新一代电信云网内生安全架构研究

Endogenous Security Architecture of Next-Generation Cloud-Network for Telecom

袁超颖/YUAN Chaoying，白景鹏/BAI Jingpeng，
袁淑美/YUAN Shumei，何国锋/HE Guofeng
（中国电信研究院，中国 上海 200123）
(China Telecom Research Institute, Shanghai 200123, China)

DOI：10.12142/ZTETJ.202503002
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20250521.1702.004.html
网络出版日期：2025-05-22
收稿日期：2025-03-25

摘要：数字化时代下，云网融合推动网络向虚拟化、服务化深度演进，传统基于边界防护的被动安全体系难以满足远程办公、智能运维等新兴场景的需求。聚焦新一代电信云网架构演进趋势，系统梳理业界内生安全技术路线，剖析其面临的云网环境下安全可见性不足、安全能力与云网业务协同滞后等挑战，提出一种深度嵌入云网基础设施的内生安全架构。该架构涵盖智能威胁感知、零信任策略联动等关键技术。本研究可为电信云网的安全范式转型及产业实践提供理论支撑与技术参考。

关键词：云网融合；内生安全；零信任；安全架构

Abstract: In the digital era, the cloud-network convergence drives networks toward deeper virtualization and servitization, while traditional passive perimeter-based security systems struggle to meet the demands of emerging scenarios such as remote work and intelligent operations. This paper focuses on the evolution trends of next-generation telecom cloud-network architectures, systematically analyzes existing endogenous security technical approaches in the industry, and examines the challenges they face in cloud-network environments, such as insufficient security visibility and delayed coordination between security capabilities and cloud-network services. We propose an endogenous security architecture deeply embedded in cloud-network infrastructure, which incorporates key technologies such as intelligent threat detection and zero-trust strategy coordination. The proposed architecture and technologies offer both theoretical foundations and technical references for the security paradigm transformation and industrial implementation of telecom cloud-network systems.

Keywords: cloud network convergence; endogenous security; zero trust; security architecture

引用格式：袁超颖，白景鹏，袁淑美，等．新一代电信云网内生安全架构研究 [J]. 中兴通讯技术，2025, 31(3): 3-8. DOI: 10.12142/ZTETJ.202503002
Citation: YUAN C Y, BAI J P, YUAN S M, et al. Endogenous security architecture of next-generation cloud-network for telecom [J]. ZTE technology journal, 2025, 31(3): 3-8. DOI: 10.12142/ZTETJ.202503002

随着云计算、5G、大数据等技术的快速发展，电信行业正加速向云网融合演进，推动企业数字化转型与产业智能化升级。然而，随着网络云化和数字化进程的推进，安全风险日益突出，网络攻击、病毒传播、信息窃取等问题频发。传统以外挂式为主的安全手段主要依赖预设规则和边界防御策略，难以应对云网环境中资源弹性化、攻击手段复杂化、威胁隐蔽化的核心挑战[1]。据报道，2024年7月，AT&T托管在Snowflake云服务公司的约1.1亿个客户的数据发生泄漏，包含6个月内的通话和短信记录，严重影响了用户隐私，甚至危及国家安全[2]。因此，保障云网基础设施的安全至关重要。

当前，业界已经在积极研究云网安全技术，提出了拟态防御、可信计算、零信任等技术路线，通过系统架构的内在特性化解或潜在风险规避，确保云网基础设施的安全。

1 内生安全路线和技术标准

1.1 内生安全的技术演进与框架适配

云网融合环境下，传统外挂式安全防御在应对弹性资源调度、未知威胁检测等场景时暴露明显短板[3]。据Gartner 2023年报告显示，73%的云安全事件源于静态防御策略与动态环境的适配失效[4]。为此，内生安全从系统设计之初将

安全能力融入架构核心，形成“安全基因”，其核心理念是通过重构系统内在架构与运行机制（而非依赖外部修补）实现动态自适应防护[5]。该理论体系最早由中国工程院邬江兴院士团队于2013年提出[6]。当前，内生安全技术路线主要围绕设计网络架构与增量式修补等路线开展。表1从核心理念、技术特点及局限性的维度对比了主流内生安全路线。

