

# 面向跨境的去中心分布式数字身份框架设计

陈健<sup>1,2</sup>, 蔡智明<sup>2</sup>, 齐佳音<sup>3,4,5\*</sup>, 方滨兴<sup>3,4,5</sup>

(1. 澳门城市大学数据科学学院, 澳门 999078; 2. 中西创新学院数字科技学院, 澳门 999078; 3. 广州大学网络空间安全学院, 广州 510006; 4. 广州大学黄埔研究院, 广州 510006; 5. 可信分布式计算与服务教育部重点实验室, 北京 100084)

**摘要:** 进入数字化时代后, 跨境数据流动衍生出数据主权利要求, 在个人数据隐私保护、灵活高效的授权访问之间矛盾凸显; 数字身份框架作为解决这一矛盾的关键基础支撑, 研究价值突出。本文在梳理跨境数字身份认证模型研究发展态势的基础上, 提出了一种去中心化分布式跨境身份认证框架, 引入数据分类分级策略, 包含基于区块链的去中心化身份管理机制、动态数据属性分类与分级的通用认证池模型、隐私保护与访问控制策略3个核心模块, 用于克服传统的集中式模型在跨境场景中的信任与合规性问题。进一步剖析了属性关联异构分级的效率和精度、跨境双方属性授权信任边界的博弈等跨境数字身份认证框架的应用难点, 从认证框架应用封装的应用程序编程接口模型、认证框架的评估标准和实施路径等方面出发完善了相应解决方案。相关框架设计方案及发展理念, 不仅为跨境数字身份认证提供了实践参考, 而且为构建跨境数据流动的统一标准和安全规范提供了新的技术思路与实施路径。

**关键词:** 跨境数据; 去中心化数字身份; 分布式系统; 隐私保护; 访问控制; 区块链技术

**中图分类号:** TP309 **文献标识码:** A

## A Framework Design for Decentralized Digital Identity Across Borders

Chen Jian<sup>1,2</sup>, Cai Zhiming<sup>2</sup>, Qi Jiayin<sup>3,4,5\*</sup>, Fang Binxing<sup>3,4,5</sup>

(1. Faculty of Data Science, City University of Macau, Macao 999078, China; 2. Faculty of Digital Science and Technology, Macau Millennium College, Macao 999078, China; 3. Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China; 4. Huangpu Graduate School of Guangzhou University, Guangzhou 510006, China; 5. Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education, Beijing 100084, China)

**Abstract:** In the digital era, the challenges of data sovereignty and the conflict between personal data privacy protection and efficient access are becoming more pronounced. As a critical foundational support for resolving this contradiction, the digital identity framework holds significant research values. Based on a review of the research and development trends in cross-border digital identity authentication models, this study proposes a decentralized, distributed framework for cross-border identity authentication. The framework incorporates a data classification and grading strategy, and features three core components: a blockchain-based decentralized identity management mechanism, a universal certification pool model for dynamic data attribute classification and grading, and privacy protection and access control strategies. These components are designed to overcome the trust and compliance issues inherent in traditional centralized models in cross-border scenarios. Furthermore, this study delves into the application

**收稿日期:** 2024-10-08; **修回日期:** 2024-11-27

**通讯作者:** \*齐佳音, 广州大学网络空间安全学院教授, 研究方向为跨境数据、网络安全; E-mail: qjjiayin@139.com

**资助项目:** 中国工程院咨询项目“关于统筹数据发展和安全的治理规则和策略研究”(2023-XBZD-20-03); 国家自然科学基金项目(72293583, 72293580); 澳门基金会学术资助计划项目(G01156-2309-262)

**本刊网址:** sscae.engineering.org.cn

challenges of the cross-border digital identity authentication framework, such as the efficiency and accuracy of attribute association and heterogeneous grading, and the strategic interaction of trust boundaries for attribute authorization between cross-border parties. It refines corresponding solutions from the perspectives of application encapsulation of the authentication framework through application programming interface (API) models, evaluation criteria for the authentication framework, and implementation pathways. The proposed framework not only provides practical references for cross-border digital identity authentication but also offers new technical insights and implementation pathways for establishing unified standards and security protocols for cross-border data flow.

**Keywords:** cross-border data; decentralized digital identity; distributed system; privacy protection; access control; blockchain technology

## 一、前言

进入数字化时代后,数据的全球性流动成为推动经济互联互通、文化交流传播的关键因素,数据安全、个人隐私保护等问题受到更多重视。《促进和规范数据跨境流动规定》(中国,2024年)<sup>[1]</sup>、《数据治理法》(欧盟,2024年)<sup>[2,3]</sup>为数据出境安全评估、个人信息出境标准合同、个人信息保护认证等提供了跨境数据的法制框架。在全球范围内构建共同认可、开放可控的隐私数据保护框架具有紧迫性<sup>[4]</sup>。

我国正在建立跨境数据流动框架。《网络数据安全管理条例》(2024年)<sup>[5]</sup>对个人信息数据、网络数据跨境作出了明确规定;工业与信息化管理部门推动分布式数字身份(DID)应用试点,探索面向机构和个人的Web 3.0数字身份认证、数字资产管理体系<sup>[6,7]</sup>;《“数字湾区”建设三年行动方案》(2023年)<sup>[8]</sup>提出,开展粤港澳三地居民统一身份认证、电子签名互认,实现企业和居民高频事项“跨境通办”。然而,跨境数字身份的实际应用仍然面临一些难点。数据主权强调国家对境内数据的控制权<sup>[9]</sup>,将直接影响跨境数据传输的法律路径与合规性要求,导致跨境数据保护实践具有复杂性和多样性,目前未能形成统一且通用的框架与技术标准。不同国家对个人数据隐私的定义以及保护层级划分存在差异,数字身份的属性在跨境中具有动态、多变的特点,构成属性分类和分级方面的技术难题<sup>[10]</sup>。在保障隐私的前提下,构建灵活且高效的授权与访问控制机制也是亟待研究的课题。

