(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106790397 B
(45)授权公告日 2020.06.09

(21)申请号 201611062906.1

(22)申请日 2016.11.28

(65)同一申请的已公布的文献号
申请公布号 CN 106790397 A

(43)申请公布日 2017.05.31

(73)专利权人 新疆熙菱信息技术股份有限公司
地址 830011 新疆维吾尔自治区乌鲁木齐市北京南路358号大成国际大厦10层

(72)发明人 孙赫 王夷 李永平 冯龙龙 刘小瑞 刘磊 张凯

(51)Int.Cl.
H04L 29/08(2006.01)

(56)对比文件
CN 103516565 A,2014.01.15,
CN 101938382 A,2011.01.05,
CN 102984170 A,2013.03.20,
CN 102244664 A,2011.11.16,
CN 103139058 A,2013.06.05,
US 2013191569 A1,2013.07.25,

审查员 王曼

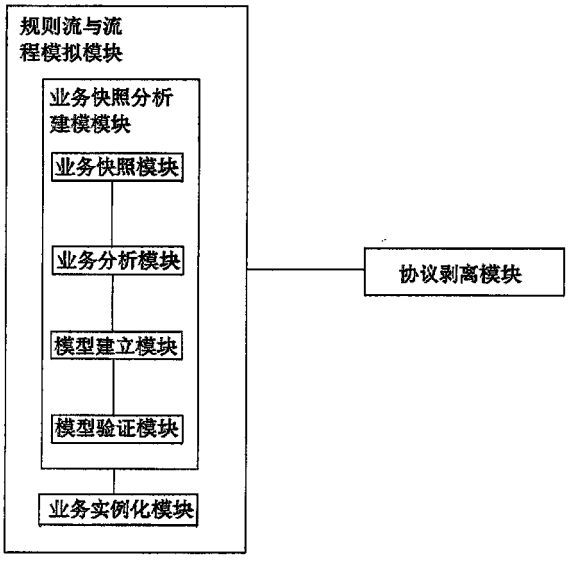
权利要求书2页 说明书4页 附图3页

(54)发明名称

一种数据的业务特征识别系统及方法

(57)摘要

本发明公开了一种数据的业务特征识别系统及方法，系统包括包括协议剥离模块和规则流与流程模拟模块；协议剥离模块用于通过其内部定义的标准审计数据结构来实现对业务数据中网络协议的剥离；规则流与流程模拟模块用于基于剥离了网络协议后的业务数据，通过业务拆分和业务组合将不同业务流程的业务数据拆分为以业务节点为基本单位，然后再由业务节点组成业务簇，业务簇组成业务流。本发明能够实现去网络协议差异化，实现面向全行业的业务审计。



CN 106790397 B

1.一种数据的业务特征识别系统，其特征在于，包括协议剥离模块和规则流与流程模拟模块；

所述协议剥离模块用于通过其内部定义的标准审计数据结构来实现对业务数据中网络协议的剥离；

所述规则流与流程模拟模块用于基于剥离了网络协议后的业务数据，通过业务拆分和业务组合将不同业务流程的业务数据拆分为以业务节点为基本单位，然后再由业务节点组成业务簇，业务簇组成业务流。

2.根据权利要求1所述的数据的业务特征识别系统，其特征在于，所述规则流与流程模拟模块通过其上的业务快照分析建模模块和业务实例化模块来实现对业务的拆分和组合，所述业务快照分析建模模块包括业务快照模块、业务分析模块、模型建立模块和模型验证模块；

所述业务快照模块用于对业务操作动作的开始和结束行为进行抓取，并在抓取过程中对数据报文和屏幕截图进行存储；

所述业务分析模块用于基于业务快照，对业务操作的数据进行识别，分析与业务操作相关的业务数据所在位置和特征，转化为业务规则；

所述模型建立模块用于将业务规则和业务本身的属性进行定义后的集合，按照统一的结构和持久方式输出为模型文件；

所述模型验证模块用于使用本地快照进行模型的验证工作，包括业务属性、数据和相关信息的对比，初步验证模型的正确性，若验证结果为正确，则进行业务的实例化操作，若验证结果为不正确，则重新进行业务的分析、业务模型的建立以及进行模型的验证；

所述业务实例化模块用于将业务模型加载到底层数据引擎，在实际的业务数据报文通过底层引擎的过程中，使用业务模型定位关注的业务操作，通过模型中定义的业务数据和属性定义，从真实业务数据报文中提取需要的数据，最终封装为对象。

