产业发展

工业互联网平台数据安全韧性评价体系构建与应用研究

陆婧瑜，杨 伟

（杭州电子科技大学管理学院，杭州 310018）

摘要：数据安全对工业互联网平台健康发展至关重要。为科学量化工业互联网平台数据安全水平，引入韧性理论。从系统安全领域对韧性内涵的理解出发，提出了工业互联网平台数据安全韧性概念，明确了数据安全韧性包括风险预期性、防御性、抵抗性和恢复性四方面。在此基础上，采用文本挖掘法并结合语义网络分析，构建了基于韧性视角的工业互联网平台数据安全评价指标体系。通过G1法确定韧性指标独立权重，使用DEMATEL法量化韧性指标的关联权重，最终得到混合权重。进一步，提出基于云模型的工业互联网平台数据安全韧性评价模型。利用该模型对YQ工业互联网平台的数据安全韧性进行评价，评价结果与实际情况相符，验证了基于混合权重和云模型的工业互联网平台数据安全韧性评价方法的科学性与合理性。最后，针对工业互联网平台现存的问题对工业互联网平台数据安全未来发展提出建议，为今后提升数据安全韧性提供一定的理论支持。

关键词：工业互联网平台；数据安全；韧性

中图分类号：F272.2 **文献标志码：**A **文章编号：**1671－1807(2025)10－0083－09

工业互联网平台代表着新一代信息技术与工业技术深度融合，形成了一种新型的工业生态系统和应用方式[1]。在工业制造流程中数据是备受瞩目的战略资产，可以被挖掘用以预测未来的生产动向、整合产业链的价值，是推进产业向智能制造转型的引擎[2]。目前，国内外学者对于工业互联网平台的研究多以平台建设[3-4]、资源配置[5-6]。国内多集中工业互联网的平台架构[7]、评价体系[8-9]及发展路径[10]等方面，对工业互联网平台的数据安全研究相对较少。

中国高度重视工业互联网平台数据安全，工信部发布《加强工业互联网安全工作的指导意见》[11]，强调要提高工业互联网数据安全保护能力、企业数据安全防护能力；建立工业互联网全产业链数据安全管理体系；围绕工业互联网风险评估、数据保护、信息共享、应急处置等方面健全安全管理制度和工作机制。工业互联网平台数据增长迅猛，价值高且流动复杂，所面对的数据安全威胁也日益多样化。选择合适的视角研究并建立工业互联网平台数据安全评价指标体系，对于预防数据安全事故，提高工业互联网平台数据安全管理水平，对工业互联网平台健康发展有重要意义。

针对工业互联网平台面临的数据安全问题，本文基于韧性视角，提出一种综合评估方法。首先，选取数据监控能力、数据处理能力、数据防护能力、数据恢复能力作为一级指标。其次，通过文本挖掘结合语义网络分析以及专家访谈，确定了与数据安全密切关联的二级评价指标，并与韧性理论中的预期性、防御性、抵抗性、恢复性相关。最后，采用定性与定量相结合的方法，综合确定了33个具体的数据采集项全面评估工业互联网平台数据安全韧性水平。本文不仅有助于深化对工业互联网平台数据安全的理论认识，也为评估工业互联网平台数据安全韧性水平提供有益的工具。

1 数据安全韧性评价维度与指标筛选

1.1 韧性视角下数据安全评价维度

虽然最初韧性是用于描述材料在负载的抗变形和抗断裂特性[12]，但是后来学者们基于他们各自

收稿日期：2024-11-17

基金项目：国家自然科学基金(72174051)

作者简介：陆婧瑜(1999—)，女，新疆克拉玛依人，硕士研究生，研究方向为工业互联网平台、数据安全、韧性；杨伟(1978—)，男，甘肃张掖人，博士，教授，博士研究生导师，研究方向为数字创新管理。

专业视角对韧性的概念进行研究。Holling[13]认为韧性是系统的持久性，及其吸收扰动和变化的能力。韧性描述了系统避免状态转变或从非常态中快速恢复的能力。Adger等[14]认为韧性应该在应对外部冲击的过程中不断学习并持续成长以更好地适应外部环境变化。李平和竺家哲[15]认为韧性是系统面对变化、压力、冲击或威胁时，能够维持系统结构、功能以及正常运行的能力。韧性理论逐渐应用于各个领域，在危机管理和风险管理中发挥重要作用，安全韧性的研究也越来越受到重视。在公共安全领域，范维澄[16]提出安全韧性的“4＋1”研究方法，实现在灾害发生时的即时响应和灾后迅速复原，以此保障城市的可持续发展和居民的安全；黄浪等[17-18]认为安全韧性不仅在于面对干扰或变化时保持功能、快速恢复，更强调能从中吸取教训提高未来应对类似情况的能力。罗通元[19]认为安全韧性指系统发生事故前的管理、监测、预测、预警的能力，事故发生中的响应、决策和协调能力，事故发生后的恢复、处置和反馈能力。

不仅如此安全韧性理论在数据安全领域也有学者展开了研究，邹纯龙等[20]基于安全韧性理论构建公共数据安全韧性治理体系，该体系主要分为预警体系、应对体系、恢复体系和成长体系四部分。本文认为工业互联网平台数据安全韧性的内涵可以从数据安全韧性和工业互联网平台两个维度加以理解。一方面，数据安全韧性是韧性概念的延伸，这种韧性并非源自单一的能力，而是由多个因素构成的复杂组合。且数据安全韧性不同于被动防御，更强调积极主动地加强安全措施和优化安全状态，是工业互联网平台内在的安全能力，核心是面对冲击时平台的数据收集、管理等活动的抵抗能力和恢复能力[21]。

