特色专题

算网安全研究及应用实践

穆琇博,柴瑶琳,韩淑君,毕立波

摘要 作为算网融合体系内的安全防护机制,算网安全的本质是一种新技术和新工程。算网安全涉及零信任、安全访问服务边缘、算网区块链等多种技术实现方式,能够以安全体系的方式为算网融合提供了设施、平台、应用、数据等多维一体的安全保障。梳理了算网安全的总体发展态势:基础设施面临严峻挑战,算网安全成为国家竞争新主题;ICT 积极响应发展机遇,算网安全打造创新发展新蓝海;数字化因素推动算网安全演进发展。重点提炼了算网安全的技术参考架构,具体涵盖设施安全、平台安全、应用安全和数据安全 4 个方面。总结了算力网络安全、云网络安全、行业融合安全 3 种典型应用实践。结合当前算网安全领域面临的严峻挑战提出持续推进标准体系建设、加快应用实践规划落地、协同构建产业生态闭环等发展建议。

关键词 算网安全;算力网络安全;零信任;SASE;SD–WAN

算网融合已经从技术创新走向规模实践,国家级算网基础设施的应用部署初具规模。2023 年 12 月,国家发展和改革委员会等 5 部门联合印发《关于深入实施“东数西算”工程 加快构建全国一体化算力网的实施意见》[1],明确提出要“构建联网调度、普惠易用、绿色安全的全国一体化算力网,助力网络强国、数字中国建设,打造中国式现代化的数字基座”,标志着“东数西算”进入深入发展的第 2 阶段。2024 年 4 月,科学技术部指导的国家超算互联网正式上线,依托一体化的算力调度、数据传输、生态协作体系,超算互联网已经初步实现了算力供给、软件开发、数据交易、模型服务等方面的产业对接,成功吸引了超过 200 家应用、数据、模型等服务商和 3200 款算力产品上线。总体上看,算网融合已经成为国内打通数字设施大动脉的重要底座[2]。

算网安全的出现是算网融合全面发展的必然结果。随着算网创新技术在关键基础设施等重要领域的应用实践日益深入,传统上以“边界防御+纵深防御”为主要特征的安全机制面临失效的风险,行业迫切需要新的安全理念和安全机制来重塑安全底座[3]。作为算网融合体系内的安全防护机制,算网安全的本质是一种新技术和新工程。从技术角度来看,算网安全涉及零信任、安全访问服务边缘(secure access service edge, SASE)、算网区块链等多种技术实现方式,能够以安全体系的方式为算网融合提供设施、平台、应用、数据等多维一体的安全保障。从工程角度来看,算网安全需要兼顾整体架构和业务创新的发展需要,从规划、设计、运营等全生命周期设计安全闭环。经过几年时间的发展,当前,算网安全已经成为算网融合创新演进的重要组成部分,被广泛视为产业发展的安全基石,也是应用创新的重要延伸。

中国信息通信研究院,北京 100191

1 算网安全的总体发展态势

1.1 全球背景:基础设施面临严峻挑战,算网安全成为国家竞争新主题

1)世界各国基础设施特别是关键基础设施面临愈演愈烈的网络安全挑战。2023 年 11 月,中国工商

收稿日期:2024-08-21;修回日期:2025-02-19

作者简介:穆琇博,高级工程师,研究方向为算网融合,电子信箱:muyubo@caict.ac.cn

引用格式:穆琇博,柴瑶琳,韩淑君,等. 算网安全研究及应用实践[J]. 科技导报, 2025, 43(9): 48-53; doi:10.3981/j.issn.1000-7857.2024.08.01037

