算力网络安全风险分析与对策研究

王馨楠[1,2]，程启月[1]，陆 军[1]
（1.量子科技长三角产业创新中心，江苏 苏州 215100；
2.北京邮电大学，北京 100876）

摘 要：伴随着数字经济时代的发展，新兴技术带来了数据量的飞速增长，社会生活的各方面对算力和网络的需求急剧增大，算力网络应运而生。然而，新的技术和新的网络架构也带来了新的安全风险，原有的安全防护措施已经无法满足对算力安全的需求。分布广、数量庞大的多源算力和网络已经打破了传统安全域羁绊，算力网络在数据安全、网络安全和隐私安全等方面受到严重威胁。从算力网络架构安全、网络数据安全、网络资源安全、计算资源安全、资源管理安全和算力服务安全等角度，梳理算力网络安全相关最新研究成果和技术，分析算力网络面临安全风险和系统威胁的成因，给出加强算力网络安全性的对策建议，旨在构建全方位、多层次的算力网络安全防护体系，抵御来自数据、网络、资源、服务等方面的系统风险。

关键词：算力网络；算力安全；风险；对策建议
中图分类号：TP393
文献标识码：A
doi：10.11959/j.issn.2096−8930.2025010

Security Risk Analysis and Countermeasure Research for Computing Power Network

WANG Xinnan[1,2], CHENG Qiyue[1], LU Jun[1]
1. Yangtze Rive Delta Industrial Innovation Center of Quantum and Information Technology, Suzhou 215100, China
2. Beijing University of Posts and Telecommunications，Beijing 100876, China

Abstract: With the development of the digital economy era, emerging technologies have brought about a rapid growth of data, the demand for computing power and network in all aspect of social life has increased dramatically. In the face of this demand, computing force network has emerged. However, new technologies and new network architectures also bring new security risks, the original security measures can no longer meet the demand for computing power security. Due to the widely distributed and massive multi-source computing power and networks have broken the traditional security domains, the computing force networks have been seriously threatened in terms of data security, network security and privacy security. The latest research results and technologies related to computing force network security were sorted out from the perspectives of computing force network architecture security, computing force network data security, network resource security, computing resource security, network resource management security and computing service security. It analyzed the causes of the security risks and system threats faced by computing force networks and give countermeasure suggestions to strengthen the security of computing force networks, aimed to establish a comprehensive and multi-layered security protection system for computing power network sand resist system risks from data, network, resources, services, and other aspects.

Keywords: computing power network, computing power security, risks, countermeasure suggestions

0 引言

伴随着 5G 和边缘计算的飞速发展和规模建设，人工智能和多媒体渲染等新型网络业务以及应用层出不穷，数据量的持续增长，对算力和网络需求提出了更为严苛的要求。与此同时，云计算、雾计算、边缘计算、

收稿日期：2024–10–10；**修回日期：**2025–01–10
基金项目：中国工程院行业院重大项目（No. 2022-HYZD-01）
Foundation Item：Major Project of Industry Institute of China Academy of Engineering (No.2022-HYZD-01)

智能终端等技术快速发展，可提供算力的计算资源逐渐丰富且呈现出泛在部署趋势。然而，计算节点间缺乏有效协同机制，计算任务分配与计算资源调度机制不完善，造成计算资源利用率低的问题更加凸显。为了实现算力资源的全局优化调度和配置，算力网络这一概念应运而生。算力网络旨在将分布式计算节点打通互联、统筹调度，通过对网络架构和协议的改进，实现网络和计算资源的优化和高效利用[1]。然而，新型网络业务快速发展对算力网络安全提出了更高的要求。现有算力网络面临多种安全风险和隐私威胁，包括算力节点安全可信水平参差不齐、攻击暴露面急剧增多；数据资源在传输、计算、调度、应用过程中遭受泄露、篡改；存证溯源困难、算力滥用等，以及管控复杂度提升后缺乏相应手段，监管机制不健全等安全风险。同时，算力网络更易受到分布式拒绝服务攻击、边信道攻击、授权攻击、恶意软件注入等各类安全威胁。面对算力网络的新架构、新技术和新服务可能带来的安全风险，需要适配与之对应的安全机制。因此，对算力网络展开安全风险对策研究迫在眉睫。