3.根据权利要求2所述的数据的业务特征识别系统，其特征在于，所述业务模型包括业务操作名称、用户标识、业务操作数据和流程关联规则。

4.根据权利要求2所述的数据的业务特征识别系统，其特征在于，所述业务实例化对象结构包括业务属性、用户数据、业务数据和审计的结果。

5.一种数据的业务特征识别方法，其特征在于，包括以下步骤：

1)通过定义的标准审计数据结构来实现对业务数据中网络协议的剥离；

2)基于剥离了网络协议后的业务数据，通过业务拆分和业务组合将不同业务流程的业务数据拆分为以业务节点为基本单位，然后再由业务节点组成业务簇，业务簇组成业务流。

6.根据权利要求5所述的数据的业务特征识别方法，其特征在于，步骤2)包括以下步骤：

2.1)业务快照：对业务操作动作的开始和结束行为进行抓取，并在抓取过程中对数据报文和屏幕截图进行存储；

2.2)业务分析：基于业务快照，对业务操作的数据进行识别，分析与业务操作相关的业务数据所在位置和特征，转化为业务规则；

2.3)建立模型：将业务规则和业务本身的属性进行定义后的集合，按照统一的结构和持久方式输出为模型文件；

2.4)模型验证:使用本地快照进行模型的验证工作,包括业务属性、数据和相关信息的对比,初步验证模型的正确性,若验证结果为正确,则进行以下步骤,若验证结果为不正确,则重新进行步骤2.2)-步骤2.4)的操作;

2.5)业务实例化:将业务模型加载到底层数据引擎,在实际的业务数据报文通过底层引擎的过程中,使用业务模型定位关注的业务操作,通过模型中定义的业务数据和属性定义,从真实业务数据报文中提取需要的数据,最终封装为对象。

7.根据权利要求6所述的数据的业务特征识别方法,其特征在于,所述业务模型包括业务操作名称、用户标识、业务操作数据和流程关联规则。

8.根据权利要求6所述的数据的业务特征识别方法,其特征在于,所述业务实例化对象结构包括业务属性、用户数据、业务数据和审计的结果。

一种数据的业务特征识别系统及方法

技术领域

[0001] 本发明涉及信息技术领域，具体来说，涉及一种数据的业务特征识别系统及方法。

背景技术

[0002] 随着互联网和电子信息产业的迅速发展，为了提高生产、经营、管理、销售等能力，越来越企业、组织和个人都将采用信息化系统和工具获取更多信息来对机构进行改造，但随之而来的就是信息安全等问题。目前大多数的安全产品主要面向网络和系统进行安全管理和监控，对于业务信息化系统和工具不能做到有效的监督和管控，在这样的环境下，隐藏着许多信息安全风险。信息安全风险产生的违法案例屡见不鲜，多种多样层出不穷。

[0003] 近年来为了更有效的降低和杜绝安全事件的出现的频率，国家政府和企事业单位对信息安全防范意识越来越重视，也出台了对应的新政策和措施。信息安全产业为了适应政策环境变化和利益，新型的信息安全相关的产品也不断涌现并占领局部市场。但随之而来的问题是，除网络与系统信息安全外，这些产品对于业务信息化系统和工具的监管作用及其有限，分析其问题主要根源在于业务安全产品着眼于企业和组织的业务信息化系统和工具，其类产品的相关技术并不成熟。

发明内容

[0004] 本发明的目的在于提出一种数据的业务特征识别系统及方法，能够实现去网络协议差异化，实现面向全行业的业务审计。

[0005] 为实现上述技术目的，本发明的技术方案是这样实现的：

[0006] 一种数据的业务特征识别系统，包括协议剥离模块和规则流与流程模拟模块；

[0007] 所述协议剥离模块用于通过其内部定义的标准审计数据结构来实现对业务数据中网络协议的剥离；

[0008] 所述规则流与流程模拟模块用于基于剥离了网络协议后的业务数据，通过业务拆分和业务组合将不同业务流程的业务数据拆分为以业务节点为基本单位，然后再由业务节点组成业务簇，业务簇组成业务流。

[0009] 进一步的，所述规则流与流程模拟模块通过其上的业务快照分析建模模块和业务实例化模块来实现对业务的拆分和组合，所述业务快照分析建模模块包括业务快照模块、业务分析模块、模型建立模块和模型验证模块；