围绕跨境数字身份实际应用面临的难点,本文从去中心化数字身份架构、身份属性数据的分类分级管理和隐私合规性评估、分布式数字身份的授权访问机制3个角度出发,构建基于隐私保护的分布式跨境数字身份认证框架;通过知识图谱识别身份属性之间的关联规律,建立属性熵空间并引

入图计算,测算隐私在不同条件下的行为变化;制定相应的属性授权与访问控制策略,为跨境数据流动中的身份认证提供实施路径。相关理论框架和技术实现方法,符合数据跨境的合规和隐私保护等要求,可为跨境数据统一标准、安全规范等研究提供理论支持。

## 二、跨境数字身份认证模型的研究发展态势

### (一) 数字身份认证模型的技术演变

与数字技术发展同步,数字身份认证模型正在经历变革。具有去中心化特征的身份主权(SSI)<sup>[11]</sup>、DID<sup>[7,12]</sup>等新模式,逐步取代依赖公钥基础设施<sup>[13]</sup>、证书颁发机构(CA)<sup>[14]</sup>的中心化框架。这种转变赋予个人对自有身份信息控制权,有利于增强隐私保护和数据安全性,更好满足数字时代对身份认证灵活性和安全性的需求。

去中心化的分布式数字身份认证,通过区块链等分布式技术实现身份的自主管理。每个用户拥有唯一的去中心化身份标识符,能够以私钥的形式持有和控制个人的身份信息。这种处理方式无须依赖中心机构,赋予用户对身份信息的掌控权,同时减少中心化伴生的单点故障风险。DID技术在国际上得到推广应用,如万维网联盟制定的去中心化身份协议,IDunion、Sovrin、uPort、Veres One、Hyperledger Indy、Blockstack等基于DID的主流SSI<sup>[15-19]</sup>。然而,这些DID都是非实名的,无法对接现实生活中的真实身份,因而在充分保障个人隐私的同时会造成诸多社会治理问题。

近年来,身份和访问管理(IAM)<sup>[20,21]</sup>研究与应用进展显著。相关IAM解决方案衍生出基于角色的访问控制、基于属性的访问控制、风险智能访问控制等模型,可适应更为复杂的企业环境与合规要求<sup>[22]</sup>。这些方法以细化权限管理和用户身份验证的方式来增强安全性,在云计算、移动通信环境中应

用居多。然而，现有的IAM系统仍然存在一些问题，如身份信息的集中存储可能引发安全漏洞，提高集成用户行为分析、动态权限调整的难度。

我国也在积极推动基于实名制的分布式数字身份体系。2023年，国家信息中心牵头的区块链服务网络（BSN）发展联盟发布了实名DID服务，基于可信身份认证平台（CTID）<sup>[23]</sup>实现中心化签发、分布式认证的功能；BSN实名的DID身份链部署在BSN公网，任何业务方采集到用户的真实身份信息后，可通过该服务向CTID身份认证平台发送请求，在经过平台进行身份核验后，即由BSN身份链签发用户的BSN个人实名DID，并为业务方提供DID管理与更新、身份证明凭证等服务。相关服务已在部分金融机构、重点企业开展试点应用。

### （二）跨境分布式数字身份认证面临的挑战与解决方向

在跨境身份认证授权方面，DID虽具有隐私保护、数据控制方面的优势，但面临多方面的挑战。私钥的安全存储及管理是关键任务，任何安全漏洞都可能导致身份信息泄露。在实际应用中，DID缺乏统一标准和互操作性，抑制了跨境认证的有效性；未建立去中心化管理方面的权威机构，容易滋生非法交易、洗钱等犯罪活动，不利于DID在跨境场景下的规模化应用。目前还没有建立可适应多样化跨境主体和场景的通用身份认证模型。

DID强调非中介（双方直接交互），而忽略了跨境实际应用中“担保人”的角色。CA在跨境数据交互中承担了验证颁发证书的作用，但没有转变为可信任机构的认定，致使DID未能介入当前的主流跨境场景应用。为此，需要在去中心化的分布式数字身份框架中融入“担保人”的角色。

现有的数字身份框架没有针对隐私属性进行精细化的分层管理。不同的身份属性隐私安全要求，对应着不同的应用服务能力。例如，身份证号码处于最高的隐私安全级别，而居民所属省市则属于一般的隐私；关联至应用服务，一般的导航服务只需授权手机号码认证，而海关过关导流导航则需要车辆属地的属性认证。因此，如需在跨境时满足不同层次的需求，就应建立关于身份属性的通用分级机制以及开展去中心化、关联化的认证。以粤澳跨境单牌车为例，过境车主身份属性中已有澳门身份

证，并不需要确切的身份证号码认证即可关联认证为澳门车辆。

针对跨境双方的多权威属性关系，建立通用的认证模型是构建跨境身份属性验证分级的基础、解决身份认证实际应用的关键。面向庞大数量的属性、众多的权威机构进行精确匹配，解决跨境双方或多方具有通配性的信任边界博弈问题是通用框架模型的能力瓶颈。研究和应用新型框架，开展属性的关联分级通用认证，支持数字身份的属性实现跨境动态关联分级和重构，确保跨境主体访问控制的跨境可信互认。多授权属性加密是代表性的访问控制模型<sup>[24]</sup>，在云授权方向获得广泛应用，能够提供理论支持框架；以太坊智能合约可提供去中心化、透明、可溯源的分布式认证框架；将两种技术结合，可支持构建适用跨境数据数字身份属性认证的通用信任框架。

## 三、去中心分布式跨境数字身份认证框架

本研究构建了一种去中心分布式跨境数据的数字身份框架，主要包括3个部分：基于区块链DID技术的分布式CA身份认证（BCA）机制<sup>[25,26]</sup>，属性联合认证关联分级的通用认证池（UCAP）模型，多授权属性级别的跨境身份认证访问控制加密（CT-MA-ABE）机制<sup>[27]</sup>。数字身份的所有权属于用户，用户可以选择可信第三方担保实体参与，以联合解决跨境双方的信任问题（见图1）。通过UCAP的属性匹配，用户可选择最小信息披露原则来提供给验证者，进而最大限度地保护隐私。通过UCAP的属性熵计算，深入挖掘隐性条件，实现身份属性的精准授权映射。

