计算机研究与发展
Journal of Computer Research and Development
https://crad.ict.ac.cn
62(11): 2784−2805, 2025

工业物联网零信任安全研究综述

王航宇[1,2] 吕 飞[1,2] 程裕亮[3] 吕世超[1,2] 孙德刚[2,4] 孙利民[1,2]
[1](中国科学院信息工程研究所 北京 100085)
[2](中国科学院大学网络空间安全学院 北京 100049)
[3](沈阳航空航天大学人工智能学院 沈阳 110136)
[4](中国科学院计算机网络信息中心 北京 100083)
(wanghangyu@iie.ac.cn)

Review of Zero Trust Security Research in Industrial Internet of Things

Wang Hangyu[1,2], Lü Fei[1,2], Cheng Yuliang[3], Lü Shichao[1,2], Sun Degang[2,4], and Sun Limin[1,2]
[1](*Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100085)
[2](*School of Cyber Security*, *University of Chinese Academy of Sciences*, *Beijing* 100049)
[3](*College of Artificial Intelligence*, *Shenyang Aerospace University*, *Shenyang* 110136)
[4](*Computer Network Information Center*, *Chinese Academy of Sciences*, *Beijing* 100083)

Abstract The industrial Internet of things (IIoT) faces increasingly severe security threats, and traditional perimeter-based security models are no longer adequate to address evolving and complex demands. Zero trust, an emerging security model centered on the core principle of "never trust, always verify," has gradually gained attention. However, the research and application of zero trust in the IIoT domain are still in their early stages, necessitating more comprehensive and systematic exploration. We provide a systematic review of the development and applications of zero trust in the industrial sector, with a focus on analyzing its core technologies and practical scenarios while identifying current research trends and future directions. We introduce the basic concepts and principles of industrial zero trust, establishing a theoretical foundation for subsequent discussions. We then systematically outline the migration strategies and evaluation methods for industrial zero trust architectures and summarize key technologies, including authentication, software-defined perimeters, micro-segmentation, secure communication channels, and trust evaluation, collectively forming the core supporting framework of industrial zero trust. Furthermore, we delve into the critical role of access control within the zero trust model and its value in fine-grained permission management. By examining typical IIoT application scenarios, we further explore the practical advantages of zero trust in complex environments. Finally, we identify existing challenges in industrial zero trust and discuss potential future development directions.

Key words zero trust; IIoT; authentication; software-defined perimeter (SDP); micro-segmentation; access control

摘 要 工业物联网(industrial Internet of things, IIoT)正面临着日益严峻的安全威胁,传统边界型安全模型已无法应对复杂多变的需求.零信任作为一种新兴的安全模型,以"绝不信任,始终认证"为核心原则,逐渐受到关注.然而,零信任在IIoT中的研究与应用仍处于起步阶段,亟需更加全面且系统的探索.系统综述了近年来工业领域零信任的发展与应用,重点分析其核心技术与实践场景,并明确当前研究趋势和

收稿日期: 2024-10-31; **修回日期**: 2025-03-27
基金项目: 北京市自然科学基金项目(L234033)
This work was supported by Beijing Natural Science Foundation (L234033).
通信作者: 吕飞(lvfei@iie.ac.cn)

未来方向. 首先介绍了工业零信任的基本概念和原则，为后续讨论奠定理论基础. 随后，系统梳理了工业零信任架构的迁移与评估方法，并总结了身份认证、软件定义边界、微隔离、信道安全及信任评估等关键技术，这些技术构成了工业零信任的核心支撑体系. 此外，深入探讨了访问控制在零信任中的关键作用及其在权限管理中的价值. 结合 IIoT 的典型应用场景，进一步分析零信任在复杂环境中的实践优势，最后总结了工业零信任的现存挑战和未来发展.

关键词 零信任；工业物联网；身份认证；软件定义边界；微隔离；访问控制

中图法分类号 TP393.08

DOI: 10.7544/issn1000-1239.202440840 **CSTR:** 32373.14.issn1000-1239.202440840

物联网通过网络将物理设备、人与物、物与物随时随地连接起来[1-2]. 工业物联网(industrial Internet of things, IIoT)专注于在工业环境中应用物联网技术，通过将各类工业设备连接到网络上，极大地提高了工业过程的智能化、效率、安全性和生产力[3]. 然而，近年来随着 IIoT 的设备数量激增以及与互联网的深度集成，使得工业系统面临的网络威胁显著增多[4]. 传统的安全架构通常利用防火墙、入侵检测系统等手段，建立安全隔离“墙”，将网络隔离为可信/不可信域，以实现安全防护. 但是这种边界安全架构正面临巨大挑战：一方面，日益复杂的设备网络模糊了传统的边界概念，使得设立明确的边界变得困难；另一方面，仅依靠边界进行防护的方式存在明显局限性，一旦攻击者渗透进可信域，便可横向移动扩大攻击范围[5]. 因此，IIoT 亟需一种可靠、稳定且高效的安全保护机制来确保信息安全.

零信任(zero trust, ZT)是一种以资源保护为核心的网络安全模型，遵循“绝不信任、始终认证”的原则. 它摒弃了传统的边界防护思想，不再对任何访问主体默认授予信任，而是通过持续的信任评估动态调整和管理安全策略. 它通过增强的身份认证、动态的访问控制以及资源间的微隔离等方式，有效抵御来自网络内部和外部的威胁[6]. 因此，零信任在 IIoT 安全领域得到了广泛关注与研究.

本文基于 Buck 等人[7]提出的文献检索方法，对谷歌学术核心数据库中近 5 年的相关文献进行系统性整理和综述. 为帮助研究者全面了解当前零信任的研究现状，我们精选了具有代表性的理论及应用类文献(涵盖 SCI 和 CCF-C 及以上级别)，深入分析零信任的概念、理论框架及核心技术，并从架构与技术组成等角度进行了系统性梳理与探讨.

本文的逻辑框架如图 1 所示，首先介绍了工业零信任架构的特点及其主要原则，阐释了零信任在工业环境中的必要性和独特价值. 然后描述了工业零信任架构的迁移与评估，旨在说明如何从传统安全架构向零信任架构过渡，以及评估零信任在 IIoT 中的实际效果，为架构设计和实施提供实践参考.

随后，本文详细介绍了工业零信任的关键技术，

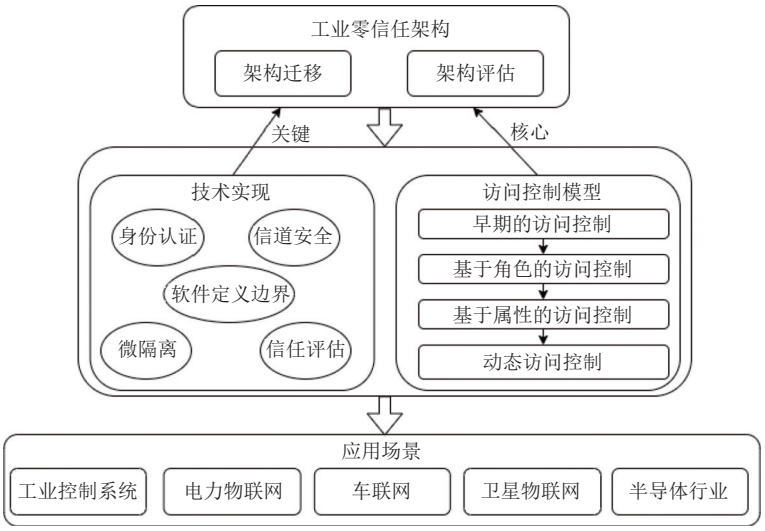


Fig. 1 Logical framework diagram of industrial zero trust

图 1 工业零信任逻辑框架图

包括身份认证、软件定义边界(software-defined perimeter, SDP)、微隔离、信道安全和信任评估(trust evaluation, TE),这些内容共同构成了工业零信任实现过程中的技术基础,有助于深入理解零信任架构如何通过多层次、多角度的防护实现系统安全.在此基础上,本文进一步深入探讨了动态访问控制这一关键机制,动态访问控制是实现工业零信任的核心.在工业环境中,设备的多样性、实时性需求以及不断变化的安全态势,使得传统的静态访问控制方法难以适应.通过动态的访问控制机制,可以实现对资源访问的细粒度管理,能够根据访问主体的实时状态和环境信息灵活调整权限,确保每个访问请求都经过严格的持续认证.这样可以有效减少信任边界的暴露,增强系统整体的安全性.因此,阐述访问控制的演进与应用是理解工业零信任体系如何在复杂工业场景中落地的必要步骤,也是实现零信任目标的关键环节.

接着,本文结合工业控制系统(industrial control system, ICS)、电力物联网(electric Internet of things, EIoT)、车联网(Internet of vehicles, IoV)、卫星物联网(satellite Internet of things, SIoT)和半导体行业等典型场景,分析了零信任模型的实际应用,通过这些案例展现零信任在不同工业领域中的广泛适用性和针对性的解决方案.

最后,本文对工业零信任的现存问题进行分析和对未来方向进行探讨,揭示了目前零信任在工业环境中的局限性和面临的挑战,分析了工业零信任的可行性与安全性,并为未来研究和实践提出可能的方向.

综上所述,本文的主要贡献有3个方面:

1)系统性介绍了IIoT中零信任架构的核心概念和关键技术,涵盖身份认证、软件定义边界、微隔离、信道安全、信任评估等内容,并与其他相关综述进行了横向对比.就我们所知,本文是系统性介绍工业领域零信任研究的综述,重点梳理了该领域的基础理论框架,分析了当前研究的进展和特点,为进一步探索工业零信任的理论和实践提供参考.

2)分析了工业零信任架构(zero trust architecture, ZTA)的设计、迁移路径及评估方法,为工业系统从传统安全架构向零信任过渡提供了理论支持和实践依据,并特别探讨了动态访问控制在应对复杂工业环境需求中的核心作用.

3)结合工业控制系统、电力物联网等典型应用场景,展示了ZTA在实际应用中的安全优势,分析其可行性和安全性,并对潜在研究方向提出展望.

1 工业零信任的引入

在介绍工业零信任的起源和发展之前,需明确工业领域的特殊需求与所面临的挑战.工业环境中设备种类多样,对安全性和实时性的要求严格,这些特性使得传统网络安全架构难以应对IIoT的复杂性.因此,零信任逐步被引入工业环境,以应对这些特定的安全挑战,从而实现更加高效、可靠的防护.本节将回顾工业零信任的发展历程,总结其特点和主要原则,并对现有工业零信任综述研究进行分析和对比,为深入探讨IIoT环境下的零信任应用场景奠定基础.

1.1 工业零信任的发展历史

“零信任”概念最早可以追溯到2004年,耶利哥论坛上首次提出了“去边界化”的安全理念[8].2007年,美国国防部和国防信息局提出“黑核(BCORE)”概念,提倡从基于边界防御转变为基于用户操作行为的安全模型[9].2010年,Forrester的Kindervag[10]提出“零信任”安全术语,标志着网络安全行业开始逐步完善并实践这一理念.2013年,云安全联盟发布了《SDP规范1.0》,详细阐述了软件定义边界及其实现方式,是零信任的解决方案[11].2014年,谷歌公司通过BeyondCorp项目,系统性介绍了企业内部如何设计与部署ZTA[12].2017年,Gartner[13]提出“持续自适应风险与信任评估”的安全架构,指出零信任是实现这一安全架构的第1步.2018年,Forrester[14]发布零信任扩展ZTX,进一步强调了网络分段的重要性.2019年,Gartner[15]发布零信任网络访问ZTNA.2020年,美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)发布“Zero Trust Architecture”,对ZTA进行了系统化定义,并介绍了通用的部署模型和应用实例,是迄今为止最权威的ZTA标准之一[6].

从2022年开始,零信任逐步应用于工业领域,初期主要用于关键基础设施的保护和ICS的安全防护.随着工业应用的深入,零信任的使用范围逐渐扩展到更多的工业场景,如EIoT、IoV、SIoT和半导体行业等.工业零信任的发展经历了从概念验证到逐步部署的过程,早期的研究和应用集中在如何为ICS提供更加安全的防护边界,以应对复杂多变的网络威胁.随着对工业场景特定需求的理解不断深入,零信任技术也不断演进,通过动态身份认证、微隔离和持续风险评估等方法提高了工业环境的整体安全性.

近年来，工业零信任技术的发展得到了广泛的关注与投入，逐渐成为 IIoT 安全领域的重要研究方向. 特别是工业企业对安全要求的不断提升，促使零信任技术在各类工业场景中的应用不断深化，从保护核心生产系统到实现全面的工业网络安全保障.

1.2 工业零信任的特点和主要原则

IIoT 的安全需求不同于传统环境，具有一系列独特的特征，这使得 ZTA 在该领域的应用显得尤为重要. 因此在设计时需要特别考虑这些因素，以确保系统的高效运作和信息安全. 以下是 IIoT 的关键特点：

1）设备多样化. IIoT 环境中包含各种工业设备，如传感器、执行器、可编程逻辑控制器（programmable logic controller, PLC）、远程终端单元（remote terminal unit, RTU）和边缘设备等. 这些设备在功能和性能上存在显著差异，需要协同工作以完成复杂的工业任务.

2）高安全性要求. 工业系统通常涉及关键基础设施，如电力、能源、交通和制造等. 这些领域一旦发生安全事件，可能对公共安全和经济稳定造成重大影响，因此 IIoT 对安全性提出了更高的要求.

3）资源受限. 许多工业设备由于计算和存储资源的限制，难以支持复杂、资源需求高的安全算法. 因此这些设备往往依赖于低功耗、高效率的安全措施，以在有限的资源条件下维持基本的安全功能.

4）私有协议和系统复杂性. 工业领域中广泛使用各种私有工业控制协议，这些协议彼此不兼容且安全性存在差异，导致系统结构复杂，难以进行统一管理.