银行美国子公司(简称“工银美国”)遭遇 LockBit 病毒勒索攻击,工银美国系统服务被迫中断。2024 年 1 月,乌克兰国家关键基础设施系统包括该国最大的国有石油天然气公司和邮政服务提供公司遭遇了大规模网络攻击,国家服务陷入全面瘫痪。2024 年 3 月,美国电话电报公司(AT&T)遭到数据泄露攻击,涉及 7300 多万公司用户信息,延伸的攻击行为导致长达 10 h 的重大网络中断事件,涉及通话、网络和应急等重要服务……当前,层出不穷的网络安全威胁严重渗透到各国国家安全命脉,成为一个亟须应对的重要问题。

2)算网安全成为世界主要国家夯实安全设施,开展国家竞争的新高地。作为基础设施实现“上云用数赋智”的安全防御机制,以零信任、SASE 等为代表的算网安全技术在国防、政务、能源等领域得到全球各国的高度重视。以零信任为例,2023 年 1 月,欧盟宣布《关于在欧盟全境实现高度统一网络安全措施的指令》(NIS 2 指令)正式生效,其中明确提出所有关键基础设施运营商(CIIO)实施零信任安全模型,并制定了执法和制裁措施,旨在提升欧盟整体的网络安全能力。2023 年 3 月,美国国防部宣布“雷霆穹顶”(Thunderdome)零信任试点计划已完成,宣告并引领陆军和空军联合区域安全堆栈(JRSS)等多安全范式正式向零信任架构迈进。2023 年 10 月,英国国家网络安全中心发布了《零信任:构建混合资产指南 1.0》,对零信任不兼容问题提出了针对性的解决方法,切实助力零信任在落地实施过程中的渗透和融合。

1.2 行业应用:ICT(信息与通信技术)积极响应发展机遇,算网安全打造创新发展新蓝海

从行业视角来看,算网安全涉及通信、互联网、交通、制造、能源等多个行业,产业生态覆盖设备芯片、解决方案、服务提供等多个方面,具有产业规模庞大、产业链条繁杂、产品方案丰富等特征。中国通信标准化协会、算网融合产业及标准推进委员会发布的《算网融合技术与产业白皮书(2023 年)》[4]相关数据显示,2023 年,中国算网融合的产业规模预计超过 1 万亿元人民币,其中,算网安全的市场规模将达到 398 亿元人民币,形成网络安全领域的一片新的发展蓝海。

1)通信行业。算力网络是当前通信行业实现智能化升级演进的重要途径,得到了国内 3 大电信服务商、电信增值服务商的高度认同。算力网络的落地部署,需要大量的泛在计算节点和网络服务节点,增加了网络暴露面,提升了审计溯源难度。算网安全是通信运营商打造安全服务底座的重要支撑。2023 年,中国移动启动了“守望者–算力网络安全信链”计划,组织了多家业内单位参与完成算网安全多个环节的技术验证,为 8 大行业 800 余家政企客户提供了超千次的安全服务,形成了良好的行业影响力。

2)IT(信息技术)行业。大模型时代下,IT 行业面临指数级增长的算力服务需要和低下的算力利用效率问题。依托跨域算力基础设施,构建融合云网络、云安全、云算力于一体的云化互联互通设施是 IT 行业全面提升服务能力的关键手段。算网安全是 IT 行业建设云网安融合一体的重要内涵,零信任、SASE 等代表性解决方案得到国内外龙头企业的大力支持。以 SASE 为例,高德纳(Gartner)公司最新统计显示,2023 年 SASE 全球市场规模已达到 90 亿美元,预计未来 5 年市场规模将以 29.4% 的复合年增长率增长,同时,思科系统公司、微软公司、华为技术有限公司、新华三集团有限公司等国内外龙头企业大力投入 SASE 商业布局,抢占生态链上游。

