

面向云网融合的零信任安全技术研究综述

王子豪¹, 崔鹏帅^{1,2,3}, 潘璠¹, 胡宇翔^{1,2,3}, 田乐^{1,2,3}, 陈鸿昶¹, 郭江兴^{1,3}

(1. 信息工程大学信息技术研究所, 河南 郑州 450002; 2. 先进通信网全国重点实验室, 河南 郑州 450002;
3. 网络空间安全教育部全国重点实验室, 河南 郑州 450002)

摘要: 云网融合通过智能协同调度云计算和网络资源, 实现了更加高效的信息基础设施服务, 但同时也带来了安全边界模糊和策略动态变化等安全问题。基于零信任理念的安全架构打破了传统内外网边界, 能够有效应对云网环境中的安全威胁。首先, 系统梳理了云网融合的研究进展, 并深入分析了云网融合场景下的安全风险; 然后, 针对云网融合的安全需求, 阐述了零信任机制在云网融合场景下的防护优势, 并对零信任安全的概念、关键技术与核心架构进行了论述; 随后, 着重探讨了云网融合场景下引入零信任安全防护机制的必要性与实施路径; 最后, 总结了云网融合零信任安全研究面临的挑战, 展望了未来的发展方向。

关键词: 云网融合; 零信任安全; SD-WAN; 云计算安全; 安全访问服务边缘

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2026015

Survey of zero trust security technology for cloud network integration

Wang Zihao¹, Cui Pengshuai^{1,2,3}, Pan Fan¹, Hu Yuxiang^{1,2,3},
Tian Le^{1,2,3}, Chen Hongchang¹, Wu Jiangxing^{1,3}

1. Institute of Information Technology, Information Engineering University, Zhengzhou 450002, China
2. National Key Laboratory of Advanced Communication Networks, Zhengzhou 450002, China
3. National Key Laboratory of Cyberspace Security, Ministry of Education, Zhengzhou 450002, China

Abstract: Efficient information infrastructure services are realized through the intelligent collaborative scheduling of cloud and network resources in cloud-network convergence. However, security issues such as blurred security boundaries and dynamic policy changes are also introduced. The traditional boundaries between internal and external networks are broken by the security architecture based on the zero trust concept, and security threats in the cloud-network environment can be effectively addressed. First, the research progress of cloud-network convergence was systematically reviewed, and the security risks in this scenario were analyzed in depth. Secondly, aiming at the security requirements, the protection advantages of the zero trust mechanism in this scenario were clarified, and the security concept, key technologies, and core architecture of zero trust were discussed. Subsequently, the importance

收稿日期: 2025-04-21; 修回日期: 2025-12-16

通信作者: 胡宇翔, chxachxa@126.com

基金项目: 国家重点研发计划 (No.2023YFB2903902); 中原科技创新领军人才项目 (No.244200510038); 国家自然科学基金 (No.62176264)

Foundation Items: The National Key Research and Development Program of China (No.2023YFB2903902), Science and Technology Innovation Leading Talents Subsidy Project of Central Plains (No.244200510038), The National Natural Science Foundation of China (No.62176264)

and implementation paths of introducing the zero trust security protection mechanism in the cloud-network convergence scenario were explored. Finally, the challenges faced by the research on zero trust security in cloud-network convergence are summarized, and future development directions are prospected.

Keywords: cloud-network integration, zero trust security, SD-WAN, cloud computing security, secure access service edge

0 引言

近年来, 5G^[1]、云计算^[2]、大数据^[3]和算力网络^[4]等新兴网络技术深刻变革了网络发展格局。2024年我国云计算市场规模达8 288亿元人民币, 预计2027年我国云计算市场将突破2.1万亿元人民币^[5]。云计算的快速发展推动网络运作模式从单一化向云与网的无缝衔接、协同运作演进。传统通信网络的数据传输等能力已难以满足当前网络发展的需求, 云网融合^[6]成为通信网络发展的必然方向。通过对计算与网络资源实施集中化管控和云端部署, 可以实现资源的统一管理与优化配置, 提升资源利用率 and 应用部署的灵活性, 进而提高网络性能与服务质量。应用软件定义网络 (software-defined network, SDN)^[7]和网络功能虚拟化 (network function virtualization, NFV) 等技术, 云网融合网络实现了业务逻辑和底层资源的解耦; 同时, 云网借助面向服务的容器编排调度能力, 推动服务编排向算力网络资源开放对接。5G网络是云网融合的典型应用场景。5G核心网采用控制平面与转发平面分离的架构, 支持网络功能的灵活部署和弹性伸缩, 通过服务注册与发现机制实现网络功能的即插即用, 同时依托网络切片^[8]和边缘计算^[2]实现业务和网络的按需定制。软件定义广域网 (software defined wide area network, SD-WAN)^[9]、分段路由 (segment routing, SR)^[10]等新型网络承载技术的出现, 进一步推动了云网架构的演进, 使网络呈现资源多级分布的特征, 最终实现云、边、端一体化协同调度。

然而, 网络云化不仅导致网络安全边界趋于模糊, 还使得云计算环境中的网络安全威胁日益增多。最初的网络边界^[11]通过边缘路由器的物理或逻辑配置实现。随着网络技术的发展, 网络边界逐渐演进为包含防火墙^[12]、网络代理^[13]和入侵防御系统 (intrusion prevention system, IPS)^[14]等

的网络安全控制层。这些安全系统通过协同联动构建纵深防护体系, 其本质上仍遵循传统边界安全模型的静态信任假设, 即依据网络拓扑位置赋予内网设备默认信任权限。然而, 随着设备的激增、云服务的普及和移动性需求的增加, 传统网络边界逐渐消融。从分布式拒绝服务 (distributed denial of service, DDoS)^[15]攻击、恶意软件感染到数据泄露、身份盗窃, 各类网络安全威胁层出不穷, 给云网安全带来巨大挑战。尤其是在人工智能和大数据技术飞速发展的背景下, 黑客攻击手段日趋复杂和隐蔽, 传统的安全防御机制已经无法满足云网在身份验证、动态访问控制、数据隐私保护和数据完整性保障等方面的安全需求^[16-17]。

为应对上述新兴安全风险, 零信任^[18]安全模型被提出。零信任安全模型重点关注资源保护, 遵循“永不信任、持续验证”原则, 通过更细粒度的边界防护抵御恶意攻击, 以动态化方式实现全网安全防护。在该模型下, 应用程序须完成身份的授权与验证, 方可访问应用程序基础设施。云网融合环境具有资源共享、设备协同运行的特征, 不同客户的应用资源和网络资源在物理层面高度融合, 难以划分明确的物理边界。在云网融合环境中部署零信任安全架构, 可以通过动态访问控制和持续身份认证等安全机制, 将传统的防御边界延伸至系统全维度, 进而构建一体化安全防护体系。

目前, 围绕云网融合技术的研究已有很多, 但针对该领域的研究综述匮乏, 且现有研究中对云网融合场景下的安全性问题鲜少探讨。鉴于此, 本文以云网融合的发展演进、潜在的安全威胁为切入点, 同步梳理零信任安全的相关技术体系与现存问题, 具体研究内容如下。

1) 梳理了国内外云网融合技术的发展趋势与研究现状, 归纳了云网融合典型应用场景下的相关研究, 并对SD-WAN的技术特点与架构体系

展开深入分析。

2) 深度剖析了云网融合存在的安全问题, 对零信任安全相关技术进行了介绍。

3) 在深入研究安全访问服务边缘技术的基础上, 阐述了在云网融合场景中实施零信任安全访问的重要性, 并提出未来构建云网融合安全体系的可行研究方向。

1 云网融合概述

1.1 云网融合的基本概念和技术特征

云计算技术涵盖计算、存储、网络等领域, 能够为用户提供高效的计算资源获取渠道, 支持用户根据业务实际需求灵活调整资源配置。网络设施作为连接和通信的基础, 能够保障多样化业务与应用的高效运行。云网融合将云计算与网络技术有机结合, 实现云与网之间的无缝衔接与协同运作, 通过统一管理和优化配置计算与网络资源, 提升资源利用率 and 应用部署的灵活性, 最终显著提高网络性能和服务质量。云网融合的整体架构如图 1 所示, 从下至上依次为云网基础设施层、云网功能层、云网控制层、云网服务层 (又称为“云网大

脑”) 和云网服务层。

云网基础设施层主要包括接入设备 (终端设备)、通信基础设施、基站等, 承担数据中心间的数据交换与传输任务。在云网融合背景下, 该层须具备网络可编程能力, 从而适应动态变化的网络需求。云网功能层围绕业务需求展开计算与网络资源的协同调度, 其中 NFV 技术可以实现网络功能的按需加载与动态卸载, 显著提升了网络的灵活性。云网控制层被视为云网融合架构的核心层, 负责对云网资源进行抽象与编排, 依托云网智能引擎、云网切片等实现网络资源的动态高效管理。云网服务层通过云接口和通用功能平台, 为用户提供个性化的服务支持。云网融合的安全防护能力贯穿架构各层级, 借助动态策略适配不同场景, 实现全方位的安全防护。

云网融合技术具有三大特点: 其一是虚拟网元在网络云上的统一承载, 这需要依赖异构计算能力来保障多专业虚拟网元的高效运行; 其二是网络云的服务能力具备开放性, 可以支持差异化、弹性化的网络服务模式; 其三是安全体系的

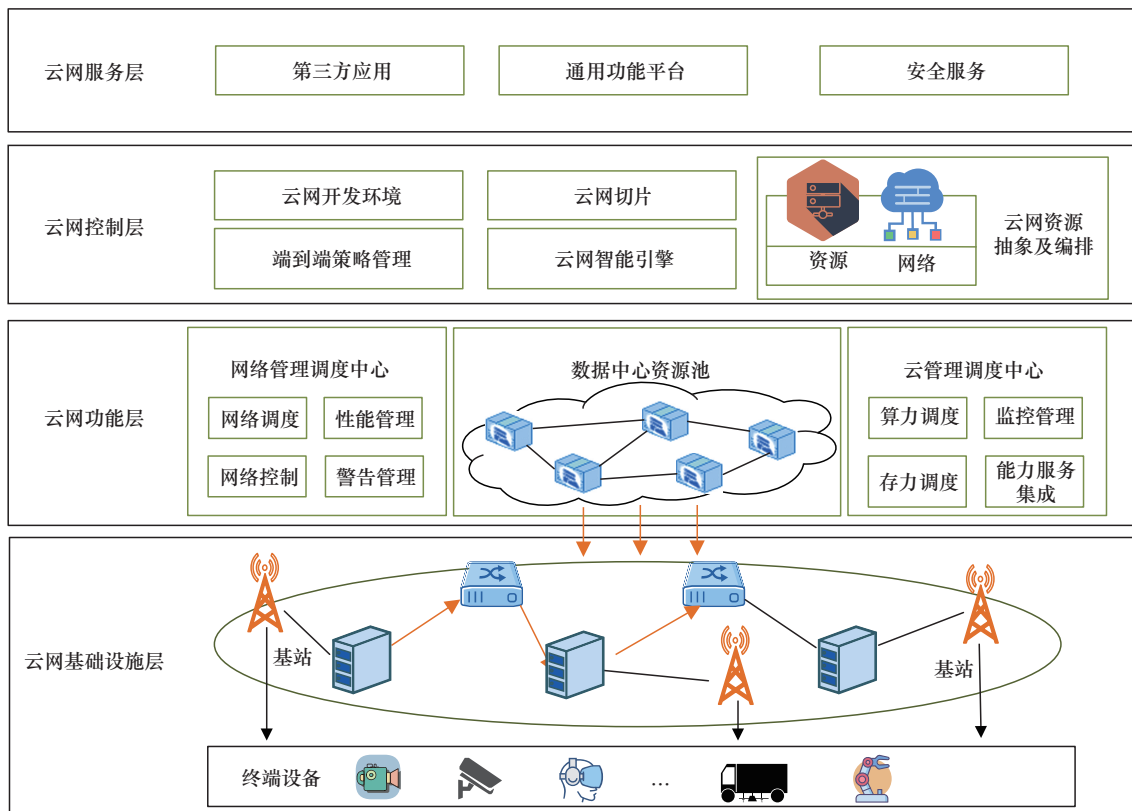


图 1 云网融合的整体架构

自主可控性，即通过构建全链路自主可控的安全防护体系，为云网融合的运行提供高安全等级的环境支撑。

SD-WAN是实现云网融合的核心技术之一，它是SDN^[19]在广域网场景的落地应用。SDN、NFV、移动边缘计算（mobile edge computing, MEC）等也是实现云网融合的关键技术，三者因在功能目标和部署方式上存在差异，故面临的安全问题也各异。移动边缘网络（mobile edge network, MEN）通过将计算、存储和网络能力下沉到靠近用户的网络边缘，显著提升了带宽利用率、服务的实时性和可靠性，成为支持5G和新兴业务场景落地的重要技术。然而，MEN的分布式架构带来了边缘节点安全防护、数据传输安全、用户隐私保护等新的挑战。

