基于知识图谱与本体驱动的数据建模框架*

徐　睿[1,2]，刘　金[1,2]，冯　志[1,2]，张雅勤[1,2]，董　伟[1,2]
（1. 中国信息安全研究院有限公司，北京　102209；2. 华北计算机系统工程研究所，北京　100083）

摘　要：针对传统数据建模方法在处理多维动态关系和异构数据集成方面的局限性，提出一种基于知识图谱与动态本体驱动的数据建模框架。该框架利用知识图谱灵活表达实体及关系的优势，结合动态本体提供的语义约束，通过实体识别、属性和关系自动映射等技术，将语义信息有效转化为结构化数据模型，提升数据建模的自动化和标准化水平。案例分析表明，该框架可广泛适用于复杂数据结构的语义表示、自动化知识抽取及跨系统的数据融合，展现了良好的通用性和应用价值。

关键词：知识图谱；动态本体；数据建模
中图分类号：TP311.13　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2025.08.006
引用格式：徐睿，刘金，冯志，等. 基于知识图谱与本体驱动的数据建模框架[J]. 网络安全与数据治理，2025，44(8)：39-45.

A data modeling framework driven by knowledge graphs and ontologies

Xu Rui[1,2], Liu Jin[1,2], Feng Zhi[1,2], Zhang Yaqin[1,2], Dong Wei[1,2]
(1. China Information Security Research Academy Co., Ltd., Beijing 102209, China;
2. National Computer System Engineering Research Institute of China, Beijing 100083, China)

Abstract: To address the limitations of traditional data modeling methods in handling multi-dimensional dynamic relationships and heterogeneous data integration, this paper proposes a data modeling framework driven by knowledge graphs and dynamic ontologies. The framework leverages the flexibility of knowledge graphs in representing entities and relationships, combines with the semantic constraints provided by dynamic ontologies, and through entity recognition, automatic mapping of attributes and relationships, and other techniques, effectively transforms semantic information into a structured data model, thereby enhancing the automation and standardization of data modeling. Case studies demonstrate that this framework is broadly applicable to semantic representation of complex data structures, automated knowledge extraction, and cross-system data integration, showcasing strong versatility and practical value.

Key words: knowledge graphs; ontologies; data modeling

0　引言

数据建模作为数据治理的核心任务，通常采用实体-关系模型，通过定义实体、属性和关系等抽象结构来描述数据的语义，再映射为具体的数据库表、字段及约束，从而实现数据的存储与管理。然而，随着数据量的迅猛增长以及业务需求的日益复杂，传统的关系型数据建模方法逐渐暴露出诸多局限性。例如，传统方法依赖于静态的表结构和字段定义，难以有效处理多维度、动态变化的数据关系，也很难适应异构数据源的集成需求。随着大数据、人工智能和知识图谱等新兴技术的快速发展，数据建模的范式也在发生深刻变化。

在这一背景下，知识图谱和动态本体技术可以在数据治理领域发挥重要作用。知识图谱通过图结构表示实体及其关系，并能够通过语义推理揭示数据之间的深层次联系。本体则为知识图谱提供了一个规范的语义框架，帮助明确各类实体及其属性的定义及相互关系。知识图谱和动态本体的结合，不仅提供了更灵活的建模手段，还能够促进跨系统的数据集成，提升数据的语义理解与质量控制。

*基金项目：中国电子信息产业集团有限公司特色科研项目(631010303)

www.pcachina.com

这一映射过程不仅是技术创新，也体现了对人类认知与理解世界方式的模拟。认知科学认为人类通过抽象符号、分类和关系表达知识，本体与知识图谱正是构建这种抽象模型的工具。在智能化趋势下，知识图谱作为模拟人类认知的“图式语言”，帮助机器理解、推理与学习数据，例如结合图神经网络（Graph Neural Network，GNN）进行推理与分析[1]。在网络安全领域，知识图谱能够通过路径推理识别攻击者的潜在利用路径（如漏洞→系统→攻击者），或通过关系映射发现未修复漏洞的关联防御措施。

