Computer Science and Application 计算机科学与应用, 2026, 16(6), 321-331
Published Online June 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.166231

Hans汉斯

面向数据出境的多维融合动态评估模型与高效计算技术

段金典，贾　丹，李文婷*，杨晓伟，张明岩，周子钰

国家工业信息安全发展研究中心，北京

收稿日期：2026年5月18日；录用日期：2026年6月22日；发布日期：2026年6月30日

摘　要

在数据跨境流动日趋频繁的现实背景下，敏感数据出境安全已成为维护国家安全、公共利益与个人信息合法权益的关键环节。当前主流的数据出境风险评估方法多依赖静态指标体系与线性加权模型，存在风险要素耦合刻画不足、动态适配能力较弱、大规模场景下计算效率偏低等问题，难以满足金融、医疗、交通、工业等重点行业对风险精准量化、实时研判的实际需求。本文面向敏感数据出境全生命周期风险管控需求，提出一种多维融合动态评估模型。该模型构建覆盖数据敏感性、出境必要性、传输安全、主体管理能力与境外接收方保障水平的多维度风险指标体系，通过自注意力机制实现风险指标权重的动态分配，引入非线性耦合函数刻画多要素间风险叠加与传导效应，并依托在线学习实现模型参数的自适应更新。本文首次将自注意力机制与非线性耦合函数结合用于数据出境风险的动态量化评估，该模型能够更好地适应敏感数据出境风险的动态演变特征，具备良好的场景适应性与计算高效性，可以为机构数据出境合规自查和风险监测提供技术支持。

关键词

数据出境，风险量化评估，多维信息融合，非线性耦合，高效计算

A Multidimensional Fusion Dynamic Evaluation Model and Efficient Computing Technology for Data Cross-Border Transfer

Jindian Duan, Dan Jia, Wenting Li*, Xiaowei Yang, Mingyan Zhang, Ziyu Zhou

China Industrial Control Systems Cyber Emergency Response Team, Beijing

Received: May 18, 2026; accepted: June 22, 2026; published: June 30, 2026

*通讯作者。

文章引用: 段金典, 贾丹, 李文婷, 杨晓伟, 张明岩, 周子钰. 面向数据出境的多维融合动态评估模型与高效计算技术[J]. 计算机科学与应用, 2026, 16(6): 321-331. DOI: 10.12677/csa.2026.166231

Abstract

Against the backdrop of increasingly frequent cross-border data flows, the security of sensitive data outbound transfer has become a critical link in safeguarding national security, public interests and the legitimate rights and interests of personal information. Most mainstream risk assessment methodologies for data outbound transfer currently rely on static indicator systems and linear weighting models. Such approaches suffer from insufficient depiction of the coupling between risk factors, weak dynamic adaptability, and low computational efficiency in large-scale scenarios, making them unable to meet the practical demands of key sectors including finance, healthcare, transportation and industry for accurate risk quantification and real-time risk analysis. Targeting the full-lifecycle risk control requirements for sensitive data outbound transfer, this paper proposes a multi-dimensional integrated dynamic assessment model. The model establishes a multi-dimensional risk indicator system covering data sensitivity, necessity of outbound transfer, transmission security, management capacity of data controllers, and the protection standard of overseas data recipients. It leverages the self-attention mechanism to dynamically assign weights to risk indicators, introduces a nonlinear coupling function to characterize the risk superposition and transmission effects among multiple factors, and realizes adaptive updates of model parameters via online learning. This paper innovatively combines the self-attention mechanism and nonlinear coupling function for the dynamic quantitative assessment of data outbound transfer risks for the first time. Capable of better adapting to the dynamic evolution characteristics of sensitive data outbound risks, the proposed model boasts favorable scenario adaptability and high computational efficiency. It can provide technical support for organizations to conduct compliance self-inspections and risk monitoring of cross-border data transfers.

Keywords

Data Outbound Transfer, Risk Quantitative Assessment, Multi-Dimensional Information Fusion, Nonlinear Coupling, Efficient Computing

1. 引言

在数字经济全球化快速发展的背景下，数据跨境流动已成为跨国企业运营、国际科研合作及跨境服务贸易的重要基础。我国的金融、医疗、交通、电信、智能制造等领域在开展境外业务过程中，常常涉及个人敏感信息、重要数据等的出境行为[1]，带来的安全风险也日益突出，数据泄露、非法滥用、境外调取等安全事件时有发生，不仅可能导致企业经济损失和声誉损害，还可能对国家安全、社会公共利益和个人信息权益构成严重威胁[2]。为规范数据出境活动、严守安全底线，我国颁布了《中华人民共和国网络安全法》[1]《中华人民共和国数据安全法》[2]《中华人民共和国个人信息保护法》[3]《促进和规范数据跨境流动规定》[4]等法律法规，明确规定重要数据处理者、关键信息基础设施运营者等主体在向境外提供数据时，必须依法开展安全评估，以识别、研判并有效控制数据出境的安全风险[3]。