近年来，国家连续发布众多法律法规以保障互联网行业的安全。其中，《中华人民共和国网络安全法》[2]中提出，积极开展网络空间治理、网络技术研发和标准制定，并指出要加强对数据的监管力度，建立数据分类分级保护制度、数据安全风险评估机制，保护数据安全。《中华人民共和国个人信息保护法》[3]对一些互联网平台设定特别的个人信息保护义务、完善平台治理、强化外部监督提出了法律层面的要求。政府在出台相关条例时，提出要加强立法和监管、提升我国关键信息的基础设施保护能力和水平的要求，如《关键信息基础设施安全保护条例》[4]的出台，体现了新型网络业务快速发展对算力网络安全的影响越来越得到国家和政府行业管理部门的重视。当前，我国互联网行业安全政策体系不断完善，正在加快构建一整套安全服务体系，以应对新型网络算力服务业务快速发展，为算力网络风险控制筑起高墙。

1　算力安全发展的机遇与面临的风险挑战

1.1　算力网络安全发展的机遇

纵观近几年政府管理部门和行业研究机构在算力安全方面开展的工作和发布的研究成果，可以见得，算力安全越来越得到重视。2019 年 11 月，中国联通网络技术研究院发布了《中国联通算力网络白皮书》[5]，介绍了算力网络的产业背景，对算力网络的概念、架构、关键技术、典型应用场景分析等方面的安全问题展开讨论。2020 年 3 月，国家发展和改革委员会、工业和信息化部印发了《关于组织实施 2020 年新型基础设施建设工程（宽带网络和 5G 领域）的通知》[6]，聚焦信息网络等新型基础设施项目，提出了要加快部署建设边缘计算设备、5G 基站、光缆、智能终端等算力网络基础设施。2021 年 5 月，国家发展和改革委员会、中央网络安全和信息化委员会办公室、工业和信息化部、国家能源局联合印发了《全国一体化大数据中心协同创新体系算力枢纽实施方案》[7]，提出要构建数据中心、云计算、大数据一体化的新型算力网络体系，加快实施“东数西算”工程，加强云算力服务、数据流通、数据应用、安全保障等方面的探索实践。2021 年 11 月，中国通信学会算力网络融合标准工作组、中国通信标准化协会无线安全与加密工作组均立项启动算力网络安全研究工作。2023 年 8 月，中国算力大会召开，从网络安全、信息安全、数据安全 3 个维度共论算力安全发展之道。这些都充分说明新型网络业务快速发展对算力网络安全的影响越来越受到重视。

1.2　算力网络安全发展面临的风险挑战

传统网络安全大多采用基于身份认证、入侵检测、加密保护及数据完整性保护为主的安全体系，同时基于以边界为中心的防御架构来部署网络防御系统。对内采取信任态度，系统采用“打补丁”的防御架构更新来抵御安全风险。与传统网络不同，算力网络构建了以新型网络连接为基础的异构算力资源接入的分布式计算形态，统一纳管了海量计算资源，现有的安全机制难以应对算力网络新的安全风险与挑战，主要包括以下几个方面[8-9]。

一是安全物理边界渐趋模糊。虚拟化技术实现了软硬件的解耦，打破了物理硬件设备操作的壁垒，部分网元以虚拟功能网元的形式部署在云化的基础设施上，基础设备间的物理边界逐渐模糊，传统的网络信任关系和安全边界已难以为继，它加大了算力网络的安全风险和威胁。

二是算力资源节点的不可信。算力网络接入大量第三方资源节点，算力资源节点可信度降低，服务节点的安全性和可靠性难以得到充分保证。攻击者会冒充算力资源供应方或消费方接入算力网络，以实现缓存污染、数据窃取等攻击。不可信节点的存在加大了算力网络的安全风险和威胁。

三是可能的攻击暴露面增多。在算力网络资源的接入、编排、调度等过程中涉及众多远程交互，这些都将导致资源的暴露面增多，易遭到“中间人”攻击；同时，相较于传统网络架构，算力网络的新型架构模式新增了算力网络感知单元和算力网络控制单元等网元，这些单元实体增多也增加了可能受到攻击的暴露面，加大了算力网络的安全风险和威胁。

