

云计算及物联网背景下的网络安全技术架构路径研究

谭云

青岛职业技术学院, 山东 青岛 266555

DOI: 10.61369/TACS.2025010001

摘 要 : 在云计算及物联网蓬勃发展的当下, 网络安全面临着全新且复杂的挑战。云计算凭借其资源共享、灵活部署等特性, 改变了传统的 IT 资源交付模式; 物联网则通过设备互联, 拓展了网络边界。二者融合虽带来诸多便利, 却也滋生了诸如数据泄露、恶意攻击等安全隐患。本文深入剖析云计算及物联网背景下网络安全技术架构面临的问题, 从数据安全、网络边界、身份认证、安全管理等维度探讨相应路径。通过强化加密技术、构建动态边界防护、创新身份认证机制、完善安全管理体系等举措, 旨在打造适应新时代需求的网络安全技术架构, 保障云计算与物联网环境下数据与系统的稳定、可靠与安全。

关 键 词 : 云计算; 物联网; 网络安全; 技术架构

Research on the Path of Network Security Technology Architecture in the Context of Cloud Computing and the Internet of Things

Tan Yun

Qingdao Vocational and Technical College, Qingdao, Shandong 266555

Abstract : With the vigorous development of cloud computing and the Internet of Things, network security is facing new and complex challenges. Cloud computing, with its characteristics of resource sharing and flexible deployment, has changed the traditional IT resource delivery model, while the Internet of Things has expanded network boundaries through device interconnection. Although the integration of the two brings many conveniences, it also gives rise to security risks such as data leakage and malicious attacks. This article deeply analyzes the problems faced by the network security technology architecture in the context of cloud computing and the Internet of Things, and explores corresponding paths from the dimensions of data security, network boundaries, identity authentication, and security management. By strengthening encryption technology, building dynamic boundary protection, innovating identity authentication mechanisms, and improving the security management system, we aim to create a network security technology architecture that meets the needs of the new era and ensures the stability, reliability, and security of data and systems in the cloud computing and Internet of Things environments.

Keywords : cloud computing; Internet of Things; network security; technology architecture

引言

在数字化转型的时代浪潮中, 云计算与物联网技术作为前沿力量, 正深刻重塑着各行业的运作模式与发展格局。云计算凭借其强大的计算资源共享、灵活的服务定制以及高效的资源调度能力, 为企业与机构提供了便捷且低成本的 IT 基础设施解决方案, 促使各类应用得以在云端高效部署与运行, 极大提升了业务的灵活性与可扩展性^[1]。物联网则通过将海量物理设备接入网络, 实现设备间的互联互通与数据交互, 使物理世界与数字世界深度融合, 催生出智能交通、智慧医疗、工业互联网等丰富多样的创新应用场景, 推动传统产业向智能化、自动化方向转型升级^[2]。然而, 这两项技术的迅猛发展与深度融合, 也使网络安全领域面临前所未有的严峻挑战。云计算环境下多租户共享资源带来的数据隔离难题、云服务的可靠性与稳定性风险; 物联网中大量设备接入导致的网络边界模糊、设备安全防护薄弱、数据传输安全隐患等问题, 都对构建稳固、可靠的网络安全技术架构提出了紧迫需求, 亟待深入研究应对之策。

一、云计算及物联网背景下网络安全面临的挑战

（一）数据安全风险

在云计算与物联网融合场景下，数据量呈爆发式增长，数据安全风险随之剧增。一方面，云计算平台上存储着海量来自物联网设备及企业用户的数据，多租户模式下，数据隔离难度加大，一旦隔离机制出现漏洞，便可能导致数据泄露，使敏感信息被恶意获取。例如，不同企业的业务数据存储在单一云平台，若因技术故障或人为攻击突破了数据隔离边界，一家企业的数据可能被其他租户窥探^[3]。另一方面，物联网设备采集的数据在传输过程中，由于其网络环境复杂，涉及多种通信协议与链路，易遭受中间人攻击，数据可能被窃取、篡改或伪造，这对依赖准确数据的业务应用，如智能医疗中的远程诊断、工业物联网中的精准生产控制等，构成严重威胁，可能引发错误决策，甚至造成安全事故。