[0010] 所述业务快照模块用于对业务操作动作的开始和结束行为进行抓取，并在抓取过程中对数据报文和屏幕截图进行存储；

[0011] 所述业务分析模块用于基于业务快照，对业务操作的数据进行识别，分析与业务操作相关的业务数据所在位置和特征，转化为业务规则；

[0012] 所述模型建立模块用于将业务规则和业务本身的属性进行定义后的集合，按照统一的结构和持久方式输出为模型文件；

[0013] 所述模型验证模块用于使用本地快照进行模型的验证工作，包括业务属性、数据

和相关信息的对比，初步验证模型的正确性，若验证结果为正确，则进行业务的实例化操作，若验证结果为不正确，则重新进行业务的分析、业务模型的建立以及进行模型的验证；

[0014] 所述业务实例化模块用于将业务模型加载到底层数据引擎，在实际的业务数据报文通过底层引擎的过程中，使用业务模型定位关注的业务操作，通过模型中定义的业务数据和属性定义，从真实业务数据报文中提取需要的数据，最终封装为对象。

[0015] 进一步的，所述业务模型包括业务操作名称、用户标识、业务操作数据和流程关联规则。

[0016] 进一步的，所述业务实例化对象结构包括业务属性、用户数据、业务数据和审计的结果。

[0017] 一种数据的业务特征识别方法，包括以下步骤：

[0018] 1)基于剥离了网络协议后的业务数据，通过定义的标准审计数据结构来实现对业务数据中网络协议的剥离；

[0019] 2)通过业务拆分和业务组合将不同业务流程的业务数据拆分为以业务节点为基本单位，然后再由业务节点组成业务簇，业务簇组成业务流。

[0020] 进一步的，步骤2)包括以下步骤：

[0021] 2.1)业务快照：对业务操作动作的开始和结束行为进行抓取，并在抓取过程中对数据报文和屏幕截图进行存储；

[0022] 2.2)业务分析：基于业务快照，对业务操作的数据进行识别，分析与业务操作相关的业务数据所在位置和特征，转化为业务规则；

[0023] 2.3)建立模型：将业务规则和业务本身的属性进行定义后的集合，按照统一的结构和持久方式输出为模型文件；

[0024] 2.4)模型验证：使用本地快照进行模型的验证工作，包括业务属性、数据和相关信息的对比，初步验证模型的正确性，若验证结果为正确，则进行以下步骤，若验证结果为不正确，则重新进行步骤2.2)-步骤2.4)的操作；

[0025] 2.5)业务实例化：将业务模型加载到底层数据引擎，在实际的业务数据报文通过底层引擎的过程中，使用业务模型定位关注的业务操作，通过模型中定义的业务数据和属性定义，从真实业务数据报文中提取需要的数据，最终封装为对象。

[0026] 进一步的，所述业务模型包括业务操作名称、用户标识、业务操作数据和流程关联规则。

[0027] 进一步的，所述业务实例化对象结构包括业务属性、用户数据、业务数据和审计的结果。

[0028] 本发明的有益效果：

[0029] 1、实现面向全行业的业务审计，不论行业类别和行业特点，数据的业务特征识别技术均能有效进行审计；

[0030] 2、实现了去网络协议差异化，不同的网络协议，虽然其数据格式千差万别，但数据的业务特征识别技术可以做到兼容任何一种网络协议；

[0031] 3、解决了产业一体化业务关联、数据关联造成的审计困难的问题，通过数据的业务特征识别技术中的业务实例化对象，将业务内容和数据关联到业务实例化对象中，实现对高度融合的产业一体化信息系统的安全审计。

附图说明

[0032] 图1是根据本发明实施例所述的系统的结构示意图；

[0033] 图2是根据本发明实施例所述的方法的流程图；

[0034] 图3是根据本发明实施例所述的协议剥离流程示意图；

[0035] 图4是根据本发明实施例所述的业务流程示意图；

[0036] 图5是根据本发明实施例所述的业务模型建立流程示意图；

[0037] 图6是根据本发明实施例所述的业务模型的结构示意图。

具体实施方式

[0038] 下面结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员所获得的所有其他实施例，都属于本发明保护的范围。

