

面向东盟的数据跨境 流通治理挑战及基础设施应用框架

Challenges and Infrastructure Application Framework of Cross-Border Data Flow Governance Towards ASEAN

曾雪云¹,张潇文¹,张汉宁²,郜怡飞¹,夏文德¹,周晖雨³(1. 北京邮电大学,北京 100876;2. 中国联通[海南]创新研究院,海南海口 570208;3. 广西壮族自治区信息中心,广西南宁 535000)

Zeng Xueyun¹,Zhang Xiaowen¹,Zhang Hanning²,Gao Yifei¹,Xia Wende¹,Zhou Huiyu³(1. Beijing University of Posts and Telecommunications, Beijing 100876, China; 2. China Unicom[Hainan] Innovation Research Institute, Haikou 570208, China; 3. Guangxi Zhuang Autonomous Region Information Center, Nanning 535000, China)

摘要:

探讨了面向东盟的数据跨境流通模式、面临的挑战及基础设施建设的可能方案。研究认为,数据跨境流通治理存在数据跨境兼容、协同治理和监管合规3个方面的挑战。基于此,提出了3种基于新型基础设施建设的治理方案:人工智能辅助的跨境数据安全方案、基于联盟链的中国—东盟跨域数据共享方案以及基于隐私保护计算的“中国—东盟”数据流通框架设计,旨在提升数据跨境流通的安全性和效率,推动数据要素在多方协作中的高效和安全流通。

关键词:

数据跨境流通;数据基础设施;人工智能;联盟链;隐私计算;东盟

doi:10.12045/j.issn.1007-3043.2025.05.003

文章编号:1007-3043(2025)05-0013-06

中图分类号:TN919.2

文献标识码:A

开放科学(资源服务)标识码(OSID):



Abstract:

It explores the cross-border data flows model, the challenges it faces and the potential infrastructure construction solutions for ASEAN. It is thought that there are three challenges in the governance of cross-border data flow: data compatibility issues, collaborative governance, and regulatory compliance concerns. Based on these challenges, it proposes three governance frameworks based on new infrastructure developments: an AI-assisted cross-border data security management system, a consortium blockchain-based China-ASEAN data-sharing model, and a privacy-preserving computing framework for secure data flows. These solutions aim to enhance the security and efficiency of cross-border data exchange, facilitating the safe and seamless circulation of data assets within a multi-stakeholder collaborative ecosystem.

Keywords:

Cross-border data flow; Data infrastructure; Artificial intelligence; Consortium blockchain; Privacy computing; ASEAN

引用格式:曾雪云,张潇文,张汉宁,等. 面向东盟的数据跨境流通治理挑战及基础设施应用框架[J]. 邮电设计技术,2025(5):13-18.

0 引言

随着全球数字经济的快速发展,数据跨境流通成为推动经济增长和科技创新的关键因素。2023年12月,习近平主席在南宁市考察中国—东盟信息港时指出,要加快建设中国—东盟信息港,推动数字互联互

通,打造数字丝绸之路。2024年11月,中国提出《全球数据跨境流动合作倡议》,倡导秉持开放、包容、安全、合作、非歧视的原则,促进数据跨境高效便利安全流动,为全球数据跨境流动合作提供了新的指引和方向。因此,研究面向东盟的数据跨境流通治理具有重要意义。

1 全球视域下的数据跨境流通模式

各经济体对数据跨境交流中的数据安全与共享的政策存在差异,均结合自身的利益和国情发展了特

基金项目:数字广西建设决策咨询重点课题(2024)(S2024344);海口市科技计划项目(2024-042)