5）高实时性要求. 工业环境通常需要在毫秒级时间内做出响应，而在高端制造领域，甚至要求微秒级的响应时间. 即便是较短的延迟也可能引发严重后果，如生产流程中断、设备损坏，甚至安全事故. 因此，保障低延迟、高效的数据处理和安全机制对于工业环境至关重要.

基于以上特点，在 IIoT 中设计 ZTA 时，需要充分考虑具体的应用场景和特定需求，从而制定合理的设计原则. 以下是设计工业 ZTA 的主要原则：

1）不可信假设. IIoT 中的设备分布广泛且类型多样，通常分散在不同地点，缺乏统一的物理边界管理，具有潜在的安全隐患. 因此，新接入的设备应被默认视为不可信，必须经过严格的认证来确保其安全性.

2）持续认证与授权. IIoT 系统涉及关键基础设施，且设备的使用周期长. 因此需对设备进行持续的身份认证与信任评估，以确保安全性和系统稳定性.

3）低时间延迟. IIoT 具有高实时性的特点，因此在进行安全防护时，需尽可能地减少安全措施对系统响应时间的影响，确保快速数据处理和即时响应.

4）通信安全性. IIoT 中使用大量私有工业控制协议进行通信，并且设备间的计算资源差异显著. 因此需结合协议特点，确保信息传递的完整性和安全性.

5）动态授权. IIoT 设备类型多样，且对实时性要求高，这使得不同设备在不同时间和环境下可能具有不同的安全需求和访问权限. 因此为应对这种动态变化，需根据设备属性、网络环境以及操作上下文，对访问请求进行动态授权，以确保访问控制能够实时响应需求变化，实现灵活而安全的管理.

6）最低安全态势. IIoT 中设备种类多样且需要协同工作，使得系统整体安全性存在多样化的风险. 因此，在评估来自工业控制设备的访问请求时，不仅要审查访问主体本身的安全性，还应结合设备和资源的整体安全态势进行综合评估，以确保系统全局的安全性和可靠性.

7）信息记录. IIoT 环境中的许多设备通常生命周期长，并在长期运行中可能经历多种状态变化. 因此，需要详细记录设备的状态、历史行为及环境参数等信息，以便及时发现潜在问题，从而保障设备的长期稳定性和安全性.

1.3 工业零信任综述研究现状

关于零信任的综述性研究对于外界了解零信任技术在不同领域的发展具有重要意义，如表 1 所示，本文总结了相关综述研究的贡献与局限性. 这些研究主要对零信任相关文献的基本信息进行了总结，但同样存在一些局限性. 例如，Buck 等人[7]、Syed 等人[16] 从零信任的基本概念与架构出发，结合应用行业和企业需求，以用户和社会需求为切入点，对零信任进行了总体概述，涵盖了零信任原则、零信任的基础架构及变体、身份认证和 SDP 等关键技术. 然而，由于其发布时间相对较早，某些基础架构和技术实现的更新较为有限. Dhiman 等人[17]、Sarkar 等人[18] 聚焦于基于 ZTA 的网络模型和框架，对其分类进行总结与分析，强调加密和微分段等技术在构建零信任安全网络中的重要性，但缺乏对 IoT 场景具体需求的考虑. Tsai 等人[19]、Bertino 等人[20] 和 Fernandez 等人[21] 侧重于 ZTA 的实现方式、步骤和相关条件，提出了策略制定、AI 技术结合、数据迁移及微服务等关键发展方向，详细阐述了 ZTA 发展中可能面临的挑战，但未给出具体领域的应用实例. 类似的，Kang 等人[22] 从信任的建立与认证问题入手，对零信任的理论与

Table 1 Advantages and Disadvantages of Related Zero Trust Reviews

表 1 相关零信任综述的优缺点

相关综述	主要贡献	局限性
文献 [7,16]	描述和总结零信任的基本架构及技术组成	未能涵盖近年出现的新兴技术
文献 [17−18]	总结了网络环境下零信任的发展与应用	未深入探讨物联网领域的零信任研究
文献 [19−21]	探讨了零信任技术的发展路线和未来方向	缺乏具体技术应用和实际案例的分析
文献 [22]	围绕信息安全中的信任概念概述了 ZTA	缺乏零信任具体场景和技术实现研究
文献 [5]	简要概述当前工业领域零信任的发展趋势	未对零信任技术和应用展开深入研究
文献 [23]	概述 IIoT 中零信任面对的挑战与应用特征	缺少对零信任技术的细节和实际应用的探讨

技术展开探讨, 关注隐式信任的持续怀疑, 但未涉及关键技术实现的具体方式与应用.

在工业零信任的综述研究中, Li 等人[5]结合 IIoT 发展的趋势和架构需求, 说明了 ZTA 在 IIoT 安全中的重要性, 认为 ZTA 在物联网领域具有广泛应用前景, 但缺乏对 IIoT 中 ZTA 具体实现的详细探讨. Federici 等人[23]概述了 IIoT 中 ZTA 面临的挑战, 包括缺乏标准化的基础设施和软件、计算资源的异构性、边缘设备平台开放性不足、遗留系统的复杂性以及行业法规的严格要求等, 但未进一步探讨具体的技术实现细节. 总体来看, 目前针对工业领域零信任应用的系统性综述研究仍较为稀缺. 因此, 本文通过系统梳理和总结工业零信任在不同场景下的应用及技术进展, 为研究者提供全面的理论基础和实践参考.

2 工业零信任架构

随着 IIoT 的快速发展, 传统的边界型安全模型在应对复杂的工业环境时逐渐暴露出诸多局限性. 工业零信任架构基于零信任理念, 将其转化为具体的技术实现, 通过精细化的访问控制和动态认证构建起无边界的安全防护体系. 本节首先将详细介绍概述工业 ZTA 的核心要素和基本流程, 接着探讨从传统架构向 ZTA 的迁移策略, 并总结评价该架构有效性的评估方法.

2.1 工业零信任架构概述

在工业 ZTA 中, 访问主体和客体构成了系统安全管理的核心. 访问主体指请求访问系统资源的实体, 包括工业设备、PLC、传感器、执行器、边缘设备、数据采集与监视控制系统(SCADA 系统)、人机界面(HMI)以及用户和操作人员. 客体指被访问对象, 涵盖工业数据、PLC、RTU、传感器、执行器、设备状态信息、设备操作参数、安全和事件日志、设备配置和固件、系统和网络配置等. 此外, 客体还包括系统中的各类资源和服务, 如工业控制服务、数据存储服务、远程监控资源以及相关的文档与操作手册.

如图 2 所示, 工业 ZTA 划分为控制平面与数据平面, 其核心组件包括策略执行点(policy enforcement point, PEP)和策略决策点(policy decision point, PDP). PDP 位于控制平面, 进一步被细分为策略管理点(policy administrator, PA)和策略引擎(policy engine, PE). PA 负责存储访问策略, 并建立或终止访问主体与资源之间的通信; PE 负责决定是否授予访问权限. PEP 位于数据平面, 负责执行访问主体与资源之间的连接操作.

除核心组件外, 供策略制定和 PE 进行信任评估

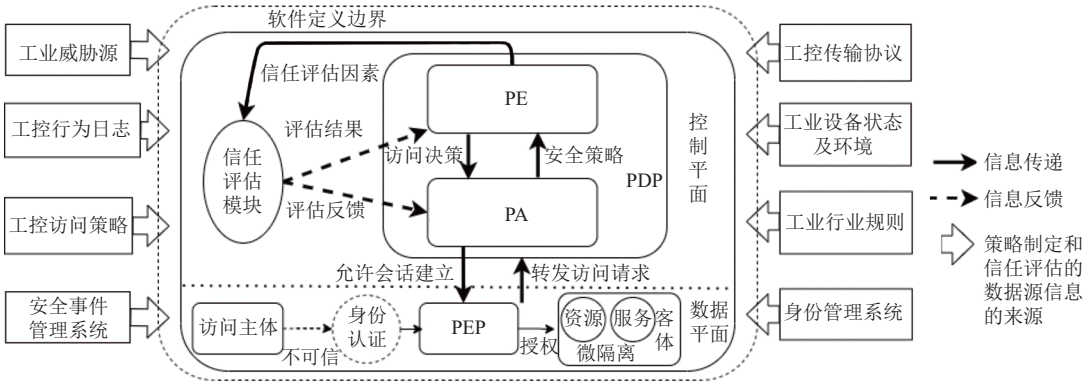


Fig. 2 Architecture diagram of industrial zero trust

图 2 工业零信任架构图

的数据源信息如下：

1)工业威胁源. 提供有关工业系统的已知漏洞及潜在威胁的信息来源，用以预测和防范未来的攻击.

2)工控传输协议. 包含工业系统中使用的各类通信协议及其安全特性的信息，用于评估这些协议在数据传输过程中的安全性及其潜在的安全风险.

3)工控行为日志. 记录工业系统中的操作和事件，分析这些日志有助于识别异常行为和潜在威胁.

4)工业设备状态及环境. 提供工业设备的运行状态和环境参数信息，通过实时监控设备健康状况，有助于及时发现异常情况.

5)工控访问策略. 围绕资源制定的访问控制策略，包括访问属性、规则和权限设置，以确保对工业数据的安全访问.

6)工业行规. 涉及工业操作中的标准和规章制度，确保系统操作符合行业规范和安全要求.

7)安全事件管理系统. 记录和管理所有安全事件，提供关于安全事件的检测、响应和解决方案的信息，提高系统的安全应对能力.

8)身份管理系统. 管理用户和设备的身份信息，确保每个访问请求的身份认证过程准确无误，防止未经授权的访问.

具体流程为访问主体最初被赋予不可信的身份，必须经身份认证后才能建立会话. 在身份认证通过后，访问主体向 PEP 发送访问请求，PEP 将请求转发至 PDP. 然后，PDP 中的 PE 根据 PA 中预设的安全策略，并结合从各数据源收集的信任信息进行评估，最终做出访问决策，最后传递给 PA. PA 依据该决策建立或拒绝访问主体与资源之间的会话，并由 PEP 执行操作.

2.2 工业零信任架构迁移

IIoT 系统通常比较复杂，立即全面替换 ZTA 可能会导致系统不稳定和业务中断[6]. 因此，在设计和实施 ZTA 时，需要结合具体的工业场景和现有设备的特点，逐步进行转型，确保系统的持续稳定运行. ZTA 的迁移主要分为以下 2 种方式.

1)从零开始的 ZTA 迁移. 该方法用于企业在完全掌握自身的运营方式和使用规则后，基于零信任原则重新设计和开发新的系统架构. Haber[8] 提出了实现 ZTA 迁移的 5 个关键步骤：识别静态和动态的敏感数据、规划数据访问路径、建立零信任微边界、进行安全监控以及采用自动化和自适应的响应机制. 这些步骤不仅有助于保护系统内部的敏感数据，还能增强其抵御外部威胁的能力.

2)基于现有架构的 ZTA 迁移. 对于现有工业系统，逐步转向 ZTA 是更常见的方法. Phiayura 等人[24] 提出了一个转向 ZTA 的 6 步法：制定零信任策略、进行背景评估、构建 ZTA、逐步迁移传统架构、持续监控与维护以及不断优化. 这种方法强调逐步替代现有的传统架构，以减少对现有系统和业务运行的影响.

此外，Collier 等人[25] 将 ZTA 应用于供应链管理，提出了一个迁移方案，涵盖了包括确定供应链参与者、识别关键资产、识别业务流程、评估风险与制定策略、选择解决方案、部署与监控等步骤. 该方案确保供应链的各个环节都在零信任的保护之下，增强供应链整体的安全性和抵御威胁的能力.

2.3 工业零信任架构评估

针对 IIoT 向 ZTA 转型的有效性，工业界仍存在一些质疑[26]，因此需要对 ZTA 的实际应用效果进行评估. 本节将概述 IIoT 的架构评估，主要分为原则性架构评估和等级式架构评估.

1)原则性架构评估. 基于零信任的条件和原则，通过构建详细的评估表来帮助管理者全面了解系统的整体成熟度. 例如，美国国防部[27] 提出了 4 个核心原则用于评估 IIoT 中的 ZTA，包括：系统协调管理与监控、假设所有请求皆为潜在威胁、假设基础设施已受损和假设对关键资源的访问存在潜在风险. 这些原则强调了从多方面确保系统的安全性和稳定性. Wang 等人[28] 进一步从成本与预算分析、数据泄露的影响等多个角度评估 ZTA 的必要性与经济可行性，以更全面地衡量其实际应用价值，帮助企业在实施过程中更好地进行资源配置和决策.

2)等级式架构评估. 通过多维度视角对系统进行成熟度评分，以帮助管理者全面评估 ZTA 各个组件的状态及其性能. 例如，Fernandez 等人[21] 通过检查不必要的冗余、安全措施的开销是否在可接受范围内等方面对 ZTA 进行了深入评估.Yeoh 等人[29] 采用了 8 个维度的加权计算，包括身份认证、端点安全、应用程序安全、数据保护、网络安全、基础设施安全、可见性与分析、自动化与编排. 这种多维度的评估方法能够更系统地反映 IIoT 中 ZTA 的整体成熟度，并为持续改进提供依据，可以更好地应对复杂的工业环境的安全需求.

3 工业零信任关键技术

本节将结合 IIoT 的特点，对工业零信任的关键

技术进行深入分析和总结，重点围绕身份认证、软件定义边界、微隔离、信道安全、信任评估等核心技术展开讨论，全面展示这些技术在工业零信任中的应用及其重要性.

3.1 身份认证

身份认证是指在用户访问资源前，对其身份的合法性进行鉴别与验证的过程[15]. 不同于其他传统场景，在 IIoT 环境中，设备常作为访问资源的主体，由于设备类型多样、使用期限长，这对身份认证的安全性、时效性和长期稳定性提出了更高的要求. 因此，IIoT 中的身份认证不仅强调多样化的身份凭据，还需要多因素的认证机制，以确保系统的安全性和稳定性. 本节将介绍当前 IIoT 中主要的零信任身份认证技术.

