DOI 10.15302/J-SSCAE-2024.03.016

数字社会身份管理的现状、问题及对策

于锐*，邓晨，赵洋，陆洪波，邱旭华，冯思琦

（公安部第一研究所，北京 100048）

摘要：当前，我国正全面迈入数字社会，对国家数字化管理能力提出新的要求。身份管理作为新时期数字中国建设和社会安全保障的重要基础支撑，直接关系到国家安全、社会安全和个人安全。本文研判了数字身份支撑数字社会管理能力发展面临的主要挑战，剖析了数字身份管理的基本现状与面临的关键问题，提出了构建安全可靠的数字社会身份管理能力发展目标与主要任务，分析了构建中国特色数字身份体系关键技术的发展趋势。研究建议，加强顶层设计、制定实施路线图，完善相关法律法规，构建“中心化管理+分布式认证”混合架构的数字身份管理体系，强化数字身份监管能力，加强参与方规范管理，推动生态合作，积极参与全球治理，以此推动数字身份体系建设，助力数字社会管理行稳致远。

关键词：数字身份；数字社会；密码学技术；大模型；分布式数字身份

中图分类号：C3　　**文献标识码：**A

Digital Social Identity Management: Current Status, Problems, and Countermeasures

Yu Rui*, Deng Chen, Zhao Yang, Lu Hongbo, Qiu Xuhua, Feng Siqi

(First Research Institute of the Ministry of Public Security of PRC, Beijing 100048, China)

Abstract: Currently, China is undergoing a comprehensive transition toward a digital society, which has placed renewed emphasis on the need for robust national-level digital management capabilities. Identity management serves as a foundational support for the construction of Digital China and social security in the new era, with direct implications for national, social, and individual security. This study explores the major challenges faced by the digital identity system in supporting digital society governance, analyzes the current status and key problems of digital identity management, proposes the development goal and major tasks of building a secure and reliable digital social identity management system, and clarifies the trend of key technologies in establishing a digital identity system with Chinese characteristics. Furthermore, we propose the following suggestions: (1) strengthening top-level design to formulate the development strategy and implementation roadmap of digital identity, (2) improving related laws and regulations, (3) establishing a digital identity management system with a hybrid architecture featuring centralized management and distributed authentication, (4) strengthening digital identity supervision capabilities, (5) enhancing the standard management of participants, (6) fostering ecological cooperation, and (7) actively engaging in global governance, thus to promote the development of the digital identity system and facilitate the long-term and stable development of digital society administration.

Keywords: digital identity; digital society; cryptography technology; large model; decentralized identity

收稿日期：2024-04-28；**修回日期：**2024-05-24

通讯作者：*于锐，公安部第一研究所研究员，主要研究方向为公安信息化建设与应用、国家法定证件与生物特装识别、网络可信身份认证；E-mail: yr9041@163.com

资助项目：中国工程院咨询项目“科技创新支撑国家安全体系和能力现代化战略研究”(2022-XBZD-28)

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

当前，我国正全面迈入数字社会，数字化转型全面渗透和深刻影响着经济运行、社会活动及国家治理的各个环节。中国互联网络信息中心发布的第53次《中国互联网络发展状况统计报告》显示，截至2023年6月，我国网民规模已达10.79亿人，大量经济活动、金融活动和社会公共活动都通过网络进行，网络社会逐渐形成新的生态，传统社会管理模式面临海量用户和数据管理挑战。

数字身份作为数字社会的入口，是重塑数字社会经济发展模式和国家治理体系的基础条件和关键要素[1]，是塑造数字生态的关键基础，已经成为实现经济健康发展与社会和谐安全稳定的基石，并在数字经济、数字社会、数字国家建设中发挥至关重要的作用[2]。由于国家、企业、个人等不同主体对数字身份的多样性需求，以及不同地区、行业、领域的政策法规对数字身份的差异化要求，亟需建立数字身份管理体系。加强数字社会身份管理，有助于防范身份数据丢失、泄露等风险，降低互联网企业过度收集、留存个人信息乱象，有力打击网络犯罪、保护公民个人敏感信息，对保护国家安全、社会安全和个人安全具有重要意义，对推进国家治理体系和治理能力现代化、建设社会诚信体系也将发挥积极影响。纵观全球，世界主要国家高度重视数字身份对数字社会管理的重要支撑作用，加大对分布式数字身份、区块链、隐私计算等技术的支持力度，纷纷出台战略规划、完善法律法规、建立标准体系，大力推动数字社会身份体系建设，提升国家竞争力。

目前，我国已完成国家网上身份认证服务基础设施（以下简称“国家基础设施”）建设，具备了依托国家基础设施、以公民身份信息为信任根、建设中国特色数字身份体系，支撑数字社会管理服务的基础能力。但是，当前我国数字身份顶层设计仍有待加强，配套法律法规仍有待完善，数字身份安全事件仍时有发生，身份数据权益保护仍面临难题，身份数据合规流动仍存在困难，影响数字身份价值全面发挥。因此，本文提出数字社会身份管理能力的发展目标，分析数字身份体系建设所需的关键技术，并提出对策建议，以期为我国数字社会安全保障能力建设提供参考。