目前，内生安全技术在一些典型场景中已取得初步成效，但其研究仍呈现显著的碎片化特征：不同路线在硬件架构、软件协议层面缺乏兼容性标准，尚未形成跨技术路线的统一框架。这种分散性导致安全能力难以按需动态整合[7-8]。

1.2 内生安全与衍生理念的协同路径

除内生安全核心技术外，业界通过架构重组与流程革新提出了多种增强方案（如表2所示）。这些理念虽未完全遵循内生定义，但在信任管理、威胁响应效率等维度与内生安全形成互补。

零信任等理念与内生安全的目标基本相同，但侧重增强特定维度的安全能力[10-11]。例如，零信任侧重解决动态访问控制问题，盾立方主动防御体系强化主动反制能力，集成的自适应网络安全防护（IACD）框架注重提升威胁响应速度。

1.3 内生安全理念相关标准

随着内生安全技术路线的多元化发展，标准化工作成为推动技术落地的关键支撑。目前国际标准化方向主要包括两种：1）面向网络安全产业提出的具有普适性、通用性、推荐性特点的技术标准，从体系架构层面指导各行业采用零信任理念来保护企业应用、网络、用户和数据的安全，如2021年国际电信联盟电信标准分局（ITU-T）发布的《服务访问过程持续保护指南》、2022年国际云安全联盟（CSA）发布的《软件定义边界（SDP）标准规范2.0》；2）面向特定安全领域（如电信网络）提出的具有独特性、先进性、部分强制性特点的技术标准，从网络系统功能、协议流程层面指导具体行业使用零信任解决方案、产品建设和运营网络安全，如2023年第3代合作伙伴计划（3GPP）R18阶段启动了首个零信任技术在5G网络应用的研究课题，2024年韩国运营商SKT通过ITU-T发布了《电信网络零信任模型与安全能力指导方针》。

其中，3GPP R18阶段的零信任研究课题仅完成技术方案收集和总结，未形成标准规范。截至2024年12月，R19零信任研究课题已基本形成结论，包括两大技术增强点：一是，对5G核心网网元进行服务化架构（SBA）协议层数据

表1 网络空间安全领域内生安全路线

路线	理念	特点	局限性
拟态防御内生安全	类比生物自我防御现象的一种主动防御行为，通过DHR构造机制提高拟态区域内装置的抗攻击能力	具有入侵容忍与持续防护能力，安全韧性高	不具有普适性
可信计算内生安全	使用基于硬件安全模块支持下的可信计算平台，形成一条自下而上的完整信任链路	具有健壮性和可信服务能力，成熟度高	扩展能力差
奇安信内生安全	以相关的安全能力组件，用系统工程方法同步构建系统的安全防护能力	联动性强	弹性扩缩能力差
蚂蚁原生安全平行切面	从系统设计开始就全面考虑安全与业务的融合问题，将安全能力整合输出为可遵循的规则和要求	兼具融合与解耦能力	实施难度大，可落地性弱

DHR：动态异构冗余

表2 业界与内生安全类似的理念和实践

路线	理念	特点
零信任	贯彻“持续验证，永不信任”网络安防理念，采用身份管理基础设施，实现访问主体到目标客体的端到端安全控制[9]	持续身份验证，动态访问控制
盾立方主动防御体系	将防御重心从传统的关注保护对象自身安全转变为关注发现和阻断攻击者	基于诱骗的攻击阻断，主动反制探测
IACD框架	在速度（时间）和规模（空间）两个维度上实施感知-理解-决策-行动循环	通过整合各方资源和能力，实现对威胁的全面感知、快速响应和有效应对
DevSecOps	融合开发、安全及运营的全新安全管理模式，将安全尽可能无缝透明地集成到DevOps流程	强调全生命周期安全责任，在需求、研发阶段进行安全介入，实现主动式安全防御
微软：Defend+Copolit	利用人工智能技术增强安全专业人员能力	集成威胁情报，使用AI模型，自动化调查和响应