[0039] 如图1所示，根据本发明的实施例所述的一种数据的业务特征识别系统，包括协议剥离模块和规则流与流程模拟模块；

[0040] 如图3所示，所述协议剥离模块用于通过其内部定义的标准审计数据结构来实现对业务数据中网络协议的剥离，后续产品业务不再关注网络协议本身，全部基于业务数据标准来进行，可以有效解耦产品业务与网络协议。

[0041] 如图4所示，所述规则流与流程模拟模块用于基于剥离了网络协议后的业务数据，通过业务拆分和业务组合将不同业务流程的业务数据拆分为以业务节点为基本单位，然后再由业务节点组成业务簇，业务簇组成业务流。通过这样的拆分和组合形成安全产品能够审计的业务流程，从而实现对不同业务系统的审计。

[0042] 在上述实施例中，进一步的，如图1所示，所述规则流与流程模拟模块通过其上的业务快照分析建模模块和业务实例化模块来实现对业务的拆分和组合，所述业务快照分析建模模块包括业务快照模块、业务分析模块、模型建立模块和模型验证模块；

[0043] 所述业务快照模块用于对业务操作动作的开始和结束行为进行抓取，并在抓取过程中对数据报文和屏幕截图进行存储；

[0044] 所述业务分析模块用于基于业务快照，对业务操作的数据进行识别，分析与业务操作相关的业务数据所在位置和特征，转化为业务规则；

[0045] 所述模型建立模块用于将业务规则和业务本身的属性进行定义后的集合，按照统一的结构和持久方式输出为模型文件；

[0046] 所述模型验证模块用于使用本地快照进行模型的验证工作，包括业务属性、数据和相关信息的对比，初步验证模型的正确性，若验证结果为正确，则进行业务的实例化操作，若验证结果为不正确，则重新进行业务的分析、业务模型的建立以及进行模型的验证；

[0047] 所述业务实例化模块用于将业务模型加载到底层数据引擎，在实际的业务数据报文通过底层引擎的过程中，使用业务模型定位关注的业务操作，通过模型中定义的业务数据和属性定义，从真实业务数据报文中提取需要的数据，最终封装为对象。

[0048] 在上述实施例中，所述业务模型包括业务操作名称、用户标识、业务操作数据和流程关联规则。

[0049] 在上述实施例中，如图6所示，业务模型由业务流程加属性、规则流加属性、用户操作特征加属性以及业务操作数据等部分构成，上述结构用于支持规则流与流程模拟技术。业务实例化对象结构是一个经过实例化的业务对象，由客户进行业务操作所产生的网络数据经我们的体系实例化而成。它可以是单一业务操作、复杂的业务流程、也可以是多个业务系统内部的流程整合而成。业务实例化对象中包含了业务属性、用户数据、业务数据和审计的结果，可以支撑上层更高级的审计应用。

[0050] 如图2所示，本发明还公开了一种数据的业务特征识别方法，包括以下步骤：

[0051] 1)基于剥离了网络协议后的业务数据，通过定义的标准审计数据结构来实现对业务数据中网络协议的剥离；

[0052] 2)通过业务拆分和业务组合将不同业务流程的业务数据拆分为以业务节点为基本单位，然后再由业务节点组成业务簇，业务簇组成业务流。

[0053] 进一步的，如图5所示，步骤2)包括以下步骤：

[0054] 2.1)业务快照：对业务操作动作的开始和结束行为进行抓取，并在抓取过程中对数据报文和屏幕截图进行存储，业务快照是后面进行业务分析和模型建立的依据；

[0055] 2.2)业务分析：基于业务快照，对业务操作的数据进行识别，分析与业务操作相关的业务数据所在位置和特征，转化为业务规则；

[0056] 2.3)建立模型：将业务规则和业务本身的属性进行定义后的集合，按照统一的结构和持久方式输出为模型文件；

[0057] 2.4)模型验证：使用本地快照进行模型的验证工作，包括业务属性、数据和相关信息的对比，初步验证模型的正确性，若验证结果为正确，则进行以下步骤，若验证结果为不正确，则重新进行步骤2.2)-步骤2.4)的操作；

[0058] 2.5)业务实例化：将业务模型加载到底层数据引擎，在实际的业务数据报文通过底层引擎的过程中，使用业务模型定位关注的业务操作，通过模型中定义的业务数据和属性定义，从真实业务数据报文中提取需要的数据，最终封装为对象，该对象即为业务的实例。