1)基于密码学的身份认证

基于密码学的身份认证方法因其高效性和强大的安全性，广泛应用于 ZTA 中. 例如，Xu 等人[30]、Bello 等人[31] 提出了单包授权方法，在服务端接收到访问请求的数据包后，通过验证其中的认证密钥和其他信息是否符合预设规则来决定是否授权访问，只有在验证成功后才会执行进一步的授权操作. 公钥密码体制因其简化的密钥管理和较高的安全性，成为身份认证的常用方法[5,32-35]. 其中，数字签名技术通过公钥验证后，将基于签名算法生成的随机哈希值嵌入身份凭证中，访问者解密哈希值后使用私钥进行签名，最终由服务端验证返回的签名以决定认证是否成功[5,32-33].Li 等人[5] 还引入了可追踪的通用指定验证者签名方案，在指定验证者成功验证数字签名后，继续进行密钥跟踪，以进一步提升安全性.Zanasi 等人[34]、Chen 等人[35] 对数字证书方案进行改进，将访问权限的安全元数据与证书 ID、合法标识等信息一同写入数字证书，作为身份凭证的一部分，从而增强认证的灵活性和安全性. Zaid 等人[36]、Szymanski[37] 结合新兴的量子密码体制，通过集成量子随机数生成器生成独特的随机数序列，并将其作为量子加密公钥，从而提高认证过程的保密性和抗量子攻击的能力.

2)基于用户证书和任务属性的多因子认证

多因子认证(multi-factor authentication, MFA)要求用户至少提供 2 种不同类型的凭证进行身份认证，提升系统的安全性[38-39].Daah 等人[40] 提出了将 MFA 令牌存储在区块链中的方法，只有提供经过区块链安全认证的 MFA 令牌后，用户才能进入授权阶段. Ali 等人[41]、McIntosh 等人[42] 将设备特性作为 MFA 的一部分，其中 Ali 等人[41] 提出将唯一物理特性用作边缘层设备的身份凭证.Filip 等人[43] 则利用局部敏感哈希算法生成的数据集指纹对访问数据集进行认证.

3)零信任凭证撤销方案

凭证撤销方案旨在解决令牌的有效期限问题，在零信任身份认证中，身份凭证必须具有明确的寿命期限，来确保认证行为的不可追溯性. 零信任凭证撤销方案通过管理令牌的有效期来实现这一目标. 例如，Liu 等人[44] 采用可撤销群签名方案，将过期时间嵌入边缘设备的密钥中，并且设计了一套符合零信任原则的本地身份认证与漫游身份认证协议. Rivera 等人[45] 则将 JSON 网络令牌作为加密元数据嵌入到不可替代令牌中，以实现一次性令牌的固定期限撤销，确保凭证在到期后无法继续使用.

4)基于 AI 算法的零信任身份认证

近年来，AI 技术逐渐应用于零信任的身份认证中，以提升认证的准确性和鲁棒性. 例如，Fang 等人[46] 采用基于共识的 ADMM 学习方法，实现对节点集的动态认证，提升认证的准确性. Ge 等人[47] 在哈希值认证的基础上，结合单边不完全信息的马尔可夫博弈对用户的连续动作进行建模，以增强身份认证的精确性和可靠性. 此外，Cheng 等人[48] 利用生物特征数据和循环神经网络的时间序列特征，设计了多模态联邦学习认证模型，提高了元宇宙场景下身份认证的稳定性和鲁棒性.

ZTA 中的身份认证不仅强调初次认证的准确性，更注重整个访问过程中身份的持续动态评估，以确保访问主体的可信度保持在可接受的水平. 持续身份认证作为 ZTA 的核心原则之一，通过实时的信任评估来确保访问主体在整个访问过程中始终可信. 当前的持续认证方案通常包括初始认证阶段和持续认证阶段. 表 2 对比了典型的零信任持续认证方案，并详细分析了它们各自的优势与局限性.

3.2 软件定义边界

软件定义边界(SDP)是一种通过隐藏基础设施来部署逻辑边界，将服务与不安全网络隔离的安全模型[55]. 其“未授权用户无法访问任何位置的资源”这一安全理念，与零信任中“授权和信任不依赖于网络位置”的核心原则高度契合. 因此，NIST 将 SDP 方法列为实现 ZTA 的关键技术之一[6]. 相较于其他场景，IIoT 对设备的分布式管理需求更为复杂，涉及许多关键基础设施，因此在工业零信任中应用 SDP 技术时，对分布式管理与系统稳定性要求更高. 本节将概述并对比 SDP 在零信任中的应用方式.

Table 2 Comparison of Continuous Authentication Solutions

表 2 持续认证方案对比

特点	初始阶段	持续认证阶段	优点	缺点
固定时间间隔认证[49-50]	静态密码体制认证	利用 XOR，Hash 等轻量级操作，每隔固定时间间隔认证	管理简单、可用性高	安全性低、漏报率高
异常行为认证[51-52]	Oauth2.0 等认证协议	持续监控，检测到异常行为时启用协议认证	及时性强、准确度高	追溯性差
动态方案实时认证[53-54]	设备指纹相互认证	利用密钥刷新机制或基于评价值等动态方案实时认证	及时性强、追溯性强、准确度高	成本高、兼容性差

在 SDP 的架构中，通常包括以下 3 个主要组件，以实现零信任环境下的安全访问控制：

1）控制器. 负责对客户端进行身份认证和授权，确保只有经过验证的客户端才能访问资源.

2）网关. 用于隐藏资源，防止未授权的访问行为，从而提供安全的访问控制.

3）客户端. 充当访问主体向系统提出访问请求.

控制器在接收到客户端的访问请求后，会对其身份进行认证与授权，只有经过认证的请求才能被转发至网关以获取相应的资源.SDP 可以根据不同的应用场景被划分为 4 种主要模型：客户端-网关模型、客户端-服务器模型、客户端-网关-客户端模型以及服务器-服务器模型，如图 3 所示.

1）客户端-网关模型

在该模型中，网关充当 PEP，部署在资源的隔离区域内. 该模式适用于陈旧数据库系统或基于云的解决方案，通过网关将数据资源隐藏在隔离区域内，只有经过认证授权后的用户才能建立与资源的连接. 例如，Alagappan 等人[32]、Chen 等人[56] 针对数字资源功能单一的问题，引入访问代理充当网关，客户端在经认证授权后，通过访问代理获取资源. Moubayed 等人[57] 处理网络中的数据配置更新问题，将网关作为 PEP 部署于服务器前，执行动态的资源更新任务. 该模式也广泛应用于云平台服务中，通过将资源隐藏在网关之后，以减少攻击面. 例如，Li 等人[38] 提出将网关作为唯一入口，基于信任评估的结果管理客户端对云平台数据的访问.

2）客户端-服务器模型

在该模型中，网关作为资源代理，部署在资源前，以建立客户端与资源之间的安全通道. 该模型广泛应用于网络层的 ZTA，例如，Sedjelmaci 等人[58] 将网关安装在 6G 网络的特定节点中，通过网关与资源间的端到端连接，提高了 ZTA 在 6G 环境下对已知攻击和零日攻击的检测精度. Shen[51] 将网关部署在资源

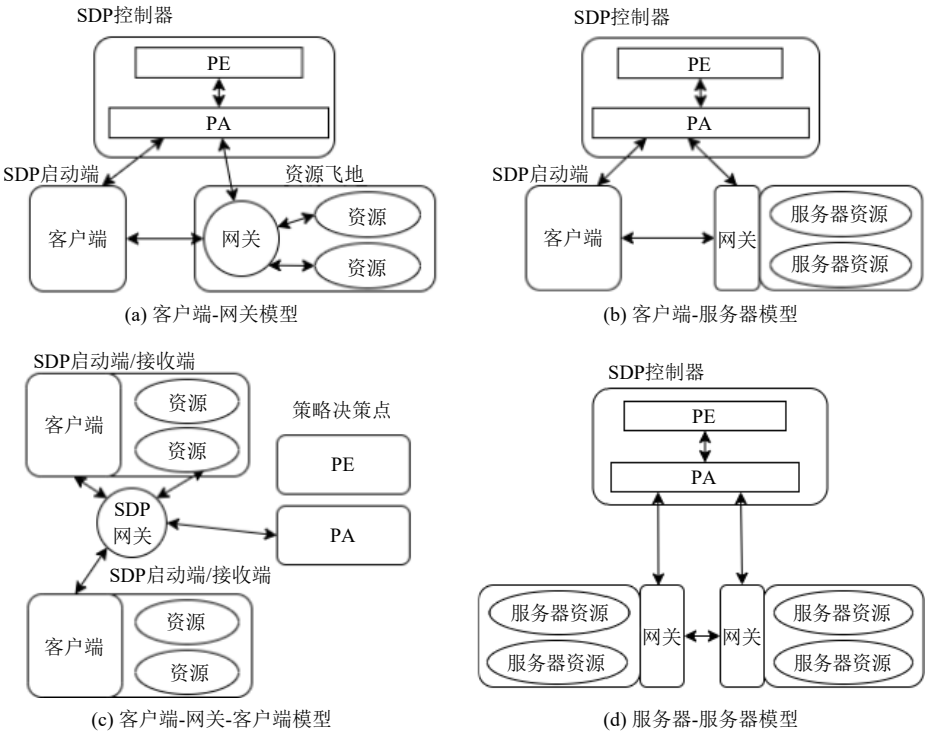


Fig. 3 Four SDP framework models

图 3 4 种 SDP 框架模型

服务器前, 充当 PEP, 依据控制器的信任评估决定是否开放访问通道, 从而有效缩短访问延迟时间. 此外, 该模型也应用于非 IP 网络中, 例如, Bradatsch 等人[59]、Huang 等人[60]将网关作为 PEP 安装于智能设备中, 通过每个网关对应一个智能设备的方式, 解决了物联网设备异构性带来的访问管理问题.

3)客户端-网关-客户端模型

在该模型中, 客户端可以作为启动端、接收端或二者皆是, SDP 网关用于连接多个客户端, 实现点对点通信. 这种模型通常用于设备间的数据交换安全性管理. 例如, Wang 等人[61]针对网络数据中 PKI/CA 存在的不可信问题, 将代理服务与控制器结合, 作为网关组件, 然后通过网关对 PKI/CA 进行信任评估, 以确保客户端之间数据交换的安全性. Ali 等人[41]、Zanasi 等人[62]提出, 针对边缘设备间的互联问题, 将边缘服务器作为任务卸载的主体, 经过网关的认证与授权后, 访问请求被卸载到相应的边缘服务器, 从而实现边缘设备间的高效互联. 该模型在 IIoT 设备的互联场景中被广泛采用.

4)服务器-服务器模型

在该模型中, 网关部署在服务器前, 用于在面对未经授权的连接时隐藏所有资源, 确保系统的整体安全性. 该模型适用于 IIoT 和虚拟机环境. 例如, Federici 等人[23]、Anderson 等人[49]针对 IIoT 设备对快速响应的需求, 将网关集成到具体设备中, 以提高 ZTA 的响应速度. Lei 等人[63]为提高 IIoT 设备之间的通信稳定性, 在网关中添加信道控制器, 提升了设备间的通信安全性和可靠性.

3.3 微隔离

微隔离是一种将数据中心基础设施划分为更小的逻辑域, 并对端口流量进行细粒度控制的方法[15]. 在 ZTA 中, 微隔离用于控制网络内部(即东西方向)的流量, 以防止攻击在网络内部的横向扩散, 有效减小攻击面, 提升系统的整体安全性. 相较于其他场景, IIoT 场景包含更为复杂的关键基础设施和高度互联的设备网络, 内部流量的横向传播风险更高. 因此, IIoT 中的微隔离不仅需要更高的精细度来管理设备间的复杂交互, 还需具备更强的安全性和可扩展性, 以适应不断变化的工业环境. 本节将概述在 IIoT 中应用微隔离的主要实施方案.

1)基于网络的微分段

该方案是微隔离最常用的方案之一, 根据具体功能将网络划分为不同的网段来实现. 在应对跨网段攻击时, 这种方法能够有效保障各个分段内资源的完整性. 例如, Daah 等人[40]、Wu 等人[64]根据不同的信任级别与安全需求, 将网络划分为具有不同信任等级的网段, 并对不同等级的网段制定相应的安全策略进行渗透拦截.Konduru 等人[65]提出使用 SD-KP(一种用于节点安全分组的算法), 根据安全策略、节点之间的距离和节点状态对网络节点进行分组与隔离. 然而, 单个网络微分段通常缺乏足够的计算资源来有效应对复杂的网络攻击, 因此需要网关安全组件提供额外保护. 为此, 可以采用智能交换机、路由器、下一代防火墙或专用网关设备来增强网络微分段的安全性[6]. 企业中还通常通过部署软件代理或防火墙实现这一方案[36].

2)基于本地设施的微分段

该方案通过将本地基础设施划分为微节点, 并部署相应的访问策略, 以实现更加精细的安全控制, 并且不需要引入额外的外部硬件. 例如, Alagappan 等人[32]对发电厂的每个设备进行了功能性隔离, 通过信任推断、数据源检测和策略应用, 有效地防范了恶意攻击在系统中的横向扩散. Gai 等人[39]结合区块链技术, 将资源信息分布在联盟链节点中, 并利用实用拜占庭容错算法严格控制设施节点的安全性, 确保了节点间通信的完整性和可靠性.

基于网络和基于本地设施的微隔离方案均存在局限性. 基于网络的微分段在功能可视性方面较为薄弱, 难以全面监控网络内部的各类活动; 基于本地设施的微分段在兼容性上面临挑战, 尤其是在传统系统和新兴技术的集成方面. 因此, 改进微隔离的实施方案是当前研究的热点之一. 例如, Hong 等人[66]引入大量可编程 API, 使管理员能够通过这些编程接口来构建和管理微服务的流规则, 提高微隔离的灵活性和扩展性. Zhang 等人[67]对 NIST 的沙箱模型进行改进, 提出基于访问行为的混合隔离模型(AB-HIM), 通过动态信任等级和 AB-HIM 标签强化沙箱间的信息流隔离, 提升系统的安全性和管理灵活性.