在此基础上，考虑到当前大部分业务系统的数据仍主要存储于结构化数据库中，而知识图谱直接应用于业务系统的落地尚存在较大挑战，因此本文提出一种基于知识图谱和本体驱动的数据建模框架。通过将知识图谱中的实体、属性和关系有效映射到数据库表结构，实现从语义建模到结构化数据存储的高效转化；并结合威胁情报自动抽取、跨系统数据融合等业务应用场景验证框架能力。

1　相关工作

1.1　知识图谱

秦锋剑[2]提出基于第三代知识图谱的政务数据治理方案，通过数据汇聚、组织、标识和关联，提高政务数据质量，并应用于公安、司法、社会治理等领域。李宏伟[3]研究实验室数据治理，构建概念模型，采用 Neo4j 数据库构建图谱，实现资源管理和教学数据的智能化支持。许强等[4]探讨政务数据知识图谱应用，提出数据预处理、实体识别、知识建模等五阶段流程，以增强数据共享和智能决策能力。高龙等[5]提出基于事理图谱的航空数据智能技术，重点研究本体建模、事件抽取和因果推理，构建航空产品质量问题知识图谱，实现智能分析和快速响应。这些工作展示了知识图谱在复杂数据语义关联、智能分析方面的优势。

1.2　动态本体

李勰婧等[6]提出面向军事领域的动态本体构建方法，通过本体自动更新提升异构数据的集成能力。刘春明等[7]将动态本体应用于情报认知决策，构建基于目标行为建模和跨域本体融合的分析框架，提升智能研判能力。李翔等[8]研究了作战数据的隐含关系重构，提出自动生成动态本体的方法，提高语义推理能力。刘伟等[9]基于动态本体优化战场目标数据关联，增强态势估计和威胁分析能力。王娜等[10]系统综述了动态本体构建的研究现状，探讨知识建模、自动更新与标准化方法，强调多源数据融合的重要性。徐超等[11]提出基于动态本体的目标特性数据组织技术，构建差异个体模型，提升数据组织与推理能力。张婉晨等[12]研究基于动态本体的知识图谱构建，采用本体自动化更新技术，优化语义匹配，提高知识图谱的自适应性。上述研究推动了动态本体在数据建模、语义推理和知识图谱构建中的发展。

1.3　数据建模

吴信东等[13]构建华谱系统，提出数据中台 + 知识图谱的家谱数据治理方案，通过优化数据采集、标准化和知识推理，实现多源异构数据的高效管理。陈渠等[14]研究基于本体的企业运营数据治理，通过领域本体建模、RDF 映射和 D2RQ 转换，提升数据标准化、语义一致性及跨系统共享能力。栾瑞鹏等[15]提出装备试验鉴定数据治理方法，结合知识图谱 + 关系数据库/数据仓库的双层架构，利用本体建模、实体识别和 Neo4j 存储优化数据关联、追溯和智能决策。研究表明，知识图谱与本体技术在数据治理、标准化建模和智能分析方面具有显著优势。

现有研究在知识图谱与动态本体的语义建模、数据融合和智能分析方面取得了一定进展，但仍缺乏从认知视角对数据建模方法的深入探讨，且自动化程度不足。本文提出基于知识图谱与本体驱动的数据建模框架，以提升数据融合能力与建模灵活性。

2　知识图谱与本体概述

随着数据复杂性和关联性的增加，传统数据建模方法难以满足需求。知识图谱通过图结构灵活表达数据实体与关系，本体则提供标准的语义框架定义数据类别、属性与关系，两者结合能显著提升语义理解与建模的准确性。本节将介绍知识图谱和本体的基本概念及其在数据建模中的协同作用。