收稿日期:2025-03-07

有的数据跨境流通规则并推动构建了相应的自由贸易协定。中国—东盟的数据跨境流通也受到全球数据跨境流通模式的影响并体现出基于双边谈判与共同诉求的区域特色。

1.1 以欧盟为代表的“数据保护”模式

欧盟主张将个人信息权作为基本人权,在跨境数据流动问题上秉持人权优先、域外充分保护的原则。2018年,欧盟《一般数据保护条例》(GDPR)正式实施。作为最严格的数据保护法案之一,GDPR设置了充分性保护标准,提高外部门槛,同时促进域内数据自由流动,降低域内数据保护成本^[1-2]。在区域贸易协定方面,2019年,《欧盟—日本经济伙伴关系协定》生效,并于2024年被正式纳入合作框架中,该协议将个人数据保护置为核心,确保个人数据得到充分保护,并限制数据本地化。

1.2 以美国为代表的“自由流动优先”模式

美国政府及业界普遍抵制通过立法手段来规范个人数据处理活动,认为严格的法律规定将“不可避免地商业运营构成障碍”。因此,美国采取了一种侧重市场导向和行业自我监管的个人数据保护策略^[3]。为了实现数据流动自由化与数据保护之间的平衡,美国还通过促进数据流动议题以及减少特定部分中的“例外”规定来提升数据跨境流通的自由度^[4]。2018年,美国以CPTPP为基础,重新谈判北美自由贸易协定,形成了《美国—墨西哥—加拿大协定》,强调数据跨境自由流动、数据存储非强制本地化等内容,进一步推动了数据流动自由化。

1.3 以中国和东盟为代表的本土化保护模式

中国秉持安全与发展平衡的原则,构建了一套中国特色的跨境数据流动规则体系,旨在促进数据跨境安全、自由流动的同时保障数据安全和个人信息权益。东盟与中国的治理理念存在一致性,强调保护个人隐私数据,并在保障数据安全的基础上促进数据的自由跨境流通^[5]。2020年,东盟10国及中国、日本、韩国、澳大利亚、新西兰共15个国家正式签署《区域全面经济伙伴关系协定》(RCEP),其跨境数据流动的相关规则体现了中国和东盟主张的“多元共治”的数据治理理念,允许缔约国出于“国家安全”和“隐私保护”的目的,在必要情况下限制数据的自由跨境流通。2021年东盟通过的《数据管理框架》(DMF)和《跨境数据流动合同范本》(MCC)、2022年越南发布的《至2025年数字经济和数字社会国家发展战略暨2030年展望》、

2024年印度尼西亚发布的《2030年数字经济发展国家战略》中均提到对数据跨境流通行为的限制和要求。

2 面向东盟的数据跨境流通治理挑战

在区域合作视域下,数据跨境兼容挑战、协同治理挑战和监管合规挑战是面向东盟的数据跨境流通治理与共享的主要困境。

2.1 “软”“硬”设施差异引发的数据跨境兼容挑战

一是东盟各国的数据技术标准、规范和机制等“软”基础设施存在差异。这一差异导致了数据分类、分级、格式、编码、传输协议等方面的不兼容问题,进而增加了数据处理和传输的复杂性,降低了数据的完整性和可用性,影响了数据利用效率^[6]。技术标准与规范的落后导致政府数据出境安全管理体系配套措施匮乏,主动数据出境规则操作性受限,数据跨境监督效率低下,这共同构成了数据跨境流通合规困境^[7]。二是东盟各国的数据存储设施、计算设施等“硬”基础设施存在“数字鸿沟”。东盟国家的网络基础设施普遍较脆弱,在数据传输、存储、处理和访问过程中面临技术兼容问题^[5],并且缺乏强有力的数据防护机制和有效的安全控制措施,这导致这些国家更容易遭受黑客入侵、数据泄露风险较高^[8],将影响其他国家和地区对东盟数据保护能力的信任,制约数据的自由流动。