AI：人工智能 DHR：动态异构冗余 IACD：集成的自适应网络安全防护

采集，用于持续的安全评估和监测；二是，将5G核心网网元作为SBA协议层安全策略执行点，用于实现动态访问控制与精细化安全策略下发[12]。

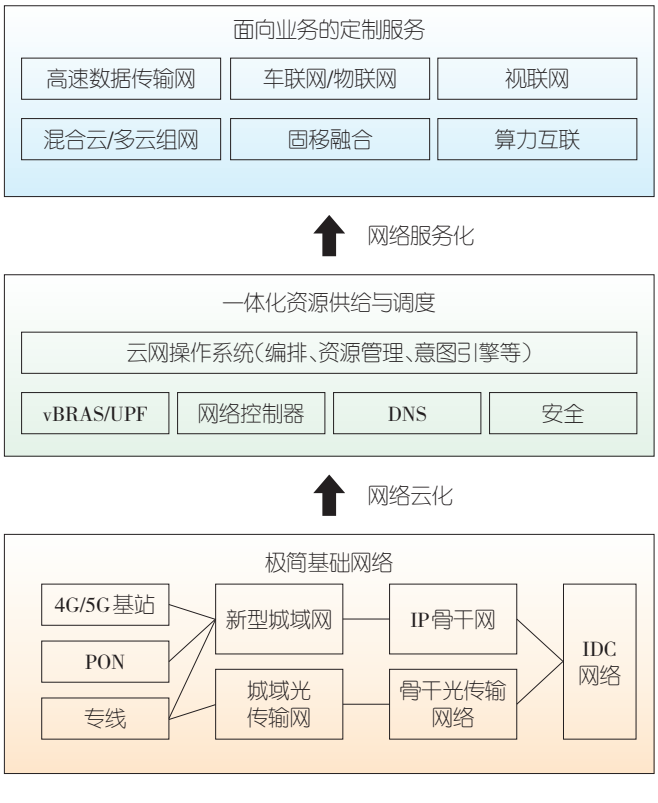
2 新一代电信云网演进与安全挑战

当前内生安全技术已在特定场景取得初步成效，但电信云网因其高动态性、异构融合性及业务复杂性，面临云化组网内安全可见性不足、云网数据与安全数据割裂、安全能力与云网业务协同滞后等挑战，对安全架构提出更高要求[13]。

2.1 新一代电信云网演进趋势及安全挑战

新一代电信云网架构采用3层演进模式（如图1所示）[14]，并呈现以下技术特征：

1）新一代电信云网架构以“云网融合、智能敏捷”为核心，形成三层协同体系。在新一代电信云网架构中，最基础的部分是统一的云网基础设施。这是因为云网基础设施涵盖了4G/5G、高速互联网、IP骨干网、骨干光传输网络等，可通过400G+光传输与IP网络的融合、5G向6G的平滑演进，实现城域智算网络强化，进而构建超大带宽、超低时延的泛在连接底座。在云网基础设施之上是资源部分，而在资源设施之上是统一云网操作系统。统一云网操作系统有助于实现资源智能编排与软件定义控制，支持5G ToB核心网弹性伸缩与流量精准调度。此外，云网操作系统还可以全面支撑数字化平台。业务服务层依托数字化平台将提供工业互联网、车联网等定制化服务，升级算力网络组网能力与端网协同效能，构筑智能业务生态体系。



DNS：域名系统　　PON：无源光网络
IDC：互联网数据中心　　UPF：用户面网元
IP：互联网协议　　vBRAS：虚拟宽带远程接入服务器

图1　新一代电信云网体系

2）电信云网体系正经历颠覆性变革。在场景层面，万物智联催生工业控制、车路协同等高实时性业务，资源、数据跨域流动增加，访问主体身份多元化，访问路径复杂，隐私泄露风险呈指数级上升；在架构层面，业务由传统单体架构转变为以云化、微服务化为主的架构，呈现出更多的弹性和动态特征；在技术层面，人工智能（AI）虽赋予网络异常检测等新能力，其模型脆弱性却可能被对抗攻击利用，而量子计算等前沿技术在提升算力的同时，也为加密体系埋下破解隐患。