1.2 软件定义广域网

广域网作为核心通信基础设施的组成部分，致力于实现地理上分散的系统与设备之间的互联^[21]。在传统广域网的发展过程中，业界先后提出了多种技术方案，主要包括异步传输模式、帧中继、多协议标签交换及虚拟专用网等。这些技术方案在可靠性、服务质量和成本方面各有侧重，但由于自身系统设计的局限性，这些方案在自适应路由、负载平衡、优先级管理及对专业硬件的依赖等方面存在不足，难以满足当前网

络的部署和管理需求。相比之下，SD-WAN基于宽带互联网构建，能够以较低的成本实现QoS保障^[22]，并提供网络管理、运维操作、自动化部署与架构简化的技术机制^[23]。SD-WAN不仅继承了SDN的集中控制能力，还将SDN中控制平面和数据平面解耦的特性应用于广域网的互联运营。

SD-WAN的核心优势之一就是集中控制能力。该特性不仅为网络管理员提供了便捷的网络监控与测量能力，也为流量工程的实施奠定了基础。正因如此，现有研究大量聚焦于如何有效监控网络状态并提升其运行效率。表1对现有SD-WAN相关研究成果进行了系统梳理。本文将SD-WAN的研究方向划分为策略优化、流量工程和网络安全3类。策略优化聚焦于SD-WAN的性能优化，涉及控制层的自动化服务编排与部署、动态路由调整及资源分配等；流量工程基于网络流量特征，致力于流量的精细化处理与深度分析；而网络安全则旨在为SD-WAN构建更完备的安全机制，包括增强系统容错与网络可靠性、保障路径可编程安全、实现恶意流量检测与防护等能力。

文献[23]提出结合基于置信度的Bootstrap方法和神经网络模型来确定流量大小的间隔与链路质量参数，并通过评估成本与服务等级协议满意度，实现对SD-WAN流量调度策略的优化。文

表1 现有SD-WAN研究成果汇总

研究方向	研究内容	文献	研究目标	实现方法	适用场景	解决方案
流量工程	流量调度	[23]	服务水平协议满意度、成本	基于置信度的Bootstrap方法结合神经网络模型	SD-WAN	基于置信度的Bootstrap方法结合神经网络模型来确定流量大小的间隔和链路质量参数，设计成本感知型在线流量调度框架
	QoS保障	[24]	服务可用性	深度强化学习	SD-WAN	采用不同的深度强化学习算法提高SD-WAN的服务可用性
策略优化	性能优化	[25]	QoS，成本	多智能体强化学习	分布式边缘网络	基于协作式多智能体强化学习框架，智能体通过交换少量信息来增强性能
	时延监控	[26]	时延小	简单双向主动测量协议	软路由	应用简单双向主动测量协议监控SRv6路径的时延
	QoS保障	[27]	QoS、成本	强化学习	企业WAN	在SD-WAN上采用强化学习算法提高QoS和降低成本
	路由策略优化	[28]	QoS和流量预测	路由决策预测，基于意图	SD-WAN	提出基于意图的策略优化模型
网络安全	离线交换机重路由	[29]	负载均衡	可预测流量工程	WAN	使用基于P4运行时的细粒度流控制器重分配和流重路由来制定优化问题
	恶意流量检测	[30]	异常流量监测	孤立森林	SD-WAN	基于分布式动态特征提取流量特征，提出采用孤立森林模型检测恶意流量

献[24]采用深度强化学习算法,提升网络的可用性与故障恢复能力。这两项研究均借助智能算法显著改善了网络流量的传输质量,但未对网络故障恢复及安全相关问题展开深入探讨。文献[25]设计了一种基于强化学习的编排平面,利用本地网络信息实施 SD-WAN 策略,通过多智能体强化学习技术实现不同服务质量需求与成本约束下的网络适配。然而,该研究既未分析边缘代理可能面临的安全风险,也未考虑异构网络环境中智能体的实际执行问题,导致其方案在云网融合的异构广域网场景下难以实现有效部署与应用。

本节仅梳理了部分针对 SD-WAN 安全的研究,关于云网融合环境下更广泛的安全风险与挑战,将在第 1.3 节中系统阐述。

1.3 云网融合面临的安全问题

云计算与网络技术的深度融合,在显著提升网络管控能力与应用部署灵活性的同时,也引入了大量未知的安全风险。这些安全风险既可能隐藏在云环境内部,也可能暴露于网络传输层面。值得注意的是,在不同的应用场景下,云网融合面临的安全风险不同。本节主要探讨通用核心广域通信网中的云边协同场景的安全性问题。作为一种融合云计算与网络资源的新型架构,云网融合的各个层面都面临特有的安全挑战。本节结合云网融合的体系架构,系统分析各层存在的安全问题,其中重点关注云网基础设施及管理层安全,并将云数据安全、云应用安全等作为网络接入边界的关键要素纳入整体安全框架进行讨论。

1.3.1 云网基础设施面临的安全风险

云网融合基础设施由物理基础设施和虚拟基础设施两部分构成,其安全防护体系覆盖物理基础设施保护、虚拟化网络保护、计算负载保护和管理平面保护等方面。SDN、NFV 等技术在提升传统网络的灵活性与可编程能力的同时,也引入了新的安全隐患。以 SDN 为例,其面临的安全风险主要集中在两个方面:其一,集中式控制架构存在单点攻击和故障风险。攻击者通过部署伪造的控制器,伪装成主控制器以劫持对 OpenFlow 交换机的控制权;其二,控制器与数据转发设备之间的南向接口易遭受攻击,进而影响网络的可用性和完整性等性能。具体而言,一方

面,SDN 集中式控制架构使 SDN 控制器成为攻击者的主要攻击目标。这是因为该控制器既是网络的集中管控节点,也可能成为单点故障源。文献[31]对 SDN 中的安全威胁与防御机制展开了系统化分析,并提出了一种基于渗透路径的新型分类方法。一旦攻击者通过定向攻击攻破控制器,便可以篡改其代码库、修改流量控制策略,进而在网络节点中过滤或隐藏恶意流量,实现对网络数据的操控。另一方面,控制器与转发设备之间的南向接口同样是攻击者的重点攻击对象。由于缺乏健全的身份认证机制,攻击者可以控制甚至伪造虚拟转发设备,并通过伪造或篡改数据包等手段破坏转发平面的性能、可用性和完整性。

1.3.2 云网功能层面临的安全风险

云网功能层主要负责对网络路由和流量进行管理和控制。在云网基础设施层中,数据的转发完全依赖于控制器下发的流表。控制器通过实时感知网络状态的变化,将应用平面的流量调度决策以流表项的形式下发给数据平面,用于指导数据转发操作。然而,一旦控制器发生故障或停止运行,对应的转发路径将随即失效,关联的交换机会同步进入离线状态,导致网络中的数据流脱离控制器的管控^[32]。由此可见,网络路由的可编程性是控制器失效场景下保障网络性能的关键支撑,而降低控制器失效概率、恢复路由的可编程性则是云网通信安全的基础防护措施。在此背景下,当承载身份授权信息的加密数据包在传输过程中遭遇路由中断或恶意篡改时,如何实现路由故障的快速恢复与高效重路由,成为云网安全防护领域亟待解决的问题。

1.3.3 云网融合数据面临的安全风险

在云网融合环境中,保障数据安全至关重要。数据在存储、传输、使用等环节发生泄露、丢失或被篡改,往往会造成严重的后果。当前数据面临的安全问题主要包括数据泄露、敏感与隐私数据保护不足、数据保护制度不健全等。在云网环境中进行大规模数据的上传、处理与分析时,如何提供更加安全可靠的隐私保护能力,已成为行业面临的主要挑战。现阶段,数据安全的常规防护手段主要围绕数据加密、信道加密等技术展开。安全套接层(secure sockets layer, SSL)

作为保障网络通信安全与数据完整性的经典加密协议，在跨域（如跨云、跨边缘节点和跨中心云）数据流动场景中，可以有效防止数据在传输过程中被非法截获或篡改。作为云网融合的基础安全技术，SSL协议通过加密、身份认证和数据完整性保护等手段保障数据传输安全，但其在密钥管理、性能开销和信任体系方面仍存在缺陷，需通过技术迭代与架构优化加以完善。联邦学习通过分布式训练机制和加密技术，实现了云网融合环境的数据隐私保护，具有显著的技术优势。然而，针对联邦学习的各类恶意攻击已成为其核心安全威胁，易导致系统层面的隐私泄露。此外，该技术在云网融合环境下还面临中间参数泄露、抗恶意攻击能力不足、计算开销过大等现实问题。因此，如何通过技术融合创新与架构优化设计，构建兼顾数据隐私、运行效率与模型性能的安全数据防护框架，成为当前亟待攻克的难题。

1.3.4 云网控制层面临的安全风险

在云网融合环境中，管理平面的访问权限一旦被攻破，攻击者即可无限制地访问云数据中心。因此，必须在云网控制层部署严格的安全机制，对身份、权限及操作实施全方位的管控。针对策略管理问题，文献[33]提出了一种基于关键属性的策略描述方法，旨在统一混合云环境下的异构策略。此外，该研究通过引入“阶段”属性标识的层次聚类算法，实现了策略的细粒度划分。然而，尽管该方法能够满足特定的静态安全需求，却未充分考虑策略执行过程中对动态环境因素的依赖。

安全策略通常以复杂且依赖网络拓扑的访问控制列表形式实现。虽然通过云管理平面可以便捷地执行虚拟机迁移、弹性资源供给，以及计算、网络和存储资源的动态配置，但首先必须确保该管理平面具备完善的身份认证、访问控制与日志监控等安全机制。其中，控制层权限管理的混乱是核心风险之一，传统权限模型难以适应云环境中资源动态扩展和多租户共享的需求，容易引发权限滥用或内部人员越权操作的问题。

云网管理平面对所有虚拟网元都具有极高的读写权限，一旦被攻陷，攻击者即可获取对所有

虚拟网元的访问权。因此，实施细粒度的权限管控至关重要，这能够帮助客户安全地管理自身用户及管理员。无论是服务提供方还是资源使用方，都应始终遵循最小权限原则，仅为用户、应用及管理组件授予完成其功能所必需的最低访问权限。

1.3.5 云网服务层面临的安全风险

在云网融合场景中，云原生网络微服务能够支持多业务、多接口的服务接入。然而，微服务的广泛应用会显著增加应用编程接口（application programming interface, API）^[34]的调用频率。若其安全控制机制仍停留在单一、静态的模式，则可能面临以下风险：难以有效鉴别客户端请求的真伪、API调用权限管控不足，以及因缺乏统一的API安全管理而引发非法访问、数据泄露等安全事件。

为提升用户体验，身份验证与接入管理流程应实现全面自动化。在此过程中，涉及用户登录云平台的所有敏感信息均需加密传输，以防止凭证或隐私数据泄露。此外，还可采用强认证机制与多因素认证等方式，进一步提升接入安全性。云网融合的核心价值在于实现计算与网络资源的统一管理 with 优化配置，从而提供可按需定制的网络服务。然而从用户视角看，网络底层信息通常处于完全屏蔽状态，服务的具体运维与管理均由网络服务提供商负责。当前，网络攻击手段日益多样化：DDoS攻击通过海量虚假请求耗尽网络资源，导致服务瘫痪而无法响应合法用户，严重影响服务可用性；攻击者利用漏洞、恶意软件等手段入侵系统，可导致数据泄露、被篡改或被删除，破坏服务的完整性与可用性。一旦网络遭受攻击，故障排查与恢复工作完全依赖提供商的安全运维体系。这不仅降低了网络服务的整体可靠性，也对运维人员的应急响应与故障处置效率提出了更高的要求。因此，网络应具备更加灵活、高效的故障自愈与恢复能力。同时，为应对多样化的流量与服务场景，网络还应拥有动态异常流量检测、安全服务链的智能编排与快速部署能力。值得注意的是，云网融合模式下网络与云资源的深度集成增加了系统配置的复杂性，配置不当极易形成新的安全漏洞。此外，网络云化加剧