具体而言，工业互联网平台的数据安全韧性包括预期性、防御性、抵抗性和恢复性四个维度。预期性强调平台对潜在数据安全威胁的洞察力与预测力，能否通过持续的风险评估来感知并识别潜在的数据安全威胁。防御性是平台采取的措施和策略，以预防各种威胁对平台造成的影响。抵抗性是在平台面对威胁时能够抵抗、减轻或阻止损害的能力，提高抵抗性可以更好地应对各种挑战。恢复性是平台在受到威胁或遭受损害后，能够迅速从中恢复并重新建立正常运作状态的能力[22]。

1.2 指标构建流程与方法

首先，对工业互联网平台数据安全韧性的相关文本进行检索收集，归纳其关键信息。其次，运用文本挖掘技术提取高频词，引入点互信息（point-wise mutual information，PMI）指标构建语义网络，通过分析高频词及其关联词，初步构建指标体系。最后，通过专家讨论与评估，进一步细化和完善指标体系。具体指标选取流程如图1所示。

1.2.1 文本材料来源

选取“数据安全韧性”为核心关键词，为了全面了解数据安全韧性，选取多个相近的关键词，如“安全韧性”“工业互联网韧性”“数据安全”等。使用选定的关键词在学术数据库、国家标准数据库、安全白皮书和行业报告等资源中进行检索，在知网进行检索共得到180篇文献。根据相关性原则对文献进行筛选，得到26篇中文核心论文，8份与工业互联网平台数据安全高度相关的国家标准。

1.2.2 文本挖掘

（1）文本清洗。将获得的文本材料转换成word格式，为保障文本的高度准确性，筛选与研究主题相关的材料，将有关工业互联网平台的数据安全、网络安全、工业互联网平台管理、数据安全管理与治理等相关内容分段整理，以行为单位放入excel表格中，共计1 056条数据。

（2）文本分词。其次对文本进行分词，以jieba分词词典作为基础，将“工业互联网”“工业数据”“分类分级”等作为补充词，补充到默认词典中。这有助于聚焦中文语境下的数据安全问题，提高分析的针对性和实用性。

（3）构建停用词词典。文本分词后，句子中会存在大量实际意义不大但是出现频率较高的语料成分，不利于后续的分析。为了提升分词的精确度，减少不必要的计算，本文的停用词表不仅包含常见的中文停用词表，还补充构建停用词词典，将这些词语从文本语料中过滤，优化分析过程精确分析结果。

（4）词频统计。以jieba分词词典作为基础，对文本进行分词后，创建一个字典来存储标准化文本的词频，确定每个词在文本中出现的频率。结果中存在“实现”“相关”“目标”等非相关词汇，词频占比大且分析无意义，对该类词汇进行人工清理。结果显示，词频最高的两个词是“数据”和“安全”，词频分别为2 840和1 623，说明研究选择的文本材料与研究的主题高度相关。

1.3 语义网络分析

在获得高频词之后，虽然已知材料与“数据”

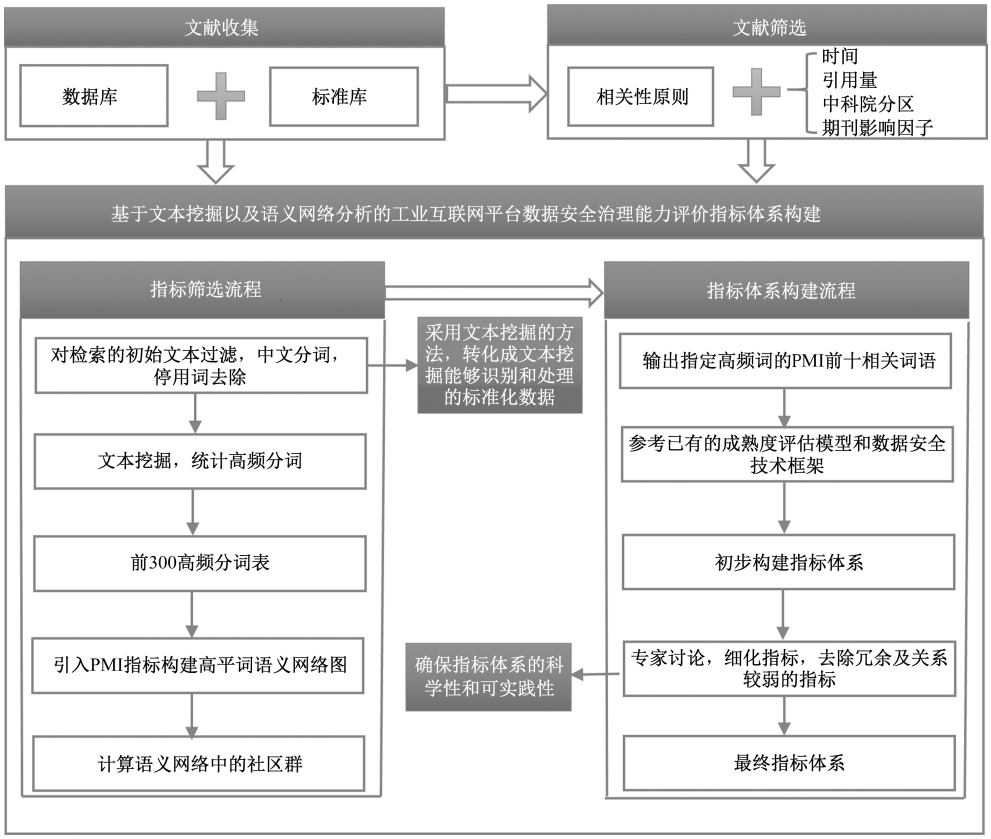

图 1　指标选取流程

“安全”“工业互联网”研究主题高度相关,但单靠高频词而构建指标体系过于主观,因此想进一步获取文本分词之间的联系。对文本材料进行了文本共现网络分析,以了解文本词语之间的关联和聚类关系。文本共现网络分析是一种简单的语义网络,当两个词语同时出现在一个句子中,认为这两个词语存在一条关系。这两个词语共同出现的次数越多,认为这两个词语联系更紧密。这种情况下,存在着无法判断是否有的词语对是偶然共现的,也无法识别有意义的共现,因此引入语义关系计算 PMI。

$$\mathrm{PMI}(W_1 = w_1, W_2 = w_2) = \log_2 \frac{P(w_1, w_2)}{P(w_1)P(w_2)} \tag{1}$$

