(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114641811 B
(45)授权公告日 2023.03.28

(21)申请号 202180005569.5
(22)申请日 2021.10.18
(65)同一申请的已公布的文献号
申请公布号 CN 114641811 A
(43)申请公布日 2022.06.17
(30)优先权数据
63/092,670 2020.10.16 US
(85)PCT国际申请进入国家阶段日
2022.03.28
(86)PCT国际申请的申请数据
PCT/US2021/055374 2021.10.18
(87)PCT国际申请的公布数据
WO2022/082091 EN 2022.04.21

(73)专利权人 维萨国际服务协会
地址 美国加利福尼亚州
(72)发明人 董博 Y·吴 Y-S·林 M·叶 H·杨
(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
专利代理师 黄晓升

(51)Int.Cl.
G08B 23/00(2006.01)
审查员 邓薇

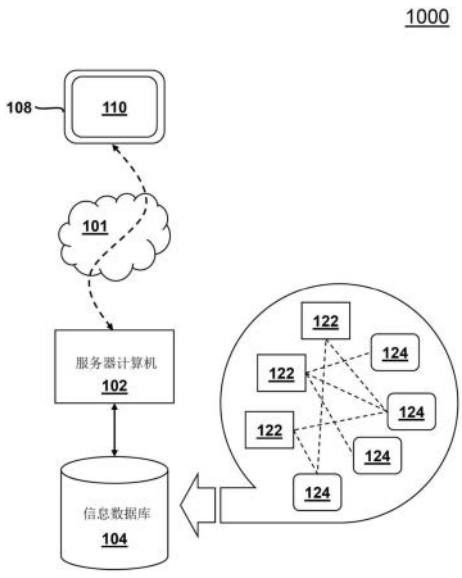
权利要求书3页 说明书19页 附图4页

(54)发明名称

用于用户网络活动异常检测的系统、方法和计算机程序产品

(57)摘要

描述一种用于用户网络活动异常检测的系统、方法和计算机程序产品。所述方法包括接收与多个用户的网络资源活动相关联的网络资源数据，以及从所述网络资源数据生成多层图的多个层。所述多个层中的每个层可以包括由多个边缘连接的多个节点，所述多个节点与用户相关联，所述多个边缘表示节点相关性。所述方法还包括从所述多个层生成多个邻接矩阵，以及基于所述多个邻接矩阵的加权和生成合并单层图。所述方法还包括针对所述合并单层图中的每个节点生成异常得分，以及基于所述异常得分确定一组异常用户。



CN 114641811 B

1.一种用于用户网络活动异常检测的方法,所述方法用计算机实施,包括:

利用至少一个处理器,在包括至少一个网络资源的网络上接收与多个用户的网络资源活动相关联的网络资源数据;

利用至少一个处理器,从所述网络资源数据生成多层图的多个层,其中所述多个层中的每个层包括由多个边缘连接的多个节点,所述多个节点中的每个节点与所述多个用户中的用户相关联,所述多个边缘中的每个边缘表示节点的相关性,并且每个层表示根据网络资源活动的唯一参数的节点的相关性;

利用至少一个处理器,生成与所述多个层中的每个层相关联的邻接矩阵以产生多个邻接矩阵;

利用至少一个处理器,将权重分配给所述多个邻接矩阵中的每个邻接矩阵以产生多个权重;

利用至少一个处理器,通过使用所述多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成合并单层图,所述合并单层图包括合并的一组节点;

利用至少一个处理器,通过针对所述合并的一组节点中的每个节点,基于所述节点的属性和在所述合并的一组节点中连接到所述节点的至少一个对等节点的至少一个属性生成异常得分,生成一组异常得分;以及

利用至少一个处理器,基于所述一组异常得分确定所述多个用户中的一组异常用户。

2.根据权利要求1所述的方法,还包括:

(a)利用至少一个处理器,基于至少一个损失函数修改所述多个权重以产生修改后的多个权重;

(b)利用至少一个处理器,通过使用所述修改后的多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成更新后的合并单层图;

(c)利用至少一个处理器,基于所述更新后的合并单层图生成一组新的异常得分;以及

(d)利用至少一个处理器,基于所述一组新的异常得分更新所述一组异常用户。

3.根据权利要求2所述的方法,其中所述至少一个损失函数包括至少两个损失函数的加权和,并且其中所述至少两个损失函数包括至少部分地基于所述合并单层图的损失函数。

4.根据权利要求3所述的方法,其中所述至少两个损失函数还包括至少部分地基于外部标识的异常用户的输入反馈的损失函数。

5.根据权利要求3所述的方法,还包括通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重,在无监督的训练环境中重复执行步骤(a)-(d)。

6.根据权利要求4所述的方法,还包括通过接收外部标识的异常用户的新输入反馈,并且通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重,在至少部分受监督的训练环境中重复执行步骤(a)-(d)。

7.根据权利要求1所述的方法,还包括:

利用至少一个处理器,基于所述一组异常用户检测欺诈性网络活动;以及

响应于检测到欺诈性网络活动,利用至少一个处理器执行至少一个欺诈缓解过程。

8.一种用于用户网络活动异常检测的系统,所述系统包括服务器,所述服务器包括至少一个处理器,所述服务器被编程或配置成:

在包括至少一个网络资源的网络上接收与多个用户的网络资源活动相关联的网络资源数据；

从所述网络资源数据生成多层图的多个层，其中所述多个层中的每个层包括由多个边缘连接的多个节点，所述多个节点中的每个节点与所述多个用户中的用户相关联，所述多个边缘中的每个边缘表示节点的相关性，并且每个层表示根据网络资源活动的唯一参数的节点的相关性；

生成与所述多个层中的每个层相关联的邻接矩阵以产生多个邻接矩阵；

将权重分配给所述多个邻接矩阵中的每个邻接矩阵以产生多个权重；

通过使用所述多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成合并单层图，所述合并单层图包括合并的一组节点；

通过针对所述合并的一组节点中的每个节点，基于所述节点的属性和在所述合并的一组节点中连接到所述节点的至少一个对等节点的至少一个属性生成异常得分，生成一组异常得分；以及

基于所述一组异常得分确定所述多个用户中的一组异常用户。

9.根据权利要求8所述的系统，其中所述服务器还被编程或配置成：

(a)基于至少一个损失函数修改所述多个权重以产生修改后的多个权重；

(b)通过使用所述修改后的多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成更新后的合并单层图；

(c)基于所述更新后的合并单层图生成一组新的异常得分；以及

(d)基于所述一组新的异常得分更新所述一组异常用户。

10.根据权利要求9所述的系统，其中所述至少一个损失函数包括至少两个损失函数的加权和，并且其中所述至少两个损失函数包括至少部分地基于所述合并单层图的损失函数。

11.根据权利要求10所述的系统，其中所述至少两个损失函数还包括至少部分地基于外部标识的异常用户的输入反馈的损失函数。

12.根据权利要求10所述的系统，其中所述服务器还被编程或配置成通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重，在无监督的训练环境中重复执行步骤(a)-(d)。

13.根据权利要求11所述的系统，其中所述服务器还被编程或配置成通过接收外部标识的异常用户的新输入反馈，并且通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重，在至少部分受监督的训练环境中重复执行步骤(a)-(d)。

14.根据权利要求8所述的系统，其中所述服务器还被编程或配置成：

基于所述一组异常用户检测欺诈性网络活动；以及

响应于检测到欺诈性网络活动，执行至少一个欺诈缓解过程。

15.一种用于用户网络活动异常检测的计算机程序产品，包括至少一个非瞬态计算机可读介质，所述至少一个非瞬态计算机可读介质包括程序指令，所述程序指令在由至少一个处理器执行时使得所述至少一个处理器：

在包括至少一个网络资源的网络上接收与多个用户的网络资源活动相关联的网络资源数据；

从所述网络资源数据生成多层图的多个层,其中所述多个层中的每个层包括由多个边缘连接的多个节点,所述多个节点中的每个节点与所述多个用户中的用户相关联,所述多个边缘中的每个边缘表示节点的相关性,并且每个层表示根据网络资源活动的唯一参数的节点的相关性;

生成与所述多个层中的每个层相关联的邻接矩阵以产生多个邻接矩阵;

将权重分配给所述多个邻接矩阵中的每个邻接矩阵以产生多个权重;

通过使用所述多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成合并单层图,所述合并单层图包括合并的一组节点;

通过针对所述合并的一组节点中的每个节点,基于所述节点的属性和在所述合并的一组节点中连接到所述节点的至少一个对等节点的至少一个属性生成异常得分,生成一组异常得分;以及

基于所述一组异常得分确定所述多个用户中的一组异常用户。

16.根据权利要求15所述的计算机程序产品,其中所述程序指令还使得所述至少一个处理器:

(a)基于至少一个损失函数修改所述多个权重以产生修改后的多个权重;

(b)通过使用所述修改后的多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成更新后的合并单层图;

(c)基于所述更新后的合并单层图生成一组新的异常得分;以及

(d)基于所述一组新的异常得分更新所述一组异常用户。

17.根据权利要求16所述的计算机程序产品,其中所述至少一个损失函数包括至少两个损失函数的加权和,并且其中所述至少两个损失函数包括至少部分地基于所述合并单层图的损失函数。

18.根据权利要求17所述的计算机程序产品,其中所述至少两个损失函数还包括至少部分地基于外部标识的异常用户的输入反馈的损失函数。

19.根据权利要求18所述的计算机程序产品,其中所述程序指令还使得所述至少一个处理器通过接收外部标识的异常用户的新输入反馈,并且通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重,在至少部分受监督的训练环境中重复执行步骤(a)-(d)。

20.根据权利要求15所述的计算机程序产品,其中所述程序指令还使得所述至少一个处理器:

基于所述一组异常用户检测欺诈性网络活动;以及

响应于检测到欺诈性网络活动,执行至少一个欺诈缓解过程。

用于用户网络活动异常检测的系统、方法和计算机程序产品

[0001] 相关申请交叉引用

[0002] 本申请要求2020年10月16日提交并且标题为“用于用户网络活动异常检测的系统、方法和计算机程序产品(System,Method,and Computer Program Product for User Network Activity Anomaly Detection)”的第63/092,670号美国临时专利申请的优先权，所述申请的全部公开内容特此以引用的方式并入本文中。

