示用户的身份验证和安全历史记录。

[0116] 这里可以应用的场景可以是,员工A在外地,要求下载一份比较重要的文件,其使用的终端设备并不是公司认证的安全设备,其第二评估值很小,可以忽略不计,因此员工A还需要实现上述交互行为数据,则可以通过当前终端设备不停的认证所述用户信息,通过对用户信息提高第一评估值PG1,通过第一评估值PG1获取交互行为数据。

[0117] 实施例4

[0118] 本实施例所述一种基于零信任网络用户的大数据行为分析系统,其与实施例1不同点在于,本实施例主要考虑的是终端设备为移动终端设备,其本身是可以随身携带的,即所述设备I D不变;但是其设备登录时间并不是用户预设的设备登录时间或预设的设备登录位置,并不符合用户的使用习惯,这里零信任网络会默认其不值得信任,需要对其进行反复的身份认证,通过身份认证后的终端设备重新考虑所述设备I D、设备登录时间和设备登录位置发生变化时,对应的安全等级赋值分别为a1 R1、a2R2、a3R3,其具体赋值根据本领域技术人员根据大量的实验可得,并结合相关算法对其进行训练学习逼近,从而获得更加真实的预测值,从而更好的获取权重a1、a2以及a3。

[0119] 实施例5

[0120] 请参阅图2所示,本实施例未详细叙述部分见实施例一描述内容,提供一种基于零信任网络用户的大数据行为分析方法,应用于服务器中,包括:

[0121] 从大数据行为中提取登录终端设备的用户信息,对所述用户信息进行评估,并生成第一评估值;

[0122] 提取所述终端设备信息,根据所述终端设备信息对所述终端设备的运行环境进行评估,并生成第二评估值;

[0123] 将用户信息以及对应的终端设备信息进行绑定,将第一评估值和第二评估值相加得到安全评估值APG,根据所述安全评估值APG获得用户在对应的终端设备上生成相应的交互行为数据权限;

[0124] 根据所述交互行为数据权限获得所述用户对应的权限数据;根据所述权限数据对大数据行为构建行为-意图二分图模型,根据行为-意图二分图模型获得所述大数据行为对应的意图数据,根据意图数据判断所述大数据行为的真实意图。

[0125] 所述用户信息包括账号身份认证信息、图像身份认证信息、音频身份认证信息、指纹身份认证信息中任意一种或至少两种组合身份认证信息;

[0126] 生成第一评估结果的逻辑为:

[0127] 获取登录终端设备的账号身份认证信息,根据所述账号身份认证信息与预设的用户信息进行身份识别,判断账号身份认证信息是否通过验证;

[0128] 若所述账号身份认证信息通过验证,则获取对应的用户在当前所述终端设备下的安全等级;将所述用户在当前所述终端设备下的安全等级标记为用户安全等级,对所述用户安全等级进行赋予相应数值,将所述用户安全等级赋予相应数值标记为AQ;

[0129] 根据所述预设的用户信息,获得所述预设的用户信息对应的预设用户安全等级,根据所述预设用户安全等级获得所述预设用户安全等级赋予相应数值标记YQ,其中YQ≥AQ;

[0130] 接收终端设备发起的再次身份认证的请求,将身份认证的请求对应的身份认证条件发送至终端设备,根据终端设备反馈本次身份认证条件对应的用户信息与预设的用户信息进行身份识别分析,若终端设备反馈本次身份认证条件对应的用户信息与预设的用户信息一致,则通过本次认证,更新用户在当前所述终端设备下的安全等级以及对应的安全赋予相应数值加1,并更新安全等级赋予相应数值AQ;

[0131] 其中,所述身份认证的请求包括图像身份认证、音频身份认证、指纹身份认证中一种或多种组合身份认证的请求;

[0132] 将所述用户安全等级赋予相应数值和所述预设用户安全等级赋予相应数值的比值标记为第一评估值PG1,所述第一评估值PG1为小于等于1的值;