3）传统安全体系与新一代电信云网体系的变革矛盾日益凸显。云网环境动态扩展与业务深度融合导致传统安全机制难以实时感知全域风险，安全数据与业务逻辑割裂进一步阻碍威胁深度分析。静态防御策略无法匹配网络资源弹性伸缩需求，尤其在应对未知威胁时暴露出响应迟滞、自适应能力薄弱等缺陷。而过度依赖黑名单的单一信任机制，在零信任架构缺失场景下系统更易被高级持续性攻击穿透[15]。这些问题本质上源于传统安全架构与云网“泛在连接、智能内生”特性的脱节，因此亟需构建覆盖监测、分析、决策的全链路主动防护体系。该体系通过安全能力与网络弹性、业务逻辑的深度协同，实现风险动态可视、防护随网智变、信任逐级验证的闭环目标。

2.2 新一代电信云网内生安全理念

当前业界主流内生安全技术（如拟态防御、可信计算等）在适配新一代电信云网时面临瓶颈：其一，部署成本高，拟态防御依赖动态异构冗余（DHR）构造，局部部署效果有限，全局部署成本高；其二，扩展能力差，可信计算依赖定制化硬件，难以匹配运营商跨域业务场景的弹性需求；其三，安全与业务断层，安全切面过于强调安全与业务解耦，实施难度大，可落地性弱[16-17]。

立足于电信自身云网优势、业务特色，综合考虑业界主流内生安全理念在云网安全领域的适用性与不足，以及监管、新兴技术发展趋势，本文提出以“主动免疫、健壮可信、自适弹性”三大特征为核心的云网内生安全理念：

通过深度解析业务逻辑，感知异常行为，实现从被动防守向主动防御的转变；通过可信机制实现硬件、软件、身份的信任传递，有效降低安全风险；通过安全能力随业务的动态调整，支持系统的自我发现、自我修复和自我平衡[18]。

3 新一代电信云网内生安全架构

基于“主动免疫、健壮可信、自适弹性”理念，本文提出面向电信云网内生安全架构（如图2所示），为未来电信云网的安全范式转型及产业实践提供理论支撑。该架构包括感知、协同、服务3层联动机制重构安全体系：在感知层，通过在“时间、空间、全栈”3个维度部署安全能力执行单元，实现云网域内安全风险感知、检测和防护；在协同层，AI驱动的安全中台与云网操作系统联动协同，推动云网安数据深度融合，同时实现安全能力动态部署；在服务层，安全中台将防护需求抽象为可编排的微服务策略包，连同云网操作系统提供面向不同业务场景的云网安一体化定制服务。下面我们将对电信云网内生安全架构的核心能力和关键技术展开说明。

3.1 新一代电信云网核心能力

1）构建覆盖云网基础设施“时间、空间、全栈”的内生安全执行体系。内生安全执行单元主要包括统一安全Agent和安全网关，深度嵌入云网基础设施层，提供覆盖终端、网络、数据的一体化全栈安全能力。内生安全执行单元通过统一接口与安全中台联动，实现安全状态多粒度感知、