2.1　知识图谱的定义与作用

知识图谱（Knowledge Graph，KG）是一种通过图结构来表示实体及其之间关系的数据模型。它由节点（实体）和边（实体之间的关系）组成，并通过图的形式呈现数据的语义。知识图谱不仅仅是一种数据存储形式，更强调通过语义关联对数据进行深度理解和推理。

知识图谱的基本构成包括：

（1）实体（Entity）：知识图谱中的节点，代表现实世界中的各种事物，如网络安全领域中的“漏洞”“服务器”“攻击者”。

（2）属性（Attribute）：实体的特征或描述，通常以键值对的形式存在，如漏洞的“CVSS 评分”“披露日期”或系统的“IP 地址”“操作系统类型”。

（3）关系（Relation）：描述实体之间的联系或相互作用的边，通常是有向的。例如，攻击者与漏洞之间可

www.pcachina.com

能有“利用”关系，系统与漏洞之间有“受影响”关系。

知识图谱能够灵活地表示复杂的多层次、多维度的数据关系，支持数据之间的语义推理和查询。通过图结构的形式，知识图谱能够展示出实体间的各种关联，便于进行跨领域、跨系统的数据集成与共享。

2.2 本体的定义与作用

本体（Ontology）是知识图谱中的核心组成部分之一，它提供了对特定领域知识的正式、精确的定义。本体通过一套规范的术语和概念描述某一领域中的事物及其相互关系。简而言之，本体为知识图谱提供了一个语义框架，定义了实体的类别、属性以及实体之间的关系。

本体的主要构成包括：

（1）类（Class）：定义了实体的类别，描述了一类具有共同特征的对象。例如，“漏洞”类可以包括所有漏洞相关的实体，“网络设备”类则可以包括所有路由器、防火墙等设备。

（2）实例（Instance）：属于某一类的具体对象。例如，某个具体的漏洞（如“CVE-2021-44228”）是“漏洞”类的一个实例。

（3）属性（Property）：描述类或实例的特征或维度。例如，“漏洞”类可能包含“CVSS 评分”“漏洞类型”等属性。

（4）关系（Relation）：描述不同类或实例之间的联系。例如，攻击者与漏洞之间的“利用”关系，补丁与漏洞之间的“修复”关系。

本体的作用不仅仅是为知识图谱提供结构，它还通过定义共享的概念和术语，确保不同系统和数据源之间的语义一致性。通过本体，数据建模者可以对领域知识进行标准化，使得不同的数据库、应用程序和分析系统能够理解和共享相同的数据语义。

与传统本体相比，动态本体（Dynamic Ontology）具有随业务环境或数据变化进行动态更新和演化的能力，能够及时调整实体、属性和关系的定义，更好地适应数据的实时性与变化性需求。通过引入动态本体，可实现语义模型的自动更新，降低人工维护成本，提高对异构数据的集成能力，提升数据建模的灵活性和适应性，特别适合实时或快速变化的数据场景，如网络安全中的实时威胁情报分析和攻击路径推理等应用。

2.3 知识图谱与本体的关系

知识图谱和本体紧密相连，但它们的功能和侧重点有所不同。知识图谱更侧重于数据的图形表示，强调如何通过图的结构来组织和存储信息；而本体则注重于领域知识的形式化描述，为知识图谱提供语义和概念框架。

（1）知识图谱是本体的实例化：本体提供了一个通用的结构和标准，定义了领域中的实体类别、属性和关系，而知识图谱则是这一结构的具体实例。简单来说，知识图谱是根据本体的定义，对现实世界中的具体数据进行建模并通过图形化的方式进行呈现。

（2）本体为知识图谱提供语义支持：知识图谱通过图结构表示数据的关联性，但没有提供具体的语义约束。而本体则通过定义术语、关系和约束，赋予知识图谱更丰富的语义信息，确保数据在不同系统和应用中的一致性和可理解性。

