(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111936996 B
(45)授权公告日 2024.10.18

(21)申请号 201980007477.3
(22)申请日 2019.04.25
(65)同一申请的已公布的文献号
申请公布号 CN 111936996 A
(43)申请公布日 2020.11.13
(30)优先权数据
15/966,450 2018.04.30 US
(85)PCT国际申请进入国家阶段日
2020.07.06
(86)PCT国际申请的申请数据
PCT/US2019/029098 2019.04.25
(87)PCT国际申请的公布数据
WO2019/212852 EN 2019.11.07

(73)专利权人 甲骨文国际公司
地址 美国加利福尼亚
(72)发明人 P·伍德沃德 S·A·塔克 S·M·金斯
(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
专利代理师 冯薇

(51)Int.Cl.
G06F 21/62(2006.01)
(56)对比文件
US 2006259954 A1,2006.11.16
审查员 邢露

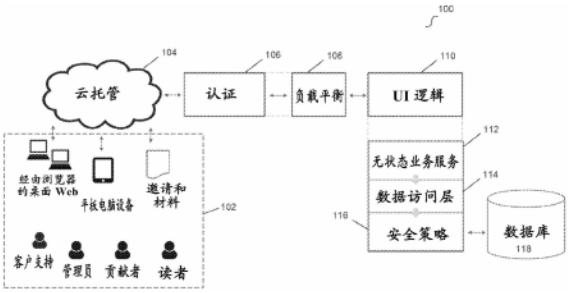
权利要求书2页 说明书30页 附图12页

(54)发明名称

为节点网络提供安全数据管理的方法、系统和介质

(57)摘要

实施例包括用于为节点网络提供安全数据管理的系统和方法。可以存储具有多个连接节点的网络,所述节点表示网络的实体。可以从网络的第一节点接收检索关于网络的第二节点的数据的请求。可以生成查询以检索所请求的数据。可以基于存储在受信存储库处的对第一节点的许可来过滤查询。可以基于对第一节点的许可来对经过滤的查询的结果中的字段进行校订。并且经校订的结果可以被提供给第一节点。



CN 111936996 B

1.一种用于为节点网络提供安全数据管理的方法,所述方法包括:

存储具有多个连接节点的网络,所述节点表示网络的实体,其中所述网络被映射到数据库的一个或多个关系数据表上;

从网络的第一节点接收检索关于网络的第二节点的数据的请求;

生成查询以从所述数据库检索所请求的数据;

通过用提供对所述数据库的记录级别访问的安全参数加强所述查询,基于存储在受信存储库处的对第一节点的许可来过滤所述查询,其中用于加强所述查询的安全参数包括一个或多个键,使得当所述一个或多个键包括与所述查询所请求的关系数据表内的受保护的记录对应的键时,检索所述受保护的记录;

基于对第一节点的许可,对经过滤的查询的结果中的字段进行校订;以及

将所校订的结果提供给第一节点。

2.如权利要求1所述的方法,还包括:

用于加强所述查询的所述一个或多个键基于相对于第二节点的对第一节点的许可。

3.如权利要求2所述的方法,其中,所述请求是从第一节点的经认证的用户接收的。

4.如权利要求3所述的方法,其中,所述经认证的用户具有查看连接到第一节点的节点的至少一些数据的许可,第一节点连接到第二节点。

5.如权利要求3所述的方法,其中,所述经认证的用户具有查看包括具有第一节点的路径的节点的至少一些数据的许可,第一节点在具有第二节点的路径上。

6.如权利要求3所述的方法,其中存储许可文件,所述许可文件定义对所述关系数据表中的一个或多个关系数据表的访问许可,该访问许可是基于拥有记录的拥有者节点和拥有者节点与请求访问的节点之间的关系针对所述关系数据表中的每个记录定义的。

7.如权利要求6所述的方法,其中,所述受信存储库不变地存储网络节点的多个键。

8.如权利要求7所述的方法,其中

所述一个或多个键包括通过访问所述许可文件从所述受信存储库检索的键列表,并且所述键列表是针对根据第一节点与节点子集之间的关系而被许可由第一节点访问的所述节点子集的。

9.如权利要求3所述的方法,其中,所述实体包括供应商和客户,并且节点之间的路径表示用于一个或多个产品的供应链网络。

10.如权利要求7所述的方法,其中,所述经认证的用户具有访问供应链网络的许可,所述供应链网络包括第一节点、包括第一节点的供应商或包括第一节点的客户。

11.一种非暂态计算机可读介质,具有存储在其上的指令,所述指令在由处理器执行时使得所述处理器为节点网络提供安全数据管理,所述提供包括:

存储具有多个连接节点的网络,所述节点表示网络的实体,其中所述网络被映射到数据库的一个或多个关系数据表上;

从网络的第一节点接收检索关于网络的第二节点的数据的请求;

生成查询以从所述数据库检索所请求的数据;

通过用提供对所述数据库的记录级别访问的安全参数加强所述查询,基于存储在受信存储库处的对第一节点的许可来过滤所述查询,其中用于加强所述查询的安全参数包括一个或多个键,使得当所述一个或多个键包括与所述查询所请求的关系数据表内的受保护的

记录对应的键时,检索所述受保护的记录;

基于对第一节点的许可,对经过滤的查询的结果中的字段进行校订;以及

将所校订的结果提供给第一节点。

12.如权利要求11所述的计算机可读介质,其中,所述请求是从第一节点的经认证的用户接收的。

13.如权利要求12所述的计算机可读介质,其中存储许可文件,所述许可文件定义对所述关系数据表中的一个或多个关系数据表的访问许可,该访问许可是基于拥有记录的拥有者节点和拥有者节点与请求访问的节点之间的关系针对所述关系数据表中的每个记录定义的。

14.如权利要求13所述的计算机可读介质,其中,所述受信存储库不变地存储网络节点的多个键。

15.如权利要求14所述的计算机可读介质,其中

所述一个或多个键包括通过访问所述许可文件从所述受信存储库检索的键列表,其中所述键列表是针对根据第一节点与节点子集之间的关系而被许可由第一节点访问的所述节点子集的。

16.如权利要求12的计算机可读介质,其中所述实体包括供应商和客户,并且节点之间的路径表示用于一个或多个产品的供应链网络,并且其中所述经认证的用户具有访问供应链网络的许可,所述供应链网络包括第一节点、包括第一节点的供应商或包括第一节点的客户。

17.一种用于为节点网络提供安全数据管理的系统,包括:

处理设备,与存储器设备进行通信,所述处理设备被配置为为节点网络提供安全数据管理,所述提供包括:

存储具有多个连接节点的网络,所述节点表示网络的实体,其中所述网络被映射到数据库的一个或多个关系数据表上;

从网络的第一节点接收检索关于网络的第二节点的数据的请求;

生成查询以从所述数据库检索所请求的数据;

通过用提供对所述数据库的记录级别访问的安全参数加强所述查询,基于存储在受信存储库处的对第一节点的许可来过滤所述查询,其中用于加强所述查询的安全参数包括一个或多个键,使得当所述一个或多个键包括与所述查询所请求的关系数据表内的受保护的记录对应的键时,检索所述受保护的记录;

基于对第一节点的许可,对经过滤的查询的结果中的字段进行校订;以及

将所校订的结果提供给第一节点。

18.一种计算机程序产品,所述计算机程序产品包括指令,所述指令在由处理器执行时,使得所述处理器执行如权利要求1-10中任一项所述的方法。

为节点网络提供安全数据管理的方法、系统和介质

[0001] 相关申请的交叉引用

[0002] 本申请要求于2018年4月30日提交的编号为15/966,450的美国专利申请的优先权,该申请的公开内容通过引用并入本文。

技术领域

[0003] 本公开的实施例涉及使用基于网络的访问许可为节点网络提供安全数据管理。

背景技术

[0004] 近年来,社交网络已经证明连接的有用性。连接节点的大型网络可以允许参与实体识别新的机会,无论这些机会是新的友谊、业务联系还是其它有用的连接。这些网络还具有发掘连接节点的组之间的协同作用的潜力。但是,连接节点的益处并非没有风险。大型网络(诸如社交网络)一直受与数据隐私、身份管理和其它数据共享相关问题的困扰。另外,由于连接的动态性质,在连接节点上执行数据分析可能带来独特的计算挑战。

发明内容

[0005] 本公开的实施例涉及对现有技术进行了实质性改进的用于为节点网络提供安全数据管理的系统和方法。

[0006] 可以存储具有多个连接节点的网络,所述节点表示网络的实体。可以从网络的第一节点接收检索关于网络的第二节点的数据。可以生成查询以检索所请求的数据。可以基于存储在受信存储库处的对第一节点的许可来过滤查询。可以基于对第一节点的许可来对经过滤的查询的结果中的字段进行校订。并且经校订的结果可以被提供给第一节点。

[0007] 实施例的特征和优点在下面的描述中阐述,或者将从描述中变得显而易见,或者可以通过实践本公开而获知。

附图说明

[0008] 通过以下结合附图对优选实施例的详细描述,进一步的实施例、细节、优点和修改将变得显而易见。

[0009] 图1图示了根据示例实施例的用于管理节点网络的数据处理的系统。

[0010] 图2图示了根据示例实施例的可操作地耦合到网络数据管理系统的计算设备的框图。

[0011] 图3图示了根据示例实施例的用于管理节点网络的数据处理的功能图解。

[0012] 图4图示了根据示例实施例的表示节点网络的图。

[0013] 图5图示了根据示例实施例的用于网络数据处理的关系数据表。

[0014] 图6图示了根据示例实施例的用于节点网络的增量处理的流程图。

[0015] 图7图示了根据示例实施例的用于节点网络的数据处理的安全管理的功能图解。

[0016] 图8图示了根据示例实施例的用于配置节点网络的视图的示例图形用户界面。

[0017] 图9图示了根据示例实施例的网络数据的饼图视图。

[0018] 图10图示了根据示例实施例的网络数据的表视图。

[0019] 图11图示了根据示例实施例的网络数据的网络图视图。

[0020] 图12图示了根据示例实施例的供应链的世界视图。

[0021] 图13图示了根据示例实施例的供应链数据的另一个世界视图。

[0022] 图14图示了根据示例实施例的供应链的另一个世界视图。

[0023] 图15图示了根据示例实施例的用于利用增量处理来管理节点网络的示例方法。

[0024] 图16图示了根据示例实施例的用于为节点网络提供安全数据管理的示例方法。

具体实施方式

[0025] 实施例管理节点网络的数据处理。示例网络可以包括多个节点,这些节点之间具有多个连接。在一些实施例中,网络可以是具有各种信息共享度的社交网络。有时,可以在两个先前未连接的节点之间生成新连接,或者可以断开先前连接的节点之间的连接。可以基于网络的当前配置(例如,节点之间的当前连接)来识别一条或多条路径。例如,路径可以从第一节点开始,并且在终止于第五节点之前经过第二节点、第三节点和第四节点。这样的识别出的路径可以用于识别模式、趋势或风险、执行预测或用于其它分析目的(即,取决于网络内的节点和特定的实施方式)。

[0026] 但是,这些网络的动态性质带来了风险和计算挑战。例如,社交网络经常在变化、构建新的节点连接并拆除旧的节点连接。因此,节点之间的路径识别在计算上可能很繁琐。如本文进一步详述的,实施例利用滴馈(drip fed)增量处理来管理网络,其在维持动态更新功能的同时实现计算效率。

[0027] 另外,在包括机密或其它敏感信息的网络中,信息共享可能具有挑战性。在一些实施例中,可以进一步定义节点连接(例如,供应商、客户、潜在供应商、潜在客户、社交连接等)以表征节点之间的关系。在这些示例中,可以基于连接类型、距网络中给定节点的距离以及给定节点的自定义首选项来定制由网络中给定节点共享的信息。实施例包括安全协议,以确保根据这些信息共享策略来检索特定于用户的数据。

[0028] 在一些实施例中,网络中的节点可以表示供应链中的供应商、中间商(intermediaries)和/或客户。例如,节点之间的连接可以表示这些实体之间的各种关系。路径可以表示多个实体之间的扩展关系。例如,通过供应商/客户关系连接的多个节点的路径可以表示商品或产品的供应链。

[0029] 基于节点之间的连接,这种网络也可以被称为图。遍历此图可能是有用的,例如,以识别供应链中的链接(link)、可以用于调整供应链的潜在链接、供应链的风险(例如,地理风险、政治风险、天气风险等),以及用于其它有用的目的。但是,由于这些网络中的一些网络(例如,社交网络)的动态性质,诸如,节点之间的连接之间的频繁变化,遍历表示节点网络的图可能带来特定的计算挑战。

[0030] 实施例实现了预计算解决方案和聚合队列中的变化记录的滴馈增量。在基于排队的变化记录(例如,点滴(drip))更新网络中的数据后,可以对图进行处理以生成针对图的节点的多个直接访问向量。实施例包括维护可以高效地检索与图遍历相关的数据的预计算网络数据的版本。例如,针对给定节点的直接访问向量指示包括针对给定节点的一条或多

条潜在路径。在一些实施例中,图处理/预计算解决方案可以包括确定传递闭包(transitive closure)。

[0031] 然后可以使用预计算解决方案和/或生成的直接访问向量来高效地遍历该图。例如,在所描述的供应链实施例中,可以基于节点的直接访问向量为给定节点识别一条或多条路径,其中这些路径可以是供应链、潜在的供应链或客户与供应商之间的某种其它关系。在各种实施例中,滴馈增量和预计算解决方案维护易于用于高效遍历的图(例如,社交网络)。

[0032] 在一些实施例中,网络的实体(例如,节点)可以具有与系统交互的授权用户。例如,授权用户可以编辑实体的简档、向网络的其它实体发送消息、更改与其它实体的关系、检索与网络的实体相关的数据、执行网络分析以及其它合适的功能。但是,在一些实施例中,可以与网络相关联地存储(例如,在数据存储库中)一个或多个实体的机密或敏感信息。例如,在社交网络中,系统可以存储第一实体的可以与其它实体的子集共享但不能与其余实体共享的敏感信息。在其它示例中,敏感信息可以被标记为私有,并且因此可以不与社交网络的任何其它实体共享。

[0033] 在一些实施例中,系统可以为网络的实体提供安全的数据检索。例如,安全子系统可以为授权用户维护一个或多个许可,其确定用户可以检索哪些信息。基于安全子系统,可以过滤数据检索请求,以确保授权用户仅被提供根据建立的许可的信息。例如,在对数据存储库执行搜索之前,可以使用关系过滤来根据许可过滤生成的查询。在另一个示例中,在将数据提供给授权用户之前,可以根据校订(redact)数据的许可对查询所检索的数据执行数据校订。安全子系统、关系过滤和数据校订可以用于确保对网络实体的敏感或机密数据进行安全数据管理。

[0034] 在网络中的节点表示供应链中的供应商、中间商和/或客户的实施方式中,安全数据管理可以用于向网络实体提供供应链信息。例如,可以基于图中表示网络的节点的路径来设置安全子系统处的许可。由于路径表示供应链,因此可以授予给定路径上的实体检索供应链的相关数据并分析结果的许可。实施例基于遍历图和检索到的安全数据显示具有供应链信息的图形用户界面。这些图形用户界面可以用于识别供应链的风险、分析供应链的效率以及用于其它目的。

[0035] 当前,零售供应链市场由数以百万计的从领域到分支的公司组成。通常,这些不同的公司操作不同的系统和实践来管理产品开发、采购、合规性、订单、运输、质量控制、库存、预测、补货等。由于行业整个供应链以及这种大批令人绝望的系统(尤其是对于某些易腐烂的商品,诸如食品或其它影响健康的商品)的复杂性、采用和能力,行业经常无法实现可追溯性。集成和API的范围受到限制,并且已经创建了数百个孤岛(silo)。一波新的透明解决方案和贸易网络在其与自己的供应链社区竞争时只是在增加更多的孤岛。

[0036] 实施例提供了平台,该平台允许各种系统、微型应用、物联网(“IoT”)和智能设备(由通过app(应用)商店原理进行注册来控制)彼此交换通用数据集、交易关键绩效指标(KPI)和数据链接。中央环境为零售商通提供与系统无关地监视跨许多流程的交易的能力、为供应链提供重新利用通用数据集的能力,从而提高效率,并且提供允许跨端到端流程的数据流的数据链接。实施例可以例如通过社交联网能力将社区聚集在一起。通过提供高效的平台和服务来管理多个系统和数据馈送(例如从一个仪表板)来鼓励采用。

[0037] 这样的采用可以带来许多益处。减少重复可以显著提高整个供应链的效率并改善数据质量。集中报告、可视化和监视整个供应链中的交易可提高效率、提高响应速度、使得能够预期风险并提供对于增加风险或造成中断的事故的重要的可追溯性。数据链接使各种解决方案能够在业务流程上进行通信,从而提高了满意度、用户体验和质量。开放的连接性促进了应用或设备的选择、激发了创新、激励了采用,并且可以针对世界各地的各种能力进行定制。

[0038] 现在将详细参考本公开的实施例,其示例在附图中示出。在以下详细描述中,阐述了许多具体细节以便提供对本公开的透彻理解。但是,对于本领域的普通技术人员将显而易见的是,可以在没有这些具体细节的情况下实践本公开。在其它情况下,没有详细描述众所周知的方法、过程、部件和电路,以免不必要地模糊实施例的各方面。只要有可能,相同的参考数字将用于相同的元素。

