内生安全：数据通信设备的必由之路

李江波　王 玥
博鼎实华（北京）技术有限公司　北京海淀　100096

摘　要：随着数据通信的发展，内生安全成为数据通信设备的关键需求。内生安全能从设备内部构建防护机制，抵御各类安全威胁，保障数据通信的稳定与可靠。强调其是数据通信设备发展的必然方向，可提升设备整体安全性与性能，推动行业健康发展。

关键词：内生安全；数据通信设备；安全防护；人工智能

引言

在数字化时代，数据通信设备的安全至关重要。传统安全防护手段面临诸多挑战，难以有效应对复杂多变的安全威胁。内生安全理念应运而生，它为数据通信设备的安全保障提供了新思路，同时人工智能（AI）技术的快速发展，为内生安全注入了新的动能，使得安全能力更加智能化、自适应，成为实现深度内生安全的关键赋能要素。探究其成为必由之路具有重要现实意义。

1 内生安全概述

1.1 内生安全定义

内生安全是一种从系统、设备内部构建安全能力的理念。它不是简单地在现有设备和系统上附加安全防护措施，而是将安全属性融入到设备的设计、开发、运行等全生命周期之中。这种融入是深层次的，涉及到硬件、软件、算法等多个层面。例如，在硬件设计阶段就考虑如何防止物理层面的攻击，像芯片的抗干扰、抗电磁脉冲能力等。在软件方面，通过优化代码结构、加密算法的嵌入等，使得软件在运行过程中具有内在的安全性。它是一种基于内生的、主动的安全防御思维，旨在从根本上提升设备应对各种安全威胁的能力。

1.2 内生安全特点

内生安全具有多方面的特点。首先是自主性，强调设备自身具备安全防护能力，不依赖于外部的防护体系。例如，数据通信设备能够独立检测和抵御网络攻击，而不需要不断从外部获取防护指令。其次是动态性，内生安全能够根据设备的运行状态、网络环境的变化等因素动态调整安全策略。比如，当网络流量突然异常增加时，设备能够自动识别并调整防火墙规则。再者是协同性，在一个复杂的系统中，各个内生安全的设备之间能够相互协作。比如，在数据通信网络中的多个路由器之间可以共享安全信息，共同应对可能的攻击。最后是适应性，可以适应不同的应用场景和安全需求。无论是在企业级的大型网络还是家庭小型网络环境下，都能发挥有效的安全防护作用。

1.3 内生安全重要性

内生安全的重要性不言而喻。在当今数字化时代，数据通信设备面临着日益复杂的安全威胁。内生安全能够从源头上减少安全漏洞的产生。传统的安全防护往往是事后补救型的，而内生安全可以在设备设计阶段就将安全隐患降至最低。人工智能技术的融入进一步放大了内生安全的价值，内生安全对于保障 AI 模型的安全运行以及 AI 驱动的安全防护机制也至关重要。数据通信设备作为关键信息基础设施，对于保障国家安全也有着至关重要的意义。例如，电力、通信等关键行业的数据通信设备如果缺乏内生安全，一旦遭受攻击，可能会导致大面积的停电、通信中断等严重后果。

2 数据通信设备现状

2.1 面临的安全威胁

数据通信设备面临着多种多样的安全威胁。网络攻击是最为常见的威胁之一，包括黑客的恶意入侵、分布式拒绝服务攻击（DDoS）等。黑客可能会试图获取设备的控制权，从而窃取敏感信息或者篡改数据。DDoS 攻击则会使设备无法正常提供服务，导致网络瘫痪。恶意软件也是一个严重的威胁，如病毒、木马等可能会感染设备，在设备内部潜伏并进行恶意操作。此外，设备的物理安全也不容忽视，例如，设备可能会遭受物理破坏或者非法访问，从而导致数据泄露或者设备损坏。随着 5G 和人工智能广泛应用的背景下，数

ISSN: 2661-3719(Print); 2661-3727(Online)

据通信设备还面临着新的安全威胁，如 5G 网络切片的安全风险、边缘计算带来的安全挑战；利用 AI 技术深度伪造流量和内容进行欺诈，针对设备中运行的 AI 模型进行攻击，篡改模型或窃取模型数据等。