四是频繁化算力的无序滥用。算力网络提供强大算力的同时，也造成在算力频繁使用过程中，没有安全门户的情况下，攻击者会实时入侵实现网络攻击、密码拆解等恶意行为，加大了算力网络的安全风险和威胁。

五是数据篡改隐私信息泄露。在算力网络运行过程中传输海量数据，其中涉及医疗、金融、军事等领域，以及个人信息等众多隐私数据，在传输过程中如果算力网络安全防护措施不到位，极可能遭受数据篡改或隐私信息泄露并造成难以估量的严重后果，这些也加大了算力网络的安全风险和威胁。

2　算力网络安全研究现状分析

目前，国内外众多学者对算力网络安全领域的研究不断深入，其核心议题广泛涵盖了网络架构安全、网络数据安全、网络资源安全、计算资源安全、资源管理安全以及算力服务安全等多个维度。本文较系统地总结归纳了涉及以上研究方向的关键技术、方法与策略，具体见表1。

（1）网络架构安全

算力网络架构安全是指满足基于算力网络的逻辑架构和物理架构等安全性需求的安全设计。袁长卿等[10]从算力网络架构的计算服务、资源编排管理以及资源底座等部分出发，依次阐述对应内容和相应的安全建设策略（如图1所示）。邱勤等[11]给出了将网络与数据资产管理、隔离技术、身份识别及访问控制、密码技术等通用安全技术作为算力网络安全基础底座，为算力网络各个环节、要素提供基础共性技术支撑的技术路径。温瑶等[12]设计了融合区块链的算力网络架构，并基于该架构设计了包含用户身份认证机制、算力服务注册机制、交易机制、信誉评估机制的信任评估与保障的技术方案。

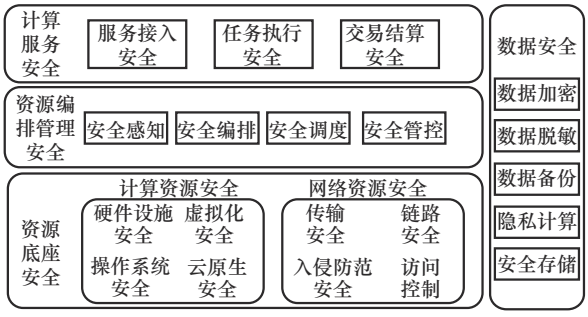

图1　算力网络安全架构

以上这些研究为算力网络的算力资源共享提供可信的安全保障，并给出了可行的技术路径和实施方案。

（2）网络数据安全

算力网络数据安全是指针对算力网络中数据分散到多方资源节点而面临的数据隐私泄露和结果篡改等风险采用数据安全防护技术，以保障数据全生命周期安全。它关注算力网络中数据全生命周期的安全防护，其中涉及数据加密、数据脱敏、数据备份、安全存储等技术环节。潘洁等[13]引入国密算法及密码应用技术框架，针对用户不同安全需求进行密码安全保障，提出了密码安全层建设的策略。Bi等[14]提出了基于模糊集的数据脱敏算法，降低了数据被恢复的概率，保障了数据的隐私。Liu等[15]基于多因素认证，提出了一种以用户为中心的数据备份方案，保护数据免受自然灾害、硬件故障等的影响，保障数据的完整性。周赞等[16]采用联邦算力网络

表1　算力网络安全研究关键技术方法与策略概览

研究领域	主要内容	关键技术/方法
网络架构安全	满足算力网络逻辑架构和物理架构的安全性需求	基础设施安全、编排管理安全、运营服务安全[10]、区块链技术、信任评估与保障[12]
网络数据安全	数据全生命周期安全防护	数据加密、数据脱敏[14]、数据备份[15]、安全存储、国密算法[13]、联邦算力网络[16]、同态加密、隐私计算[17]
网络资源安全	保护网络软硬件资源免受未授权访问、干扰和损坏	入侵检测技术[18]、隐藏马尔可夫模型[19]、多层DDoS攻击缓解框架[20]、侧信道攻击防御[22]
计算资源安全	保护计算软硬件资源免受未授权访问、干扰和损坏	形式化软件验证[23]、硬件冗余、硬件安全模块、多核处理器隔离[24]
资源管理安全	对网络资源进行有效的保护和管理	远程故障检测[25]、算力资源安全通告协议、算力资源校验、算力请求安全解析[26]
算力服务安全	针对算力服务中的安全风险进行安全防护	用户接入安全、算力网络编排安全、任务执行安全、交易结算安全[27]