[0039] 图1图示了根据示例实施例的用于管理节点网络的数据处理的系统。系统100包括客户端设备102、云服务器104、认证服务器106、负载平衡器108、用户界面逻辑110、无状态业务服务层112、数据访问层114、安全策略116和数据库118。客户端设备102可以是计算设备,诸如台式机、膝上型平板设备、蜂窝电话等。例如,客户端设备102可以是类似于系统210的任何计算设备。在一些实施例中,客户端设备102可以执行与云服务器104进行通信以访问用于节点网络的软件服务的应用(例如,本地存储的应用、基于web的应用等)。

[0040] 例如,可以使用一种或多种web技术(例如,超文本标记语言(“HTML”)5.0、JavaScript、级联样式表(CSS)、可缩放向量图形(“SVG”)等)来实现客户端应用。可以使用台式机或移动设备从标准或移动浏览器两者查看此类应用。在一些实施例中,可以开发可下载的移动应用(例如,用于iOS、Android等)。例如,可下载的应用可以是内部使用“无控制”浏览器来显示网站的容器应用(例如,使用Cordova技术)。在各种实施例中,当使用标准浏览器(例如,桌面)、移动浏览器、可下载的应用或任何其它合适的配置时,用户对应用的体验是一致的。向客户端设备102发送和从客户端设备102接收的示例通信可以包括邀请、网络消息、与网络相关的数据以及与网络相关的其它材料。

[0041] 云服务器104可以是适合于托管用于节点网络的基于云的软件服务平台的服务器。例如,云服务器104可以是类似于系统210的任何计算设备并且/或者可以包括嵌入在**Oracle®** Cloud(Oracle云)、**Oracle®** Bare Metal、**Oracle®** WebLogic服务器和/或其它合适的部件(例如,操作系统,诸如Linux,web技术,诸如**Oracle®** Java™企业版(Enterprise Edition,“EE”)等)中的接合引擎(“EE”)的各种模块。

[0042] 在一些实施例中,云服务器104与认证服务器106、负载平衡器108和UI逻辑110进行通信。例如,客户端设备102中的一个的用户可以被认证服务器106认证。然后,可以将经认证的用户与身份管理服务中的身份相关联。认证服务器106的示例是**Oracle®**身份云服务(Identity Cloud Service,“IDCS”)。然后,用户可以基于用户的认证身份访问网络应用服务。

[0043] 负载平衡器108可以是将负载分配到一个或多个处理器(或一个或多个计算设备)以有效地管理系统的计算资源的服务器或模块。负载平衡器108可以是类似于系统210的任何计算设备。

[0044] UI逻辑110可以是服务器或模块,该服务器或模块包括用于向客户端设备102中的

一个或多个呈现用户界面的软件。例如,UI逻辑110可以与在客户端设备102之一上运行的应用进行通信,以呈现用于与用于节点网络的软件服务进行交互的界面。UI逻辑110可以将客户端设备102之一进行配置以显示本文公开的各种图形用户界面。

[0045] 无状态业务服务层112可以为节点网络提供无状态软件服务。例如,可以定义安全地检索、更新或写入网络数据、遍历网络、向网络中的参与者发送消息等的一个或多个微服务。这些无状态微服务在本文中进一步描述。

[0046] 数据访问层114可以是执行诸如查询生成之类的数据处理功能的软件层。例如,基于来自无状态业务服务层112的请求,可以在数据访问层114处接收与所存储的网络数据相关的一个或多个请求、命令或更新。可以基于接收到的请求(例如,结构化查询语言(“SQL”)查询)为数据库118生成查询或命令。

[0047] 安全策略116可以是根据存储的安全策略来保护数据库118的数据检索、更新或命令的软件层。例如,数据库118可以是用于存储网络数据的任何合适的数据库(例如,**Oracle®**关系数据库)。网络数据可以包括网络参与者的机密或敏感信息。安全策略116可以处理来自数据访问层114的更新、命令(例如,数据库写入)或检索尝试(例如,查询),以根据存储的安全策略来过滤网络数据。

[0048] 在一些实施例中,云服务器104、认证服务器106、负载平衡器108、用户界面逻辑110、无状态业务服务层112、数据访问层114、安全策略116和数据库118可以被合并到单个系统或计算设备中、可以跨各种计算设备分布,并且在一些实施方式中,可以跨各种位置分布,可以以任何其它合适的方式来配置这些的组合。在示例实施方式中,云服务器104、认证服务器106、负载平衡器108、用户界面逻辑110、无状态业务服务层112、数据访问层114、安全策略116和数据库118可以是软件、硬件或它们的组合。

[0049] 图2是根据实施例的计算机服务器/系统210的框图。如图2所示,系统210可以包括被配置为在系统210的各个部件(诸如处理器222和存储器214)之间传送信息的总线设备212和/或(一个或多个)其它通信机制。另外,通信设备220可以通过对要通过网络(未示出)从处理器222发送到另一个设备的数据进行编码并且对于处理器222对通过网络从另一个系统接收到的数据进行解码来实现处理器222和其它设备之间的连接。

[0050] 例如,通信设备220可以包括被配置为提供无线网络通信的网络接口卡。可以使用各种无线通信技术,包括红外、无线电、**Bluetooth®**(蓝牙)、Wi-Fi和/或蜂窝通信。替代地,通信设备220可以被配置为提供(一个或多个)有线网络连接,诸如以太网连接。

[0051] 处理器222可以包括一个或多个通用或专用处理器,以执行系统210的计算和控制功能。处理器222可以包括单个集成电路,诸如微处理设备,或者可以包括多个集成电路设备和/或电路板,它们协同工作以完成处理器222的功能。另外,处理器222可以执行存储在存储器214内的计算机程序,诸如操作系统215、网络管理器216和其它应用218。

[0052] 系统210可以包括用于存储信息和指令以供处理器222执行的存储器214。存储器214可以包含用于检索、呈现、修改和存储数据的各种部件。例如,存储器214可以存储在由处理器222执行时提供功能的软件模块。这些模块可以包括为系统210提供操作系统功能的操作系统215。这些模块可以包括操作系统215、被配置为管理网络的数据处理的网络管理器216以及其它应用模块218。操作系统215为系统210提供操作系统功能。网络管理器216可以包括一个或多个API,该一个或多个API使得能够进行与网络相关的数据处理的系统调

用,或者还可以提供本公开的任何其它功能。在一些情况下,网络管理器216可以被实现为存储器中配置。

[0053] 非暂态存储器214可以包括可以由处理器222访问的各种计算机可读介质。例如,存储器214可以包括以下的组合:随机存取存储器(“RAM”)、动态RAM(“DRAM”)、静态RAM(“SRAM”)、只读存储器(“ROM”)、闪存、高速缓存存储器和/或任何其它类型的非暂态计算机可读介质。

[0054] 处理器222经由总线设备212进一步耦合到显示器224,诸如液晶显示器(“LCD”)。键盘226和光标控制设备228,诸如计算机鼠标,进一步耦合到通信设备220,以使用户能够与系统210对接。

[0055] 在一些实施例中,系统210可以是更大系统的一部分。因此,系统210可以包括一个或多个附加功能模块218以包括附加功能。其它应用模块218可以包括例如嵌入在Oracle®云中的接合引擎(“EE”)的各个模块。数据库217耦合到总线设备212,以向诸如216和218之类的模块提供集中式存储,并且存储例如无线设备活动,并且在一些实施例中,存储用户简档、交易历史等。数据库217可以将数据存储在逻辑上相关的记录或文件的集成集合中。数据库217可以是操作数据库、分析数据库、数据仓库、分布式数据库、最终用户数据库、外部数据库、导航数据库、存储器中数据库、面向文档的数据库、实时数据库、关系数据库、面向对象的数据库、HFDS或本领域已知的任何其它数据库。

[0056] 虽然被示出为单个系统,但是系统210的功能可以被实现为分布式系统。例如,存储器214和处理器222可以跨共同表示系统210的多个不同的计算机分布。在一个实施例中,系统210可以是设备(例如,智能电话、平板电脑、计算机等)的一部分。

[0057] 在实施例中,系统210可以与设备分离,并且可以远程为设备提供所描述的功能。此外,可以不包括系统210的一个或多个部件。例如,对于作为用户或消费者设备的功能,系统210可以是智能电话或其它无线设备,其包括处理器、存储器和显示器,不包括图2所示的一个或多个其它部件,并且包括未在图2中示出的其它部件。

[0058] 图3图示了根据示例实施例的用于管理节点网络的数据处理的功能图解。图解300描绘了可以为网络的用户提供服务的示例软件框架。图3包括应用开发框架(“ADF”)面302、ADF任务流304、beans306、数据模型308、服务310、数据平台312、安全平台314、数据存储装置316和可扩展标记语言(“XML”)定义318。

[0059] ADF面302可以是软件框架的视图部分,包括HTML、CSS和用于提供用户界面的任何其它合适的代码。本文公开的多个图形用户界面之一可以由ADF面302提供。ADF任务流304可以用于配置一个或多个用户界面元素以执行软件功能。Beans 306可以提供用户界面逻辑,并与模型层的业务逻辑规则集成。ADF任务流304和beans306可以是软件框架的控制器部分。例如,ADF任务流304可以位于beans 306的顶部,并且实现用于客户端页面的框架。在一些实施例中,ADF任务流304可以提供一组任务流构造(construct),其可以用来管理用户通过一系列应用屏幕的行程。本文公开的图形用户界面的元素的一个或多个功能可以由ADF任务流304和/或beans 306提供。

[0060] 数据模型308可以是软件框架的模型部分。数据模型308可以提供用于在用户界面(例如,视图和控制器)和软件服务(例如,软件框架的业务服务部分)之间对接的业务逻辑规则和结构。服务310可以是软件框架的业务服务部分。服务310可以提供业务规则、逻辑、

验证和结构以使得能够例如在存储的网络数据上执行软件服务。服务310可以包括本文公开的微服务中的一个或多个。

[0061] 数据平台312、安全平台314和数据存储装置316可以是软件框架的数据服务部分。数据平台312可以将逻辑数据映射到物理存储装置。例如,基于来自服务310的请求,数据平台312可以生成数据命令(例如,查询、改变请求等)以检索、存储或改变存储在数据存储装置316处的数据。这些数据命令由安全平台314保护。安全平台314可以存储用于过滤来自数据平台312的数据命令的安全策略。因此,存储在数据存储装置316处的数据受安全平台314的保护。数据平台312和安全平台314可以由XML定义318定义。因此,这些软件部件是敏捷的,因为它们可以通过更新XML定义318容易地进行更新和/或重建。参考图7进一步描述服务310、数据平台312、安全平台314和数据存储装置316。

[0062] 返回参考图1,在一些实施例中,系统100可以为由图表示的节点网络提供软件服务。图4图示了根据示例实施例的表示节点网络的图(下文中称为网络图400)。图4中的网络图400可以表示节点402和连接404的网络。每个节点402可以表示参与图/网络的实体,并且每个连接404可以表示实体之间的关系。在一些实施例中,图4中的网络图400是有向非循环图(“DAG”)或适合于表示网络(例如,社交网络)的任何其它图。

[0063] 在一些实施例中,图1的系统100可以为由图4中的网络图400表示的网络提供软件服务。例如,节点402可以各自表示组织,并且与这些组织关联的用户可以使用客户端设备102之一来访问网络。这些用户可以与云服务器104以及系统100的其余元件进行通信,以便访问、操纵节点网络或与节点网络进行交互。例如,用户的身份可以由认证服务器106(例如,IDCS服务或任何其它合适的身份管理服务)进行认证,然后用户可以根据与他或她的认证身份相关联的许可与网络进行交互。

[0064] 在一些实施例中,由节点402表示的每个组织可以向网络注册。例如,可以为注册的组织存储简档,该简档可以包括以下中的一个或多个:名称、地址或位置(例如,纬度、经度、归属国和任何其它合适的位置信息)、与组织相关联的品牌、主页统一资源定位符(“URL”)、组织的社交媒体账户、这些的组合以及其它合适的信息。

[0065] 在实施例中,节点网络可以表示供应商、客户和/或中间商的网络。在这样的示例中,组织简档还可以包括以下中的一个或多个:出售的产品、购买的产品、来自第三方协会的证书、来自第三方协会的过期证书、直接供应商(例如,来自网络中的其它实体当中的供应商)、直接客户(例如,来自网络中的其它实体当中的客户)、商品或产品的计划(例如,配方)、商品或产品的部分(例如,成分)、这些的组合、以及针对产品或商品的买方或卖方的任何其它合适的信息。

[0066] 在一些实施例中,来自第三方协会的证书包括食品或药品安全证书(例如,清真证书、符合犹太教教规的证书)、公平贸易证书、来自一个或多个已知认证实体(例如,全球食品安全倡议(“GFSI”)、英国零售联合会(“BRC”)、食品和药品管理局(“FDA”)、美国农业部(“USDA”)、海洋管理委员会(“MSC”)、安全优质食品协会(“SQF”)等)的证书、危害分析和关键控制点(“HACCP”)证书等。这些证书通常需要续签,并且因此证书可能会不时过期。取决于商品或产品的最终目的地(例如,目的地国家和当地法规),过期的证书可能在供应链中产生潜在的问题。

[0067] 在一些实施例中,商品或产品的计划包括配方或用于制造商品或产品的成分列

表。例如,产品A可以包括一个或多个配方,诸如配方B,该配方B列出成分C、D、E和F。商品或产品的示例可以是果汁。当给定组织具有产品(诸如果汁)的配方时,该组织可以被视为另一个组织的客户。果汁中的成分可以是水果浓缩物(例如,蔓越莓、苹果等)、不同类型的水果和其它合适的成分。当给定组织具有另一个组织的配方的成分时,该组织可以被视为供应商。

[0068] 一旦被注册,组织就可以在网络中彼此交互。例如,由节点402表示的组织可以彼此发送消息、生成可以共享的帖子、"点赞"来自其它组织的帖子、向其它组织发送加入网络的邀请、以及执行适合于社交网络的其它功能。

[0069] 在一些实施例中,可以在图4中的网络图400中基于连接404在节点402之间识别一条或多条路径。例如,路径406可以包括四个节点402,如图4所示。在实施例中,节点402表示可以是涉及商品或产品的交易的客户、供应商和中间商的实体,并且路径406可以表示供应链。例如,路径406可以表示在端点(例如,客户)处终止的节点402之间的商品或产品流。在一些实施例中,端点可以是表示供应链内请求信息的实体的节点402之一。例如,表示路径406的端点的节点402可以请求关于到表示该节点的实体的商品或产品流的信息。在一些情况下,该端点可以是中间商,因为实体可以向下游客户出售商品或产品,但是路径406可以表示该实体的供应链。实体的授权用户(例如,经认证的身份)可以与网络的软件服务交互,以检索该供应链信息,如将在下面进一步详细描述的。

[0070] 在一些实施例中,连接404可以表示组织(例如,客户和供应商)之间的贸易关系。例如,组织A可以邀请组织B成为其供应商之一,和/或组织B可以邀请组织A成为其客户之一。当组织B具有组织A的配方之一的成分时,可能发生这种情况。在网络内,组织A和组织B之间的连接404可以在从一个组织发送贸易关系邀请并且被另一个组织接受时建立。

[0071] 在实施例中,一旦两个组织已发送并接受处于贸易关系的邀请,它们就可以识别哪些配方和成分依赖于这种关系。客户组织可以将其配方中使用的一些成分分配给新的供应商组织。类似地,供应商组织可以为其供应的产品的配方分配客户组织的名称。关于图4,当连接404表示贸易关系时,网络图400示出了贸易组织之间的潜在商品流(例如,供应链)。例如,当供应商组织具有与客户组织相关联的至少一个产品配方,并且客户组织具有配方,该配方具有与供应商组织相关联的至少一个成分时,该供应商组织将被显示在该客户组织的供应链内(被视为客户组织的供应链的一部分)。

[0072] 在一些实施例中,连接404可以表示(不进行贸易的)社会关系。例如,组织A可以向组织B提交社交连接请求,并且可以形成表示社交连接的连接404。

[0073] 在一些实施例中,网络数据可以被映射到关系数据库中的多个关系数据表上。图5图示了根据示例实施例的用于网络数据处理的关系数据表。图5中图示的示例数据表包括组织502、连接504、配方506、成分508、Recipe_Ingredients(配方_成分)510、Recipes_Consumers(配方_消费者)512和Ingredients_Suppliers(成分_供应商)514。数据表可以包括属性(例如,ID、名称等),并且在一些情况下可以包括键(key)信息(例如,主键和外键)。为了本公开的目的,图示的数据模式已经被简化,并且用于网络数据的数据模式的实现可能比图示的示例大得多。也可以实现其它合适的模式。

[0074] 在一些实施例中,组织502可以存储组织简档信息,诸如组织ID、名称、本文详述的其它简档信息以及任何其它合适的组织简档信息。连接504可以存储关于节点之间的连接

的信息,诸如连接ID、消费ID(例如,客户ID)、生产ID(例如,供应商ID)以及任何其它合适的连接信息。在一些实施例中,节点之间的连接可以基于商品或产品的实现流(例如,实现的供应商/客户关系)。

[0075] 在一些实施例中,配方506可以存储配方信息,诸如配方ID、配方描述、所有者组织ID以及任何其它合适的配方信息。类似地,成分508可以存储成分信息,诸如成分ID、成分标题、所有者组织ID以及任何其它合适的成分信息。Recipe_Ingredients 510可以存储所拥有的配方和所拥有的成分之间的关联。

[0076] 在一些实施例中,Recipes_Consumers 512可以存储使配方与消耗配方的连接相关联的信息,诸如由存储在连接504中的连接ID表示的组织之间的连接。类似地,Ingredients_Suppliers 514可以存储关于成分和供应成分的连接的信息。例如,Recipes_Consumers 512和Ingredients_Suppliers 514可以用于确定来自给定连接的组织如何连接(例如,它们之间存在的配方/成分贸易关系)。