### （一）BCA机制

将区块链技术应用于身份认证，进而实现分布式的身份认证管理，这是BCA机制的研究出发点。BCA机制应用区块链技术的不可篡改性和分布式特性，能够解决中心化身份认证中可能存在的单点故障，适应更高层次的安全需求；提供对实体身份的映射能力，也可保证同一身份在各种应用中的分离，以可重构的身份标签、分级的授权机制来更好保护用户隐私。

传统证书的颁发机构、审核机构，认可且能对

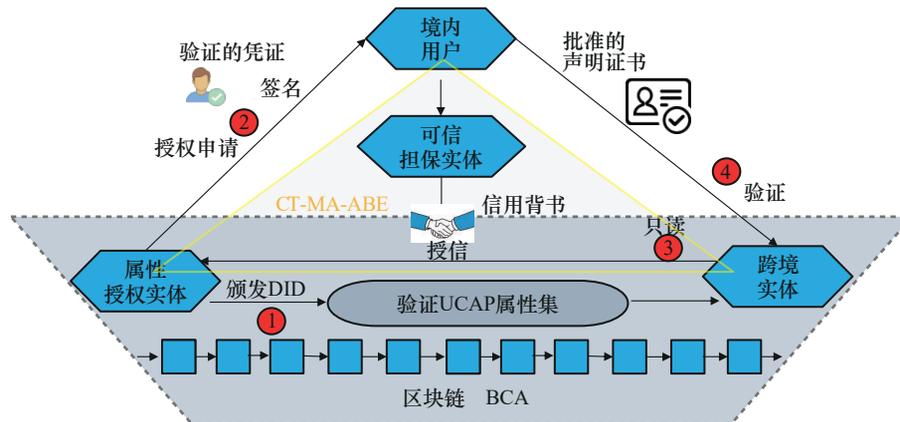


图1 去中心分布式跨境数字身份认证框架

用户身份属性进行核实授权的中介机构都是CA。预言机是将现实世界的数据（链下数据）传递到区块链上的机制。在跨境身份认证框架中，预言机可用于从外部数据源获取必要的身份验证信息并将之安全地传递到区块链上，以便智能合约执行相关操作。BCA 可视为在跨境环境下建立的网络基础设施、服务内容和节点，向区块链CA、预言机提供所需授信并促进两者的协同，既可保留区块链本身的安全属性，又通过预言机扩展功能形成高级的混合型智能合约。BCA 是属性匹配空间的容器，利用双线性配对实现全部的伪随机生成器功能<sup>[28]</sup>；基于智能合约中数据库管理的独特识别地址、具有抗干扰能力的代码运行能力，形成部署在链上时的高度透明性、安全性、防篡改性。

授权机构属于不同的法律框架，因而无法由信任第三方提供安全性和透明度。利用主链地址的唯一性来部署智能合约并进行交互，则分属不同领域的授权机构可核验对方提交的零知识证明来确保真实性。在本研究构建的框架下，利用区块链进行分属不同法律框架机构之间的通信，在链上部署智能合约。① 授权机构初始化零知识证明所需的公共参数，通过区块链分发并确保一致性。② 被验证方利用自身的私有信息生成包含身份属性合法性的零知识证明，无需泄露具体数据。③ 验证方通过智能合约调用零知识验证算法，对零知识证明进行有效性和规则匹配等检查。④ 验证结果以加密方式反馈至被验证方，通过预言机<sup>[29]</sup>生成并分发密钥，密钥用作授权机构的身份认证，允许指定的信任实体进行认定和签署。通过上述过程，授权机构在无需共享敏感信息的条件下完成身份验证，平衡了数据隐私

保护与真实性保障需求，增强了跨境身份认证的合规性与可追溯性。

## （二）UCAP 模型

UCAP 模型包含了跨境数字身份认证分类分级体系，为不同敏感度的数据提供分层次的保护机制（见图2）。参考《数据安全技术数据分类分级规则》（GB/T 43697—2024）<sup>[30]</sup>，根据数据的敏感度、业务价值、风险评估结果，将数据划分为多个保护层级，为每个层级设定相应的访问权限和安全措施。

### 1. 构建属性关联分级

分析身份属性的类型、用途、潜在风险，确定身份属性的敏感度。用户的身份认证信息、财务数据等敏感度较高的数据，将被赋予较高的保护级别。按照业务需求与合规要求，评估不同类型数据的潜在风险；在跨境数据流动场景中，数据泄露或非法访问的风险通常更高。属性关联分级的构建过程，重在形成身份属性匹配空间的分级分类表达式，与空间中动态稳定结构的迭代更新相匹配<sup>[31]</sup>，可借鉴知识图谱和图计算方法。

知识图谱<sup>[32,33]</sup>用于存储和推理实体之间的关系，在跨境身份认证框架中用于构建属性熵空间，分析授信属性的关联性和相关性，支持形成属性分级分类标签以及进一步的多层次属性关联分级结构。基于图形的机器学习、深度学习方法，利用知识图谱中的结构和属性信息，对新关系进行预测和推理，将更深入地理解并利用复杂的关系，为各种应用场景提供解决方案。根据属性的关联性分析和结构稳定性评估结果，制定动态更新策略，诸如添加、删除、调整、匹配空间中的节点和边，更好地反映实