（二）网络边界模糊带来的威胁

传统网络具有清晰的边界，便于实施安全防护措施，但云计算与物联网打破了这一界限。云计算的分布式特性使得数据与应用在云端、边缘端和用户端之间流动，网络边界被极大拓展且动态变化^[4]。物联网中，大量设备通过无线、有线等多种方式接入网络，从智能家居设备到工业现场的传感器、执行器，设备类型繁杂，接入点众多，难以进行统一有效的边界管理。黑客可利用这些模糊的边界，通过物联网设备作为跳板，潜入云计算平台，或者绕过传统安全防护机制，对网络核心区域发起攻击，导致安全防护难度大幅提升，传统基于固定边界的防火墙等安全设备难以发挥有效作用^[5]。

（三）设备身份认证与访问控制难题

物联网设备数量庞大、种类多样，且部分设备计算与存储资源有限，难以采用复杂的身份认证与访问控制机制。许多物联网设备在出厂时默认配置简单，如默认密码等，用户往往未及时修改，这为攻击者提供了可乘之机，容易引发设备被劫持、非法访问等问题^[6]。在云计算环境中，用户与应用对云资源的访问频繁且复杂，传统静态的身份认证方式，如用户名加密码，已无法满足安全需求，难以应对日益增长的网络攻击手段，如暴力破解、密码窃取等。若身份认证与访问控制环节存在漏洞，攻击者可轻易获取合法身份，肆意访问和操作云资源与物联网设备，对系统造成严重破坏^[7]。

（四）安全管理复杂性增加

云计算及物联网的广泛应用，使网络环境变得错综复杂，安全管理的难度和复杂性显著提升。从管理对象来看，涉及云服务提供商、物联网设备制造商、网络运营商、企业用户等多个主体，各方在安全责任界定、协调合作等方面存在诸多难题^[8]。例如，当出现安全事件时，难以快速确定是云平台的安全漏洞、物联网设备的安全隐患，还是用户自身操作不当所致。从技术层面，云计算与物联网涉及多种新技术、新协议，如虚拟化技术、边缘计算、MQTT 协议等，安全管理人员需要掌握大量不同领域的知识，才能有效应对安全问题，这对人员的专业素质提出了极高要求，也增加了安全管理的人力成本与技术难度^[9]。

二、云计算及物联网背景下网络安全技术架构构建路径

（一）强化数据安全保护技术

为应对云计算及物联网中的数据安全风险，需从数据加密、

存储与传输安全等方面强化技术手段。在数据加密方面，采用先进的加密算法，如国密算法 SM4 等，对静态存储在云平台的数据和传输过程中的物联网数据进行加密处理，确保数据在任何状态下的保密性。对于不同敏感度的数据，设置不同的加密级别，提高加密效率与安全性^[10]。在存储安全上，云平台应构建冗余存储机制，通过多副本存储技术，防止因硬件故障或攻击导致数据丢失，并采用数据完整性校验技术，定期检测数据是否被篡改。在数据传输环节，利用虚拟专用网络（VPN）技术，建立安全加密通道，结合传输层安全协议（TLS）等，保障数据在复杂网络环境中传输的安全性，防止数据被窃取或篡改^[11]。

（二）构建动态网络边界防护体系

针对网络边界模糊的问题，构建动态网络边界防护体系至关重要。摒弃传统固定边界防护思路，引入软件定义网络（SDN）和网络功能虚拟化（NFV）技术，实现网络边界的动态调整与灵活配置。通过 SDN 控制器，实时感知网络流量与设备接入情况，根据预先设定的安全策略，动态调整网络拓扑结构，隔离异常流量与非法接入设备^[12]。利用 NFV 技术，将传统网络安全设备，如防火墙、入侵检测系统等，进行虚拟化部署，使其能够快速适应网络边界的变化，在不同网络节点灵活部署安全功能。同时，采用零信任安全理念，对网络内外部的所有访问请求进行持续验证与授权，不论其是否来自传统意义上的内部网络，以最小权限原则严格控制访问，有效抵御从模糊边界发起的攻击^[13]。

（三）创新身份认证与访问控制机制

为解决设备身份认证与访问控制难题，需创新相关机制。对于物联网设备，采用轻量级身份认证技术，结合设备的唯一标识、硬件特征等，生成设备的数字证书，利用椭圆曲线密码体制（ECC）等高效加密算法，在资源受限的设备上实现安全可靠的身份认证。同时，引入基于生物特征的认证方式，如指纹识别、人脸识别等，应用于具备相应功能的物联网设备，增强认证的准确性与安全性^[14]。在云计算环境中，推行多因素身份认证，除传统用户名密码外，结合短信验证码、硬件令牌、生物特征等多种因素进行身份验证，大幅提高认证强度。采用基于属性的访问控制（ABAC）模型，根据用户、设备、资源的属性及环境因素，动态授予访问权限，实现细粒度、灵活的访问控制，有效防止非法访问与权限滥用^[15]。