[0059] 在上述实施例中，所述业务模型包括业务操作名称、用户标识、业务操作数据和流程关联规则。

[0060] 在上述实施例中，如图6所示，业务模型由业务流程加属性、规则流加属性、用户操作特征加属性以及业务操作数据等部分构成，上述结构用于支持规则流与流程模拟技术。业务实例化对象结构是一个经过实例化的业务对象，由客户进行业务操作所产生的网络数据经我们的体系实例化而成。它可以是单一业务操作、复杂的业务流程、也可以是多个业务系统内部的流程整合而成。业务实例化对象中包含了业务属性、用户数据、业务数据和审计的结果，可以支撑上层更高级的审计应用。

[0061] 综上所述，借助于本发明的上述技术方案，本发明的数据的业务特征识别系统及方法能够为不同行业，不同网络协议的企业业务系统的信息安全提供全方位的技术支持。

[0062] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

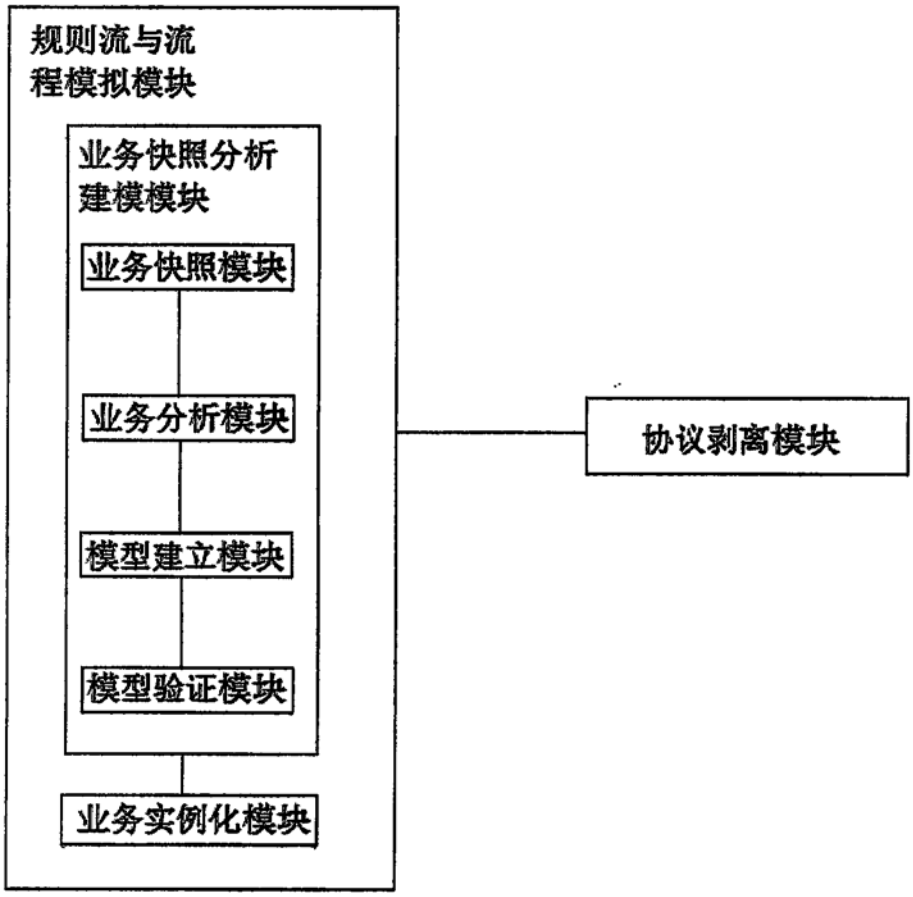

规则流与流
程模拟模块
业务快照分析
建模模块
业务快照模块
业务分析模块
模型建立模块
模型验证模块
业务实例化模块
协议剥离模块

图1

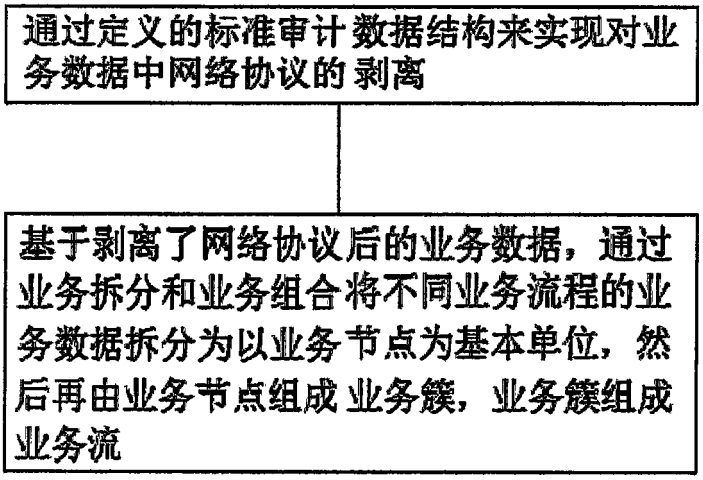

通过定义的标准审计数据结构来实现对业务数据中网络协议的剥离
基于剥离了网络协议后的业务数据，通过业务拆分和业务组合将不同业务流程的业务数据拆分为以业务节点为基本单位，然后再由业务节点组成业务簇，业务簇组成业务流