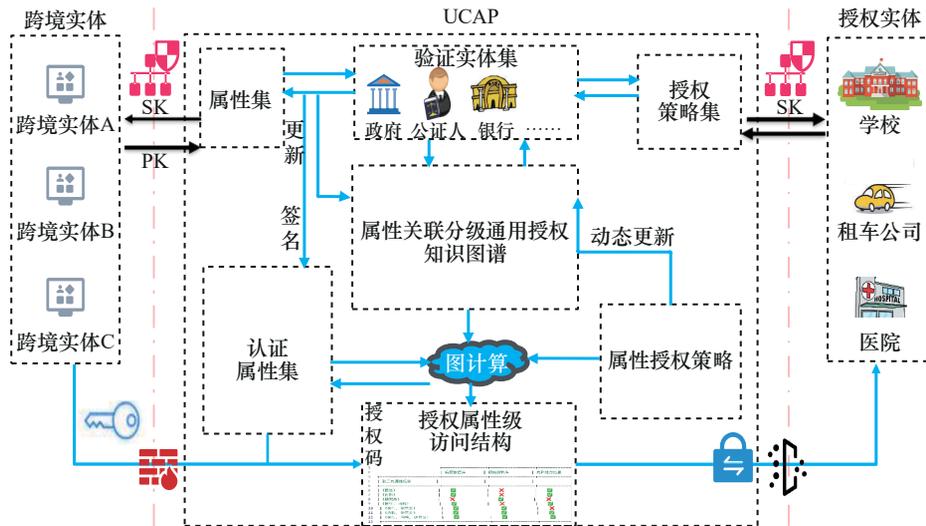


图2 UCAP 模型结构图  
注：PK 表示公钥；SK 表示私钥。

体之间的关系；基于动态更新策略，对匹配空间的结构进行迭代更新。构造属性关系数据库，建立 UCAP 通用库，与多个权威机构的属性加密相匹配。

### 2. 建立属性隐私行为评估模型

采用基于多层模糊综合评估的隐私保护方法<sup>[34]</sup>建立属性隐私行为评估模型，用于量化跨境数据流动中的隐私风险，为数据分类分级提供依据。通过模糊逻辑评估不同场景下的隐私需求，结合隐私权理论的“目的限制原则”（即数据收集和使用应仅限于特定的合法目的），从数据生命周期的整体视角出发，提供更为精准的隐私保护策略。

在模型设计时，需要采集用户的历史行为数据、隐私偏好、跨境数据流动的特征信息。应用机器学习、数据挖掘等技术，预测用户在不同场景下的隐私保护需求，评估不同条件下的隐私风险<sup>[35,36]</sup>。为每个用户或数据类型生成个性化的隐私保护策略，提供更加精细化的跨境数据流动隐私保护能力。根据风险评估结果，为每种数据类型确定适当的保护层级；采取访问控制、算法加密、数据脱敏等保护措施，确保数据在跨境流动过程中得到充分保护。

面向跨境数字身份认证分类分级构造的 UCAP 模型，创建跨境数据分类分级清单，详细记录数据的来源、类型、敏感性、传输需求，将关键数据分配至不同安全级别，有效保护跨境身份认证中的敏感信息；涵盖数据分类清单生成、数据存储与访问控制、数据处理与分析、跨境数据流动与调度、接

口管理、数据安全与隐私保护、数据合规在内的全过程，支持构建完整的数据属性分级分类体系（见图3）。① 数据存储与访问控制模块采用严格的安全协议和访问策略，仅允许授权用户访问高敏感性数据。② 数据处理与分析模块引入模糊匹配、人工审核等机制，提升数据处理效率、降低数据泄露风险，使用关键字分类系统来快速识别并处理高风险数据。③ 跨境数据流动与调度模块用于监控和管理数据流动，确保数据传输的合规与高效，兼顾资源配置优化。④ 接口管理模块通过应用程序编程接口（API）与群控接口实现跨境数据安全传输和集中管理身份认证及访问权限。⑤ 数据安全与隐私保护模块依托态势感知平台进行数据安全方面的实时监控，防范隐私泄露和滥用风险。⑥ 数据合规模块利用大数据模型进行合规风险分析，确保数据传输符合相关法律法规。

在跨境数据流动的背景下，UCAP 模型能够识别数据的敏感性和重要性，数据的拥有者可以根据识别的结果来存储和处理相应的数据。在实际操作中，跨境数据应按照性质和敏感性进行分类。例如，医疗健康数据、金融信息等高敏感性数据优先考虑本地化存储，避免潜在的法律风险和隐私泄露；公开市场的调查数据等低敏感性数据可采用全球存储的方式，充分提高数据的利用效率。需要注意的是，UCAP 模型收集属性数据目的是捕捉属性匹配的规则，无需存储个体的数据，因而不存在跨

境泄露隐私的情况；最终在跨境交互时，会提取平台双方 UCAP 一致的属性授权匹配对，作为数字身份授权的基础。

(三) CT-MA-ABE 机制

跨境身份数据的授权与访问控制是保障数据安

全、实施隐私保护的关键环节。本研究提出了一种跨境数据属性的多授权机构控制机制，即 CT-MA-ABE（见图4）。该机制将区块链技术与智能合约相结合，实现对身份数据的去中心化管理和精细化访问控制。