算法，给出了在数据不出本地的环境下的协同训练高质量模型。通过协调训练，该模型统筹数据本地化的边缘算力节点，规避传输过程中隐私泄露的风险。针对存在通过窃取模型参数和可见梯度权重进行逆向推断，间接侵犯用户隐私的问题，为了进一步保护用户隐私，将同态加密等技术引入联邦算力网络，对其进行隐私计算的增强。张海涛等[17]将隐私计算赋能算力网络，构建安全可信的计算平台，关注数据流通过程中的安全、信任和隐私保护等关键环节中的问题，保障数据流通全生命周期安全。

以上这些研究基于安全可信计算环境技术，可信计算环境与数据合约绑定，为每个计算任务创建了独立的安全可信计算环境，为最终实现数据的“可用不可见”“可控可计量”，保障多方数据安全计算提供了可靠可控的条件、方法和手段。

（3）网络资源安全

网络资源安全是指保护网络软硬件资源免受未经授权的访问、干扰和损坏，在维持快速有效的通信的同时保证网络的安全性。在网络资源安全方面，在网络空间中，各种软硬件实体都会存在漏洞和后门，当前的主流防御思路是对具体的漏洞和后门进行安全增强。如在入侵检测技术方面，为及时发现和排除复杂异构边缘环境中的边缘节点异常，参考文献[18]引入了雾计算入侵检测系统框架，提出了基于此框架的最佳入侵响应策略，可以有效地稳定雾计算中入侵者的入侵频率。Samir等[19]使用隐藏马尔可夫模型来检测边缘集群工作负载中的异常行为，通过识别不同类型的异常和跟踪分布式系统中的异常原因，提高异常检测的准确性。针对分布式拒绝服务（Distributed Denial of Service, DDoS）攻击，Yan等[20]提出了一种包括云计算、雾计算、边缘计算的多层DDoS攻击缓解框架，通过边缘计算、雾计算捕获网络流量信息，再利用云服务器进行网络流量信息的聚合和DDoS攻击检测。针对侧信道攻击，Molnar等[21]提出一种通用的源代码到源代码转换方法，防止控制流侧信道攻击。Pu等[22]基于注意力机制，提出了非伪装侧信道攻击架构，通过在网络层后附加注意力机制以提供正确密钥的定量预测。

以上这些研究提出了多种方法和技术来应对不同类型的网络威胁和攻击，以维护网络资源的安全性，增强了整体网络资源的可信性、稳定性和科学性。

（4）计算资源安全

计算资源安全是指保护计算软硬件资源免受未经授权的访问、干扰和损坏，它包括云、边、端可用计算资源在软硬件方面的安全保障。其中，硬件的瞬时故障和错误可能危害整体信息系统的正确性。Elphinstone等[23]在形式化软件验证的基础上，分析商用硬件的可靠性特征，利用冗余的多核处理器以提高现有硬件的可信度，并实现安全部署。这样做可将硬件安全模块引入计算资源系统，起到硬件安全模块负责存储并管理用于认证和加密的私有密钥作用，具有极高的加解密运算速度和安全保护级别，且易与其他设备相整合。Azab等[24]设计了不依赖操作系统的且为敏感工作负载提供硬件级隔离和保护的框架，该框架使用多核处理器，允许隔离的环境在不受信任的主机旁边并发地安全运行。