例如，在网络安全领域，本体可能定义了“漏洞”“网络设备”和“攻击者”这三个类，并且规定了它们的属性（如漏洞类具有 CVSS 评分、披露日期等属性）。而在实际构建知识图谱时，这些类的具体实例（如“CVE-2021-44228”作为漏洞实例）将根据本体的定义被映射成图中的节点，通过关系（如攻击者利用漏洞）连接起来，形成一个完整的知识图谱。

2.4 知识图谱与本体在数据建模中的作用

知识图谱与本体的结合为数据建模提供了传统方法难以实现的能力，主要体现在以下四方面：

（1）增强语义理解：本体为字段赋予明确语义，使知识图谱不仅存值，还能表达含义。如“CVSS 评分”被定义为漏洞严重度量化指标，可直接驱动自动风险分级。

（2）促进跨系统集成：统一术语与结构后，异构数据源（如 CVE 库、ATT&CK 矩阵）可语义对齐；知识图谱将漏洞事件与防御技术（D3FEND）串联，形成攻防全景。

（3）提升数据质量：本体规范约束属性格式，避免冗余与错误。例如规定“CVE 编号”必须匹配 CVE-YYYY-XXXX 正则，自动阻断非法值。

（4）支持推理分析：结合规则与 GNN，可从图中推断隐藏关联：如识别 APT 组织可能利用的未修复漏洞，或根据补丁状态生成修复优先级。

3 基于知识图谱的数据建模框架

基于知识图谱的数据建模框架主要包括数据源、实体与关系抽取、本体/规则定义、属性与关系映射以及业务应用层等关键组成部分，如图 1 所示。这些组成部分相互衔接，构成了完整的数据建模流程，通过知识图谱与本体驱动的语义约束机制，以及 GNN 动态关系推理能力的支撑，能够更有效地表达复杂数据关系，提升数据建模的自动化水平，并确保数据的一致性与质量。

3.1 实体建模与属性映射

在传统的数据建模过程中，实体通常对应着数据库中的表格，而实体的属性则对应着表中的字段。然而，

www.pcachina.com

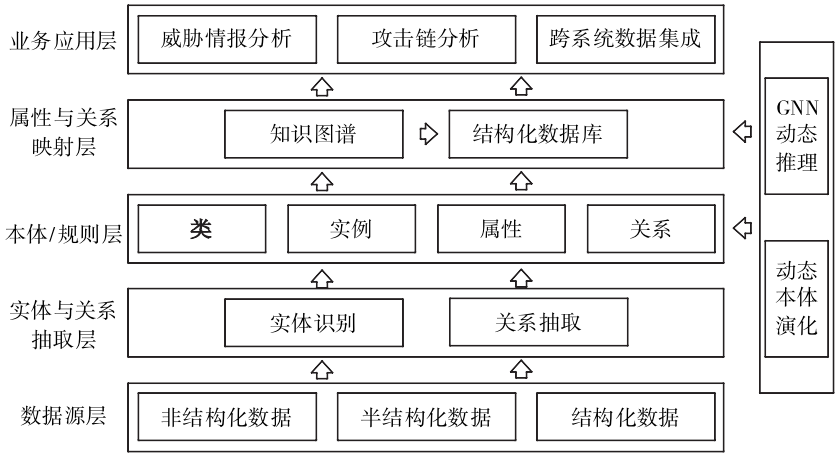

图 1　基于知识图谱的数据建模总体框架

传统方法往往难以处理复杂的数据关系和动态变化的需求。基于知识图谱的建模方法通过引入语义层次的实体建模，能够更好地表达实体的多维属性。

在知识图谱中，实体通过节点进行表示，每个节点都具有特定的属性。这些属性不仅仅是简单的字段值，还可以是其他更为复杂的关系或属性的组合。例如，在网络安全领域中，“漏洞”实体可能包含 CVSS 评分、漏洞类型、披露日期等属性，而这些属性可以进一步与其他实体（如“攻击者”或“系统”）之间建立联系。通过本体的定义，可以对每个属性的语义进行明确规定，例如在网络安全本体中，“CVSS 评分”属性被约束为［0，10］区间的浮点数，且必须关联 CVE 编号实体，这种形式化规则保障了多源漏洞数据的语义一致性。此外，针对属性缺失场景（如日志中未标注漏洞类型），引入图神经网络的邻域特征聚合机制，通过分析关联实体（如攻击者 IP、受影响系统）的图结构特征，可以实现属性值的概率化推断。