CT-MA-ABE 算法与 UCAP 的通用验证权威池

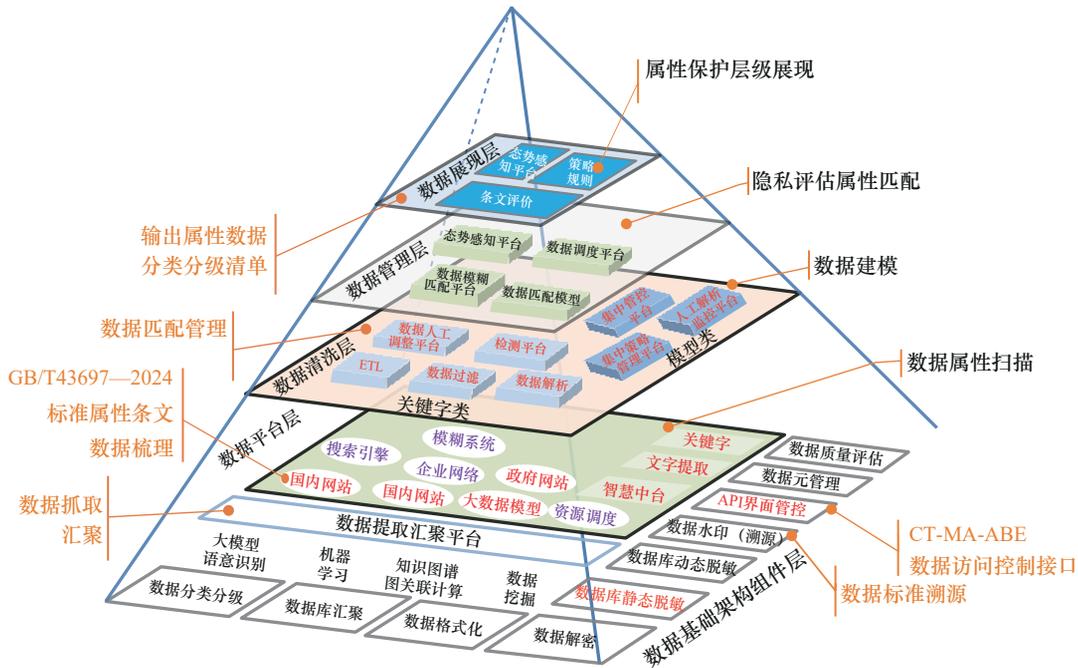


图3 跨境数字身份认证的分类分级构造模型

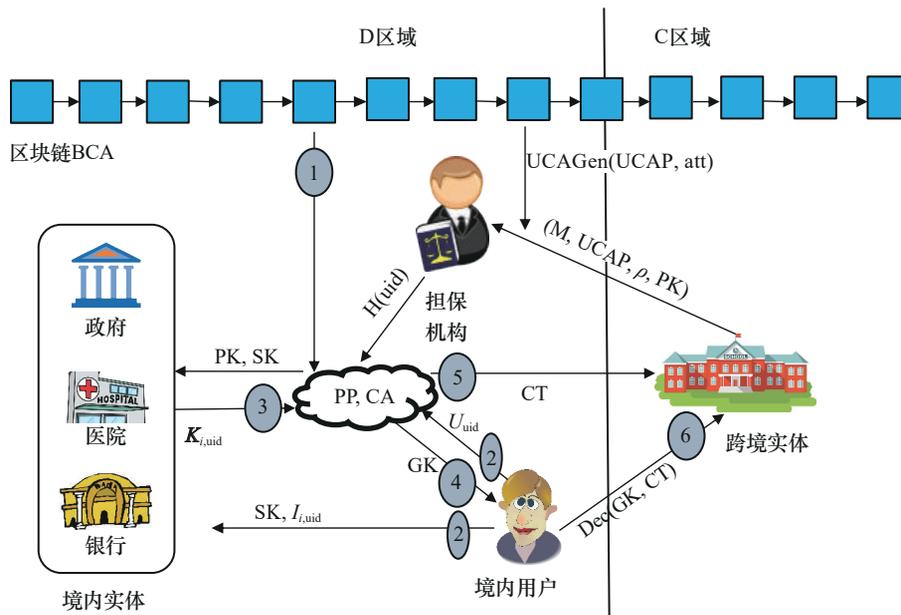


图4 CT-MA-ABE 属性访问控制结构

注：PP表示公共参数；CT表示授信跨境实体；Dec表示解密；H(uid)表示哈希用户标签；M表示访问结构；ρ表示属性映射；I表示属性集合；K表示属性的密钥；GK表示全局密钥；UCAGen(UCAP, att)表示基于UCAP和属性att的算法函数，从BCA取出相关属性。

相结合，实现信任身份属性的多级验证，提高了验证效率和身份属性管理的可靠性。算法中引入了“担保人”这一具有权威机构特征的角色，解决了跨境交互中的信任问题，为跨境身份认证提供了兼顾实用性和效率的支持能力。

基于跨境双方属性授权信任边界的博弈策略，重在实现双方在属性授权方面的信任与合作。①开展属性分级分类标签化评分，建立多层次的属性关联分级结构，为属性授权提供详细的内容指导，作为后续授权决策的参考依据。②引入博弈算法，促进双方在属性授权方面的动态平衡和调整，尤其是授权决策能够及时根据双方的属性进行调整，增强授权策略的灵活性和适应性。③配置动态更新结构搜索空间的约束模型，实现授权空间的自适应调整，使授权决策适应环境变化，更好满足双方的实际需求。

#### 四、跨境数字身份认证框架的应用难点与解决方案

去中心分布式跨境数字身份认证框架的推广应用仍然存在一些技术性难题，涉及加密计算的复杂度、各种系统的适配复杂度、去中心化和中心化博弈的边界问题等。需要在确保身份属性完整且精确匹配的情况下，持续提升加密算法的性能，快速准确地执行跨境身份认证的通用任务。针对性提出API模型以及相应的评估标准，进一步探讨跨境数字身份认证模型在不同国家法律体系下的解决方案。

##### （一）属性关联异构分级的效率和精度

UCAP模型的效率受跨境数据交互规模的影响，当数据量庞大且分散时，UCAP在处理身份属性的关联异构分级时将出现效率下降的情况。UCAP需要在大量数据中进行属性的匹配和关联，显著扩大的数据规模会导致搜索复杂度大幅增加，而复杂的搜索可能降低属性匹配的精度。

利用知识图谱建立匹配库，描述匹配空间的多态关系，据此构建复杂度模型。在不断的积累和迭代后，权威机构的属性分级将趋于稳定。使用图计算技术检索权威机构的属性匹配空间，在增量式更新后扩展到全局属性的分层定义，实现动态稳定。

构建匹配空间的重构更新机制，实现属性关联随时间的自动调整。当属性分级、匹配量级达到一定程度后，所需的计算规模会下降。知识图谱的属性关联分级表达、匹配空间动态稳定结构的迭代更新、基于图计算的属性空间库时间计算等的综合运用，为解决跨境身份认证中的属性交互问题提供了有效的解决方案。

##### （二）跨境双方属性授权信任边界的博弈

跨境身份认证中缺失实体的中间诚信人角色，因而双方属性授权信任边界的博弈成为重要内容。不同地区和组织在身份属性的授权标准与信任边界方面可能存在分歧，导致进一步的博弈和冲突。例如，一方可能要求更高的隐私保护标准，而另一方则更注重数据的高效流动，需要采取技术手段调和这种矛盾。

探索基于属性分级分类标签化评分的多样性控制机制，明晰属性标记且可量化。例如，将“姓名”“身份证号”等属性划分为高敏感度类别，赋予较高权重；将“职业”“兴趣”等属性划分为低敏感度类别，赋予较低权重。通过这种方式，属性标记得以明晰且可量化，为后续的博弈分析提供数据基础。