了对第三方服务提供商的依赖, 供应链中任一环节的安全问题都可能波及整个系统。攻击者还可能利用云网集成的特性, 发起跨平台、跨层次的协同攻击, 此类攻击模式在传统单一网络环境中较为罕见。同时, 新型技术及其应用也为网络攻击提供了新的载体, 使得攻击行为更隐蔽、更灵活, 攻击技术的智能化也加大了威胁检测与溯源分析的难度。

2 零信任安全模型

2.1 零信任安全架构

零信任网络访问 (zero-trust network access, ZTNA) 认为: 内部网络与外部网络都是不可信任、不安全的。其打破了“内部即可信、外部即不可信”的传统安全理念, 转向以数据为中心构建全新的安全边界, 并依托强身份验证技术实现对核心数据资产的防护。在 ZTNA 框架下, 企业应用程序不再暴露于公网, 从而有效规避来自外部攻击者的无差别探测与攻击。该架构通过部署信任代理组件, 建立用户与企业应用程序之间的安全连接通道, 并依据身份、属性、环境信息等动态授予访问权限, 阻止未授权访问行为, 进而降低数据泄露风险。

典型的零信任安全架构如图 2 所示, 通常由策略引擎、信任引擎和策略执行器 (policy enforcement point, PEP) 三大核心组件组成。策略执行器充当网络实体与资源之间的网关, 负责拦截请求并执行访问控制决策。信任引擎作为零信任架构的智能决策中枢, 通过实时融合用户行为基线、设备安全状态及环境上下文等数据进行安全风险的研判, 为策略引擎提供决策依据和指标。而策略引擎则依据企业安全策略与规则、持续监控数据、访问控制逻辑、信任评估结果、行为分析工具生成的遥测数据, 结合身份与访问管理相关算法, 进行访问控制决策。

控制平面是零信任安全架构的大脑中枢。任何用户访问受保护的资源时, 其请求都必须提交至控制平面的控制引擎进行验证。用户的身份认证流程与权限分配机制, 均严格遵循控制平面预设的细粒度访问控制策略。当用户需要访问更高安全级别的资源时, 系统将自动触发更加严格的身份核验机制。

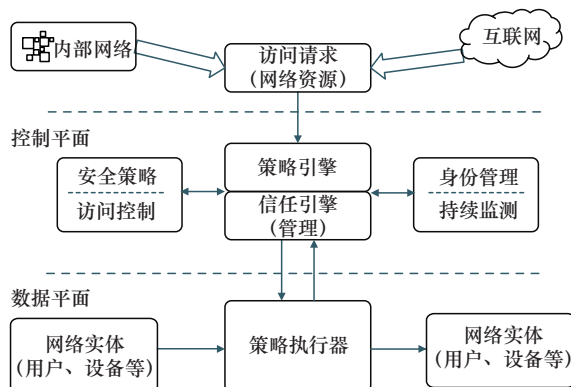


图2 典型的零信任安全架构

2.2 零信任关键技术

零信任安全模型的核心持续防护能力主要包括^[35]: 身份授权与访问管理、微隔离及持续监测。本节将对当前零信任安全领域的热点技术展开介绍。首先阐述软件定义边界 (software defined perimeter, SDP) 技术, 随后分别对身份授权与访问管理、微隔离、持续监测展开分析。

2.2.1 软件定义边界

SDP 是国际云安全联盟于 2014 年提出的一种基于零信任理念的网络安全模型。该模型遵循“先验证, 后连接”的原则, 只有在客户端身份通过严格验证后, 才允许其访问受保护的内部资源^[36]。SDP 规范中的一项关键技术是单包授权 (single-packet authorization, SPA)。在该技术中, 客户端基于共享密钥生成一次性密码, 并将其作为基于哈希消息认证码 (hash-based message authentication code, HMAC)^[37] 的认证载荷, 嵌入连接建立过程中的首个网络数据包中, 提交给 SDP 控制器及网关完成身份核验。

SDP 架构主要由 SDP 客户端 (即发起主机)、控制器和 SDP 网关 (即接受主机) 3 部分组成, 其认证过程如图 3 所示。控制器是 SDP 架构的核心组件, 扮演信任代理角色, 负责处理 SDP 主机与后端安全控制策略之间的控制信令交互, 具体涵盖设备认证、证书颁发及访问权限验证等, 并协助在 SDP 客户端和 SDP 网关之间建立双向传输层安全 (transport layer security, TLS) 隧道^[38]。SDP 客户端负责向控制器发起访问服务或应用程序的请求, 控制器通过验证 SDP 客户端设备的硬件或软件信息完成身份认证, 并在授权后建立连

接隧道以实现安全访问。SDP网关作为授权服务或应用程序的接收端，默认拒绝来自控制器以外的数据包。只有在控制器提供经过认证的SDP客户端地址和相应证书后，SDP网关才允许建立双向TLS隧道，从而确保数据传输的安全性。

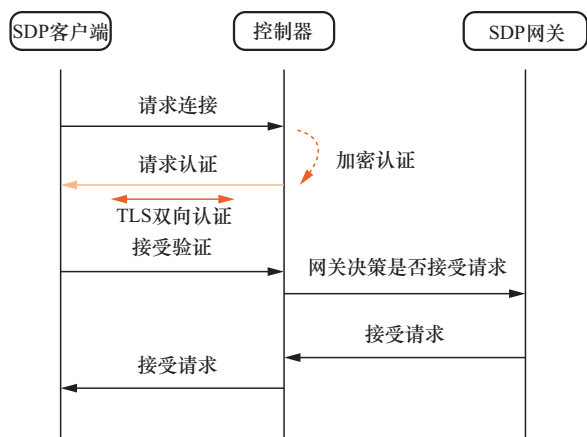


图3 SDP认证过程

文献[39]系统地介绍了SDP的概念和架构，并提出了针对该框架的定量分析评估方法。该研究同时梳理了现代基于云的网络面临的安全和隐私挑战。此外，该研究还探讨了基于SDP的网络功能虚拟化多层次安全机制，其主要方法是将在SDP的边界安全能力应用于虚拟网络功能的访问控制与部署，从而有效抵御拒绝服务攻击。文献[40]提出了一种增强型SDP体系结构，通过增强到SDP控制器的控制信道消息来扩展SDP授权规则，进而实现深度防御。

2.2.2 身份授权和访问管理

零信任网络要求对所有访问网络资源的实体执行严格且持续的身份验证，且该验证过程不依赖于实体所处的网络位置（即无论其位于网络边界之内或之外）。文献[41]强调，将持续身份验证与用户及设备的活动集成，有助于减少安全漏洞。该研究融合了多因素身份验证与行为分析技术，在提升安全性的同时，保障了用户在验证流程中的无缝体验。文献[42]从通信接入视角，提出了一种面向多用户场景的轻量级连续验证方案。该方案通过挖掘用户接入信道的多维度信息，实现通信效率与安全性能的提升。该方案将多用户接入的时间帧分配、子信道选择及功率调控问题转化为联合优化模型，借助非正交多址接入

（non-orthogonal multiple access, NOMA）技术^[43]，在对用户身份进行持续认证的同时，最大化系统的可达和速率（achievable sum rate, ASR）。

零信任网络通过评估网络活动的多种属性来识别当前访问请求的风险。这些属性包括时间属性、空间属性和行为属性^[44]。将访问请求的各类细节纳入考量与分析，可以实现更精细的授权判定。依据授权决策所依赖的核心特征差异，访问控制模型可以划分为基于属性的访问控制模型、基于角色的访问控制模型、基于策略的访问控制模型和基于自适应的访问控制模型^[45]。各类模型的技术特点与应用特性如下。

1) 基于属性的访问控制模型：其核心逻辑是依据访问请求涉及的各类实体的属性完成授权和判定。这些属性既可以是访问主体属性（如姓名、年龄、职业等），也可以是访问资源属性、访问环境属性^[46]及访问主体的上下文信息等。文献[47]提出了一种基于属性的增强云存储的访问控制方案。文献[48]探讨了使用强化学习技术持续验证用户和系统的身份的方法，确保资源访问权限仅向授权用户开放。

2) 基于角色的访问控制模型：其核心逻辑是依据用户的角色完成授权和判定。该类模型在用户与访问目标之间引入角色这一中间层，且用户角色可以根据实际需求动态调整，这一设计显著提升了权限管理的灵活性。但在零信任网络的动态应用场景中，该模型因缺乏对环境上下文信息的考量，且易引发身份爆炸等问题，存在一定的应用局限性。

3) 基于策略的访问控制模型：该类模型的核心逻辑是通过预先定义的规则集合（策略），将安全需求转化为具体的逻辑判定条件，从而实现访问控制逻辑与业务应用代码的解耦。基于策略的访问控制模型采用策略决策点与策略执行点相分离的架构，能够综合评估主体、资源、动作及环境上下文等维度的变量，并通过布尔逻辑、算术比较及正则匹配等方式执行复杂的权限判定。相较于基于角色的访问控制模型，基于策略的访问控制模型在控制粒度上更加精细，能够精准落实零信任架构中的最小权限原则。然而，随着网络规模的不断扩大，海量策略的管理与维护也面

临挑战。

4) 基于自适应的访问控制模型：其设计初衷是应对动态变化的网络环境态势。该类模型在授权决策前的信任评估环节^[49]，将当前访问业务对应的威胁等级、业务重要性等纳入考量范畴。在信任评估时，通过对用户、终端设备、应用程序及运行环境的实时监测与分析，为动态授权决策提供量化依据，这一特性与零信任网络对持续、多维信任评估的核心要求高度契合。

在零信任模型中，访问权限不再依赖静态的 IP 地址或网络位置，而是基于用户身份、设备安全状态、访问时间、地理位置等数据进行信任评分。信任评估的关键在于构建全面且多维度的信任证据体系。常见的信任证据来源包括：用户与系统的交互行为数据、访问控制请求记录、威胁情报库数据及资源访问需求特征等。在此基础上，信任评估算法通过执行信任聚合与动态更新操作，结合时序行为特征与时间驱动行为模式，实现对实体信任状态的动态化评估。

2.2.3 微隔离

微隔离作为零信任架构的重要组成部分，其通过在不同的应用、网络构件、网络边界或服务周边建立微型边界，并实施针对性的访问控制与安全防护措施，实现对资源的保护。在物联网环境中，文献[50]基于零信任架构的分段技术，在设备、雾计算及边缘计算层级部署微隔离，并实施了相应的隔离策略。文献[51]采用集中控制的方式实现网络流量的统一管控，并在设备遭受威胁时自动撤销其访问权限，从而有效实现设备与资源的隔离。文献[52]开发了一种分析框架，用于量化微隔离在增强网络安全方面的有效性，这为微隔离的应用提供了参考。文献[53]提出了一种支持零信任的新型网络安全架构，通过检查网络流量中的端口和协议信息，确保仅允许已授权的通信。

容器安全是一套保障容器化应用安全的技术体系，主要关注云环境下的空间隔离与全生命周期防护。在容器安全技术体系中，微隔离作为其网络层的核心实现手段，通过细粒度的访问控制与动态策略协同，能够阻断容器环境中的横向攻击链路，有效防范数据泄露等安全风险。需要明

确的是，微隔离与容器安全在概念上存在显著区别。微隔离聚焦于网络通信层的细粒度访问控制，其核心目标是通过动态适配的安全策略，对容器或服务间的横向交互流量进行限制。而容器安全则覆盖容器全生命周期的防护，包括镜像漏洞管理、运行时异常行为监控、内核级资源隔离和供应链安全等。微隔离主要应对云环境中东西向流量所衍生的安全威胁，而容器安全则须应对更广泛的威胁（如镜像投毒、运行时逃逸及配置错误等）。

2.2.4 持续监测

零信任网络要求对网络状态进行实时监视。持续身份认证和动态访问控制都依赖于对网络状态的快速感知、响应与分析。实时监视有助于及时发现潜在的安全风险，并识别与阻止恶意用户或设备。网络参与者的活动是零信任网络进行信任评估的主要依据，因此持续监视网络活动成为零信任网络的关键环节。入侵检测系统（intrusion detection system, IDS）已被广泛用于监控网络流量与实施访问控制^[54]。在零信任架构中，IDS 可以与其他安全组件结合形成安全服务功能链，从而提供协同防护^[55]。文献[56]提出一种基于联邦学习的物联网 IDS，该系统结合卷积神经网络与双向长短期记忆网络，实现有效的入侵检测。