以上这些研究基于计算资源中的软硬件基础设施，提出创新性的方法和技术，以提高软硬件的可信度和安全性，从而增强整个网络计算资源的安全性和可靠性。

（5）资源管理安全

资源管理安全是指在算力网络中对网络资源进行有效的保护和管理，有效地规划、配置、监控和维护网络中的资源，确保网络资源的可用性、保密性和可靠性，防止未经授权的访问、攻击。针对远程故障检测安全，Liang等[25]设计了一种名为CFN-Watchdog的新型远程故障检测程序，以及时监控任务和虚拟机的状态，通过及时回收故障/恶意占用的资源池，显著提高系统的吞吐量。但它主要分析的是在理想条件（如完美时间同步）下的CFN-Watchdog协议对系统吞吐量的影响，并未在更现实的环境中研究其对更多性能指标的影响。高凯辉等[26]提出算力网络资源管理安全架构，使用算力资源安全通告协议、高效算力资源校验和算力请求安全解析机制，为算力网络安全体系的建设提供支撑。

以上这些研究提出了多种方法和技术来应对不同类型的网络威胁和攻击以维护网络资源的安全性，并对算力网络资源采取有效的规划、配置、监控等手段进行管理，确保网络的可用性和安全性。

（6）算力服务安全

算力服务安全是指针对算力网络为各行各业提供的计算服务中的安全风险进行安全防护。在算力服务安全方面，张逸然等[27]关注算力网络业务运行的安全，依次分析了用户接入、算力网络编排、任务执行、交易结算等算力网络业务运行机制的4个阶段面临的安全挑战，给出了相应的安全策略，根据业务场景在不同可信度的节点间灵活调度计算任务，以满足不同安全需求。

以上这些研究涵盖了算力服务在各个关键阶段的安全策略和措施，保障了从用户接入到任务执行再到交易结算这一完整计算服务的可信度和安全性，减少了潜在的风险和威胁。

3 加强算力网络安全的对策建议

算力网络通过协同调度算力和网络资源，极大地提高了对闲置资源的利用率，提升了对海量数据的处理效率，它对推动数字经济发展具有重大意义。算力网络安全为算力网络在数字经济的算力服务中，维护数据安全、隐私安全，发挥社会效能提供了安全保障。当前，人们对算力网络安全的重要性还缺乏全面认识，算力网络安全机制尚未建立健全，算力网络安全测量标准还未规范，算力网络安全防护手段还较局限，根据以上风险分析，给出以下对策建议。

一是树立全流程防护算力网络安全观，建立健全算力网络安全体制机制。面对算力网络规模大、资源节点泛在、安全风险增大的问题，必须树立全流程防护的算力网络安全观，就是要在制度、技术、服务等各个层面，提高对算力网络安全重要性的全面认识，如引入零信任理念，即树立“永不信任，始终验证”理念。零信任是一种新型的模型，是指在算力网络场景适配和流程架构的设计中以零信任理念对网络中的所有对象进行验证，授予其最小访问权限，同时对所有的访问行为进行持续、动态的评估决议，从而实现安全、可靠的访问控制与调度管理。必须建立健全算力网络安全体制机制，通过各种技术手段和管理措施，使算力网络系统正常运行，确保算力服务数据的可用性、完整性和保密性。如，使用不同的隔离防护机制，如路由、互联网协议安全性（Internet Protocol Security，IPSec）、虚拟局域网（Virtual Local Area Network，VLAN）、虚拟专用网络（Virtual Private Network，VPN）等技术为用户提供差异化的安全防护策略。在应对算力网络场景中的网络安全、数据安全等方面，仅仅局限在技术层面，在传统的安全方案基础上做边界加固和单点增强，已经难以系统性地缓解各种安全问题。这就要在算力服务的各个环节建立安全防护机制，通过科学的技术手段和严密的管控机制使得算力网络受到机密性、完整性和真实性的保护。