式中:$P(w_1, w_2)$为两个词语(事件)w_1 和 w_2 共同出现的概率;$P(w_1)$、$P(w_2)$为词语(事件)w_1 和 w_2 单独出现的概率。

依据上文获得的分词结果按照共词分析法构建共词矩阵,并且采用 PMI 统计方法对结果进行优化。在 Python 中调用 Networks 模块生成无向图网络,图的节点为前 300 个高频词,边的权重为两个节点之间的 PMI 值。节点的大小则反映了中心度的值,节点越大,说明该词汇与多个词汇有链接关系,线的粗细则体现了 PMI 统计值的大小。但是由于数据、安全这两个主题词与文本材料高度相关,会产生大量的线导致网络过密,所以去除这两个词生成网络图。根据图的连接关系对节点归类,在模块化设置中,设置解析度为标准解析度 1.0,共生成 8 个社区,由于其中一个社区占比过少只有 0.33% 且词语对整体研究无意义,因此选择过滤该社区,如图 2 所示。

数据安全协同管理社区(21.67%):该社区强调数据安全的综合性,涉及数据管理、供应链管理、隐私保护和风险控制。核心节点如“数据管理”“分类分级”揭示数据处理和决策的关键环节,特别关注数据的全生命周期管理和跨部门协同机制,数据源的获取、数据的隐私与安全保护、数据的有效管理等体现多方参与者在数据安全中的协作。

数据安全应急保障社区(18%):聚焦于对安全事件的应急响应处理的相关内容,语义网络显示,关键数据的备份、安全事件的识别和处理及应急预案的制定和响应能力是保障工业互联网平台数据安全的关键部分。这些要素相互联系,构成数据安全应急管理的完整体系。

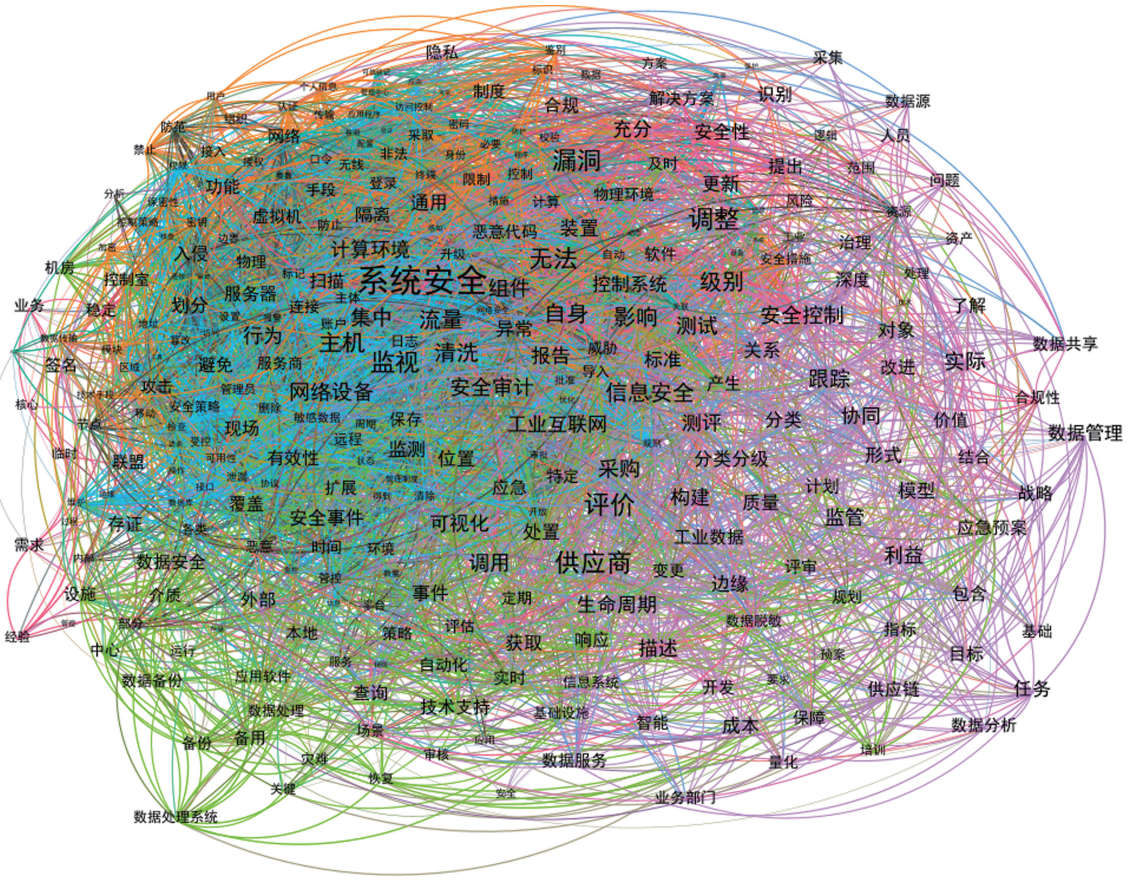

图 2　语义网络结果

数据安全控制策略社区(15%):主要涉及安全控制策略。关键节点涉及“敏感数据”“访问控制”和“数据销毁”,通过管理员权限与审批流程,远程访问和口令保护等这些措施共同构成一个完整且有效的数据保护体系。确保数据分类和权限管理的合规性和有效性,防止权限滥用等。