实体建模的过程通常由以下几个步骤构成：

（1）识别实体：从数据源中提取具有独立意义的对象，如“攻击者”“漏洞”“系统”等。

（2）定义实体属性：根据领域知识为每个实体定义相关属性，如“漏洞”的“CVSS 评分”属性、“系统”的“操作系统类型”属性等。

（3）映射到字段：将实体的属性映射到数据库表的字段中，从而将实体的语义信息转化为数据库的结构化数据。

3.2　关系建模与表结构映射

除了实体与属性的建模，基于知识图谱的数据建模还涉及实体之间关系的定义和表示。在传统的关系型数据库中，实体之间的关系通常通过外键或关联表来表示。然而，这种方式难以处理多对多、递归关系等复杂结构，且缺乏灵活性。

基于知识图谱的建模方法通过图结构自然地表达实体之间的多层次关系。关系可以是有向的，指明实体之间的关系方向，也可以是无向的，表示实体间的相互作用。例如，在网络安全领域，“攻击者”与“漏洞”之间的关系可以通过“利用”关系来表示，而这一关系可以在知识图谱中清晰地映射为“攻击者 - 利用 - 漏洞”这样的三元组。同时，通过 GNN 动态关系推理模块，能够从历史攻击数据中自动发现潜在关系（如攻击者 A 与漏洞 B 的间接关联置信度 >0.8 时生成新边）。

在数据库中，关系可以通过关联表来实现，通常包含外键字段。与传统建模不同，基于知识图谱的建模方法能够在数据库表结构中更为灵活地实现复杂关系的映射。例如，“漏洞利用记录”表不仅包含攻击时间、攻击方式等基本信息，还可以通过外键与“漏洞”表、“系统”表建立复杂的关系。每一条关系都可以明确描述数据之间的连接规则，从而提供更清晰的数据结构。

3.3　数据建模过程中的自动化与标准化支持

知识图谱的一个显著优势是它能够提高数据建模的自动化和标准化程度。传统的数据建模方法依赖人工定义每个数据表及其字段，在大规模数据系统中，这种方式不仅耗时，还容易出错。而基于知识图谱的建模方法，通过本体的定义和图谱的构建，可以在较少人工干预的情况下自动识别实体、属性和关系，并将它们映射到数据库表中。

具体来说，基于知识图谱的数据建模过程可以通过以下几种方式实现自动化：

（1）自动化实体识别：利用自然语言处理（Natural Language Processing，NLP）技术，从非结构化数据中自

www.pcachina.com

动识别实体。例如，从漏洞报告、日志文件中提取出“漏洞”“攻击者”“系统”等实体。

（2）属性和关系自动映射：基于本体中的定义，可以自动识别每个实体的属性和它们之间的关系。例如，本体可以明确“漏洞”实体具有“CVSS 评分”“CVE 编号”等属性，并通过定义好的规则自动将它们映射到表字段。同时，结合 GNN 的图嵌入技术，实现威胁情报实体消歧（如区分“CVE-2021-44228”在不同日志中的别名表述），使跨系统实体对齐准确率得到提升。

（3）图谱更新与扩展：当新的数据或关系出现时（如新漏洞披露或攻击事件），知识图谱能够根据定义自动更新或扩展现有模型。这使得数据建模能够适应安全需求的变化，减少了人工干预和更新的成本。

标准化则通过统一的本体定义和建模框架，确保数据建模过程中的一致性。通过标准化，组织可以在不同系统或业务部门之间共享统一的数据模型，提高威胁情报共享和协同防御能力。