（四）完善安全管理体系

面对云计算及物联网环境下安全管理复杂性的显著增加，完善安全管理体系是保障网络安全的核心任务。明确各方安全责任是构建有效安全管理体系的基础。云服务提供商作为云平台的运营者，承担着保障云平台基础设施安全、数据存储与传输安全的主要责任，需确保云平台具备完善的安全防护措施，防止因平台漏洞导致用户数据泄露或服务中断。物联网设备制造商在设备生产过程中，应充分考虑设备的安全性，采用安全的芯片、操作系统与通信协议，确保设备在出厂时具备基本的安全防护能力，并及时为设备提供安全漏洞修复与升级服务。网络运营商负责保障网络传输的稳定性与安全性，防止网络链路遭受攻击或出现故障影响数据传输^[16]。其次，建立统一的安全管理平台，整合云计算与物联网中的安全信息，实现对设备状态、网络流量、安全事件等的集中监控与管理。利用大数据分析技术，对海量安全数据进行实时分析，及时发现潜在安全威胁与异常行为，提前预警并采

取相应措施^[17]。再者，加强安全人才培养，通过组织专业培训、开展安全技术竞赛等方式，提升安全管理人员的专业素养与实战能力，使其能够熟练应对云计算及物联网环境下复杂的安全管理任务。

三、云计算及物联网背景下网络安全技术架构的发展趋势

（一）人工智能与机器学习助力安全防护

随着人工智能与机器学习技术的不断发展，其在网络安全领域的应用将愈发广泛与深入。在云计算及物联网安全防护中，利用机器学习算法对大量网络流量数据、设备行为数据进行学习与分析，建立正常行为模型^[18]。一旦网络流量或设备行为偏离正常模型，系统可自动识别并预警潜在的安全威胁，如入侵行为、恶意软件传播等。人工智能还可用于优化安全策略，根据实时安全态势自动调整访问控制策略、动态部署安全防护措施，提高安全防护的精准性与效率，实现从被动防御向主动防御的转变，有效应对日益复杂多变的网络攻击手段。

（二）量子加密技术提升数据安全

随着量子计算技术的发展，传统加密算法面临被破解的风险，而量子加密技术作为一种新兴的加密方式，为数据安全提供了更高等级的保障。量子加密基于量子力学原理，利用量子态的不可克隆性与测量坍缩特性，实现信息的安全传输。在云计算及物联网场景中，量子加密可用于保护关键数据的传输与存储安全，如金融交易数据、医疗敏感信息等。采用量子密钥分发技术，生成绝对安全的加密密钥，确保数据在传输与存储过程中无法被窃听与篡改，极大增强数据的保密性与完整性，为云计算及物联网的数据安全构筑坚固防线^[19]。

（三）云边协同安全架构的深化应用

云边协同作为云计算与物联网融合发展的重要模式，其安全架构也将不断深化应用。在这种架构下，云计算中心负责提供强大的计算资源与全局安全策略管理，边缘计算节点则靠近物联网设备，承担本地数据处理与实时安全防护任务^[20]。通过云边协同，实现安全数据的共享与联动，如边缘节点实时采集设备安全

信息并上传至云端，云端利用大数据分析 with 人工智能技术进行综合研判，将分析结果与安全策略反馈至边缘节点，指导其进行本地安全防护。同时，云边协同安全架构可根据网络状况、业务需求等动态调整安全防护资源的分配，提高整体安全防护效能，适应云计算及物联网环境下多样化的安全需求。

（四）标准化与合规化发展

随着云计算及物联网在各行业的广泛应用，网络安全的标准化与合规化发展成为必然趋势。一方面，行业组织与标准化机构将制定更加完善、统一的网络安全标准，涵盖云计算服务安全标准、物联网设备安全标准、数据安全标准等，为企业与机构实施网络安全防护提供明确指导，促进不同厂商产品与服务之间的兼容性与互操作性。另一方面，各国政府也将加强网络安全立法与监管，出台严格的法律法规，要求企业在使用云计算与物联网技术时，必须遵守数据保护、隐私安全等方面的规定，对违规行为进行严厉处罚。企业与机构为满足合规要求，将不断完善自身网络安全技术架构与管理体系，推动整个行业网络安全水平的提升。