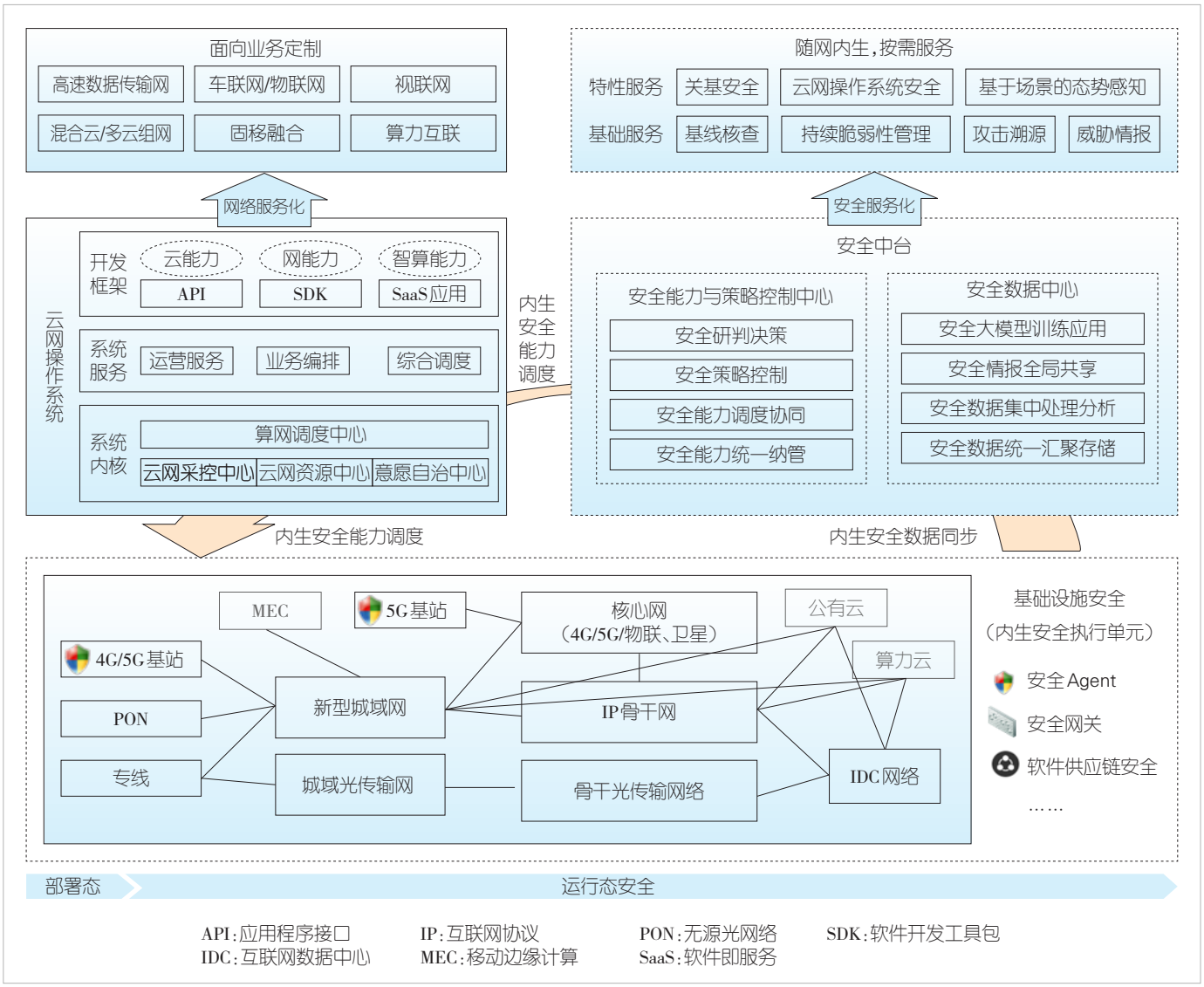


图2 新一代电信云网内生安全架构

威胁处置闭环执行，可破解传统架构中“跨域不可见、处置不同步”的黑盒效应，最终达成威胁自发现、攻击自防护、信任自传递的主动防御目标。

2）AI驱动的安全中台与云网操作系统高效协同。依托云网操作系统的资源拓扑感知能力，安全中台实时获取基础设施层流量特征、资源层弹性状态及业务层意图信息，借助云网操作系统充分整合云、网、安、算力资源，通过安全大模型构建，指导启动智能决策程序，形成全局安全协同剧本，并向云网操作系统发出安全资源管控、网络管控、安全策略管控请求，实现云网安全自主决策、自适弹性。