二、数字社会身份管理面临的主要挑战

在数字化时代的大背景下，数字身份对于维护网络空间安全、促进经济发展、保障社会秩序起到关键作用。随着技术进步和应用场景的扩展，数字身份管理面临着前所未有的挑战，主要涉及外部威胁、安全风险、监管挑战以及政策法规的适应性等。

（一）诸多矛盾叠加、风险隐患增多，数字身份管理面临威胁

新时期的一个重要特征就是诸多矛盾叠加、风险隐患增多，重大战略机遇期与多种风险高发期相互交织。与此同时，数字化活动不断渗透到现实生活的各个方面，其虚拟性、无国界、难追踪等特点带来了新的安全风险与挑战。一是一些别有用心的势力未进行网络实名身份认证，以虚拟数字身份对我国进行网络舆情渗透，利用社交媒体传播负面虚假信息，危害国家意识形态及政治安全。二是随着数字化的深入发展，网络攻击手段不断演化，对数字身份管理构成新的威胁，敌对势力利用先进的技术手段，如零日攻击、高级持续性威胁攻击等，针对关键信息基础设施进行渗透，窃取身份验证数据，严重危害政治安全、扰乱社会秩序、侵害公私财产安全。2022年9月，西北工业大学遭受的非法入侵事件，凸显了加强身份认证系统安全性的紧迫程度。

（二）个人身份关联数据全生命周期安全问题长期存在

数字身份关联着海量的个人行为、偏好和生物特征等个人敏感数据，这些数据的全生命周期安全管理是数字身份应用领域亟需解决的复杂问题。一是传统的数字身份存储模式，由于其中心化的架构，对数据权益构成重大威胁。一旦身份凭证数据被寻求数据商品化的组织利用，庞大的数字身份生态系统可能会增加个人数据被市场化甚至用于违法犯罪的风险。二是个人敏感数据在共享流转过程中面临被滥用的风险。攻击者可能利用“中间人”攻击等手段，劫持个人数字身份信息，进而侵犯个人的金融资产。三是口令存在泄露失控风险。通过社会工程学等手段，攻击者能够轻易获取并滥用用户账户口令。从个人用户到大型企业，数据泄露的风险无处不在，这要求我们采取更为严格的安全措施

来保护用户身份信息。

（三）社会治理工作对数字身份监管提出新要求

在数字化转型的浪潮中，电信诈骗等网络犯罪手法日益翻新，数字身份冒领冒用问题日益突出，社会治理体系正面临着前所未有的挑战。数字身份作为个体在网络空间的标识，其可靠性和真实性对于维护社会秩序和促进经济发展至关重要，强化数字身份监管要求势在必行。这不仅需要立法机构制定和完善相关法律法规，明确数字身份的使用规范和保护措施，还需要监管机构利用先进的技术手段，如人工智能、生物识别等技术，提升监管能力。此外，加强跨部门合作，建立统一的监管框架，也是提升监管效能的关键。在全面建设数字中国的大背景下，社会治理体系的数字化转型不仅要做技术层面的更新，也要对监管理念和方法进行全面革新，确保有效预防和打击网络犯罪，为数字经济的健康发展提供坚实保障。

（四）数据要素市场进入快速发展阶段，亟需解决个人数据安全合规流通难题

在《中华人民共和国网络安全法》《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》的联动推进下，我国数据要素市场进入安全合规发展阶段。《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》指出，建立健全个人信息数据确权授权机制，规范对个人信息的处理活动，保障使用个人信息数据时的信息安全和个人隐私，探索个人、企业、公共数据分享价值收益方式。数据安全合规是数据要素流通交易的底线和红线，面临着如下的机遇与挑战：一是现有法规制度强调数据的规范利用和隐私安全，不过各主体难以把握监管尺度和合规依据，参与数据流通顾虑大；二是商业机构对数据具有充分的决定权，用户对个人数据很难主动行使权利。当前，国外主要国家多将散落在不同机构的个人信息汇聚到个人数据账户中，方便用户自主管理和分享收益的新模式开始出现并逐步被推广应用[3,4]。

三、数字社会身份管理的基本现状与面临的关键问题

构建国家数字社会身份管理体系是关乎未来数字社会治理与新的数字生态架构建设的战略工作，不仅需要政府推动，也离不开多维度的技术创新。当前，国家基础设施充分运用先进技术手段，初步达到保障数字身份管理体系安全运行的基本要求。但正如前文所述，外部势力的攻击手段不断演变，数据泄露和滥用的风险日益增加，人工智能应用在身份认证中的“双刃剑”效应，以及与数字身份绑定的数据要素流转的复杂性等形势为数字社会身份管理带来新的挑战。数字身份管理在身份数据流转技术信任、身份数据密态共享、数字身份监管、个人数据确权授权等方面，仍存在较为突出的问题。