技术领域

[0003] 本公开大体上涉及网络行为分析，并且在非限制性实施例或方面中涉及用于通过对行为进行多层绘图来进行异常检测的系统、方法和计算机程序产品。

背景技术

[0004] 检测群体内的异常对于许多不同类型的系统是有益的。然而，典型的异常检测是基于单层信息。这与现实世界应用中常见的条件不匹配，在现实世界应用中可能需要多个输入来确定群体内的异常。此外，基于与给定用户的对等方的活动的比较，所述用户的行为可能是异常的，也可能不是异常的。因此，有必要基于组成员之间的关系将群体分成不同的组，并且基于多个输入来标识组内的异常。这样做会提高检测异常网络活动的准确性，进而通过准确标识和响应异常行为来节约网络资源，无论是通过缓解所述行为还是重新分配网络资源以适应异常行为。

发明内容

[0005] 根据一些非限制性实施例或方面，提供一种用于用户网络活动异常检测的计算机实施的方法。所述方法包括利用至少一个处理器，在包括至少一个网络资源的网络上接收与多个用户的网络资源活动相关联的网络资源数据。所述方法还包括利用至少一个处理器，从所述网络资源数据生成多层图的多个层。所述多个层中的每个层包括由多个边缘连接的多个节点。所述多个节点中的每个节点与所述多个用户中的用户相关联。所述多个边缘中的每个边缘表示所述节点的相关性。每个层表示根据网络资源活动的唯一参数的节点的相关性。所述方法还包括利用至少一个处理器，生成与所述多个层中的每个层相关联的邻接矩阵以产生多个邻接矩阵。所述方法还包括利用至少一个处理器，将权重分配给所述多个邻接矩阵中的每个邻接矩阵以产生多个权重。所述方法还包括利用至少一个处理器，通过使用所述多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成合并单层图，所述合并单层图包括合并的一组节点。所述方法还包括利用至少一个处理器，通过针对所述合并的一组节点中的每个节点，基于所述节点的属性和在所述合并的一组节点中连接到所述节点的至少一个对等节点的至少一个属性生成异常得分，生成一组异常得分。所述方法还包括利用至少一个处理器，基于所述一组异常得分确定所述多个用户中的一组异常用户。

[0006] 在另外的非限制性实施例或方面中，所述方法还可包括(a)利用至少一个处理器，

基于至少一个损失函数修改所述多个权重以产生修改后的多个权重。所述方法还可包括(b)利用至少一个处理器，通过使用所述修改后的多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成更新后的合并单层图。所述方法还可包括(c)利用至少一个处理器，基于所述更新后的合并单层图生成一组新的异常得分。所述方法还可包括(d)利用至少一个处理器，基于所述一组新的异常得分更新所述一组异常用户。

[0007] 在另外的非限制性实施例或方面中，所述至少一个损失函数可包括至少两个损失函数的加权和。所述至少两个损失函数可包括至少部分地基于所述合并单层图的损失函数。所述方法还可包括通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重，在无监督的训练环境中重复执行上述步骤(a)-(d)。

[0008] 在另外的非限制性实施例或方面中，所述至少两个损失函数还可包括至少部分地基于外部标识的异常用户的输入反馈的损失函数。所述方法还可包括通过接收外部标识的异常用户的新输入反馈，并且通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重，在至少部分受监督的训练环境中重复执行上述步骤(a)-(d)。

[0009] 在另外的非限制性实施例或方面中，所述方法还可包括利用至少一个处理器，基于所述一组异常用户检测欺诈性网络活动。所述方法还可包括响应于检测到欺诈性网络活动，利用至少一个处理器执行至少一个欺诈缓解过程。

[0010] 根据一些非限制性实施例或方面，提供一种用于用户网络活动异常检测的系统。所述系统包括服务器，所述服务器包括至少一个处理器。所述服务器被编程或配置成在包括至少一个网络资源的网络上接收与多个用户的网络资源活动相关联的网络资源数据。所述服务器还被编程或配置成从所述网络资源数据生成多层图的多个层。所述多个层中的每个层包括由多个边缘连接的多个节点。所述多个节点中的每个节点与所述多个用户中的用户相关联。所述多个边缘中的每个边缘表示所述节点的相关性。每个层表示根据网络资源活动的唯一参数的节点的相关性。所述服务器还被编程或配置成生成与所述多个层中的每个层相关联的邻接矩阵以产生多个邻接矩阵。所述服务器还被编程或配置成将权重分配给所述多个邻接矩阵中的每个邻接矩阵以产生多个权重。所述服务器还被编程或配置成通过使用所述多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成合并单层图，所述合并单层图包括合并的一组节点。所述服务器还被编程或配置成通过针对所述合并的一组节点中的每个节点，基于所述节点的属性和在所述合并的一组节点中连接到所述节点的至少一个对等节点的至少一个属性生成异常得分，生成一组异常得分。所述服务器还被编程或配置成基于所述一组异常得分确定所述多个用户中的一组异常用户。

[0011] 在另外的非限制性实施例或方面中，所述服务器还可被编程或配置成(a)基于至少一个损失函数修改所述多个权重以产生修改后的多个权重。所述服务器还可被编程或配置成(b)通过使用所述修改后的多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成更新后的合并单层图。所述服务器还可被编程或配置成(c)基于所述更新后的合并单层图生成一组新的异常得分。所述服务器还可被编程或配置成(d)基于所述一组新的异常得分更新所述一组异常用户。

[0012] 在另外的非限制性实施例或方面中，所述至少一个损失函数可包括至少两个损失函数的加权和。所述至少两个损失函数可包括至少部分地基于所述合并单层图的损失函数。所述服务器还可被编程或配置成通过在每次新执行步骤(a)之前改变所述至少两个损

失函数的所述加权和的权重，在无监督的训练环境中重复执行步骤(a)-(d)。

[0013] 在另外的非限制性实施例或方面中，所述至少两个损失函数还可包括至少部分地基于外部标识的异常用户的输入反馈的损失函数。所述服务器还可被编程或配置成通过接收外部标识的异常用户的新输入反馈，并且通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重，在至少部分受监督的训练环境中重复执行步骤(a)-(d)。

[0014] 在另外的非限制性实施例或方面中，所述服务器还可被编程或配置成基于所述一组异常用户检测欺诈性网络活动。所述服务器还可被编程或配置成响应于检测到欺诈性网络活动，执行至少一个欺诈缓解过程。

[0015] 根据一些非限制性实施例或方面，提供一种用于用户网络活动异常检测的计算机程序产品。所述计算机程序产品包括至少一个非瞬态计算机可读介质，所述至少一个非瞬态计算机可读介质包括程序指令，所述程序指令在由至少一个处理器执行时，使得所述至少一个处理器在包括至少一个网络资源的网络上接收与多个用户的网络资源活动相关联的网络资源数据。所述程序指令还使得所述至少一个处理器从所述网络资源数据生成多层图的多个层。所述多个层中的每个层包括由多个边缘连接的多个节点。所述多个节点中的每个节点与所述多个用户中的用户相关联。所述多个边缘中的每个边缘表示所述节点的相关性。每个层表示根据网络资源活动的唯一参数的节点的相关性。所述程序指令还使得所述至少一个处理器生成与所述多个层中的每个层相关联的邻接矩阵以产生多个邻接矩阵。所述程序指令还使得所述至少一个处理器将权重分配给所述多个邻接矩阵中的每个邻接矩阵以产生多个权重。所述程序指令还使得所述至少一个处理器通过使用所述多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成合并单层图，所述合并单层图包括合并的一组节点。所述程序指令还使得所述至少一个处理器通过针对所述合并的一组节点中的每个节点，基于所述节点的属性和在所述合并的一组节点中连接到所述节点的至少一个对等节点的至少一个属性生成异常得分，生成一组异常得分。所述程序指令还使得所述至少一个处理器基于所述一组异常得分确定所述多个用户中的一组异常用户。

[0016] 在另外的非限制性实施例或方面中，所述程序指令还使得所述至少一个处理器(a)基于至少一个损失函数修改所述多个权重以产生修改后的多个权重。所述程序指令还使得所述至少一个处理器(b)通过使用所述修改后的多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成更新后的合并单层图。所述程序指令还使得所述至少一个处理器(c)基于所述更新后的合并单层图生成一组新的异常得分。所述程序指令还使得所述至少一个处理器(d)基于所述一组新的异常得分更新所述一组异常用户。

[0017] 在另外的非限制性实施例或方面中，所述至少一个损失函数可包括至少两个损失函数的加权和。所述至少两个损失函数还可包括至少部分地基于所述合并单层图的损失函数。

[0018] 在另外的非限制性实施例或方面中，所述至少两个损失函数可包括至少部分地基于外部标识的异常用户的输入反馈的损失函数。所述程序指令还使得所述至少一个处理器通过接收外部标识的异常用户的新输入反馈，并且通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重，在至少部分受监督的训练环境中重复执行步骤(a)-(d)。

[0019] 在另外的非限制性实施例或方面中，所述程序指令还使得所述至少一个处理器基于所述一组异常用户检测欺诈性网络活动。所述程序指令还使得所述至少一个处理器响应于检测到欺诈性网络活动执行至少一个欺诈缓解过程。

[0020] 将在以下编号条款中阐述其它非限制性实施例或方面：

[0021] 条款1：一种计算机实施的方法，包括：利用至少一个处理器，在包括至少一个网络资源的网络上接收与多个用户的网络资源活动相关联的网络资源数据；利用至少一个处理器，从所述网络资源数据生成多层图的多个层，其中所述多个层中的每个层包括由多个边缘连接的多个节点，所述多个节点中的每个节点与所述多个用户中的用户相关联，所述多个边缘中的每个边缘表示所述节点的相关性，并且每个层表示根据网络资源活动的唯一参数的节点的相关性；利用至少一个处理器，生成与所述多个层中的每个层相关联的邻接矩阵以产生多个邻接矩阵；利用至少一个处理器，将权重分配给所述多个邻接矩阵中的每个邻接矩阵以产生多个权重；利用至少一个处理器，通过使用所述多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成合并单层图，所述合并单层图包括合并的一组节点；利用至少一个处理器，通过针对所述合并的一组节点中的每个节点，基于所述节点的属性和在所述合并的一组节点中连接到所述节点的至少一个对等节点的至少一个属性生成异常得分，生成一组异常得分；以及利用至少一个处理器，基于所述一组异常得分确定所述多个用户中的一组异常用户。