态势感知作为零信任网络中的一种动态、持续的安全监测与分析机制，其核心目标在于实时评估网络环境的风险态势，并据此动态调整访问控制策略。该机制的运行过程可以划分为以下 4 个阶段。

1) 多源数据采集：采集网络流量、安全日志、端点行为、身份验证信息、系统事件及外部威胁情报等数据。在零信任架构中，需要重点关注用户身份、设备状态、访问行为等动态信息。

2) 态势分析研判：采用机器学习和大数据技术对采集的数据进行关联分析，建立正常行为为基线。例如，通过用户行为分析，识别异常登录或权限滥用行为；同时，结合规则引擎和 AI 模型，精准检测高级持续性威胁攻击链中的渗透、提权、数据外发等阶段，并引入威胁情报进行验证，从而提升检测结果的准确性。

3) 风险评估与策略调整：基于资产价值、漏洞利用概率及威胁影响范围评估风险等级，动态调整访问权限。通过时序分析与攻击图建模预测潜在攻击路径，并生成实时安全告警。

4) 自动化响应与优化：根据风险评估结果，联动安全设备自动执行阻断、隔离等操作，缩短事件响应时间，同时以日志的形式记录事件处置的整个过程并更新威胁情报库。

实时恶意流量检测是网络管理员监测基础设施健康状态的重要环节。零信任架构对网络流量提出了高可信度要求，无论是控制平面的信令流量，还是数据平面的用户加密流量，都需要保障流量特征的一致性。控制器作为零信任架构的核心枢纽，其收发的控制数据包会直接影响全局访问策略的执行，因此必须对这类流量进行实时监测。文献[31]提出一种面向SD-WAN的实时恶意流量检测方案，该方案采用动态分布式特征提取技术从原始流量中提炼代表性特征，并基于真实数据集完成了方案的有效性验证。

由于大部分安全损害源于内部风险，因此用户行为分类与异常检测在零信任网络中占据至关重要的地位。通过机器学习方法执行网络用户行为生成任务，可以实现高效的用户行为建模和分析^[57]。

2.3 安全访问服务边缘-SASE

Gartner在2019年9月发表了题为*The Future of Network Security Is in the Cloud*的报告，首次提出安全访问服务边缘（secure access to service edge, SASE）这一概念。SASE将SD-WAN的固有安全特性与以云为中心的安全性相结合，旨在安全、高效地连接和保护人员与应用程序。作为SD-WAN的扩展框架，SASE整合了云访问安全代理、安全Web网关、零信任网络访问、防火墙即服务和数据防泄露等云原生安全服务。SASE是网络与安全一体化架构^[58]，依托云网大脑的智能决策与分析能力，将网络连接能力与安全防护能力在网络节点上进行高效部署与协同调度，最终形成统一的内生安全防护体系。其架构如图4所示，可以划分为以下4层。

1) 终端接入层：作为最下层，负责终端的安全接入，并将终端行为事件上报至上层进行检测与分析。

2) 安全基础设施层：该层包含各类物理与虚拟化的设备、节点及安全资源。通过虚拟化技术将计算、存储、安全等资源统一抽象为可灵活调度的云资源。该层部署具备网络转发与安全防护能力的智能网关，实现就近防护与流量处理。

3) 决策层：作为中间层，决策层通过身份安

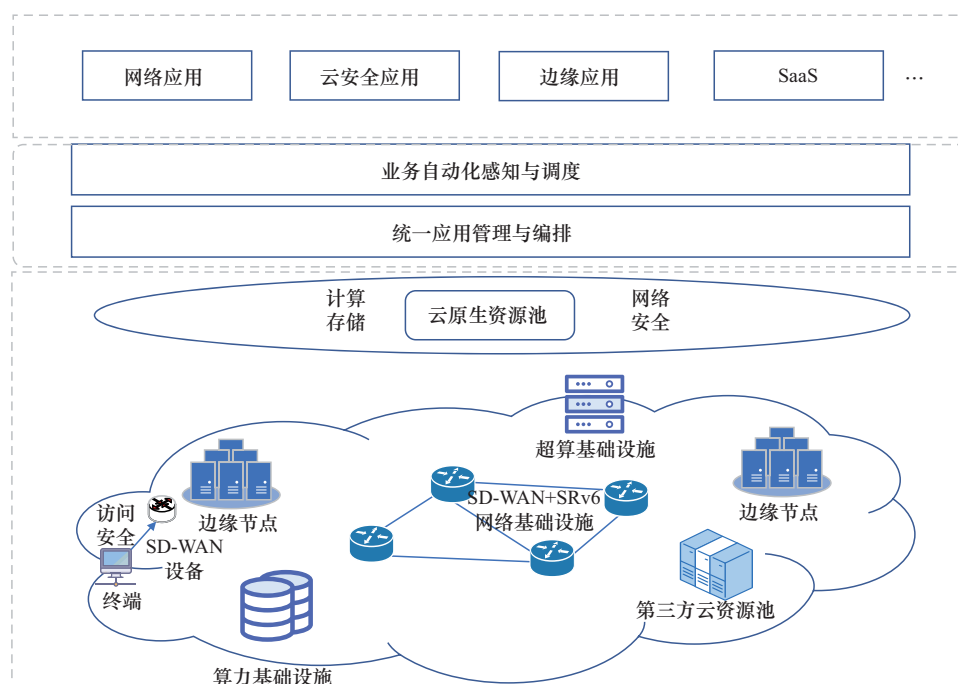


图4 SASE体系架构

全、网络安全、数据安全等策略,实现对云网安全的统一编排与协同防护。

4) 应用层:作为最上层,该层叠加部署网络层面的管理、控制与分析功能,以及安全领域的管理与分析服务,实现管理、控制、分析一体化的运营服务。该层也是零信任架构的“智能大脑”,负责集中分析威胁态势并执行零信任策略下的处置动作。

作为云网融合背景下的安全框架,SASE已实现产业化落地,相关技术研究主要集中在访问控制与安全策略等方面。文献[59]提出一种基于属性的SASE安全访问技术方案,并设计了动态路由架构;文献[60]对SASE的关键技术和产业发展进行了详细的阐述;文献[61]全面地分析了SASE的研究进展及其未来发展面临的挑战。

SASE融合了SD-WAN的网络灵活性与零信任的安全理念,形成了统一协调、智能决策的一体化防护能力,在云网融合落地实践中展现出显著潜力。

一个完善的零信任架构除了包括策略引擎和网关等核心部件,还应有相应的支撑组件。安全信息和事件管理(security information and event management, SIEM)在零信任落地中至关重要,它能够采集和存储各类网络与安全设备的日志与事件,通过持续分析这些数据,实现威胁与合规性检测。安全编排、自动化与响应(security orchestration, automation and response, SOAR)作为SIEM的重要组件,可以通过灵活的流程编排和事件驱动的自动化响应,提高安全运营的效率。关于安全服务自动化编排的实现机制将在第3.2.4节进行讨论。

3 面向云网融合的零信任安全技术

3.1 典型应用场景和研究进展

随着企业数字化转型进程的加速,云网融合技术正加速向多领域渗透,其应用范围不仅覆盖通信、能源、电力、制造、教育等传统行业,还延伸至电商、直播等新兴市场。通过整合人工智能与大数据等前沿技术,企业得以对自身信息技术系统的硬件和软件进行升级,推动新应用的快速开发与部署流程的优化,进而加速数据的流转、整合、分析与价值转化,实现生产效率的提

升。此外,云网融合重构了传统信息基础设施的架构形态,增强了基础设施的灵活性,提升了企业的运营效能。

表2对现有云网融合零信任安全研究技术进行了对比。

云网融合典型应用场景包括混合云广域网络、物联网、移动通信网等。针对不同场景下零信任安全技术的研究现状,本文进行了系统性梳理与总结。

混合云可以实现企业本地计算环境与公有云资源池的高速互联,以满足数据迁移、容灾备份、跨域数据通信等业务需求。在该场景下,企业可以利用云专线、云专网保障网络连接的稳定性和安全性,避免数据在传输过程中被窃取。文献[62]开发了一种基于联邦人工智能的零信任算法,通过分布式协作学习实现动态访问控制与持续监控,在“从不信任、持续验证”的原则下构建自适应安全防护机制。文献[65]提出了一种适用于云计算环境的可生存零信任架构,该架构具有较高的安全性和鲁棒性,能够在特定条件下容忍入侵行为,并在遭受攻击或故障后快速恢复。文献[53]提出一种基于网络微分段的零信任网络安全架构,该架构通过检测网络流量的端口与协议信息来授权通信。

随着工业系统数字化程度的不断提高和云技术的日益普及,物联网基础设施的安全管理面临严峻挑战,网络连接规模的持续扩大不可避免地增加了系统的攻击面。文献[68]提出一种面向工业物联网的集成零信任安全架构,通过将网络微分段技术无缝融入现有工业网络环境,实现跨异构环境策略的统一抽象与实施。文献[69]开发了物联网各安全层次的核心映射结构,系统分析了在物联网中实施零信任架构面临的挑战与障碍。文献[70]提出一种基于博弈论的零信任认证框架,利用动态博弈模型设计相互依赖的信任评估和认证策略,并通过马尔可夫博弈模型来描述动态行为;面向5G物联网场景,该研究还提出移动时域计算方法,支撑零信任策略的在线决策与对环境动态变化的快速响应。

在个性化服务需求持续增长的背景下,移动通信网的安全威胁呈现出复杂化、多样化的演变

表2 现有云网融合零信任安全技术对比

文献	架构	关键技术				
		动态访问控制	身份验证与授权	微隔离	持续监控	其他技术
[62]	分布式	√			√	联邦学习
[63]	分布式		√			区块链
[64]	分布式	√				
[65]	集中控制	√	√			
[66]	集中控制		√	√		密码学
[67]	集中控制		√			最低有效位加密
[68]	集中控制			√		
[69]	集中控制	√	√			
[70]	分布式		√			
[71]	分布式	√				
[72]	分布式		√			区块链
[73]	分布式	√				区块链
[74]	集中控制	√				
[75]	集中控制	√				区块链
[76]	集中控制				√	自适应AI
[77]	集中控制				√	多智能体强化学习
[78]	分布式	√				
[79]	集中控制	√			√	
[80]	集中控制	√	√	√	√	移动目标防御
[81]	集中控制	√	√	√	√	物理层认证
[82]	集中控制	√	√	√	√	

趋势，零信任架构凭借动态、细粒度的防护特性，近年来在无线通信、卫星通信等移动通信领域得到广泛应用。无线通信场景的显著特征是接入设备的异构性与多样性，这对用户身份认证的精准性与安全性提出了更高的要求。与 5G 网络不同，6G 网络采用软件化、模块化设计理念，将各类网络功能与应用服务封装为独立的软件模块，可以支持万物互联、延展实境、智能电网、智能交通等应用。文献[79]研究了在 6G 网络中实现零信任安全定制服务的软件化资源分配问题，通过将零信任安全的持续验证能力应用于定制服务的安全检查中，有效增强了异构设备接入的安全性。文献[80]提出一种融合动态移动目标防御机制的 SDP 方法，该方法基于 6G 网络特性在 6G 核心网中构建安全的零信任环境，通过引入移动目标防御机制，增强了网络的韧性。文献[81]提出一种面向 6G 网络的零信任安全架构，可以实现跨用户设备（UE）、跨服务节点（SN）、跨归属网络（HN）域的身份认证、行为监管和

数据安全防护，并分析了可用于完善该安全架构的前沿技术。此外，在车联网场景中对该架构的有效性进行了评估，结果表明，零信任架构下的车辆服务时延能够保持相对稳定，其物理层认证与安全传输机制在无线环境中的表现优于传统加密算法。在攻击防御方面，文献[82]提出的 6G 零信任安全架构（ZTA-6G）在防御非欺骗性分布式拒绝服务攻击时表现突出，与基于信任的包过滤（trust based packet filtering, TBPf^[83]）、互联网透明安全（transparency for better internet security, TRIS^[84]）等安全架构相比，ZTA-6G 的攻击包过滤率达到 90% 以上，且随着仿真周期的延长，防御效果始终保持最优。其中，TRIS 架构由于无法拦截恶意用户设备的首次攻击，因此在初始时其防御效果最差；TBPf 架构的防御性能较好；而 ZTA-6G 通过对源社区恶意终端的自评估过滤，以及对目的社区存在恶意行为的终端重新进行可信评估，从而实现了攻击报文过滤率的最大化。