数据信息安全防护社区(13.33%):“网络”“隔离”“流量”“主机”等词语在同一个社区,这些词反映在工业互联网平台中对网络设备的管理,分别要从流量监控、恶意代码防范、设置隔离边界等方面进行,通过这些策略和技术手段,有效提升安全性和稳定性。

传输安全与身份校验社区(13%):关注数据传输安全和身份认证,核心节点如“数据传输”和“身份认证”揭示了对数据流动的监控与访问控制的重要性。社区强调通过身份鉴别、网络扫描和密钥管理等技术手段确保数据的完整性和个人信息的保护。

数据安全漏洞防护社区(11%):“系统安全”处于网络的中心位置,“漏洞”“计算环境”等节点的连线表明,系统安全需要考虑多个层面的因素,如漏洞修补、计算环境的安全及“数据脱敏”“安全审计”节点的出现体现了数据的处理能力也对工业系统有重要作用。

数据安全风险监控预警社区(7.67%):该社区强调可信验证、报警系统和管理中心的协调。核心节点如“可信验证”和“警报”展示了通过报警和实时监控来应对潜在数据威胁的重要性,确保系统及时发现并响应危险。表明对数据安全威胁的察觉很重要,及时的报警和对危险的防护以确保数据机密性和完整性。

将已获得的高频分词作为指标体系构建的基础,筛选与数据安全韧性高度相关的词汇,利用 Python 定义函数 get_max_pmi(word, n),从现有语义网络中提取与该高频分词 PMI 最高的前 10 个词,并输出相应分词及其 PMI 值。在此基础上,初步构建指标体系,邀请领域专家评审讨论,提出修改意见。结合专家反馈、成熟度评估模型[9,23]及数据安全技术框架,进一步细化和优化指标,确保其适用性和可行性,具体如表 1 所示,并对每个指标进行简单的定义。

表 1　高频分词指标汇总

指标	高频分词(频数)
数据访问监控	访问(323)访问监控(146)
数据安全分析	分析(382)数据分析(99)
数据安全审计	审计(412)安全审计(74)
数据分类分级	分类分级(92)分类(45)
数据脱敏	敏感数据(41)数据脱敏(37)
数据加密	加密(92)密钥(36)
数据销毁	销毁(112)清除(39)
身份与访问管理	访问控制(259)身份(157)验证(102)
数据库防火墙	数据库(36)防火墙(22)
可信验证	可信验证(66)
平台边界安全网关	隔离(456)边界(165)入侵检测(97) 安全网闸(27)
应急响应	应急响应(69)报警(77)响应(75)
安全日志	记录(271)日志(71)
物理环境安全	环境(140)物理(126)
数据安全问题溯源	问题溯源(158)问题追踪(78)
数据备份恢复	恢复(268)备份(196)数据备份(91)
数据风险应急预案	应急(79)应急预案(30)

1.4　数据安全韧性指标定义

数据访问监控指通过可视化手段实时监测工业设备和生产过程中的数据安全状况;数据安全分析用于识别平台潜在风险与漏洞,保障数据的机密性、完整性和可用性;数据安全审计则通过收集和分析安全日志,追踪数据操作,确保合规性,避免违规引发法律与财务风险。

数据分类分级根据安全需求和法律法规,对生成和收集的数据进行标识,并采取相应的安全措施;数据脱敏对敏感数据进行处理,降低敏感性,保护个人信息在使用和共享中的隐私;数据加密通过生成密钥、执行加密算法,对平台各层面数据进行加密,确保安全存储和传输;数据销毁通过物理破坏或逻辑删除彻底清除数据,防止其被恢复。

身份与访问管理通过唯一标识和鉴别用户身份,分配账户与权限,并建立验证与授权机制,确保权限匹配和定期更新。数据库防火墙位于服务器与网络之间,通过监控、过滤和验证流量,确保仅授权用户或系统可访问和修改数据。平台边界安全网关作为网络边界的防护点,阻止恶意攻击与未授权访问,提供安全接口,确保数据流通安全。应急响应体系及时发现并隔离安全事件,迅速采取应对措施。安全日志记录关键操作、访问和活动,用于追踪和审计用户行为、系统和安全事件。可信验证依托可信根机制,结合动态监控与审计功能,确保数据环境持续可信。物理环境安全通过保护平台物理资源,防范火灾、盗窃和自然灾害等外部威胁,保障设备安全。

数据安全问题溯源通过追踪和分析数据安全事件的发生过程,找出问题根源。数据备份恢复通过定期创建数据副本并存储在可靠介质中,以便在数据丢失或损坏时迅速恢复。数据风险应急预案确保在风险发生时,能够快速恢复数据和业务功能,并明确规划工作内容与步骤,确保责任落实到人。

1.5　数据安全韧性评价体系构建

根据文本挖掘得到的高频分词,再结合数据安全韧性要求,确定四项一级指标,分别为数据监控能力、数据处理能力、数据防护能力、数据恢复能力。数据监控能力旨在反映工业互联网平台在事故发生前的管理、监测、预测和预警方面的能力;数据处理能力和数据防护能力反映平台在数据事故发生后的响应、决策和协调能力;数据恢复能力反映平台在事故发生后,恢复数据并进行反馈的能力具体如图 3 所示。需要指出的是,由于平台内部的强耦合性,韧性指标会与多个能力相关联。