[0022] 条款2：根据条款1所述的计算机实施的方法，还包括：(a)利用至少一个处理器，基于至少一个损失函数修改所述多个权重以产生修改后的多个权重；(b)利用至少一个处理器，通过使用所述修改后的多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成更新后的合并单层图；(c)利用至少一个处理器，基于所述更新后的合并单层图生成一组新的异常得分；以及(d)利用至少一个处理器，基于所述一组新的异常得分更新所述一组异常用户。

[0023] 条款3：根据条款1或2所述的计算机实施的方法，其中所述至少一个损失函数包括至少两个损失函数的加权和，并且其中所述至少两个损失函数包括至少部分地基于所述合并单层图的损失函数。

[0024] 条款4：根据条款1至3中任一项所述的计算机实施的方法，其中所述至少两个损失函数还包括至少部分地基于外部标识的异常用户的输入反馈的损失函数。

[0025] 条款5：根据条款1至4中任一项所述的计算机实施的方法，还包括通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重，在无监督的训练环境中重复执行步骤(a)-(d)。

[0026] 条款6：根据条款1至5中任一项所述的计算机实施的方法，还包括通过接收外部标识的异常用户的新输入反馈，并且通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重，在至少部分受监督的训练环境中重复执行步骤(a)-(d)。

[0027] 条款7：根据条款1至6中任一项所述的计算机实施的方法，还包括：利用至少一个处理器，基于所述一组异常用户检测欺诈性网络活动；以及响应于检测到欺诈性网络活动，利用至少一个处理器执行至少一个欺诈缓解过程。

[0028] 条款8：一种包括服务器的系统，所述服务器包括至少一个处理器，所述服务器被编程或配置成：在包括至少一个网络资源的网络上接收与多个用户的网络资源活动相关联

的网络资源数据;从所述网络资源数据生成多层图的多个层,其中所述多个层中的每个层包括由多个边缘连接的多个节点,所述多个节点中的每个节点与所述多个用户中的用户相关联,所述多个边缘中的每个边缘表示所述节点的相关性,并且每个层表示根据网络资源活动的唯一参数的节点的相关性;生成与所述多个层中的每个层相关联的邻接矩阵以产生多个邻接矩阵;将权重分配给所述多个邻接矩阵中的每个邻接矩阵以产生多个权重;通过使用所述多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成合并单层图,所述合并单层图包括合并的一组节点;通过针对所述合并的一组节点中的每个节点,基于所述节点的属性和在所述合并的一组节点中连接到所述节点的至少一个对等节点的至少一个属性生成异常得分,生成一组异常得分;以及基于所述一组异常得分确定所述多个用户中的一组异常用户。

[0029] 条款9:根据条款8所述的系统,其中所述服务器还被编程或配置成:(a)基于至少一个损失函数修改所述多个权重以产生修改后的多个权重;(b)通过使用所述修改后的多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成更新后的合并单层图;(c)基于所述更新后的合并单层图生成一组新的异常得分;以及(d)基于所述一组新的异常得分更新所述一组异常用户。

[0030] 条款10:根据条款8或9所述的系统,其中所述至少一个损失函数包括至少两个损失函数的加权和,并且其中所述至少两个损失函数包括至少部分地基于所述合并单层图的损失函数。

[0031] 条款11:根据条款8-10中任一项所述的系统,其中所述至少两个损失函数还包括至少部分地基于外部标识的异常用户的输入反馈的损失函数。

[0032] 条款12:根据条款8至11中任一项所述的系统,其中所述服务器还被编程或配置成通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重,在无监督的训练环境中重复执行步骤(a)-(d)。

[0033] 条款13:根据条款8至12中任一项所述的系统,其中所述服务器还被编程或配置成通过接收外部标识的异常用户的新输入反馈,并且通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重,在至少部分受监督的训练环境中重复执行步骤(a)-(d)。

[0034] 条款14:根据条款8至13中任一项所述的系统,其中所述服务器还被编程或配置成:基于所述一组异常用户检测欺诈性网络活动;以及响应于检测到欺诈性网络活动,执行至少一个欺诈缓解过程。

[0035] 条款15:一种计算机程序产品,包括至少一个非瞬态计算机可读介质,所述至少一个非瞬态计算机可读介质包括程序指令,所述程序指令在由至少一个处理器执行时,使得所述至少一个处理器:在包括至少一个网络资源的网络上接收与多个用户的网络资源活动相关联的网络资源数据;从所述网络资源数据生成多层图的多个层,其中所述多个层中的每个层包括由多个边缘连接的多个节点,所述多个节点中的每个节点与所述多个用户中的用户相关联,所述多个边缘中的每个边缘表示所述节点的相关性,并且每个层表示根据网络资源活动的唯一参数的节点的相关性;生成与所述多个层中的每个层相关联的邻接矩阵以产生多个邻接矩阵;将权重分配给所述多个邻接矩阵中的每个邻接矩阵以产生多个权重;通过使用所述多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成合并单

层图，所述合并单层图包括合并的一组节点；通过针对所述合并的一组节点中的每个节点，基于所述节点的属性和在所述合并的一组节点中连接到所述节点的至少一个对等节点的至少一个属性生成异常得分，生成一组异常得分；以及基于所述一组异常得分确定所述多个用户中的一组异常用户。

[0036] 条款16：根据条款15所述的计算机程序产品，其中所述程序指令还使得所述至少一个处理器：(a)基于至少一个损失函数修改所述多个权重以产生修改后的多个权重；(b)通过使用所述修改后的多个权重基于所述多个邻接矩阵的加权和合并所述多个层来生成更新后的合并单层图；(c)基于所述更新后的合并单层图生成一组新的异常得分；以及(d)基于所述一组新的异常得分更新所述一组异常用户。

[0037] 条款17：根据条款15或16所述的计算机程序产品，其中所述至少一个损失函数包括至少两个损失函数的加权和，并且其中所述至少两个损失函数包括至少部分地基于所述合并单层图的损失函数。

[0038] 条款18：根据条款15至17中任一项所述的计算机程序产品，其中所述至少两个损失函数还包括至少部分地基于外部标识的异常用户的输入反馈的损失函数。

[0039] 条款19：根据条款15至18中任一项所述的计算机程序产品，其中所述程序指令还使得所述至少一个处理器通过接收外部标识的异常用户的新输入反馈，并且通过在每次新执行步骤(a)之前改变所述至少两个损失函数的所述加权和的权重，在至少部分受监督的训练环境中重复执行步骤(a)-(d)。

[0040] 条款20：根据条款15至19中任一项所述的计算机程序产品，其中所述程序指令还使得所述至少一个处理器：基于所述一组异常用户检测欺诈性网络活动；以及响应于检测到欺诈性网络活动，执行至少一个欺诈缓解过程。

[0041] 在参考附图考虑以下描述和所附权利要求书之后，本公开的这些和其它特征和特性以及相关结构元件和各部分的组合的操作方法和功能以及制造经济性将变得更加显而易见，所有附图形成本说明书的部分，其中相似附图标号在各图中标示对应部分。然而，应明确地理解，图式仅用于说明及描述的目的，且不希望作为对本公开的限制的定义。除非上下文另外明确规定，否则在本说明书和权利要求书中使用时，单数形式“一”和“所述”包括多个指示物。

附图说明

[0042] 下文参考附图中说明的示例性实施例更详细地解释本公开的额外优点和细节，在附图中：

[0043] 图1是根据一些非限制性实施例或方面的用于多层图异常检测的方法的过程图；

[0044] 图2是根据一些非限制性实施例或方面的用于多层图异常检测的系统的示意图；

[0045] 图3是根据一些非限制性实施例或方面的一个或多个组件、装置和/或系统的图；

[0046] 图4是根据一些非限制性实施例或方面的用于多层图异常检测的方法的流程图；并且

[0047] 图5是根据一些非限制性实施例或方面的用于多层图异常检测的方法的流程图。

[0048] 本领域的技术人员应了解，本文中的任何框图表示体现本发明主题的原理的说明性系统的概念视图。类似地，可了解，任何流程图表、流程图、状态转换图、伪代码等表示可

基本上在计算机可读介质中表示并且由计算机或处理器执行的各种过程，无论是否明确示出此类计算机或处理器。

具体实施方式

[0049] 为了进行以下描述，术语“上”、“下”、“右”、“左”、“竖直”、“水平”、“顶部”、“底部”、“横向”、“纵向”以及其派生词应如其在附图中的定向那样与非限制性实施例或方面相关。然而，应理解，除了明确指定为相反的情况之外，非限制性实施例或方面可采用各种替代变化和步骤顺序。还应理解，附图中所示的以及在以下说明书中描述的特定装置和过程仅仅是示例性实施例或方面。因此，与本文所公开的实施例有关的特定尺寸和其它物理特性不应被视为限制性的。

[0050] 本文所使用的方面、组件、元件、结构、动作、步骤、功能、指令等都不应当被理解为关键的或必要的，除非明确地如此描述。且，如本文所使用，冠词“一”希望包括一个或多个项目，且可与“一个或多个”和“至少一个”互换使用。此外，如本文所使用，术语“集合”希望包括一个或多个项目(例如，相关项目、不相关项目、相关项目与不相关项目的组合等)，并且可以与“一个或多个”或“至少一个”互换使用。在希望仅有一个项目的情况下，使用术语“一个”或类似语言。且，如本文中所使用，术语“具有”等希望是开放式术语。另外，除非另外明确陈述，否则短语“基于”希望意味着“至少部分地基于”。

[0051] 本文中结合阈值描述一些非限制性实施例或方面。如本文所使用，满足阈值可以指值大于阈值、多于阈值、高于阈值、大于或等于阈值、小于阈值、少于阈值、低于阈值、小于或等于阈值、等于阈值等。

[0052] 如本文所使用，术语“收单方机构”可指由交易服务提供商许可和/或批准以使用与交易服务提供商相关联的支付装置发起交易(例如，支付交易)的实体。收单方机构可发起的交易可包括支付交易(例如，购买、原始信用证交易(OCT)、账户资金交易(AFT)等。在一些非限制性实施例中，收单方机构可以是金融机构，例如银行。如本文所使用，术语“收单方系统”可以指由收单方机构或代表收单方机构操作的一个或多个计算装置，例如执行一个或多个软件应用程序的服务器计算机。