3.2 云网融合零信任关键技术研究

云网融合技术凭借其云网一体集成的架构特性,具备资源统一调度与弹性部署的能力,为零信任安全架构的落地实施提供了有效保障。现有云网融合场景下零信任安全的关键技术体系如图5所示。

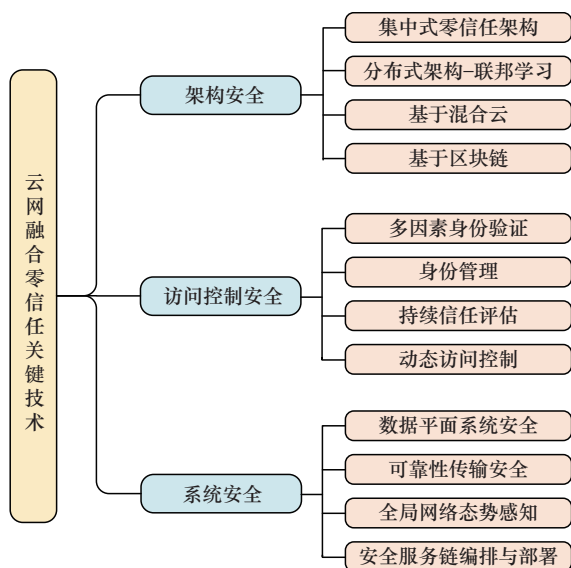


图5 云网融合场景下零信任关键技术体系

基于云计算和基于承载网的相关技术为零信任安全能力的加固提供了支撑。在零信任安全架构的演进过程中,各类新兴技术为云网融合安全提供了更多的可能性。在云网融合零信任关键技术框架中,架构安全与访问控制(如身份管理)虽被划分为两个独立的模块,但在实际的研究与应用中,架构安全技术与其他技术相辅相成,二者并无严格区分。本文重点关注访问控制相关技术,架构安全层面的相关技术不再单独划分章节介绍,而是结合具体的技术与应用场景进行一体化介绍。

3.2.1 身份管理与访问控制技术

本节将身份管理视为访问控制的上游环节。多因素身份认证能够强化身份可信度,常见的认证方法包括传统的静态密码、动态令牌、生物特征和基于SIM卡或硬件的强认证机制。在云网融合零信任架构中,多因素身份认证展现出更强的场景适应与技术融合能力,云端强大的算力与数据处理能力能够提升认证的可靠性与效率。其中,无密码认证技术可以结合SIM卡安全芯片或

硬件密钥,实现身份与设备的强绑定,依托运营商网络的身份核验能力,构建“通信身份+密码身份”的双因子认证体系。

动态访问控制是零信任安全体系的核心。实现细粒度的访问控制已成为当前研究的重点。在云网融合环境中,网络访问主体呈现异构化、复杂化的特征,用于信任评估的属性特征数据体量庞大,传统基于规则的访问控制策略不仅处理成本高昂,而且难以适配动态变化的网络环境。机器学习^[85]算法在多维数据处理方面已有成熟的应用,其在多维属性特征提取方面具有显著的优势。基于机器学习的动态访问控制是一种利用机器学习技术实时调整和优化网络安全策略的方法。具体而言,该技术以采集的网络流量、用户行为日志、设备信息等数据作为模型训练的输入,模型从海量原始数据中提取有用的特征,这些特征对于理解网络活动至关重要;整合多维度数据源,并利用不同类型的机器学习技术开展协同分析,可以提高模型的鲁棒性和检测的准确性。基于机器学习的动态访问控制系统可以提高网络的安全性,使防御措施更加智能化和自动化。实现此类系统仍需克服若干技术挑战,包括大规模数据的处理、低时延的实时响应、模型泛化能力及抗欺骗能力的提升等。

云网融合环境中的接入设备类型多样、属性不一,如何对具有多属性身份或行为特征的访问主体进行动态信任评估,是当前零信任访问控制领域的核心技术难题之一。现有研究普遍采用机器学习算法对当前访问属性进行特征提取,并基于身份、行为或上下文等特征制定动态访问控制策略。文献[86]基于深度强化学习方法实现了物联网设备的最佳访问控制,该系统通过学习历史能量到达信息来预测物联网设备的能量状态,将其输出作为学习模型的状态信息。

区块链^[87]是一种分布式账本技术,其核心价值在于构建了一套不可篡改、全程可追溯的数据记录体系。区块链技术的兴起,为构建新型零信任网络访问控制机制提供了新思路。区块链技术的去中心化、不可篡改和可溯源的特性能够为零信任网络提供更加可靠的安全防护能力。此外,云网融合场景天然的分布式架构与区块链网

络具有高度适配性，有助于区块链节点的部署与运行。在云网控制层引入区块链技术，可以实现资源的分布式管理，从而提升网络数据的安全性。

目前已有研究将区块链智能合约技术应用于身份管理与访问控制领域。文献[88]基于区块链与智能合约设计了一套支持分布式多权限属性的访问控制框架。文献[89]研究了基于智能合约的细粒度数据访问控制方法，并通过智能合约实现了基于属性的访问控制模型。

3.2.2 云网零信任系统安全

随着5G、人工智能等网络应用的快速发展，网络安全技术（即能够检测并防范各类网络攻击的技术）在网络管理体系中的战略地位日益突出。可编程交换机的出现为网络安全技术的演进提供了关键支撑，使其具备易于管理、成本较低、灵活性高和性能优越等特点。借助可编程交换机，可在零信任架构的关键节点部署安全功能，将安全逻辑以数据平面程序的形式定义，并加载至其匹配一动作流水线中执行^[90]。这种自上而下的实现方式将安全能力直接嵌入数据平面交换设备，从而提供体系化的防护保障。

近年来兴起的分布式云计算模式，利用邻近智能设备的计算与存储资源进行计算与缓存。然而，该模式的落地应用仍面临诸多挑战，包括设备算力与功耗限制、邻近设备移动导致连接不稳定，以及向邻近设备卸载计算任务时的数据安全保障等问题。因此，构建兼具高安全性、高能效、高稳定性和强大处理能力的新型计算架构，被视为对现有计算范式的重要补充。

基于可编程数据平面的网络内计算范式^[91]能够在网络边缘提供处理能力强大的网络单元，其具备每秒处理数十亿数据包的能力。该范式具有低时延、高能效的优势^[92]，在云网融合的零信任场景中，可以通过数据平面转发加速云应用流量的访问与处理。

系统安全同样是当前零信任环境下安全防护的重点方向。现有研究大多从网络安全层面入手，主要依赖第三方安全产品（如IDS、下一代防火墙或云端安全服务等）提供边界防护。而系统安全则致力于在云网融合零信任体系内部构建

第二道安全防线，使得攻击者在突破外围防御后，仍需面对系统级别的监测与处置。文献[93]提出了一种可编程的系统安全框架，能够实现统一、动态、细粒度的零信任系统资源管控，并评估了该框架抵御多种安全威胁的能力。相比其他方案，该框架在典型场景下性能开销极低，插入10万条流表规则时延仅为1.7 ms，阻断漏洞攻击的时延低至2.0 μ s，较传统日志方案实时性提升超过80%。

SRv6^[94]是一种基于IPv6数据平面的分段路由网络架构，支持在头节点插入转发指令以引导数据包转发。在云网融合网络中，SRv6为网络路由提供了强大的可编程能力。当链路或节点发生故障或恢复时，可能引发数据包丢失，SRv6通过拓扑无关的无环备份快速重路由、防微环机制、中间节点保护、尾节点保护等高可靠性机制，避免业务流量长时间中断。文献[95]聚焦基于IPv6分段路由技术的SD-WAN服务，提出利用简单双向主动测量协议（simple two-way active measurement protocol, STAMP）监测STAMP会话发送器与反射器之间SRv6路径的时延。由此可见，基于SRv6构建的云网融合零信任数据转发层，具有更高的可靠性与流量监测能力。

3.2.3 全局网络态势感知

全局网络态势感知（global network situational awareness, GNSA）^[96]是一种综合性的网络安全管理方法，其核心在于对整个网络环境进行持续监测、分析与理解，从而实现对潜在安全威胁的及时识别与高效响应。通过实时采集网络流量、用户行为等数据，GNSA系统能够迅速发现异常行为模式与潜在风险点。基于采集的数据开展安全风险评估，量化分析各类威胁可能对组织造成的损害程度。在检测到攻击行为时，该系统可协助安全管理人员快速启动响应流程，执行针对性处置措施以减轻影响，并为后续系统恢复提供决策支持。此外，借助机器学习与统计模型，GNSA系统还能预测潜在安全事件，推动防护模式从被动应对向主动预防转变。GNSA旨在构建覆盖全网的安全态势视图，帮助安全管理人员全面把握并动态管控网络安全风险，提升对复杂多变威胁的应对能力。通过持续监测与分析来

不断优化网络防御措施,适应日益演进的网络威胁环境。

在安全响应层面,云网融合环境借助软件定义安全 (software defined security, SDS)^[97]和云原生安全控制等技术,实现了安全策略的灵活、高效部署,构建起“感知-分析-响应”的闭环安全防护机制。同时,云平台提供的高级可视化工具能够直观呈现复杂态势信息,辅助安全管理人员进行分析研判与趋势预测。

然而,云网融合也为态势感知带来若干技术挑战,包括异构数据的语义融合、跨域分析中的隐私保护机制,以及对云环境动态变化的自适应能力等。这些问题既是当前研究的前沿课题,也为未来技术创新指明了方向。

3.2.4 安全服务链编排与部署

安全服务链编排是一种网络安全管理策略,通过将防火墙、IDS、防病毒软件等安全服务按逻辑顺序串联起来,引导网络流量有序、高效地经过各安全功能节点,从而确保数据在传输过程中的安全性与合规性。

在零信任网络架构中,安全服务可以根据实际需求动态调整数据流路径,实现更细粒度的访问控制^[98]。零信任体系对网络及其组件提出了明确的安全要求,包括对所有网络流量进行身份验证、授权、加密与检查^[63]。因此,安全服务

链架构也必须满足这些要求,才能符合零信任安全标准并实现可靠部署。文献[99]将SDP组件作为安全服务链中的可编排模块,为NFV中的虚拟网络功能提供逻辑隔离边界,仅允许通过可信认证的客户端进行访问与连接。自动化服务编排能够依据业务属性,将不同的安全服务灵活地组织为对应的业务链,从而为各类业务提供差异化的安全防护能力。图6展示了典型的基于SDP的安全服务链编排与部署流程。用户请求在访问目标服务前,需依次经过防火墙、入侵检测等安全功能的检查。安全资源池根据用户服务需求,自动完成服务链的编排与执行,实现安全策略的动态适配与高效实施。

云网融合与安全服务链编排之间存在多维的相互作用关系,这种关系深刻影响着现代网络安全架构的演进方向。云网融合环境通过NFV和SDN技术为安全服务链的构建提供了关键的技术基础和灵活的部署平台,使得各类安全功能能够以虚拟化形式动态部署并弹性调度。这种基于软件定义的方式显著提升了安全服务链的灵活性和适应性,使安全防护体系能够更有效地应对复杂多变的网络环境和持续演进的安全威胁。此外,云平台内置的弹性资源调度能力进一步增强了安全服务链的性能与可靠性,确保在面对突发安全事件时,系统可以快速调配充足的资源。