[1]https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm
[2]https://flk.npc.gov.cn/detail?id=021e7d7684474107b8f3febbb1c4f8b5
[3]https://flk.npc.gov.cn/detail?id=ff8081817b6472a3017b656cc2040044
[4]https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm

在政策驱动与现实需求的双重推动下，数据出境风险评估逐渐成为网络空间安全领域的研究热点。然而在实际应用中，现有评估方法仍存在多方面局限性。一是现有评估体系呈现静态化特征，指标选取及其权重设定多依赖专家预先界定，无法灵活适配业务场景更迭、接收方安全状态波动、数据敏感级别调整等各类动态情形，进而导致评估结果与实际风险变化存在滞后性。二是风险融合手段较为单一，多数评估模型采用线性加权求和方式计算综合风险，未能考虑不同风险要素之间可能存在的相互激发、叠加放大及链式传导等非线性耦合效应，使得评估结果易出现保守化倾向或精准度不足的问题。三是动态评估水平有待提升，部分模型虽引入权重调整机制，却缺乏对风险演化规律的持续学习能力，无法达成真正意义上的动态研判目标。四是工程化应用效率偏低，面对高并发、大批量、高频次的数据出境场景时，复杂评估模型普遍存在计算延迟较高、资源占用量大、响应速度迟缓等问题，难以适配实时监测与在线评估的实际应用需求。

针对上述问题，本文围绕敏感数据出境风险的多维性[4]、耦合性与动态性特征[5]，开展多维融合动态评估模型与高效计算技术的研究。在指标体系方面，构建覆盖数据自身、业务场景、传输过程、主体管理及境外接收方的统一框架，并支持面向典型行业的灵活扩展。在风险建模方面，引入自注意力机制实现权重动态分配，构建非线性耦合融合模型以提高风险刻画的准确性。在动态更新方面，采用在线学习方式实现参数的增量调整，使得评估结果能够实时反映风险态势的演变。在计算效率方面，借助轻量化结构、流式处理与缓存优化策略提升推理性能，从而增强模型在真实场景中的可用性。

2. 相关理论与技术基础

2.1. 信息安全和数据安全的风险评估技术

针对信息安全和数据安全的风险评估，旨在识别、评估和管理信息系统面临的各种风险[6]。它通过全面分析组织的信息系统、数据流程、安全措施和相关威胁，确定风险的概率和影响，并提供有针对性的控制措施和解决方案。信息与数据安全风险评估不仅是组织信息安全管理的必要手段，也是实现信息化发展的根本保障。针对信息安全和数据安全进行风险评估需要全面考虑风险的类型、来源以及应对措施等多个因素，并根据具体场景进行分类评估，如企业网络安全评估[7]、云环境安全评估[8]以及移动应用安全评估[9] [10]等。

国际标准化组织发布了 ISO/IEC 27005《信息技术 安全技术 信息安全风险管理》[5]，提供开展有效风险管理的框架指南，具体过程如图 1 所示。美国国家标准与技术研究所(NIST, National Institute of Standards and Technology)发布的 NIST SP 800-30《风险评估实施指南》[6]，给出的信息安全风险评估过程包括准备风险评估、进行风险评估、维护风险评估三个过程，包括风险评估、风险处理、风险监控和风险沟通等方面，被广泛用于公共部门和商业组织中。

表 1 中汇总了风险评估过程涉及的所有任务。美国能源部网络安全、能源安全和应急响应办公室、电力分部门协调委员会等部门开发了网络安全能力成熟度模型(C2M2, Cybersecurity Capability Maturity Model)，基于多个关键维度，即：战略规划和管理、风险管理、控制和协调等，提供了组织网络安全风险管理的综合视图。Open FAIR (Factor Analysis of Information Risk)基于科学、透明和标准化原则开发了 FAIR 方法，以帮助组织通过标准化方法评估、分析和处理信息安全风险，该方法被广泛应用于企业和政府机构中。卡内基梅隆大学开发的 OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)是一种基于风险的战略评估和规划技术，它由操作风险和安全实践驱动，使用三个阶段、子过程和任务