（一）数字社会身份管理现状

当前，国内外在数字身份管理领域的研究和实践正不断深化。国际上，许多国家和地区积极探索符合本地特点的数字身份管理模式，以适应全球化背景下的数据流通和身份认证需求。例如，欧盟通过《通用数据保护条例》，强化了个人数据保护，同时，也在推动数字身份的互操作性和跨境认证。美国则通过“网络空间可信身份国家战略”等项目，鼓励创新和安全的数字身份解决方案。

我国通过立法和政策引导，不断加强数字身份管理的规范性和系统性。目前，我国已具备较成熟的数字身份管理机制与丰富的技术应用，基本满足数字身份的管理需求。国家基础设施是整个数字身份管理体系的信任基础，是国家层面提供的权威、统一的认证源头，为进一步支撑不同信任等级的数字身份和个人数据跨层级、跨地域、跨系统、跨业务的关联、聚合与互认打下了坚实基础。

在此背景下，提升数字身份管理能力来支持国家政策落实是现阶段的研究重点。国家正在通过《“数据要素X”三年行动计划（2024—2026年）》等政策文件，大力推动数据要素价值的释放，其中数据要素流通是激发数据价值的关键。身份数据作为数字身份的核心，是连接各类个人数据的纽带，其安全性关乎到公民隐私安全、社会安全、政治安全，保障身份数据全生命周期的安全是数字身份管理的一项重要研究议题。此外，随着数字身份的广泛应用，对监管能力也提出了更高的要求，除了实施实名制等基本政策措施，监管机构正积极探索应用人工智能等前沿技术，构建更为高效和先进的监管策略。

（二）数字社会身份管理面临的关键问题

虽然数字身份管理已具备较为坚实的基础，但是随着技术的发展和应用场景的拓展，新的问题和挑战也随之而来，主要包括身份数据流转技术信任、身份数据密态共享、数字身份监管、个人数据确权授权等。

在身份数据流转技术信任方面，主要存在以下几点问题：一是缺乏多云环境数据流转的解决方案。随着云计算的广泛应用，跨云平台的身份数据流转需求日益增长[5,6]，解决方案的缺少限制了数字身份管理的灵活性和扩展性。二是多方联合风控计算性能受到制约。现行风控计算框架在多方参与时性能受限，参与方数量增加会导致性能急剧下降，成本呈指数级增长，严重制约了身份数据流转的效率。三是统一规范化的成本负担大。当多个需求方进行数据流通时，需要对接不同的隐私计算厂商，对中小企业来说成本过高。

目前，数据加密大多停留在存储和传输阶段，一旦涉及计算，数据往往需要回到安全性弱、容易失控的明文状态。在身份数据密态共享方面，主要面临两大挑战：一是数字身份在使用过程中，需要进行多次加解密操作，可能导致身份数据明文信息暴露，进而导致身份数据被非法窃取或泄漏[7]，特别是政务、金融、医疗等敏感信息密集行业，风险更为严峻。二是数据传输过程依托密码技术实现多方通信，但随着计算能力的提升，传统密码算法面临被破解的风险，进而可能导致个人隐私数据被窃取。这些挑战凸显了实现身份数据使用权的跨域管控和数据流转安全可控的紧迫性。

在数字身份监管方面也面临着重大挑战：一是用户数字身份画像难以快速整合，溯源时间长；数据规模不断增大，数字身份信息分散存放，要形成完整的数字画像，需要具备丰富的实践经验及高效的多源信息能力。二是非法势力利用深度伪造、人工智能等技术进行数字身份冒领、冒用事件层出不穷，增大了网络犯罪溯源及监管的难度。三是数字人、元宇宙等新业态带来新的数字身份监管问题。未来自然人可通过“数字分身”或以“中之人”的形式参与到虚拟世界，可能带来新型伦理危机和新型网络犯罪。

在个人数据确权授权方面存在以下问题：一是身份“信息孤岛”化、机构间彼此不互认。各部门、各行业自行规划分散建设的身份管理体系之间，身份信息难以互认，在不同场景下需要重复提供或验证身份信息，增加了认证成本以及个人数据泄露和滥用的风险。二是用户无法有效行使个人数据权利问题。用户数字身份的关键控制点即账号口令由机构控制，用户处于弱势地位，无法主动决定和管理个人数据。商业机构普遍采用“一揽子授权”、强制同意等方式，用户授权形同虚设，违规收集和使用个人数据现象普遍。

四、数字社会身份管理的目标与主要任务

（一）数字社会身份管理的目标

在数字化时代，数字身份管理已成为社会治理和个人隐私保护的重要基石。数字社会身份管理的目标是利用数据跨云互联、密态计算、大模型、分布式数字身份等新一代信息技术，打造安全可靠的、具有中国特色的数字身份管理体系，以适应多样化的应用场景，满足不同主体的身份管理需求，为数字社会的健康发展奠定基础。