[0133] 重复操作身份认证的请求,更新第一评估值PG1。

[0134] 对所述第一评估值PG1的分析逻辑为:

[0135] 将所述第一评估值PG1代入安全梯度参考值Ph1和Ph2进行比对分析,其中Ph1＜Ph2;

[0136] 若第一评估值PG1大于或等于安全梯度参考值Ph2时,则将用户信息对应的交互行为数据权限标记为高级交互权限;

[0137] 若第一评估值PG1小于安全梯度参考值Ph2,且安全评估值APG大于或等于安全梯度参考值Ph1时,则将对应的交互行为数据权限标记为中级交互权限;

[0138] 若第一评估值PG1小于安全梯度参考值Ph1时,则将用户信息对应的交互行为数据权限标记为低级交互权限。

[0139] 所述终端设备信息包括第一终端设备的设备I D、设备登录时间和设备登录位置;

[0140] 将所述设备I D、设备登录时间和设备登录位置的安全等级分别赋予相应数值,并将赋予相应数值分别标记为R1、R2和R3;其中R1＞R2＞R3;

[0141] 若所述设备I D、设备登录时间和设备登录位置未发生变化,则对所述设备I D、设备登录时间和设备登录位置的安全等级赋值分别为R1、R2、R3;

[0142] 将所述设备I D、设备登录时间和设备登录位置对应的安全等级赋值相加累计为第二评估值PG2,即PG2＝R1+R2+R3;

[0143] 若所述设备I D、设备登录时间和设备登录位置发生变化,则对改变的所述设备I D、设备登录时间或设备登录位置的安全等级赋值分别为a1 R1、a2R2、a3R3;

[0144] 其中,a1+a2+a3＝1,a1、a2以及a3为大于0且小于1的权重;a1为所述设备I D的安全等级赋值R1的权重;a2为设备登录时间的安全等级赋值R2的权重;a3为设备登录位置发生变化的安全等级赋值R3的权重;

[0145] 将所述设备I D、设备登录时间和设备登录位置对应的安全等级赋值相加累计为第二评估值PG2,即PG2＝a1 R1+a2R2+a3R3。

[0146] 根据第一评估值和第二评估值相乘得到安全评估值APG,将所述安全评估值APG代入安全梯度参考值Ph1和Ph2进行比对分析,其中Ph1＜Ph2;

[0147] 将所述第一评估值PG1代入安全梯度参考值Ph1和Ph2进行比对分析,其中Ph1＜Ph2;

[0148] 若安全评估值APG大于或等于安全梯度参考值Ph2时,则将用户信息对应的交互行为数据权限标记为高级交互权限;

[0149] 若安全评估值APG小于安全梯度参考值Ph2，且安全评估值APG大于或等于安全梯度参考值Ph1时，则将对应的交互行为数据权限标记为中级交互权限；

[0150] 若安全评估值APG小于安全梯度参考值Ph1时，则将用户信息对应的交互行为数据权限标记为低级交互权限。

[0151] 根据所述交互行为数据权限获得所述用户对应的权限数据集；所述权限数据集包括n个意图数据，所述意图数据为所述大数据行为的关联数据。

[0152] 根据行为-意图二分图模型获得所述大数据行为对应的意图数据的生成逻辑为：

[0153] 行为-意图二分图模型表示为G＝(V,S,E)，其中V表示数据交互系统中请求接入的大数据行为集合，S表示大数据行为对应的意图数据集合，共有m个大数据行为和n个意图数据，E表示大数据行为和意图数据之间可选链路的集合，可选链路是二分图中的边e＝(v,s)，e∈E，v∈V，s∈S，每条可选链路均具有权值$l_{m,n}$，权值$l_{m,n}$为可选链路的匹配数据，通过匹配数据将大数据行为与意图数据之间进行数字关联。