[5]https://std.samr.gov.cn/gb/search/gbDetailed?id=71F772D80651D3A7E05397BE0A0AB82A
[6]https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

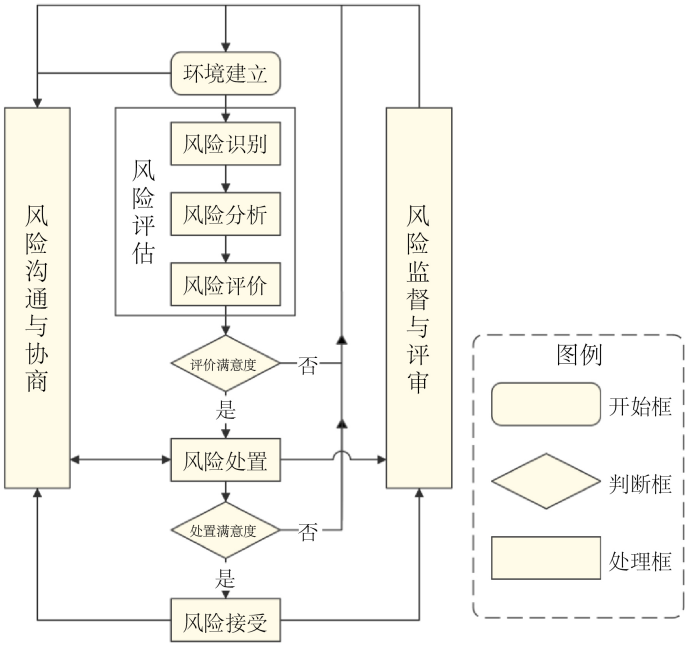

Figure 1. Risk assessment process
图 1. 风险评估过程

Table 1. Risk assessment process
表 1. 风险评估过程

步骤	任务	任务描述
第一步：准备风险评估	识别目的	从评估将产生的信息和评估将支持的决策的角度来看，识别风险评估的目的
	识别范围	从组织的适用性、支持的时间框架，以及体系架构、技术等方面的考虑出发圙识别风险评估的范围
	识别假设条件和约束	识别进行风险评估的特定假设条件和约束
	识别信息来源	识别风险评估中使用的威胁、脆弱性和影响信息的来源
	完善风险模型	定义或完善风险评估所用的风险模型
第二步：进行风险评估	识别威胁源	识别组织相关的威胁源，并描述其特征，包括威胁的性质和对抗性威胁、能力、意图和目标特点的
	识别威胁事件	识别潜在的威胁事件，与组织的相关性，以及可能启动该事件的威胁源
	识别脆弱性和假设条件	识别对组织产生负面影响的威胁事件的可能性的脆弱性和诱发条件
	确定可能性	确定对组织产生负面影响的威胁事件的可能性
	确定影响	确定所关注的威胁事件对组织产生的负面影响，要考虑可能驱动改时间的威胁源的特征；已识别的脆弱性和诱发条件；反映阻碍这类事件的已计划或已实施的防护措施
	确定风险	确定所关注的威胁源对组织造成的风险，要考虑：该事件造成的影响；事件发生的可能性
第三步：维护风险评估	监视风险因素	持续监视可能对组织运行和资产、个人、其他组织或国家造成风险变化的因素
	更新风险评估	使用持续监视风险因素的结果，更新现有的风险评估

活动来构建组织信息安全需求的全面图景[11]。欧盟开发的 CORAS (Construct a platform for Risk Analysis of Security Critical Systems)是一个基于模型的安全关键系统风险评估框架，使用统一建模语言(UML, Unified Modeling Language)图来表示用户和工作环境之间的关系和依赖关系，决策的最终结果基于涉及每个资产的 UML 类图[12]。Karabacak 和 Sogukpinar 开发了基于调查的 ISRAM (Information Security Risk Analysis Method)，ISRAM 采用 7 步流程以确定每个安全漏洞的可能性和后果[13]。然而，ISRAM 的 7 步流程需要广泛的准备，数学公式复杂，难度较大[14]。其他知名的信息安全风险评估模型框架还包括 SANS (SysAdmin、Audit、Network、Security)开发的 RMMM (Risk Management Maturity Model)框架、CIS (Center for Internet Security)开发的 CIS Controls 框架、信息系统审计与控制协会(ISACA, Information System Audit and Control Association)开发的 COBIT (Control Objectives for Information and Related Technology)框架等此外，信息安全咨询公司与服务提供商，如 Deloitte、KPMG、IBM 等，也积极致力于提供各种安全咨询服务与评估方法，协助企业与组织制定定制化的安全防御策略。