四、总结

云计算及物联网的融合发展，为社会带来了巨大的发展机遇，但也使网络安全形势变得异常严峻。数据安全风险、网络边界模糊、设备身份认证与访问控制难题以及安全管理复杂性增加等问题，严重威胁着云计算及物联网环境下信息系统的稳定运行与数据安全。通过强化数据安全保护技术，从加密、存储、传输等多维度保障数据安全；构建动态网络边界防护体系，利用新技术实现边界的灵活管控；创新身份认证与访问控制机制，提高认证强度与访问控制的精准性；完善安全管理体系，明确各方责任、建立统一平台并加强人才培养，能够有效应对当前网络安全挑战，构建起适应云计算及物联网发展的网络安全技术架构。展望未来，人工智能与机器学习、量子加密技术、云边协同安全架构以及标准化与合规化发展等趋势，将为网络安全技术架构的进一步优化与完善指明方向，持续推动云计算及物联网行业在安全的轨道上蓬勃发展，为各行业数字化转型与智能化升级提供坚实保障。

参考文献

- [1] 达斯孟. 基于网络安全维护的计算机网络安全技术分析 [J]. 集成电路应用, 2024, 41(4): 298-299.
- [2] 徐梓容. 大数据时代计算机网络安全技术的优化策略 [J]. 电子元器件与信息技术, 2024, 8(3): 192-195, 199.
- [3] 魏国富, 石英村. 人工智能数据安全治理与技术发展概述 [J]. 信息安全研究, 2021, 7(2): 110-119.
- [4] 钟国辉, 郎颂. 面向智慧安防的新型网络安全技术思考与探索 [J]. 中国安防, 2024, (11): 109-113.
- [5] 陆海峰, 张雅娟. 物联网技术在网络安全策略中的应用 [J]. 集成电路应用, 2024, 41(10): 41-43.
- [6] 王雪. 大数据技术应用背景下计算机网络安全技术专业人才培养的探讨 [J]. 电脑知识与技术, 2024, 20(09): 148-150.
- [7] 陆海峰, 张雅娟. 物联网背景下计算机网络安全技术分析 [J]. 中国新通信, 2024, 26(05): 50-52+85.
- [8] 郝博麟. 物联网在提升网络安全技术中的应用分析 [J]. 网络安全技术与应用, 2023, (11): 6-7.
- [9] 杜璞, 宫甜甜. 云计算及物联网背景下的网络安全技术架构 [J]. 信息系统工程, 2023, (05): 11-13.
- [10] 刘陈晓. 基于大数据的 5G 物联网安全分析 [J]. 电子元器件与信息技术, 2023, 7(02): 198-201.
- [11] 胡璇, 李伟明, 冷昊, 程德斌. 美军网络安全技术研究现状及发展趋势 [J]. 电子产品可靠性与环境试验, 2022, 40(06): 96-104.
- [12] 张赛男. 区块链技术的网络安全技术的有效应用 [J]. 电子技术与软件工程, 2022, (21): 5-8.
- [13] 郭娇娇. 物联网背景下计算机网络安全技术研究 [J]. 电子技术与软件工程, 2022, (11): 30-33.
- [14] 宋采燕. 移动物联网智能信息终端网络安全技术的应用分析 [J]. 电子技术与软件工程, 2022, (10): 26-29.
- [15] 李星. 云计算及物联网背景下的网络安全新技术 [J]. 数字技术与应用, 2022, 40(02): 209-212.
- [16] 刘沛. 探析云计算及物联网背景下的网络安全新技术 [J]. 电子世界, 2021, (20): 166-167.
- [17] 田赓文. 物联网技术背景下网络安全及应用——评《物联网网络安全及应用》[J]. 热带作物学报, 2021, 42(08): 2459.
- [18] 梁军. 物联网技术背景下探讨网络安全问题及应对策略研究——评《物联网网络安全及应用》[J]. 中国测试, 2021, 47(05): 174.
- [19] 郑轶, 王路路, 胡志锋, 陈琳. 泛在物联网背景下智慧电力物联网网络安全技术探索 [J]. 网络空间安全, 2020, 11(12): 65-72.
- [20] 陈飞. 云计算及物联网背景下的网络安全新技术探究 [J]. 数码世界, 2020, (06): 266.