二是规范算力网络安全评价指标体系，加快算力网络安全分类分级标准制定。目前，算力网络安全评价指标的制定“各自为战”，尚未形成统一的评价指标体系，同时，算力安全分类分级标准在业界尚未规范统一，敏感级别的划分也未达成共识，这些对提供算力服务安全等级的界定带来了复杂性和不确定性。加快算力网络安全分类分级标准制定，必须开展对算力网络安全评价指标体系的研究。应在算力网络安全的不同环节采用不同的方式、方法建立评测指标，形成算力网络安全评价指标体系。如在用户端登录入网身份认证和授权环节，为了保证算力网络中计算资源纳入和用户接入的安全和隐私，在对操作者身份进行确认的过程中，建立判断目标用户获取资源访问和控制权限的安全性测量指标；在访问控制环节，针对不同的访问模式、技术和手段，如自主访问控制、强制访问控制、基于角色的访问控制等，制定访问操作管理控制对应的安全性测量指标，为算力网络安全标准分类分级制定打下良好的基础。算力网络安全标准是指为了在一定的范围内获得算力服务最佳秩序，制定并由公认机构批准的共同使用的和重复使用的一种规范性文件。制定算力网络安全标准，才能保证是以科学、技术和实践经验的算力网络安全性综合成果为基础，制定共同可遵守的准则和依据，才能保障提供对应安全等级的算力服务。

三是强化算力网络安全加密技术研究，促进数据安全动态感知的预测智能化。为了保证数据安全，确保攻击者用恶意手段获取数据时用户数据具有机密性，通常数据以加密的形式存储在服务器上。针对传统加密方案，如高级加密标准（Advanced Encryption Standard，AES）、三重数据加密标准（Triple Data Encryption Standard，3DES）等密文对于大多数应用（如数据库应用、Web 应用、移动应用、数据分析工具等）不可用，应加强算力网络安全能力动态感知加密机制研究，如密码学界提出的在加密数据上采用具有高安全性加密机制——同态加密机制、函数加密机制[28]、可搜索加密机制等。这里的同态加密[29]是指支持密文层面的运算，使用“数据加密-密文计算-结果解密”的模式被构造于各类隐私保护计算技术和应用场景；函数加密是指根据密文上函数的范围，制定完全同态加密方案和部分同态加密方案；可搜索加密能够对密文进行有效检索，保证了数据可用性。在实践中，算力资源的安全能力在算力网络中是实时变化的，通过对算力网络安全能力的动态实时感知和预测，更加智能化地进行安全合理的编排管理。为促进数据安全动态感知预测的时效性、准确性、可靠性，必须在编排管理算法、动态实时感知和安全能力预测等环节，加大技

术研究和智能化系统研发，促进算力网络安全能力的提升。

四是加大算力网络安全手段建设投入，保证算力计算服务安全的针对性。算力网络服务应用场景复杂，为保障在不同的业务和任务中用户有专用的传输通道，应采用不同的算力网络安全手段，如网络物理隔离可以使多个不同范畴的网络系统相对独立，适用于可信和不可信网络之间进行数据交换[30]，也可以使用单主板隔离机[31]、网络安全隔离卡[32]、网络安全集线器、网闸等物理隔离技术为其提供安全保障。针对不同业务对安全性的要求，应根据业务和数据资产的重要性，采用切片间隔离技术[33]为用户提供相应切片服务的同时，保障切片网络与用户之间的安全边界。建立切片 3 级立体化安全隔离体系[11]，提供切片间有效隔离，保证切片有相应的安全级别。

4　结束语

本文深入剖析了算力网络面临的安全风险，通过系统性地审视算力网络的整体安全架构以及资源层、编排管理层、服务层等多个维度，全面梳理了当前算力网络安全领域的研究现状与研究成果。并针对性地提出了加强算力网络安全性的对策建议，这些建议不仅着眼于当前的安全挑战，也为未来的研究方向与应用实践提供了宝贵的参考与指导，为算力网络安全发展之路铺设了坚实的基石，并为后续研究工作的深入开展奠定了良好的理论基础与实践框架。

参考文献：

[1] 贾庆民, 丁瑞, 刘辉, 等. 算力网络研究进展综述[J]. 网络与信息安全学报, 2021, 7(5): 1-12.
JIA Q M, DING R, LIU H, et al. Survey on research progress for compute first networking[J]. Chinese Journal of Network and Information Security, 2021,7(5): 1-12.

[2] 中国人大网. 中华人民共和国网络安全法[EB]. 2016.
China People's Congress Network. Network security law of the People's Republic of China[EB]. 2016.

[3] 中国人大网.中华人民共和国个人信息保护法[EB].2021.
China People's Congress Network. The People's Republic of China (PRC) personal information protection law[EB].2021.