3.4 信道安全

信道安全是指零信任系统在数据传输或处理过程中, 通过信道加密等技术手段保护数据的机密性和完整性, 以防止信息泄露或篡改[15]. 与传统物联网场景相比, IIoT 场景对时间延迟高度敏感, 并且涉及大量私有工业通信协议, 这使得信道安全技术不仅需要保障数据安全, 还必须满足高实时性的要求. 本节将介绍 IIoT 中用于保护零信任数据交换和传输安全的信道加密方法.

网络数据加密协议在零信任数据加密中应用广

泛，具有较高的成熟度和良好的兼容性. 例如，SSL 协议作为常用的加密协议，往往通过结合其他算法用于保护数据交换安全. Li 等人[38] 提出一种基于 SM2, SM3, SM4 算法的双向 SSL 协议，用于对交换数据进行加密，以保证通信的安全性和可靠性. Buck 等人[7]、Anderson 等人[49] 使用 TLS 协议对数据链路进行单向加密，确保数据在传输过程中的保密性. mTLS 是对 TLS 的拓展，通过双向认证提升了通信的安全性，广泛应用于 ZTA 中的组件间通信加密[56]. 例如，在数据链路中应用 mTLS 协议，不仅对访问方进行认证，还对资源方进行认证，以确保数据的安全传输[68-69].

在 IIoT 的具体场景中，许多零信任数据加密方案需要在传统加密方案的基础上进行改进，以适应工业环境的特殊需求. 例如，Filip 等人[43] 提出一种基于鲁棒水印的半结构化加密方案，通过为同一数据集设计不同的水印，确保数据集在分发过程中的安全性和完整性. Ahmed 等人[70] 选择带有关联数据的认证加密算法，用于半导体节点间的数据交换，提高数据传输的保密性和抗篡改能力. Shah 等人[53] 创建了随时间变化的轻量级可调线性或非线性函数，用于保护 IIoT 通信路径免受协议攻击. Tsai[71] 提出一种基于一次性密码本的加密流程，提高数据传输的安全性.

3.5 信任评估

信任评估是指对访问实体的信任程度进行评估的过程，是策略引擎的核心组成部分，也是 ZTA 的基石. 由于 IIoT 具有设备类型多样性、高实时性和高准确性的需求，ZTA 中的信任评估展现出综合因素评估、集成边缘计算和行为序列结合等特点.

信任评估的关键在于算法输入的数据源，这些数据源通常包括：访问请求、访问主体数据库、虚拟资产数据库、访问资源要求和威胁情报等. 信任评估算法根据这些数据赋予不同的权重值并进行最终计算. 其中，信任评估的计算方法和实现方式极其多样，不同的 ZTA 会根据感知的重要性对上述数据进行权衡与取舍. 根据评估方式和最终结果，将信任评估分为基于分值的信任评估和基于条件的信任评估；根据时间序列行为的关联性，分为独立的信任评估和基于上下文的信任评估.

1）基于条件的信任评估

在该方案中，访问主体需满足一组由策略管理员根据资源特点配置的属性条件，只有满足所有条件的主体才能获得访问权限. 这种评估方式通常是二元的，即允许访问或拒绝访问，缺乏动态适应性. 例如，Shen[51]、Csikor 等人[69] 通过检测终端设备的网络接入属性（如域名权限）来评估设备是否能够接入零信任网络. Gai 等人[39]、Wang 等人[72] 依据预设的属性条件，对跨组织数据共享的参与方进行评估，并根据符合条件的程度决定是否授予其访问权限.

2）基于分值的信任评估

该方案通过为每个数据源分配权重来计算信任等级或信任分值. 当信任分值或信任等级高于资源设定的阈值时，授予权限；否则，拒绝或降低其访问权限. 该方法通常需先设立一个动态的分值或等级标志，但信任分值的计算过程复杂且资源消耗较大. Ameer 等人[73] 和 Park 等人[74] 认为基于信任分值的评估应成为主流. 信任评估的难点在于信任等级或信任分值的算法设计，例如，Wang 等人[75] 使用模糊层次分析法结合多维度信息来计算信任分值. Zanasi 等人[62] 和 Wang 等人[76] 通过综合评估访问主体的信息及其应用场景设定信任阈值.

3）独立的信任评估

该方案对每次访问请求单独处理，不考虑历史行为与主体之间的关联，评估速度快. 但当攻击者的行为仍处于允许的角色范围内时，恶意活动难以被检测到. 例如，Al 等人[77] 通过联盟区块链实时收集设备的信任因子，提交至边缘服务器以提取异常与敏感因子来提升设备状态感知. Fu 等人[78] 将卫星的多维度信息作为信任评估的关键因素，并采用独立评估机制，即该过程不依赖其他互联设备的数据交换. 这种方法能够减少外部干扰，避免因数据共享或设备依赖性而带来的安全风险，从而提高信任评估的独立性与准确性.

4）基于上下文的信任评估

该方案在评估访问请求时，将访问主体的历史行为及其相关联系作为关键因素. PE 通过对主体状态信息进行分析，提高评估的准确度，但计算资源和时间开销较大. 例如，PE 会对访问主体的历史行为进行记录，并结合威胁情报和多维度的信息进行信任评估，更准确地做出授权决策[39,49,62]. 此外，基于上下文的信任评估还重视访问实体之间的关系，例如，Ge 等人[47] 和 Wang 等人[79] 采用博弈论思想，让 2 个访问主体相互评估与态势监控，确保信任评估达到动态平衡. N’goran 等人[80] 将这一思想应用在社区云环境，通过安全域内受信组织之间的直接交互，对声誉值进行评估.

上述 4 种信任评估方式并不是互相排斥的. 独立或基于上下文的信任评估可以与基于条件或分值的评估方式结合使用，以增强整体评估的准确性和适

应性. 随着 AI 技术的发展, AI 在信任评估中的应用正逐渐成为重要方向, 以提高评估的智能化和可靠性. 表 3 中展示了 5 种 AI 技术在 ZTA 信任评估中的应用. 通过使用联邦学习、强化学习、深度学习、监督学习和无监督学习等方法, 提升信任评估的准确性和动态适应性. 联邦学习和强化学习在综合各组织数据的独立性和历史行为的动态反馈方面具有显著优势. 监督学习和深度学习通过优化计算方式和行为模式识别, 增强了信任评估的精确度和自适应能力. 这些 AI 技术的应用不仅提升了系统的安全性, 也为应对 IIoT 环境中多样化和复杂的安全需求提供了强有力的支持.

Table 3 Application of AI Technologies in Trust Evaluation

表 3 AI 技术在信任评估的应用

信任评估的 AI 技术	应用方式
联邦学习[77,81]	零信任中央协调器从各组织独立的联邦学习模型中收集信任属性并统一进行信任评估
强化学习[48,82]	将历史的决策结果和主体行为作为关键因素参与；信任参数的计算与评估方法的更新
深度学习[64,83]	结合神经网络等技术，以行为分析与模式识别为基础，对信任参数进行自适应更新
监督学习[78,84]	利用标记数据训练模型，学习输入与输出间的关系，逐步提高信任参数的预测精度，并优化信任评估机制
无监督学习[85-86]	完全依赖未标记的数据，通过分析数据中的内在结构和模式进行信任参数的更新

4 工业零信任的访问控制

访问控制是一种机制, 用于确保系统资源的访问仅限于被授权的主体(包括经过身份认证的用户或代表用户的进程), 并阻止所有未经授权的访问请求[87]. 访问控制的核心目的是保护设备、数据等资源的可用性和安全性. 基本流程包括主体向访问控制系统进行自我识别, 并使用密码、令牌或指纹等认证凭据进行身份认证, 身份认证的结果决定了主体是否可以访问相应资源[88].

在工业 ZTA 中, 访问控制被视为实现零信任理念的关键机制之一. 通过对访问权限的精细化分配和实时管理, 最大限度减少信任边界的暴露, 防止未经授权的主体获得过度的访问权限, 增强系统的整体安全性. 访问控制的动态特性能够根据工业场景的安全需求灵活调整策略, 使其在工业零信任环境中显得尤为重要. 本文将从访问控制的发展历程出发, 深入探讨其在工业零信任中的应用与演进.

4.1 访问控制模型的早期发展

1969 年, Lampson[89] 通过访问控制矩阵的形式对访问控制问题进行了抽象化. 由于矩阵形式过于庞大, 后续提出了以文件为中心和以用户为中心的访问控制列表来简化访问控制矩阵的使用. 随后, 基于主体身份和授权来决定访问模式的自主访问控制模型被提出, 以用于多用户数据的保护[90]. 虽然其具有较高的灵活性, 但在安全性方面存在不足. 为了实现更为严格的访问控制策略, 根据主客体的安全级别标记来决定访问模式的强制访问控制模型被提出, 该模型注重保密性但缺乏灵活性[91]. 此外, 基于任务的访问控制、基于组的访问控制、基于场所的访问控制、基于规则的访问控制、风险自适应访问控制等多种访问控制模型相继被提出, 以解决特定的访问控制需求[92-96].

4.2 基于角色的访问控制模型

基于角色的访问控制(role based access control, RBAC)通过访问主体在组织中的角色来决定其访问权限, 角色的访问权限在角色定义阶段预先设定[97]. 访问主体尝试访问资源时, RBAC 机制将主体的角色与规则进行匹配, 以确定是否允许此访问请求. 根据模型的复杂程度, RBAC 可分为 4 类[98]: 1)基本的 RBAC, 由用户、角色、会话、权限 4 个要素组成, 表达了支持 RBAC 系统的最小需求; 2)具有角色层次的 RBAC, 引入了角色继承的概念; 3)具有约束的 RBAC, 在基本 RBAC 的基础上增加了约束; 4)统一角色层次和约束的 RBAC, 综合了角色继承和约束, 为角色间和角色与权限之间提供了更灵活的限制.

RBAC 在 ZTA 中扮演着重要角色, 通过基于角色的权限管理机制简化对资源的访问控制.RBAC 允许根据主体在组织中的角色来定义和分配权限, 减少了对每个主体单独设定权限的繁琐过程, 降低管理复杂性. 在 IIoT 环境中, 由于设备数量众多且类型复杂, RBAC 提供了一种可扩展的权限管理方式. 虽然 RBAC 提高了管理效率, 但其静态的角色分配方式无法完全应对动态变化的安全需求, 因此在复杂的工业环境中需要与其他访问控制机制结合使用, 以实现更高的灵活性和安全性[99]. 例如, Shin 等人[100] 将 DDS 协议(一种数据分发服务协议)与 RBAC 相结

合，利用 DDS 协议的高效发布/订阅通信机制以及 RBAC 的角色分配和权限管理功能，实现支持不同协议的设备之间的数据交互，减少未经授权的访问和提高资源利用率. Zaidi 等人[101]将区块链技术与 RBAC 结合，引入角色管理系统并采用共识机制确定访问权限，以便根据预定义规则解决冲突，提高系统安全性的同时减少并发请求的响应时间. Xu 等人[102]利用 RBAC 模型实现用户与多个设备之间的安全认证，通过访问控制列表限制用户操作权限，并引入秘密共享机制以便于密钥形成，避免敏感数据泄露并减少重复认证的时间成本.

RBAC 的角色继承和灵活的权限管理机制使其成为工业 ZTA 实现中不可或缺的一部分. 通过在不同层级间实现权限的继承和限制，RBAC 能够动态调整访问权限，确保权限最小化的同时保持业务的灵活性和高效性.

4.3 基于属性的访问控制模型

基于属性的访问控制(attribute based access control, ABAC)通过评估访问主体、访问客体、环境条件和资源属性来判断是否允许主体对客体进行操作[103]. 当主体发出访问请求时，ABAC 机制会综合评估主体、客体、环境和操作属性，以确定是否授权访问[104]. 根据属性特征，ABAC 可以进一步划分为基于用户属性的 ABAC、基于资源属性的 ABAC、基于环境属性的 ABAC、基于操作属性的 ABAC，以及结合多个属性的组合 ABAC.

ABAC 在 IIoT 场景中被广泛应用，来实现细粒度的访问控制[105]. 在工业 ZTA 中，ABAC 通过对访问主体的多重属性进行评估，提供灵活的访问策略管理. 这使得 ABAC 能够根据不同设备和用户的属性调整权限，适应复杂多变的工业环境. 尽管 ABAC 在灵活性上具有优势，但处理大量动态属性时，面临较高的计算成本和管理复杂度.

ABAC 在工业 ZTA 中的重要性主要体现在其支持细粒度访问控制的能力，能够减少对静态权限配置的依赖，提升系统在动态环境中的适应性. 例如，Cremonezi 等人[106]提出一种基于 ABAC 的属性缓存优化方法，通过将属性存储在更靠近访问请求的位置以降低时间成本，应对大规模物联网场景中的属性管理挑战. Alshehri 等人[107]结合区块链技术和 ABAC 模型，通过模糊逻辑方法生成访问控制策略，以减少决策延迟和存储开销. Pathak 等人[108]在边缘物联网场景下应用 ABAC，通过属性智能合约和访问机制智能合约评估访问请求，减少时间延迟并提升资源利用率.

虽然 ABAC 能够提供高度灵活的访问控制，但其在 IIoT 中的应用也伴随着高计算负担和复杂的属性管理. 因此，在实际应用中需要平衡 ABAC 的灵活性与其实现的复杂性，确保其在工业零信任环境中能够高效、安全地运作. ABAC 在工业环境下，具有动态权限调整和细粒度访问控制的优势，使其能够更好地满足安全性与业务效率的双重需求.

4.4 工业 ZTA 的动态访问控制模型

IIoT 的复杂网络环境使得传统依赖静态规则的访问控制模型难以应对这些场景的灵活性需求[109]. 为应对不断增加的安全威胁，动态访问控制在 IIoT 中的 ZTA 被广泛应用，其根据上下文信息(如时间、地点、设备状态等)实时调整访问权限，从而提供更灵活和更安全的访问策略[110].