[0077] 例如,第一组织拥有的配方A可以包括成分B、C和D。第二组织拥有的成分可以包括成分D、E和F。因为第一组织拥有包括由第二组织所拥有的成分(成分D)的配方,因此在第一组织和第二组织之间存在潜在的商品或产品流。在一些示例中,第一组织和第二组织可以确认贸易关系,从而可以形成连接(具有连接ID)。一旦被连接,第一组织就可以将配方A与该连接相关联,并且第二组织可以将成分D与该连接相关联。可以在图5中所示的表中填充相关的连接、成分和配方信息。

[0078] 返回参考图4,将节点网络映射到数据表上可以包括存储组织502中的针对节点402的特定于实体(例如,组织简档)的信息以及存储连接504中的连接404的节点连接信息。如下面详述的,处理网络以生成针对节点402的向量可以基于由配方506、成分508、Recipe_Ingredients 510、Recipes_Consumers 512和/或Ingredients_Suppliers 514指示的拥有的配方和拥有的成分之间的关联来管理。

[0079] 在一些实施例中,(例如,与网络的节点/实体之一相关联的)用户可以请求更新或改变。例如,经认证的用户可以请求对网络的改变,诸如对商品或产品流的改变(例如,新的或更新的供应商/客户关系)、新的商品或产品流、对拥有的配方或成分的改变、新的配方或成分、或任何其它合适的改变。对网络的改变还可以包括基于新注册的组织创建新的节点/实体。新的节点/实体可以基于现有的或新的商品或产品流来生成与现有实体/节点的连接。

[0080] 图4所示的新连接408可以是对网络图400的改变的结果。例如,通过新连接408连接的节点402可以录入用于商品或服务贸易的协定。基于对网络图400的更新,生成新路径和新潜在路径。如本文中详述的,处理以高变化频率而遍历诸如社交图之类的图的请求可能在计算上具有挑战性。实施例实现了滴馈增量处理来提供即使存在频繁变化的情况下也能遍历网络图400的高效技术。

[0081] 图6图示了根据示例实施例的用于节点网络的增量处理的流程图。可以请求增量602对(例如,存储在关系数据表中的)网络数据606的更新或改变。增量602可以存储在队列604中,诸如先进先出(FIFO)队列或任何其它合适的队列。每次处理的改变或更新都可以被视为滴馈增量处理流中的点滴。当对网络数据606执行更新或改变时,可以改变网络实体之间的一条或多条路径或潜在路径。例如,增量602之一可能导致改变,该改变(例如,基于对

拥有的成分、配方或产品的改变)生成新的产品或商品流(或新的潜在的产品或商品流)和/或生成类似于新连接408的连接。在完成对网络数据606的更新之后,可以执行下一个点滴(例如,可以根据队列604顶部的增量602来更新或改变网络数据606)。

[0082] 在一些实施例中,网络数据606可以表示基础(underlying)网络数据的预计算版本(例如,存储在图5所示的关系表中)。例如,网络数据606可以是对网络信息的高效检索有用的预计算数据,诸如节点/实体之间的路径(例如,供应链信息)。用户(例如,具有适当安全性的经认证的用户)例如通过登录客户端应用并与之交互可以容易地更新/改变基础网络数据,并且这些更新/改变可以反映在基础网络数据中,而无需使用队列。但是,增量602可以表示影响网络数据606(例如,基础网络数据的预计算版本)的更新/改变。实施例在更新网络数据606以维护基础网络数据的该预计算版本时实现滴馈增量技术,这对于高效检索网络信息是有用的。

[0083] 在一些实施例中,网络数据606存储在与基础网络数据分离的关系数据表的集合中。网络数据606可以被认为是预计算形式的基础网络数据的副本。为了维持这种预计算形式(以及高效的网络数据检索的益处),通过公开的滴馈增量技术来管理更新。换句话说,它是对(例如,在队列604中)排队并被执行为滴馈增量的相关数据表的单独集合的更新/改变(例如,增量602)。网络数据606最终与基础网络数据一致(在执行滴馈增量之后),并提供使得能够进行网络的高性能查询的结构。

[0084] 在一些实施例中,增量602的处理是基于可用的计算资源在尽力而为条件下执行的。处理延迟可能是由于服务器(根据用户的活动)可以生成增量602的速率与预计算引擎可以从队列604处理/移除它们的速率之间存在差异。在一些实施例中,增量处理可能延迟和/或可能以预定间隔被执行(例如,延迟可能内置在处理中)。

[0085] 在一些实施例中,可以跟踪(track)对基础网络数据的更新/改变(例如,对图5的关系数据表的改变)以确定影响存储网络数据606的单独数据表的改变。例如,以下场景表示影响网络数据606的改变(例如,要进行排队的改变):

[0086] 1)两个组织创建新的贸易关系或终止现有的贸易关系;

[0087] 2)两个组织终止现有的贸易关系;

[0088] 3)由客户或供应商维护的配方或成分被更新,以关联新组织作为(产品/配方的)客户或(成分的)供应商;以及

[0089] 4)由客户或供应商维护的配方或成分被更新,使得他们移除不再作为成分的供应商或产品/配方的客户的组织。

[0090] 在一些实施例中,可以跟踪对基础网络数据的更新/改变以识别这些以上场景中的一个或多个。例如,参考图5的关系表结构,可以将以下更新/改变识别为影响网络数据606。

[0091] 向/从配方添加/删除消费者(对RECIPES_CONSUMERS 512进行插入(INSERT)、删除(DELETE))

[0092] 向/从配方添加/删除成分(对表RECIPE_INGREDIENTS 510进行插入、删除)

[0093] 向/从成分添加/删除供应商(对表INGREDIENTS_SUPPLIERS 514进行插入、删除)

[0094] 应该注意的是,在这些情况中的每种情况下,改变都可以由用户(例如,具有许可的经认证的用户)使用客户端应用来实现。所公开的技术的实施例产生与这些改变对应的

增量602,该增量602用于更新网络数据606以维护基础网络数据的预计算版本。

[0095] 在一些实施例中,数据库功能(例如,Oracle®RDBMS触发器)可以用于处理增量602。排队的示例技术包括Oracle®高级排队(Advanced Queuing,“AQ”)。可以处理队列604中的增量602,并且可以递增地更新存储网络数据606(例如,包括图的传递闭包)的数据表。在一些实施例中,可以在其中实现多个队列消费者,并且这些消费者可以由各种组织共享。存储网络数据606的数据表的示例模式可以如下:

[0096] PC_RECIPE_CON_SUP—存储配方与消费组织关系(配方ID、消费组织ID和供应(拥有)组织ID)的预计算副本。

[0097] PC_RECIPE_INGREDIENTS—存储成分与配方关系(配方ID和成分ID)的预计算副本。

[0098] PC_INGREDIENT_CON_SUP—存储成分与供应组织关系的预计算副本(成分ID、消费(拥有)组织ID和供应组织ID)。

[0099] PC_INGREDIENT_CONNECTIONS—将预计算版本的成分存储到可能的成分连接中,并且因此可以用于遍历通过网络。这用于辅助对传递闭包的增量评估。

[0100] PC_ORG_TC_RECURSIVE—将预计算版本的组织存储到组织传递闭包中,并且作为应用用来查询网络的表之一。在一些实施例中,表的设计是简单的,并且由(该递归传递闭包条目(entry)的)ID、消费组织ID和供应组织ID组成。

[0101] PC_ORG_TC_PATH—在PC_ORG_TC_RECURSIVE中存储可以从消费组织ID到供应组织ID获得的所有方式(路径)的预计算版本。

[0102] PC_ORG_TC_ING_CONN_PATH_H—该表保持成分路径的报头(header)记录。该记录包括该成分路径使之可能的来自PC_ORG_TC_PATH的组织传递闭包路径ID。这用于辅助对传递闭包的增量评估。

[0103] PC_ORG_TC_ING_CONN_PATH_D—该表保持来自PC_ORG_TC_ING_CONN_PATH_H的成分路径的详细记录。这用于辅助对传递闭包的增量评估。

[0104] 实施例包括生成对存储与被识别为影响网络数据606的跟踪的改变对应的网络数据606(例如,以上模式)的数据表的更新/改变(例如,增量602)。例如,跟踪的改变可以被识别为对两个实体/节点之间的贸易关系的更新。可以生成一个或多个增量602来更新存储网络数据606的数据表。例如,基于实现的模式,跟踪的改变可以对应于更新/改变存储网络数据606的多个表的多个增量602。

[0105] 在一些实施例中,执行点滴(例如,增量)包括确定网络的传递闭包。参考图4,可以基于作为具有给定节点的路径或潜在路径的一部分的节点402的子集,为给定节点维护网络图400的传递闭包。可以基于在为网络数据606维护的数据模式(例如,以上公开的数据模式)中存储和更新的成分、配方、关联实体/节点以及相关信息来识别商品或产品的潜在连接或流。一般而言,对于给定节点,图4中的网络图400的传递闭包表示可以被包括在具有给定节点的路径(例如,现有路径或潜在路径)上的节点402的子集。网络图400的传递闭包可以以任何合适的方式来确定(例如,图的广度优先或深度优先搜索、Floyd-Warshall算法等)。

[0106] 在确定传递闭包时,可以使用枚举从一个节点到其它节点的路径的规则或数据集。在各种实施例中,节点/实体之间建立的贸易关系可以用作枚举路径的技术。以下是用

于确定图4中的网络图400的传递闭包的示例算法：

[0107] 对于(For)节点X：

[0108] 对于X的每个配方，

[0109] 对于配方的每个成分

[0110] 对于成分的每个供应商

[0111] 将供应商添加到潜在供应商节点列表

[0112] 对于“潜在供应商节点”列表中的每个节点

[0113] 检查以查看该节点是否具有用作为客户的节点X标记的至少一个配方

[0114] 如果否，那么从“潜在供应商节点”列表中移除该节点

[0115] //“潜在供应商节点”是节点X的供应链中的下一层节点。

[0116] 该算法在列表中的每个节点上递归执行，以产生节点的下一级供应商。对于每个新的递归，作为当前迭代主体的节点成为新的“X”。

[0117] 所确定的传递闭包的结果可以被存储为(例如，与示例模式类似的数据表中的)网络数据606。参考图6，可以基于由用户执行的对(例如，存储在图5的数据表中的)基础网络数据的一个或多个改变来生成增量602，使得存储网络数据606的受对基础网络数据的改变影响的每个数据表被更新。换句话说，在对一条信息A的网络数据改变的情况下，可以生成增量602，以更新存储信息A或者存储依赖于信息A的信息的网络数据606的任何数据表。

[0118] 在一些实施例中，维护图4中的网络图400的传递闭包包括修改网络数据(例如，网络数据606)的预计算版本，而不是重新计算整个传递闭包。如果请求完全重建(例如，基于数据库故障或某些其它需求)，那么可以基于连接、配方和成分记录来执行传递闭包的重建。

[0119] 在一些实施例中，对图4中的网络图400的传递闭包的确定为每个节点402提供了直接访问向量。例如，网络图400的传递闭包可以提供可从给定节点到达的所有节点的列表：

[0120] 给定节点“X”，“X”的闭包是对象列表，其中每个对象由以下表示：

[0121] 1)可以从“X”到达的节点(“Y”)的ID

[0122] 2)一组替代路径，其描述在图中从“X”到达“Y”的所有可能方式。每个替代路径可以包括将从“X”遍历以到达“Y”的节点ID的列表。

[0123] 可以在关系数据查询中选择给定节点的直接访问向量，以返回作为具有给定节点的路径的一部分的节点子集。换句话说，遍历图4中的网络图400并返回针对给定节点的路径的请求可以使用给定节点的直接访问向量和关系查询来高效地从关系数据表(例如，网络数据606的数据模式)中检索所请求的网络数据。实施例提供了用于遍历网络图400的计算上高效的技术，以便提供网络软件服务，诸如路径识别和对应的数据检索。

[0124] 在一些实施例中，诸如无状态微服务之类的软件服务可被利用来访问、更新、改变、删除或检索节点网络的数据。对网络数据进行更新或改变的增量处理允许高效地访问该数据，但是，一些组织可能将敏感或机密信息存储在系统中。因此，可以提供网络数据的安全策略和安全过滤，以进一步改善网络数据的管理。

[0125] 图7图示了根据示例实施例的用于节点网络的数据处理的安全管理的功能图解。例如，图解700可以表示用于实现本文公开的节点网络的安全数据处理的软件功能。

[0126] 图解700包括服务702、数据平台704、安全平台706和数据存储装置708。数据平台704可以包括应用编程接口(“API”)710、XML定义712以及逻辑到物理映射714。安全平台可以包括数据校订716、关系过滤718、受信(trusted)存储库720和XML配置722。在一些实施例中,服务702、数据平台704、安全平台706和数据存储装置708可以类似于图3的服务310、数据平台312、安全平台314和数据存储装置316。

[0127] 在一些实施例中,服务702可以包括提供给用户以与节点网络进行交互的多个微服务。例如,隶属于注册组织(例如,网络的实体)的(操作客户端设备的)用户可以使用多个公开的API来调用各种微服务,以与网络系统对接并访问网络数据。

[0128] 在一些实施例中,服务702使用API 710与数据平台704进行通信,以便访问、更新、改变或删除存储在数据存储装置708处的网络数据。XML定义可以定义可从数据存储装置708检索的数据。此外,逻辑到物理的映射714可以用于将逻辑数据请求或命令映射到物理级别的请求或命令(例如,关系数据查询)。

[0129] 在一些实施例中,在对数据存储装置708执行物理级别的请求或命令之前,将这些请求或命令(例如,结构化查询语言(“SQL”)命令或查询)传送到安全平台706以根据所存储的安全协议进行过滤或加强(augmenting)。受信存储库720是存储注册用户和组织的访问许可的网络的安全策略的不可变来源。

[0130] 例如,可以根据存储在受信存储库720处的访问许可来保护对数据存储装置708的访问。在一些实施例中,受信存储库720可以存储用于写入第一组织简档数据的组织键。在这个示例中,第一组织的用户将能够把简档数据写入到他们自己的组织,但是被阻止将简档数据写入到任何其它组织,即使这样的写入是由一个或多个服务702或由网络系统的其它代码所请求的。

[0131] 在一些实施例中,可以根据受信存储库720处存储的安全策略,通过关系过滤718对从数据平台704传输的查询或命令(例如,SQL)进行过滤或加强。此外,可以根据存储在受信存储库720处的安全策略,由数据校订716校订由过滤或加强的查询检索到的任何数据。在一些实施例中,可以使用XML配置722来配置安全平台706,XML配置722包括定义安全协议(例如,访问许可、查询过滤和数据校订)的多个XML文件。

[0132] 实施例包括可用于与网络系统对接的多个无状态微服务。在一个实施例中,微服务是可独立部署的服务。在一个实施例中,术语“微服务”构想了软件体系架构设计模式,其中复杂的应用由使用语言无关的API彼此通信的小型独立进程组成。在一个实施例中,微服务是小型的、高度解耦的服务,并且每个微服务都可以专注于完成小的任务。在一个实施例中,微服务体系架构风格是将单个应用开发为一组小型服务的方法,每个小型服务在其自己的进程中运行并与轻量级机制(例如,HTTP资源API)进行通信。在一个实施例中,微服务相对于执行全部或许多相同功能的单件式服务更容易替换。此外,可以在不对其它微服务产生不利影响的情况下更新每个微服务。作为对照,对单件式服务的一部分的更新可能非期望地或无意地负面影响单件式服务的其它部分。在一个实施例中,可以围绕微服务的能力来有益地组织微服务。在一个实施例中,微服务集合中的每个微服务的启动时间比共同执行这些微服务的所有服务的单个应用的启动时间少得多。

[0133] 在一个实施例中,微服务体系架构是指用于构建灵活的、可独立部署的软件系统的面向服务的体系架构(“SOA”)的专用化(即,系统内的任务的分离)和实现方法。微服务体

系架构中的服务是为了实现目标而通过网络相互通信的进程。在一个实施例中,这些服务使用与技术无关的协议。在一个实施例中,服务具有较小的粒度并使用轻量级协议。在一个实施例中,服务是可独立部署的。通过将系统的功能分布到不同的小型服务中,可以增强系统的凝聚力,并减少系统的耦合。这样可以更容易地随时更改系统并向系统添加功能和质量。它还允许通过连续重构(refactoring)来形成个体服务的体系架构,并且因此减少了对大型前期设计的需求,并允许提前和连续地发布软件。

[0134] 在一个实施例中,在微服务体系架构中,将应用开发为服务的集合,并且每个服务运行相应的进程并使用轻量级协议进行通信(例如,每个微服务的唯一API)。在微服务体系架构中,可以根据要提供的服务以不同的粒度级别将软件分解成个体服务/功能。服务可以是运行时部件/进程。每个微服务可以是可以与其它模块/微服务对话的自包含模块。每个微服务都可以具有未命名的通用端口,其它端口可以与之联系。在一个实施例中,微服务的未命名通用端口是微服务按照惯例公开的标准通信信道(例如,作为常规的超文本传输协议(“HTTP”)端口),并且允许相同服务内的任何其它模块/微服务与其对话。在一个实施例中,微服务彼此独立、是原子的并且无状态。微服务或任何其它自包含功能模块通常可以被称为“服务”。