一是创新数字社会治理能力。以数字身份为信任基础，推动数字社会治理向智能化、高效化和透明化转型，实现科学决策与精准施策，助力构建先进的数字社会治理体系。二是实现个人数据安全协同共享。在保护个人隐私的前提下，促进个人数据跨行业、跨机构、跨部门安全共享融合，满足社会治理的资源整合需求。三是增强数字社会风险防控能力。利用数字身份管理，及时准确感知群众需求和社会发展态势，提升预测预警预防和突发事件快速处置的能力，切实支撑公共安全风险防控体系关口前移。四是支撑数据要素流通。通过创新数字身份管理架构，消除“信息孤岛”，确保个人数据在合法、合规的框架内流通，促进数据资源的有效利用，推动数字经济的繁荣发展。

（二）数字社会身份管理的主要任务

为实现数字社会身份管理的目标，本文提出以下四项主要任务：一是建立安全可信的数字身份技术信任体系，发展身份数据的跨云密态流转和计算技术，实现数字社会广泛普惠的互联互通，同时研究大数据安全共享场景下密态化技术升级，降低密态技术使用门槛，推动密态化技术能力与业务服务融合便捷化。二是推进数字身份在数据隐私共享、数字社会治理方面发挥基础支撑作用，通过发展密

态计算技术，提供数字身份保障所需的高性能、高可用、高安全的密码算法能力，基本形成可信的国家数字身份认证安全保障平台和数据确权体系。三是发展人工智能技术辅助的数字身份监管技术，在数据安全合规的要求下，提升身份数据监管的精细化和智能化能力，进一步预防数字身份被利用的风险，防范个人信息泄露。四是将区块链和隐私计算等新技术融入国家数字身份体系，形成具有中国特色和国际标准特征、“中心化+分布式”混合架构[2]的多层级数字身份管理服务，建立“根身份+业务身份”的可信标识、属性凭证和个人数据账户一体化的先进数字身份体系，支持个人数据的自主授权和合规流通。

五、数字社会身份管理的关键技术

为解决数字身份管理面临的问题与挑战，本节将重点分析数据跨云互联、密态计算、基于大模型的数据身份监管以及分布式数字身份等关键技术，并探讨这些技术如何帮助解决数字身份管理的多样性需求和面临的挑战。

（一）数据跨云互联技术

作为身份数据密态流转的技术基础设施，数据跨云互联技术可以构建多云环境下安全可信、互联互通的身份数据托管平台，创新国家数字身份服务模式，依法合规管理数字身份，提升身份数据协同共享的安全能力，满足日趋严格的合规监管、日渐强化的政策引导以及日益旺盛的市场需求（见图1）。

数据跨云互联技术主要由隐私保护共享和匿名化技术组成。

1. 隐私保护共享技术

隐私保护共享网络是融合云环境下安全可信的数据互联互通密态流转网络，可提供数据的跨云互联和计算服务。网络上各个节点能够通过密态计算因子便捷、安全地进行数据流通融合。可依托隐私保护共享网络搭建全国身份数据密态流转技术基础设施，实现多方跨云数据互联互通和数字身份可信托管，支撑数据要素广泛、安全、可控地流转。

目前，隐私保护共享网络规模扩展仍受限，信任被破坏风险也较高。特别是对于中小企业，隐私保护共享技术的门槛高，同时缺乏隐私计算和数据密态相关技术人才，无法实现大范围落地和广泛应用。此外，目前隐私保护共享技术体系没有系统的指导性原则，可能会导致行业倾向于选择性能好但安全性差的技术路线，带来一定的安全风险。