在 IIoT 场景下，访问主体与客体之间属性差异显著，并伴随数据泄露风险，因此工业 ZTA 的动态访问控制通常需要结合加密技术来加强安全性. 例如，Salehi 等人[111]结合了传统 ABAC 和基于属性的加密技术，将用户属性与跨设备环境中的访问控制结构结合，使用户可以避免依赖第三方进行数据访问. Huang 等人[60]用 AES-256 和隐藏属性的 CP-ABE 等加密算法进行数据加密，数据所有者通过隐藏部分的访问策略，使访问者在不了解完整访问策略的情况下仍能认证访问属性，保证敏感数据的机密性.

IIoT 场景中复杂的环境条件和资源属性使得传统静态访问控制机制难以快速适应变化. 因此，工业 ZTA 的动态访问控制通常需要根据时间或操作序列的变化灵活调整策略. 例如，García-Teodoro 等人[82]使用动态监管程序监测安全配置文件，并结合环境因素决定允许、限制或拒绝访问请求，动态掌握设备状态并及时调整策略. Wang 等人[75]引入信任分值来量化用户可信度，通过属性信息和信任分值精确控制用户行为及环境属性的变化，实现行为监测和策略调整.

此外，IIoT 场景中的设备异构性极高，不同设备之间的属性和计算资源差异巨大，这对访问控制机制的兼容性提出了很高的要求. 工业 ZTA 的动态访问控制常采用多层授权架构应对此类挑战. 例如，Federici 等人[23]使用 2 层访问控制架构，利用 2 阶段授权模式和覆盖边缘域保护为遗留和专有设备提供安全支持，在简化访问控制策略管理的同时兼容遗留设备. Zhang 等人[112]设计并实现一个 3 层访问控制框架，可以对不同设备的实时数据和历史数据进行

认证，并允许用户通过 API 开发相应的访问控制模型，提高 ZTA 的扩展性以适应异构设备.

总的来说，工业 ZTA 中的动态访问控制机制通过结合上下文信息、动态调整访问权限，以及应用多层授权架构，有效应对 IIoT 环境的复杂性和安全性挑战. 这些机制不仅提升了系统的灵活性，还增强了各类工业设备之间的兼容性和整体安全性，从而实现更加全面且可靠的访问控制，为应对日益复杂的 IIoT 环境提供重要支持.

5 工业零信任在典型场景中的应用

本文选取 ICS、EIoT、IoV、SIoT 和半导体行业作为工业零信任应用的研究对象. 这些场景具有高度的代表性和重要性，涵盖了工业自动化、关键基础设施、动态网络环境以及高密度信息处理，对系统的安全性和实时性要求较高. 通过研究这些典型场景，可以全面评估和认证 ZTA 在 IIoT 中的有效性和适用性，确保系统的安全运行和高效管理.

ICS 涉及复杂的控制逻辑和实时数据处理，EIoT 强调电力系统的稳定性和连续性，IoV 注重动态网络连接和移动性，SIoT 需要处理低时延和高并发的数据传输，半导体行业强调知识产权保护和内部安全. 这些场景的特点和差异，使它们成为研究和验证 ZTA 在工业领域应用的理想对象.

5.1 零信任在 ICS 中的应用

ICS 是工业自动化的重要组成部分，负责管理和控制各种工业设备和过程. 由于其在关键基础设施中的重要性，ICS 的安全性成为 IIoT 领域的重点研究方向. 零信任在 ICS 中的应用，旨在解决传统安全架构难以应对的复杂性和多样化威胁，确保系统的整体安全. 下面将详细介绍零信任在 ICS 场景中的应用及其实现方式.

ICS 中的设备种类繁多，不同设备之间支持的数据交换协议各异，这导致了数据交换的复杂性. 同时，设备的计算资源也存在显著差异，这可能影响 PDP 的决策速度. 针对这一问题，ICS 中的零信任系统通过数据转发设备完成不同设备之间的通信. 例如，Ali 等人[41] 针对 ICS 中大量边缘节点数据传输协议不同的问题，提出一种任务卸载的 ZTA.通过零信任编排器对访问节点进行集中式持续认证与评估，然后将任务从编排器卸载到对应的边缘服务器，使支持不同数据交换协议的边缘服务器之间可以实现高效的数据交互. Li 等人[38] 基于区块链技术实现了不同协议设备之间的轻量级数据共享，利用多重签名协议和智能合约的跨组织 RBAC 机制搭建零信任环境，并通过决策合约对支持不同通信协议的设备之间的数据交互进行协调与管理.

ICS 设备通常面临计算资源匮乏的问题，可能无法独立完成信任评估或访问决策等复杂计算任务，并且设备之间的计算资源可能分布不均. 因此，ICS 中的零信任系统需要完善的任务分配机制. Ali 等人[41] 提出利用联邦学习模型集中边缘节点的计算资源进行零信任规则训练的方案，每个节点基于本地数据获得相应模型梯度，最终通过汇聚各节点的梯度训练整体的工控零信任模型. Cheng 等人[48] 基于联邦学习优化了 ZTA 的任务分配体系，使得所有设备在决策模型训练中能够获得合理的参与位置，从而提升了异构节点的兼容性.

此外，ICS 设备之间的数据链路往往缺乏安全协议保护，特别是在无线信道中. 因此，零信任模型需要确保工控设备之间数据传输的安全，并根据具体应用场景开发适当的信道安全协议. 例如，Zanasi 等人[62] 提出一种以身份为中心的授权机制，基于对风险级别和环境的持续评估，将用户信息、设备身份、健康状况、运行状态、风险态势感知状态和上下文信息作为数据链路安全的判别条件. Lei 等人[63] 开发一种增强 IIoT 的 ZTA，通过人工噪声预编码形成安全区域，对生成的波束进行轻量级加密，作为安全隧道，提升无线信道下的抗干扰能力.

ICS 对决策速度和信息延迟要求严格. 为满足这一需求，Singh 等人[113] 设计了一种基于压缩密钥方法的 ZTA，通过 Streebog 加密压缩算法替换排列网络模型来对工控设备的密钥进行压缩，缩短了决策的反应时间. Kobayashi[114] 将 PDP 和 PEP 分开工作，将基本访问原则以 PDP 子集的形式进行压缩，提高单个端点的访问决策速度.

5.2 零信任在 EIoT 中的应用

EIoT 中的设备分布广泛，需要处理来自不同用户节点的大规模电力数据，这对决策速度、数据处理能力以及信息隐私提出了巨大挑战[115]. 随着越来越多的智能设备接入电网，电力系统正面临设备多样化、数据流复杂化、能源供应效率低下，以及安全性和连续性方面等问题[32]. 传统的网络安全架构已经无法有效应对这些问题，ZTA 通过其独特的安全策略，为 EIoT 提供了新的解决方案.

在 EIoT 中，零信任系统通过分布式架构来平衡计算资源，同时单独保护敏感数据，确保数据安全和

系统稳定运行. 例如, Alagappan 等人[32]提出一种针对小型发电机构成的分布式零信任 EIoT 架构, 将每个发电机都作为独立的数据存储与处理设备, 设备间通过数据与故障的隔离来有效解决数据冗余和服务整合问题. Al 等人[77]在设备周围部署了分布式零信任引擎, 将监控与认证功能下沉至边缘设备, 减轻了边缘服务器的负载, 有效解决了电网内部的点对点故障和拒绝服务攻击等问题.

在 EIoT 环境中, 大量串行工作的生产设备面临着长时间停产的风险. 尽管通过微分段可以在一定程度上隔离设备, 但内联设备的停产仍可能影响整体的安全性和连续性. 因此, 零信任系统不仅需要对电力设备进行隔离, 还必须具备持续监控与主动干预能力, 而非单纯地停止设备运行. 例如, 当电网系统在非正常时间段检测到攻击行为时, 会对受攻击设备进行详细的流量和时间戳分析, 将其标记为疑似受攻击设备[32]. Huang 等人[60]设立持续感知分析中心, 收集并分析电网设备的多维信息, 作为信任评估的基础, 实时掌握设备的运行状态, 并调整安全策略, 避免因攻击或设备受损导致大规模停运.

为增强对充电终端设备的安全性, Li 等人[38]提出一种动态信任评估机制, 来解决充电终端网络设备间不安全的数据通信问题, 并防止恶意固件攻击. 该系统根据设备的稳定度、亲密度和异常程度等指标, 对充电设备的状态进行实时评估, 从而能够快速检测并响应受损设备的情况, 确保电网的安全性和可靠性.

5.3 零信任在 IoV 中的应用

随着自动驾驶技术的不断成熟和车载智能化程度的提升, IoV 逐渐成为现代移动出行物联网的重要组成部分. IoV 的智能终端对系统响应时间和效率要求极高, 需要精准的状态切换和对复杂环境的感知. 因此, 零信任模型在 IoV 中的应用不仅限于传统的身份认证, 更关注车辆间的实时认证与动态状态切换. 本节将从 IoV 面临的常见问题出发, 探讨零信任在该领域的应用及其实现方式.

在 IoV 场景中, 车辆、路边基础设施等设备之间的信息传递和认证非常频繁, 传统的集中式身份认证方式难以保证认证的准确性和数据的安全性. 因此, IoV 中的零信任模型通过设备间的相互认证和加密信息传输, 确保数据安全和认证的高效性. 例如, Anderson 等人[49]提出一种利用边缘节点对车辆信息进行采集并通过加密信息流来保障数据传递安全的方法. 在信息流的持续过程中, 上下文管理器和 PDP 对车辆进行持续的身份认证, 确保车辆在运动状态下的认证准确性. Hao 等人[116]利用车路协同的技术框架, 通过车载设备与道路基础设施的双向信息交互, 实现动态身份认证. 将路侧基础设施收集的路况信息作为标准, 与车载设备上传的数据进行对比, 完成身份认证. 然后将认证信息和隐私数据上传至区块链, 实现分布式存储和隐私保护, 防止信息泄露. Fang 等人[46]开发了一种基于边缘信息协作认证的零信任模型, 通过多个边缘节点收集信号强度、到达时间和到达时间差等信息来协作认证车辆, 路边基础设施有效认证附近车辆的消息并将认证结果广播给车辆, 减少不必要的冗余认证.

在现代出行场景中, 车辆需在复杂路况和动态交通环境下快速进行态势感知和状态切换. 但由于计算开销较大, 难以满足高动态环境对实时决策的需求. 为应对这些挑战, IoV 中的零信任系统通过引入边缘智能和无缝切换方案, 来实现快速决策. 例如, Fang 等人[46]提出一种基于去中心化边缘协作的无缝切换认证方案, 通过多维信息融合和信誉评估, 将安全保障从网络中心移至边缘节点, 实现多个认证节点之间的协作. Wang 等人[75]在边缘节点收集了车辆主体信息、计算资源以及环境信息, 综合这些信息进行状态切换决策, 实现更为灵活的车辆状态管理. Zhang 等人[112]通过上下文监控组件对系统事件序列进行记录, 提高相似状态下的决策速度, 并在不同维度的数据源之间捕获访问行为, 从而提供高效的动作控制服务, 减少信息收集和处理的时间.

5.4 零信任在 SIoT 中的应用

SIoT 是物联网的重要组成部分, 应用于各类卫星通信和监测系统中. SIoT 在许多关键场景下, 要求低时延和高并发的数据传输, 这对系统的安全性和稳定性提出了严峻挑战[78]. 随着卫星通信需求的不断增长, 如何确保数据的安全交互和高效管理成为亟待解决的问题. 零信任通过持续认证和动态信任评估, 有效应对 SIoT 的复杂安全需求. 本节将深入探讨 ZTA 在卫星系统中的具体应用.

SIoT 系统的独特环境对认证速度和准确性提出了极高要求, 传统的认证方法难以满足这些需求. 为此, ZTA 被引入以解决 SIoT 的复杂安全问题, 通过持续切换认证来缩短认证时间, 并保证多并发任务下的认证准确性. 例如, Cui 等人[117]提出一种分阶段的零信任切换认证方法, SIoT 设备首先通过用户设备注册进行初步认证, 获得数据交互授权, 然后在切换认证阶段决定最终交互状态. 这种方法缩短了认

证的前置时间成本,提高了整体认证效率. Tian 等人[118]设计了一个零信任双向安全认证协议,认证代理通过响应激励机制和模糊提取器生成认证密钥,用于下次认证,缩短信息收集时间,提高了认证的准确性和效率.

此外,由于 SIoT 中不同设备间支持的通信协议与交互的数据类型可能存在巨大差异,致使通信过程的数据交互往往缓慢而危险[119]. 为应对这一安全隐患,SIoT 零信任系统通常采用分布式边缘架构. 例如,Falco 等人[120]开发了一种完全分布式的卫星零信任系统,设备节点通过共同参与信誉共识的判定,有异常行为的节点会逐步被阻止发送访问请求及参与共识,有效规避由设备异构性导致的数据交互风险. Cui 等人[117]进一步提出在网络侧监控设备间的数据交互并执行适当的控制策略,边缘服务器在记录设备历史行为的同时向核心网络推荐间接信任值. 这种基于同类设备的间接信任值增强了零信任系统对设备状态的感知能力,有效检测和防范不同类型卫星设备的内部攻击行为.

5.5 零信任在半导体行业中的应用

半导体行业作为全球科技发展的基石,面临着知识产权保护和机密设计防泄露等严峻的安全挑战. 在全球化和快速发展背景下,如何保护半导体设计的安全已成为亟待解决的问题.ZTA 通过多层次的身份认证和访问控制,为半导体行业提供了一种全新的安全防护手段,帮助企业应对硬件木马注入和知识产权盗窃等复杂威胁.