2.2. 数据出境风险评估模型

数据出境风险评估已从早期合规核查逐步转向量化与动态化方向。早期研究多依托静态指标体系与 AHP、模糊综合评价等方法，完成出境场景的合规判定与风险分级，但普遍依赖人工设定权重，难以适配接收方状态、传输链路、数据敏感等级等动态变化，评估结果存在滞后性与保守性问题。近年来，学界开始引入动态评估思路，部分文献采用滑动窗口、变权理论、贝叶斯网络等实现权重自适应更新，一定程度提升了动态性，但仍以线性加权为主，对风险叠加、传导、放大等非线性耦合效应刻画不足。

2.3. 风险评估综合分析模型

不确定性信息的量化分析技术在数据安全风险评估中的应用具有重要意义，它们往往综合使用，并需要结合 AHP、ANP 和贝叶斯分析技术，建立起数据安全风险评估综合分析模型，进一步提高评估的精度和准确性。文献[15]提出了模糊集与熵混合方法提供了更准确的故障项风险排序结果。文献[16]构建了基于模糊评判的资产评估模型和基于 AHP 的脆弱性评估模型。文献[17]提出了采用模糊层次分析法对风险进行量化分析的方法，采用三角模糊数来表示基于群组决策的信息安全风险各因素的判断矩阵，用层次分析法来对专家判断结果进行处理。文献[18]通过威胁分析、梯形模糊数、层次分析法，结合多属性决策理论得到威胁发生的概率、后果属性以及属性值，得到电子政务系统信息安全威胁指数，最后利用威胁指数对风险进行排序，得到系统信息安全的风险等级 AHP 层次分析法。文献[19]提出了一种将模糊集理论与 D-S 证据理论进行结合的风险评估方法。

2.4. 基于神经网络的风险评估模型

通过神经网络进行风险评估是一个发展方向，基于神经网络，研究者能够自动从输入的特征中提取有用的信息和模式，而无需手动进行特征选择和提取。此外，神经网络的非线性模型能够更好地适应复杂的风险评估场景，能够捕捉到特征之间的复杂交互关系。

文献[20]将信息系统的安全保护级别分为五个等级，把模糊数学理论与 BP (Back Propagation)神经网络相结合，建立对信息系统中存在的风险进行评估的方法。文献[21]提出时序自注意力与自适应自回归融合模型，用于金融与生产系统风险预测，在非线性依赖与极端波动场景下表现更优。Relation-aware GCN 与注意力融合机制被用于动态风险分析，能够挖掘异质网络中的关联强度与动态权重。但现有研究存在明显局限：要么用注意力做动态权重但忽略要素间耦合，要么用非线性耦合但依赖固定权重，尚未出现将自注意力机制与非线性耦合函数有机结合、用于数据出境风险动态量化的工作。

2.5. 非线性耦合风险评估

非线性耦合是刻画风险叠加、传导、放大效应的关键手段。多灾害耦合、基础设施安全、工程风险等领域已广泛采用耦合函数、Copula 函数、N-K 模型、系统动力学等方法，证明非线性建模可显著提升评估精度。文献[22]针对多灾害耦合提出高阶拓扑图神经网络，有效刻画系统交互与失效传导；文献[23]针对滨海工程结构建模腐蚀与疲劳的双向耦合，解决传统单向耦合低估风险的问题。然而在数据出境评估中，绝大多数模型仍停留在线性加权，极少考虑组合下的风险激增效应，导致高风险场景预警滞后、量化失真。

2.6. 动态风险评估

在动态风险评估方面，现有研究多通过变权理论、滑动窗口、贝叶斯网络、增量学习等实现权重或状态更新。文献[24]系统梳理了数据出境监测预警技术，指出动态适配与全域协同是核心瓶颈，现有方案普遍缺乏对跨境全链路风险的实时感知与持续更新能力。文献[4]构建数据出境风险要素体系，覆盖数据内容、安全保护、境外环境等维度，但仍采用静态权重与专家排序，未实现动态自适应。

3. 敏感数据出境多维融合动态评估模型

3.1. 模型总体架构

本文提出的敏感数据出境多维融合动态评估模型整体分为五层结构，分别为风险指标体系层、特征标准化层、多维融合计算层、动态自适应层和评估输出层。指标体系层提供统一且可扩展的风险指标框架，覆盖数据、业务、传输、主体、接收方五大维度；特征标准化层对定量与定性指标进行归一化映射，消除量纲差异，保证计算一致性；多维融合计算层利用自注意力机制分配动态权重，并通过非线性耦合函数实现多要素风险综合聚合；动态自适应层基于在线学习实现权重与耦合系数的增量更新，使模型具备持续演进能力；评估输出层输出量化风险值并划分风险等级，同时支持结果缓存与高效查询。模型以风险要素变化为驱动，以非线性融合为核心，以动态更新为增强手段，整体形成闭环式评估机制。