2. 匿名化技术

《中华人民共和国个人信息保护法》指出，匿

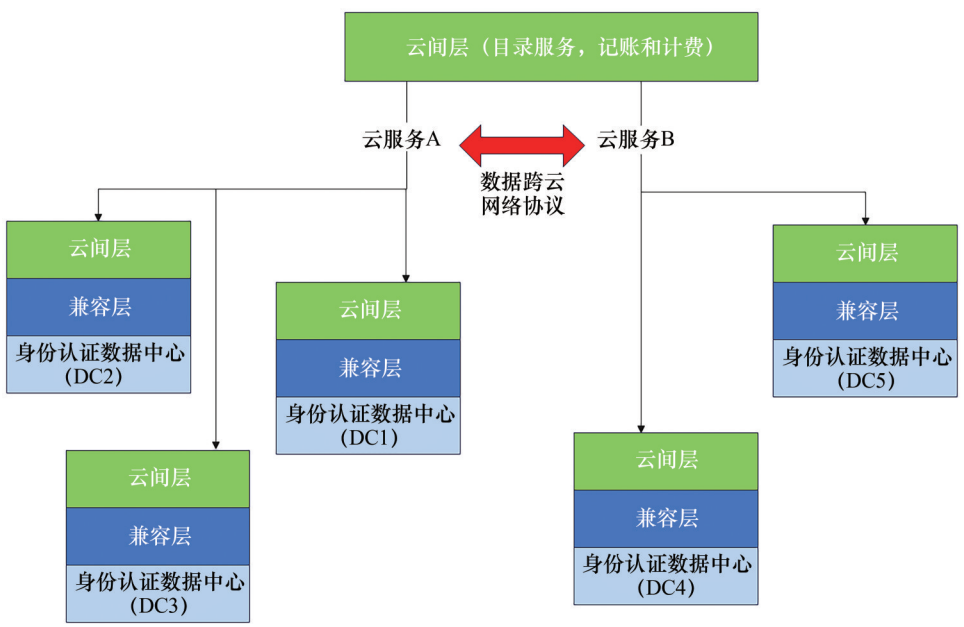

图1 数据跨云互联基础架构图

名化是指个人信息经过处理无法识别特定自然人且不能复原的过程，可以有效保障个人的隐私权。匿名化的过程通常是对数据进行模糊处理，如密码算法变换、添加噪声或者区间化。在开放的空间中（匿名化信息能够公开获取），匿名化和个体粒度的数据要素价值是两个不可调和的对立面，绝对匿名化的个体粒度信息实际上也不再具备使用价值。因此，在绝对匿名化会损失数据价值的情况下，相对匿名化逐渐成为匿名化技术未来的发展趋势。

相对匿名化指的是在不结合密钥、外部场景信息的情况下，无法恢复出个人身份的匿名化技术[8]。但是网络公共空间的相对匿名化数据看似与个人信息无关，通过深入的数学分析后仍能定位出个人信息，从而泄露个人信息。因此，如何在数据价值损失有限的前提下对属性信息进行模糊处理，并对匿名化数据与外部的交互进行严格管控，是需要尽快解决的问题。

（二）密态计算技术

数据密态的核心任务是要把加密延展到计算环节，意味着即使在运算期间，也不会出现明文数据（见图2）。密态计算技术包含同态加密技术、机密计算技术等。

1. 同态加密技术

同态加密技术能够在不受信任的第三方处理者、不完全信任的计算环境中实现身份数据密文计算。基于同态加密算法，数据经过加密变为密文之后，用户对密文进行某种特定的计算再解密后得到的明文，等同于直接对明文进行相应的计算。

近几年，国际商业机器公司、微软公司、阿里巴巴集团等国内外多家企业开始加大对同态加密技术的研究和应用，但仍然存在着效率与通用性的矛盾。一方面，支持任意运算类型的“全同态算法”的运算效率、密钥数据量和密文数据量均难以满足实际应用需要；另一方面，算法效率较高的半同态算法在国际上已有国际标准化组织制定的标准（支持加法运算的Paillier算法、支持乘法运算的ElGamel算法），国内也提出了基于国密算法的半同态算法，但该算法不支持浮点数运算、比较大小等运算逻辑，应用场景相对受限。

目前，国内的同态加密技术在落地应用方面还存在着落地成本高昂、计算效率低等问题。需要通过研究同态加密新方案降低同态加密的成本，以及通过软硬件协同技术实现基于硬件的同态加密加速，从而让同态加密技术在身份认证和数据共享应用场景中能够落地使用，解决数据隐私安全难题。

2. 机密计算技术

机密计算技术是基于可信执行环境的一种隐私计算技术，能够通过硬件隔离的方式为数据提供安全的计算空间，从而使数据明文在可信执行环境中能够安全计算而不泄露敏感数据[9]。目前，国内外多家企业推出定制化的机密计算技术，在服务器端和终端市场，英特尔公司SGX和ARM的TrustZone占据了主导地位。2022年，英伟达公司发布的GPU H100，内部集成了机密计算模块，预示着机密计算将与人工智能技术融合发展。

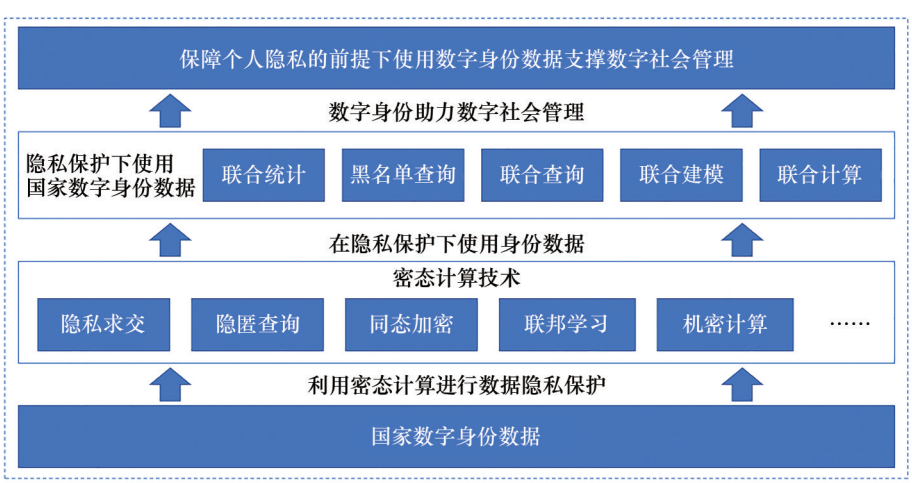

图2　密态计算助力数字社会管理

由于可信执行环境与通用执行环境共用内存，当遭到侧信道攻击时会导致明文泄漏，单纯使用机密计算的技术路径已经无法保障数据在传输过程中的安全性，且硬件成本和技术门槛较高，在应用推广过程中有一定难度，因此将同态加密、安全多方计算等技术与机密计算技术相结合成为主流趋势。当前市场缺少在个人数字身份数据共享场景下基于国产化机密计算平台实现密态计算的相关产品，需要综合研究机密计算、同态加密以及其他隐私计算技术，将各类技术路径有机融合，打造面向数字身份认证的工程化计算应用。