[0053] 如本文所使用，术语“账户标识符”可包括一个或多个主账号(PAN)、令牌或与顾客账户相关联的其它标识符。术语“令牌”可指用作PAN等原始账户标识符的替代或替换标识符的标识符。账户标识符可以是文数字或字符和/或符号的任何组合。令牌可与一个或多个数据结构(例如一个或多个数据库和/或其类似者)中的PAN或其它原始账户标识符相关联，使得令牌可用于进行交易而无需直接使用原始账户标识符。在一些实例中，例如PAN等原始账户标识符可以与用于不同个人或目的的多个令牌相关联。

[0054] 如本文中所使用，术语“通信”可以指数据(例如，信息、信号、消息、指令、命令等)的接收、接纳、发送、传送、提供等。一个单元(例如，装置、系统、装置或系统的组件、其组合等)与另一单元通信意味着所述一个单元能够直接或间接地从所述另一单元接收信息和/或向所述另一单元发送信息。这可指在本质上有线和/或无线的直接或间接连接(例如，直接通信连接、间接通信连接等)。另外，尽管所发送的信息可以在第一单元与第二单元之间被修改、处理、中继和/或路由，但这两个单元也可以彼此通信。例如，即使第一单元被动地接收信息且不会主动地将信息发送到第二单元，第一单元也可以与第二单元通信。作为另

一示例，如果至少一个中间单元处理从第一单元接收的信息且将处理后的信息传送到第二单元，那么第一单元可以与第二单元通信。

[0055] 如本文中所使用，术语“计算装置”可以指被配置成处理数据的一个或多个电子装置。在一些示例中，计算装置可以包括接收、处理和输出数据的必要组件，例如处理器、显示器、存储器、输入装置、网络接口等。计算装置可以是移动装置。作为示例，移动装置可以包括蜂窝电话(例如，智能手机或标准蜂窝电话)、便携式计算机、可穿戴装置(例如，手表、眼镜、镜片、衣物等)、个人数字助理(PDA)和/或其它类似装置。计算装置还可以是台式计算机或其它形式的非移动计算机。“应用程序”或“应用程序编程接口”(API)可指计算机代码或在计算机可读介质上排序的其它数据，其可以由处理器执行以促进软件组件之间的交互，例如客户侧前端和/或服务器侧后端的交互以用于从客户端接收数据。“界面”可指生成的显示，例如一个或多个图形用户界面(GUI)，用户可以直接或间接地(例如，通过键盘、鼠标等)与所述图形用户界面交互。

[0056] 如本文所使用，术语“电子钱包”和“电子钱包应用程序”是指被配置为发起和/或进行支付交易的一个或多个电子装置和/或软件应用程序。例如，电子钱包可包括执行电子钱包应用程序的移动装置，并且还可包括用于维护交易数据并将交易数据提供给移动装置的服务器端侧软件和/或数据库。“电子钱包提供商”可包括为客户提供和/或维护电子钱包的实体，例如Google Pay®、Android Pay®、Apple Pay®、Samsung Pay®和/或其它类似电子支付系统。在一些非限制性实例中，发行方银行可是电子钱包提供商。

[0057] 如本文所使用，术语“发行方机构”可指例如银行的一个或多个实体，其向客户提供账户以进行交易(例如支付交易)，例如发起信用和/或借记支付。例如，发行方机构可以向客户提供唯一地标识与所述客户相关联的一个或多个账户的账户标识符，例如主账号(PAN)。账户标识符可以在例如实体金融工具(例如，支付卡)等便携式金融装置上实施，和/或可以是电子的且用于电子支付。术语“发行方系统”指由发行方机构或代表发行方机构操作的一个或多个计算机装置，例如执行一个或多个软件应用程序的服务器计算机。例如，发行方系统可包括用于授权交易的一个或多个授权服务器。

[0058] 如本文所使用，术语“商家”可以指基于例如支付交易的交易向客户提供商品和/或服务或者对商品和/或服务的访问的个人或实体。术语“商家”或“商家系统”还可以指由商家或代表商家操作的一个或多个计算机系统，例如执行一个或多个软件应用程序的服务器计算机。如本文所使用，“销售点(POS)系统”可指由商家用来与客户进行支付交易的一个或多个计算机和/或外围装置，包括一个或多个读卡器、扫描装置(例如，代码扫描仪)、Bluetooth®通信接收器、近场通信(NFC)接收器、射频标识(RFID)接收器和/或其它非接触收发器或接收器、基于接触的接收器、支付终端、计算机、服务器、输入装置和/或可用于发起支付交易的其它类似装置。

[0059] 如本文所用，术语“支付装置”可指支付卡(例如，信用卡或借记卡)、礼品卡、智能卡、智能介质、工资卡、医疗保健卡、腕带、含有账户信息的机器可读介质、钥匙链装置或吊坠、RFID应答器、零售商折扣或会员卡、蜂窝电话、电子钱包移动应用程序、PDA、寻呼机、安全卡、计算装置、访问卡、无线终端、应答器等。在一些非限制性实施例中，支付装置可包括存储信息(例如账户标识符、账户持有者姓名等)的易失性或非易失性存储器。

[0060] 如本文所使用，术语“支付网关”可以指实体和/或由这种实体或代表这种实体操

作的支付处理系统，所述实体(例如，商家服务提供商、支付服务提供商、支付服务商、与收单方签约的支付服务商、支付集合商等)将支付服务(例如，交易服务提供商支付服务、支付处理服务等)提供给一个或多个商家。支付服务可以与由交易服务提供商管理的便携式金融装置的使用相关联。如本文所使用，术语“支付网关系统”可以指由支付网关或代表支付网关操作的一个或多个计算机系统、计算机装置、服务器、服务器群组等。

[0061] 如本文所使用，术语“服务器”可指或包括由互联网等网络环境中的多方操作或促进所述多方的通信和处理的一个或多个计算装置，但应了解，可通过一个或多个公共或专用网络环境促进通信，并且可能有各种其它布置。另外，在网络环境中直接或间接通信的多个计算装置(例如，服务器、POS装置、移动装置等)可以构成“系统”。如本文所使用，对“服务器”或“处理器”的提及可指陈述为实施先前步骤或功能的先前所述服务器和/或处理器、不同的服务器和/或处理器，和/或服务器和/或处理器的组合。例如，如在说明书和权利要求书中所使用，陈述为实施第一步骤或功能的第一服务器和/或第一处理器可指代陈述为实施第二步骤或功能的相同或不同服务器和/或处理器。

[0062] 如本文所使用，术语“交易服务提供商”可指从商家或其它实体接收交易授权请求且在一些情况下通过交易服务提供商与发行方机构之间的协议来提供支付保证的实体。例如，交易服务提供商可包括例如Visa®之类的支付网络，或处理交易的任何其它实体。术语“交易处理系统”可指由交易服务提供商或代表交易服务提供商操作的一个或多个计算机系统，例如执行一个或多个软件应用程序的交易处理服务器。交易处理服务器可以包括一个或多个处理器，并且在一些非限制性实施例中，可以由交易服务提供商或代表交易服务提供商操作。

[0063] 如本文所使用，电子支付处理网络可指一个或多个实体之间用于处理货币资金向一个或多个交易的转移的通信。电子支付处理网络可以包括商家系统、收单方系统、交易服务提供商和发行方系统。

[0064] 解决方案的详细描述

[0065] 本文所述的系统、方法和计算机程序产品在用于确定异常的系统中提供许多技术优点。例如，标识行为异常可能是标识公司员工安全风险的一个重要方面。如果只关注员工活动的一个方面，则可能很难实现这一点。本文所述的非限制性实施例提高了标识异常行为的准确性。通过标识员工的对等组并将员工与这些对等组进行比较，可以利用减少的计算资源标识异常行为，例如通过减少分析时间和减少所收集的比较所需的历史数据量来标识异常行为。改进的用户对等标识和异常检测提高了例如欺诈检测系统等后续依赖系统的效率(例如，降低处理时间和容量)。允许用户输入改变异常排名的结果也可以提高系统的准确性。

[0066] 所述系统从多层图的不同图层的合并开始。如本文所用，“图”可指图论的关系表示，其中包括节点(例如，顶点、点等)的数学结构通过边缘(例如，链接、线等)连接，以表示节点之间的成对关系。可使用邻接矩阵的加权和产生合并单层图，所述加权和表示多层图的每个层的连接性。如本文所用，“邻接矩阵”可指用于表示顶点对是否在图中邻近(例如，连接)以及所述连接是否具有关系值(例如，成本、相关性强度等)的矩阵。

[0067] 系统接着进行异常检测，所述异常检测可以接收上述合并过程的结果。对于特定节点(例如，用户)，可以从所述特定节点所属的集群中找到节点的对等方。本文提供计算每

位员工的异常得分的函数。异常检测部分的输出可以是具有对应异常得分的一组异常用户。可以为异常得分设置阈值，并且可以根据所述阈值确定用户是否异常。基于第三方(例如，专业人员、用户等)的反馈和/或基于图合并的损失函数，可以调整系统以获得更好的性能。

[0068] 下文更详细地描述基于多层图的异常检测系统，其使用由图中的层生成的多个集群，采用加权层合并，并基于所述节点的对等方检测图中的异常节点(例如，用户)。还可以基于部分可用的反馈数据来检测异常节点。所描述的系统解决了在进行异常检测时经常遇到的挑战，例如，反馈稀疏。所描述的系统进一步解决了多层图的挑战，例如，找到多个集群的一致性。

[0069] 在一些现实世界应用中，假设图中的单个层封装所有所需信息可能是不自然的。在所有类型的信息都聚集在一起的单个图上操作可能也不太方便。例如，当考虑基于不同类型的边缘的异常节点时，将所有类型的边缘放在一起使得很难对图进行聚类和基于指定的边缘类型提取对等方和社区。此外，当在不区分连接类型的情况下对不同类型的异常进行后聚合时，可能难以将有意义的权重分配给由不同类型的连接生成的异常。所描述的系统解决了这些问题。

[0070] 下文提供了技术问题的定义和所公开的方法的系统概述。令多层图为G＝(V,E)，其中图由节点V＝{v1,…,vn}和边缘E＝{E1,…,Em}组成，所述节点在G中的所有层中都是公共的，所述边缘中的每一个对应于图中的m个层之一，并且每个Ei是边缘集合。此外，Ei∈E存储其对应层的边缘信息。符号Gi＝(V,Ei)可用于表示第i个层图，而ai可用于表示与vi相关联的属性。对于节点(例如，用户)v，可以假设其大部分时间的行为与其对等方类似，这在多层图G中表现出类似的行为。如本文所述，节点v的“对等方”可以指表现出类似于v的行为或在图中与v紧密连接的一组节点v′。节点vi∈V的对等方是给定单层图G＝(V,E)中强连接到vi的一组np个节点$\mathbf{Vi'} \subset \mathbf{V}$。符号E[i,j]可用于表示节点vi与其对等方vj之间的边缘权重。多层图的每个层都可以对节点之间的一种关系建模。