3.4 本体增强模型的灵活性与扩展性

本体不仅在知识图谱构建中起着核心作用，还能够增强数据建模模型的灵活性和扩展性。传统数据建模方法中，模型一旦定义完成，往往较难调整和扩展，尤其是当业务需求发生变化时。而基于本体的建模方法，能够通过动态本体演化等机制来灵活调整模型结构，适应新的数据类型和业务需求。

例如，当一个新的安全实体（如“零日漏洞”）需要加入系统时，只需在本体中定义该实体及其属性（如“利用难度”“未公开补丁状态”），然后通过图谱的扩展机制将其加入到已有的模型中。这一过程不需要大规模修改原有数据结构，使得模型的扩展更加高效。

4 应用案例分析：基于开源知识图谱的数据建模

本节将通过使用常见的开源数据集或知识图谱（如 CVE、ATT&CK）来展示基于知识图谱的数据建模方法的应用。通过选择一个具体领域（如威胁情报分析或漏洞管理），展示如何将开源知识图谱中的实体、属性和关系映射到数据库表中，并探讨这种方法的实际效果与优势。

4.1 选择开源知识图谱

开源知识图谱在网络安全领域具有重要价值，如：

（1）CVE：全球标准化的漏洞标识库，提供漏洞编号、描述、CVSS 评分等结构化数据。

（2）ATT&CK：MITRE 开发的对抗战术与技术知识库，描述攻击者的行为模式、技术手段及关联漏洞。

这些开源知识图谱已经构建了丰富的安全实体（如“漏洞”“攻击技术”“防御措施”）、属性（如“CVSS 评分”“攻击阶段”）和关系（如“利用”“防御对抗”），可作为数据建模的基础。

4.2 选择应用领域：威胁情报分析示例

为了直观展示基于知识图谱的数据建模方法，本文选择了威胁情报分析作为应用场景。在安全运营中，攻击者、漏洞、系统、攻击链等实体和它们之间的关系是数据建模的关键对象。本文将基于 ATT&CK 知识库和 CVE 数据，描述攻击者、漏洞和攻击技术之间的关联，进而将它们映射到数据库表结构中。

4.3 实体建模与属性映射

从 ATT&CK 知识库和 CVE 中提取与威胁情报相关的实体及其属性，如表 1 所示。

表 1 实体及其属性

	实体	属性
1	漏洞（Vulnerability）	CVE 编号、CVSS 评分、受影响系统类型、披露日期
2	攻击者（Attacker）	攻击组织名称（如 APT29）、常用攻击技术、活跃时间范围
3	系统（System）	IP 地址、操作系统类型、补丁状态

映射到数据库表结构，如表 2 所示。

表 2 实体数据库表结构

	漏洞表（Vulnerability）	攻击者表（Attacker）	系统表（System）
1	ID	ID	ID
2	CVE 编号	攻击组织 ID	系统 ID
3	CVSS 评分	组织名称	IP 地址
4	受影响系统类型	常用攻击技术	操作系统类型
5	披露日期	活跃时间范围	补丁状态

4.4 关系建模与表结构映射

关键安全关系定义与映射：

（1）利用（Exploit）：攻击者利用漏洞实施攻击；

（2）影响（Affect）：漏洞对特定系统类型产生影响；

（3）修复（Patch）：补丁与漏洞的修复关系。

关联表设计如表 3 所示。

4.5 案例分析：基于 ATT&CK 知识库的攻击链建模

假设从 ATT&CK 知识库和 CVE 中获取以下信息：

（1）漏洞“CVE-2021-44228”：CVSS 评分 10.0，影响 Log4j 库的远程代码执行漏洞。

（2）攻击者“APT29”：常用技术包括 T1190（利用公开应用漏洞）、T1059.001（PowerShell 脚本攻击）。

www.pcachina.com

表 3　关联表结构

	攻击事件表（AttackEvent）	漏洞影响表（VulnerabilityAffect）	补丁管理表（PatchManagement）
1	ID	ID	ID
2	事件 ID	CVE 编号	补丁 ID
3	攻击组织 ID	受影响系统类型	CVE 编号
4	CVE 编号	验证状态	发布日期
5	攻击时间		部署状态
6	攻击技术		