2.2 传统防护的局限

传统的安全防护措施在应对数据通信设备的安全问题时存在诸多局限。传统防护主要以防火墙、入侵检测系统等为代表。防火墙虽然能够在一定程度上阻止外部网络的非法访问，但对于内部网络的攻击或者绕过防火墙的攻击往往无能为力。入侵检测系统只能在攻击发生后进行检测，无法做到事前预防。而且，传统防护措施往往是针对特定类型的攻击进行设计的，对于新型的复杂攻击手段，如高级持续性威胁（APT），很难有效地进行识别和防御。此外，传统防护无法有效检测和防御针对 AI 模型的攻击，也难以适应 AI 环境下快速变化的安全威胁。

2.3 发展趋势分析

数据通信设备的安全防护呈现出一些发展趋势。首先是智能化的趋势，随着人工智能和机器学习技术的发展，安全防护将更加智能化。例如，通过机器学习算法对海量网络流量和用户行为进行实时分析，建立正常行为基线，能够更精准、更快速地识别未知威胁和异常行为（如零日攻击、隐蔽的 APT 攻击）。其次是融合化的趋势，安全防护将与设备的其他功能更加深度融合。不再是单独的安全模块，而是贯穿于设备的各个功能环节。再者是云和算力的趋势，借助云计算的强大计算能力和存储能力，安全防护将可以实现更加高效的资源共享和协同防御。最后是标准化的趋势，随着行业的发展，安全防护的标准将不断完善，这有助于提高不同设备之间的兼容性和互操作性，AI 模型接口、威胁情报格式等数据标准化也将是智能化内生安全协同的基础。

3 内生安全在数据通信设备的应用

3.1 应用原理

内生安全在数据通信设备中的应用原理基于多种技术的融合。从硬件角度看，通过采用可信计算技术，为设备建立可信根。例如，在芯片制造过程中嵌入可信模块，该模块可以对设备的启动过程、硬件组件的完整性等进行验证。集成 AI 加速引擎（如 NPU）的专用安全芯片，可显著提升设备本地执行复杂安全算法的效率，AI 模型作为核心安全策略引擎，能够根据实时学习到的威胁态势动态生成和调整访问控制规则、入侵检测签名、行为分析策略等。此外，还利用加密技术，对设备中的数据进行加密处理，AI 技术可用于优化密钥管理、检测加密通信中的异常模式。同时，利用零信任架构的思想，不再默认网络内部的任何设备或用户是可信的，而是对每一个访问请求进行严格的身份验证和授权，AI 在零信任架构中也扮演关键角色，通过持续的行为分析评估用户 / 设备的信任度，实现动态、细粒度的访问控制决策。

3.2 应用方式

内生安全在数据通信设备中的应用方式多种多样。在设计阶段，就将安全功能集成到硬件和软件的设计中。例如，设计具有内置安全防护功能的芯片和具有安全机制的操作系统。在部署阶段，通过配置参数，使设备能够适应特定的网络环境。例如，设置不同的加密强度和访问控制策略，并加载预训练或云端下发的 AI 安全模型。在设备运行过程中，系统可以实时监测设备的运行状态，对异常情况进行及时处理。例如，当检测到设备组件遭受攻击时，基于 AI 的异常检测系统能更快定位问题根源，自动采取相应的防御措施。此外，设备间互联互通时，实现内生安全能力的共享。例如，在网络中的多个交换机之间可以通过联邦学习等技术，在保护隐私的前提下共享安全威胁特征和模型更新，共同提升网络的整体安全水平，形成群体智能防御能力。

3.3 应用效果

内生安全在数据通信设备中的应用效果显著。首先，通过内置的安全功能可以有效抵御各种网络攻击和恶意软件的入侵。例如，具备 AI 分析能力的路由器能够更有效地识别和缓解 DDoS 攻击。其次，增强了设备的可靠性，可以及时发现设备的故障隐患并进行修复，减少设备的故障率。AI 驱动的预测性维护功能可基于设备运行数据（如温度、功耗、日志）预测硬件故障，提前预警或启动修复流程。再者，提高了设备的适应性。无论是企业环境还是家庭网络下，AI 模型都能够根据环境特征自我调优安全策略，发挥良好的安全防护作用。最后，促进了设备的创新发展。内生安全与 AI 能力结合的需求，推动了数据通信设备在硬件和软件设计方面的创新，例如，促使设计更具安全性能的芯片，开发更智能的操作系统。

4 实现内生安全的途径

实现内生安全需要多方面的努力。首先是硬件技术的

创新，开发具有更高安全性能的芯片是关键。例如，研发具有内置 AI 加速单元、抗干扰能力强、支持硬件级可信执行环境的芯片。同时，要改进硬件的架构设计，采用分层架构、模块化设计等方式，提高硬件的可维护性和安全性。在软件技术方面，应采用安全编码规范，避免常见的安全漏洞。此外，还需要加强加密技术的应用，采用更高级的加密算法，提高数据的保密性和完整性。并且，要推动人工智能和机器学习技术在安全领域的应用，以识别和预测安全威胁。