[0071] 可能存在显示每个节点的对等方的合并图。具有m个层的多层图G的合并图G_{merge}＝(V,E_{merge})可以是如下的单层图：(i)通过合并G中的层而生成，例如，G_{merge}＝merge(G_1,…,G_m)且(ii)包含对等关系信息。

[0072] 在G中的所有m个层中，作为对等方的用户节点很可能始终相似。如果节点v与其在G中特定层中的对等方明显不同，则可以假设v是潜在的异常。按照这样的逻辑，此框架的目标是，给定多层图作为输入，可根据异常对节点进行得分。为了实现这一点，本文所述的框架可以包括层合并、异常检测和优化的过程阶段。

[0073] 具体参考图1，描绘根据一些非限制性实施例或方面的多层图异常检测的过程图。所公开的方法可包括三个过程阶段：层合并阶段16、异常检测阶段28和优化阶段34。如本文所用，过程的阶段可以指将由一个或多个处理器执行的方法的一系列步骤。任何阶段可以由相同或不同的处理器集合执行。

[0074] 所述系统可以如下工作。在层合并阶段16，系统使用加权和合并函数(参见下文的公式1)基于学习的权重$\bar{w}_i$将多层图10a、10b、10c、10m组合成单层图。在异常检测阶段28，系统可以确定节点的对等方(步骤20)并使用其属性24和由合并图给出的对等属性22来计算每个节点的异常得分26(参见下文的公式8)。在优化阶段34，系统可以细化在合并函数中使

用的权重。用于优化阶段中的权重的训练环境可以是无监督或半监督的。在完全无监督的训练模式中，可以通过深度嵌入聚类(DEC)损失模型36(参见下文的公式2)和对准损失模型38(参见下文的公式6)优化权重。当训练环境包括人类反馈时，可以使用由研究员(例如，与异常检测系统交互并且至少部分地操作异常检测系统的用户)提供的标签使用排名损失模型(参见下文的公式11)来细化权重。

[0075] 在层合并阶段16，用于生成合并图14的层合并算法可包括加权和合并函数。加权和合并函数通过计算每个层的邻接矩阵12a、12b、12c、12m的加权和来合并层，即，$E_{merge}=w_1E_1+\cdots+w_mE_m$，其中：

[0076] 公式1：

[0077] $$w_i=\frac{e^{\bar{w}_i}}{\sum_j e^{\bar{w}_j}}$$

[0078] 并且每个E_i的$\bar{w}_i$是可学习的参数。为了学习这些权重，系统可以解决对等分组问题。对等分组问题的目的是将给定图G的节点聚类为k个组。具体地，可以优化下文定义的深度嵌入聚类(DEC)损失函数：

[0079] 公式2：

[0080] $$\mathcal{L}_{DEC}=\sum_i\sum_j p_{ij}\log\frac{p_{ij}}{q_{ij}}$$

[0081] 其中q_{ij}和p_{ij}是软集群分配和硬集群分配。软集群分配可以由给定节点i(例如，v_i)与集群质心j(例如，c_j)之间的相似性定义，所述相似性用学生t-分布测量，如下所示：

[0082] 公式3：

[0083] $$q_{ij}=\frac{\sum_{j'}1+\|v_i-c_{j'}\|^2}{1+\|v_i-c_j\|^2}$$

[0084] 当计算与学生t-分布的相似性时，自由度可以设置为1。硬集群分配可以如下计算：

[0085] 公式4：

[0086] $$p_{ij}=\frac{q_{ij}^2/\sum_{i'}q_{i'j}}{\sum_{j'}q_{ij'}^2/\sum_{i'}q_{i'j'}}$$

[0087] 可以使用k均值聚类算法来计算初始集群质心。当计算q_{ij}和初始质心两者时，每个节点$v_i\in V$可以表示为向量，指示v_i与V中的其它节点的连接性。换句话说，v_i可以由第i行E_{merge}表示，并且v_i与v_j之间的距离可以如下计算：

[0088] 公式5：

[0089] $$||\varepsilon_{merge}[i,:]-\varepsilon_{merge}[j,:]||^2$$

[0090] 除了DEC损失36之外，还可以优化对准损失38。对准损失38尝试将节点属性与节点的聚类对准(例如，属于相同集群的节点应具有相似的属性值)。一对节点(例如，v_i和v_j)的

对准损失38可以如下计算：

[0091] 公式6：

[0092] $$\mathcal{L}_{\text{align}} = \text{similarity}(a_i, a_j)\log \sum_l q_{il} q_{jl}$$

[0093] 其中similarity()是输出v_i的属性a_i与v_j的属性a_j之间的相似性的函数。应当理解，可以使用返回非负相似性的任何函数。在所描述的系统中，可以通过将差转换为相似性来计算相似性，例如：

[0094] 公式7：

[0095] α_{max}-abs(a_i-a_j)

[0096] 其中a_{max}是任何对节点的属性之间的最大可能差。q_{il}和q_{jl}两者都可以用(上文的)公式3计算。

[0097] 为了获得节点v_i的最终异常得分，可以使用以下公式，其基于合并图中v_i的对等方(例如，V_i')及其属性a_i：

[0098] 公式8：

[0099] $$s_i = \frac{|a_i - \mu_i|}{\sigma_i}$$

[0100] 其中μi和σi可通过下式计算：

[0101] 公式9：

[0102] $$\mu_i = \frac{\sum_{v_j \in \mathcal{V}_i'} \mathcal{E}[i,j] a_j}{\sum_{v_j \in \mathcal{V}_i'} \mathcal{E}[i,j]}$$

[0103] 以及

[0104] 公式10：

[0105] $$\sigma_i = \sqrt{\frac{\sum_{v_j \in \mathcal{V}_i'} \mathcal{E}[i,j](a_j - \mu_i)}{\sum_{v_j \in \mathcal{V}_i'} \mathcal{E}[i,j]}}$$

[0106] 如上所示，μ_i和σ_i是v_i的对等方的属性的加权平均值和标准偏差；并且v_i在其属性与对等方相比有很大差异时可能具有高异常得分。

[0107] 在研究员提供一组小的已标记异常节点作为反馈32的情况下，可以采用排名损失模型30，如下所示：

[0108] 公式11：

[0109] $$\mathcal{L}_{\text{rank}} = \max(V_0 - V_1, 0)$$

[0110] 其中V_0是来自已标记正常节点的小批量样本，并且V_1是来自已标记异常节点的小批量样本。排名损失可以帮助模型学习一组更好的层合并权重w_i，以揭示异常节点。考虑到DEC损失36、对准损失38和排名损失30，由系统计算的总体损失可如下表示：

[0111] 公式12：

[0112] $$\mathcal{L} = \alpha\mathcal{L}_{\mathrm{DEC}} + \beta\mathcal{L}_{\mathrm{align}} + \gamma\mathcal{L}_{\mathrm{rank}}$$

[0113] 其中α、β和γ是超参数，用于权衡不同项的贡献。

[0114] 上述方法和阶段可用于合成和现实世界数据集两者。可以为将在本文所述的系统中使用的数据施加三个参数。第一参数可包括数据被格式化为图的能力。只要在相同类型或不同类型的实体之间存在至少一种关系，就可以生成数据的图。实体(例如，用户、账户、商家、支付装置等)可以用公式表示为节点，并且所述关系可以由边缘表示。边缘可以是定向的或无向的，并且可以是加权的或未加权的。如上所述，图必须能够转换为邻接矩阵。

[0115] 第二参数可包括将绘制的数据拆分成多个层的能力。多组节点可以在多个层上相同，并且数据可以包括将单个图拆分成多个层的多种方式，例如，通过边缘的类型、边缘的时间戳等。第三参数可包括数据中异常的存在。因为目前描述的系统是异常检测系统，所以假定数据将包括要检测的有意义的异常。例如，对于表示用户的节点，异常可包括组织内部的恶意员工、泄露的用户账户、欺诈性用户活动等。对于表示传感器网络中的传感器的节点，异常可包括故障传感器。应当理解，异常的类型可以有所不同，并且可以取决于要分析的系统。

[0116] 可以针对半监督学习方法施加第四参数，这可能需要异常反馈的可用性。关于异常反馈的可用性，数据集还可以包含异常的反馈，例如异常的地面真相。如果反馈不是直接可用的，则可以接受的是，可以从数据集合理地得出真实异常。

[0117] 非限制性实施例和方面

[0118] 现在参考图2，示出了根据一些非限制性实施例或方面的用于多层图异常检测的系统1000。计算装置108经由例如互联网或专用网络等网络环境101与服务器计算机102通信。服务器计算机102与包括信息数据库104的数据存储装置通信。服务器计算机102可以与欺诈检测和/或缓解系统相关联和/或包括在欺诈检测和/或缓解系统中。信息数据库104可包括与至少两个节点122的活动相关联的一组或多组数据。每个节点可以表示不同的实体，例如个人、用户、计算装置、交易账户等。所述一组或多组数据可包括与用户相关活动相关联和/或与用户的网络资源124(例如，网络安全数据)相关联的网络资源数据，例如每个节点的电子邮件事务、每个节点的网站流量、对硬件和/或软件的访问请求等。服务器计算机102可以包括信息数据库104。

[0119] 服务器计算机102可以基于一组或多组信息生成多层图，每组数据用于在多层图中生成其自身的层。多层图的每个层可以包含一组节点，所述一组节点由从所述层中包含的每个节点的数据生成的一组边缘连接。服务器计算机102可以为多层图的每个层生成邻接矩阵。层合并算法可以将权重应用于每个邻接矩阵并且基于加权邻接矩阵。服务器计算机102可以基于层合并算法生成合并单层图，并基于节点和节点的对等方的属性(例如，网络资源活动数据参数，例如活动时间、与之交互的资源、计算机资源大小/带宽等)生成每个节点的异常得分。服务器计算机102可以基于异常得分对所有节点进行排名。服务器计算机102可以基于排名异常得分确定每个节点的初始异常评估。服务器计算机102可以基于初始异常评估确定一组异常节点。