[0154] 在交互行为数据权限下，根据意图数据判断所述大数据行为的真实意图的生成逻辑为：

[0155] 意图数据包括b个数据包x，以及每个所述数据包x相对应的浏览时间t，将数据包x与数据包x相对应的浏览时间t之和标记为表现系数z；统计b个数据包x的表现系数z_b，将表现系数z_b中最大的表现系数z1对应的数据包x作为意图数据的意图信号z；根据行为-意图二分图模型获得所述意图数据对应的匹配数据$l_{m,n}$；意图信号z与对应的匹配数据$l_{m,n}$的乘积标记为意图预测值；

[0156] 将权限数据集内最大的意图预测值对应的意图数据作为大数据行为的真实意图；若意图预测值数量为至少两个时，则任意确定一个意图预测值，将意图预测值对应的意图数据作为大数据行为的真实意图。

[0157] 上述公式均是去量纲取其数值计算，公式是由采集大量数据进行软件模拟得到最近真实情况的一个公式，公式中的预设参数以及阈值选取由本领域的技术人员根据实际情况进行设置。

[0158] 上述实施例，可以全部或部分地通过软件、硬件、固件或其他任意组合来实现。当使用软件实现时，上述实施例可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令或计算机程序。在计算机上加载或执行所述计算机指令或计算机程序时，全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机可以为通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线网络或无线网络方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集合的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质(例如，软盘、硬盘、磁带)、光介质(例如，DVD)、或者半导体介质。半导体介质可以是固态硬盘。

[0159] 本领域普通技术人员可以意识到，结合本发明中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人

员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0160] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0161] 在本发明所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的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，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0162] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者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者全部单元来实现本实施例方案的目的。

[0163] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

[0164] 需要说明的是，以上内容仅仅说明了本发明的技术思想，不能以此限定本发明的保护范围，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰均落入本发明权利要求书的保护范围之内。