1.3 能力驱动:数字化因素推动算网安全演进发展

1)数字经济提出了安全防护新体制的发展要求。随着数字化进程的不断深入,软件定义广域网、算力网络、边缘计算、高性能计算等算网融合创新技术得到了普及,形成了一系列的新场景和新业态。当前,智慧医疗、智慧交通、智能金融等智慧场景不断涌现,越来越多的个人、社会信息进入数字化,国民经济迫切需要从基础设施到应用数据全面提升安全防护水平。另外,由于虚拟化、软件化和智能化技术的广泛应用,智能化应用场景打破了传统的网络安全边界,使得基础设施层面的“云网边端数”各个环节都可能成为网络攻击的重点目标。当前,能够兼顾“大连接、高算力、强安全”的安全防护新体制成为千行百业实现数字化转型发展的重点方向。

2)算网安全是数字应用全面发展的必然结果。根据中国通信标准化协会、算网融合产业及标准推进委员会发布的《算网融合技术与产业白皮书(2023 年)》的相关数据显示,以自动驾驶、元宇宙、智能制

造等场景为例,预计到2030年前后,实时算力需求将提升几千倍,网络服务质量需要实现质的升级,安全防护需要兼顾代价高昂的人身安全以及日益严峻的网络安全形势,更是要实现全面升级。作为一种新技术和新工程,算网安全借助零信任、SASE、算网区块链等技术手段,对设备部署、数据系统到平台设计进行全方位的升级,推动数字设施、网络设施、应用设施于一体的安全重构。算网安全能够以用户安全和数据安全为中心,从设施、平台、数据、应用等多个方面,满足创新应用场景的数字化发展需求。

2 算网安全的技术发展及应用实践

2.1 算网安全的技术参考架构

作为一个热点方向,算网安全的技术研讨得到了ICT、安全、金融、能源等多个行业的高度认同,出现了算力网络安全、云网络安全、行业融合安全等多种解决方案。为凝聚行业共识,加快标准化和规范化工作进程,2024年1月,中国通信学会算网融合标准工作组联合产学研各方,正式发布了“T/ZGTXXH 088—2024算网安全通用技术要求”[5],形成了算网安全的参考架构(图1)。

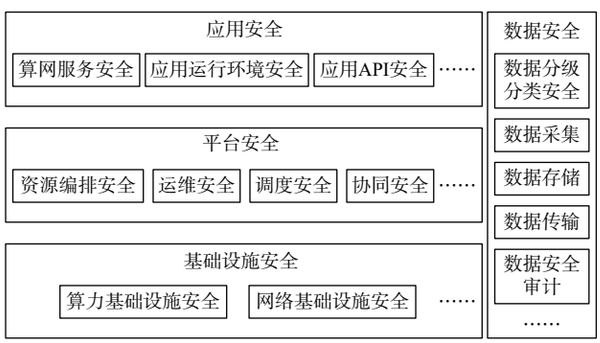

图1 算网安全参考架构

算网安全的技术架构涵盖了设施安全、平台安全、应用安全和数据安全4个方面。

1)设施安全奠定了算网安全的基础底座。设施安全需要统筹考虑算力基础设施、网络基础设施,以及融合设施的安全发展需要,通过构建零信任体系,分离算网基础设施的控制面与数据面,对算网各个节点实现资产隐身保护,同时支持端到端算网环境智能监测能力来自动阻断安全攻击,对云算力中心、边缘计算中心、高性能计算中心、通用传输网络、新型数据网络等设施进行全面的安全防护。

2)平台安全打造了算网安全的智慧中枢。算网平台是兼顾“高算力、大连接、强安全”的关键。平台安全要求在不影响算网调度和运维管理的前提下,提供资源编排、运维调度、业务协同等方面的安全防护能力,具体的技术性要求指标包括平台接口校验、平台安全漏洞管理以及安全能力度量等方面。

3)应用安全丰富了算网安全的创新模式。主要包括算力交易安全、算网服务环境安全、身份管理安全等内容。应用安全需要匹配多种算网服务模型,通过支持算网应用服务全流程编排管理、自动化智能化一体化安全服务运营,能够提供多种情况下算网服务的生命周期管理安全、算网应用的供应链安全以及算网应用算力负载/数据隔离等安全能力。