[0120] 继续参考图2，计算装置108可以基于从服务器计算机102接收的数据显示GUI 110。GUI 110可在主GUI内或作为单独GUI包括一个或多个窗口(例如，第一GUI、第二GUI、第

三GUI等)。GUI 110可以将多个图层、合并单层图和/或异常得分显示给用户。用户可以经由GUI 110向服务器计算机102提供反馈,以改变一个或多个节点的图或异常得分/排名,和/或提供已知节点标签(例如,异常用户、非无害用户等)的反馈。服务器计算机102可以重新生成邻接矩阵的权重,重新生成合并单层图,并且基于用户提供的反馈重新生成每个节点的异常得分。

[0121] 现在参考图3,示出了根据一些非限制性实施例或方面的装置900的示例组件的图式。装置900可以对应于计算装置108、服务器计算机102、通信网络101、信息数据库104、节点122、网络资源124等的一个或多个装置,如图2所示。在一些非限制性实施例或方面中,此类系统或装置可以包括至少一个装置900和/或装置900的至少一个组件。作为示例提供图3中所示的组件的数量和布置。在一些非限制性实施例或方面中,与图3中所示的那些相比,装置900可以包括额外组件、更少的组件、不同的组件或以不同方式布置的组件。另外或替代地,装置900的一组组件(例如,一个或多个组件)可以执行被描述为由装置900的另一组组件执行的一个或多个功能。

[0122] 如图3所示,装置900可包括总线902、处理器904、存储器906、存储组件908、输入组件910、输出组件912和通信接口914。总线902可包括准许装置900的组件之间的通信的组件。在一些非限制性实施例或方面中,处理器904可以在硬件、固件或硬件和软件的组合中实施。例如,处理器904可包括处理器(例如中央处理单元(CPU)、图形处理单元(GPU)、加速处理单元(APU)等)、微处理器、数字信号处理器(DSP)和/或可被编程以执行功能的任何处理组件(例如现场可编程门阵列(FPGA)、专用集成电路(ASIC)等)。存储器906可包括随机存取存储器(RAM)、只读存储器(ROM),和/或存储供处理器904使用的信息和/或指令的另一类型的动态或静态存储装置(例如,闪存存储器、磁存储器、光学存储器等)。

[0123] 继续参考图3,存储组件908可存储与装置900的操作和使用相关的信息和/或软件。例如,存储组件908可包括硬盘(例如磁盘、光盘、磁光盘、固态磁盘等)和/或另一类型的计算机可读介质。输入组件910可包括准许装置900例如通过用户输入(例如触摸屏显示器、键盘、小键盘、鼠标、按钮、开关、麦克风等)接收信息的组件。另外或替代地,输入组件910可包括用于感测信息的传感器(例如全球定位系统(GPS)组件、加速度计、陀螺仪、致动器等)。输出组件912可包括从装置900提供输出信息的组件(例如显示器、扬声器、一个或多个发光二极管(LED)等)。通信接口914可包括使装置900能够例如通过有线连接、无线连接或有线和无线连接的组合与其它装置通信的收发器类组件(例如收发器、单独的接收器和传送器等)。通信接口914可准许装置900从另一装置接收信息和/或提供信息给另一装置。例如,通信接口914可包括以太网接口、光接口、同轴接口、红外接口、射频(RF)接口、通用串行总线(USB)接口、Wi-Fi®接口、蜂窝网络接口,和/或其类似者。

[0124] 装置900可执行本文中所描述的一个或多个过程。装置900可基于处理器904执行由存储器906和/或存储组件908等计算机可读介质存储的软件指令来执行这些过程。计算机可读介质可包括任何非瞬态存储器装置。存储器装置包括位于单个物理存储装置内部的存储器空间或散布于多个物理存储装置上的存储器空间。软件指令可通过通信接口914从另一计算机可读介质或从另一装置读取到存储器906和/或存储组件908中。在被执行时,存储在存储器906和/或存储组件908中的软件指令可使处理器904执行本文中所描述的一个或多个过程。另外或替代地,硬接线电路系统可替代软件指令或与软件指令结合使用以执

行本文中所描述的一个或多个过程。因此，本文所描述的实施例不限于硬件电路系统和软件的任何特定组合。本文所使用的术语“被编程或配置”是指一个或多个装置上的软件、硬件电路系统或其任何组合的布置。

[0125] 现在参考图4，示出了根据本公开的一些非限制性实施例或方面的用于多层图异常检测的方法的流程图。所述方法可以由服务器计算机102、信息数据库104和/或其它计算装置的一个或多个处理器执行。由第一处理器执行的一个或多个步骤可由相同或不同的处理器执行。

[0126] 在步骤300中，可以接收与节点行为相关联的数据。例如，服务器计算机102可以在包括至少一个网络资源(例如，联网计算装置的硬件和/或软件)的网络上接收与多个用户(例如，节点)的网络资源活动(例如，与之进行的一个或多个通信)相关联的网络资源数据。在组织结构中，节点可以是员工，并且网络资源活动可以是与组织内的各种联网装置的通信类型。在电子支付处理网络中，节点可以是交易账户，并且网络资源活动可以是与商家、发行方、支付网关和/或交易服务提供商的一个或多个装置的交易。

[0127] 在步骤302中，可以生成多层图的多个层。例如，服务器计算机102可以从网络资源活动的网络资源数据生成多层图的多个层。多个层中的每个层可以包括由多个边缘连接的多个节点。多个节点中的每个节点可以与多个用户中的用户相关联。多个边缘中的每个边缘可以表示节点的相关性(例如，统计关系、共享属性等，例如相似资源访问)。每个层可以表示根据网络资源活动的唯一参数(例如，时间、资源标识符、通信信道、用户计算装置类型等)的节点的相关性。

[0128] 在步骤304，可以生成多个邻接矩阵。例如，服务器计算机102可以生成与多个层中的每个层相关联的邻接矩阵(例如，距离矩阵)，以产生多个邻接矩阵。

[0129] 在步骤306，可将权重分配给每个邻接矩阵。例如，服务器计算机102可以将权重分配给多个邻接矩阵中的每个邻接矩阵以产生多个权重。可以利用重复测试异常检测模型，例如通过无监督和/或半监督测试方法重新分配/重新生成权重。

[0130] 在步骤308，可以生成合并单层图。例如，服务器计算机102可以通过使用多个权重基于多个邻接矩阵的加权和合并多个层来生成合并单层图。合并单层图可以包括合并的一组节点。

[0131] 在步骤310，可以生成一组异常得分。例如，服务器计算机102可以通过针对合并的一组节点中的每个节点基于所述节点的属性和在合并的一组节点中连接到所述节点的至少一个对等节点的至少一个属性生成异常得分来生成一组异常得分。节点的对等方可能与被评估节点具有强烈的相关性。

[0132] 在步骤312，可以确定一组异常用户。例如，服务器计算机102可以基于所述一组异常得分确定多个用户中的一组异常用户。例如，可以将节点的异常得分的值与阈值进行比较，并且如果满足阈值，则基于节点与网络中用户的对应，可以确定异常用户的身份。阈值可以是预定的或动态的，例如基于与平均值的统计方差/偏差。

[0133] 在步骤314，可以修改多个权重。例如，服务器计算机102可以基于至少一个损失函数(例如，DEC损失、对准损失、排名损失等)修改多个权重以产生修改后的多个权重。响应于步骤314，所述方法可以回到步骤308，在所述步骤中生成更新后的合并单层图。例如，服务器计算机102可以通过使用修改后的多个权重基于多个邻接矩阵的加权和合并多个层来生

成更新后的合并单层图。然后，所述方法可以进行到步骤310，在所述步骤中生成一组新的异常得分。例如，服务器计算机102可以基于更新后的合并单层图生成一组新的异常得分。然后，所述方法可以进行到步骤312，在所述步骤中更新所述一组异常用户。例如，服务器计算机102可以基于所述一组新的异常得分更新所述一组异常用户。应了解，步骤308、310、312和314的上述周期可以定期间隔、触发时间等重复，包括在根据学习方法对各种权重、超参数等进行调整之后。

[0134] 除了上述情况，步骤314的至少一个损失函数可以是两个或更多个损失函数的加权和(例如，DEC损失、对准损失等)。两个或更多个损失函数可以至少部分地基于合并单层图。步骤308、310、312和314可以通过在每次新执行步骤314之前改变两个或更多个损失函数的加权和的权重而在无监督训练环境中重复执行。

[0135] 除了上述情况，步骤314的至少一个损失函数可以是包括至少一个损失函数的两个或更多个损失函数的加权和，所述至少一个损失函数至少部分地基于外部标识的异常节点的输入反馈(例如，由个人或预定异常用户系统独立确定)。步骤308、310、312和314可以通过接收外部标识的异常节点的新输入反馈并且通过在每次新执行步骤314之前改变两个或更多个损失函数的加权和的权重而在半监督训练环境中重复执行。

[0136] 现在参考图5，示出了根据本公开的一些非限制性实施例或方面的用于多层图异常检测的方法的流程图。所述方法可以由服务器计算机102、信息数据库104和/或其它计算装置的一个或多个处理器执行。由第一处理器执行的一个或多个步骤可由相同或不同的处理器执行。

[0137] 在步骤312确定一组异常用户(同样参见图4)之后，可以在步骤402检测欺诈性网络活动(例如，交易欺诈、恶意网络活动等)。例如，服务器计算机102可以基于所述一组异常用户检测欺诈性网络活动。可以(例如，与单独评估所有网络活动相比)基于所提供的一组异常用户检取和评估网络资源活动的数据，这可以减少检测网络中欺诈所需的总体计算资源使用和时间。响应于检测到欺诈性网络活动，可以在步骤404执行至少一个欺诈缓解过程。例如，服务器计算机102可以阻止与异常用户的计算装置(例如，支付装置)相关联的其它网络通信，限制与异常用户相关联的多种类型的通信，限制异常用户对网络资源的访问等。这样做可以减轻计算机资源损失，并且可以解决由异常高的网络资源活动引起的网络活动负担。

[0138] 合成数据的方法评估

[0139] 基于500个用户(节点)访问组织内的资源的情境，针对合成数据集评估前述系统和方法以模拟六层图。如果两个用户访问相同的资源，则他们(R1与R2)之间可能存在无向加权边缘。