3.2. 多维风险指标体系构建

多维信息融合是一种将多源、异构、跨维度信息进行统一表示、关联分析与综合决策的技术体系，可按照融合层次分为数据层融合、特征层融合与决策层融合。数据层融合直接对原始信息进行处理，保留了较完整的信息，但易受噪声干扰且计算开销较大；决策层融合则在各维度独立决策后对结果进行聚合，灵活性较高，但可能丢失中间关联信息；特征层融合在提取各维度关键特征的基础上进行统一计算，在信息完整性、抗干扰能力与计算效率之间具有较好的平衡，适合用于复杂风险评估场景。

为全面覆盖敏感数据出境风险来源，本文构建包含多级指标的评估体系，分别为出境数据敏感性、出境必要性、传输安全水平、主体管理能力以及境外接收方保障能力。在一级指标下进一步细化多级可量化二级指标，涵盖数据级别、敏感字段占比、业务匹配度、出境频次、加密强度、权限管控水平、接收方资质、境外合规环境、数据再利用约束等内容。指标体系同时支持金融、医疗、工业、电信等典型行业扩展，可根据领域风险评估要求与业务特点灵活增删专项指标。

为实现统一计算，所有指标需映射至[0, 1]区间。对原始数值型指标采用极值归一化方法进行标准化。对于连续型定量指标(如出境数据规模、传输加密强度等)，采用极值归一化：

$$x_{\text{norm}}^{(i)} = \frac{x^{(i)} - x_{\min}^{(i)}}{x_{\max}^{(i)} - x_{\min}^{(i)}} \tag{1}$$

式中：

$x^{(i)}$ 为第 i 项指标原始观测值；

$x_{\min}^{(i)}$，$x_{\max}^{(i)}$ 为该指标在行业场景下的合理上下边界；

$x_{\text{norm}}^{(i)} \in [0,1]$，值越大代表该项指标带来的风险越高。

该式将原始指标线性映射到统一风险区间，保证不同维度指标在数学上具备可加性与可对比性，避免因数量级差异导致模型失效。对于定性指标，通过模糊语义分级映射为[0, 1]区间数值，实现定性与定量指标统一表征。经过标准化后，得到风险特征向量：

$$X = \left[x_{\text{norm}}^{(1)}, x_{\text{norm}}^{(2)}, \cdots, x_{\text{norm}}^{(n)} \right]^{\mathrm{T}} \tag{2}$$

作为模型输入。

3.3. 基于自注意力机制的动态权重计算

在多维度风险评估中，不同指标在不同场景下对整体风险的贡献度存在显著差异，固定权重难以适应动态变化的出境环境。为此，模型引入自注意力机制实现权重自适应分配。

本文使用自注意力机制实现数据驱动的动态权重分配，其核心是通过特征间相似度自动学习指标重要程度。

将标准化特征向量通过线性变换得到查询向量 Q、键向量 K、值向量 V：

$$Q = XW_Q \tag{3}$$

$$K = XW_K \tag{4}$$

$$V = XW_V \tag{5}$$

其中 W_Q，W_K，W_K 为可学习投影矩阵。自注意力输出为：

$$\text{Attention}(Q,K,V) = \text{softmax}\left(\frac{QK^{\mathrm{T}}}{\sqrt{d_k}} \right) V \tag{6}$$

其中，d_k 为键向量特征维度，引入缩放项避免内积数值过大导致梯度消失或不稳定；softmax 函数将特征相似度归一化为权重分布，使模型自动聚焦高影响力风险要素。为进一步提升权重表达鲁棒性，可采用多头注意力结构，在多个子空间内并行学习风险关联关系，最终融合得到综合动态权重 $\omega = (\omega_1, \omega_2, \cdots, \omega_n)$，softmax 输出结果即为动态权重分布：

$$\omega_i = \text{softmax}\left(\frac{QK^{\mathrm{T}}}{\sqrt{d_k}} \right)_i, \ \sum_{i=1}^{n} \omega_i = 1 \tag{7}$$