3）面向全场景的云网安全一体化定制服务。基于业务场景特征（如工业控制时延敏感度、车联网身份动态性），安全中台将防护需求抽象为微服务策略包，通过云网操作系统的智能编排引擎，将内生安全执行单元按需注入基础设施层的传输节点、资源层的虚拟化实例及业务层的应用接口。此外，安全中台与云网操作系统支持根据业务负载自动扩缩防护单元密度，实现从“通用安全基线”到“场景免疫”的跃迁。

3.2 新一代电信云网关键技术

3.2.1 统一安全Agent

统一安全Agent内生部署在服务器操作系统上，提供覆盖终端、网络、数据的一体化全栈安全能力，可通过统一采集流量、行为、日志、资产等数据，实时向安全能力中心上报主机安全数据。安全中台通过安全能力中心查看主机防护状态和检测结果，同步向安全能力中心下发安全策略配置，实现安全管理平台的统一。该机制攻克了传统云网域内安全监测碎片化、防御响应迟滞的难题，解决了云网基础设施域内安全自治的监测、防御能力不足的问题，实现云网域内安全自主感知、检测和防护。

3.2.2 安全网关

安全网关与统一安全Agent协同构建云网基础设施的主动防御体系，其核心价值在于跨域协同与全栈防护[19]。相较于传统网关堆叠式架构，内生安全网关通过标准化网元（如C-IWF、小基站网关）实现与业务的深度集成，将安全能力嵌入信令交互、协议解析等核心环节，显著提升威胁拦截效率。同时，其全栈检测能力覆盖基础设施层至业务协议层，通过流量异常识别、用户行为建模及网关自身完整性监测，形成“物理-逻辑-业务”三位一体的纵深防御。依托安全中台的AI大模型，网关可动态调整策略，构建分布式信任链，在复杂云网环境中实现对未知威胁的主动响应。未来，内生安全网关将进一步向多域分布式架构演进，通过跨域策略实现与通感融合、空天地一体、无源物联等新兴业务的安全协同。

3.2.3 云网操作系统

云网操作系统作为资源调度的智能中枢，通过统一网络、算力及安全资源，实现“业务需求-资源分配-安全策略”的联动。其策略控制中心与安全中台深度耦合，将威胁分析结果实时转化为资源编排指令，精准部署安全执行单元至传输节点、虚拟实例及业务接口，确保防护能力随业务弹性扩缩、动态适配。

4 结束语

当前通用型安全技术标准难以精准适配电信云网“内生安全、动态弹性、全域协同”的技术特性，其落地指导性与场景适配性显著不足，亟需加速标准化工作的推进，以更好地满足实际需求。

本文在分析电信云网内生安全架构和实现方案的基础上，将从研究课题出发，逐步推动电信云网架构的标准化，特别是针对具体电信云网场景的安全需求，如定制化网络安全场景的标准化制定工作。同时，将持续关注3GPP、ITU等国际标准化组织的标准演进动态，深度参与3GPP R20/R21等国际标准的制定工作，提出内生安全与云网融合协同的研究课题方向，全面评估和研判内生安全对电信云网安全建设与应用的影响。

新型信息基础设施的加速演进与数字化业务的深度融合，正推动电信云网安全范式从“外挂式修补”向“内生式免疫”跨越。本文基于“主动免疫、健壮可信、自适弹性”的理念，构建了覆盖云网基础设施层、资源操作系统层、业务服务层的三维内生安全架构，通过全域感知、智能协同与场景化服务三重机制，破解了传统安全体系在动态弹性、跨域信任、未知威胁应对等维度的结构性矛盾。当前，尽管云网内生安全领域已有一定的研究成果，但面对量子计算冲击、高级持续恶意攻击（APT）攻击链隐蔽化等威胁形态的持续进化，仍需在动态信任评估、安全能力原子化编排、零信任架构标准化等方向深化探索。