（三）基于大模型的数据身份监管技术

大模型成为人工智能迈向通用智能的里程碑技术。大模型是指具有庞大的参数规模和复杂程度的机器学习模型，通常是指具有数十亿到千亿参数的神经网络模型[10]。大模型的设计和训练旨在提供更强大、更准确的模型性能，以应对更复杂、更庞大的数据集或任务。大模型通常能够学习到更细微的模式和规律，具有更强的泛化能力和表达能力，在分析处理文本以及多模态数据上具有独特优势[11]。目前，大模型的热度从通用大模型开始转入垂直领域大模型，与通用大模型相比，垂直领域大模型经过某个特定领域专业知识的训练，具备更高的领域知识理解力和实用性。

基于大模型的数字身份监管技术利用大模型技术，通过分析多维度的数据，以理解人们的行为和偏好，识别和监测潜在的风险。通过与数据工程结合，大模型技术能够快速、精准地处理海量数据，挖掘数据的潜在价值，快速整合用户数字身份画像。利用大模型可以对个人数据进行大规模的分析和比对，从而更准确地识别潜在的风险因素，如欺诈、恶意行为等。数字身份监管技术的发展需要依赖于大模型和大数据分析等领域的成果，以满足复杂的数字身份监管需求。

（四）分布式数字身份技术

分布式数字身份是基于区块链的新型数字身份认证技术，支持数字身份的自主管理、可信验证、隐私保护和跨域互认，被普遍认为是元宇宙和互联网3.0的身份层。

分布式数字身份技术具备以下特点：一是实现了多方共建共治的分布式公钥基础设施。用户将自主创建的公私钥对和标识存储到难以篡改的区块链上，以确保身份信息的真实可信。签发方对携带用户属性信息的可验证凭证做数字签名，依赖方访问区块链验证用户和签发方的数字签名、属性信息，利用区块链技术的去中心化特点实现分布式身份认证。二是改变了中心化机构控制数字身份的模式。由用户自主控制和管理自己的数字身份，保障个人数据隐私和权益。三是制定身份层标准协议，满足跨应用的互操作性[12]。

分布式数字身份取得了快速发展。一是标准化逐步推进，万维网联盟、去中心化身份基金会、IP 信任基金会等多个国际组织都在积极开展标准化工作。二是应用范围逐步扩大，得到了主要的区块链厂商支持，并已在我国及美国、欧盟、加拿大、韩国等世界主要国家和地区应用。高德纳咨询公司预测，到2026年，全球至少有5亿智能手机用户将使用基于分布式数字身份技术的移动卡包进行可信认证。三是在未来相当长一段时期内，分布式数字身份将持续处于“中心化+分布式”混合发展阶段。

当前，分布式数字身份技术还存在如下问题：一是典型的基于公链技术的分布式数字身份解决方案，允许用户匿名自签发数字身份和管理个人私钥及数据，不符合实名制要求，致使监管缺失，审计困难，缺乏与真实身份的关联和溯源机制；且由于缺乏统一的根身份，不同方法标识符将建立起新的“身份孤岛”。二是分布式数字身份作为新的数字身份技术体系，需逐步建立标准规范，形成行业广泛共识，才能推动应用生态的落地。三是所采用的区块链技术要达到国家基础设施级别的服务保障和支撑能力，在性能、易用性、可扩展性和安全性方面都有待进一步提高。

六、对策建议

（一）加强顶层设计，制定数字身份发展战略和实施路线图

一是从国家层面制定网络空间数字身份国家战略，明确国家数字身份战略实施路线图，在政策法律、标准规范、技术路线、应用模式等方面加强统筹规划和布局。尤其是针对数据要素、数

字人、Web 3.0、元宇宙等新兴市场和新型网络空间，积极开展与数字身份相关的制度标准建设并推动创新应用。二是公安部、网络安全和信息化委员会办公室、市场监督管理总局等部门建立信息沟通机制，着力解决多头监管、标准不一等问题，有效落实《中华人民共和国个人信息保护法》《中华人民共和国反电信网络诈骗法》等法律法规的要求。