[0140] 用随机数初始化层合并阶段16的权重。使用初始合并权重获得合并图Gmerge。利用初始合并图Gmerge，用k均值聚类算法计算初始聚类质心。以niter次迭代训练权重$\overline{w}$。在受监督的学习环境中，算法将向用户显示顶部h＝10和底部h＝10个节点(基于使用当前Gmerge估计的每个节点的当前异常得分)，并且要求用户对2h个所提供节点进行注释。值h是超参数，其可以基于在反馈中请求的标签数来设置。受监督的学习环境可能会也可能不会在每次迭代中要求反馈，但可能会将对反馈的请求错开到每几次迭代或更多。可以基于所需的监督级别设置反馈之间的迭代次数。在获得反馈之后，基于总损失(参见公式12)更

新$\overline{w}$,并用更新后的$\overline{w}$重新生成Gmerge。在多次迭代之后,将学习到的$\overline{w}$作为异常检测问题的选定上下文返回给用户。

[0141] 为多层图生成六个层,其中三个良好层与异常检测任务相关并且三个不良层与之不相关。当仅考虑三个相关层时,500个用户形成五个集群。这提供了良好层的最终学习权重应高于不良层的期望。

[0142] 对于每个用户节点,通过标识与主题用户节点最接近的50个用户节点来确定对等方。对于五个集群中的每个集群,随机分配平均值和标准偏差以形成高斯分布,这进一步为所述集群中的用户(R3)分配了属性。为了注入异常用户,基于所述用户的集群的高斯分布,改变用户子集(5%)以使相关联的属性为三个标准偏差。还基于注入的异常为节点(R4)生成反馈标签。

[0143] 在受监督(改变超参数α和β)和无监督设置(改变超参数α、β和γ)下对合成数据集进行敏感性分析。将所描述的系统的性能与使用单个图层进行对等选择的对等分组基准进行比较,所述单个图层可以是各图层中的任一个或所有各层的平均层。使用曲线下面积(AUC)得分来评估性能。

[0144] 如下执行基准方法,依次取每个层和所有层的平均值:

[0145] 表1

[0146]

图	AUC
地面真相	1.0000
平均值	0.4370
层0	0.4500
层1	0.5438
层2	0.5063
层3	0.4527
层4	0.4969
层5	0.4917

[0147] 如下表2-5所示,所描述系统在受监督和无监督设置下通常都优于基准方法。表2-5中的每一个示出了给定不同的超参数α(行)和β(列)的所描述系统的AUC得分。表2反映了所描述系统在无监督方法中的性能,其中γ=0,并且α和β以0.0、0.1、1.0和10.0的值变化。

[0148] 表2

[0149]

		β			
		0.0	0.1	1.0	10.0
α	0.0	-	0.9992	0.9972	0.9983
	0.1	0.7817	0.9984	0.9985	0.9978
	1.0	0.9990	0.8908	0.9981	0.9997
	10.0	0.7964	0.7972	0.8538	0.9979

[0150] 表3反映了所描述系统在半监督方法中的性能,其中γ=0.1,并且α和β以0.0、

0.1、1.0和10.0的值变化。

[0151] 表3

		β			
		0.0	0.1	1.0	10.0
α	0.0	-	0.9991	0.9981	0.9988
	0.1	0.9992	0.9993	0.9989	0.9983
	1.0	0.8485	0.9043	0.9993	0.9988
	10.0	0.7953	0.9976	0.9992	0.9655

[0152]

[0153] 表4反映了所描述系统在半监督方法中的性能，其中γ＝1，并且α和β以0.0、0.1、1.0和10.0的值变化。

[0154] 表4

		β			
		0.0	0.1	1.0	10.0
α	0.0	-	0.9990	0.9981	0.9987
	0.1	0.7917	0.9989	0.9991	0.9985
	1.0	0.9976	0.9362	0.9979	0.9991
	10.0	0.9984	0.8066	0.8648	0.9992

[0155]

[0156] 表5反映了所描述系统在半监督方法中的性能，其中γ＝10，并且α和β以0.0、0.1、1.0和10.0的值变化。

[0157] 表5

		β			
		0.0	0.1	1.0	10.0
α	0.0	-	0.9205	0.9982	0.9992
	0.1	0.5216	0.5589	0.9982	0.9995
	1.0	0.5012	0.8497	0.9995	0.9987
	10.0	0.9012	0.9987	0.8339	0.9992

[0158]

[0159] 除了通过AUC得分评估所描述的系统之外，还通过预测层权重的值来评估所描述的系统。对于合成数据集的地面真相，层权重被分配为0.2508、0.3857、0.3635、0.0000、0.0000和0.0000，这指示前三个层是良好层，而其余层是不良层。所描述的系统能够预测层权重值为0.2470、0.3852、0.3602、0.0025、0.0024和0.0027，这非常接近初始设置值。总之，所描述的系统在检测异常方面示出了改进的性能，这会提高检测准确性及其缓解，从而提高网络效率。

[0160] 尽管已出于说明的目的而基于当前被认为是最实用和优选的实施例或方面详细描述了本发明，但应理解，此类细节仅用于所述目的，且本发明不限于所公开实施例，而相反，旨在涵盖在所附权利要求书的精神和范围内的修改和等效布置。例如，应理解，本发明

预期,在可能的范围内,任何实施例的一个或多个特征可以与任何其它实施例的一个或多个特征组合,并且可以用与本发明中呈现的次序不同的次序采取一个或多个步骤。

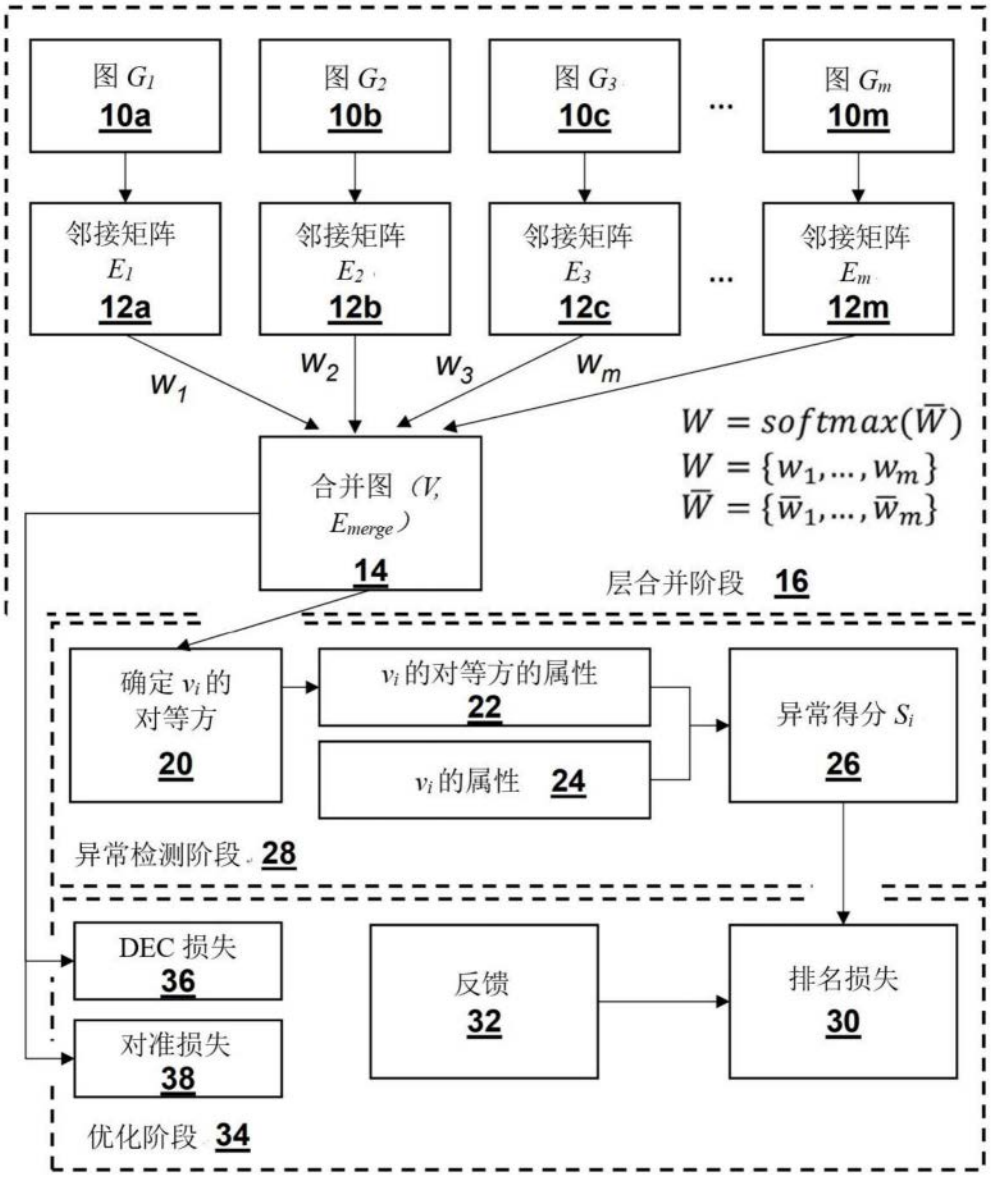


图 G_1 10a
图 G_2 10b
图 G_3 10c
...
图 G_m 10m
邻接矩阵 E_1 12a
邻接矩阵 E_2 12b
邻接矩阵 E_3 12c
...
邻接矩阵 E_m 12m
w_1
w_2
w_3
w_m
$W = softmax(\bar{W})$
$W = \{w_1, \ldots, w_m\}$
$\bar{W} = \{\bar{w}_1, \ldots, \bar{w}_m\}$
合并图 (V, E_{merge}) 14
层合并阶段 16
确定 v_i 的对等方 20
v_i 的对等方的属性 22
v_i 的属性 24
异常得分 S_i 26
异常检测阶段 28
DEC 损失 36
对准损失 38
反馈 32
排名损失 30
优化阶段 34