图2

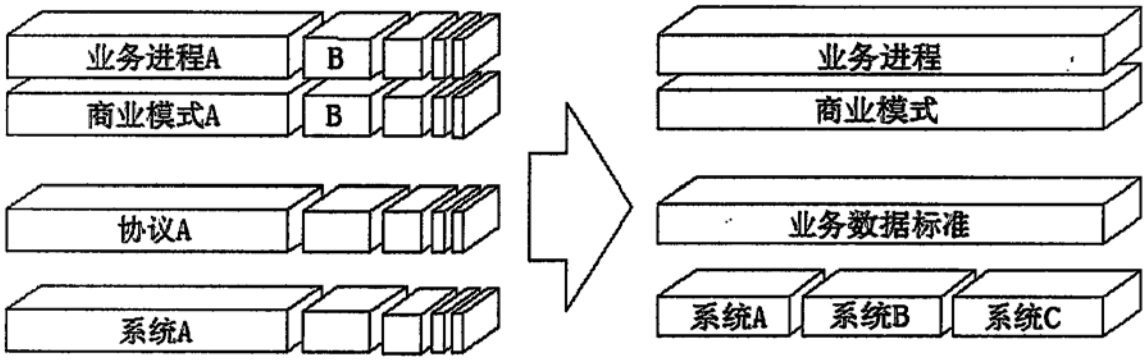

业务进程A
B
商业模式A
B
协议A
系统A
业务进程
商业模式
业务数据标准
系统A
系统B
系统C

图3

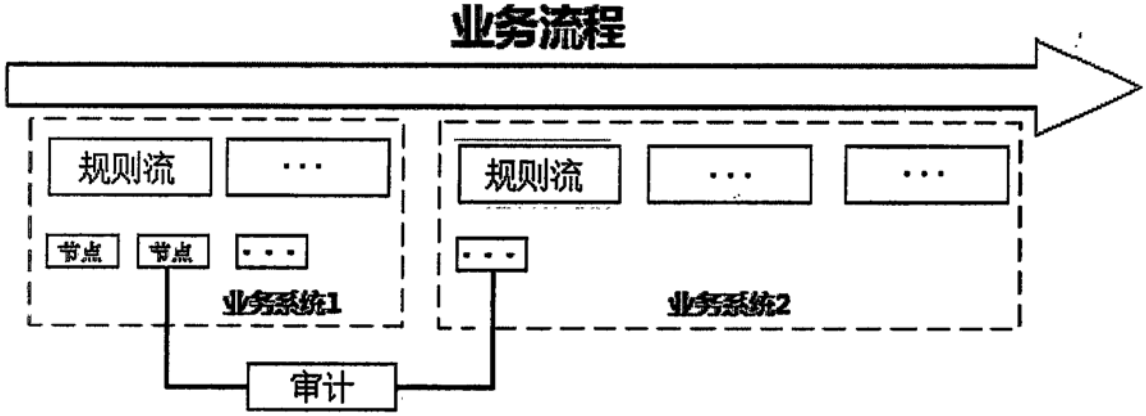

业务流程
规则流
...
节点
节点
...
业务系统1
规则流
...
...
...
业务系统2
审计

图4