[0135] 例如,无状态微服务之一可以是用于认证用户的身份的身份管理服务,诸如IDCS微服务。例如,与组织相关联的用户可以提供其组织凭证,并且IDCS微服务可以被配置为使用用户的组织的身份管理系统执行认证,以确保相关系统正确认证用户的身份。以下示例表示IDCS微服务的API的子集:

[0136] User(用户)GetCurrentUser

[0137] 获取通过当前登录的用户识别的当前用户。

[0138] User GetUser(String(字符串)emailAddress)

[0139] 获取通过电子邮件地址识别的用户。它针对用户名属性查询IDCS。

[0140] String CreateUser(User toCreate)

[0141] 创建新用户并将其添加到组中。组显示名称可在应用的上下文参数中配置(web.xml)。在创建用户之前,可以搜索添加用户的IDCS组。搜索可以调用API并搜索显示名称与配置的参数相匹配的组。一旦找到,它就可以提取组ID(在UI中不可见),并使用该组ID向IDCS服务器创建更新(PATCH)请求,以添加新创建的用户。在操作成功之后,返回新创建的用户ID

[0142] (GUID)。

[0143] 在一些实施例中,各种微服务可以彼此依赖于API来执行功能。例如,IDCS微服务可以依赖于由一个或多个其它微服务提供的功能,以便完成上述针对示例API的功能。此外,IDCS微服务可以从组织的身份管理系统请求功能,以便完全实现用户认证。例如,组织可以实现基于云的用户认证系统,诸如美国专利号9,838,376中描述的系统。

[0144] 在另一个示例中,一个或多个微服务可以用于从数据存储装置708创建、读取、更新或删除(“CRUD”)网络数据。例如,各种微服务可以公开自定义或CRUD接口,该自定义或CRUD接口提供对微服务表示的“业务功能”的访问。在一些示例中,微服务可以表示业务实体(例如,公司简档、邀请列表、配方等)。CRUD动词可以允许读取或操纵对应的实体流。如将在下面进一步详述的,这样的服务还可以依赖安全平台706的功能来确保符合系统的安全

策略。以下示例表示一个或多个CRUD微服务的API的子集：

[0145] Void Create(T items)

[0146] Void Create(IDDRS<T>items)

[0147] IDDRS<T>Read(Map<String,Object>parameters,FilterClause filterClause, SortClause sortClause)

[0148] IDDRS<T>Read(Class<T>returnDataRecordClass,Map<String,Object> parameters,FilterClause filterClause,SortClause sortClause)

[0149] PagedData<?>ReadPage(Map<String,Object>params,,FilterClause filterClause,SortClause sortClauseOverride,int firstRecord,int PageSize)

[0150] IDDRS<T>ReadMetaData()

[0151] Void Update(IDDRS<T>updates)

[0152] Void Delete(IDDRS<T>deletes)

[0153] Void UpdateCreate<IIDRS<T>updateCreates)

[0154] CRUD Base

[0155] GRUD Base(CRUD基)

[0156] -由希望在基础数据储存库上使用标准CRUD的服务实现所使用的ICRUD接口的实现。

[0157] -基于的CRUD将预期数据储存库id来指引CRUD操作。

[0158] Generic CRUD(通用CRUD)

[0159] -ICRUD接口的通用数据实现,用于对数据储存库没有类型的(un-typed)CRUD动作。该服务将预期数据储存库id来指示CRUD操作。

[0160] CRUD factory(CRUD工厂)

[0161] -构造ICRUD接口的通用数据实现的工厂

[0162] 在另一个示例中,组织微服务可以用于管理向节点网络注册的组织的信息。例如,如先前所公开的,每个组织可以具有带有多个属性的简档。组织微服务可以调用CRUD微服务的一个或多个函数来访问、创建或更新存储在数据存储装置708中的组织信息。例如,组织微服务可以提供以下函数：

[0163] Create(创建)

[0164] -基于CRUD微服务的标准创建

[0165] -依靠数据源中的数据约束来强制执行必填(mandatory)字段

[0166] Read(读取)

[0167] -基于CRUD微服务的标准读取

[0168] Update(更新)

[0169] -基于CRUD微服务的标准更新

[0170] -依靠数据源中的数据约束来强制执行必填字段

[0171] Update Create(更新创建)

[0172] -基于CRUD微服务的标准更新创建

[0173] -依靠数据源中的数据约束来强制执行必填字段

[0174] 用户还可以使用组织微服务来查找特定于组织的信息和检索组织的产品。以下示

例表示组织微服务的API的子集：

[0175] Public IDynamicDataRecordSet<Organisation>find(long orgId)

[0176] Public IDynamicDataRecordSet<Product>getProducts(Organisation org)

[0177] 在一些实施例中,IDynamicDataRecordSet(IDRS)是允许表示可变数据流的通用数据结构。IDRS可以包括若干个部分：

[0178] 1)数据流表示的记录列表,例如每个实体一条记录。

[0179] 2)每条实体记录可以具有一组属性对:属性ID和属性值。

[0180] 3)每条实体记录可以自包含实体记录列表。包括此类特征的示例可以允许分层级表示。

[0181] 4)与上述数据平行,IDRS可以包含元数据。元数据可以针对实体记录中可用的每个属性具有一个条目。该元数据描述了数据的特性。示例如下：

[0182] a.数据库中的物理数据类型,例如文本

[0183] b.业务类型-例如密码

[0184] c.可能值的范围

[0185] d.必填标志

[0186] e.验证规则

[0187] f.默认值

[0188] g.等等。

[0189] 利用IDRS的实施例可以利用数据结构的益处,至少是因为该结构可以以标准方式表示值、记录、列表、层次结构和其它概念。这些表示可以例如由于所包含的元数据而是自描述的。网络数据的实施例可以表示为IDRS结构。这样的实施例允许通用处理单元或UI部件接受不寻常数据阵列,至少是因为IDRS结构提供了关于如何导航和理解它的指示。

[0190] 在另一个示例中,用户简档微服务可以用于为节点网络的用户管理用户简档。例如,每个用户可以具有包括特定于用户的信息的简档,诸如组织从属关系。用户简档微服务可以调用CRUD微服务的一个或多个函数来访问、创建或更新存储在数据存储装置708中的用户简档信息。例如,以下表示用户简档微服务可以提供的函数的子集：

[0191] Create(创建)

[0192] -基于CRUD微服务的标准创建

[0193] Read(读取)

[0194] -基于CRUD微服务的标准读取

[0195] Update(更新)

[0196] -基于CRUD微服务的标准更新

[0197] Update Create(更新创建)

[0198] -基于CRUD微服务的标准更新创建

[0199] 在另一个示例中,成分微服务可以用于与存储在数据存储装置708中的成分信息对接。成分微服务的功能的子集如下：

[0200] 定义：

[0201] 元数据定义

[0202] • 成分

[0203] 如由RdbmsStandardAttributes提供

[0204] •Ingredients_CRUD(成分_CRUD)

[0205] 如由RdbmsStandardAttributes提供

[0206] 动态数据定义

[0207] •成分

[0208] 读取标题(Caption)、ParentProductId和OwnerOrgId

[0209] •Ingredients_CRUD

[0210] 如由RdbmsStandardAttributes提供

[0211] 功能:

[0212] 标准CRUD操作的实现如下:

[0213] 读取(Read)

[0214] 使用成分数据流作为CrudBase的一部分实现。

[0215] 删除(Delete)

[0216] 使用Ingredients_CRUD数据流覆盖。

[0217] CreateItemsEx(Long ownerOrgId,Long parentProductId,IDynamicDataRecordSet items)抛出ORSCN_ServiceException

[0218] 迭代通过项目列表并设置OwnerOrgId和parentProductId

[0219] 使用Ingredient_CRUD数据流调用储存库创建。

[0220] UpdateCreateEx(Long ownerOrgId,Long parentProductId,IDynamicDataRecord item)throws ORSCN_ServiceException

[0221] 设置OwnerOrgId和parentProductId

[0222] 使用Ingredient_CRUD数据流调用储存库updateCreate。

[0223] ReadIngredient(Long ingredientId)抛出ORSCN_ServiceException

[0224] •在成分实体上调用静态readIngredient

[0225] o如果IngredientId为null(空),那么返回null

[0226] o使用在IngredientsId上进行过滤的Ingredients_CRUD数据流来调用储存库读取。

[0227] o如果返回了成分,那么通过使用IngredientSuppliersCaptions数据流对储存库调用读取来扩展供应商信息,并替换supplierIds属性。

[0228] 更新(Update)

[0229] 未实现,抛出异常。

[0230] 创建(Create)

[0231] 未实现,抛出异常。

[0232] 创建/更新(Create/Update)

[0233] 未实现,抛出异常。

[0234] 在另一个示例中,可以使用类似的配方微服务与存储在数据存储装置708中的配方信息对接。配方微服务的功能的子集如下:

[0235] 定义:

[0236] 元数据定义

[0237] • 配方

[0238] 如由RdbmsStandardAttributes提供

[0239] • Recipes_CRUD(配方_CRUD)

[0240] 如由RdbmsStandardAttributes提供

[0241] 动态数据定义

[0242] • 配方

[0243] 读取标题(Caption)、ParentProductId和OwnerOrgId

[0244] • Recipes_CRUD

[0245] 如由RdbmsStandardAttributes提供

[0246] 功能:

[0247] 标准CRUD操作的实现如下:

[0248] 读取(Read)

[0249] 使用配方数据流作为CrudBase的一部分实现。

[0250] 删除(Delete)

[0251] 使用Recipes_CRUD数据流覆盖。

[0252] CreateItemsEx(Long ownerOrgId,Long parentProductId,IDynamicDataRecordSet items)抛出ORSCN_ServiceException

[0253] 迭代通过项目列表并设置OwnerOrgId和parentProductId

[0254] 使用Recipes_CRUD数据流调用储存库创建。

[0255] UpdateCreateEx(Long ownerOrgId,Long parentProductId,IDynamicDataRecord item)抛出ORSCN_ServiceException

[0256] 设置OwnerOrgId和parentProductId

[0257] 使用Recipes_CRUD数据流调用储存库updateCreate。

[0258] ReadRecipe(Long recipeId)抛出ORSCN_ServiceException

[0259] • 在配方实体上调用静态readRecipe

[0260] o如果recipeId为null(空),那么返回null

[0261] o使用在recipeId上进行过滤的Recipes_CRUD数据流调用储存库读取。

[0262] o如果返回了配方,那么通过使用RecipeConsumersCaptions数据流对储存库调用读取来扩展消费者信息,并替换consumerIds属性。

[0263] o如果返回了配方,那么使用RecipeIngredientsCaptions数据流对储存库调用读取来扩展成分信息,并替换ingredientIds属性。

[0264] 更新(Update)

[0265] 未实现,抛出异常。

[0266] 创建(Create)

[0267] 未实现,抛出异常。

[0268] 创建/更新(Create/Update)

[0269] 未实现,抛出异常。

[0270] 如前所述,示例微服务在实施例中可以是无状态的,因此极大简化了它们彼此之间的交互。在一些实施例中,提供会话状态微服务以允许访问保持在应用会话上的分布式

对象模型(“DOM”)对象。在示例中,用于会话状态微服务的简化API是以下接口:sessionDOMGetSessionDOM(),该接口可以返回提供会话DOM的对象。

[0271] 在实施例中,DOM对象可以是数据结构,该数据结构搜集各种数据集,该数据集表示登录到网络中的用户会话的状态。数据可以是按需累积的频繁访问数据(例如,安全规则),或者是与登录用户相关的离散项集合(例如,当前用户、语言选择、用户来源、当前网络可视化报告等)。根据微服务体系架构,实施例包括读取和更新DOM中的数据的单个服务。当从DOM请求数据时,网络应用逻辑可以使用该服务。在一些实施例中,可以将DOM中的数据物理地锚定到(例如,由应用服务器维护的)会话状态。

[0272] 如本文所述,针对网络的滴馈增量处理维护对于给定组织/实体/节点的网络配置(例如,给定节点的直接访问向量),该网络配置可以容易地用于查询数据存储装置708以遍历表示节点网络的图(例如,识别包括给定节点的现有或潜在路径/供应链)。可以提供用于遍历网络以返回组织(例如,网络中的实体或节点)的路径的示例网络遍历微服务。示例网络遍历微服务的功能的子集如下:

[0273] 数据布局(Data Layout)

[0274] 简单的4列的表(Simple 4column table)(connectionId,to,from,type),其中每个连接一行。不存储反向连接。

[0275] 给定节点X和Y,其中类型c=消费(consumes)并且s=供应(supplies)

[0276] X c Y(X消费Y)

[0277] 和

[0278] Y s X(Y供应X)

[0279] 是等效的。

[0280] 对象(Objects)

[0281] 网络(Network)

[0282] IDDRS<Organisations>Organisations

[0283] List<Connection>connections

[0284] Connections(连接)

[0285] Long formNodeId

[0286] Long toNodeId

[0287] Enum connectionType

[0288] API

[0289] public Network readNetwork(Int startOrganisationId,int depth)

[0290] 在一些实施例中,网络遍历微服务可以返回用于请求用户的组织的网络路径(例如,供应链)。例如,除了连接这些组织(例如,贸易伙伴、供应商、客户等)的关系的性质之外,返回的数据还可以表示诸如组织对(例如,通过ID识别)之类的路径。在一些实施例中,该服务可以用于显示和搜索组织的供应链。

[0291] 表示供应链的组织(由该服务返回)可以通过它们之间的连接以及交易的商品或产品来定义。在一些实施例中,为了递送连接节点的列表,微服务利用关于接受的连接和交易的产品的信息,虽然在一些实施方式中,该信息被使用但未被返回。例如,在一些实施方式中,返回了表示供应链的组织的结果集,但是没有返回用于确定结果集的注释的附加信

息。

[0292] 如参考图8-图14进一步详述的,可视化可以显示给网络系统的用户,在一些情况下,可视化可以包括使用网络系统的安全策略保护的数据可视化,诸如对表示供应链的节点/实体的路径的可视化。可以提供用于创建、编辑或更新网络系统的可视化的示例可视化微服务。可视化微服务的功能的子集如下:

[0293] 功能:

[0294] • 创建(Create)

[0295] o确保提供了所有必需的属性

[0296] o创建新的可视化。

[0297] • 读取(Read)

[0298] o读取当前组织的当前可视化。以这种方式检索可视化将返回除实际数据之外创建可视化所需的一切。这可以用于检索和编辑可视化规范,而无需读取所有网络数据。

[0299] • 读取可视化数据

[0300] o该操作将读取可视化,包括UI显示所需的实际网络数据。

[0301] • 更新(Update)

[0302] o利用提供的数据更新可视化

[0303] • 删除(Delete)

[0304] 从DOM中移除虚拟化

[0305] 可视化可以如下定义:

[0306]

属性	注释
Id	生成的整数，必填 ID
类型	饼图、条形图、网络图、世界地图或表之一。 必填
标题	可视化的友好名称。 用于显示。 必填
过滤器	过滤器，描述要在可视化中使用的数据中包括或排除的内容。这是通过 UI 创建的。
选项	包含特定于可视化的类型的选项的数据记录，当前只有饼图/条形图将其用于“数据属性”以便正确显示。
数据	显示可视化所需的数据。

[0307]

	这在需要时通过读取可视化数据操作进行查找。

[0308] 创建(Creation)

[0309] 创建可视化需要提供必填属性,否则将抛出异常。一旦可视化被创建,就可以对其进行编辑。在显示可视化数据之前,经由连接服务对其进行查找。此时,考虑选项和过滤器。

[0310] 编辑(Editing)

[0311] 除ID之外,任何属性都可以被编辑。改变可视化属性可能需要重新读取数据,以使改变生效。(例如,选项或过滤器改变)。

[0312] 返回参考图7,服务702、数据平台704、安全平台706和数据存储装置708可以被配置为允许网络中的实体/节点/组织之间的信息共享。即使在这些数据中的一些数据机密或敏感的情况下,网络系统也基于流畅的数据共享而不是私有数据的孤岛。因此,可以根据基于请求访问数据的节点/实体/组织与拥有被请求的数据记录的节点/实体/组织之间的关系的共享规则,在节点/实体/组织之间共享网络数据。

[0313] 以下为对于给定节点/实体/组织共享规则的示例:给定实体拥有的数据记录(例如,表的一行)允许访问其中给定实体存在现有商品或产品流的任何实体(例如,实体是贸易伙伴或在供应链路径上),并且不允许访问没有此类现有商品或产品流的实体。换句话说,给定实体可以允许贸易伙伴访问非贸易伙伴无法访问的某些数据。可以为同一记录(例如,行)内的不同组的字段数据(例如,列)定义不同的网络共享规则。在一些实施例中,可以为网络系统的每个不同功能区域的各个用户定义共享规则。

[0314] 如本文详述的,节点网络的实体可以是组织,并且数据存储装置708可以存储组织的简档信息。例如,可以为注册的组织存储简档,该简档可以包括以下中的一个或多个:名称、地址或位置(例如,纬度、经度、归属国和任何其它合适的位置信息)、与组织相关联的品牌、主页统一资源定位符(“URL”)、组织的社交媒体账户、这些的组合以及其它合适的信息。

[0315] 在实施例中,节点网络可以表示供应商、客户和/或中间商的网络。在这样的示例中,组织简档还可以包括以下中的一个或多个:出售的产品、购买的产品、来自第三方协会的证书、来自第三方协会的过期证书、直接供应商(例如,来自网络中的其它实体当中的供应商)、直接客户(例如,来自网络中的其它实体当中的客户)、商品或产品的计划(例如,配方)、商品或产品的部分(例如,成分)、这些的组合、以及针对产品或商品的买方或卖方的任何其它合适的信息。