图1

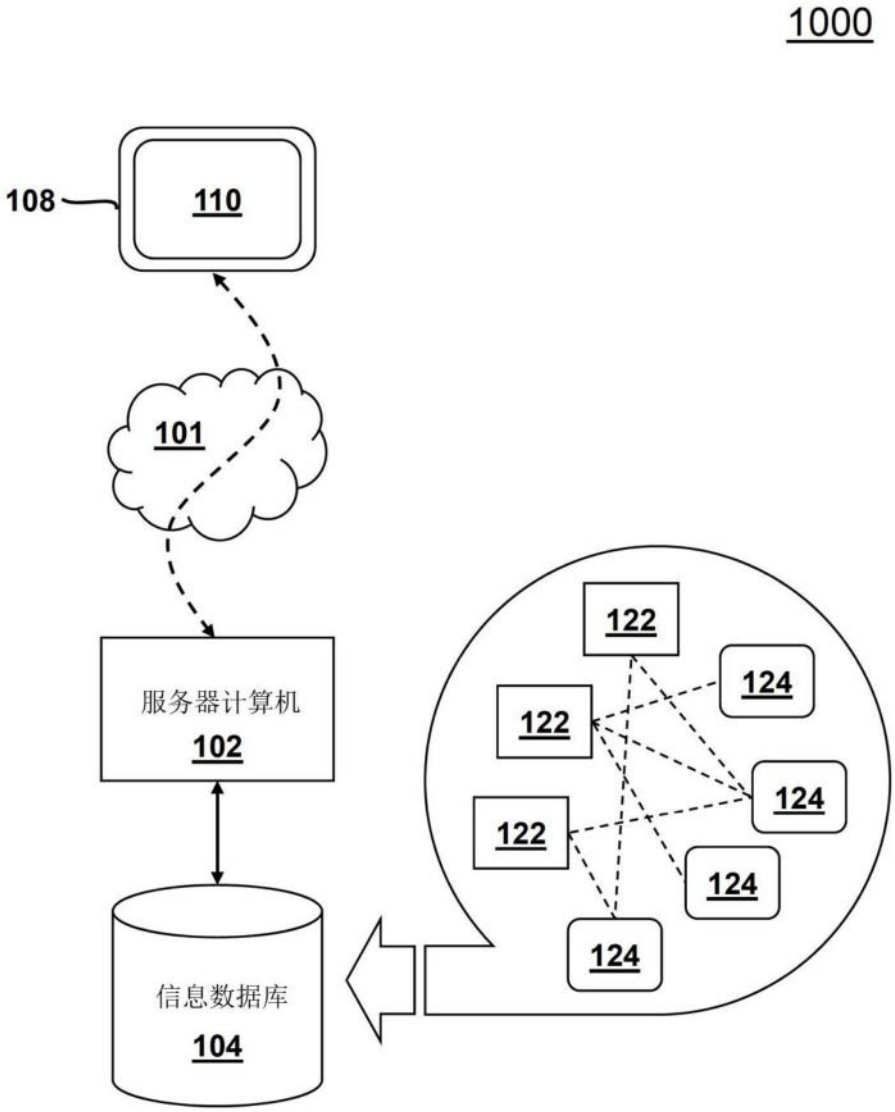

1000
108
110
101
服务器计算机
102
信息数据库
104
122
122
122
124
124
124
124

图2

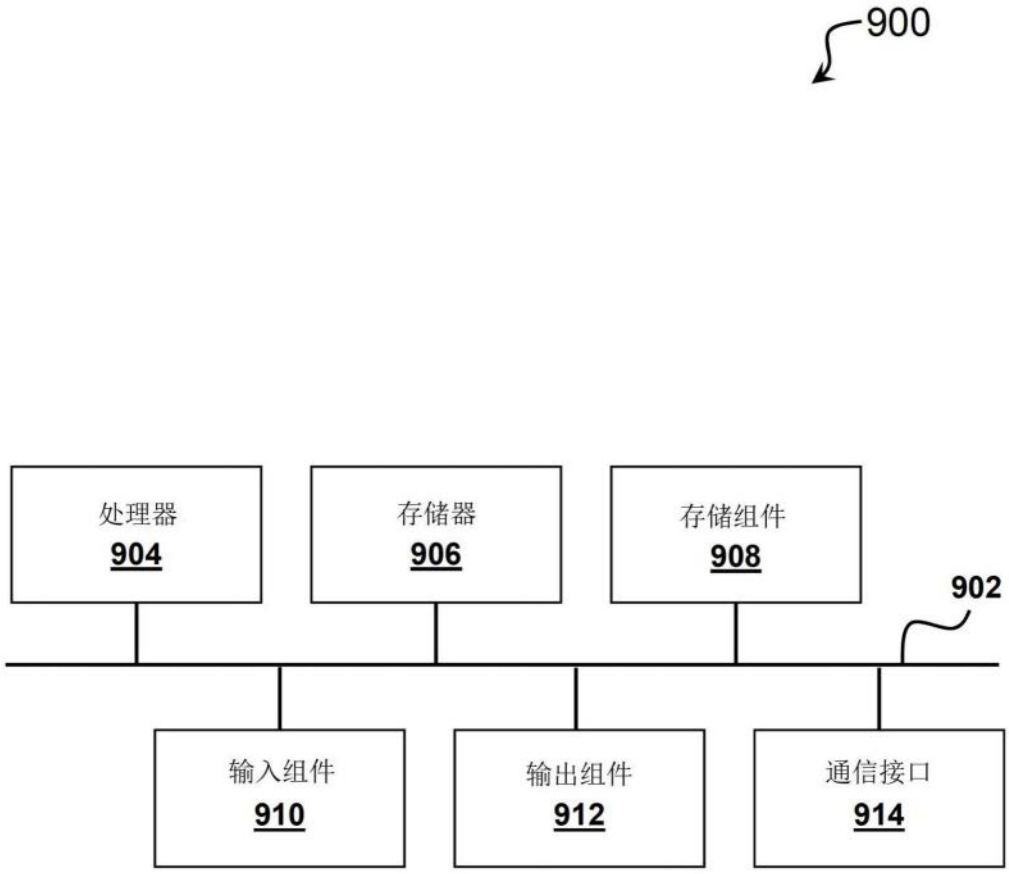


图3

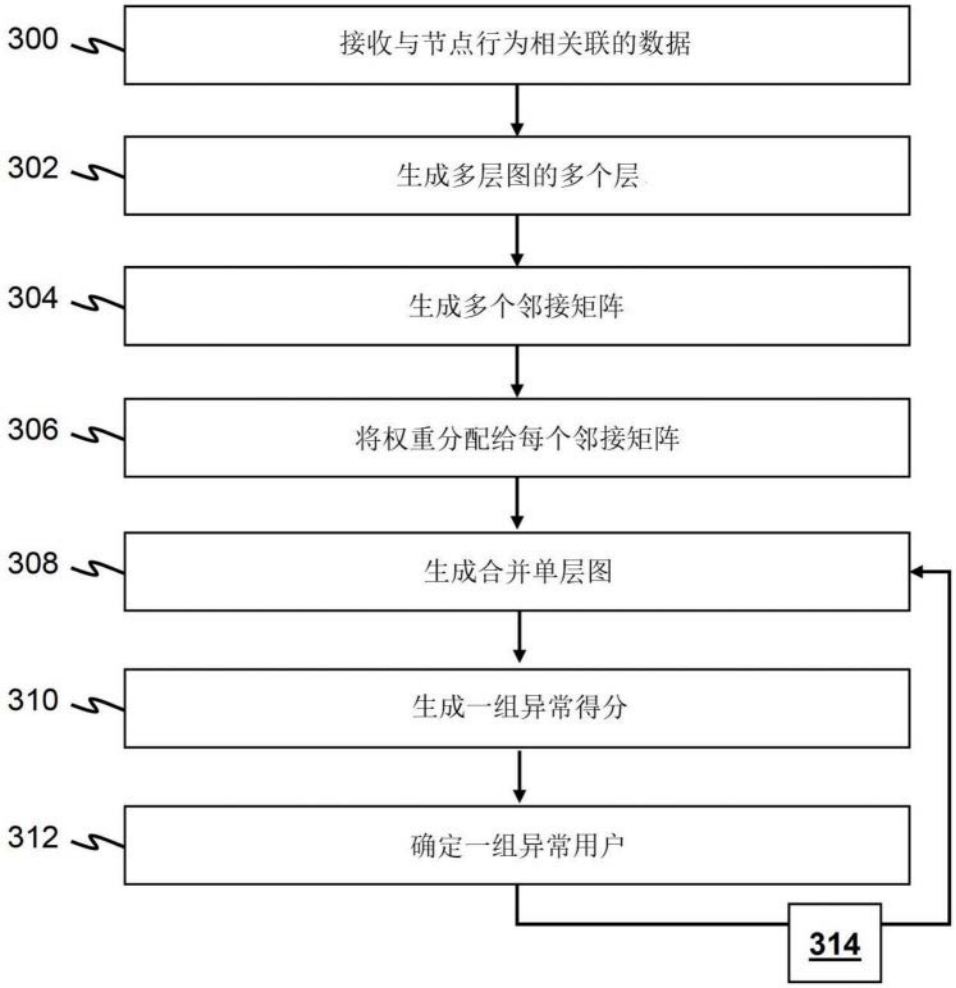

300
接收与节点行为相关联的数据
302
生成多层图的多个层
304
生成多个邻接矩阵
306
将权重分配给每个邻接矩阵
308
生成合并单层图
310
生成一组异常得分
312
确定一组异常用户
314

图4

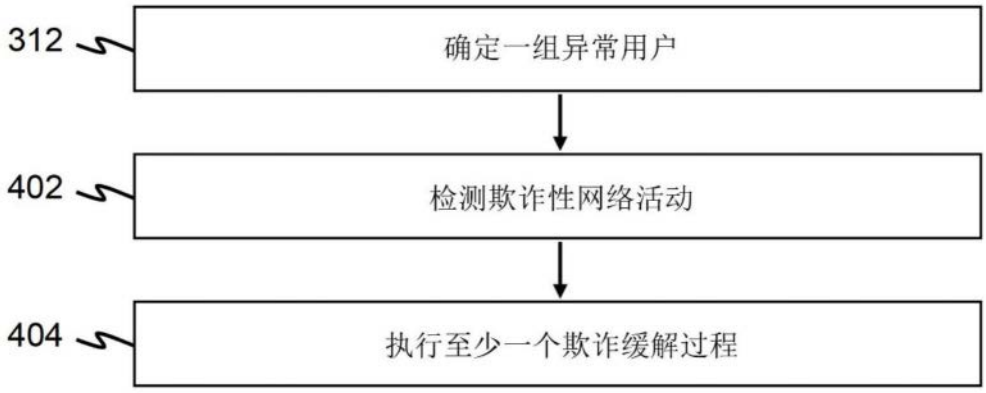

312
确定一组异常用户
402
检测欺诈性网络活动
404
执行至少一个欺诈缓解过程

图5