2　指标综合权重的确定

2.1　G1 法

G1 法是王学军和郭亚军[24]提出的一种基于层次分析法优化衍生出的改进主观赋权法[25]。该方

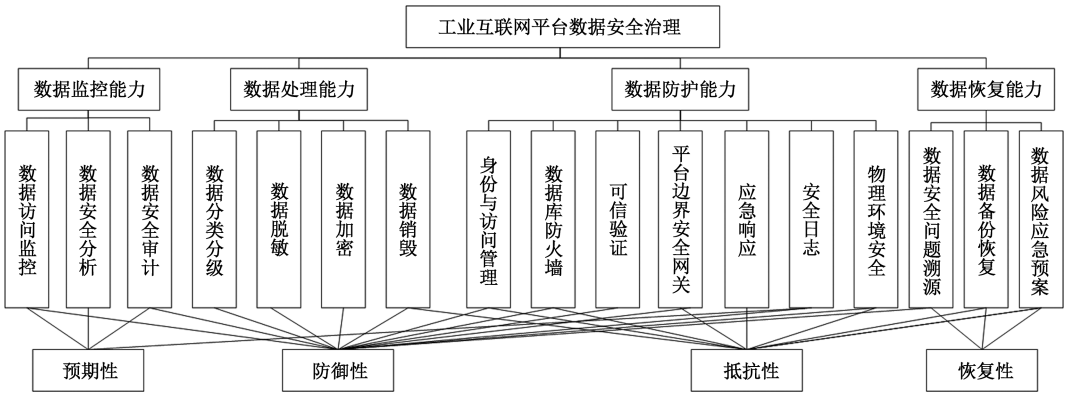

图 3　工业互联网平台数据治理韧性评价指标体系

法适用于评价指标体系具有随机性、模糊性且指标个数较多的决策分析过程，可简单高效地确定指标独立权重，且无须构建重要性判断矩阵，解决了需要通过一致性检验的难题。首先由领域内经验丰富的专家，根据重要程度确定工业互联网平台数据安全韧性评价指标序关系。其次，确定各指标的相对重要程度 r_k，r_k 为 X_{k-1}^* 与 X_k^* 重要程度比值，w_k 代表第 k 个指标的权重。最后依据专家的赋权情况，计算第 k 个指标的权重，并根据公式(2)计算各指标的 G1 权重。

$$\begin{cases} w_k = \left(1 + \sum_{k=2}^{n} \prod_{i=k}^{n} r_i\right)^{-1} \\ w_{k-1} = r_k w_k,\ k = n, n-2, \cdots, 3, 2 \end{cases} \tag{2}$$

式中：r_k 为韧性指标重要程度比值。

2.2　DEMATEL 法

决策实验分析法，简称 DEMATEL 法，是一种分析复杂因素间关联关系的方法[26]。基于图论和矩阵系统，不仅可以识别韧性指标之间的相互影响关系，明确各指标的中心度和原因度，以此计算韧性指标的权重具体步骤如下。

首先，建立初始直接影响矩阵，根据前文提出的“工业互联网平台数据安全韧性指标体系”，进行问卷设计和数据收集。邀请专家对韧性指标间的相互影响程度打分，0～4 的分值表示“无影响”“影响小”“影响适中”“影响大”“影响极大”。对所有专家的评分进行算术平均处理后得出初始直接影响矩阵 $\boldsymbol{A} = (a_{ij})_{n\times n}$。其次，规范化直接影响矩阵可得到标准化直接影响矩阵 $\boldsymbol{B}$。随后，构建综合影响矩阵 $\boldsymbol{T} = (t_{ij})_{n\times n} = \lim_{h\to\infty}(\boldsymbol{B} + \boldsymbol{B}^2 + \cdots + \boldsymbol{B}^n)$。同时可以根据综合影响矩阵 $\boldsymbol{T}$ 中每行之和以及每列之和计算各指标的中心度 M_i 和原因度 R_i。最后根据公式 $w_i = \dfrac{M_i}{\sum_{i=1}^{n} M_i}$ 计算各指标权重，$w_i \in (0,1)$。

2.3　计算混合赋权

邀请多位工业互联网领域具有丰富数据安全管理经验的学者和专家，首先对工业互联网平台数据安全韧性指标的独立重要性进行客观判断，根据意见结合 G1 赋权法确定韧性指标的独立权重。接着引入 DEMATEL 法求出其关联权重。最后将 DEMATEL 关联权重 w_i 与 G1 法所得指标独立权重 w_k 根据公式 $Z_i = \dfrac{W_{A_i} W_{D_i}}{\sum_{i=1}^{n} W_{A_i} W_{D_i}}$ 进行复合，得到工业互联网平台数据安全韧性评价体系指标混合权重 Z_i。如表 2 所示。

表 2　韧性指标权重

指标	W_A	W_D	M_i	Z_i
A_1	0.066	0.058 8	15.02	0.067
A_2	0.079	0.059 8	15.28	0.081
A_3	0.066	0.061 5	15.73	0.069
B_1	0.075	0.063 3	16.19	0.081
B_2	0.061	0.052 7	13.47	0.054
B_3	0.082	0.059 0	15.07	0.083
B_4	0.057	0.049 8	12.73	0.049
C_1	0.048	0.058 5	14.96	0.045
C_2	0.054	0.060 7	15.52	0.056
C_3	0.043	0.058 3	14.92	0.042
C_4	0.051	0.061 1	15.61	0.052
C_5	0.059	0.059 0	15.08	0.060
C_6	0.032	0.061 9	15.82	0.034
C_7	0.032	0.055 8	14.26	0.030
D_1	0.064	0.058 6	14.99	0.062
D_2	0.066	0.057 3	14.66	0.063
D_3	0.065	0.064 0	16.37	0.070