（二）完善数字身份相关法律法规，统一全国网络身份认证体系

加快完善数字身份管理相关法律法规，为快速推广应用提供法律保障。一是在《中华人民共和国居民身份证法》等法律法规中明确数字身份（电子身份证）与实体身份证具有同等的法律效力，通过修法予以认可。二是采取“三步走”策略统一全国网络身份认证体系。第一阶段，在公安领域发布管理规章，在公安电子政务等便民服务项目上推广应用，办理身份证的同时注册数字身份，并出台数字身份注册、应用、管理等方面的要求；第二阶段，根据已有成功经验，扩大使用范围到全国电子政务以及各行业应用；第三阶段，推动《中华人民共和国居民身份证法》修订，明确法定数字身份概念，主管部门、应用行业领域等以此全面实现数字身份统一管理。三是统筹规范各类数字身份的生成运行规则和技术规范，统一全国网络身份认证体系，满足远程在线查验居民身份的刚性需求，确保公民身份数据安全。

（三）构建“中心化管理+分布式认证”混合架构的数字身份管理体系，夯实数字社会信任基础

基于国家基础设施，深化对自主身份与分布式数字身份技术的探索，构建“中心化管理+分布式认证”混合架构的自主可信数字身份管理体系[13,14]（见图3），实现数字身份的可靠认证、安全存储和高效流转，为数字社会提供坚实的信任支撑。同时，研究优化高效的密码算法和网络调度算法，构建统一技术栈，通过密态即服务、技术开源等方式，降低技术门槛，推动大数据平台从明文计算迈向密文计算，实现身份数据的互联互通和安全共享，保障数据资产的持有权不失控，实现使用权的跨域管控。

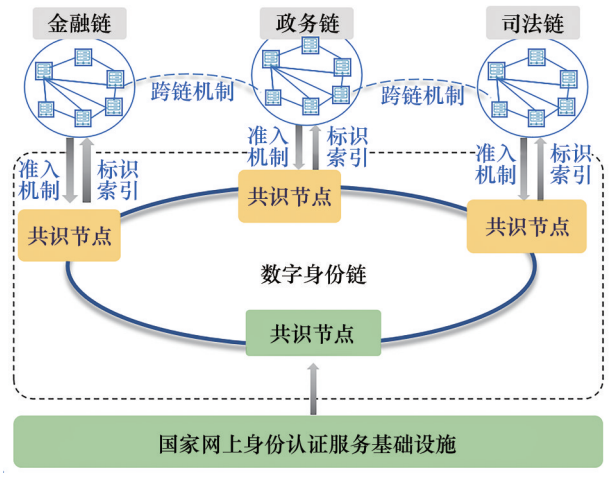

图3　“中心化管理+分布式认证”混合架构的数字身份链

（四）发展基于大模型技术的数字身份监管能力

积极发展基于大模型技术的数字身份监管能力。研究基于多系统数据的多模态大模型，构造精准的用户画像。结合人工智能算法，根据用户画像分析用户的行为模式，优化数字身份冒领、冒用检测技术。此外，建设大规模异构智能算力平台，从计算架构出发，充分利用计算资源并行分布，构筑支持异构算力的资源集池，实现从内部网络的互联到公共网络的优化调整，以及模型的灵活适配调整，以强劲的算力支撑驱动大模型的高效运行（见图4）。

（五）加强数字身份管理全领域参与方的规范管理

围绕数字身份生命周期的活动、角色、功能较为复杂，建议对身份信息管理参与方（包括凭证服务提供方、凭证数据处理方等）实行备案制，并对其进行分级评估，在取得相应服务资质后才能开展相应的身份管理服务。身份提供方应制定身份信息的安全保护策略，分别从身份信息敏感等级、处理设备安全等级等方面规范安全保障程度[15]。通过有效地实施数字身份安全管理制度，降低数字身份应用风险，确保数字身份安全，助力数字社会有序管理。

（六）推动产业链上下游各机构、产业联盟等加强合作

利用区块链共识机制，设计多方联合运营机制，共建共享共赢数字身份生态，行业业务数据和个人身份数据联动，打破“数据孤岛”，促进多方数据资产流通，共同推进数字产业化和产业数字

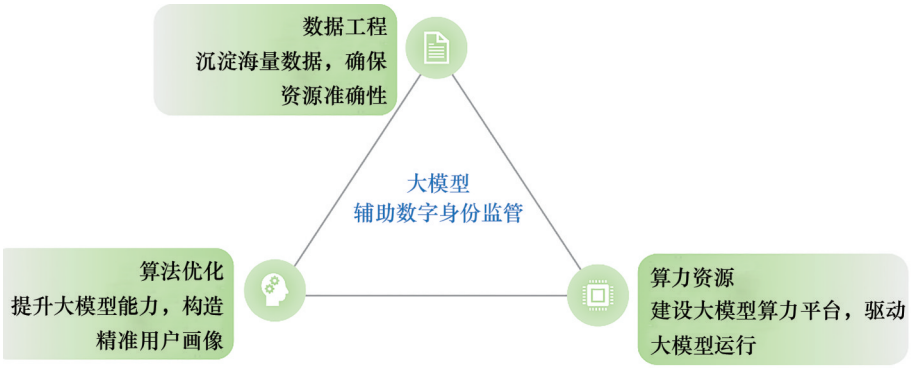

图4　基于大模型技术的数字身份监管架构

化；学、研、用三方并进，借助部委和学术专家优势资源，形成数字身份智库，做好技术和应用的转化衔接，推动数字身份创新链、产业链、人才链、政策链、资金链深度融合；搭建行业主管部门、政府机构和龙头企业联合运营、协商治理的数字身份联盟链网。