2.2 文化差异导致的协同治理挑战

东盟各国之间以及与中国文化背景、价值观和社会习俗存在一定差异,这直接影响了数据隐私管理和使用的观念和规则。在东盟“多元共治”的理念下,印度尼西亚、文莱和越南在数据保护和政策方面采取了较为严格的措施,注重个人隐私保护。以越南为例,2019年正式生效的越南《网络安全法》中规定:在越南网络空间提供服务的国内外企业,若有收集、开发、分析、处理个人通信数据、业务使用者关系数据和业务使用者在越南产生的数据的活动,要在政府规定的时间内在越南储存这些数据。相比之下,菲律宾、新加坡和泰国对数据处理和共享的态度则更加开放^[8]。数据开放观念与文化差异可能导致数据持有方对数据共享的担忧,影响合作国政府与跨国企业在数据管理和使用方面的决策,从而限制数据跨境流通意愿,增加跨境数据合作以及数据跨境流通治理的难度。

2.3 制度差异导致的监管治理挑战

数据跨境流通涉及到大量的数据传输、存储和处

理活动,面临着合规成本和监管风险等问题。加入区域性或国际性信息保护组织或平台后,企业在数据跨境传输与隐私保护方面将受到“数据源国”与“数据目标国”各自的数据跨境法律框架、规则和标准的制约,为避免高昂的违规罚款,通常会主动推进数据传输的合规措施与技术升级,然而,这将持续增加企业的运营成本和合规成本^[9]。在中国与东盟国家的跨境数据流通中,部分东盟国家数据共享利益分配机制欠佳、数据安全保护能力较弱、数据价值链地位偏低等问题较为突出,导致中国—东盟跨境数据的收集成本上涨^[8]。

3 新信息技术赋能数据跨境流通的治理方案

区块链、人工智能、隐私计算等新一代信息技术的应用,为数据的跨境流通带来了技术支撑与创新解决方案。

3.1 基于人工智能的跨境数据安全方案

人工智能算法通过智能分析与自动化处理,可以实时监控跨境数据传输过程中的异常活动,迅速识别并应对潜在威胁,提升数据安全监控和异常检测的精准度。联邦学习将模型训练分布在多个数据持有者之间,使各方能够在不交换实际数据的前提下,协同构建和优化机器学习模型,有效保护各方数据的隐私^[10]。而机器学习在对海量数据进行分析时,能够预测和预防可能的安全漏洞和攻击路径,从而提升整体数据安全防御水平^[11],进而加强数据流通中的风险管理和隐私保护^[12]。

针对数据跨境流通中的监管合规挑战,本文提出一个适用于跨境数据传输的安全管理方案,该方案主要包括数据采集与预处理、智能分析、动态响应、可视化与监测四大模块(见图1)。

a) 数据采集与预处理模块。数据采集与预处理模块主要负责跨境数据传输中的数据采集、清洗和标准化处理,并将清洗好的数据输入到智能分析模块。该模块通过 DBSCAN 等聚类算法清除异常数据点,并利用 Word2Vec 等模型实现文本数据的向量化表达,实时采集和处理流量、元数据、行为日志等多源异构数据。通过整合和提取数据特征,该模块有效减少了数据噪声和冗余,为后续智能分析提供高质量的输入。