3　基于云模型的评价指标体系应用案例

3.1　云模型

云模型能够有效实现定性与定量相互转换的工具。其核心特点在于将模糊性与随机性有机结合，既能够反映定性描述中的随机性，又能够捕捉样本的不确定性[27-28]。近年来，云模型评价法被应用到管理领域。李君等[29]构建了基于成熟度的生产设备数字化管理能力评价研究，运用云模型实现生产设备数字化管理能力评价。田红娜和孙钦琦[30]构建汽车制造企业绿色技术创新能力评价指标体系，建立综合评价云模型并判断是否为最终的评价云模型。

云的数字特征可以用期望 Ex、熵 En、超熵 He 来表示，其中，Ex 为反映论域空间的中心值，最能够代表定性概念的点[29]；期望 Ex 在本文中表示专家对工业互联网平台数据安全韧性水平的评价，期望越高表示对该平台的数据安全韧性水平越认可；熵 En，评价对象的随机性和模糊性均体现在熵的数值上，熵的“广度”表示概念定量化的随机性。云滴的范围越广云图越宽，熵越大。超熵 He，是熵不确定的表现，表示熵的随机性和模糊性。体现在云层的“厚度”，“云层”越厚则表示超熵越大。本文基于韧性视角构建了数据安全评价体系，通过云发生器将定性指标量化，并应用于对 YQ 工业互联网平台的综合评价。

3.2 YQ工业互联网平台数据安全韧性评价流程

YQ供应链管理有限公司的YQ工业互联网平台是全球首个专注钢板切割个性化定制的工业互联网平台,依托云计算、大数据、5G等技术,整合产业链上下游,优化供应链透明度、数据协同、智能制造和绿色发展,推动中小微企业数字化转型。为应对技术升级需求,平台加快构建高效的数据采集体系,强化设备接入与应用开发。面对用户增长和数据复杂度提升,平台的数据安全管理评价与优化升级具有紧迫性,采用云模型进行数据安全韧性评价具备重要的代表性与可行性。

基于构建的工业互联网平台数据安全韧性指标体系,结合云切工业互联网平台的数据安全实际情况进行赋分,分值区间为[0,100],利用逆向云发生器计算各指标的云数字参数,结合指标组合赋权值进行计算工业互联网平台数据安全韧性的综合云计算,利用正向云发生器生成韧性综合评价云图,并将其与韧性标准评价云进行相似度对比,得到最终综合韧性评价等级。

标准评价云是韧性评价的基准参照图,令评语集对应的论域为[0,100],评语集里每一个评语对应一个论域的区间。本文将评语集划分为5个,即$C=\{$韧性不足,低韧性,中韧性,较高韧性,高韧性$\}$,各评语对应变化对于中间区间选择双边约束$[N_i^{\min},N_i^{\max}]$,端点选择半边云模型进行,表示该区间对应的云特征为$(\mathrm{Ex}_i,\mathrm{En}_i,\mathrm{He}_i)$,如表3所示。

综合10位专家的评价结果,利用逆向云发器计算各指标云数字特征,计算结果如表4所示。

由计算结果可以看出,大部分指标得期望Ex平均值达到了80分左右,根据工业互联网数据安全韧性水平等级划分,大部分评价结果处于良好阶段,但是数据安全分析、数据安全审计、身份与访问监控、可信验证期望值较低,影响了YQ工业互联网平台的数据安全韧性水平。由三级指标的云参数以及权重按照综合云计算规则,利用MATLAB进行计算,可以得到一级指标的云参数各准则层指标的期望75分以上,说明准则层指标的数据安全水平均为良好,将准则层的评价结果以云图的形式展现如图4(a)~图4(d)所示。

表3 评语

评语集	韧性不足	低韧性	中韧性	较高韧性	高韧性
区间	[0,40]	(40,60]	(60,80]	(80,90]	(90,100]
云参数	(20,16.9,0.8)	(50,8.49,0.8)	(70,8.49,0.8)	(85,4.25,0.8)	(95,4.25,0.8)

表4 韧性指标云数字特征值

一级指标	一级指标云特征值	二级指标	二级指标云特征值
A	(79.29,0.49,0.55)	A_1	(90.4,2.47,1.30)
		A_2	(74.4,5.62,1.89)
		A_3	(68.7,4.83,2.04)
B	(83.15,1.31,2.45)	B_1	(81.4,6.37,4.76)
		B_2	(81.9,6.34,0.73)
		B_3	(84.5,9.60,0.71)
		B_4	(82.9,7.55,4.15)
C	(84.20,0.98,1.22)	C_1	(74.9,6.99,2.81)
		C_2	(86.8,7.06,2.12)
		C_3	(77,9.81,0.76)
		C_4	(81.8,8.34,1.89)
		C_5	(87.7,2.42,0.91)
		C_6	(86.1,8.71,1.99)
		C_7	(81.2,4.2,3.30)
D	(87.23,0.72,1.04)	D_1	(82,10.66,1.026)
		D_2	(90.5,3.90,1.58)
		D_3	(85.6,3.44,0.94)

根据表4所得的二级指标云特征值及权重,结合云模型综合评价的计算公式,可得YQ工业互联网平台数据安全韧性综合评价云特征值为(82,8.7,2.3),如图4(e)所示。云滴比较密集,说明韧性评价结果稳定。计算综合评价云相似度,根据最大相似度原则,判定韧性等级为"较高韧性,微偏向中韧性"。该评价结果与调研情况相符,表明评价模型具有良好的可靠性与适用性。

4 结论

提升工业互联网平台数据安全韧性是推动数字经济时代工业互联网快速发展的必然路径。本文通过梳理国内外研究现状,深入分析工业互联网及其安全韧性的内涵与发展,利用文本挖掘和语义网络模型构建数据安全韧性评价指标体系,并通过云模型进行检验,旨在为工业互联网中数据治理标准体系研究提供理论支持的同时,为工业互联网平台安全运营提供保障。