这一过程本质上是让模型自动识别：哪些指标在当前出境场景下对风险贡献更大，从而实现权重自适应，而非依赖人工经验赋值。

3.4. 高效计算与轻量化推理技术

传统线性加权模型假设风险要素相互独立，无法反映风险叠加、传导与放大效应，与真实风险机理存在偏差。为此，本文构建非线性耦合融合模型，在单要素风险贡献基础上增加跨要素耦合项，提升风险综合表达精度。

首先对单个指标计算基础风险贡献：

$$f(x_i) = a_i x_i^2 + b_i x_i + c_i \tag{8}$$

其中 a_i，b_i，c_i 为根据风险机理设定的非线性系数，用于描述指标变化对风险的非线性影响。在此基础

上，引入双要素耦合项表示风险相互作用：

$$g\left(x_i,x_j\right)=x_i x_j\cdot\mu_{ij} \tag{9}$$

其中 c_i 为耦合系数，反映要素间关联强度，可通过历史规律分析与先验知识确定。综合风险值由单要素加权和与耦合项共同构成：

$$R=\sum_{i=1}^{n}\omega_i f\left(x_i\right)+\alpha\sum_{1\le i<j\le n}\omega_i\omega_j g\left(x_i,x_j\right) \tag{10}$$

其中 α 为耦合调节系数，控制耦合风险在整体风险中的比重，通常取值于(0, 1)。最终综合风险值 $R\in[0,1]$，数值越高表示敏感数据出境风险越高。

3.5. 动态自适应更新机制

为实现动态评估，模型采用在线学习方式对权重与耦合系数进行增量更新。设损失函数为模型评估结果与校验逼近值之间的均方误差：

$$L\left(\omega,\mu\right)=\frac{1}{2}\left(\hat{R}-R\right)^2 \tag{11}$$

其中 $\hat{R}$ 为外部监测、事件核查或专家校验给出的真实风险逼近值，R 为模型当前输出。采用小批量梯度下降对参数进行更新：

$$\begin{aligned}\omega_{t+1}&=\omega_t-\eta\cdot\nabla_{\omega}L\left(\omega_t,\mu_t\right)\\ \mu_{t+1}&=\mu_t-\eta\cdot\nabla_{\mu}L\left(\omega_t,\mu_t\right)\end{aligned} \tag{12}$$

其中 η 为学习率，控制更新步长。通过增量更新，模型无需全量重训即可实现风险态势跟踪，具备较强的动态适配能力。

3.6. 模型关键参数

为保证模型在真实场景中的可复现性、评估一致性与工程落地能力，本章对模型中所有关键参数的物理意义、计算逻辑、获取路径与约束条件进行统一说明，包括单指标非线性系数 a_i，b_i，c_i、双要素耦合系数 c_i、耦合调节系数 α 和学习率 η 等，它们共同决定风险计算的准确性、动态更新的稳定性以及评估结果的可解释性。

在单指标风险计算中，为反映风险随指标升高呈现非线性放大的真实规律，模型采用二次函数计算单项风险贡献，其中非线性系数 a_i，b_i，c_i 共同决定风险上升的快慢与曲线形态。本模型采用专家知识与历史数据回归相结合的方式：先由领域专家根据风险机理设定低、中、高风险区间的上升趋势，确保风险曲线符合业务认知；再利用同场景历史数据，通过最小二乘法进行拟合，曲线单调递增，使输出结果落在合理风险区间。数据敏感性等高风险指标采用强非线性放大，管理类指标采用温和非线性曲线，从而在保证合理性的同时支持快速部署。

为刻画多风险要素之间的叠加、传导与放大效应，模型引入双要素耦合项，其中 c_i 为耦合系数，用于衡量指标 i 与指标 j 之间风险关联强度。耦合系数的确定采用数据驱动与专家校准相结合的方式：先根据风险传导机理划分强耦合、中耦合、弱耦合关系，再通过历史数据计算指标间 Pearson 系数或互信息并归一化到[0, 1]区间，同时结合专家 1~5 分制打分结果进行映射修正，最终取均值作为 c_i。

在综合风险计算中，耦合项的整体影响由耦合调节系数 α 控制。α 用于平衡独立风险与耦合风险的占比，避免耦合效应过强导致结果偏保守，或过弱导致风险被低估。实际使用时，常规场景取 $\lambda=0.2$，高敏感数据场景提高至 0.35，低风险常规业务取 0.1，并将其约束在(0, 0.5]区间，保证评估结构均衡、结