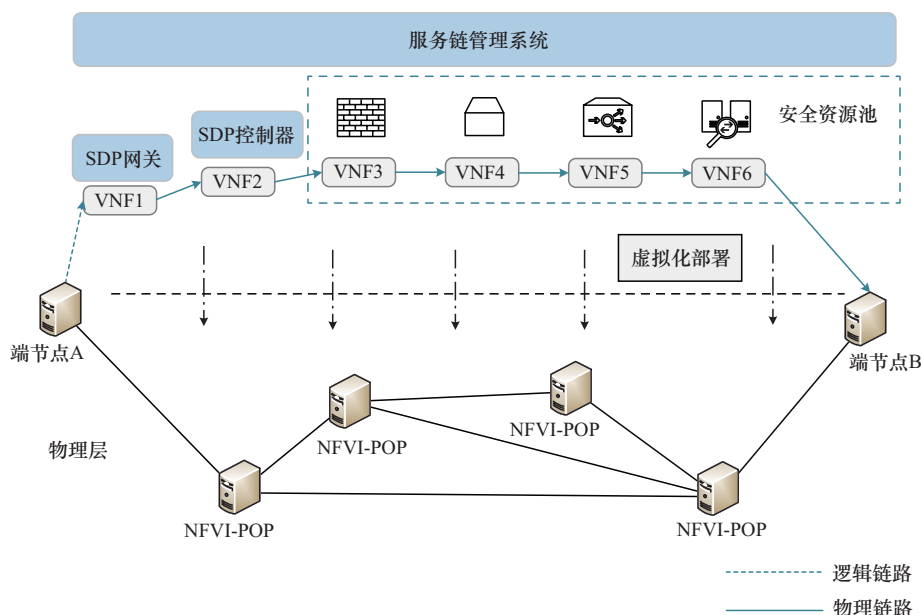


图6 基于SDP的安全服务链编排与部署流程

4 未来趋势和挑战

零信任安全模型通过在动态环境中对用户、设备及应用程序身份进行持续验证，能够有效缩小攻击面并降低数据泄露风险。随着分布式云计算的规模化部署、移动终端与物联网设备的广泛接入、远程办公模式的普及和“自带设备办公”的兴起，传统的网络边界日益模糊，为攻击者渗透网络与窃取敏感数据创造了更多的机会。正因如此，传统安全模型已难以应对当前复杂且持续演变的威胁环境，零信任安全模型的部署显得尤为必要。

然而，在异构网络环境中实施零信任仍面临诸多挑战，主要体现在架构的复杂性、系统的互操作性、实施与维护的成本、对用户体验的影响及海量策略的协调与管理等方面。因此，要成功落地零信任安全方案，必须立足动态变化的网络环境，从网络架构的适配性、关键技术的成熟度、访问策略的可扩展性3个维度开展全面评估。

4.1 持续信任评估与身份授权

动态访问控制与身份授权是零信任安全体系的核心能力，其技术实现主要依赖于策略引擎与信任评估两大组件的协同运作。在复杂多变的网络环境中，网络实体的各类行为可能存在不可信因素，从而增加了应用访问的安全风险。传统基于公钥基础设施和数字证书的静态信任机制，由于难以适应网络环境的动态变化，已无法满足复杂网络域下的身份认证与访问控制需求。在此背

景下，动态信任关系管理逐渐成为新型网络环境中信任管理领域的研究热点。零信任架构中的信任评估过程如图7所示，首先对采集的多源异构数据进行分析，综合考量各类信任特征；随后在信任引擎中对数据进行处理，最终输出动态且精准的信任评估结果。文献[100]提出了一种基于持续信任评估与混合加密的多属性认证方法，通过动态更新令牌和信任值来分配访问权限，解决了电力物联网中传统静态与动态认证方式存在的安全隐患。但该方案未深入探讨实际部署中的计算开销问题及信任评估的实时性缺陷。文献[101]设计了一种多维信任融合策略，借助动态评分分析、权重优化和奖惩机制，解决雾计算中数据稀疏和恶意伪装导致的信任评估精度不足问题。

零信任环境中的信任评估须具备上下文感知能力，这对评估算法的设计与实现提出了更高的要求。目前，许多研究借助机器学习技术来感知并融合多维度上下文信息。根据上下文信息的组织方式，现有信任评估策略可以分为事件序列与时隙序列两大类型。现有信任评估研究大多聚焦于图结构环境中的实体信任评估。文献[102]设计了一种分层结构，将信任的时间序列状态划分为多时隙和单时隙两种模式进行讨论，并采用基于位置感知的注意力机制聚合上下文信息。该研究重点考察了图数据对信任评估的影响，但未充分考虑网络环境本身的异构性。因此，有必要研究更适应云网融合异构场景的信任评估算法，从

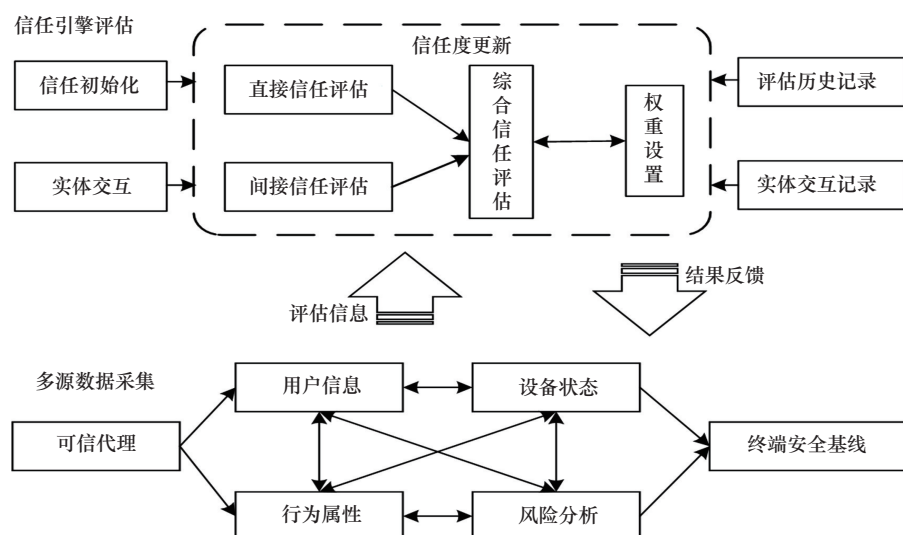


图7 信任评估过程

而实现更细粒度、持续动态的信任评估能力。

生物识别、行为分析与上下文感知认证等技术的融合运用,有望构建更安全、无缝的身份验证机制。然而,该领域仍面临多重挑战:一方面,多云环境下身份的统一管理有待解决,即如何实现跨云服务的身份同步与状态一致性;另一方面,安全性与用户体验之间的平衡也需要解决,即在强化身份验证的同时,避免为用户带来额外的认证负担。未来的研究可能需要探索新的身份联邦技术,发展更智能、自适应的认证系统。

4.2 联邦学习等新型技术的应用与挑战

在云网融合环境中,联邦学习的分布式训练范式与跨域数据安全协作需求具有天然的适配性。云网融合架构借助虚拟化技术实现计算资源与网络资源的深度协同,其典型特征表现为分布式云节点、异构边缘终端和多租户服务模式的有机整合。在这一环境下,联邦学习可作为实现跨域隐私计算的核心技术载体:在纵向维度上,支持中心云与边缘节点之间进行分层模型聚合,避免原始数据跨安全域流动;在横向维度上,构建多云服务商间的联邦协作联盟,通过加密参数交换打破数据孤岛壁垒。该分布式协作机制与零信任架构“永不信任、持续验证”的原则相辅相成——联邦学习协议本身内置身份验证与数据最小化设计,而零信任的动态风险评估引擎则可以实时监控参与节点的行为,实现细粒度的模型更新授权。

值得强调的是,在边缘计算场景中,联邦学习与云网融合的协同效应更为显著。边缘节点既执行本地数据处理任务,又参与全局模型优化,这种双重角色使得传统中心化训练面临数据泄露与网络时延的双重挑战。对此,动态联邦学习框架可以构建3层防护机制:首先,基于区块链实现节点准入认证,确保参与方身份可信;其次,在模型更新阶段采用自适应梯度裁剪技术,同步进行异常行为检测;最后,集成轻量级同态加密算法,保障参数传输的机密性。文献[103]提出的拜占庭容错机制能够有效抵御超过20%节点的恶意攻击,若将其与该框架中的实时信任评分系统结合,则可实现安全防护强度与计算资源开销

之间的动态平衡。

4.3 跨域跨层传输的安全管理问题

在管理层面,自动化与编排技术将成为破解零信任架构复杂性的关键。未来将出现更先进的安全策略自动生成和优化工具,以及支持跨云、跨网络的统一安全管理平台,从而显著提升安全管理的效率与一致性。然而,这一演进也带来了新的挑战:一方面,如何确保这些自动化系统自身的可靠性和安全性是一个关键问题;另一方面,跨云场景下不同服务提供商之间的策略冲突如何协调,以实现真正的统一安全管理,也成为亟待解决的难题。面对这两大挑战,未来的研究可以探索基于意图的安全策略语言设计和开发更智能的冲突检测与解决算法。

在架构层面,异构网络协议的深度融合与动态路由环境对零信任安全模型的适应性提出了新的要求。随着5G核心网与IPv6+协议的规模部署,跨域传输面临多协议栈并存带来的安全策略协同挑战。这种网络架构的演进要求零信任机制能够同时支持多种传输层协议的安全封装,并在动态拓扑变化中维持端到端安全策略的持续生效。同时,在SDN/NFV架构下,如何实现传输层安全策略的实时同步与验证,特别是应对网络切片带来的多租户安全隔离需求,也是亟待解决的问题。最新研究表明,基于分段路由的可编程数据平面可能为跨域策略实施提供新路径,但其在策略冲突检测方面仍存在协议适配层面的障碍。基于此,未来的研究需要重点关注多协议环境下的策略统一表达机制和NFV场景中的安全传输隧道动态构建技术。

4.4 新兴安全威胁的防御与挑战

新兴安全威胁的快速演化对零信任网络的防御能力提出了更高的要求。尽管零信任架构在应对传统安全问题方面具有显著优势,但在动态攻击、身份欺骗、内部威胁和后量子计算等新型威胁面前,其技术体系仍需不断优化以适配威胁变化。其中,高级持续性威胁攻击者会长期潜伏在网络中,利用多层次、多阶段的攻击手段试图绕过零信任架构的身份验证和访问控制机制^[104]。

量子通信技术在安全数据传输领域的突破性进展,为构建量子安全网络提供了新范式,这一

点体现在量子密钥分发 (quantum key distribution, QKD) 技术的实际部署中^[105]。我国建成的世界首条量子保密通信干线“京沪干线”与“墨子号”量子科学实验卫星构成的天地一体化网络,已在政务、金融等高安全需求领域,实现量子密钥的可靠分发与数据的安全传输。这种基于量子不可克隆原理的密钥协商机制,能够与零信任架构的动态访问控制形成协同防御(量子信道保障密钥协商过程的前向安全性,而零信任策略则持续验证通信实体的身份合法性),共同构建防御量子计算威胁的多层防护体系。

与此同时,量子计算带来的潜在威胁也推动了后量子密码学与零信任安全的融合研究。虽然全功能量子计算机尚处于研发阶段,但秀尔算法的理论突破已对现有非对称加密体系构成实质性威胁。由美国国家标准与技术研究院推进的后量子密码标准化工作,为算法迁移提供了参考框架,但在实际应用中仍面临双重挑战:其一,后量子算法的计算复杂度较现行算法平均提升3~5倍,可能在零信任架构的实时会话验证中引发性能瓶颈;其二,混合密码系统的过渡管理需要解决传统公钥基础设施与后量子算法之间的兼容性问题,尤其是在量子随机数生成器与经典密钥派生函数的互操作层面仍存在技术障碍。研究显示,采用格基加密与QKD结合^[106]的混合方案,能够在零信任网络中将端到端时延控制在15 ms内,同时实现NIST安全等级IV的量子抗性,这为构建量子安全的动态访问控制机制提供了可行路径。

展望未来,云网融合零信任安全研究将朝着更智能、更动态的防护体系发展。然而,量子通信的大规模应用仍受限于光纤信道损耗和可信中继节点的安全隐患。通过开发量子中继器与测量设备无关的QKD协议,结合零信任架构的微隔离策略,有望构建覆盖广域云网环境的量子安全传输平面,最终形成“身份可信验证-通信量子加密-访问动态授权”的完整防御链条。

5 结束语

云网融合是下一代通信网络发展的必然趋势,面对日益复杂的网络攻击,传统的安全防御边界已无法保障云网内部安全。零信任网络访问

作为一种新的网络安全架构,基于“永不信任、持续验证”的理念,通过更细粒度的边界保护资源免受恶意主体的侵害,以动态方式保护网络。

本文针对云网融合场景下的安全性问题,系统分析了零信任网络访问在云网融合领域的应用逻辑与有效性。首先,对零信任安全的基本概念、关键技术(包括身份验证与授权、访问控制、微隔离、网络监控)、架构进行了描述;其次,对集成了SD-WAN、零信任、云安全服务等能力的一体化架构SASE进行了讨论;接着,归纳了云网融合的典型应用场景及相关研究进展,并对用于增强零信任安全能力的关键技术(如区块链、联邦学习、可编程数据平面、安全服务链编排等)进行了讨论,为未来的技术发展提供了可行的研究方向。