[0316] 在包括网络节点的社交方面(例如,帖子、消息等)的实施例中,系统可以管理实体的社交数据,诸如消息、帖子、讨论组以及其它社交交互的数据。另外,实体还包括与它们在网络中的定向相关的网络数据,诸如实体/节点之间的连接、具有实体/节点的路径(例如,直接访问向量)、以及与网络中的实体/节点的定向相关的其它合适的信息。

[0317] 在一些实施例中,实体可以为该实体拥有的各个数据片段(例如,与组织简档、社交网络数据、网络定向数据等相关的不同数据项)定义特定的共享规则。例如,组织的简档的一部分可以具有公共共享规则(例如,任何人都可用),而证书或过期的证书可以具有直接贸易关系共享规则(例如,仅对贸易伙伴可用)。示例共享规则为:

[0318] 公开—数据对互联网上的任何人都可用。

[0319] 网络—数据对任何注册用户/组织可用。具有用户账户的任何人都可以登录到系统。

[0320] 直接贸易连接—数据对与源组织具有直接贸易关系的组织内的用户可用。他们向

源组织直接供应、消耗、或者既供应又消耗。

[0321] 客户连接—数据对作为源组织的客户的组织内的用户可用。

[0322] 供应商连接—数据对作为源组织的供应商的组织内的用户可用。潜在连接—基于组织拥有的成分和配方之间的匹配,数据对与源组织具有潜在连接(例如,潜在的商品或产品流)的组织内的用户可用(如本文所述)。

[0323] 特定组织—数据对来自特定组织列表内的任何人可用。可以从网络上的所有组织中选择该组织。

[0324] 私有—数据仅对拥有数据的组织内的用户可用。

[0325] 在一些实施例中,安全平台706基于针对每个源实体的这些共享规则(例如,存储为访问许可)以及源实体与请求源实体的数据的用户之间的关系来做出访问许可决定。实体/组织之间的关系可以存储为网络数据。在一些示例中,可以通过发送和接受邀请以指示贸易关系来定义该关系。例如,客户“X”可以请求组织“Y”作为供应商与他们连接。如果该邀请被接受,那么供应商“Y”将能看到拥有者“X”已标记为“仅供应商可见”的数据。

[0326] 在一些实施例中,在解析数据共享规则并确定用户是否被许可检索源实体所拥有的数据后,关系过滤718对代表经认证的用户(经由服务702和数据平台704)提交的带有从数据存储装置708中检索数据的“键”的数据查询(例如,SQL查询)进行加强。然后可以在数据存储装置708处执行加强的查询以检索所请求的数据。在一些实施例中,在数据存储装置708确定用户不被许可访问所请求的数据的情况下,将不将用于该数据的相关“键”添加到查询,因此当在数据存储装置708处执行查询时将不返回该数据。

[0327] 在一些实施例中,安全平台706访问“当前登录的组织ID”。可以基于与经认证的用户相关联的组织,通过登录处理将“当前登录的组织ID”不可变地存储在受信存储库720中。数据存储装置708内包含敏感信息(例如,由上述安全策略/共享规则之一保护的信息)的表可以使它们的记录通过被认为“拥有”该记录的实体/组织的组织ID作为键。如上所述,每个实体/组织可以基于特定的共享规则/访问许可(例如,客户、供应商等)以特定的方式授予对各个组织或与它们相关的“组织类别”的访问权限。

[0328] 在一些实施例中,在数据存储装置708中存储网络数据的表具有相关联的“安全描述符”或规则的XML表示,其示出了请求访问数据的组织必须如何与数据行的拥有者相关(如果该行要被访问)。例如,XML可以为相关联的数据表的记录定义共享规则/访问许可。安全平台706使用XML关系规则和“当前登录的组织ID”来确定可以访问其数据的其它可能组织的集合。

[0329] 在一些实施例中,关系过滤718修改SQL访问语句,使得附加的WHERE子句(clause)修饰符被添加到已经在SQL中(例如,由数据平台704)指定的任何过滤。这个附加的限制器可以列出有效组织ID的集合(例如,根据当前登录的组织ID和XML安全描述符),其中一个必须存在于数据行的组织键中才能使记录匹配并包含在查询的范围内。

[0330] 在一些实施例中,在接收到SQL结果之后但是在其被返回给调用应用之前,可以通过数据校订716来执行数据缩减。例如,WHERE键修改处理将限制SQL访问的行,但是这些行的各个字段将在不考虑安全协议的情况下被读取。在一些情况下,数据拥有者可能已允许访问记录,但不允许访问记录中的所有字段。数据校订716可以用于处理这种场景并校订列级数据。

[0331] 在一些实施例中,返回的每条记录由数据校订716进行后处理(post-process),以移除未被数据拥有者授权作为可由当前组织访问的任何字段数据。在一些实施例中,仅在键过滤和校订之后才返回行集(例如,返回的数据集)。

[0332] 作为示例,发出请求的组织/应用/微服务可以尝试使用不受限制的“*”SQL where子句来读取表。然后,安全平台706可以使用“当前登录的组织ID”从受信存储库720中识别请求者。然后,安全平台706可以计算已授予对该组织的访问权限的其它组织的集合。关系过滤718可以向SQL添加附加的WHERE修饰符,以过滤掉未授予该访问权限的组织所拥有的数据。因此,由于添加的WHERE修饰符,因此从这种不受限制的SQL语句中进行检索将返回安全得多的记录集。

[0333] 在一些实施例中,数据校订716然后可以分析检索到的数据以移除记录的拥有组织不允许请求者查看的任何字段。例如,对于每条记录,可以访问安全协议(例如,访问许可/数据共享规则/安全描述符文件)以确定发出请求的组织相对于记录的拥有者的列级别访问。当确定发出请求的组织没有对数据的列级别访问权限时,可以从结果集中移除该数据。然后,可以将经关系过滤和校订的数据返回给发出请求的组织。在一些实施例中,这可能是空的记录集。

[0334] 以下表示示例XML,该示例XML定义了安全平台706用于执行上述安全功能的访问许可:

[0335] <?xml version="1.0"?>

[0336] <!--组织有权访问其创建的任何请求(CREATED_ORG_ID)或针对该组织的而非针对用户的任何请求(TARGET_ORG_ID)。用户有权访问对于其作为成员的任何组织的任何请求(@SecureAvailableOrganisations)或针对该用户的任何请求。不能删除记录。仅能更新状态ID、更新的日期和时间、更新的组织ID和更新的用户ID-->

[0337] <SecurityDefinition id="Rdbms_INVITE_STREAM"><DataSources><Rdbms

[0338] id="InviteStreamDataSource"allowedOperations="Create,Read"

[0339] source="INVITE_STREAM"><Fields><Field

[0340] writeValue="@'SecureSelectedOrganisationId'"

[0341] sourceName="CREATED_ORG_ID"logicalName="CreatedOrgId"/><Field

[0342] sourceName="TARGET_ORG_ID"logicalName="TargetOrgId"/><Field

[0343] sourceName="TARGET_USER_ID"logicalName="TargetUsrId"/><Field

[0344] allowedOperations="Create,Read,Update"writeValue="@CurrentDateTime"

[0345] sourceName="UPDATED DATETIME"

[0346] logicalName="UpdDateTime"/><Field

[0347] allowedOperations="Create,Read,Update"

[0348] writeValue="@'SecureSelectedOrganisationId'"

[0349] sourceName="UPDATED_ORG_ID"logicalName="UpdatedOrgId"/><Field

[0350] allowedOperations="Create,Read,Update"sourceName="STATUS_ID"

[0351] logicalName="StatusId"/><Field allowedOperations="Create,Read,Update"

[0352] sourceName="CODE"logicalName="Code"/></Fields></Rdbms>

[0353] </DataSources><Transforms><Filterid="FilteredRequestStreamTransform"

[0354] input="InviteStreamDataSource"><Clauses><Or><LeftClause><Clause

[0355] rightValue="@'SecureAvailableOrganisationIds'"relation="="

[0356] leftValue="CreatedOrgId"/></LeftClause><RightClause><Or><LeftClause><And><LeftClause><Clause rightValue="@'SecureAvailableOrganisationIds'"relation="="leftValue="TargetOrgId"/></LeftClause><RightClause><ClauserightValue="NULL"relation="="

[0357] leftValue="TargetUsrId"/></RightClause></And></LeftClause><RightClause><Clause rightValue="@'SecureUserId'"relation="="

[0358] leftValue="TargetUsrId"/></RightClause></Or></RightClause></Or></Clauses></Filter></Transforms></SecurityDefinition>

[0359] <?xml version="1.0"?>

[0360] <SecurityConfiguration><Entity defaultSourcePrefix="ORG"

[0361] knownEntity="Organisation"><Attributes><Attribute

[0362] logicalName="ProductsPurchased"><Storage><Rdbms

[0363] source="ORG_PRODUCTS_PURCHASED/ORG_ID"/><Rdbms

[0364] source="ORG_PRODUCTS_PURCHASED/PRODUCT_ID"/></Storage></Attribute><Attribute logicalName="ProductsSold"><Storage><Rdbms

[0365] source="ORG_PRODUCTS_SOLD/ORG_ID"/><Rdbms

[0366] source="ORG_PRODUCTS_SOLD/PRODUCT_ID"/></Storage></Attribute></Attributes></Entity><AttributeGroup

[0367] name="OrganisationProductsTraded"><Attributes><Attribute

[0368] id="Organisation/ProductsPurchased"/><Attribute

[0369] id="Organisation/ProductsSold"/></Attributes></AttributeGroup><DataEntry caption="_TRANS_View Products Traded"globalDefaultRule="Network"

[0370] attributeGroupName="OrganisationProductsTraded"><Verbs><Verb

[0371] name="Read"/></Verbs></DataEntry></SecurityConfiguration>

[0372] 在一些实施例中,基于用户的功能安全规则控制源组织内“谁”可以做“什么”。它们还可以控制谁具有基础源组织数据的哪些访问权限。安全模板用于定义这些模板在创建时用户具有的功能安全性。管理员(具有足够特权的用户)可以通过功能安全性设置控制其组织内的给定用户是否被授予权限或被撤消权限。可用的安全模板及其相关联的特权在下面的表1和表2中示出。例如,可以考虑三个模板:管理员-能够完全管理组织的用户,包括管理用户、连接和属于其组织的所有数据;用户编辑者-可以通过发布社交帖子、管理公司简档等做出贡献的用户,但是不能进行与安全相关的操作,诸如管理用户、连接等;用户读者-只能查看和分析信息的用户。他们不能进行任何改变。

[0373] 一般而言,这种用户是只读用户。

[0374]

功能	通过安全模板访问		
	管理员	编辑者	读者
组织简档			
更新公共信息	✓	✓	✗
更新贸易产品	✓	✓	✗
更新认证和证书	✓	✓	✗
更新位置	✓	✓	✗
更新联系人	✓	✓	✗
更新偏好	✓	✗	✗
更新 PIN	✓	✗	✗
帖子			
管理讨论组订阅	✓	✓	✗
更新帖子	✓	✓	✗
安全性			
管理数据可见性安全性	✓	✗	✗
管理特征和功能安全性	✓	✗	✗
查看审核	✓	✗	✗

[0375] 表1

[0376]

功能	通过安全模板访问		
	管理员	用户编辑者	用户读者
邀请			
管理连接	✓	✗	✗
管理组织链接	✓	✗	✗
管理用户	✓	✗	✗
查看通知	✓	✓	✗
查看连接	✓	✓	✓
查看链接的组织	✓	✓	✓
查看用户	✓	✓	✓
网络			
使用报告和可视化工具	✓	✓	✓
浏览组织	✓	✓	✓
原材料			
更新原材料和产品线	✓	✗	✗
查看原材料和产品线	✓	✓	✓

[0377] 表2

[0378] 在一些实施例中,从社交网络检索到的数据可以用于各种功能目的。例如,可以生成图示组织在路径(例如,供应链)中的定向的一个或多个可视化。图8图示了根据示例实施例的用于配置节点网络的视图的示例图形用户界面。例如,组织内的用户可以操作客户端设备,该客户端设备被配置为显示用于显示供应链可视化的仪表板800。被检索以生成可视化的网络数据可以利用所公开的一个或多个功能。例如,可以基于从存储的网络数据的预计算版本中检索到的给定节点的向量(例如,直接访问向量)来生成可视化。还可以使用关系过滤和数据校订功能来保护检索到的网络数据,该功能管理相对于给定节点的存储安全策略。

[0379] 在一些实施例中,仪表板800可以包括用户界面元素(例如,小部件(widget)),用户界面元素包括过滤器选项802、配置选项804、启用806、深度808、可视化选项810和属性812。例如,过滤器选项802可以用于确定用于由可视化显示的组织数据的过滤器类型。图示的选项包括国家过滤器、组织名称过滤器、购买的产品过滤器、出售的产品过滤器、过期证书过滤器、原材料过滤器(例如,成分)和产品线过滤器。

[0380] 图8图示了其中“过期证书”是所选择的过滤器的示例。配置选项804可以允许配置所选择的过滤器。在图示的实施例中,过滤器被配置为显示供应链中具有大于“0”个过期证书的实体。启用806允许用户启用或禁用过滤器。

[0381] 深度808可以允许用户选择供应链的深度(例如,显示具有小于或等于所选择的深度的距离的节点/实体/组织,其中距离是远离网络中的源节点/实体/组织的跳跃(jump)数或跳(hop)数)。可视化选项810允许用户选择可视化类型,诸如饼图、条形图、网络图、表或世界地图。图9图示了根据示例实施例的网络数据的饼图可视化。图10图示了根据示例实施例的网络数据的表可视化。图11图示了根据示例实施例的网络数据的网络图可视化。图12-图14图示了根据示例实施例的供应链数据的世界视图可视化。

[0382] 数据属性812允许用户选择由一些可视化使用的数据属性。例如,图9的饼图900图示了按国家划分的饼图。如果用户期望对供应链可视化具有更广阔的数据视图,那么图10的数据表1000提供了更大的网络数据横截面。图11的网络图1100描绘了网络节点以及这些网络节点之间的连接的可视化,该可视化显示了供应链中包括的各个链接。

[0383] 图12的世界视图可视化1200描绘了覆盖在世界地图上的供应链连接。在这个示例中,向用户示出了供应链中的各种区域风险。用户可以通过选择(例如,点击或轻击)供应链中的一个点来进一步请求关于供应链中的链接的更粒度的信息。图13的世界视图可视化1300包括在选择供应链中的链接后显示的小部件1302、概要(summary)1304和指示符1306。

[0384] 小部件1302可以用于选择用于显示的组织信息。概要1304提供了所选择的组织的概要,包括许多过期证书(例如,用于生成所描绘的可视化的过滤器)。指示符1306可以指示用于生成可视化的特定过滤器的条件。在图示的实施例中,指示符1306示出红色感叹号,因为所选择的组织具有过期的证书。在一些示例中,如果组织没有过期的证书,那么可以显示绿色的对勾。图4的可视化1400类似地包括小部件1402和概要1404,其显示供应链中不同组织的概要。

[0385] 所公开的各种实施例具有优于常规数据管理和安全应用的许多优点。例如,包括滴馈增量处理和网络数据的预计算版本的实施例可以大大降低与遍历大型节点图相关联的计算复杂度。至少所生成的直接访问向量为查询关系数据库提供了高效的解决方案,以快速且准确地检索网络数据。这样的效率和高可访问性允许来自网络系统的健壮的软件服务产品,诸如本文公开的可视化。常规数据管理系统采用的较为繁琐、效率较低和计算上具有挑战性的方法无法实现这些益处。

[0386] 例如,一些数据模式实现被设计为表示和回答连接图网络上的问题。但是,其中许多已针对频繁读取和偶尔更新进行了优化。在各种实施例中,随着新的关系连接和贸易商品或产品在参与组织之间被添加/更新,网络有时可能受到频繁更新。在这样的环境中,所公开的滴馈增量处理提供了技术优势。

[0387] 另一个替代方案可以是关系网络连接表的简单按需递归。利用这种简单系统的常

规方法可以处理频繁的更新,但是遍历由存储的数据表示的图形可能带来计算上的挑战。滴馈增量处理解决方案和网络数据的预计算版本即使在频繁更新的情况下也可以提供高效的遍历,这比那些常规技术产生性能益处。

[0388] 另外,包括受信存储库和数据安全策略的实施例确保节点网络可以在供应链中的不同组织之间或者在一些情况下在可以被添加到供应链的潜在组织之间存储和共享私有、敏感或机密数据。特别地,通过安全子系统对数据请求进行漏斗收缩(funneling)以及由安全子系统和受信存储库实现的关系过滤和数据校订确保了不会向任何用户或组织提供对其不具有查看、更新或删除许可的数据的访问权限。

[0389] 例如,传统的基于角色的安全性机制通常假定使用要授予访问的用户或用户组的固定列表来授予数据访问权限。实施例基于“数据拥有者与数据消费者之间的关系”来提供访问。例如,当为组织的“客户”授予对某个数据片段的访问权限时,属于该“客户”类别的组织可以随着贸易关系的更新而流畅地改变,因此,被授权访问数据片段的组织可以流畅地改变。实施例提供了可以在存在这样的改变的情况下高效地且有效地保护数据检索的许可策略。另外,传统的安全性也常常基于记录键。实施例包括更精细的粒度,其中在记录的每个字段上独立地设置安全性。