b) 智能分析模块。智能分析模块对数据异常行为进行分析,同时评估跨境数据流转的风险并检验其

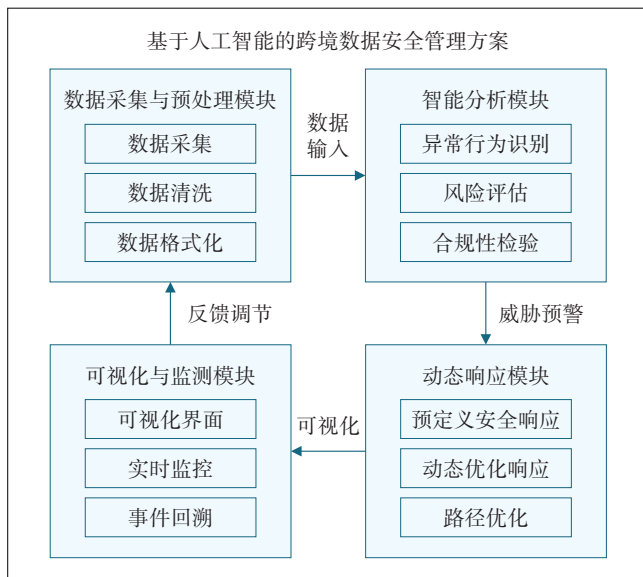


图1 基于人工智能的跨境数据安全方案架构

合规性,在发现异常情况时对动态响应模块发出预警信号。该模块通过孤立森林算法识别异常数据点,采用 LSTM 算法分析时间序列数据的异常趋势,并基于 Transformer 模型对传输内容的语义结构进行建模。在合规性检验方面,该模块结合 LDA 主题模型判断数据敏感性,并通过规则匹配算法检查数据是否符合 GDPR、CCPA 等法规要求。

c) 动态响应模块。动态响应模块在识别出威胁后,通过预定义安全响应和动态优化响应进行处理,并将处理结果反馈到可视化与监测模块,在此过程中通过路径优化保障数据传输的安全性和持续性。该模块在处理程序化威胁时,使用决策树算法触发安全响应,如中断连接或隔离异常数据流;在处理非程序化威胁时,采用强化学习算法(DQN)动态优化响应策略,降低误报和漏报。在路径优化方面,该模块结合 Q-Learning 和遗传算法(GA),寻找安全性与传输效率的平衡点,选择最优的数据传输路径。

d) 可视化与监测模块。可视化与监测模块实时接收动态响应模块的数据,通过用户界面提供跨境数据传输状态可视化、实时监控和事件回溯功能,并根据实际情况对数据采集与预处理模块进行反馈调节。该模块基于时序分析算法(ARIMA)绘制数据流量趋势图,帮助快速定位异常行为问题。事件回溯功能提取日志中的关键信息链路,重建事件因果关系,实现对威胁或泄露事件的源头追踪。

3.2 基于联盟链的中国—东盟跨域数据共享方案

区块链技术在数据跨境流通中的优势在于安全可信和高透明度带来的数据不可篡改性、多方验证及全程可追溯等特性,强化了数据跨境流动的合规性,同时有效遏制了隐私泄露风险。区块链的智能合约功能能够自动执行和验证跨境数据交易,确保数据流通的合法性和合规性,从而减少人为干预和错误,提升数据交易的安全性和可靠性。有学者在碳数据领域基于区块链技术设计了一个UG-CET系统来解决数据安全问题的,该系统不要求各国共享详细数据,只提供广义数据即可实现数据审计与数据一致性,既保护本国的数据,也确保其他国家共享数据的真实性^[13]。还有学者将区块链技术与同态加密相结合,为跨境数据共享提供了新的解决方案。例如,文献[14]结合属性基础访问控制(ABAC)和区块链智能合约的访问控制模型(Fabric-ABAC)实现了联盟区块链中跨域数据安全共享的细粒度、多层次和可审计的访问控制,并利用代理重加密技术保护跨域数据交易的机密性。

联盟链作为一种结合了公有链与私有链特点的区块链技术,可以在保护各国数据主权的前提下,实现数据的高效、安全流通。中国—东盟数据跨境流动框架如图2所示,数据提供者将数据上传至联盟链网络,并通过加密技术确保数据的安全性。在数据上传

后,数据进入智能合约控制的共享环节。在隐私保护方面,隐私计算技术被应用于数据的共享过程中,确保数据在不离开原始数据库的情况下完成计算和分析。通过这种方式,数据所有者能够在保护数据隐私的同时,允许跨境合作伙伴利用数据创造价值。最后,数据消费者通过联盟链获取经过验证的数据使用权限。在整个过程中,数据的存储、传输以及使用都经过严格的加密和权限管理,确保了数据在跨境流动中的安全性和合法性。同时,通过联盟链的分布式账本技术,确保每一笔数据操作的透明和可追溯性,从而增强各方对数据共享的信任。