（3）系统“192. 168. 1. 100”：操作系统为 Ubuntu 20. 04，未部署 Log4j 补丁。

映射到数据库表结构如表 4 ~ 表 6 所示。

表 4　漏洞表数据

No	CVE 编号	CVSS 评分	受影响系统类型	披露日期
1	CVE-2021-44228	10. 0	Java 应用	2021 - 12 - 09

表 5　攻击者表数据

No	攻击组织 ID	组织名称	常用攻击技术
1	APT29	Cozy Bear	T1190，T1059. 001

表 6　攻击事件表数据

No	事件 ID	攻击组织 ID	CVE 编号	攻击时间
1	2023-001	APT29	CVE-2021-44228	2023 - 05 - 15

4. 6　案例中的挑战与解决方案

案例中存在的挑战及解决方案如下：

（1）数据异构性：不同知识图谱（如 CVE 与 ATT&CK）的数据粒度差异。通过定义映射规则（如 CVE 关联 ATT&CK 技术 T1190）实现跨图谱整合。

（2）实时性要求：漏洞披露和攻击事件需快速更新模型。结合流处理技术（如 Apache Kafka）触发图谱动态扩展。

（3）复杂关系推理：攻击链涉及多跳关系（如漏洞→利用技术→防御措施）。通过图数据库（如 Neo4j）的路径查询支持实现关联分析。

5　结论与未来展望

5. 1　研究总结

本文从认知科学与符号学理论的交叉视角出发，提出了一种基于知识图谱与本体驱动的数据建模框架。针对传统关系型建模方法在网络安全领域面临的复杂攻击链表征、异构威胁情报融合等难题，本研究通过引入本体驱动的语义约束机制与图神经网络的动态关系推理能力，实现了多源数据的高效语义对齐与上下文感知建模。

相较于静态表结构建模范式，本文的创新性体现在三个方面：

（1）通过实体 - 属性 - 关系的认知分层架构，模拟了网络安全专家在威胁分析中的多粒度推理逻辑，使得漏洞关联、攻击模式识别等场景的建模效率得到提升；

（2）基于动态本体演化机制，构建了具有普适性的建模体系，解决了传统方法因固定模式导致的模型迭代滞后问题；

（3）以数据要素为核心驱动，设计了面向网络安全领域的知识资产化路径，通过威胁情报的语义标注与跨系统流通，验证了数据要素在提升安全运营协同性中的枢纽作用。

5. 2　实践启示

本研究的成果为数据密集型行业的智能化建模提供了可复用的方法论：

（1）网络安全领域

基于攻击链知识图谱的动态推理引擎，可支持多跳攻击路径的实时推演（如 Log4j 漏洞在云原生环境中的传播链预测）。

（2）跨行业推广

①金融行业：通过交易实体本体与行为图谱的融合建模，可突破传统反洗钱规则引擎的阈值限制，实现异常资金网络的概率化识别。

②医疗行业：基于设备资产本体的医疗数据互操作性框架，能够打通影像数据、电子病历与药品供应链的语义壁垒，为隐私计算环境下的跨机构数据协同提供基础设施。

③数据要素开发：知识图谱的语义增强能力可提升非结构化数据（如安全日志、医疗文本）的要素化效率。

5. 3　未来展望

面向数据要素全域流通与行业数字化转型深度融合的趋势，后续研究可从以下方向突破：

（1）理论深化层面

探索知识图谱与因果推理的结合路径，解决当前模型在 APT 攻击归因、金融系统性风险传导等场景中的解释性瓶颈，构建符合《中华人民共和国数据安全法》要求的可审计建模框架。