在实际运用中,工业互联网平台应该制定综合的数据安全策略,建立完善的数据安全标准体系,包括技术、流程和管理等方面。通过制定统一的数据标准,打破数据孤岛,提高数据互通性。同时加强人员培训,提供定期的安全培训和教育,激励员工参与到数据安全管理中,鼓励他们报告安全漏洞和提出改进建议。企业需要持续监控更新安全措施,安全工作不是一次性的,及时发现和应对潜在的安全威胁,保持安全措施的有效性。工业互联网平台企业可以通过加强与其他企业的合作与共享打破数据孤岛,共同应对安全挑战,推动整个生态系统的安全发展。

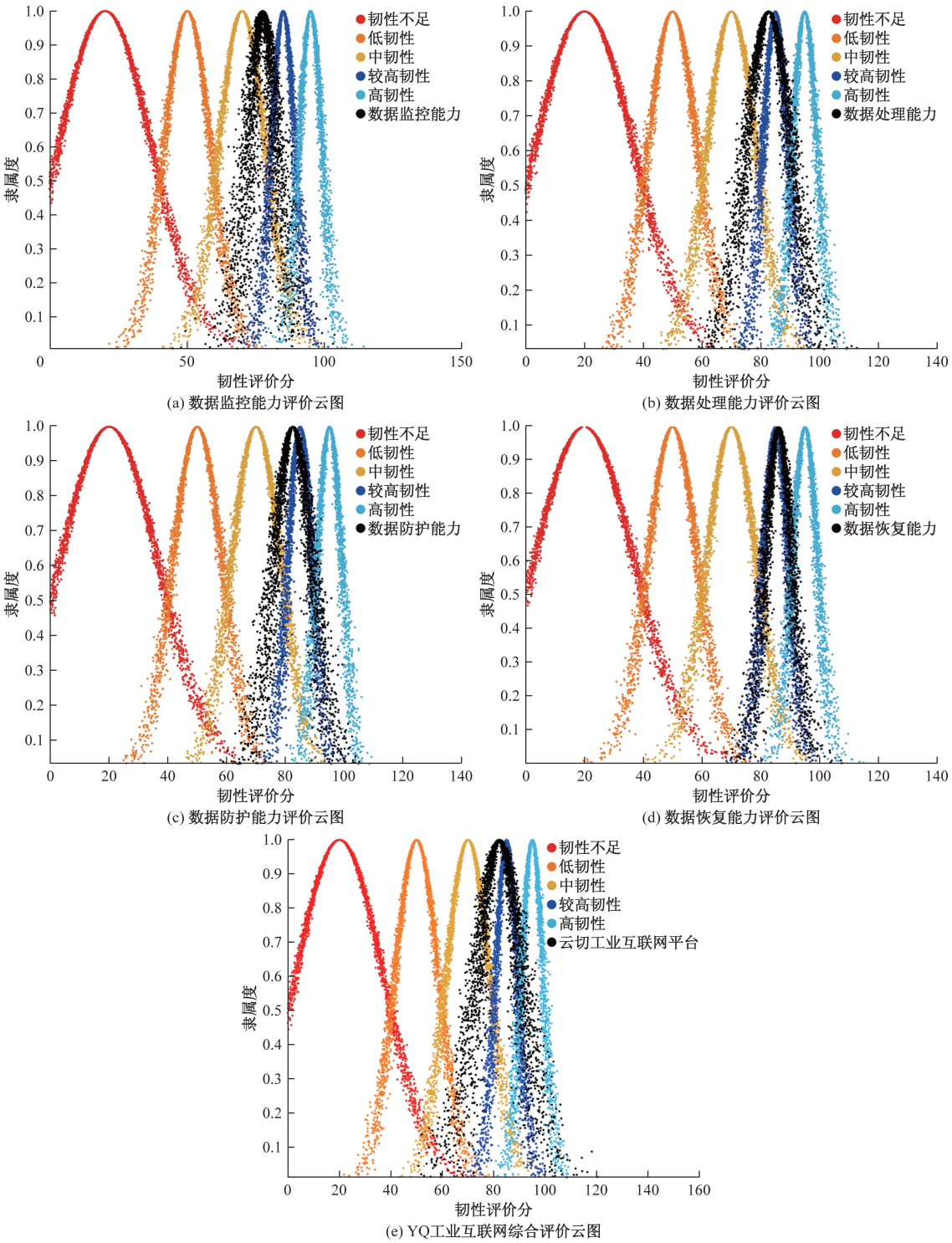

图 4　准则层云图及综合评价云图

参考文献

[1] 杨晨，马瑞成，王雨石，等. 深度学习与工业互联网安全：应用与挑战[J]. 中国工程科学，2021，23(2)：95-103.

[2] 樊佩茹，王冲华. 数据安全视角下工业互联网平台的攻击与防护[J]. 网络空间安全，2020，11(2)：75-80.

[3] MENON K，KÄRKKÄINEN H，LASRADO L. Towards a maturity modeling approach for the implementation of industrial internet[C]//Proceeding of the 20th Pacific Asia conference on information systems (PACIS 2016). Taiwan，China：Association for Information Systems(AIS)，2016：38.