[4] 中国政府网.关键信息基础设施安全保护条例[EB].2021.
China Government Network. Regulations on the security protection of key information infrastructure [EB].2021.

[5] 中国联通网络技术研究院. 中国联通算力网络白皮书[R].2019.
China Unicom Network Technology Research Institute. China Unicom computing network white paper [R].2019.

[6] 5G工业物联.国家发展和改革委员会办公厅 工业和信息化部办公厅关于组织实施2020年新型基础设施建设工程(宽带网络5G领域)的通知[EB].2021.
5G Industry Federation. Notice of the general office of the ministry of industry and information technology of the general office of the national development and reform commission on organizing the implementation of the new infrastructure construction project in 2020 (broadband network 5G field)[EB].2021.

[7] 中国政府网.全国一体化大数据中心协同创新体系算力枢纽实施方案[EB].2021.
China Government Network. Implementation plan for computing hub of collaborative innovation system of national integrated big data center[EB].2021.

[8] AZIZ N A, MANTORO T, KHAIRUDIN M A, et al. Software defined networking (SDN) and its security issues[C]//Proceedings of the 2018 International Conference on Computing, Engineering, and Design (ICCED). Piscataway: IEEE Press, 2018: 40-45.

[9] ALWAKEEL A M, ALNAIM A K, FERNANDEZ E B. A survey of network function virtualization security[C]//Proceedings of the Southeast 2018. Piscataway: IEEE Press, 2018: 1-8.

[10] 袁长卿, 苏越, 赵伟博. 面向算力网络的安全体系研究[J]. 信息通信技术与政策, 2023(2): 82-86.
YUAN C Q, SU Y, ZHAO W B. Research on security system for computing power network[J]. Information and Communications Technology and Policy, 2023(2): 82-86.

[11] 邱勤, 徐天妮, 于乐, 等. 算力网络安全架构与数据安全治理技术[J]. 信息安全研究, 2022, 8(4): 340-350.
QIU Q, XU T N, YU L, et al. Computing force network security architecture and data security governance technology[J]. Journal of Information Security Research, 2022, 8(4): 340-350.

[12] 温瑶, 陆晶晶, 卢华, 等. 融合区块链的算力网络信任评估与保障方案研究[J]. 南京邮电大学学报(自然科学版), 2021, 41(4): 99-106.
WEN Y, LU J J, LU H, et al. Blockchain-based trust evaluation and guarantee scheme for computing power network[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2021, 41(4): 99-106.

[13] 潘洁, 叶兰, 张鹏飞, 等. 基于国密算法的算力网络安全研究[J]. 电信科学,2023,39(8): 1-16.
PAN J, YE L, ZHANG P F, et al. Research on computer network

security based on state secret algorithm[J]. Telecommunication Science, 2023,39(8): 1-16.

[14] BI T, CHEN X H, LI J, et al. Research on industrial data desensitization algorithm based on fuzzy set[C]//Proceedings of the 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications(AEECA).Piscataway: IEEE Press, 2020: 1-5.

[15] LIU Y N, ZHONG Q, CHANG L, et al. A secure data backup scheme using multi-factor authentication[J]. IET Information Security, 2017, 11(5): 250-255.

[16] 周赞, 张笑燕, 杨树杰, 等. 面向联邦算力网络的隐私计算自适激励机制[J]. 计算机学报, 2023,46(12): 2705-2725.
ZHOU Z, ZHANG X Y, YANG S J, et al. Adaptive incentive mechanism of privacy computing for federated computing network [J]. Chinese Journal of Computers, 2023,46(12): 2705-2725.

[17] 张海涛, 包森成, 何志坚 . 隐私计算在算力网络中的实践应用[C]//首批可信计算认证产品发布会论文集 . 出版地不详: 出版者不详, 2023: 132-135.
ZHANG H T, BAO S C, HE Z J. Practical application of privacy computing in computing network[C]//Proceedings of the First Batch of Conference on Trusted Computing Certification Products. [S.l: s.n.], 2023: 132-135.

[18] AN X S, LIN F H, XU S G, et al. A novel differential game model-based intrusion response strategy in fog computing[J]. Security and Communication Networks, 2018.