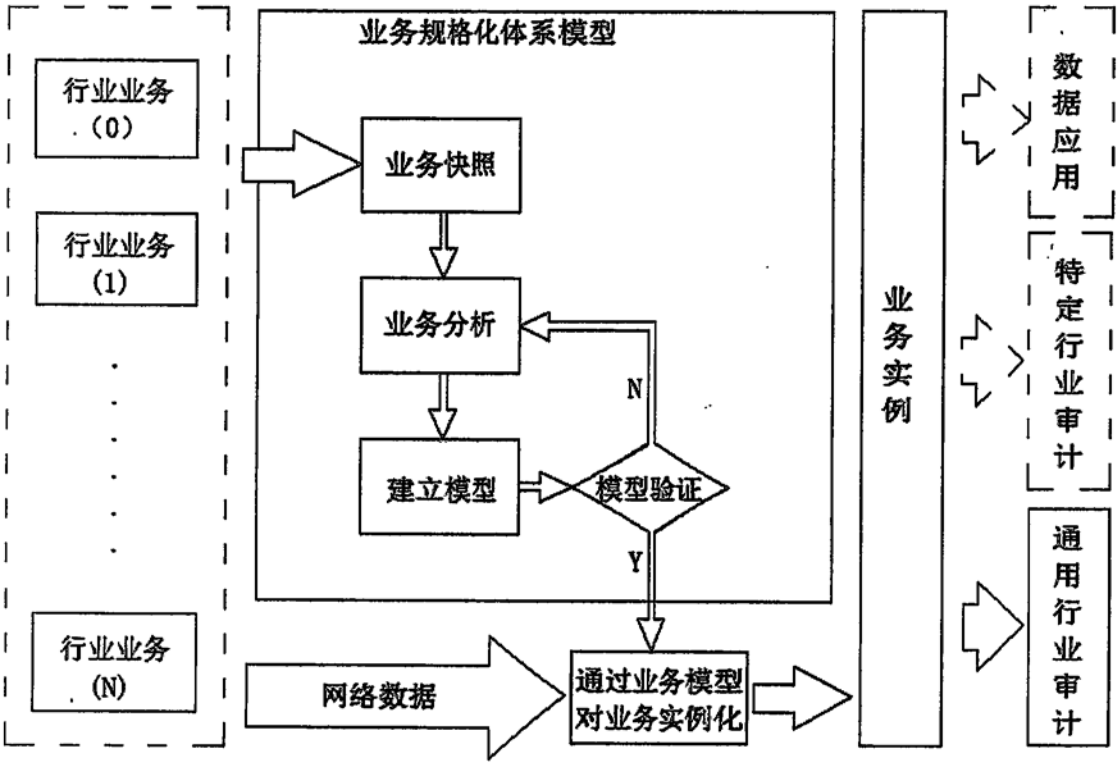

业务规格化体系模型
行业业务（0）
行业业务（1）
行业业务（N）
业务快照
业务分析
建立模型
模型验证
N
Y
网络数据
通过业务模型对业务实例化
业务实例
数据应用
特定行业审计
通用行业审计

图5

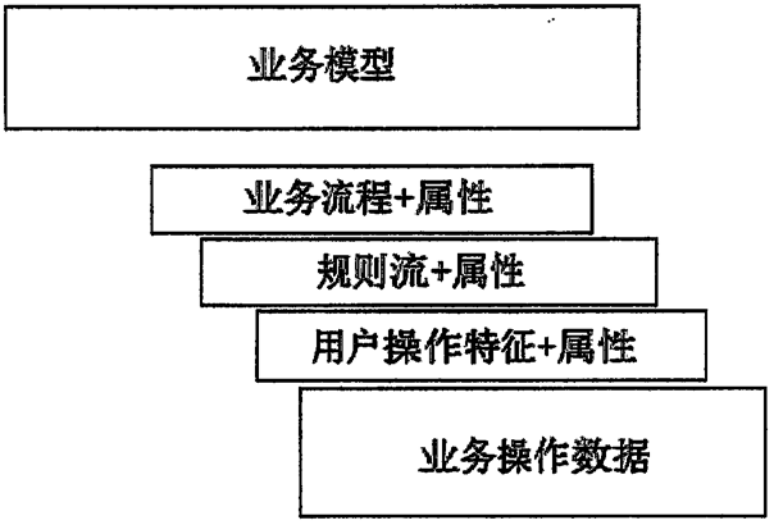

业务模型
业务流程+属性
规则流+属性
用户操作特征+属性
业务操作数据

图6