[4] MENON K，KÄRKKÄINEN H，WUEST T. Role of openness in industrial internet platform providers' strategy[C]//Product Lifecycle Management and the Industry of the Future：14th IFIP WG 5.1 International Confer-

ence. Seville, Spain: Springer International Publishing, 2017: 92-105.
[5] USLÄNDER T. Agile service-oriented analysis and design of industrial internet applications[J]. Procedia CIRP, 2016, 57: 219-223.
[6] SZYMANSKI T H. Supporting consumer services in a deterministic industrial internet core network[J]. IEEE Communications Magazine, 2016, 54(6): 110-117.
[7] 李君, 邱君降, 窦克勤. 工业互联网平台参考架构、核心功能与应用价值研究[J]. 制造业自动化, 2018, 40(6): 103-106.
[8] 邱君降, 李君, 成雨, 等. 制造业与互联网融合背景下工业设备"上云"的现状、问题与路径研究[J]. 制造业自动化, 2018, 40(10): 37-41.
[9] 李君, 邱君降, 窦克勤, 等. 基于成熟度视角的工业互联网平台评价研究[J]. 科技管理研究, 2019, 39(2): 43-47.
[10] 李君, 邱君降, 柳杨, 等. 工业互联网平台评价指标体系构建与应用研究[J]. 中国科技论坛, 2018(12): 70-86.
[11] 工信部. 加强工业互联网安全工作的指导意见[J]. 机械工业标准化与质量, 2019(10): 7-9.
[12] KLEIN R J T, NICHOLLS R J, THOMALLA F. Resilience to natural hazards: how useful is this concept [J]. Environmental Hazards, 2004, 5(1): 35-45.
[13] HOLLING C S. Resilience and stability of ecological systems[J]. Annual Review of Ecology and Systematics, 1973(4): 1-23.
[14] ADGER W N, HUGHES T P, FOLKE C, et al. Social-ecological resilience to coastal disasters[J]. Science, 2005, 309: 1036-1039.
[15] 李平, 竺家哲. 组织韧性: 最新文献评述[J]. 外国经济与管理, 2021, 43(3): 25-41.
[16] 范维澄. 构建智慧韧性城市的思考与建议[J]. 中国建设信息化, 2015(21): 20-21.
[17] 黄浪, 吴超, 王秉. 系统安全韧性的塑造与评估建模[J]. 中国安全生产科学技术, 2016, 12(12): 15-21.
[18] 黄浪, 吴超, 杨冕, 等. 韧性理论在安全科学领域中的应用[J]. 中国安全科学学报, 2017, 27(3): 1-6.
[19] 罗通元. 安全韧性学基本概念和理论体系探讨[J]. 安全与环境学报, 2022, 22(1): 280-291.
[20] 邹纯龙, 马海群, 王今. 公共数据安全韧性治理体系的系统动力学分析[J]. 图书情报工作, 2024(3): 3-14.
[21] 马飞, 苟慧艳, 杨梦楠, 等. 考虑灰色攻击的多制式区域轨道交通网络韧性评估[J]. 中国安全科学学报, 2023, 33(12): 148-159.
[22] 宋亮亮, 张劲松, 杜建波, 等. 基于组合赋权和云模型的水利工程运行安全韧性评价[J]. 水资源保护, 2023, 39(2): 208-214.
[23] 国家信息安全标准化委员会. 信息安全技术 数据安全能力成熟度模型: GB/T 37988—2019[S]. 北京: 中国标准化出版社, 2019.
[24] 王学军, 郭亚军. 基于G1法的判断矩阵的一致性分析[J]. 中国管理科学, 2006(3): 65-70.
[25] 陈陌, 郭亚军, 于振明. 改进型序关系分析法及其应用[J]. 系统管理学报, 2011, 20(3): 352-355.
[26] 王伟明, 邓潇, 徐海燕. 基于三维密度算子的群体DEMATEL指标权重确定方法[J]. 中国管理科学, 2021, 29(12): 179-190.
[27] 王肖鑫, 岑威钧, 晏成明, 等. 基于改进赋权的山区堤防安全云模型评价方法[J]. 水利水电科技进展, 2022, 42(5): 58-63.
[28] 陈义安, 王斯, 杨澈洲. 基于云模型的乡村振兴战略实施效果综合评价[J]. 重庆社会科学, 2022(11): 53-66.
[29] 李君, 窦克勤, 周勇, 等. 基于成熟度视角的生产设备数字化管理能力评价研究[J]. 科技管理研究, 2023, 43(2): 57-64.
[30] 田红娜, 孙钦琦. 基于云模型的汽车制造企业绿色技术创新能力评价研究[J]. 管理评论, 2020, 32(2): 102-114.
[31] 沈进昌, 杜树新, 罗祎, 等. 基于云模型的模糊综合评价方法及应用[J]. 模糊系统与数学, 2012, 26(6): 115-123.

Research on the Construction of Data Security Resilience Evaluation Indicator System for Industrial Internet Platforms

LU Jingyu, YANG Wei

(School of Management, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: Data security is critical for the healthy development of industrial internet platforms. To scientifically quantify the data security level of these platforms, resilience theory was introduced. Based on the understanding of resilience in the field of system security, the concept of data security resilience for industrial internet platforms was proposed, which included four dimensions, such as risk anticipation, defense, resistance and recovery. Building on this, a data security evaluation index system for industrial internet platforms from a resilience perspective was developed using text mining and semantic network analysis. The G1 method was applied to determine the independent weights of resilience indicators, while the DEMATEL method was used to quantify the interrelationships among these indicators, resulting in hybrid weights. Furthermore, a cloud model-based evaluation model for data security resilience of industrial internet platforms is proposed. This model is applied to assess the data security resilience of the YQ industrial internet platform, with the results aligning with actual conditions, thus validating the scientific and rational basis of the hybrid-weighted and cloud model-based evaluation method. Finally, recommendations are made for the future development of data security resilience in industrial internet platforms, providing theoretical support for enhancing data security resilience moving forward.

Keywords: industrial internet platforms; resilience; data security