半导体的集成电路在知识产权保护和设计机密性方面容易受到硬件木马注入等攻击[121]. 为应对这些复杂的安全威胁,零信任系统往往通过 IP 加密等方式保护集成电路(integrated circuit, IC)中的设计版权. 例如,Stern 等人[122]提出一种综合了加密、逻辑锁定、临时逻辑元素插入、访问控制和操作日志记录的 ZTA,其根据 IP 的价值来决定加密或逻辑锁定的复杂程度,以防止设计 IP 在制造过程中的泄露和滥用. Buras 等人[123]将零信任技术与 ACS edge 系统(一种用于在测试期间托管工作负载的计算设备)结合,利用用户的私有密钥和第三方证书签发机构对设备间进行认证,实现高级别的设备隔离和信任,满足了对复杂计算环境的需求.

此外,随着 IC 设计复杂性的增加以及节点尺寸的缩小,芯片间信息传递的准确性和安全性也面临着巨大挑战[124]. 为此,大规模 IC 系统中的 ZTA 通常采用符合 IC 特征的通信协议,以确保数据的完整性和传输的准确性. 例如,Deric 等人[125]提出一种基于信号延迟物理不可克隆函数(physically unclonable functions, PUF)的 ZTA,用于检查数据的完整性. 该方案允许单个芯片对邻近芯片执行身份认证协议,并利用信号传播延迟的独特变化作为 PUF 进行身份认证,有效检测信息传递的完整性.Ahmed 等人[70]提出一种基于零信任原则的芯片到芯片(C2C)架构,通过 SPDM 协议在主机系统与各芯片之间建立通信,芯片间的信任依托信任认证机构,而非芯片供应链中生成的数据,提高了数据传输过程的安全性.

6 工业零信任的分析与展望

6.1 现存问题

随着 ZTA 在工业环境中的逐步应用,一些潜在的问题和挑战也逐渐显现出来. 工业领域涉及设备类型多样、网络复杂和实时性要求高等特点,使得零信任的实施面临诸多困难. 本节将详细分析当前工业零信任在理论与实践中的主要难点,涵盖系统可行性、技术实现以及实际部署等方面,为未来的改进提供依据和方向.

尽管零信任的研究和安全理念发展迅速,有效弥补了现有安全体系在防御横向移动攻击方面的不足,但在实际应用中也暴露出了一些新的问题. 零信任核心理念的可行性仍受质疑. 例如,Michael 等人[126]从思想、实施和部署等多个角度对零信任的可行性提出质疑,指出零信任中存在许多隐含的信任区域,如策略决策点、人类决策者和信任算法等. 这些区域的可信度尚未得到充分验证. 此外,Loftus 等人[127]探讨了零信任的发展意义,指出尽管零信任在抑制攻击横向移动方面表现出良好效果,但其更适合作为一种理念而非具体的实现方案,其能否满足市场预期仍存在不确定性.

在实际应用中,零信任系统的部署也面临质疑. 比如,将企业遗留系统和基础设施改造成 ZTA 可能具有技术和经济上的困难. Bertino[127]指出,虽然零信任模型可以提高安全性,但从技术和组织的角度来看,部署后的效果难以达到预期. Swearingen 等人[128]以电网为例,认为部署在电网中的零信任系统可能会导致延迟,甚至阻碍控制系统获取关键信息. Cyber-Defense[8]指出,当前的零信任理念和实施技术都不成熟,许多实例只实现了零信任的初步方案,未达到完整的 ZTA 标准.

ZTA 的实施依赖于第 3 节中的关键技术,但其

尚未完全成熟，ZTA 的开发具有很大挑战. 例如，Sengupta 等人[129]和 Ferretti 等人[130]提出，当 ZTA 应用于多智能体结构时，多个 PDP 之间的信任分配和信息交换会显著增加决策时间延迟. Tsai[71]在面向 6G 物联网的应用中指出，普通的 ZTA 信道在处理海量数据操作时，难以保持性能和决策准确率. Zhang 等人[67]指出，零信任的沙箱模型未能有效实现逻辑隔离，存在沙箱逃逸风险.

在组织部署阶段，ZTA 的实施也面临诸多挑战，许多文献对此进行了分析，如表 4 所示. 综上所述，虽然 ZTA 提供了增强系统安全的创新性方法，但其在部署过程中依然面临多种复杂的挑战，尤其是在企业系统的适配性、实施成本以及资源协调方面. 因此，在考虑采用 ZTA 时，需全面评估这些困难，并制定相应的解决策略，以确保实现既定的安全目标并提升实施的有效性和效率.

Table 4 Challenges and Issues of ZTA in the Stage of Organization and Deployment

表 4 ZTA 在组织部署阶段的难点与问题

问题/难点	详细叙述
应用程序开发[66,131]	零信任相较于其他安全模式的差异性致使企业需要开发新的零信任内部应用程序
网络技术的阻碍[8,69]	部分点对点通信技术几乎默认特权行为的横向移动（windows 的 P2P 技术等），这会对网络环境下的零信任实现有极大的阻碍
转型成本[21,132]	零信任对数据处理及存储的要求较高，某些企业可能无法支付高昂的技术升级成本
团队协调[127,133]	组织内的管理问题相当重要，零信任的覆盖范围广，这要求需要协调好组织间的关系
遗留设施冲突[8]	ZTA 在搭建过程中可能会与不同协议、型号、数字化程度的遗留设施具有技术冲突，如何平衡新旧设施十分困难
孤岛问题[127]	ZTA 增量部署可能会出现“ZTA 孤岛”
时间开销[28,75,118,125]	ZTA 保护系统时产生大量时间开销

6.2 可行性与安全性分析

在 IIoT 环境中，设备资源受限和高实时性需求带来了特有的挑战，使 ZTA 的实施变得更具复杂性和针对性. 不同于传统环境，IIoT 中的设备多为低功耗、低存储的传感器和控制器，且对响应速度有严格要求. 为了在 IIoT 环境中实现零信任的有效性，ZTA 的设计不仅要考虑技术实现的可行性，还需确保架构在系统安全性方面的稳健性. 从以下 2 个方面对其适用性进行详细分析.

1）资源受限环境下的可行性. 在资源有限的环境中，ZTA 的关键技术需进行轻量化处理：

①简化身份认证流程. 传统的身份认证协议通常较为复杂，对资源要求较高. 针对 IIoT 设备，可以采用轻量级的单包认证协议或简化的公钥密码体制，这些协议能够显著减少计算和传输负担，适用于低功耗设备. 此外，通过将身份认证等复杂计算任务卸载至边缘计算节点或网关，可以有效降低单一设备的资源消耗，提升整个系统的认证效率.

②优化微隔离策略. 在工业场景中，实现全面微隔离虽然可以提高安全性，但往往增加系统复杂性和资源开销. 为了适应 IIoT 资源受限的特性，可以根据设备的功能和安全需求实施差异化的隔离策略. 例如，对高风险区域和关键设备设置强隔离，对低风险区域实施简化的分段方案. 通过在特定区域部署轻量级网关或代理服务器实现局部隔离，可以确保资源的合理分配，降低整体资源消耗.

2）高实时性需求下的安全性保障. ZTA 中动态访问控制的设计需在确保系统安全性的同时降低延迟，提升响应速度.

①低延迟的动态访问控制. 在高频访问的 IIoT 系统中，动态访问控制可通过本地缓存和预认证机制减少延迟. 对于频繁请求访问的设备，可以利用缓存存储设备的短期认证信息，减少重复认证带来的延迟. 例如，通过对已认证的设备设定短时间内的“快速通道”处理，可以避免频繁认证过程，确保安全性的同时满足实时性需求.

②降低资源依赖的访问控制. 在 IIoT 环境中，动态访问控制通常需要实时分析设备状态. 可以利用分层控制策略降低资源依赖：对关键设备和高风险设备执行更高频的访问认证和实时监控；对低风险设备放宽重新认证的频率，以平衡安全性与资源消耗. 此外，通过引入轻量级机器学习算法预测设备访问行为，根据历史数据简化部分设备的访问控制流程，进一步减少系统的资源负担，确保系统安全性和响应速度的稳定性.

综合来看，工业 ZTA 在 IIoT 中的应用需在可行性和安全性上找到平衡点，以满足 IIoT 环境的特定需求. 通过轻量化和差异化的技术方案，ZTA 能够在 IIoT 设备的资源限制和高实时性要求下实现安全保障，为 IIoT 提供一种有效的安全防护策略.

6.3 未来展望

近年来,零信任逐渐成为学术界的研究热点,并涌现出大量相关成果.其在去边界化趋势下的系统安全防护方面具有重要意义,并已经在实际应用中发挥了作用.展望未来,零信任的发展方向至关重要,本节将对其未来的潜在方向进行概述.

1)与AI技术的深度结合

ZTA中的信任评估、身份认证等核心功能将越来越多地依赖于联邦学习、深度学习和强化学习等AI技术的支持.AI技术能够动态分析和处理大量数据,实现更加智能化的访问控制和威胁检测.然而,AI在ZTA中的应用面临以下挑战:

①数据隐私与安全.在IIoT环境中,AI算法的应用需要处理大量敏感数据,如何在确保数据隐私的同时避免数据泄露,是亟需解决的关键问题.

②计算资源需求.AI算法通常依赖高计算资源,这在资源受限的IIoT设备中尤为突出.未来的研究需要专注于优化算法,以提高其在有限硬件条件下的适应性和效率.

③算法透明度与可解释性.AI算法的黑箱特性使其决策过程难以解释,这在需要高可信度和可追溯性的安全环境中可能引发信任问题.因此,提高AI技术在ZTA中的透明度和可解释性已成为必须解决的关键挑战.

2)与密码学技术的深度结合

密码学技术在ZTA中发挥着关键作用,特别是在身份认证、数据加密和安全通信等方面.未来,随着量子计算和生物识别技术的不断发展,零信任与密码学技术的结合将更加紧密.然而,以下挑战仍需引起足够重视:

①量子计算威胁.量子计算机的出现可能会使现有的加密算法失效,从而对ZTA中的安全机制构成威胁.开发抗量子攻击的加密算法和技术将成为未来的重要研究方向.

②密码学的计算负担.与高效密码学算法的结合可能会增加IIoT设备的计算负担,这对于资源受限的设备尤其困难.因此,需在安全性和计算负担之间找到平衡点,以确保密码学技术的有效应用.

3)零信任技术在IIoT中的深入应用

随着IIoT设备的不断增多,零信任技术将在工业环境中得到更广泛的应用,但也面临如下挑战:

①复杂异构环境的兼容性.IIoT环境中存在大量不同类型和不同协议的设备,零信任技术如何在这样复杂的异构环境中实现兼容性和互操作性,将直接影响其应用的广泛性和有效性.

②实时性要求与安全性的权衡.IIoT场景中对系统的实时性要求很高,这可能与ZTA中的严格安全措施产生冲突.未来研究需重点解决如何在不影响系统实时性的情况下实现高水平的安全防护.

通过对这些具体挑战的讨论,本文不仅展望了零信任技术的未来发展方向,还深入分析了各方向的可行性及其潜在风险与局限性.这不仅为零信任技术的进一步发展提供了重要思路,也对其在IIoT中的应用提出了更高要求.如何有效平衡安全性、性能和可扩展性,将成为未来零信任研究和实践的关键.

7 总 结

相比于传统的基于边界的安全模型,消除隐式信任的零信任安全模型更能确保IIoT的内部安全.本文对零信任安全的理论和应用进行了综述,系统回顾了零信任基本知识,概述了工业零信任及架构迁移和评估,分析介绍了工业零信任的关键技术,详细描述了工业零信任的访问控制,整理了在IIoT场景的特点和具体应用,并提出了零信任现存的问题和未来展望.

与其他零信任综述文章不同,本文聚焦于零信任在IIoT环境中的具体应用,特别是在ICS, EIoT, IoV, SIoT以及半导体行业中的安全性表现.然而,现有的零信任模型在应对复杂异构网络、高实时性需求和资源受限设备等方面仍面临诸多挑战.未来的研究应优先考虑优化零信任技术,以提高其适应性和灵活性,同时开发高效的认证与信任评估机制.本文旨在帮助研究者全面了解零信任在IIoT中的具体实现与应用,并为后续研究提供参考.

作者贡献声明: 王航宇负责论文整体设计和论文撰写;吕飞指导论文设计;程裕亮负责数据整理和协助撰写;吕世超指导论文修改;孙德刚、孙利民负责指导论文框架设计、论文审阅.