（2）技术融合方向

①针对医疗、金融等行业对实时性的特殊需求，研究流式图谱与时序本体（Temporal Ontology）的协同演化机制；

②开发支持联邦学习的分布式建模架构，在保障数

www.pcachina.com

据主权的前提下实现跨行业威胁情报的共享推理。

（3）生态构建维度

①建立覆盖网络安全、金融、医疗等领域的本体互操作标准，破解跨行业数据要素流通的语义异构难题；

②设计基于数据要素贡献度的价值分配模型，为威胁情报市场、医疗科研数据湖等新型数据要素交易模式提供激励机制。

本研究揭示的知识驱动建模范式，本质上是通过机器可理解的语义符号系统重构人类认知世界的抽象逻辑。随着“数据二十条”对数据要素化的制度性推进，基于知识图谱的认知型数据建模框架，或将成为打通行业知识壁垒、释放数据要素价值的通用基础设施。未来研究需在技术可行性与社会接受度的平衡中，探索符合人类价值观的机器认知演进路径。

参考文献

[1] 孙水发，李小龙，李伟生，等. 图神经网络应用于知识图谱推理的研究综述［J］. 计算机科学与探索，2023，17（1）：27－52.

[2] 秦锋剑. 基于第三代知识图谱的政务数据治理［J］. 软件和集成电路，2019（8）：78－79.

[3] 李宏伟. 基于知识图谱的实验室数据治理［J］. 实验科学与技术，2025，23（2）：138－143.

[4] 许强，孟宇桥. 基于知识图谱的政务数据应用分析［J］. 集成电路应用，2022，39（9）：272－273.

[5] 高龙，卫青延，陶剑，等. 事理图谱赋能的航空数据智能技术研究［J］. 航空工程进展，2023，14（2）：178－190.

[6] 李勰婧，胡建军，吴迪，等. 面向军事领域的动态本体构建技术研究［J］. 现代防御技术，2023，51（6）：52－61.

[7] 刘春明，张伟康，陈汉一. 基于动态本体的情报认知决策分析技术［J］. 网络安全技术与应用，2023（6）：50－53.

[8] 李翔，刘坤，刘艺，等. 面向动态本体的作战数据隐含关系重构方法研究［C］//中国指挥与控制学会. 第十二届中国指挥控制大会论文集（下册），2024：116－121.

[9] 刘伟，翟崎，李子，等. 基于动态本体的战场目标数据关联技术［J］. 指挥信息系统与技术，2023，14（4）：51－56.

[10] 王娜，蒋智慧. 动态本体构建的国内外研究现状综述［J］. 现代情报，2020，40（4）：159－166.

[11] 徐超，白洁，陈莉，等. 一种基于动态本体的目标特性数据组织技术［J］. 中文科技期刊数据库（全文版）自然科学，2023（6）：147－150.

[12] 张婉晨，郭黎，张毅，等. 动态本体的知识图谱构建技术［J］. 信息工程大学学报，2024，25（4）：417－422，498.

[13] 吴信东，盛绍静，蒋婷婷，等. 从知识图谱到数据中台：华谱系统［J］. 自动化学报，2020，46（10）：2045－2059.

[14] 陈渠，凌卫青，王坚. 基于本体的企业运营数据治理［J］. 电脑知识与技术，2017，13（3）：1－3.

[15] 栾瑞鹏，张静，刘立坤. 面向装备试验鉴定领域数据治理的知识图谱本体构建［J］. 系统工程与电子技术，2024，46（3）：1013－1020.

（收稿日期：2025－04－18）

作者简介：

徐睿（1990－），男，博士，高级工程师，主要研究方向：信息内容安全、自然语言理解、数据治理。

刘金（1990－），通信作者，女，硕士，高级工程师，主要研究方向：网络安全、数据分析处理。E-mail：liujin972181761@126.com。

冯志（1990－），男，硕士，高级工程师，主要研究方向：网络安全、工控安全、移动网络安全等。

www.pcachina.com

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com