基于属性标签化评分，建立通用的授权信任博弈评估函数。该函数综合考虑双方的利益诉求，通过数学模型量化信任边界的分歧点，为构建属性分层级的稳定模式提供基础方法，确保模型的通用性和适应性。例如，利用博弈论中的纳什均衡原理，计算双方在属性授权中的最优策略。

采用博弈算法中跨境双方利益最大化原则，计算标签化后的属性评分，通过迭代优化以明确最优的通用结构。

##### （三）认证框架的应用封装API模型

本研究设计了一种应用封装API模型（见图5），将计算量控制在用户端，降低大量交互时网络的属性匹配计算资源开销。该API模型采用分层架构，由服务器端的区块链层、API调用层及本地应用层构成。

服务器端的区块链层作为核心模块，部署在公网且不受框架双方控制，主要承担属性的智能匹配计算任务。利用区块链的分布式账本特性，确保数据的不可篡改性和透明可追溯性。通过智能合约实

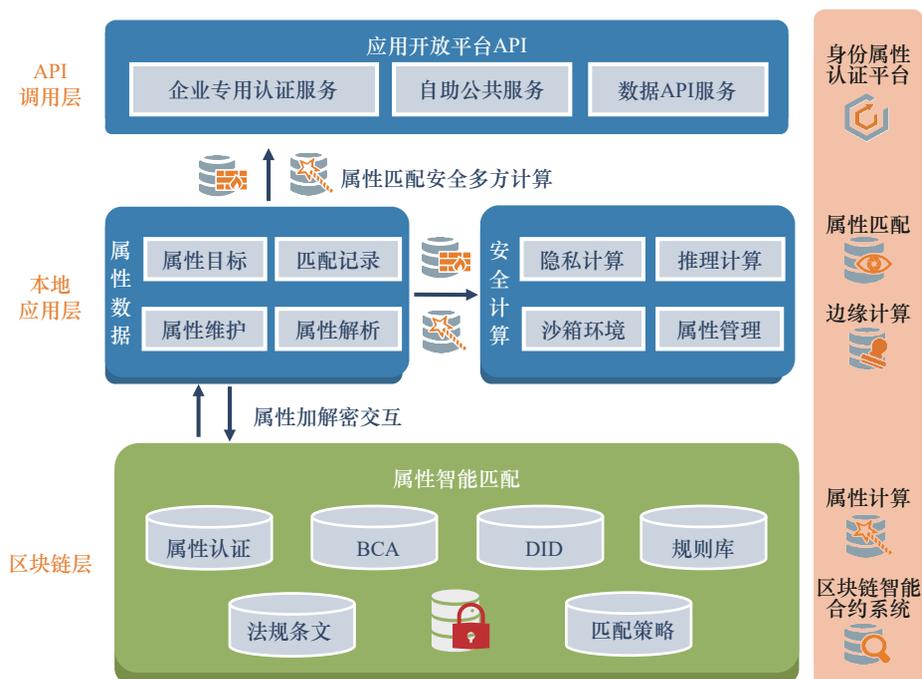


图5 分布式数字身份应用封装API模型

现属性匹配规则的自动化执行，减少人为干预。相应的计算量虽然较大，但位于后台进行，不会影响前端身份属性交互验证的性能。服务端在验证用户请求后，将加密的匹配规则通过API调用层推送到终端用户。

API调用层作为服务器端与用户端的“桥梁”，采用轻量级数据传输协议，支持多种编程语言和平台调用。通过加密通信保障数据在传输过程中的安全性。API调用层能够高效、安全地将匹配规则传递到用户端，同时支持动态更新以适应不断变化的属性匹配需求。

本地应用层在用户端执行属性匹配计算，终端用户为了减轻计算压力、提高系统响应速度、在大量交互时维持性能，可采取利用本地计算能力、部署边缘计算节点以就近处理属性规则数据、优化智能合约代码、实施负载均衡、使用缓存机制、预处理用户端数据、动态调整计算资源分配等策略。

#### （四）认证框架的评估标准和实施路径

本研究提出了评估跨境身份认证框架的核心标准，确保跨境数字身份认证框架的技术性能、安全性、兼容性、法规合规性达到预期目标，可在跨境双方有效运行。相关评估标准提供了技术优化方向，为制定实施路径提供了参考依据。针对加密计算的

时间复杂度问题，以计算完成率、平均响应时间来衡量加密计算的效率。系统适配性的评估重点在于不同系统之间的接口兼容性、数据格式的统一性，可促进框架的广泛适用。以框架在不同场景下的适应能力来评价去中心化与中心化的平衡状态，可更好满足多样化的业务需求和安全要求。认证成功率是衡量身份认证系统有效性的核心指标，突出匹配精度、处理效率：前者由误匹配率、匹配成功率来衡量，后者通过处理时间、系统资源消耗来评估。

跨境数字身份授权分级分层还面临着其他挑战，如法律规章差异、数据敏感度差异、管理模式选择、数据源复杂性、动态授权管理、隐私保护与数据利用平衡、技术标准不统一等，不仅影响跨境数据的流动效率，而且增加身份认证和授权系统的实施难度。例如，《通用数据保护条例》（欧盟，2018年）要求跨境数据传输必须遵守数据最小化原则并确保用户知情同意，《中华人民共和国个人信息保护法》（2021年）强调跨境数据传输需进行安全评估并采用数据本地存储方式，美国的州、联邦层面与数据相关的法规差异较大。这就要求跨境框架具有良好的适应性和动态调整能力，在数据分级分层管理中支持灵活的合规模式，使授权系统兼顾跨国法规的合规性、数据流动的高效性及安全性。还需在全球范围内加强合作，推动技术创新与政策

调整,构建兼容、高效、安全的跨境身份认证与授权的标准体系。

在构建标准体系的过程中,最佳的实施路径为:率先建立本国的标准体系,然后在一定区域内、若干国家和地区间建立共识,如在东南亚国家联盟的成员国之间、我国粤港澳大湾区内进行应用推广并不断积累经验;通过试点形成应用范例,在实践中逐步扩大不同国家体系的数据格式融入范围,最终形成具有广泛接受度的国际通行标准。