[0390] 图15图示了根据示例实施例的用于利用增量处理来管理节点网络的示例方法。在一个实施例中,以下图15和图16的功能由存储在存储器或其它计算机可读或有形介质中的软件实现,并由处理器执行。在其它实施例中,每个功能可以由硬件执行(例如,通过使用专用集成电路(“ASIC”)、可编程门阵列(“PGA”)、现场可编程门阵列(“FPGA”)等)或硬件和软件的任何组合来执行。

[0391] 在1502处,存储具有多个连接节点的网络,这些节点表示网络的实体。例如,连接节点的网络可以被映射到关系数据表上。在实施例中,网络可以是由有向图表示的社交网络。

[0392] 在1504处,可以接收对网络的一个或多个增量,该一个或多个增量指示对多个节点之间的连接的更新。例如,可以从与网络的实体相关联的经认证的用户接收对网络信息的更新,并且可以基于该更新来生成一个或多个增量。在1506处,可以将增量添加到队列。在1508处,可以使用队列中的增量来更新网络的节点之间的连接。例如,队列可以是FIFO队列,并且可以处理队列顶部的增量以更新网络。

[0393] 在1510处,可以在更新节点之间的连接之后处理网络以生成针对给定节点的向量。例如,可以在更新网络之后确定网络的传递闭包,并且该传递闭包可以用于为网络中的每个节点生成直接访问向量。

[0394] 在一些实施例中,滴馈增量处理可以包括将网络数据的预计算版本存储在关系数据表集合中。例如,基于存储在数据表中的预计算的网络数据,这个预计算版本可以提供高效的网络遍历。在一些实施例中,处理网络可以包括更新存储网络数据的预计算版本的一个或多个数据表中的数据。在一些实施例中,网络数据的预计算版本提供了可以通过查询数据表来检索的网络节点的直接访问向量。直接访问向量可以指示包括与给定节点的连接的连接节点以及作为包括给定节点和至少一个连接节点的路径的一部分的间接节点。

[0395] 在1512处,可以基于生成的向量来识别针对给定节点的一条或多条路径。例如,可以使用直接访问向量查询关系数据表,以返回给定节点的路径信息。在实施例中,可以在更

新网络的节点之间的链接时创建包括给定节点的识别出的路径。

[0396] 在实施例中,可以为网络的节点定义一个或多个部分以及包括多个部分的一个或多个计划,并且网络的两个节点之间的连接可以是基于为两个节点中的第一节点定义的计划与为两个节点中的第二节点定义的部分匹配的对应关系的。例如,计划可以是配方,并且部分可以是配方的成分。在实施例中,实体可以包括供应商和客户,并且连接可以表示实体之间的交易。例如,识别出的路径可以表示至少一个商品或产品的供应链。在实施例中,可以使用基于连接节点的计划和部分之间的对应关系的网络连接来确定传递闭包。

[0397] 图16图示了根据示例实施例的用于为节点网络提供安全数据管理的示例方法。在1602处,存储具有多个连接节点的网络,这些节点表示网络的实体。例如,连接节点的网络可以被映射到关系数据表上。在实施例中,网络可以是由有向图表示的社交网络。

[0398] 在1604处,可以从第一节点接收检索关于网络的第二节点的数据的请求。例如,可以从由第一节点表示的实体的授权用户接收请求。在1606处,可以生成查询以检索所请求的数据。

[0399] 在1608处,可以基于存储在受信存储库处的对第一节点的许可来过滤查询。例如,可以利用用于基于存储在受信存储库处的相对于第二节点的对第一节点的许可来检索所请求的数据的键来加强查询。

[0400] 在一些实施例中,存储了许可文件,该许可文件定义了对一个或多个关系数据表的访问,访问许可是基于拥有记录的拥有者节点和拥有者节点与请求访问的节点之间的关系为关系数据表中的每个记录定义的。受信存储库可以不变地存储用于网络节点的多个键。在一些实施例中,基于存储在受信存储库中的对第一节点的许可来过滤查询包括访问许可文件以从受信存储库中检索键列表,其中键列表是针对根据第一节点与节点子集之间的关系而被许可由第一节点访问的节点子集。加强查询可以包括将键列表添加到查询,其中当键列表包括与查询所请求的关系数据表内的受保护的记录对应的键时,检索该受保护的记录。

[0401] 在实施例中,经认证的用户具有查看与第一节点连接的节点的至少一些数据的许可,第一节点与第二节点连接。在实施例中,经认证的用户具有查看包括具有第一节点的路径的节点的至少一些数据的许可,第一节点在具有第二节点的路径上。

[0402] 在1610处,可以基于对第一节点的许可来对经过滤的查询的结果中的字段进行校订。例如,可以访问许可文件来确定第一节点相对于返回的记录的拥有者具有哪些访问许可。在返回查询结果之前,可以删除确定第一节点无权访问的任何列级别数据。在1612处,可以将校订结果提供给第一节点。

[0403] 在实施例中,由节点表示的实体可以是供应商和客户,并且节点之间的路径可以表示一个或多个产品的供应链网络。例如,经认证的用户可以具有访问包括第一节点、包括第一节点的供应商或包括第一节点的客户的供应链网络的许可。

[0404] 实施例管理节点网络的数据处理。示例网络可以包括多个节点,这些节点之间具有多个连接。在一些实施例中,网络可以是具有各种程度的信息共享的社交网络。有时,可以在两个先前未连接的节点之间生成新连接,或者可以断开先前连接的节点之间的连接。可以基于网络的当前配置(例如,节点之间的当前连接)来识别一条或多条路径。例如,路径可以从第一节点开始,并且在终止于第五节点之前经过第二节点、第三节点和第四节点。这

样的识别出的路径可以用于识别模式、趋势或风险、执行预测或用于其它分析目的(即,取决于网络内的节点和特定的实施方式)。

[0405] 但是,这些网络的动态性质带来了风险和计算挑战。例如,社交网络经常在变化,构建新的节点连接并拆除旧的节点连接。因此,节点之间的路径识别在计算上可能很繁琐。如本文进一步详述的,实施例利用滴馈增量处理来管理网络,这在维持节点连接的动态更新功能的同时实现计算效率。

[0406] 在一些实施例中,网络的实体(例如,节点)可以具有与系统交互的授权用户。例如,授权用户可以编辑实体的简档、向网络的其它实体发送消息、更改与其它实体的关系、检索与网络的实体相关的数据、执行网络分析以及其它合适的功能。但是,在一些实施例中,可以与网络相关联地存储(例如,在数据存储库中)一个或多个实体的机密或敏感信息。例如,在社交网络中,系统可以存储第一实体的可以与其它实体的子集共享但不能与其余实体共享的敏感信息。在其它示例中,敏感信息可以被标记为私有,并且因此可以不与社交网络的任何其它实体共享。

[0407] 在一些实施例中,系统可以为网络的实体提供安全的数据检索。例如,安全子系统可以为授权用户维护一个或多个许可,其确定用户可以检索哪些信息。基于安全子系统,可以过滤数据检索请求,以确保授权用户仅被提供根据建立的许可的信息。例如,在对数据存储库执行搜索之前,可以使用关系过滤以根据许可来过滤所生成的查询。在另一个示例中,在将数据提供给授权用户之前,可以根据校订数据的许可对查询所检索的数据执行数据校订。安全子系统、关系过滤和数据校订可以用于确保对网络实体的敏感或机密数据进行安全数据管理。

[0408] 贯穿本说明书描述的本公开的特征、结构或特性可以在一个或多个实施例中以任何合适的方式组合。例如,在整个说明书中,使用“一个实施例”、“一些实施例”、“某个实施例”、“某些实施例”或其它类似语言是指这样的事实,即结合该实施例描述的特定特征、结构或特性可以被包括在本公开的至少一个实施例中。因此,贯穿本说明书的短语“一个实施例”、“一些实施例”、“某个实施例”、“某些实施例”或其它类似语言的出现不一定全都指同一组实施例,并且在一个或多个实施例中,所描述的特征、结构或特性可以以任何合适的方式组合。

[0409] 本领域普通技术人员将容易理解,可以以不同顺序的步骤和/或以与所公开的配置不同的配置中的元件来实践如上所述的实施例。因此,虽然本公开考虑了概述的实施例,但是对于本领域技术人员而言显而易见的是,某些修改、变化和替代构造将是显而易见的,同时仍保持在本公开的精神和范围内。因此,为了确定本公开的范围和界限,应当参考所附权利要求。

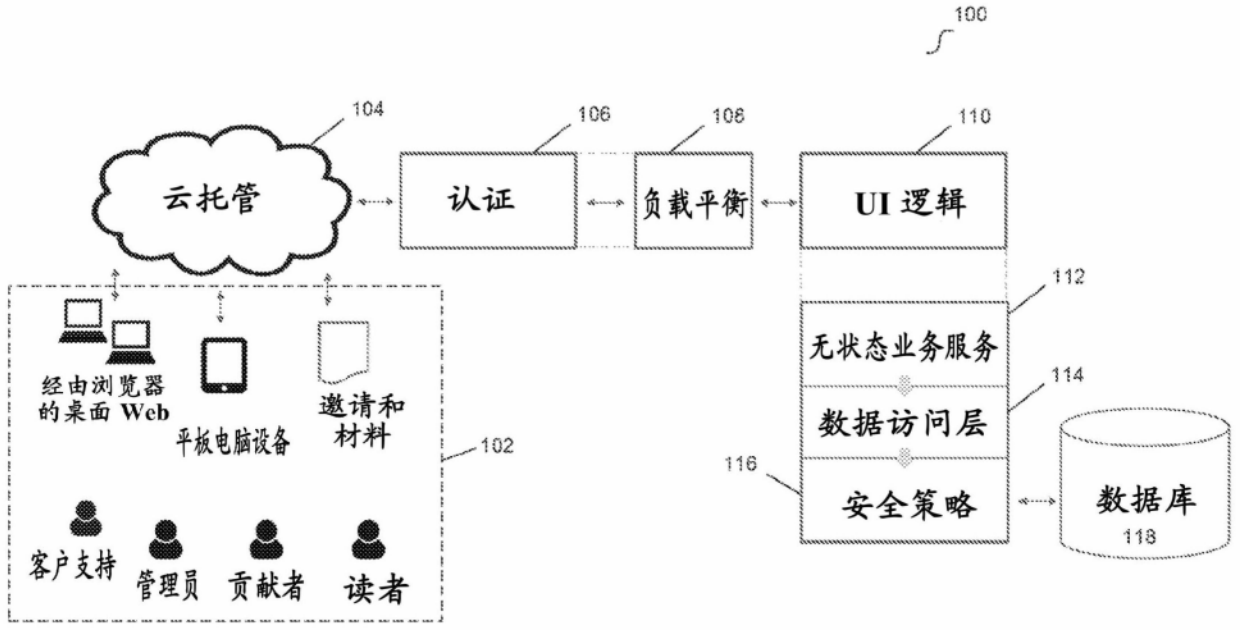

100
104
云托管
106
认证
108
负载平衡
110
UI 逻辑
112
无状态业务服务
114
数据访问层
116
安全策略
数据库
118
102
经由浏览器的桌面 Web
平板电脑设备
邀请和材料
客户支持
管理员
贡献者
读者

图1

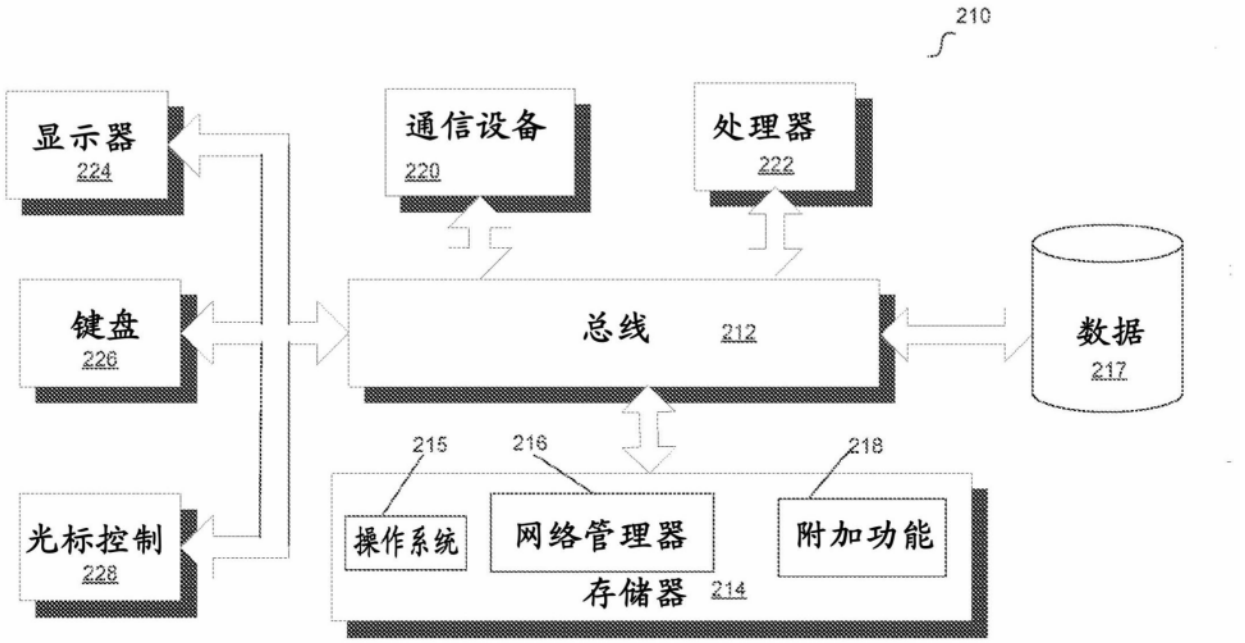

210
显示器
224
通信设备
220
处理器
222
键盘
226
总线
212
数据
217
215
216
218
光标控制
228
操作系统
网络管理器
附加功能
存储器
214

图2

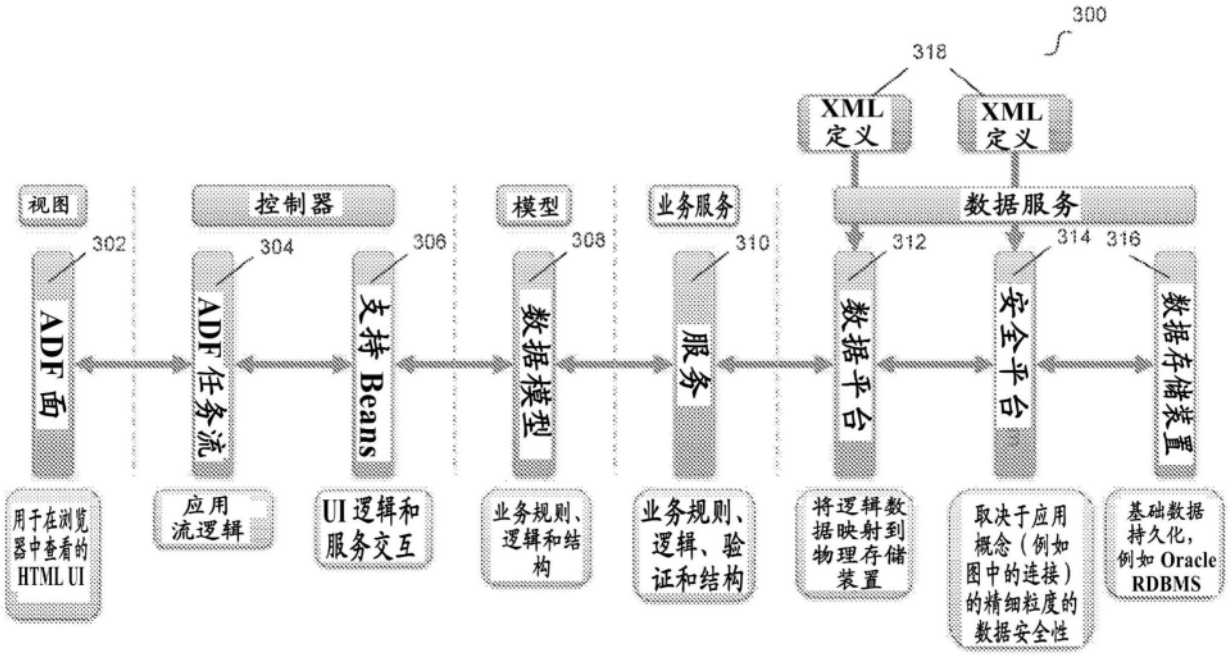

300
318
XML 定义
XML 定义
视图
控制器
模型
业务服务
数据服务
302
304
306
308
310
312
314
316
ADF 面
ADF 任务流
支持 Beans
数据模型
服务
数据平台
安全平台
数据存储装置
用于在浏览器中查看的 HTML UI
应用流逻辑
UI 逻辑和服务交互
业务规则、逻辑和结构
业务规则、逻辑、验证和结构
将逻辑数据映射到物理存储装置
取决于应用概念（例如图中的连接）的精细粒度的数据安全性
基础数据持久化，例如 Oracle RDBMS