区块链在中国—东盟数据跨境流动中通过去中心化的权限管理和智能合约机制,实现了安全、高效和透明的数据共享。整个流程涉及数据所有者、数据请求者、区块链平台三方协作,以确保数据的访问权限受到严格控制,同时保证所有访问操作的可追溯性。基于区块链的中国—东盟数据跨境流动框架涵盖了数据所有者、数据访问请求、区块链管理以及数据请求者之间的交互机制。数据所有者是负责存储、管理数据并控制访问权限的一方,可以进行数据全生命周期的管理,包括创建新的数据资源、设置访问权限、共享资源、数据管理操作等。数据请求者是希望

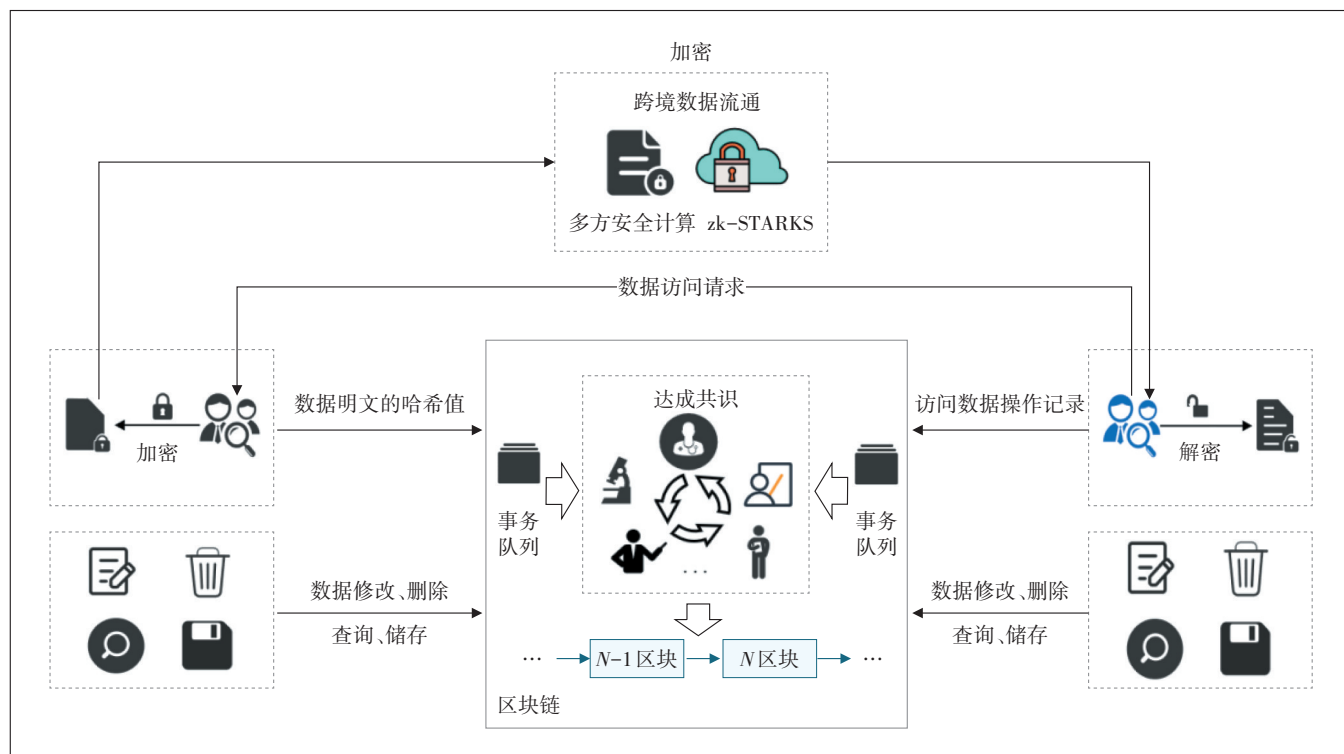


图2 中国—东盟数据跨境流动框架

访问数据的一方,当数据请求者需要访问某个数据资源时,他们需要提交数据访问请求,区块链平台会介入管理权限验证,如果权限验证成功,数据请求者可以查看、编辑或下载数据。区块链平台在数据访问控制中发挥核心作用,它通过多方安全计算和零知识可扩展透明知识论证技术(zk-STARKs)确保数据流动的安全性、透明度和可追溯性。

3.3 基于隐私保护计算的“中国—东盟”数据流通框架设计

隐私计算技术,包括多方安全计算、同态加密和差分隐私等,能够实现数据使用过程中的安全计算和隐私保护,从而有效保障数据主体的权益。多方安全计算允许多个参与方在不泄露各自数据隐私的情况下进行协同计算和结果共享,从而实现数据的安全合作与共享^[15]。