## 五、结语

本文针对跨境数据流动中的隐私保护与身份认证问题,通过分析跨境数据流动的法规框架、现有身份认证与授权机制、隐私保护技术手段以及面临的挑战,提出了一种基于隐私保护的去中心化分布式跨境数字身份认证框架。该框架应用了区块链和智能合约技术,保障了跨境数据传输的安全。利用知识图谱技术识别身份属性之间的关联规律,构建了属性熵空间,并结合图计算监测隐私行为变化,为跨境身份属性的分类分级提供了新的解决方案。此外,该框架制定了相应的属性授权与访问控制策略,提高了跨境数据流动的安全性以及保护隐私与合规,为不同敏感度的数据属性提供了差异化的保护层级。

本研究提出了一种去中心分布式跨境数字身份认证框架,引入数据分类分级策略,为多种场景下的跨境身份认证需求提供了系统化的理论支持与技术方法。相关框架具有良好的实践应用潜力,可为管理部门和企业跨境数据流动、隐私保护方面的实践提供参考;在应用于跨境数字身份验证场景外,可合理简化后应用于医疗、金融等行业的数据共享。后续研究将侧重完善跨境数字身份认证体系,加强去中心化技术的创新应用研究,探索在属性语义解析与数据管理中深度嵌入人工智能大模型,为全球数据治理提供智能化、多元化的技术支撑。

也要注意,在技术快速发展、跨境数据流动需求不断变化的背景下,去中心分布式跨境数字身份认证框架的建设与实施策略仍有提升空间。可提高属性关联的异构分级精度及效率,优化隐私计算方法,开发更精细的动态信任边界算法,实现隐私保护与系统效率之间的最佳平衡。在平台应用方

面,可深入研究区块链、智能合约技术在不同司法辖区的适配性,不同平台之间的互操作性,为跨境数据流动提供完善的技术基础。针对跨境数据流动的法律规章差异明显、数据主权存在冲突、合规性管理机制尚不完善的现状,可从技术与政策协同的角度进一步优化实施路径,如率先凭借我国海量的跨境数据交易规模优势建立中国标准,然后逐步推动形成具有广泛适用性的通用跨境数据治理国际标准。

### 利益冲突声明

本文作者在此声明彼此之间不存在任何利益冲突或财务冲突。

**Received date:** October 8, 2024; **Revised date:** November 27, 2024

**Corresponding author:** Qi Jiayin is a professor from the Cyberspace Institute of Advanced Technology, Guangzhou University. Her major research fields include cross-border data, cyber security. E-mail: qijiayin@139.com

**Funding project:** Chinese Academy of Engineering project “Study on Governance Rules and Strategies for Coordinated Development and Security of Data” (2023-XBZD-20-03); National Natural Science Foundation Project (72293583, 72293580); Macao Foundation’s Academic Funding Program (G01156-2309-262)

### 参考文献

- [1] 促进和规范数据跨境流动规定 [EB/OL]. (2024-03-22)[2024-12-15]. [https://www.gov.cn/gongbao/2024/issue\\_11366/202405/content\\_6954192.html?xxgkhide=1](https://www.gov.cn/gongbao/2024/issue_11366/202405/content_6954192.html?xxgkhide=1). Regulations on promoting and standardizing cross-border data flow [EB/OL]. (2024-03-22)[2024-12-15]. [https://www.gov.cn/gongbao/2024/issue\\_11366/202405/content\\_6954192.html?xxgkhide=1](https://www.gov.cn/gongbao/2024/issue_11366/202405/content_6954192.html?xxgkhide=1).
- [2] European Commission. New practical guide to the *Data governance act* [EB/OL]. (2024-09-24)[2024-12-25]. <https://digital-strategy.ec.europa.eu/en/library/new-practical-guide-data-governance-act>.
- [3] Carovano G, Finck M. Regulating data intermediaries: The impact of the *Data governance act* on the EU’s data economy [J]. *Computer Law & Security Review*, 2023, 50: 105830.
- [4] 陈嘉丽. 个人数据跨境流动法律规制研究 [D]. 北京: 北方工业大学(硕士学位论文), 2022. Chen J L. Research on legal regulation of cross-border flow of personal data [D]. Beijing: North China University of Technology (Master’s thesis), 2022.
- [5] 网络数据安全条例 [EB/OL]. (2024-09-24)[2024-12-15]. [https://www.gov.cn/zhengce/zhengceku/202409/content\\_6977767.htm](https://www.gov.cn/zhengce/zhengceku/202409/content_6977767.htm). Network data security management regulations [EB/OL]. (2024-09-24)[2024-12-15]. [https://www.gov.cn/zhengce/zhengceku/202409/content\\_6977767.htm](https://www.gov.cn/zhengce/zhengceku/202409/content_6977767.htm).
- [6] 焦志伟, 吴正豪, 徐亦佳, 等. 基于隐私保护的分布式数字身份认证技术研究及实践探索 [J]. *信息通信技术与政策*, 2024 (1): 59–66. Jiao Z W, Wu Z H, Xu Y J, et al. Research and practice of decen-