[19] SAMIR A, PAHL C. Detecting and predicting anomalies for edge cluster environments using hidden Markov models[C]//Proceedings of the 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC). Piscataway: IEEE Press, 2019: 21-28.

[20] YAN Q, HUANG W Y, LUO X P, et al. A multi-level DDoS mitigation framework for the industrial Internet of Things[J]. IEEE Communications Magazine, 2018, 56(2): 30-36.

[21] MOLNAR D, PIOTROWSKI M, SCHULTZ D, et al. The program counter security model: automatic detection and removal of control-flow side channel attacks[C]//Information Security and Cryptology - ICISC 2005. Heidelberg: Springer Berlin Heidelberg, 2006: 156-168.

[22] PU K R, DANG H, KONG F C, et al. A quantitative analysis of non-profiled side-channel attacks based on attention mechanism[J]. Electronics, 2023, 12(15): 3279.

[23] ELPHINSTONE K, SHEN Y Y. Increasing the trustworthiness of commodity hardware through software[C]//Proceedings of the 2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Piscataway: IEEE Press, 2013: 1-6.

[24] AZAB A M, NING P, ZHANG X L. SICE: a hardware-level strongly isolated computing environment for x86 multi-core platforms[C]//Proceedings of the 18th ACM Conference on Computer and Communications Security. New York: ACM, 2011.

[25] LIANG H, FENG L, XU F X, et al. A novel CFN-Watchdog protocol for edge computing[J]. Applied Soft Computing, 2021, 113: 107873.

[26] 高凯辉, 李丹, 陈力 . 算力网络资源管理安全架构与关键技术[J]. 信息通信技术, 2023, 17(3): 13-20.
GAO K H, LI D, CHEN L. Secure architecture and key technologies for resource management in computing first network[J]. Information and Communications Technologies, 2023, 17(3): 13-20.

[27] 张逸然, 耿慧拯, 粟栗, 等 . 算力网络业务安全技术研究[J]. 移动通信, 2022, 46(11): 90-96.
ZHANG Y R, GENG H Z, SU L, et al. Research on security technology for computing force network service[J]. Mobile Communications, 2022, 46(11): 90-96.

[28] 董秋香, 关志, 陈钟 . 加密数据上的计算密码学技术研究综述[J]. 计算机应用研究, 2016, 33(9): 2561-2572.
DONG Q X, GUAN Z, CHEN Z. Cryptographic technologies enabling computation over encrypted data[J]. Application Research of Computers, 2016, 33(9): 2561-2572.

[29] RIVEST R L, ADLEMAN L M, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Compuation, 1978.

[30] 王永建, 杨建华, 郭广涛, 等 . 网络安全物理隔离技术分析及展望[J]. 信息安全与通信保密, 2016, 14(2): 117-122.
WANG Y J, YANG J H, GUO G T, et al. Analysis and prospect of physical isolation technology for network security[J]. Information Security and Communications Privacy, 2016, 14(2): 117-122.

[31] 曾明 . AirGap 机制及实现研究[D]. 昆明: 昆明理工大学, 2003.
ZENG M. Research on AirGap mechanism and its implementation [D]. Kunming: Kunming University of Science and Technology, 2003.

[32] 张莉 . 网络安全技术及解决方案探讨[J]. 广东公安科技, 2003, 11 (2): 47-48.
ZHANG L. Discussion on network security technology and solutions[J]. Guangdong Public Security Science and Technology, 2003, 11(2): 47-48.

[33] 毛玉欣, 陈林, 游世林, 等 . 5G 网络切片安全隔离机制与应用[J].

移动通信, 2019, 43(10): 31-37.

MAO Y X, CHEN L, YOU S L, et al. 5G network slicing security isolation mechanism and application[J]. Mobile Communications, 2019, 43(10): 31-37.

[作者简介]

王馨楠（1999– ），女，北京邮电大学硕士生，主要研究方向为算力网络安全。

程启月（1957– ），女，博士，教授，主要研究方向为信息系统建模与仿真、量子计算。

陆军（1964– ），男，中国工程院院士，主要研究方向为综合电子信息系统。