同态加密技术可在无需解密数据的情况下对跨境加密数据进行操作,适用于敏感数据的处理,但同态加密操作的效率较低,不适合实时响应的应用场景^[16]。

本文提出一个嵌入隐私计算的跨境数据流通基础设施解决方案。当数据供方和数据需方在数据交

易平台上进行需求撮合后,会转至线下并利用“点对点”的方式私有化部署隐私计算节点,这导致数据流通平台无法有效获取计算过程的安全管控、计算用量与费用等信息。本文研究设计了一个统一的隐私计算框架,该框架能够兼容不同的数据流通交易平台和隐私计算服务平台,实现互联互通,将隐私计算技术与数据流通场景进行基础设施整合,提升数据流通的安全性和效率,以解决当前数据流通平台与隐私计算平台的离断问题。通过建构“三层架构、双轨互通、一体生态”的统一隐私计算框架(见图3),促进数据流通交易平台与隐私计算服务平台之间的一体化,保障不同隐私计算服务平台间的互操作性,从而构筑涵盖数据流通交易全生命周期的生态系统,推动数据要素在多方协作环境中的高效、安全流通。

基于数据跨境流通场景的统一隐私计算框架由数据流通管理与交互平台和底层支持与隐私计算平台2个部分组成,提供分布式信任与安全管理、跨平台与跨域数据流通支持、隐私计算与合规管理三大核心服务。数据流通管理与交互平台主要负责数据目录、数据资产、数据订单、计费与审计、用户权限等的管