- tralized digital identity authentication technology based on privacy protection [J]. *Information and Communications Technology and Policy*, 2024 (1): 59–66.
- [7] Liu Y Z, Zhao B Y, Zhao Z D, et al. SS-DID: A secure and scalable Web3 decentralized identity utilizing multilayer sharding blockchain [J]. *IEEE Internet of Things Journal*, 2024, 11(15): 25694–25705.
- [8] “数字湾区”建设三年行动方案 [EB/OL]. (2023-11-07)[2024-12-15]. [http://www.gd.gov.cn/zwgk/gongbao/2023/31/content/post\\_4287722.html](http://www.gd.gov.cn/zwgk/gongbao/2023/31/content/post_4287722.html).  
Three-year action plan for the construction of “digital bay area” [EB/OL]. (2023-11-07)[2024-12-15]. [http://www.gd.gov.cn/zwgk/gongbao/2023/31/content/post\\_4287722.html](http://www.gd.gov.cn/zwgk/gongbao/2023/31/content/post_4287722.html).
- [9] Hummel P, Braun M, Tretter M, et al. Data sovereignty: A review [J]. *Big Data & Society*, 2021, 8(1): 2053951720982012.
- [10] 王文泽. 我国数据分类分级保护法律制度的完善 [D]. 长春: 吉林大学(硕士学位论文), 2023.  
Wang W Z. Perfection of China’s legal system of data classification and classification protection [D]. Changchun: Jilin University (Master’s thesis), 2023.
- [11] Samir E, Wu H Y, Azab M, et al. DT-SSIM: A decentralized trustworthy self-sovereign identity management framework [J]. *IEEE Internet of Things Journal*, 2022, 9(11): 7972–7988.
- [12] Lin I C, Yeh I L, Chang C C, et al. Designing a secure and scalable data sharing mechanism using decentralized identifiers (DID) [J]. *Computer Modeling in Engineering & Sciences*, 2024, 141(1): 809–822.
- [13] Hummel P, Braun M, Tretter M H, et al. Data sovereignty: A review [J]. *Big Data & Society*, 2021, 8(1): 205395172098201.
- [14] Jajodia S, Samarati P, Yung M. *Encyclopedia of cryptography, security and privacy* [M]. Berlin: Springer Berlin, 2021.
- [15] Deng H T, Liang J W, Zhang C, et al. Future DID: A fully decentralized identity system with multi-party verification [J]. *IEEE Transactions on Computers*, 2024, 73(8): 2051–2065.
- [16] Naik N, Jenkins P. uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain [C]. Vienna: 2020 IEEE International Symposium on Systems Engineering (ISSE), 2020.
- [17] Khovratovich D, Law J. Sovrin: Digital identities in the blockchain era [EB/OL]. [2024-12-25]. <https://sovrin.org/wp-content/uploads/AnonCred-RWC.pdf>.
- [18] Bai Y R, Leo H, Li S Z, et al. Decentralized and self-sovereign identity in the era of blockchain: A survey [C]. Espoo: 2022 IEEE International Conference on Blockchain, 2022.
- [19] Dunphy P, Petitcolas F A P. A first look at identity management schemes on the blockchain [J]. *IEEE Security & Privacy*, 2018, 16(4): 20–29.
- [20] Badirova A, Dabbaghi S, Moghaddam F F, et al. A survey on identity and access management for cross-domain dynamic users: Issues, solutions, and challenges [J]. *IEEE Access*, 2023, 11: 61660–61679.
- [21] Singh C, Thakkar R, Warraich J. IAM identity access management—Importance in maintaining security systems within organizations [J]. *European Journal of Engineering and Technology Research*, 2023, 8(4): 30–38.
- [22] Regateiro D, Pereira Ó, Aguiar R L. On the application of fuzzy set theory for access control enforcement [C]. Madrid: Proceedings of the 14th International Joint Conference on e-Business and Telecommunications, 2017.
- [23] 吴国英, 杨林, 邱旭华. 可信身份认证平台的构建 [J]. *信息安全研究*, 2022, 8(9): 888–894.  
Wu G Y, Yang L, Qiu X H. Construction of a trusted authentication platform [J]. *Journal of Information Security Research*, 2022, 8(9): 888–894.
- [24] Dixit S, Joshi K P, Choi S G. Multi authority access control in a cloud EHR system with MA-ABE [C]. Milan: 2019 IEEE International Conference on Edge Computing (EDGE), 2019.
- [25] Idrees S M, Nowostawski M. *Blockchain transformations* [M]. Cham: Springer Nature Switzerland, 2024.
- [26] Dash S P, Jena A K. An efficient approach for optimizing the CA selection search space in a blockchain network [C]. Bhubaneswar: 2024 International Conference on Emerging Systems and Intelligent Computing (ESIC), 2024.
- [27] Chen J, Lu F, Liu Y Z, et al. Cross trust: A decentralized MA-ABE mechanism for cross-border identity authentication [J]. *International Journal of Critical Infrastructure Protection*, 2024, 44: 100661.
- [28] Hatami P, Hoza W. *Paradigms for unconditional pseudorandom generators* [M]. Boston: Now Foundations and Trends, 2024.
- [29] Kosuge H, Xagawa K. Probabilistic hash-and-sign with retry in the quantum random oracle model [M]. Cham: Springer Nature Switzerland, 2024.
- [30] 全国网络安全标准化技术委员会. 数据安全技术 数据分类分级规则(GB/T 43697—2024) [S]. 北京: 中国标准出版社, 2024.  
National Technical Committee 260 on Cybersecurity of Standardization Administration of China. Data security technology—Rules for data classification and grading (GB/T 43697—2024) [S]. Beijing: Standards Press of China, 2024.
- [31] Ju W, Yi S Y, Wang Y F, et al. A survey of graph neural networks in real world: Imbalance, noise, privacy and OOD challenges [EB/OL]. (2024-03-07)[2024-12-25]. <https://arxiv.org/abs/2403.04468v1>.
- [32] Liu J, Shang L T, Su Y T, et al. Privacy-preserving multi-source cross-domain recommendation based on knowledge graph [J]. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 2024, 20(5): 1–18.
- [33] Chen C C, Zheng F, Cui J, et al. Survey and open problems in privacy-preserving knowledge graph: Merging, query, representation, completion, and applications [J]. *International Journal of Machine Learning and Cybernetics*, 2024, 15(8): 3513–3532.
- [34] Zhang X L, Xu R. A multi-level fuzzy comprehensive evaluation method for knowledge transfer efficiency in innovation cluster [J]. *Mobile Information Systems*, 2022 (9): 1–12.
- [35] Wang J T, Zhu Y, Wang Y X, et al. A privacy-friendly approach to data valuation [EB/OL]. (2023-09-22)[2024-12-15]. <https://openreview.net/forum?id=FAZ3i0hvm0>.
- [36] Zhang X Y, Xu H Y, Ba Z J, et al. PrivacyAsst: Safeguarding user privacy in tool-using large language model agents [J]. *IEEE Transactions on Dependable and Secure Computing*, 2024, 21(6): 5242–5258.