参考文献:

- [1] Vaezi M, Azari A, Khosravirad S R, et al. Cellular, wide-area, and non-terrestrial IoT: a survey on 5G advances and the road toward 6G[J]. IEEE Communications Surveys & Tutorials, 2022, 24(2): 1117-1174.
- [2] Duan S J, Wang D, Ren J, et al. Distributed artificial intelligence empowered by end-edge-cloud computing: a survey[J]. IEEE Communications Surveys & Tutorials, 2022, 25(1): 591-624.
- [3] Liu L B, Li J E, Lyu J M, et al. Privacy-preserving and secure industrial big data analytics: a survey and the research framework[J]. IEEE Internet of Things Journal, 2024, 11(11): 18976-18999.
- [4] Tang S J, Yu Y, Wang H, et al. A survey on scheduling techniques in computing and network convergence[J]. IEEE Communications Surveys & Tutorials, 2024, 26(1): 160-195.
- [5] 中国信息通信研究院. 云计算白皮书[R]. 2024. China Academy of Information and Communication Research. Cloud computing white paper [R]. 2024.
- [6] 中国电信集团公司. 云网融合2030技术白皮书[R]. 2019. China Telecom Group Corporation. Cloud-network convergence 2030 technology white paper [R]. 2019.
- [7] Rawat D B, Reddy S R. Software defined networking architecture, security and energy efficiency: a survey[J]. IEEE Communications Surveys & Tutorials, 2017, 19(1): 325-346.
- [8] Saha N, Zangoeei M, Golkarifard M, et al. Deep reinforcement learning approaches to network slice scaling and placement: a survey[J]. IEEE Communications Magazine, 2023, 61(2): 82-87.
- [9] Duliński Z, Stankiewicz R, Rzym G, et al. Dynamic traffic management for SD-WAN inter-cloud communication[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(7): 1335-1351.
- [10] Ventre P L, Salsano S, Polverini M, et al. Segment routing: a comprehensive survey of research activities, standardization efforts, and implementation results[J]. IEEE Communications Surveys & Tuto-

- rials, 2020, 23(1): 182-221.
- [11] Avolio F M, Ranum M J, Glenwood M D. A network perimeter with secure external access[C]//Proceedings of the Internet Society Symposium on Network and Distributed System Security, 1994, 109-119.
 - [12] Liang J Y, Kim Y. Evolution of firewalls: toward securer network using next generation firewall[C]//Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). Piscataway: IEEE Press, 2022: 752-759.
 - [13] Perdices D, López De Vergara J E, González I, et al. Web browsing privacy in the deep learning era: Beyond VPNs and encryption[J]. Computer Networks, 2023, 220: 109471.
 - [14] Lee A Y P, Wang M I C, Hung C H, et al. PS-IPS: Deploying intrusion prevention system with machine learning on programmable switch[J]. Future Generation Computer Systems, 2024, 152: 333-342.
 - [15] Li Q, Huang H, Li R Y, et al. A comprehensive survey on DDoS defense systems: new trends and challenges[J]. Computer Networks, 2023, 233: 109895.
 - [16] 范其纲, 蒋忠元, 李兴华, 等. 基于序参量的云边端分布式体系协同安全评估[J]. 网络与信息安全学报, 2024, 10(3): 38-51.
Fan Q G, Jiang Z Y, Li X H, et al. Collaborative security assessment of cloud-edge-device distributed systems based on order parameters[J]. Chinese Journal of Network and Information Security, 2024, 10(3): 38-51.
 - [17] Khalid T, Abbasi M A K, Zuraiz M, et al. A survey on privacy and access control schemes in fog computing[J]. International Journal of Communication Systems, 2021, 34(2): e4181.
 - [18] Stafford V. Zero trust architecture[R]. NIST special publication. 2020.
 - [19] Priyadarsini M, Bera P. Software defined networking architecture, traffic management, security, and placement: a survey[J]. Computer Networks, 2021, 192: 108047.
 - [20] Wyle M F. A wide area network information filter[C]//Proceedings of the Proceedings First International Conference on Artificial Intelligence Applications on Wall Street. Piscataway: IEEE Press, 1991: 10-15.
 - [21] Yang Z J, Cui Y, Li B C, et al. Software-defined wide area network (SD-WAN): architecture, advances and opportunities[C]//Proceedings of the 2019 28th International Conference on Computer Communication and Networks (ICCCN). Piscataway: IEEE Press, 2019: 1-9.
 - [22] Alwasel K, Li Y H, Jayaraman P P, et al. Programming SDN-native big data applications: research gap analysis[J]. IEEE Cloud Computing, 2017, 4(5): 62-71.
 - [23] Zhang Y C, Zhang H H, Cong P Z, et al. Grandet: cost-aware traffic scheduling without prior knowledge in SD-WAN[C]//Proceedings of the 2023 IEEE/ACM 31st International Symposium on Quality of Service (IWQoS). Piscataway: IEEE Press, 2023: 1-10.
 - [24] Troia S, Sapienza F, Varé L, et al. On deep reinforcement learning for traffic engineering in SD-WAN[J]. IEEE Journal on Selected Areas in Communications, 2021, 39(7): 2198-2212.
 - [25] Botta A, Canonico R, Navarro A, et al. Adaptive overlay selection at the SD-WAN edges: a reinforcement learning approach with networked agents[J]. Computer Networks, 2024, 243: 110310.
 - [26] Scarpitta C, Sidoretti G, Mayer A, et al. High performance delay monitoring for SRv6-based SD-WANs[J]. IEEE Transactions on Network and Service Management, 2024, 21(1): 1067-1081.
 - [27] Borgianni L, Troia S, Adami D, et al. Assessing the efficacy of reinforcement learning in enhancing quality of service in SD-WANs[C]//Proceedings of the GLOBECOM 2023 - 2023 IEEE Global Communications Conference. Piscataway: IEEE Press, 2023: 1765-1770.
 - [28] Anh Quang P T, Martin S, Leguay J, et al. Intent-based routing policy optimization in SD-WAN[C]//Proceedings of the ICC 2022 - IEEE International Conference on Communications. Piscataway: IEEE Press, 2022: 4914-4919.
 - [29] Dou S S, Qi L, Guo Z H. ARES: predictable traffic engineering under controller failures in SD-WANs[C]//Proceedings of the ACM Web Conference 2024. New York: ACM, 2024: 2703-2712.
 - [30] Zhang P, He F Z, Zhang H, et al. Real-time malicious traffic detection with online isolation forest over SD-WAN[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2076-2090.
 - [31] Kim J, Seo M, Lee S, et al. Enhancing security in SDN: systematizing attacks and defenses from a penetration perspective[J]. Computer Networks, 2024, 241: 110203.
 - [32] 郭泽华, 窦松石, 齐力, 等. 面向软件定义广域网的路径可编程性保障研究综述[J]. 电子与信息学报, 2023, 45(5): 1899-1910.
Guo Z H, Dou S S, Qi L, et al. A survey of maintaining the path programmability in software-defined wide area networks[J]. Journal of Electronics & Information Technology, 2023, 45(5): 1899-1910.
 - [33] 林莉, 毛新雅, 储振兴, 等. 混合云环境下面向数据生命周期的自适应访问控制[J]. 软件学报, 2024, 35(3): 1357-1376.
Lin L, Mao X Y, Chu Z X, et al. Adaptive access control oriented to data life cycle in hybrid cloud environment[J]. Journal of Software, 2024, 35(3): 1357-1376.
 - [34] Wang Z R, Liu Y, Huang J. An open API architecture to discover the trustworthy explanation of cloud AI services[J]. IEEE Transactions on Cloud Computing, 2024, 12(2): 762-776.
 - [35] Ito C, Ozer M. Multivocal literature review on zero-trust security implementation[J]. Computers & Security, 2024, 141: 103827.
 - [36] Palmo Y, Tanimoto S, Sato H, et al. Optimal federation method for embedding internet of things in software-defined perimeter[J]. IEEE Consumer Electronics Magazine, 2022, 12(5): 68-75.
 - [37] Lawrence T, Li F G, Ali I, et al. A computationally efficient HMAC-based authentication scheme for network coding[J]. Telecommunication Systems, 2022, 79(1): 47-69.
 - [38] Banerjee U, Juvekar C, Fuller S H, et al. eeDTLS: energy-efficient datagram transport layer security for the Internet of Things[C]//Proceedings of the GLOBECOM 2017 - 2017 IEEE Global Communications Conference. Piscataway: IEEE Press, 2017: 1-6.
 - [39] Moubayed A, Refaey A, Shami A. Software-defined perimeter (SDP): state of the art secure solution for modern networks[J]. IEEE Network, 2019, 33(5): 226-233.
 - [40] Lefebvre M, Nair S, Engels D W, et al. Building a software defined perimeter (SDP) for network introspection[C]//Proceedings of the 2021 IEEE Conference on Network Function Virtualization and

- Software Defined Networks (NFV-SDN). Piscataway: IEEE Press, 2021: 91-95.
- [41] Xiao S Y, Ye Y H, Kanwal N, et al. SoK: context and risk aware access control for zero trust systems[J]. *Security and Communication Networks*, 2022, 2022(1): 7026779.
- [42] Fang H, Wang X B, Al-Dhahir N, et al. Joint design of multi-dimensional multiple access and lightweight continuous authentication in zero-trust environments[C]//*Proceedings of the GLOBECOM 2023 - 2023 IEEE Global Communications Conference*. Piscataway: IEEE Press, 2023: 3366-3371.
- [43] Dai L L, Wang B C, Ding Z G, et al. A survey of non-orthogonal multiple access for 5G[J]. *IEEE Communications Surveys & Tutorials*, 2018, 20(3): 2294-2323.
- [44] Karimi L, Aldairi M, Joshi J, et al. An automatic attribute-based access control policy extraction from access logs[J]. *IEEE Transactions on Dependable and Secure Computing*, 2022, 19(4): 2304-2317.
- [45] Zheng W Y, Chen B, He D B. An adaptive access control scheme based on trust degrees for edge computing[J]. *Computer Standards & Interfaces*, 2022, 82: 103640.
- [46] 单棣斌, 杜学绘, 王文娟, 等. 基于场景感知的访问控制模型[J]. *网络与信息安全学报*, 2024, 10(1): 58-78.
- Shan D B, Du X H, Wang W J, et al. Scenario-aware access control model[J]. *Chinese Journal of Network and Information Security*, 2024, 10(1): 58-78.
- [47] 李琦, 樊昊源, 陈伟, 等. 面向云存储的属性基双边访问控制方案[J]. *通信学报*, 2024, 45(4): 128-136.
- Li Q, Fan H Y, Chen W, et al. Attribute-based bilateral access control scheme for cloud storage[J]. *Journal on Communications*, 2024, 45(4): 128-136.
- [48] Zhang K X, Xu S J, Shin B. Towards adaptive zero trust model for secure AI[C]//*Proceedings of the 2023 IEEE Conference on Communications and Network Security (CNS)*. Piscataway: IEEE Press, 2023: 1-2.
- [49] You H, Ko D, Kim D, et al. Dynamic access control method for SDP-based network environments[J]. *EURASIP Journal on Wireless Communications and Networking*, 2023, 2023(1): 94.
- [50] Bayılmış C, Ali Ebleme M, çAvuşOğLu ü, et al. A survey on communication protocols and performance evaluations for internet of things[J]. *Digital Communications and Networks*, 2022, 8(6): 1094-1104.
- [51] T N N, Pramod D, Singh R. Zero trust security model: defining new boundaries to organizational network[C]//*Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing*. New York: ACM, 2023: 603-609.
- [52] Basta N, Ikram M, Ali Kaafar M, et al. Towards a zero-trust micro-segmentation network security strategy: an evaluation framework[C]//*Proceedings of the NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. Piscataway: IEEE Press, 2022: 1-7.
- [53] Sheikh N, Pawar M, Lawrence V. Zero trust using network micro segmentation[C]//*Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. Piscataway: IEEE Press, 2021: 1-6.
- [54] Kern M, Landauer M, Skopik F, et al. A logging maturity and decision model for the selection of intrusion detection cyber security solutions[J]. *Computers & Security*, 2024, 141: 103844.
- [55] Alalmaie A, Nanda P, He X J. Zero trust network intrusion detection system (NIDS) using auto encoder for attention-based CNN-BiLSTM[C]//*Proceedings of the 20th International Conference on Security and Cryptography*. 2023: 99-110.
- [56] Javeed D, Saeed M S, Adil M, et al. A federated learning-based zero trust intrusion detection system for Internet of Things[J]. *Ad Hoc Networks*, 2024, 162: 103540.
- [57] Qu Y S, Chen J F, Li M, et al. Abnormal user behavior generation based on DCGAN in zero trust network[J]. *Procedia Computer Science*, 2022, 214: 1500-1505.
- [58] Wood M. How SASE is defining the future of network security[J]. *Network Security*, 2020, (12): 6-8.
- [59] 金盛豪, 郑宇, 涂昱, 等. 基于属性的SASE访问控制及动态路由技术研究[J]. *数据与计算发展前沿(中英文)*, 2024, 6(6): 97-108.
- Jin S H, Zheng Y, Tu Y, et al. Attribute-based SASE access control and dynamic routing technology[J]. *Frontiers of Data & Computing*, 2024, 6(6): 97-108.
- [60] 柴瑶琳, 韩维娜, 张云畅, 等. SASE关键技术与产业发展研究[J]. *中兴通讯技术*, 2024, 30(2): 72-75.
- Chai Y L, Han W N, Zhang Y C, et al. Key technology and industry development of secure access service edge[J]. *ZTE Technology Journal*, 2024, 30(2): 72-75.
- [61] Aiello S, Rimal B P. Secure access service edge convergence: recent progress and open issues[J]. *IEEE Security & Privacy*, 2024, 22(2): 8-16.
- [62] Hussain M, Pal S, Jadidi Z, et al. Federated zero trust architecture using artificial intelligence[J]. *IEEE Wireless Communications*, 2024, 31(2): 30-35.
- [63] Alevizos L, Ta V T, Hashem Eiza M. Augmenting zero trust architecture to endpoints using blockchain: a state-of-the-art review[J]. *Security and Privacy*, 2022, 5(1): e191.
- [64] García-Teodoro P, Camacho J, Maciá-Fernández G, et al. A novel zero-trust network access control scheme based on the security profile of devices and users[J]. *Computer Networks*, 2022, 212: 109068.
- [65] Ferretti L, Magnanini F, Andreolini M, et al. Survivable zero trust for cloud computing environments[J]. *Computers & Security*, 2021, 110: 102419.
- [66] Zaheer Z, Chang H, Mukherjee S, et al. eZTrust: network-independent zero-trust perimeterization for microservices[C]//*Proceedings of the 2019 ACM Symposium on SDN Research*. New York: ACM, 2019: 49-61.
- [67] Liu s, Zhuang Y J Huang L, et al. Exploiting LSB self-quantization for plaintext-related image encryption in the zero-trust cloud[J]. *Journal of Information Security and Applications*, 2022, 66: 103138.
- [68] Zanasi C, Russo S, Colajanni M. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures[J]. *Ad Hoc Networks*, 2024, 156: 103414.
- [69] Liu C W, Tan R, Wu Y, et al. Dissecting zero trust: research landscape