图3

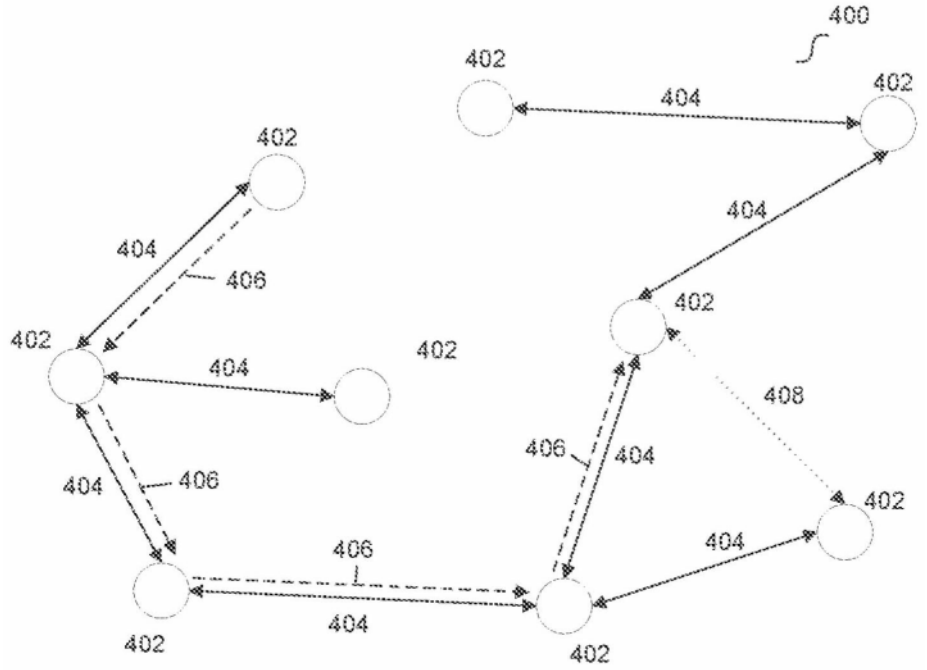

400
402
404
406
408

图4

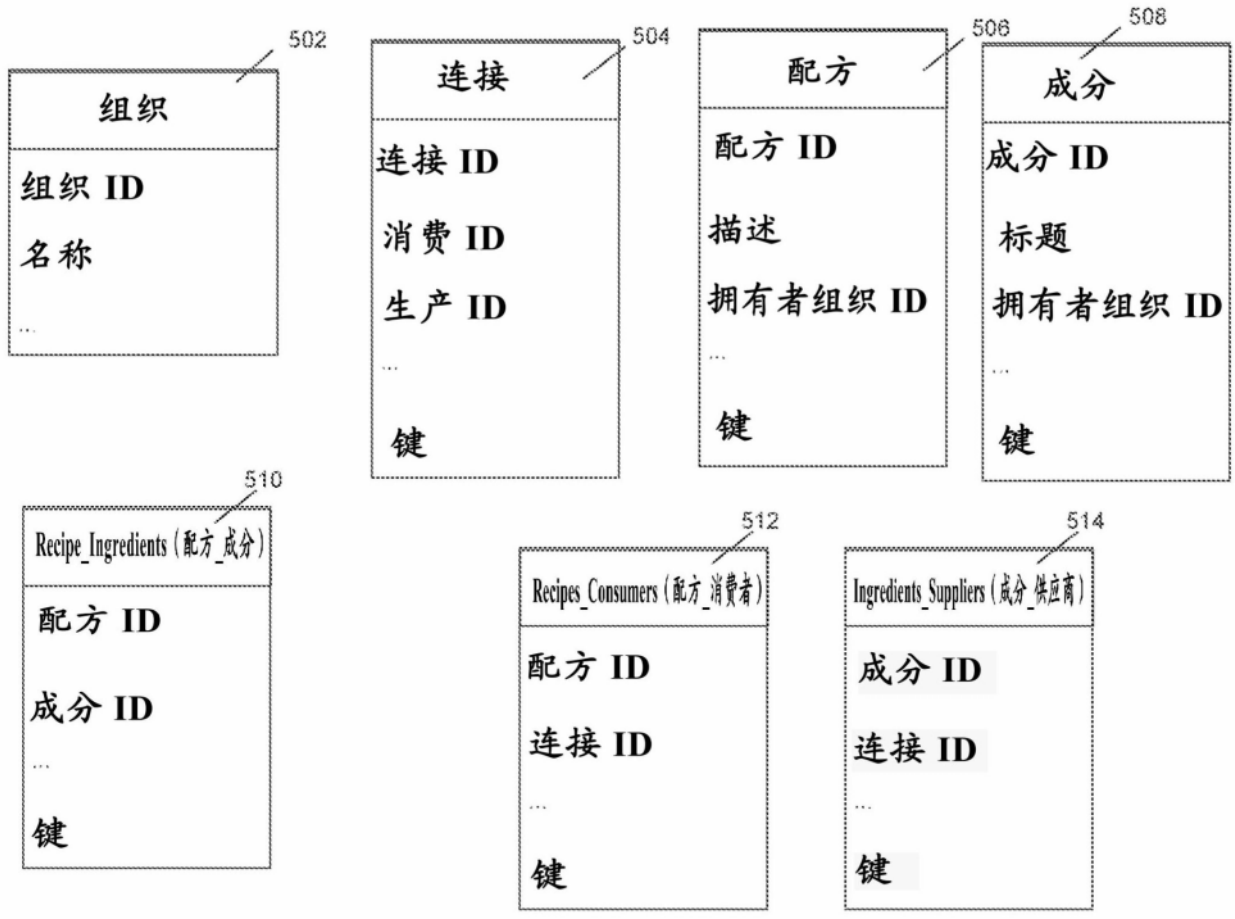

502
组织
组织 ID
名称
...
504
连接
连接 ID
消费 ID
生产 ID
...
键
506
配方
配方 ID
描述
拥有者组织 ID
...
键
508
成分
成分 ID
标题
拥有者组织 ID
...
键
510
Recipe_Ingredients (配方_成分)
配方 ID
成分 ID
...
键
512
Recipes_Consumers (配方_消费者)
配方 ID
连接 ID
...
键
514
Ingredients_Suppliers (成分_供应商)
成分 ID
连接 ID
...
键

图5

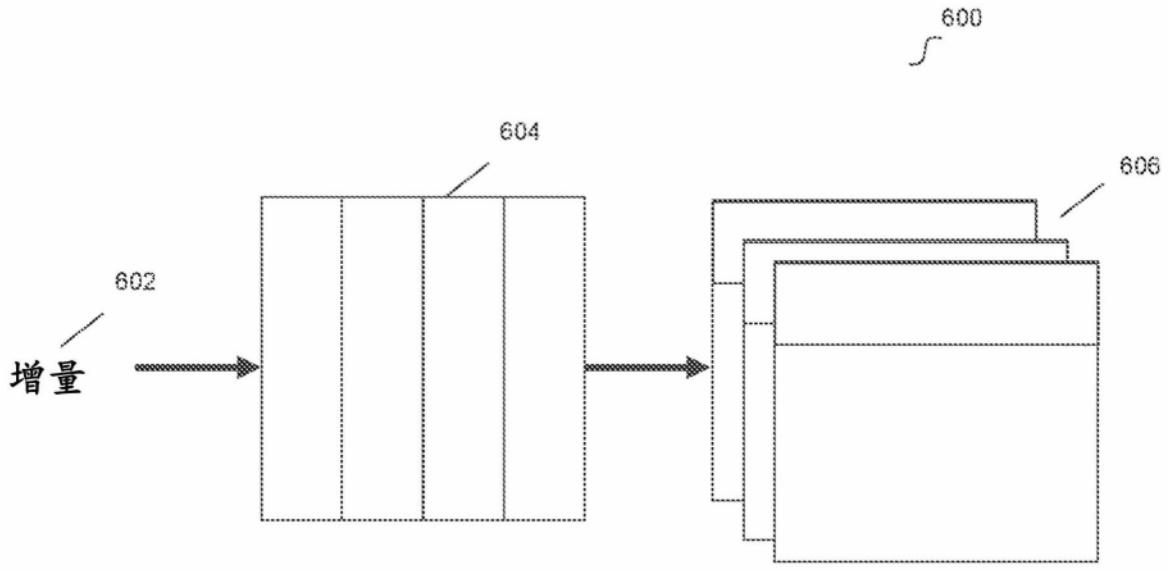

600
604
606
602
增量

图6

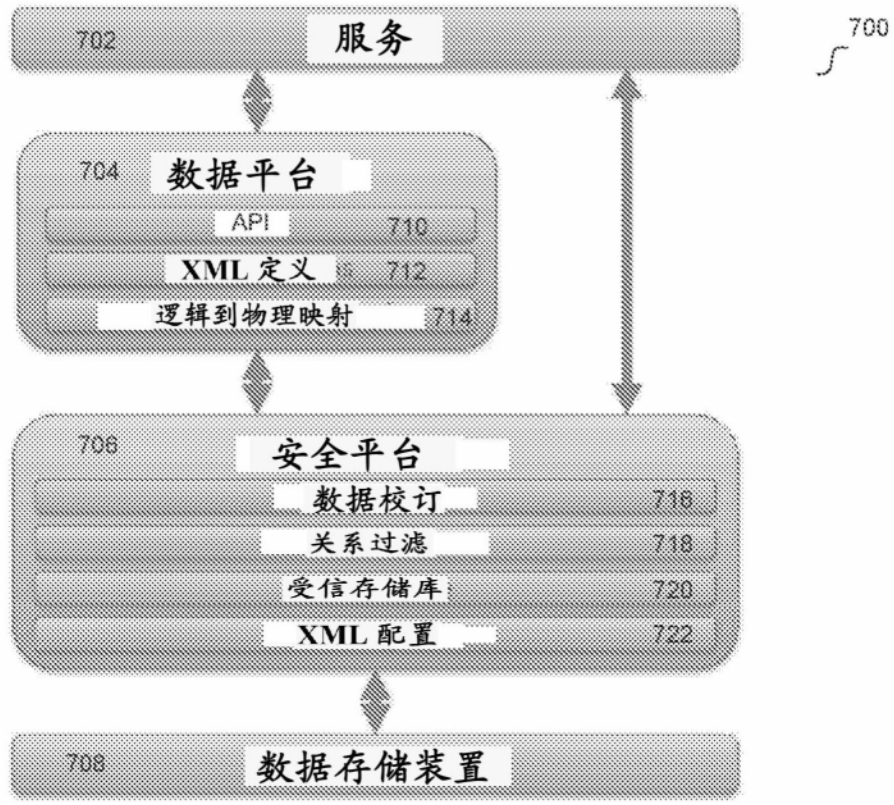

702
服务
700
704
数据平台
API
710
XML 定义
712
逻辑到物理映射
714
706
安全平台
数据校订
716
关系过滤
718
受信存储库
720
XML 配置
722
708
数据存储装置

图7


创建供应链可视化
800
可视化标题
可视化 1
构建供应商过滤器
802
国家
组织名称
购买的产品
出售的产品
过期证书
原材料
产品线
过期证书
大于
804
806
启用过滤器
做出选择以专注于将哪些供应商包括在可视化中
选择要探索的连接深度
级别
808
选择可视化类型以显示您的供应链
810
饼图
条形图
网络图
表
时间地图
数据属性
812
国家
保存改变
取消

图8

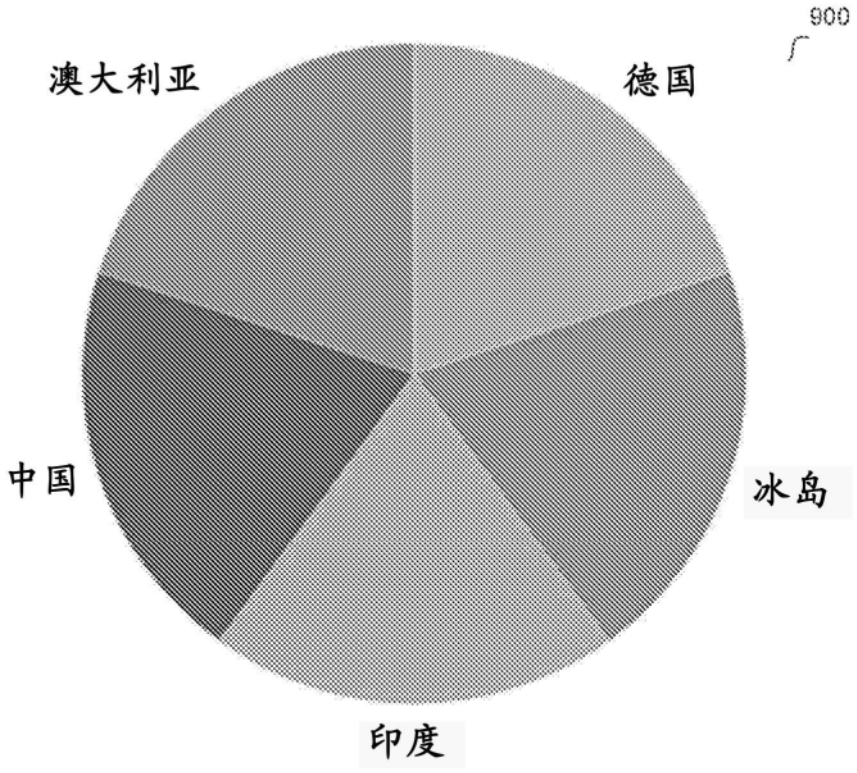


图9

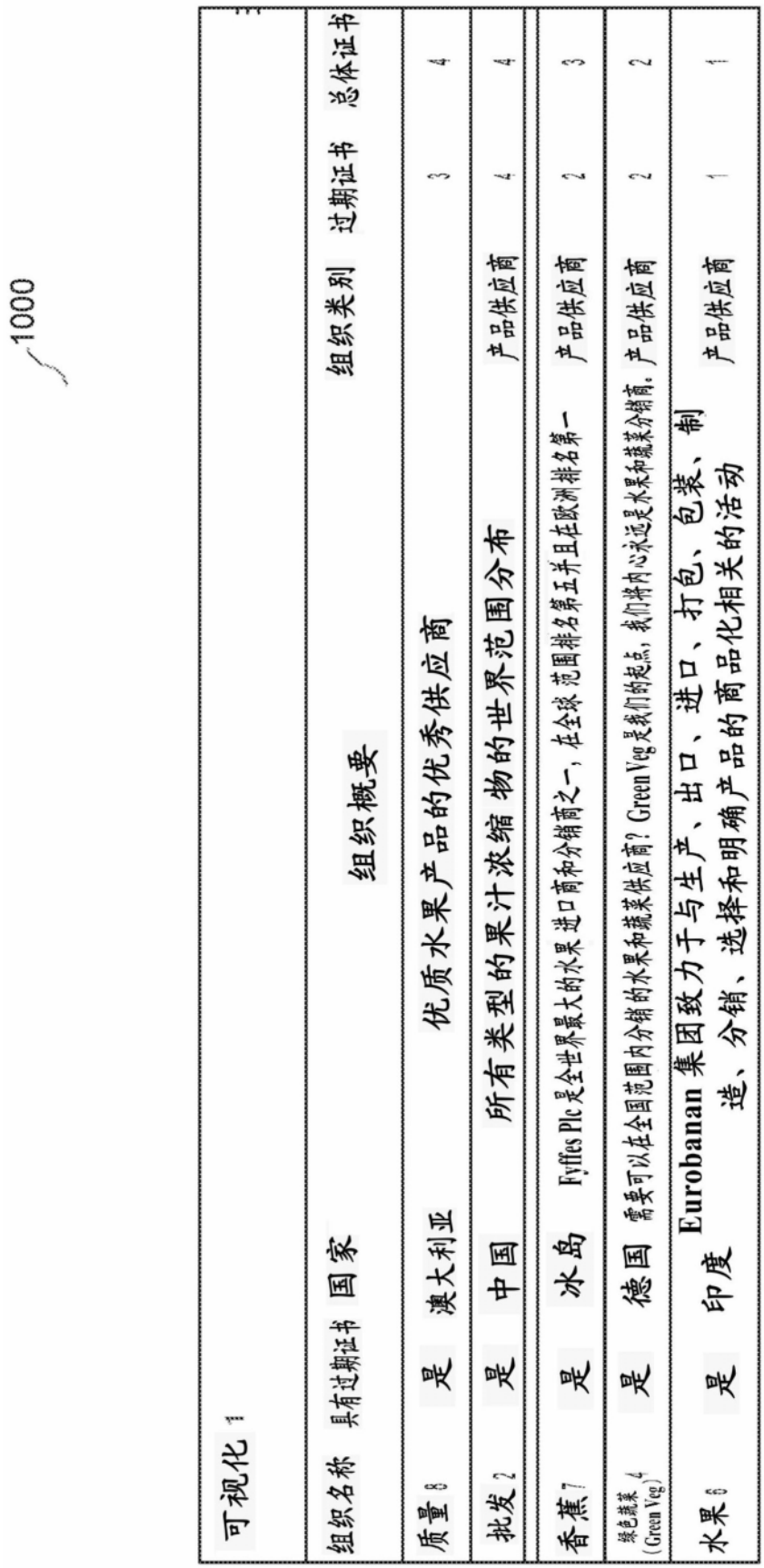

1000
可视化 1
组织名称 具有过期证书 国家 组织概要 组织类别 过期证书 总体证书
质量 8 是 澳大利亚 优质水果产品的优秀供应商 3 4
批发 2 是 中国 所有类型的果汁浓缩 物的世界范围分布 产品供应商 4 4
香蕉 7 是 冰岛 Fyffes Plc是全世界最大的水果进口商和分销商之一，在全球范围排名第五并且在欧洲排名第一 产品供应商 2 3
绿色蔬菜 4 (Green Veg) 是 德国 需要可以在全国范围内分销的水果和蔬菜供应商？Green Veg是我们的起点，我们将内心永远是水果和蔬菜分销商。 产品供应商 2 2
水果 6 是 印度 Eurobanan 集团致力于与生产、出口、进口、打包、包装、制造、分销、选择和明确产品的商品化相关的活动 产品供应商 1 1