4)数据安全构成了算网安全的关键要素。数据安全涉及数据采集、数据传输、数据存储、数据处理、数据销毁、数据审计等多个方面内容。数据安全需要满足《中华人民共和国数据安全法》、“数据二十条”等安全监管要求,还需要根据不同的数据实体和敏感级别,分别制定差异化的安全处理机制,通过融合多方安全计算、联邦学习、可信执行环境等隐私计算技术来保障原始算力数据安全和用户隐私,完成对多算力用户数据要素安全流通共享,切实保障算网数据在流通与融合过程中“可用不可见”。

2.2 算网安全的技术应用实践

当前算网安全的技术发展路线出现了算力网络安全、云网络安全、行业融合安全3种主流方案。

2.2.1 算力网络安全

1)算力网络安全是算力网络部署的重要环节。参照国内首个算力网络行业标准“YD/T 4255—2023算力网络总体技术要求”[6]的标准要求,算力网络“基础设施层+编排管理+运营服务”的功能架构取得了行业发展共识。当前,算力网络引入新架构、应用新技术、提供新服务,同时也带来新的安全风险。

(1)基础设施攻击暴露面问题严重:具体包括泛在计算、网络节点增加暴露面,算力节点安全可信水平参差不齐。(2)编排管理管控复杂度全面升级:具体包括算力调度威胁严重,AI(人工智能)模型投毒风险及算力滥用攻击风险。(3)运营服务审计溯源情况

复杂:具体包括算力交易不可信,计算结果不可信等问题。

2)算力网络安全得到了国内运营商的高度重视。中国移动以“算力网络安全一体化全程可信”为目标,从节点接入认证监测、原子化安全能力编排和数据流转安全3个方面出发设计安全保障体系,以实现算力网络端到端的安全可信。中国移动提出了“守望者–算力网络安全智能云池”解决方案,依托其算力网络实验验证平台CFITI(中国未来信息科技基础设施),组织部署集中–分布式2级安全架构,打造具备自主安全、主动安全、弹性安全和智能安全的新型解决方案。2022年,中国移动发布了《算力网络安全白皮书》,2024年,中国移动迭代发布了《算力网络安全一体化全程可信解决方案白皮书》。中国联通以“算力网络一体化安全”为目标,从开放融合、内生免疫、弹性健壮、网安自治4个方面设计体系化安全体制。中国联通的算力网络安全体系架构从算力网络3层架构出发,借助身份标识技术、密码技术、区块链技术等手段,为上层算力网络创新应用提供支撑。2024年7月,中国联通正式发布《算力网络安全白皮书》,为后续的中国联通开展算力网络安全建设指明了方向。

2.2.2 云网络安全

1)云网络安全是“云算力+云网络+云安全”的能力集合。作为IT行业全面提升产业价值的关键发力点和重要增长点,以SASE为代表的云网络安全技术得到了互联网公司的极大关注。SASE以业务与应用需求为导向,融合零信任网络访问、SD–WAN(软件定义广域网)、云原生网络、网络安全即服务等技术能力,是一种基础性、融合性、服务型的云安全技术体系。中国通信标准化协会组织了SASE领域首个行业标准“基于安全访问服务边缘(SASE)网络总体技术要求”编制,对于SASE的基础能力形成了行业共识。

(1)零信任构筑了内生的安防机制:零信任为SASE提供了全新的访问框架,通过一整套面向服务的安全管控机制,提供了无边界、自适应、可持续的安全增强服务。(2)SD–WAN打造弹性的网络底座:借助弹性服务、按需部署等方面的技术优势,SD–WAN能够为SASE提供软件定义、算力随想等方面的能力支撑,提供良好的基础底座。(3)云原生网络提供网络服务微化支撑:云原生网络具备轻量级虚拟化、微服务和服务网格等技术优势,能够全面提升云网安服务一体化协同能力,提高SASE服务管控的精细化程度。(4)网络即服务NaaS是SASE服务化的安全接口:SaaS化的网络安全资源池是NaaS的主要实现方式,NaaS通过网络安全服务功能链SFC,以及API Gateway(应用程序编程接口网关)等方式为SASE提供一站式全流程安全服务入口。