果可解释。

在线学习过程中的在工程实践中，$\hat{R}$ 主要来自周期性专家评估，以季度或半年度为周期由多名专家独立定级取均值；当发生数据泄露、接收方违约等安全事件时按事件等级直接赋值；也可映射监管评估结论；在冷启动无标注阶段，可使用模型连续多日评估均值作为伪标签，保证在线学习持续稳定运行。为兼顾响应速度与模型稳定性，冷启动数据较少时取 $\eta = 0.05$，稳定运行阶段取 $\eta = 0.1$，高波动场景取 $\eta = 0.02$，并将其约束在$[0.01, 0.2]$区间，避免更新过快导致震荡或过慢导致滞后。

4. 模型综合性能优势分析

从模型合理性层面来看，传统线性风险模型未考虑各类风险要素间的耦合关联，当多种风险因素同步发生时，极易造成风险程度低估。本文构建的非线性耦合模型新增耦合项，能够直观刻画风险的叠加效应与跨要素传导逻辑，更加贴合敏感数据跨境出境风险的实际生成机制。同时模型引入动态注意力权重机制，可随业务场景的实时变化自主调节各风险要素的权重占比，针对异常数据传输、接收主体状态异动、数据敏感等级上调等风险场景拥有更优异的识别效果；配套风险评估指标体系覆盖维度完整、支持拓展新增指标，整体模型具备良好通用适配性。

在动态环境适配层面，传统静态评估模型依靠人工周期性修正模型参数，风险响应存在明显滞后性，还会引发评估结果偏离真实水平的问题。本文模型融合在线学习框架完成参数增量更新，一旦监测到风险要素发生变动，模型将自动启动风险重评估流程，持续动态拟合真实风险变化态势。相关理论推导结果证实，该动态更新机制能够有效优化风险评估结果的时效性与稳定度，完全适配长期、连续、高频次的敏感数据出境风险监测评估工作。

针对计算运行效率维度，传统全量重估模式的时间复杂度过高，落地大规模业务场景时会产生严重的评估延迟。本文通过轻量化网络结构设计、流式增量计算方案搭配多级缓存优化策略，大幅缩减单次风险评估的运算成本，将模型时间复杂度与空间复杂度控制在工程落地可承受区间；依托并行计算能力，模型还能进一步优化多评估任务并发运行效果。理论分析证明，该模型可在常规通用计算设备中稳定完成推理运算，能够满足产业规模化落地的性能需求。

5. 原型系统设计与应用展望

基于多维融合动态评估模型与高效计算技术，可研发敏感数据出境风险动态评估原型系统。系统采用微服务架构，主要包括风险要素采集模块、指标管理模块、模型推理模块、动态更新模块、可视化展示模块与合规报告生成模块。系统可对接机构内部数据资产管理平台、业务系统、安全审计设备与流量监测设备，自动抽取出境数据信息、传输行为特征、管理状态与接收方信息，实现全流程自动化评估。

在应用层面，该系统可为数据出境机构提供风险自查、风险预警、出境方案优化、合规材料生成等功能，降低企业合规成本与安全风险；可为相关部门提供重点主体监测、风险态势分析、高风险行为识别、跨境数据溯源等支撑能力，提升评估精准化与智能化水平。未来可进一步结合知识图谱技术增强风险关联分析能力，引入联邦学习实现跨机构隐私保护下的联合评估，同时与大语言模型结合提升风险研判与合规建议的智能化水平，扩展模型在复杂出境场景下的适用性。

6. 结论

针对当前敏感数据出境风险评估存在的静态化、线性化、动态性不足、计算效率偏低等问题，本文提出一种多维融合动态评估模型与高效计算技术。模型构建覆盖数据敏感性、出境必要性、传输安全、主体管理、境外接收方的多维度指标体系，通过自注意力机制实现动态权重分配，利用非线性耦合函数

提升风险融合表达精度，并依托在线学习实现模型参数自适应更新。同时，通过轻量化推理、流式计算与缓存优化提升运行效率，增强工程落地能力。

理论分析与可行性推演表明，所提模型能够更准确地刻画敏感数据出境风险的多维耦合与动态演化特征，具备较强的场景适配性与计算高效性，可为机构合规运营与风险管控提供有效技术支撑。未来研究将进一步优化风险耦合机理建模方式，提升小样本与异常场景下的自适应能力，加强模型与法律法规、行业标准的深度适配，推动技术成果在更多真实场景中规模化应用。

基金项目

项目等级：国家重点研发计划，项目名称：基于安全标识的敏感数据出境安全风险评估和预警技术，项目编号：2023YFB3106400，课题编号：2023YFB3106403。

参考文献

[1] 马述忠, 房超, 梁银锋. 数字贸易及其时代价值与研究展望[J]. 国际贸易问题, 2018(10): 16-30.