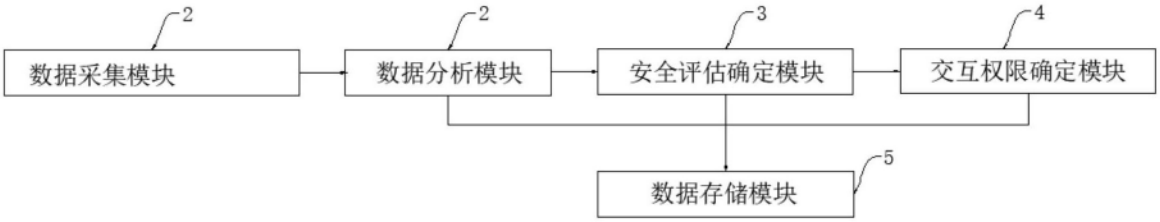

2
数据采集模块
2
数据分析模块
3
安全评估确定模块
4
交互权限确定模块
5
数据存储模块

图1

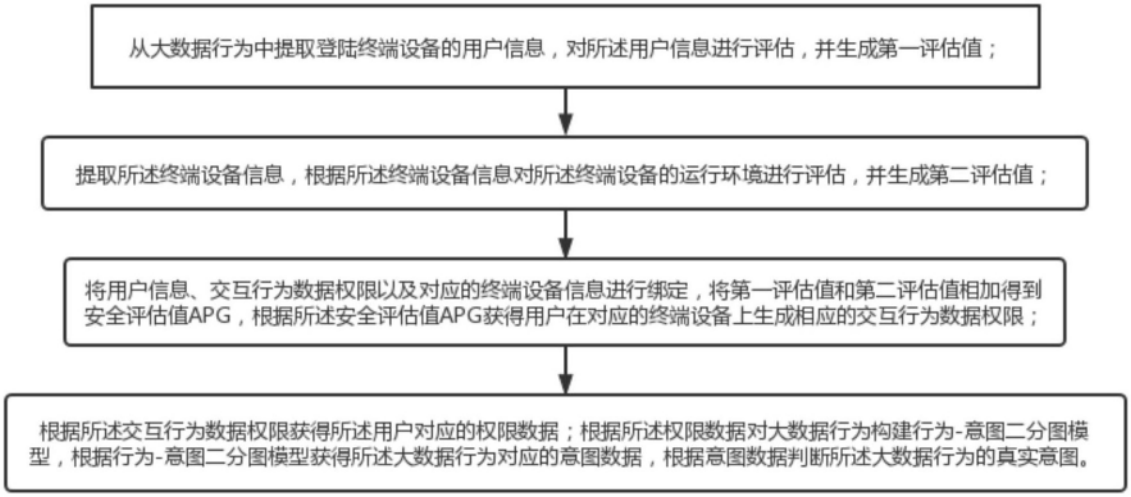

从大数据行为中提取登陆终端设备的用户信息，对所述用户信息进行评估，并生成第一评估值；
提取所述终端设备信息，根据所述终端设备信息对所述终端设备的运行环境进行评估，并生成第二评估值；
将用户信息、交互行为数据权限以及对应的终端设备信息进行绑定，将第一评估值和第二评估值相加得到安全评估值APG，根据所述安全评估值APG获得用户在对应的终端设备上生成相应的交互行为数据权限；
根据所述交互行为数据权限获得所述用户对应的权限数据；根据所述权限数据对大数据行为构建行为-意图二分图模型，根据行为-意图二分图模型获得所述大数据行为对应的意图数据，根据意图数据判断所述大数据行为的真实意图。

图2

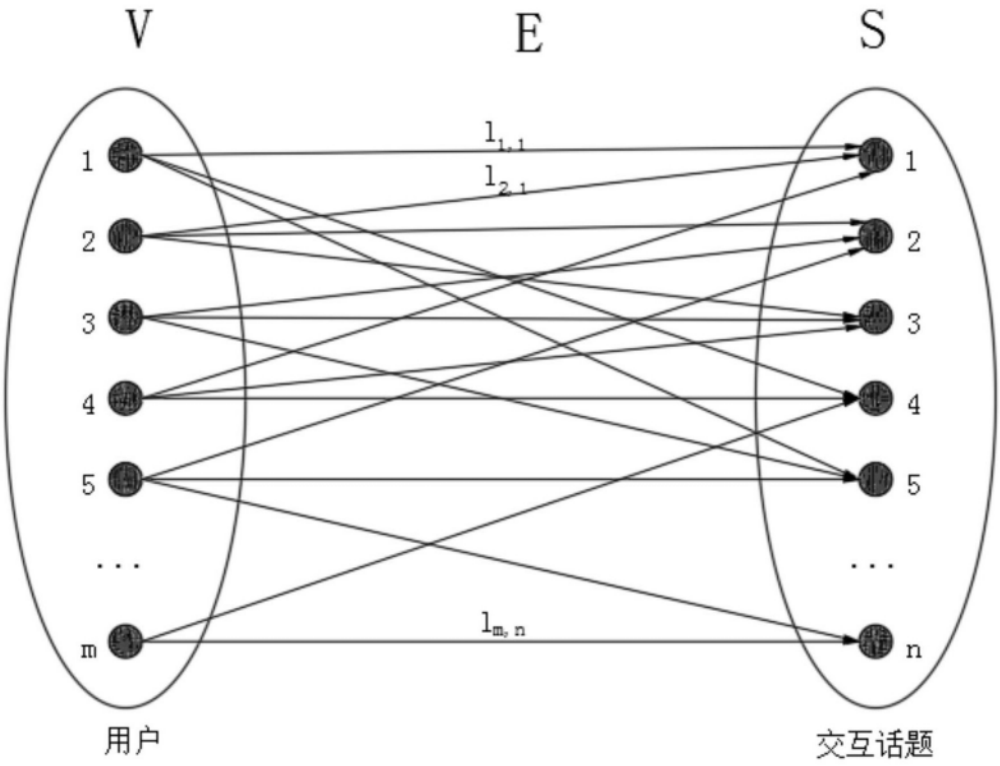


图3