2)云网络安全的行业应用广泛而深刻。IDC(国际数据公司)调查显示,2024年,75%的全球客户已经部署或将要部署SASE架构能力,SASE解决方案受到了全球用户的青睐。根据中国通信标准化协会、算网融合产业及标准推进委员会发布的《SD–WAN/SASE优秀案例2023》[7]显示,SASE已经在国内金融、政务、医疗、保险、通信等行业进行了广泛的部署,出现了一系列有代表性的应用案例。SASE的产业生态包括了电信运营商、开源社区、第三方组织、解决方案提供商、服务提供商、设备提供商等,目前,提供SD–WAN服务的融合安全厂商占据了主导位置(图2)。

图2 国内SASE产业生态

2.2.3 行业融合安全

随着算网融合在交通、政务、安防、医疗、制造、零售等领域的广泛部署,带有行业属性的融合安全方案也不断出现。

1)智慧交通算网安全方案助力路网安全调度。交通场景安全与人身安全息息相关,安全风险较大,安全代价高昂。智慧交通的算网安全方案要求能够全方位保护路网信息的安全交互,面向无人驾驶、自主泊车、AI引擎等路网安全细分场景,对终端、平台、业务提供端到端的安全防护。智慧交通的算网安

全方案重点发力算力安全管控,全力保障算网基础设施安全,提供面向服务的编排安全管理机制,为传统交通行业实现数字化升级转型提供有力的安全支撑。

2)智慧政务算网安全方案奠基政策大模型。生成式大模型与政策应用相结合是当前智慧政务的重点要求,这种场景需要兼顾政务环境的安全敏感需求及政策服务的高可用性。算网安全系统在可信算网基础设施的基础上,从数据和模型 2 个层面出发,设计安全管理方案。在数据层面,对齐中央网信办等部门发布的《生成式人工智能服务管理暂行办法》要求,确保数据信息与管理规范保持无偏差[8]。在模型层面,通过模型优化和安全加固等方法,对包含对抗攻击、越狱攻击、多模态攻击等攻击行为进行针对性保护。

3)智慧零售算网安全方案协助全球化零售网络。全球化零售企业需要打造智慧零售平台,实现线上线下全渠道的无缝连接和精准营销。智慧零售的算网安全方案能够协助用户以“消费者为中心”建立安全服务平台,借助 SASE 安全服务链、算网安全控制器等安全防护手段,解决网络业务和安全业务相分离的设计缺陷,实现防护组件定制化组合,提升安全防护效率。

3 中国算网安全的挑战及发展建议

3.1 主要挑战

作为一种新技术和新工程,算网安全领域整体发展仍然处于初级阶段,面临一系列严峻挑战,需要政产学研用各方共同发力,积极应对。

1)技术创新研究亟须深入完善。与算网基础设施的落地部署相比,算网安全的创新研究仍处于初级阶段。当前,算网安全在整体架构、安全机制、融合要求等方面,仍然需要进一步深入开展技术讨论,聚焦关键技术组织研究力量开展能力攻关。

2)应用部署需要进一步落地实践。尽管多个垂直行业已经开始对算网安全进行试点部署,但应用范围、场景相对集中,缺乏深度场景适配和行业属性的差异化赋能,行业亟须从“千行百业”的数字化转型发展需求出发,建立算网安全的适配模型。