[2] 李航. 我国数据跨境流动规则的不足与完善[D]: [硕士学位论文]. 上海: 华东政法大学, 2018.

[3] 石进, 徐宗煌, 邵波, 等. 总体国家安全观下数据跨境流动风险治理研究[J]. 学术探索, 2026(3): 131-145.

[4] 董克, 吴佳纯, 马廷灿. 我国数据出境安全风险要素体系研究[J]. 情报理论与实践, 2024, 47(6): 49-59.

[5] 赵兴文, 蔡佳音, 李晖, 等. 企业数据出境动态风险评估与安全监管体系研究[J]. 信息安全研究, 2026, 12(2): 124-133.

[6] 彭勇, 江常青, 谢丰, 戴忠华, 熊琦, 高洋. 工业控制系统信息安全研究进展[J]. 清华大学学报: 自然科学版, 2012, 52(10): 1396-1408.

[7] 杨云雪, 鲁骁, 董军. 基于企业环境的网络安全风险评估[J]. 计算机科学与探索, 2016, 10(10): 1387-1397.

[8] 李存斌, 蔺帅帅, 徐方秋. 基于改进 VIKOR 法的云计算环境下用户行为安全的评估研究[J]. 计算机科学, 2017, 44(12): 105-109+119.

[9] 肖招娣. 移动互联网应用平台中信息安全态势评估研究[J]. 计算机仿真, 2017, 34(3): 423-426.

[10] 陈璐, 刘行, 陈牧, 李尼格, 戴造建. 基于图的可扩展移动应用安全评估模型[J]. 计算机工程, 2018, 44(5): 78-82.

[11] Alberts, C. and Dorofee, A. (2002) Managing Information Security Risks: The OCTAVE Approach. Addison Wesley Longman Publishing Co.

[12] Stolen, K., den Braber, F., Dimitrakos, T., Fredriksen, T., Gran, B.A., Houmb, S., *et al*. (2002) Model-Based Risk Assessment—The CORAS Approach.

[13] Karabacak, B. and Sogukpinar, I. (2005) ISRAM: Information Security Risk Analysis Method. *Computers & Security*, **24**, 147-159. https://doi.org/10.1016/j.cose.2004.07.004

[14] Vorster, A. and Labuschagne, L. (2005) A Framework for Comparing Different Information Security Risk Analysis Methodologies. *Proceedings of SAICSIT* 2005, White River, 20-22 September 2005, 95-103.

[15] Chang, K.H., Chung, H.Y., Wang, C.N., *et al*. (2023) A New Hybrid Fermatean Fuzzy Set and Entropy Method for Risk Assessment. *Axioms*, **12**, Article 58. https://doi.org/10.3390/axioms12010058

[16] 吴文刚, 张志文, 王庆生. 基于模糊综合评判和 AHP 信息安全风险评估模型[J]. 重庆理工大学学报(自然科学版), 2017, 31(7): 156-161.

[17] 王奕, 费洪晓, 蒋蘋. FAHP 方法在信息安全风险评估中的研究[J]. 计算机工程与科学, 2006, 28(9): 4-6+12.

[18] 张本群. 基于危险理论的电子政务系统信息安全风险评估[J]. 微电子学与计算机, 2012, 29(9): 71-73+78.

[19] 王姣, 范科峰, 莫玮. 基于模糊集和 DS 证据理论的信息安全风险评估方法[J]. 计算机应用研究, 2017, 34(11): 3432-3436.

[20] 冯雪峰, 龚军, 吕小毅. 模糊神经网络信息安全风险评估方法在信息系统中的应用[J]. 现代计算机, 2018, 24(16): 50-54.

[21] Lin, X. and Qi, Z. (2025) Dynamic Risk Prediction in Financial-Production Systems Using Temporal Self-Attention and Adaptive Autoregressive Models. *Frontiers in Physics*, **13**, Article 1627551. https://doi.org/10.3389/fphy.2025.1627551

[22] 索玮岚, 徐文杰, 孙晓蕾. 多灾害耦合情境下城市关键基础设施失效风险建模研究[J]. 中国管理科学, 2023, 31(6): 1-12.

[23] 张蛟磊, 李刚, 余定浩, 等. 考虑腐蚀与疲劳耦合损伤的滨海工程结构地震风险分析[J]. 工程力学, 2026, 43(5): 1-12.

[24] 张凯, 时金桥, 马乐乐, 等. 数据出境安全风险监测预警关键技术综述[J]. 通信学报, 2025, 46(12): 1-18.