5 内生安全对行业的影响

5.1 对企业的影响

内生安全对企业有着深远的影响。对于数据通信设备制造企业来说，内生安全的需求促使企业加大在研发方面的投入。企业需要研发更具安全性能的设备，这就要求企业不断探索 AI 芯片、成 AI 框架软件，以及安全算法，提高自身的技术创新能力。同时，内生安全也有助于企业提高产品的竞争力。在市场上，具有内生安全功能的设备更受客户的青睐，因为它能够为客户提供更可靠的安全保障。对于使用数据通信设备的企业而言，内生安全可以降低企业的安全风险。例如，金融企业采用具备 AI 内生安全能力的数据通信设备可以更有效地识别和阻止针对交易系统的欺诈和攻击，更好地保护客户的资金和交易信息。企业对掌握 AI 与安全双重技能的人才需求也急剧增加。

5.2 对市场的影响

内生安全对市场产生了多方面的影响。在市场需求方面，随着企业和用户对安全的重视，特别是对智能化、自动化安全防护的需求增长，内生安全的数据通信设备市场需求不断增加。这促使市场上的供应商不断调整产品策略，加大对内生安全设备的研发和生产。在市场竞争方面，内生安全成为企业竞争的一个新的焦点。能够提供更先进 AI 内生安全技术、更高效智能安全模型和解决方案的企业将在市场竞争中占据优势。例如，一些大型的通信设备制造商通过不断提升自身内生安全技术水平，扩大了市场份额。在市场规范方面，内生安全的发展也促使相关部门制定更加完善的市场标准和规范。AI 模型安全性、可解释性、数据隐私保护等方面的标准也将成为未来规范制定的重要方向。这有助于规范市场秩序，防止不良企业的不正当竞争，促进市场的健康发展。

5.3 对社会的影响

内生安全对社会的影响是积极而广泛的。在保障国家安全方面，内生安全的数据通信设备有助于保护国家的关键信息基础设施。例如，在国防、能源、通信等领域，AI 深度赋能的内生安全可以防止外部势力的网络攻击，保障国家的安全和稳定。在促进社会数字化转型方面，内生安全为数字经济的发展提供了安全保障。内生安全可以确保联网、大数据这些新技术在安全的环境下发展，支撑智慧城市、工业互联网、自动驾驶等关键应用的落地。在保护公民隐私方面，内生安全的数据通信设备可以防止个人信息在数据通信过程中的泄露，AI 技术有助于更精准地识别和阻止针对个人信息的窃取和滥用行为，保护公民的隐私权，提高公民对数字化社会的信任度。内生安全与 AI 的融合，是构建安全、可信、智能数字社会的关键基石。

6 结束语

综上所述，内生安全作为数据通信设备的必由之路，在保障设备安全、推动行业发展等方面具有不可替代的作用。人工智能技术的融入，为内生安全开辟了智能化、自适应、主动防御的新维度，成为其发展的核心驱动力。企业应积极投入内生安全技术研发与应用，提升数据通信设备的安全性与竞争力，共同营造安全可靠的通信环境。政府、学术界、产业界需协同努力，完善相关标准与法规，培养复合型人才，推动 AI 赋能的深度内生安全生态体系的建设。

参考文献：

[1] 马康白 . 数据通信网络的运行管理与维护策略探讨 [J]. 网络安全技术与应用 ,2023,(07):13-14.

[2] 宋鹏 . 浅析数据通信网络维护与网络安全问题 [J]. 电子元器件与信息技术 ,2021,5(09):243-244.

[3] 冯丽娜 . 移动互联环境下数据通信安全技术的应用研究 [J]. 无线互联科技 ,2021,18(15):1-2.

[4] 何代菊 . 大数据背景下计算机网络信息安全问题分析 [J]. 南方农机 ,2021,52(23):126-128.

[5] 杨瑀 . 人工智能技术赋能通信工程产业的逻辑与路径 [J]. 营销界，2021（31）：103-104.

[6] 何世鹏 , 陈昕 , 姜家驷 , 等 . 信息通信行业网络内生安全现状、问题和建议 [J]. 通信企业管理 ,2023,(08):42-44.

作者简介：李江波 (1986—), 男，汉族 , 陕西 , 中级工程师，学士，研究方向为算力网络、数通设备、网络安全等。