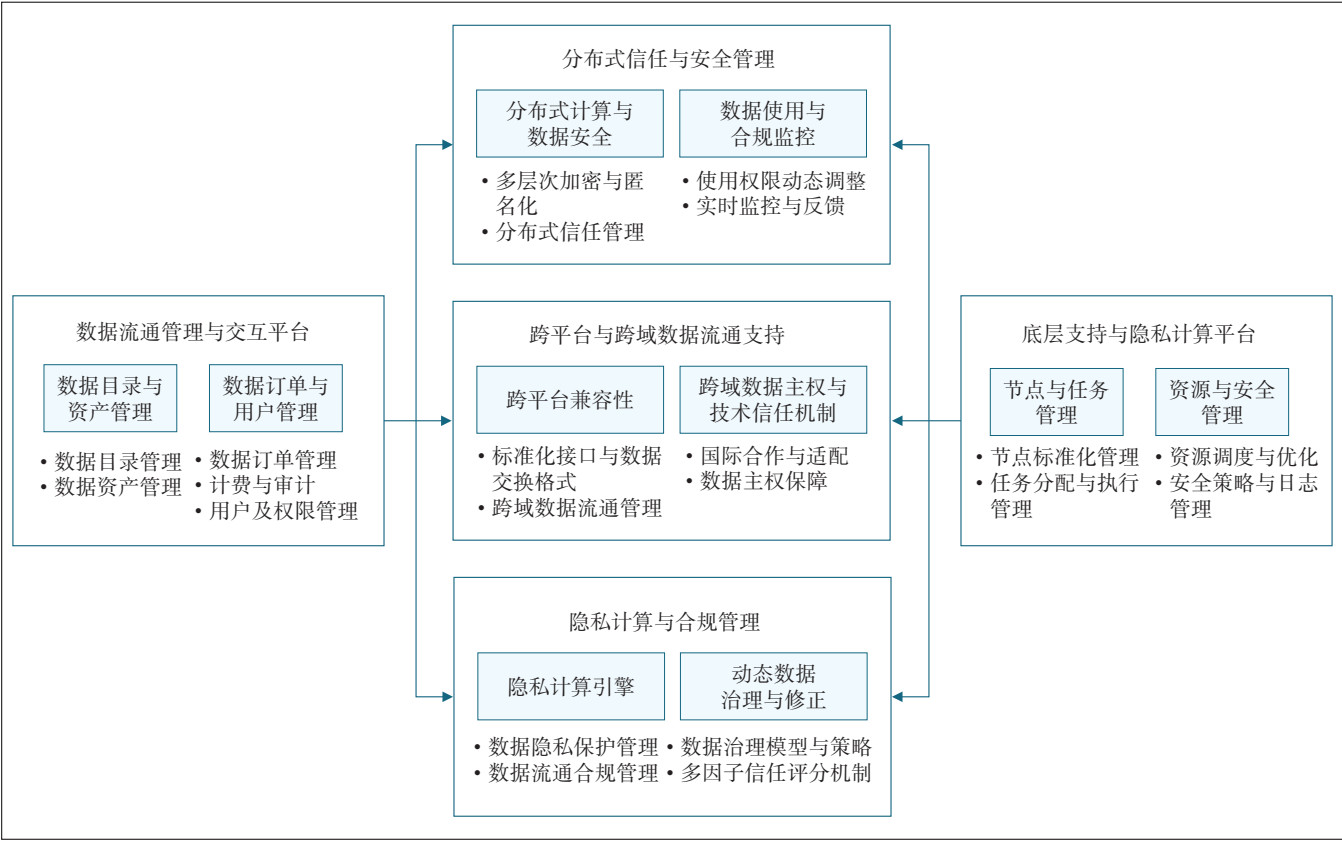


图3 基于数据跨境流通场景的统一隐私计算框架

理,而底层支持与隐私计算平台则实现节点标准化管理、任务分配与执行管理、资源调度与优化、安全策略与日志管理等功能。两大平台协同工作,共同支撑数据的安全流通与隐私保护。在三大核心服务中,分布式信任与安全管理包括分布式计算与数据安全、数据使用与合规监控2个部分,实现了多层次加密与匿名化、使用权限动态调整、分布式信任管理、实时监控与反馈等功能;跨平台与跨域数据流通支持包括跨平台兼容性与跨域数据主权及技术信任机制,涉及标准化接口与数据交换格式、跨域数据流通管理、国际合作与适配、数据主权保障等;隐私计算与合规管理则由隐私计算引擎和动态数据治理与修正组成,提供数据隐私保护管理、数据流通合规管理、数据治理模型与策略、多因子信任评分机制等功能。该框架通过多层次的技术手段和管理机制,确保跨境数据流通的安全性、合规性和可控性。

4 结束语

中国和东盟国家对数据流通的需求与承受能力不同,在数据治理制度、标准、网络和计算基础设施等方面存在显著差异,为数据跨境流通治理带来了较大挑战。针对数据跨境流通治理中安全监管滞后、共享信任缺失、隐私保护不足等问题,本文提出了新一代信息技术赋能数据跨境流通的治理方案,结合人工智能技术的实时监测与预测能力、联盟链的去中心化审计与追溯机制以及隐私计算的安全协同计算方法,为提升跨境数据流通的效率、安全性和互信度提供新的技术思路和方案。