图10

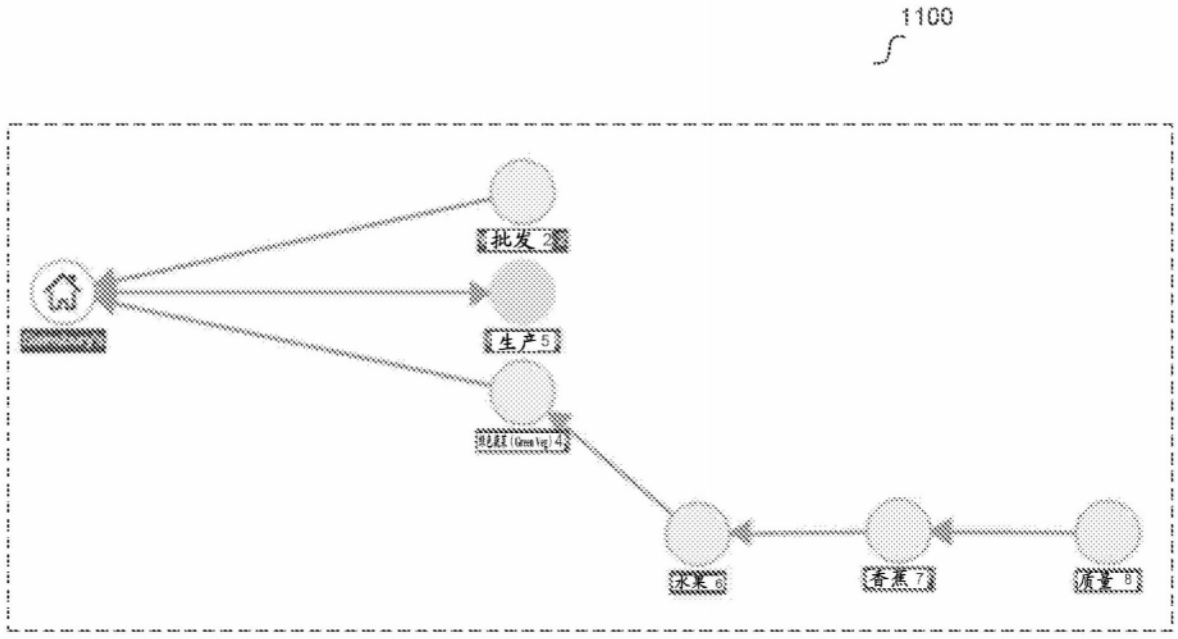


图11

图12

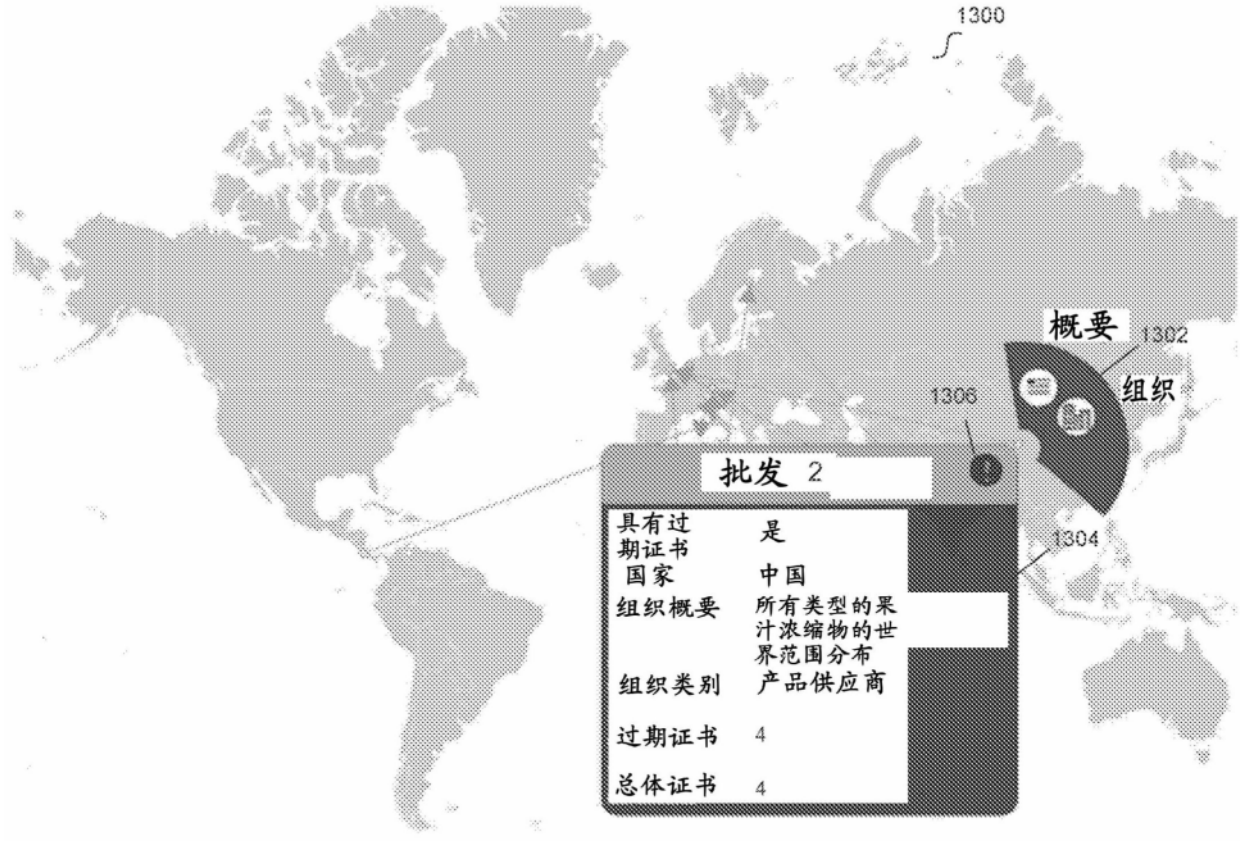

1300
概要
1302
组织
1306
批发 2
具有过期证书 是
国家 中国
组织概要 所有类型的果汁浓缩物的世界范围分布
组织类别 产品供应商
过期证书 4
总体证书 4
1304

图13

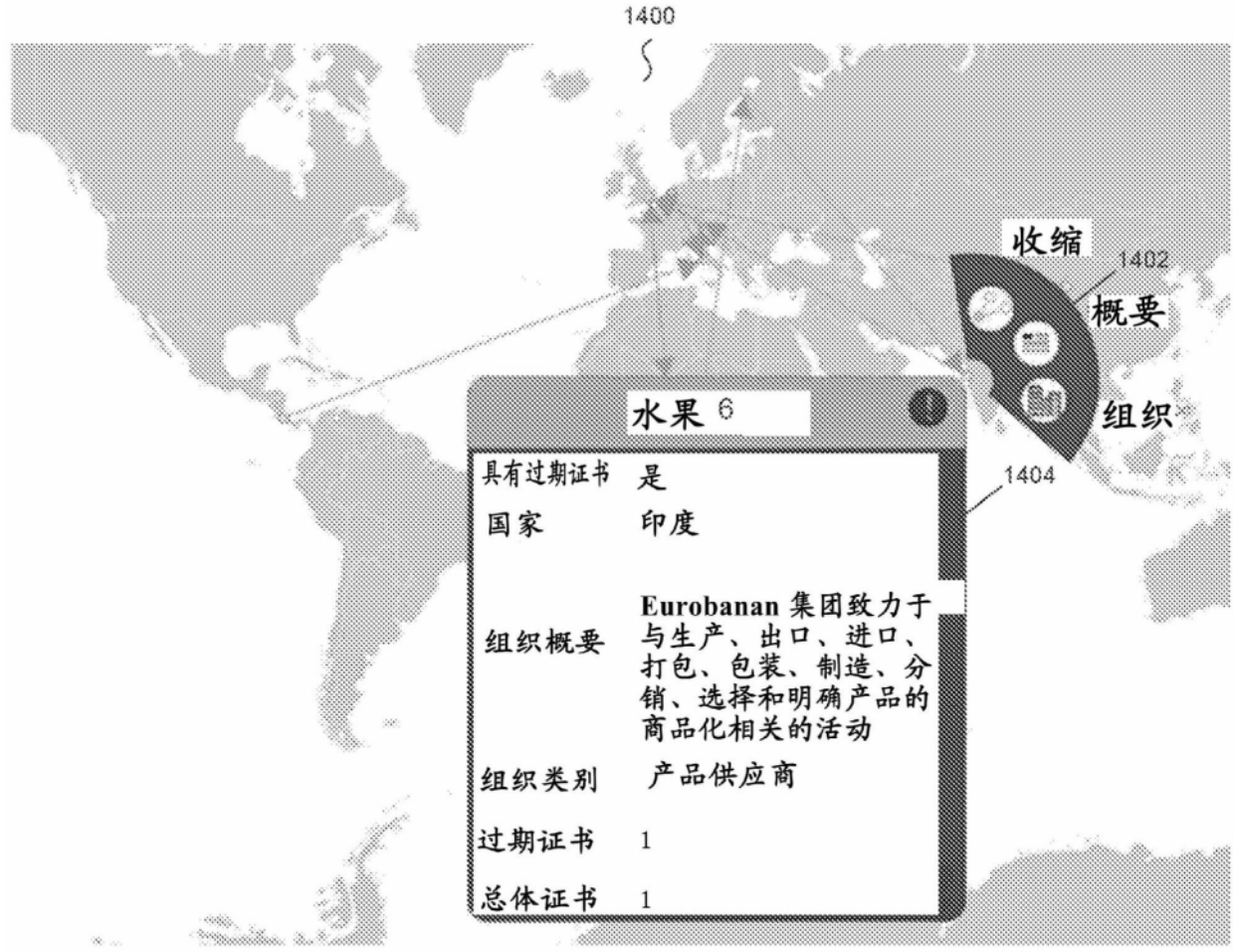

1400
收缩
1402
概要
组织
1404
水果 6
具有过期证书 是
国家 印度
组织概要 Eurobanan 集团致力于与生产、出口、进口、打包、包装、制造、分销、选择和明确产品的商品化相关的活动
组织类别 产品供应商
过期证书 1
总体证书 1

图14

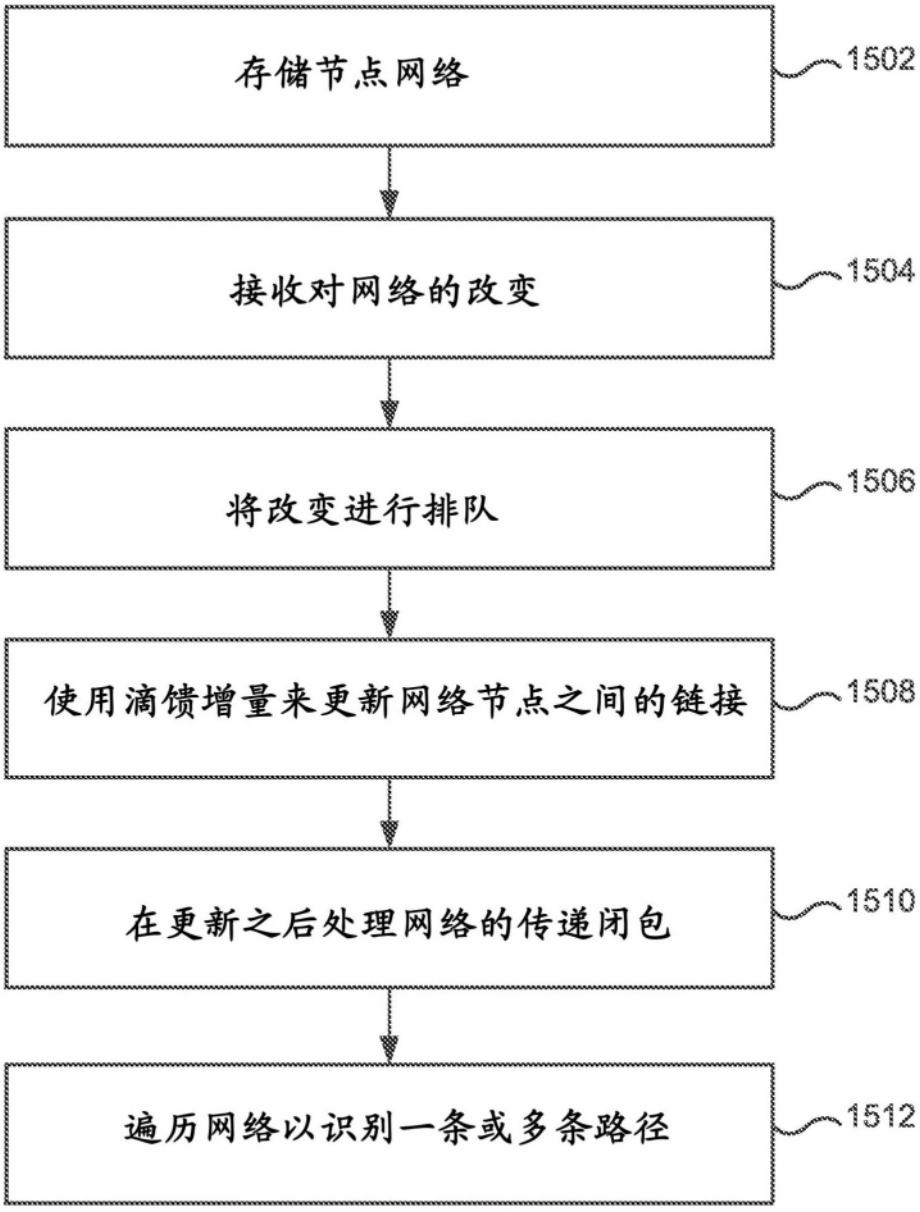

存储节点网络
1502
接收对网络的改变
1504
将改变进行排队
1506
使用滴馈增量来更新网络节点之间的链接
1508
在更新之后处理网络的传递闭包
1510
遍历网络以识别一条或多条路径
1512

图15

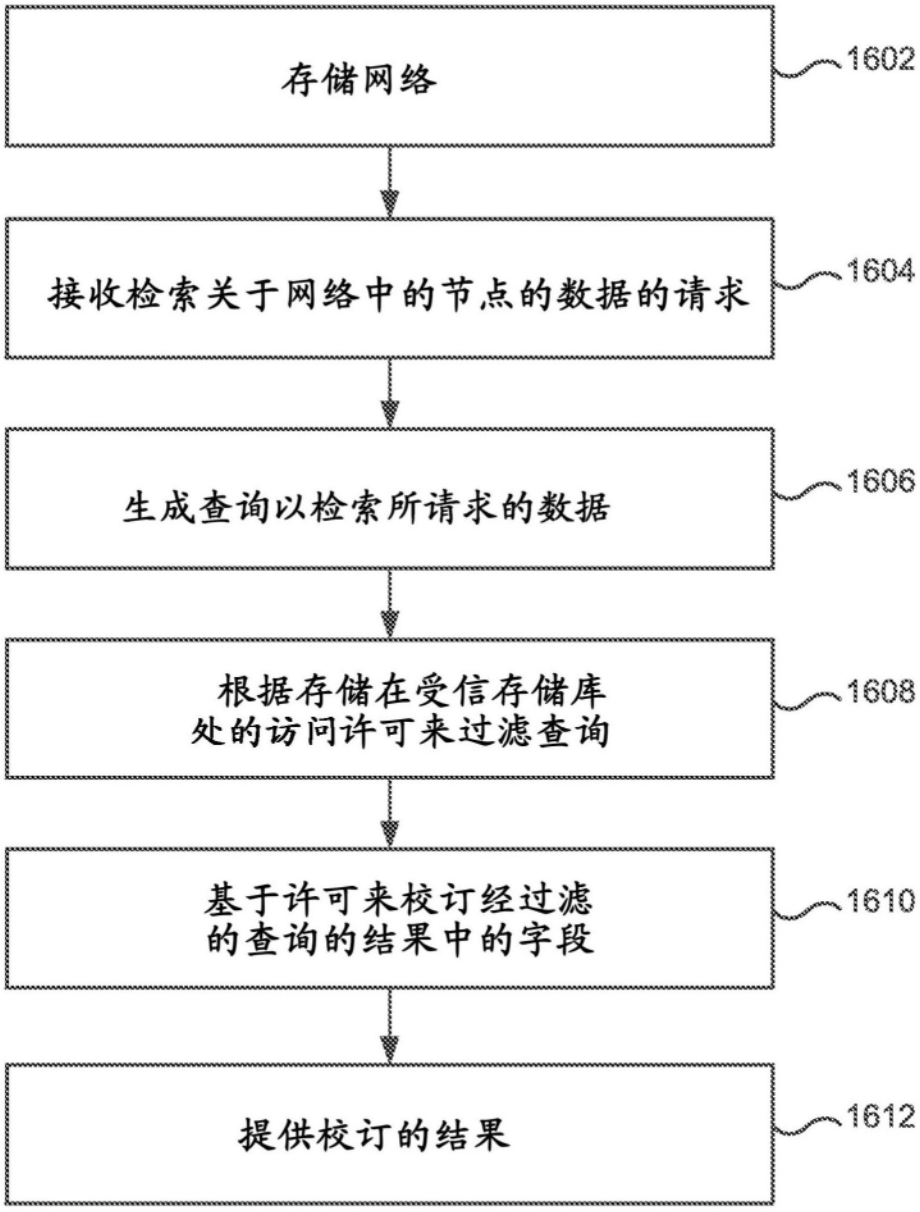

存储网络
1602
接收检索关于网络中的节点的数据的请求
1604
生成查询以检索所请求的数据
1606
根据存储在受信存储库
处的访问许可来过滤查询
1608
基于许可来校订经过滤
的查询的结果中的字段
1610
提供校订的结果
1612

图16