参 考 文 献

[1] Cui Jie, Zhu Yihu, Hong Zhong, et al. Efficient blockchain-based mutual authentication and session key agreement for cross-domain IIoT[J]. IEEE Internet of Things Journal, 2024, 11(9): 16325−16338

[2] May M C, Glatter D, Arnold D, et al. IIoT system canvas-from architecture patterns towards an IIoT development framework[J]. Journal of Manufacturing Systems, 2024, 72: 437−459

[3] Hu Yujiao, Jia Qingmin, Yao Yuan, et al. Industrial Internet of things intelligence empowering smart manufacturing: A literature review[J]. IEEE Internet of Things Journal, 2024, 11(11): 19143−19167

[4] Hai Tao, Sarkar A, Aksoy M, et al. Complex-valued hyperchaos-assisted vector-valued artificial neural key coordination for improving security in the industrial Internet of things[J/OL]. Engineering Applications of Artificial Intelligence, 2024[2024-09-30]. https://doi.org/10.1016/j.engappai.2023.107561

[5] Li Shan, Iqbal M, Saxena N. Future industry Internet of things with zero-trust security[J]. Information Systems Frontiers, 2024, 26: 1653−1666

[6] Stafford V A. Zero trust architecture[EB/OL]. NIST Special Publication, 2020[2024-09-30]. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[7] Buck C, Olenberger C, Schweizer A, et al. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust[J/OL]. Computers & Security, 2021[2024-09-30]. https://doi.org/10.1016/j.cose.2021.102436

[8] Haber M J. Privileged Attack Vectors[M]. Berkeley, CA: Apress, 2020: 295−304

[9] Enterprise D D. Department of defense global information grid architectural vision[EB/OL]. 2007[2024-09-30]. https://acqnotes.com/Attachments/DoD%20GIG%20Architectural%20Vision,%20June%2007.pdf

[10] Kindervag J, Balaouras S. No more chewy centers: Introducing the zero trust model of information security[EB/OL]. 2010[2024-09-30]. https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

[11] Bilger B, Boehme A, Flores B, et al. Software defined perimeter working group SDP specification 1.0[EB/OL]. (2014-04-30)[2024-09-30]. https://cloudsecurityalliance.org/download/artifacts/sdp-specification-v1-0

[12] Ward R, Beyer B. BeyondCorp: A new approach to enterprise security[J]. The Magazine of USENIX & SAGE, 2014, 39(6): 6−11

[13] Weinberg A I, Cohen K. Zero trust implementation in the emerging technologies era: Survey[J]. arXiv preprint, arXiv: 2401.09575, 2024

[14] Cunningham C, Blankenship J, Balaouras S, et al. The zero trust eXtended(ZTX)ecosystem[EB/OL].2018[2024-09-30].https://www.cisco.com/c/dam/m/en_sg/solutions/security/pdfs/forrester-ztx.pdf

[15] MacDonald N, Orans L, Skorupa J. The future of network security is in the cloud[EB/OL]. (2019-08-30)[2024-09-30]. https://vertassets.blob.core.windows.net/download/4b40e73f/4b40e73f-a2f0-4e01-93ce-351e5512590a/gartner_wp___sase___the_future_of_network_security_is_in_the_cloud_08_30_19.pdf

[16] Syed N F, Shah S W, Shaghaghi A, et al. Zero trust architecture (ZTA): A comprehensive survey[J]. IEEE Access, 2022, 10: 57143−57179

[17] Dhiman P, Saini N, Gulzar Y, et al. A review and comparative analysis of relevant approaches of zero trust network model[J/OL]. Sensors, 2024[2024-09-30]. https://doi.org/10.3390/s24041328

[18] Sarkar S, Choudhary G, Shandilya S K, et al. Security of zero trust networks in cloud computing: A comparative review[J/OL]. Sustainability, 2022[2024-09-30]. https://doi.org/10.3390/su141811213

[19] Tsai M, Lee S, Shieh S W. Strategy for implementing of zero trust architecture[J]. IEEE Transactions on Reliability, 2024, 73(1): 93−100

[20] Bertino E, Brancik K. Services for zero trust architectures: A research roadmap[C]//Proc of the IEEE Int Conf on Web Services (ICWS). Piscataway, NJ: IEEE, 2021: 14−20

[21] Fernandez E B, Brazhuk A. A critical analysis of zero trust architecture (ZTA)[J/OL]. Computer Standards & Interfaces, 2024[2024-09-30]. https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4210104

[22] Kang Hongzhaoning, Liu Gang, Wang Quan, et al. Theory and application of zero trust security: A brief survey[J/OL]. Entropy, 2023[2024-09-30]. https://www.mdpi.com/1099-4300/25/12/1595/pdf

[23] Federici F, Martintoni D, Senni V. A zero-trust architecture for remote access in industrial IoT infrastructures[J/OL]. Electronics, 2023[2024-09-30]. https://www.mdpi.com/2079-9292/12/3/566/pdf

[24] Phiayura P, Teerakanok S. A comprehensive framework for migrating to zero trust architecture[J]. IEEE Access, 2023, 11: 19487−19511

[25] Collier Z A, Sarkis J. The zero trust supply chain: Managing supply chain risk in the absence of trust[J]. International Journal of Production Research, 2021, 59(11): 3430−3445

[26] Loftus M, Vezina A, Doten R, et al. The arrival of zero trust: What does it mean?[J]. Communications of the ACM, 2023, 66(2): 56−62

[27] National Security Agency. Embracing a zero trust security model[EB/OL]. (2021-02-25)[2024-09-30]. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

[28] Wang Tao, Kang Li, Duan Jiang. Dynamic fine-grained access control scheme for vehicular ad hoc networks[J/OL]. Computer Networks, 2021[2024-09-30]. https://doi.org/10.1016/j.comnet.2021.107872

[29] Yeoh W, Liu M, Shore M, et al. Zero trust cybersecurity: Critical success factors and a maturity assessment framework[J/OL]. Computers & Security, 2023[2024-09-30]. https://www.sciencedirect.com/science/article/pii/S016740482300322Xs

[30] Xu Mingyang, Guo Junli, Yuan Haoyu, et al. Zero-trust security authentication based on SPA and endogenous security architecture[J/OL]. Electronics, 2023[2024-09-30]. https://www.mdpi.com/2079-9292/12/4/782/pdf

[31] Bello Y, Hussein A R, Ulema M, et al. On sustained zero trust conceptualization security for mobile core networks in 5G and beyond[J]. IEEE Transactions on Network and Service Management, 2022, 19(2): 1876−1889

[32] 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(1): 1309−1320

[33] Sultana M, Hossain A, Laila F, et al. Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology[J]. BMC Medical Informatics and Decision Making, 2020, 20: 1−10

[34] Zanasi C, Russo S. Flexible zero trust architecture for the

cybersecurity of industrial IoT infrastructures[J/OL]. Ad Hoc Networks, 2024[2024-09-30]. https://doi.org/10.1016/j.adhoc.2024.103414

[35] Chen Xu, Feng Wei, Ge Ning, et al. Zero trust architecture for 6G security[J]. IEEE Network, 2023, 38(4): 224−232

[36] Zaid B, Sayeed A, Bala P, et al. Toward secure and resilient networks: A zero-trust security framework with quantum fingerprinting for devices accessing network[J/OL]. Mathematics, 2023[2024-09-30]. https://doi.org/10.3390/math11122653

[37] Szymanski T H. The "cyber security via determinism" paradigm for a quantum safe zero trust deterministic Internet of things (IoT)[J]. IEEE Access, 2022, 10: 45893−45930

[38] Li Peirong, Ou Wei, Liang Haozhe, et al. A zero trust and blockchain-based defense model for smart electric vehicle chargers[J/OL]. Journal of Network and Computer Applications, 2023[2024-09-30]. https://doi.org/10.1016/j.jnca.2023.103599

[39] Gai Keke, She Yufeng, Zhu Liehuang, et al. A blockchain-based access control scheme for zero trust cross-organizational data sharing[J]. ACM Transactions on Internet Technology, 2023, 23(3): 1−25

[40] Daah C, Qureshi A, Awan I, et al. Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework[J/OL]. Electronics, 2024[2024-09-30]. https://doi.org/10.3390/electronics13050865

[41] Ali B, Gregory M A, Li Shuo, et al. Implementing zero trust security with dual fuzzy methodology for trust-aware authentication and task offloading in multi-access edge computing[J/OL]. Computer Networks, 2024[2024-09-30]. https://doi.org/10.1016/j.comnet.2024.110197

[42] McIntosh T, Kayes A S M, Chen Y P P, et al. Dynamic user-centric access control for detection of ransomware attacks[J/OL]. Computers & Security, 2021[2024-09-30]. https://doi.org/10.1016/j.cose.2021.102461

[43] Filip I D, Ionite C, González-Cebrián A, et al. SMARDY: Zero-trust FAIR marketplace for research data[C]//Proc of IEEE Int Conf on Big Data. Piscataway, NJ: IEEE, 2022: 1535−1541

[44] Liu Haiqing, Ai Ming, Huang Rong, et al. Identity authentication for edge devices based on zero-trust architecture[J/OL]. Concurrency and Computation: Practice and Experience, 2022[2024-09-30]. https://doi.org/10.1002/cpe.7198

[45] Rivera J J D, Khan T A, Akbar W, et al. Secure enrollment token delivery for zero trust networks using blockchain[C/OL]//Proc of the 23rd Asia-Pacific Network Operations and Management Symp (APNOMS). Piscataway, NJ: IEEE, 2022[2024-09-30]. https://doi.org/10.23919/APNOMS56106.2022.9919940

[46] Fang He, Zhu Yongxu, Zhang Yan, et al. Decentralized edge collaboration for seamless handover authentication in zero-trust IoV[J]. IEEE Transactions on Wireless Communications, 2024, 23(8): 8760−8772

[47] Ge Yunfei, Zhu Quanyuan. 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

[48] Cheng Ruizhi, Chen Songqing, Han Bo. Towards zero-trust security for the metaverse[J]. IEEE Communications Magazine, 2023, 62(2): 156−162

[49] Anderson J, Huang Qiqing, Cheng Long, et al. A zero trust architecture for connected and autonomous vehicles[J]. IEEE Internet Computing, 2023, 27(5): 7−14

[50] Meng Lei, Huang Daochao, An Jiahang, et al. A continuous authentication protocol without trust authority for zero trust architecture[J]. China Communications, 2022, 19(8): 198−213

[51] Shen Quan. Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach[J/OL]. Computers & Security, 2024[2024-09-30]. https://doi.org/10.1016/j.cose.2023.103537

[52] Liu Yizhong, Xing Xinxin, Tong Ziheng, et al. Secure and scalable cross-domain data sharing in zero-trust cloud-edge-end environment based on sharding blockchain[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 21(4): 2603−2618

[53] Shah S W, Syed N F, Shaghaghi A, et al. LCDA: Lightweight continuous device-to-device authentication for a zero trust architecture (ZTA)[J/OL]. Computers & Security, 2021[2024-09-30]. https://doi.org/10.1016/j.cose.2021.102351

[54] Chen Lu, Sun Yuwei, Sun Zhixin. A mobile Internet multi-level two-way identity authentication scheme based on zero trust[C]//Proc of IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys). Piscataway, NJ: IEEE, 2021: 1650−1656

[55] Singh J, Refaey A, Shami A. Multilevel security framework for NFV based on software defined perimeter[J]. IEEE Network, 2020, 34(5): 114−119

[56] Chen Baozhan, Qiao Siyuan, Zhao Jie, et al. A security awareness and protection system for 5G smart healthcare based on zero-trust architecture[J]. IEEE Internet of Things Journal, 2020, 8(13): 10248−10263

[57] 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

[58] Sedjelmaci H, Tourki K, Ansari N. Enabling 6G security: The synergy of zero trust architecture and artificial intelligence[J]. IEEE Network, 2023, 38(3): 171−177

[59] Bradatsch L, Miroshkin O, Kargl F. ZTSFC: A service function chaining-enabled zero trust architecture[J]. IEEE Access, 2023, 11: 125307−125327

[60] Huang Wenhua, Xie Xuemin, Wang Ziying, et al. ZT-Access: A combining zero trust access control with attribute-based encryption scheme against compromised devices in power IoT environments[J/OL]. Ad Hoc Networks, 2023[2024-09-30]. https://doi.org/10.1016/j.adhoc.2023.103161

[61] Wang Liang, Ma Hailong, Li Ziyong, et al. A data plane security model of SR-BE/TE based on zero-trust architecture[J/OL]. Scientific Reports, 2022[2024-09-30]. https://www.nature.com/articles/s41598-022-24342-y

[62] Zanasi C, Magnanini F, Russo S, et al. A zero trust approach for the cybersecurity of industrial control systems[C/OL]//Proc of the IEEE 21st Int Symp on Network Computing and Applications (NCA).

Piscataway, NJ: IEEE, 2022[2024-09-30]. https://doi.org/10.1109/NCA57778.2022.10013559

[63] Lei Wenxin, Pang Zhibo, Wen Hong, et al. Physical layer enhanced zero-trust security for wireless industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2023, 20(3): 4327−4336

[64] Wu Anbin, Feng Zhiyong, Li Xiaohong, et al. ZTWeb: Cross site scripting detection based on zero trust[J/OL]. Computers & Security, 2023[2024-09-30]. https://doi.org/10.1016/j.cose.2023.103434

[65] Konduru P, Nethravathi N P. Secure and energy-efficient routing protocol based on micro-segmentation and batch authentication [J/OL]. Computer Networks, 2024[2024-09-30]. https://doi.org/10.1016/j.comnet.2024.110293

[66] Hong Sungmin, Xu Lei, Huang Jianwei, et al. SysFlow: Toward a programmable zero trust framework for system security[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2794−2809

[67] Zhang Jingci, Zheng Jun, Zhang Zhang, et al. Hybrid isolation model for device application sandboxing deployment in zero trust architecture[J]. International Journal of Intelligent Systems, 2022, 37((12):): 11167−11187

[68] Bradatsch L, Haeberle M, Steinert B, et al. Secure service function chaining in the context of zero trust security[C]//Proc of the IEEE 47th Conf on Local Computer Networks (LCN). Piscataway, NJ: IEEE, 2022: 123−131

[69] Csikor L, Ramachandran S, Lakshminarayanan A. ZeroDNS: Towards better zero trust security using DNS[C]//Proc of the 38th Annual Computer Security Applications Conf. New York: ACM, 2022: 699−713

[70] Ahmed A, Shoufan A. Formal verification of light-weight security protocol and data model for chip-to-chip zero trust[J]. IEEE Access, 2023, 11: 60335−60348

[71] Tsai W C. Field-programmable gate array-based implementation of zero-trust stream data encryption for enabling 6G-narrowband Internet of things massive device access[J/OL]. Sensors, 2024[2024-09-30]. https://doi.org/10.3390/s24030853

[72] Wang Jin, Chen Jiahao, 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

[73] Ameer S, Gupta M, Bhatt S, et al. Bluesky: Towards convergence of zero trust principles and score-based authorization for IoT enabled smart systems[C]//Proc of the 27th ACM on Symp on Access Control Models and Technologies. New York: ACM, 2022: 235−244

[74] Park U H, Hong J, Kim A, et al. Endpoint device risk-scoring algorithm proposal for zero trust[J/OL]. Electronics, 2023[2024-09-30]. https://doi.org/10.3390/electronics12081906

[75] Wang Jiuru, Wang Zhiyuan, Song Jingcheng, et al. Attribute and user trust score-based zero trust access control model in IoV[J/OL]. Electronics, 2023[2024-09-30]. https://doi.org/10.3390/electronics-12234825

[76] Wang Zhiqiang, Yu Xinyue, Xue Peiyang, et al. Research on medical security system based on zero trust[J/OL]. Sensors, 2023[2024-09-30]. https://doi.org/10.3390/s23073774