（七）积极参与数字身份的国际合作和全球治理，贡献中国方案

加强国际交流合作，参与国际标准编制，共同构建支持跨境数据交换和身份互认的数据治理体系，积极参与全球互联网治理体系中与数字身份相关的建设工作，为共建网络空间命运共同体贡献中国智慧和中国方案。

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: April 28, 2024; **Revised date:** May 24, 2024

Corresponding author: Yu Rui is a research fellow from First Research Institute of the Ministry of Public Security of PRC. His major research fields include public security informatization construction and application, national legal certificates and biometric special identification, network trusted identity authentication. E-mail: yr9041@163.com

Funding project: Chinese Academy of Engineering project “Strategic Research Project on Scientific and Technological Innovation to Support the Modernization of National Security System and Capabilities” (2022-XBZD-28)

参考文献

[1] 田轩. 完善数据基础设施 构筑金融科技数据治理体系 [J]. 中国银行业, 2023 (4): 49.
Tian X. Perfecting data infrastructure and constructing financial science and technology data governance system [J]. China Banking, 2023 (4): 49.

[2] 于锐. 各国数字身份建设情况及我国可信数字身份发展路径 [J]. 信息安全研究, 2022, 8(9): 858–862.
Yu R. The status of digital identity construction in various countries and the development path of trusted digital identity in China [J]. Information Security Research, 2022, 8(9): 858–862.

[3] 刘新海, 安光勇. 个人金融数据商业新模式——以韩国 MyData 为例 [J]. 清华金融评论, 2023 (4): 95–98.
Liu X H, An G Y. A new business model for personal financial data—Taking MyData from Republic of Korea as an example [J]. Tsinghua Financial Review, 2023 (4): 95–98.

[4] 刘新海, 安光勇. 数字经济下个人信息保护的挑战和应对——基于本人数据管理的新思路 [J]. 清华金融评论, 2021 (3): 95–96.
Liu X H, An G Y. Challenges and responses to personal information protection in the digital economy: A new approach based on personal data management [J]. Tsinghua Financial Review, 2021 (3): 95–96.

[5] McKeen F, Alexandrovich L, Berenzon A, et al. Innovative instructions and software model for isolated execution [R]. New York: the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy, 2013.

[6] McMahan B H, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data [R]. Lauderdale: The 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 2017.

[7] Bonawitz K, Ivanov V, Kreuter B, et al. Practical secure aggregation for privacy-preserving machine learning [R]. Texas: The 2017 ACM SIGSAS Conference on Computer and Communications Security, 2017.

[8] 韦韬, 潘无穷, 李婷婷, 等. 可信隐私计算: 破解数据密态时代“技术困局” [J]. 信息通信技术与政策, 2022 (5): 15–24.
Wei T, Pan W Q, Li T T, et al. Trusted privacy computing: Breaking the “technical dilemma” in the era of data privacy [J]. ICT and policy, 2022 (5): 15–24.

[9] Gao W, Hei X H, Wang Y C. The data privacy protection method for hyperledger fabric based on trustzone [J]. Mathematics, 2023, 11(6): 1357.

[10] Zhao W X, Zhou K, Li J, et al. A survey of large language models [EB/OL]. (2023-03-31)[2024-03-18]. https://arxiv. org/abs/

2303.18223.

[11] Ouyang L, Wu J, Jiang X, et al. Training language models to follow instructions with human feedback [J]. Advances in Neural Information Processing Systems, 2022, 35: 27730–27744.

[12] 杨林, 国伟, 章锋, 等. 我国网络可信身份发展路径探索与展望 [J]. 信息安全研究, 2022, 8(12): 1236–1240.
Yang L, Guo W, Zhang F, et al. Exploration and prospect of the development path of trusted identity in China's network [J]. Information Security Research, 2022, 8(12): 1236–1240.

[13] 杨滢, 陈绍泉. 元宇宙时代下的数字身份初探 [J]. 警察技术, 2023 (4): 36–38.
Yang Y, Chen S Q. A preliminary exploration of digital identity in the Metaverse era [J]. Police Technology, 2023 (4): 36–38.

[14] 郝久月, 杨林, 李頔, 等. 关于区块链支撑网络可信身份发展的研究与探索 [J]. 警察技术, 2023 (1): 32–36.
Hao J Y, Yang L, Li D, et al. Research and exploration on the development of trusted identity in blockchain supported networks [J]. Police Technology, 2023 (4): 32–36.

[15] 李俊, 柴海新. 数字身份安全治理研究[J]. 信息安全研究, 2021, 7(7): 598–605.
Li J, Chai H X. Research on secure governance of digitai ldentity [J]. Information Security Research, 2021, 7(7): 598–605.