- and its implementation in IoT[J]. *Cybersecurity*, 2024, 7(1): 20.
- [70] Ge Y F, Zhu Q Y. GAZETA: game-theoretic zero-trust authentication for defense against lateral movement in 5G IoT networks[J]. *IEEE Transactions on Information Forensics and Security*, 2023, 19: 540-554.
- [71] Alagappan A, Venkatachary S K, Andrews L J B. Augmenting zero trust network architecture to enhance security in virtual power plants[J]. *Energy Reports*, 2022, 8: 1309-1320.
- [72] Liu Y Z, Hao X H, Ren W, et al. A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust Internet-of-things[J]. *IEEE Transactions on Computers*, 2023, 72(2): 501-512.
- [73] Wang J, Chen J H, Xiong N, et al. S-BDS: an effective blockchain-based data storage scheme in zero-trust IoT[J]. *ACM Transactions on Internet Technology*, 2023, 23(3): 1-23.
- [74] Huang W H, Xie X M, Wang Z Y, et al. ZT-Access: a combining zero trust access control with attribute-based encryption scheme against compromised devices in power IoT environments[J]. *Ad Hoc Networks*, 2023, 145: 103161.
- [75] Han C C, Chenchen Han G K, Gwang-Jun Kim O A, et al. ZT-BDS: a secure blockchain-based zero-trust data storage scheme in 6G edge IoT[J]. *Journal of Internet Technology*, 2022, 23(2): 289-295.
- [76] Sedjelmaci H, Tourki K, Ansari N. Enabling 6G security: the synergy of zero trust architecture and artificial intelligence[J]. *IEEE Network*, 2024, 38(3): 171-177.
- [77] Xu X L, Zhou X H, Zhou X K, et al. Distributed edge caching for zero trust-enabled connected and automated vehicles: a multi-agent reinforcement learning approach[J]. *IEEE Wireless Communications*, 2024, 31(2): 36-41.
- [78] Ali B, Gregory M A, Li S, et al. Implementing zero trust security with dual fuzzy methodology for trust-aware authentication and task offloading in multi-access edge computing[J]. *Computer Networks*, 2024, 241: 110197.
- [79] Cao H T, Yang L X, Garg S, et al. Softwarized resource allocation of tailored services with zero security trust in 6G networks[J]. *IEEE Wireless Communications*, 2024, 31(2): 58-65.
- [80] Abdelhay Z, Bello Y, Refaey A. Toward zero-trust 6GC: a software defined perimeter approach with dynamic moving target defense mechanism[J]. *IEEE Wireless Communications*, 2024, 31(2): 74-80.
- [81] Liu Y L, Su Z, Peng H X, et al. Zero trust-based mobile network security architecture[J]. *IEEE Wireless Communications*, 2024, 31(2): 82-88.
- [82] Chen X, Feng W, Ge N, et al. Zero trust architecture for 6G security[J]. *IEEE Network*, 2024, 38(4): 224-232.
- [83] Meng W Z, Li W J, Kwok L F. Towards effective trust-based packet filtering in collaborative network environments[J]. *IEEE Transactions on Network and Service Management*, 2017, 14(1): 233-245.
- [84] Pappas C, Lee T, Reischuk R M, et al. Network transparency for better Internet security[J]. *IEEE/ACM Transactions on Networking*, 2019, 27(5): 2028-2042.
- [85] Zhu C X, Dastani M, Wang S H. A survey of multi-agent deep reinforcement learning with communication[J]. *Autonomous Agents and Multi-Agent Systems*, 2024, 38(1): 4.
- [86] Xu L J, Qin M, Yang Q H, et al. Learning-aided dynamic access control in MEC-enabled green IoT networks: a convolutional reinforcement learning approach[J]. *IEEE Transactions on Vehicular Technology*, 2022, 71(2): 2098-2109.
- [87] Ben farah M, Ahmed Y, Mahmoud H, et al. A survey on blockchain technology in the maritime industry: Challenges and future perspectives[J]. *Future Generation Computer Systems*, 2024, 157: 618-637.
- [88] Jiang P, Liu Q, Zhu L H. SanIdea: exploiting secure blockchain-based access control via sanitizable encryption[J]. *IEEE Transactions on Information Forensics and Security*, 2023, 19: 1589-1600.
- [89] He G X, Li C L, Shu Y, et al. Fine-grained access control policy in blockchain-enabled edge computing[J]. *Journal of Network and Computer Applications*, 2024, 221: 103706.
- [90] Chen X, Wu C M, Liu X, et al. Empowering network security with programmable switches: a comprehensive survey[J]. *IEEE Communications Surveys & Tutorials*, 2023, 25(3): 1653-1704.
- [91] Kianpisheh S, Taleb T. A survey on in-network computing: programmable data plane and technology specific applications[J]. *IEEE Communications Surveys & Tutorials*, 2023, 25(1): 701-761.
- [92] Mai T L, Yao H P, Guo S, et al. In-network computing powered mobile edge: toward high performance industrial IoT[J]. *IEEE Network*, 2021, 35(1): 289-295.
- [93] Hong S, Xu L, Huang J W, et al. SysFlow: toward a programmable zero trust framework for system security[J]. *IEEE Transactions on Information Forensics and Security*, 2023, 18: 2794-2809.
- [94] Liu Y, Xia Y, Zhang W T, et al. SFANT: a SRv6-based flexible and active network telemetry scheme in programming data plane[J]. *IEEE Transactions on Network Science and Engineering*, 2024, 11(3): 2415-2425.
- [95] Scarpitta C, Sidoretti G, Mayer A, et al. High performance delay monitoring for SRv6-based SD-WANs[J]. *IEEE Transactions on Network and Service Management*, 2024, 21(1): 1067-1081.
- [96] 龚俭, 臧小东, 苏琪, 等. 网络安全态势感知综述[J]. *软件学报*, 2017, 28(4): 1010-1026.
- Gong J, Zang X D, Su Q, et al. Survey of network security situation awareness[J]. *Journal of Software*, 2017, 28(4): 1010-1026.
- [97] Rahman M A, Hossain M S. A deep learning assisted software defined security architecture for 6G wireless networks: IIoT perspective[J]. *IEEE Wireless Communications*, 2022, 29(2): 52-59.
- [98] Teerakanok S, Uehara T, Inomata A. Migrating to zero trust architecture: reviews and challenges[J]. *Security and Communication Networks*, 2021, 2021(1): 9947347.
- [99] Singh J, Refaey A, Shami A. Multilevel security framework for NFV based on software defined perimeter[J]. *IEEE Network*, 2020, 34(5): 114-119.
- [100] Guo J, Li B S, Du P, et al. Multi-attribute authentication method based on continuous trust evaluation[C]//*Smart Computing and Communication*. Cham: Springer, 2022: 90-100.
- [101] Liu X, Tan Z C, Liang L, et al. A multidimensional trust evaluation mechanism for improving network security in fog computing[J]. *IEEE Transactions on Industrial Informatics*, 2024, 20(12): 14287-14296.

- [102] Wang J, Yan Z, Lan J H, et al. TrustGuard: GNN-based robust and explainable trust evaluation with dynamicity support[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(5): 4433-4450.
- [103] Vucovich M, Quinn D, Choi K, et al. FedBayes: a zero-trust federated learning aggregation to defend against adversarial attacks[C]// Proceedings of the 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC). Piscataway: IEEE Press, 2024: 28-35.
- [104] Mutalib N H A, Sabri A Q M, Wahab A W A, et al. Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: a review[J]. Artificial Intelligence Review, 2024, 57(11): 297.
- [105] 周天, 郑昉昱, 林璟镔, 等. 后量子密码算法的软件实现研究[J]. 密码学报(中英文), 2024, 11(2): 308-343.
Zhou T, Zheng F Y, Lin J Q, et al. On software implementations of post-quantum cryptography[J]. Journal of Cryptologic Research, 2024, 11(2): 308-343.
- [106] 张雪, 高飞, 秦素娟, 等. 量子密码协议研究现状与未来发展[J]. 中国工程科学, 2022, 24(4): 145-155.
Zhang X, Gao F, Qin S J, et al. Current status and future development of quantum cryptographic protocols[J]. Strategic Study of CAE, 2022, 24(4): 145-155.

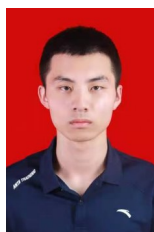
[作者简介]



王子豪 (1998-), 男, 河南许昌人, 信息工程大学博士生, 主要研究方向为云网融合、网络空间安全、机器学习等。



崔鹏帅 (1990-), 男, 河南安阳人, 信息工程大学副研究员, 主要研究方向为新型网络体系结构、可编程数据平面。



潘潘 (2001-), 男, 安徽安庆人, 信息工程大学博士生, 主要研究方向为云网融合、网络空间安全、匿名网络等。



胡宇翔 (1982-), 男, 河南周口人, 信息工程大学教授、博士生导师, 主要研究方向为新型网络体系结构、路由与交换技术、网络空间安全。



田乐 (1987-), 男, 陕西咸阳人, 博士, 信息工程大学副研究员, 主要研究方向为新型网络体系结构、时间敏感网络、路由与交换技术。



陈鸿昶 (1964-), 男, 河南新密人, 信息工程大学教授, 主要研究方向为未来网络体系结构、网络安全、人工智能等。



邬江兴 (1953-), 男, 安徽金寨人, 中国工程院院士, 信息工程大学教授, 博士生导师, 主要研究方向为网络通信与安全。