参考文献

[1] 王瀚洲, 刘建伟. 网络内生安全研究现状与关键技术 [J]. 中兴通讯技术, 2022, 28(6): 2-11. DOI: 10.12142/ZTETJ.202206002
[2] CN-SEC中文网. 几乎所有客户被波及！美国电信巨头AT&T再曝重大数据泄漏事故 [EB/OL]. (2024-07-17)[2025-03-25]. https://cn-sec.com/archives/2967820.html
[3] LIU X Y, WANG H Z, LI C X. A review of endogenous security

research [J]. Electronics, 2024, 13(11): 2185. DOI: 10.3390/electronics13112185
[4] 199IT. Cybersecurity Insiders: 2023年云安全报告 [EB/OL]. (2023-07-29) [2025-03-25]. https://www. 199it. com/archives/1625456. html
[5] 中国电信. 云网内生安全白皮书 [R]. 2023
[6] 邬江兴. 网络空间内生安全发展范式 [J]. 中国科学: 信息科学, 2022, 52(2): 189-204
[7] JI X S, WU J X, JIN L, et al. Discussion on a new paradigm of endogenous security towards 6G networks [J]. Frontiers of information technology & electronic engineering, 2022, 23(10): 1421-1450. DOI: 10.1631/FITEE.2200060
[8] 吴建军, 孙黎, 王东晖, 等. 面向6G网络的内生安全架构和关键技术思考 [J]. 中国科学: 信息科学, 2024, 54(12): 2881-2904
[9] AHMADI S. Zero trust architecture in cloud networks: application, challenges and future opportunities [J]. Journal of engineering research and reports, 2024, 26(2): 215-228. DOI: 10.9734/jerr/2024/v26i21083
[10] 王群, 袁泉, 李馥娟, 等. 零信任网络及其关键技术综述 [J]. 计算机应用, 2023, 43(4): 1142-1150
[11] 刘云峰, 翟大海, 段张珏. 零信任网络理念、架构及关键技术综述 [J]. 现代传输, 2024(5): 61-70
[12] 3GPP. Study on enablers for zero trust security: 3GPP TR 33.794 [S]. 2023
[13] 史凡. 云网络: 云网融合的新型网络发展趋势 [J]. 中兴通讯技术, 2022, 28(1): 8-10. DOI: 10.12142/ZTETJ.202201004
[14] 中国电信. 云网融合2030技术白皮书 [R]. 2020
[15] DHIMAN P, SAINI N, GULZAR Y, et al. A review and comparative analysis of relevant approaches of zero trust network model [J]. Sensors, 2024, 24(4): 1328. DOI: 10.3390/s24041328
[16] 粟栗, 庄小君, 杜海涛, 等. 6G网络内生安全架构研究 [J]. 中国科学: 信息科学, 2022, 52(2): 205-216
[17] QiAnXin Strategy Consulting and Planing Department & QiAnXin Industry Research Center. Built-in security: new generation of network security frame system and practice [M]. Beijing: People's Posts and Telecom Press, 2021
[18] 何国锋, 段赟, 刘东鑫, 等. 面向未来网络的高可信内生安全体系研究 [J]. 网络安全与数据治理, 2023, 42(4): 45-50. DOI:10.19358/j.issn.2097-1788.2023.04.008
[19] PATEL N. Secure access service edge (SASE): evaluating the impact of converged network security architectures in cloud computing [J]. Journal of emerging technologies and innovative research, 2024, 11(3): 12

作 者 简 介

袁超颖，中国电信研究院网络安全研究工程师；主要研究方向为5G/6G网络安全、AI安全、零信任；发表论文3篇，申请专利5项。

白景鹏，中国电信研究院网络安全研究工程师；主要研究方向为5G/6G网络安全；发表论文5篇，申请专利10余项，获授权国家发明专利4项。

袁淑美，中国电信研究院网络安全高级工程师；主要负责零信任安全网关、AI安全、软件供应链安全等多个领域的内生安全解决方案和产品规划工作。

何国锋，中国电信研究院安全技术研究所所长，教授级高级工程师；主要从事网络安全、软件安全、PKI体系的研究和规划工作。