参考文献:

- [1] SULLIVAN C. EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era[J]. Computer Law & Security Review, 2019, 35(4): 380-397.
- [2] 夏杰长,张雅俊. 数字贸易中跨境数据流动的规制困境与优化路径[J]. 经济纵横, 2024(4): 39-46.
- [3] 许多奇. 个人数据跨境流动规制的国际格局及中国应对[J]. 法学论坛, 2018, 33(3): 130-137.
- [4] 陈寰琦. 从“例外”和“负面清单”看美国跨境数据自由流动限制性措施[J]. 国际经贸探索, 2023, 39(9): 99-116.
- [5] 吴希贤. 东盟数据治理: 全球背景、规制框架与中国合作[J]. 亚太经济, 2022(4): 1-10.
- [6] SHAHRIAR RAHMAN M, AL OMAR A, BHUIYAN M Z A, et al. Accountable cross-border data sharing using blockchain under re-

- laxed trust assumption[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1476-1486.
- [7] 熊光清,张素敏. 总体国家安全观视角下我国数据出境安全管理制度完善[J]. 哈尔滨工业大学学报(社会科学版), 2023, 25(5): 32-40.
 - [8] 李正彪,陈晔婷. RCEP生效赋能中国—东盟高质量跨境数据共享的机遇、挑战及对策[J]. 国际贸易, 2024(5): 36-43, 58.
 - [9] XU Z Y. International law protection of cross-border transmission of personal information based on cloud computing and big data[J]. Mobile Information Systems, 2022(1): 9672693.
 - [10] ZHANG H, XUE J B, WANG Q, et al. A security optimization scheme for data security transmission in UAV-assisted edge networks based on federal learning[J]. Ad Hoc Networks, 2023, 150: 103277.
 - [11] HU H D, LIN C L, CHANG C C, et al. Enhanced secure data backup scheme using multi-factor authentication[J]. IET Information Security, 2019, 13(6): 649-658.
 - [12] DAS S, BALMIKI A K, MAZUMDAR K. A review on AI-ML based Cyber-Physical systems security for industry 4.0[M]//BANERJEE J S, BHATTACHARYYA S, OBAID A J, et al. Intelligent Cyber-Physical Systems Security for Industry 4.0. New York: Chapman and Hall/CRC, 2022: 203-216.
 - [13] SU M T, ZHAO R Y, JIANG J J, et al. A blockchain system supporting cross-border data protection and consistency verification in unified global carbon emissions trading framework[J]. Journal of Cleaner Production, 2024, 448: 141693.
 - [14] LIU Y, YANG W D, WANG Y L, et al. An access control model for data security sharing cross-domain in consortium blockchain[J]. IET Blockchain, 2023, 3(1): 18-34.
 - [15] TSO R, ALELAIWI A, MIZANUR RAHMAN S M, et al. Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud[J]. Journal of signal processing systems, 2017, 89(1): 51-59.
 - [16] LIU Y, YANG C S, LIU Q, et al. PDPHE: personal data protection for trans-border transmission based on homomorphic encryption[J]. Electronics, 2024, 13(10): 1959.

作者简介:

曾雪云,北京邮电大学教授、博士生导师,博士,主要从事公司金融、数字经济、数据要素领域的研究工作;张潇文,北京邮电大学硕士在读,主要从事人工智能、计算机视觉领域的研究工作;张汉宁,毕业于西安交通大学,中国联通(海南)创新研究院常务副院长,教授级高级工程师,博士,主要从事人工智能、大数据分析、智能系统等方面的研究工作;郜怡飞,北京邮电大学博士在读,主要从事数据资产化领域的研究工作;夏文德,北京邮电大学博士在读,主要从事数据资产会计处理领域的研究工作;周晖雨,教授级高级工程师,主要从事大数据发展和大模型应用等研究工作。