3)产业生态建设需要加强发力。作为一个新方向,现有的算网安全产业在产能聚合、服务创新等方面存在发展进度缓慢等问题,产业生态仍然需要进一步丰富和发展。

3.2 发展建议

1)持续推进标准体系建设。加强以零信任、SASE、区块链、隐私计算等技术为核心的算网安全体系研究,根据算网安全产业发展情况分步分阶建立健全中国算网安全标准体系建设。优先制定基础、共性、关键产品、重点应用等急需标准,再逐步配套能力成熟度评估和产品测试类标准制定,切实满足产业应用需求,发挥标准的引导和示范作用,为算网安全稳定运行提供强有力的保障。

2)加快应用实践规划落地。推动算网安全与算网基础设施同步建设、一体部署,全面提升算网融合重要节点、关键系统、核心应用安全保障水平。广泛征集算网安全创新应用实践案例,并对优秀案例进行推广,打造具有行业影响力的应用标杆。同步针对不同行业的个性化算网安全需求制定具有可推广性的安全服务方案,推动算网安全相关技术规模化落地实践。

3)协同构建产业生态闭环。打造算网安全产业合作平台,组织供需对接、产融合作、市场推广等活动,促进产学研用各方开展交流合作。共建算网安全联合创新体,整合并优化设备商、服务商、运营商、垂直行业用户等各环节的优势能力,加快科技成果转化,有效推动产业链上下游技术创新协作、资源共享,构建良好产业生态闭环,促进中国算网安全高质量、高速度发展。

参考文献(References)

[1] 中华人民共和国国家发展和改革委员会. 关于深入实施“东数西算”工程加快构建全国一体化算力网的实施意见[EB/OL].(2023–12–25)[2024–08–06]. https://zfxxgk.ndrc.gov.cn/web/iteminfo.jsp?id=20303.

[2] 穆琁博, 韩淑君, 柴瑶琳, 等. 算网融合的现状和发展趋势[J]. 信息通信技术, 2022, 16(2): 27−33.

[3] 柴瑶琳, 穆琁博, 张云畅, 等. 算网安全架构、能力要求及发展趋势研究[J]. 信息安全与通信保密, 2024, 22(1): 86−94.

[4] 穆琁博, 韩淑君, 张寒月, 等. 算网融合技术与产业白皮书(2023年)[EB/OL]. [2022–12–01]. http://www.ccnis.org.cn/wh-tiepaper.html.

[5] 算网安全通用技术要求: T/ZGTXXH 088—2024[S]. 北京: 人民邮电出版社, 2023.
[6] 算力网络 总体技术要求: YD/T 4255—2023[S]. 北京: 人民邮电出版社, 2023.
[7] 中国通信标准化协会, 算网融合产业及标准推进委员会. SD–WAN/SASE优秀案例 2023[EB/OL]. [2024–03–01]. http://www.ccnis.org.cn/Assets/file/case/tc6212023sdwan.pdf.
[8] 中央网络安全和信息化委员会办公室. 生成式人工智能服务管理暂行办法[EB/OL]. (2023–05–23)[2024–08–06]. https://www.cac.gov.cn/2023–07/13/c_1690898327029107.htm.

Research and practical applications in security of networking and computing

MU Yubo, CHAI Yaolin, HAN Shujun, BI Libo

China Academy of Information and Communications Technology, Beijing 100191, China

Abstract As a security protection mechanism for convergence of computing and networking, security of networking and computing is a new technology and new engineering. Security of networking and computing involves zero trust, security access service edges, and blockchain of networking and computing and other technologies. It can provide a multi–dimensional security guarantee for the integration of the network, platform, application, and data in a security system. This article outlines the overall development trend of security of networking and computing, extracts the technical reference architecture of security of networking and computing, summarizes three typical application practices including security of computing and network convergence, security of cloud and network, and security of industry integration. Finally, combined with the severe challenges faced by the current security of networking and computing field, three aspects of development suggestions from standard system construction, application practice planning, and industrial ecological construction are given three aspects of development.

Keywords security of networking and computing; computing network security; zero trust; SASE; SD–WAN

（责任编辑　王微）