[77] Al S A M, Rizwan A, Sánchez-Chero M, et al. Blockchain-enabled federated learning for prevention of power terminals threats in IoT environment using edge zero-trust model[J]. The Journal of Supercomputing, 2024, 80(6): 7849−7875

[78] Fu Peiyu, Wu Jun, Lin Xi, et al. ZTEI: Zero-trust and edge intelligence empowered continuous authentication for satellite networks[C]//Proc of IEEE Conf on Global Communications (GLOBECOM). Piscataway, NJ: IEEE, 2022: 2376−2381

[79] Wang Peng, Xu Ning, Zhang Haibin, et al. Dynamic access control and trust management for blockchain-empowered IoT[J]. IEEE Internet of Things Journal, 2021, 9(15): 12997−13009

[80] N'goran R, Tetchueng J L, Pandry G, et al. Trust assessment model based on a zero trust strategy in a community cloud environment[J]. Engineering, 2022, 14(11): 479−496

[81] Ramezanpour K, Jagannath J. Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN[J/OL]. Computer Networks, 2022[2024-09-30]. https://doi.org/10.1016/j.comnet.2022.109358

[82] 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/OL]. Computer Networks, 2022[2024-09-30]. https://doi.org/10.1016/j.comnet.2022.109068

[83] Nkoro E C, Njoku J N, Nwakanma C I, et al. Zero-trust marine cyberdefense for IoT-based communications: An explainable approach[J/OL]. Electronics, 2024[2024-09-30]. https://doi.org/10.3390/electronics13020276

[84] Akbar W, Rivera J J D, Ahmed K T, et al. Software defined perimeter monitoring and blockchain-based verification of policy mapping[C/OL]//Proc of the 23rd Asia-Pacific Network Operations and Management Symp(APNOMS). Piscataway, NJ: IEEE, 2022[2024-09-30]. https://doi.org/10.23919/APNOMS56106.2022.9919959

[85] Gudala L, Shaik M, Venkataramanan S. Leveraging machine learning for enhanced threat detection and response in zero trust security frameworks: An exploration of real-time anomaly identification and adaptive mitigation strategies[J]. Journal of Artificial Intelligence Research, 2021, 1(2): 19−45

[86] He Yuanhang, Huang Daochao, Chen Lei, et al. A survey on zero trust architecture: Challenges and future trends[J/OL]. Wireless Communications and Mobile Computing, 2022[2024-09-30]. https://doi.org/10.1155/2022/6476274

[87] Ouaddah A, Mousannif H, Abou Elkalam A, et al. Access control in the Internet of things: Big challenges and new opportunities[J/OL]. Computer Networks, 2017[2024-09-30]. https://doi.org/10.1016/j.comnet.2016.11.007

[88] Sandhu R, Samarati P. Authentication, access control, and audit[J]. ACM Computing Surveys, 1996, 28(1): 241−243

[89] Lampson B W. Dynamic protection structures[C]//Proc of the Fall Joint Computer Conf. New York: ACM, 1969: 27−38

[90] Hao Xiaohan, Ren Wei, Fei Yangyang, et al. A blockchain-based cross-domain and autonomous access control scheme for Internet of things[J]. IEEE Transactions on Services Computing, 2022, 16(2):

773−786

[91] Lindqvist H. Mandatory access control [D]. Sweden: Department of Computing Science, Umea University, 2006

[92] Wang Baoyi, Zhang Shaomi. An organization and task based access control model for workflow system[C]//Proc of the Asia-Pacific Web Conf. Berlin: Springer, 2007: 485−490

[93] Hu Donghui, Hu Chunya, Fan Yuqi, et al. oGBAC — A group based access control framework for information sharing in online social networks[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 18(1): 100−116

[94] Ray I, Kumar M. Towards a location-based mandatory access control model[J]. Computers & Security, 2006, 25(1): 36−44

[95] Anutariya C, Chatvichienchai S, Iwiahara M, et al. A rule-based xml access control model[C]//Proc of the 2nd Int Workshop on Rules and Rule Markup Languages for the Semantic Web(RuleML). Berlin: Springer, 2003: 35−48

[96] Andriotis P, Stringhini G, Sasse M A. Studying users' adaptation to Android's run-time fine-grained access control system[J]. Journal of Information Security and Applications, 2018, 40(1): 31−43

[97] Bertino E. RBAC models — Concepts and trends[J]. Computers & Security, 2003, 22(6): 511−514

[98] Bakar A A, Ismail R, Jais J. A review on extended role based access control (E-RBAC) model in pervasive computing environment [C]//Proc of the 1st Int Conf on Networked Digital Technologies. Piscataway, NJ: IEEE, 2009: 533−535

[99] Pal S, Jadidi Z. Protocol-based and hybrid access control for the IoT: Approaches and research opportunities[J/OL]. Sensors, 2021[2024-09-30]. https://doi.org/10.3390/s21206832

[100] Shin S H, Park M J, Kim T W, et al. Architecture for enhancing communication security with RBAC IoT protocol-based microgrids[J/OL]. Sensors, 2024[2024-09-30]. https://doi.org/10.3390/s24186000

[101] Zaidi T, Usman M, Aftab M U, et al. Fabrication of flexible role-based access control based on blockchain for Internet of things use cases[J]. IEEE Access, 2023, 11: 106315−106333

[102] Xu Zhengnan, Dong Guofang, Yang Ruicheng. RBAC-based one-to-many authentication and key negotiation scheme in smart factory[J]. IEEE Access, 2024, 12: 189202−189218

[103] Yuan E, Tong J. Attributed based access control (ABAC) for web services[C]// Proc of the IEEE Int Conf on Web Services (ICWS'05). Piscataway, NJ: IEEE, 2005: 569−578

[104] Shang Siyuan, Wang Xiaohan, Liu Aodi. ABAC policy mining method based on hierarchical clustering and relationship extraction[J/OL]. Computers & Security, 2024[2024-09-30]. https://doi.org/10.1016/j.cose.2024.103717

[105] Chen Zhonghua, Goyal S B, Rajawat A S. Smart contracts attribute-based access control model for security & privacy of IoT system using blockchain and edge computing[J]. The Journal of Supercomputing, 2024, 80(2): 1396−1425

[106] Cremonezi B, Vieira A B, Nacif J, et al. Identity management for Internet of things: Concepts, challenges and opportunities[J]. Computer Communications, 2024, 224: 72−94

[107] Alshehri S, Bamasag O. Aac-IoT: Attribute access control scheme for IoT using lightweight cryptography and hyperledger fabric blockchain[J/OL]. Applied Sciences, 2022[2024-09-30]. https://doi.org/10.3390/app12168111

[108] Pathak A, Al-Anbagi I, Hamilton H J. TABI: Trust-based ABAC mechanism for edge-IoT using blockchain technology[J]. IEEE Access, 2023, 11: 36379−36398

[109] Ragothaman K, Wang Y, Rimal B, et al. Access control for IoT: A survey of existing research, dynamic policies and future directions[J/OL]. Sensors, 2023[2024-09-30]. https://doi.org/10.3390/s23041805

[110] Patil P, Sangeetha M, Bhaskar V. Blockchain for IoT access control, security and privacy: A review[J]. Wireless Personal Communications, 2021, 117(3): 1815−1834

[111] Salehi A, Han Runchao, Rudolph C, et al. DACP: Enforcing a dynamic access control policy in cross-domain environments[J/OL]. Computer Networks, 2023[2024-09-30]. https://doi.org/10.1016/j.comnet.2023.110049

[112] Zhang Qingyang, Zhong Hong, Cui Jie, et al. AC4AV: A flexible and dynamic access control framework for connected and autonomous vehicles[J]. IEEE Internet of Things Journal, 2020, 8(3): 1946−1958

[113] Singh A, Dhanaraj R K, Ali M A, et al. Transfer fuzzy learning enabled Streebog cryptographic substitution permutation based zero trust security in IIoT[J]. Alexandria Engineering Journal, 2023, 81: 449−459

[114] Kobayashi N. Zero trust security framework for IoT actuators [C]//Proc of the 47th IEEE Annual Computers, Software, and Applications Conf (COMPSAC). Piscataway, NJ: IEEE, 2023: 1285−1292

[115] Feng Jingyu, Yu Tingting, Wang Ziying, et al. An edge zero-trust model against compromised terminals threats in power IoT environments[J]. Journal of Computer Research and Development, 2022, 59(5): 1120−1132 (in Chinese)
(冯景瑜, 于婷婷, 王梓莹, 等. 电力物联场景下抗失陷终端威胁的边缘零信任模型[J]. 计算机研究与发展, 2022, 59(5): 1120−1132)

[116] Hao Min, Tan Beihai, Wang Siming, et al. Exploiting blockchain for dependable services in zero-trust vehicular networks[J/OL]. Frontiers of Computer Science, 2024[2024-09-30]. https://link.springer.com/10.1007/s11704-023-2495-0

[117] Cui Qimei, Zhu Zengbao, Ni Wei, et al. Edge-intelligence-empowered, unified authentication and trust evaluation for heterogeneous beyond 5G systems[J]. IEEE Wireless Communications, 2021, 28(2): 78−85

[118] Tian Minqiu, Li Zifu, Li Fenghua, et al. A terminal security authentication protocol for zero-trust satellite IoT[C]//Proc of the IEEE Int Conf on Trust, Security and Privacy in Computing and Communications (TrustCom). Piscataway, NJ: IEEE, 2022: 299−306

[119] Pokhrel S R. Poster: Orbital ZTA! Secure satellite communication networks with zero trust architecture[C]//Proc of the ACM SIGCOMM Conf: Posters and Demos. New York: ACM, 2024: 33−35

[120] Falco G, Gordon N G. A zero-trust satellite services marketplace

enabling space infrastructure as a service[J]. IEEE Access, 2024, 12: 71066−71075

[121] Kulkarni A, Hazari N A, Niamat M. A zero trust-based framework employed by blockchain technology and ring oscillator physical unclonable functions for security of field programmable gate array supply chain[J]. IEEE Access, 2024, 12: 89322−89338

[122] Stern A, Wang H, Rahman F, et al. ACED-IT: Assuring confidential electronic design against insider threats in a zero-trust environment[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 41(10): 3202−3215

[123] Buras B, Xanthopoulos C, Butler K, et al. Zero trust approach to IC manufacturing and testing[C]//Proc of the IEEE Int Test Conf (ITC). Piscataway, NJ : IEEE, 2022: 583−586

[124] Belwafi K, Alshamsi H, Ahmed A, et al. Enhancing circuit authentication through secure isolation[C/OL]//Proc of the IEEE Int Symp on Circuits and Systems (ISCAS). Piscataway, NJ: IEEE, 2024[2024-09-30]. https://doi.org/10.1109/ISCAS58744.2024.10558551

[125] Deric A, Holcomb D. Know time to die–integrity checking for zero trust chiplet-based systems using between-die delay PUFs[J/OL]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022[2024-09-30]. https://doi.org/10.46586/tches.v2022.i3.391-412

[126] Michael J B, Dinolt G C, Cohen F B, et al. Can you trust zero trust?[J]. Computer, 2022, 55(8): 103−105

[127] Bertino E. Zero trust architecture: Does it help?[J]. IEEE Security & Privacy, 2021, 19(5): 95−96

[128] Swearingen M T, Michael J B, Weiss J, et al. Resilient without zero trust[J]. Computer, 2024, 57(1): 120−122

[129] Sengupta B, Lakshminarayanan A. Distritrust: Distributed and low-latency access validation in zero-trust architecture[J/OL]. Journal of Information Security and Applications, 2021[2024-09-30]. https://doi.org/10.1016/j.jisa.2021.103023

[130] Ferretti L, Magnanini F, Andreolini M, et al. Survivable zero trust for cloud computing environments[J/OL]. Computers & Security, 2021[2024-09-30]. https://doi.org/10.1016/j.cose.2021.102419

[131] Dubin R. Content disarm and reconstruction of RTF files: A zero file trust methodology[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 1461−1472

[132] Adahman Z, Malik A W, Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security [J/OL]. Computers & Security, 2022[2024-02-20]. https://doi.org/10.1016/j.cose.2022.102911

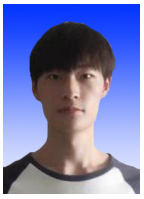
[133] Spencer M, Pizio D. The de-perimeterisation of information security: The jericho forum, zero trust, and narrativity[J/OL]. Social Studies of Science, 2023[2024-09-30]. https://doi.org/10.1177/030631272-31221107

Wang Hangyu, born in 1997. PhD candidate. His main research interest includes access control and zero-trust security in IIoT.

王航宇, 1997 年生. 博士研究生. 主要研究方向为工业物联网中的访问控制和零信任安全.

Lü Fei, born in 1987. PhD, engineer. His mian research interest includes the protection of the IIoT.

吕　飞, 1987 年生. 博士, 工程师. 主要研究方向为工业物联网防护.



Cheng Yuliang, born in 2002. Master candidate. His main research interests include access control, zero-trust security, and information security.

程裕亮, 2002 年生. 硕士研究生. 主要研究方向为访问控制、零信任安全、信息安全.

Lü Shichao, born in 1985. PhD, senior engineer. His main research interest includes active defense, proactive monitoring, and security enhancement for ICS.

吕世超, 1985 年生. 博士, 高级工程师. 主要研究方向为工控系统主动防御、主动监测与安全增强.

Sun Degang, born in 1970. PhD, professor, PhD supervisor. His main research interests include electromagnetic leakage protection, wireless communication technology, and high security level information system protection technology.

孙德刚, 1970 年生. 博士, 教授, 博士生导师. 主要研究方向为电磁泄漏防护、无线通信技术、高安全级别信息系统防护技术.

Sun Limin, born in 1966. PhD, professor, PhD supervisor. Senior member of CCF. His main research interests include ICS security and IoT security.

孙利民, 1966 年生. 博士, 教授, 博士生导师. CCF 高级会员. 主要研究方向为工控安全、物联网安全.