人工智能物联网

超越当前物联网的安全连接技术

目录

人工智能：不仅仅是宣传 4

现状 5

什么是人工智能? 7

什么是机器学习? 8

什么是深度学习? 9

自2013年以来，人工智能领域的投资额增长了三倍 10

经济前景一片光明 11

将人工智能技术推动到物联网的边缘节点应用1： 13

量子计算：创建强人工智能的灵丹妙药? 16

将人工智能技术推动到物联网的边缘节点应用2： 18

人工智能：对物联网安全的意义 20

隐私保护机器学习 23

攻击机器学习：训练时攻击 26

展望未来： 28

人工智能：
不仅仅是宣传

倘若真有一个能够衡量**新技术**是否是具有“颠覆性”的指标，那么应该是公众对该技术是否感到恐惧和怀疑。但当如果我们将此看作是以社会的关注程度作为衡量标准，那么，当前**人工智能**(AI)的复兴，非常符合“颠覆性”技术突破的特征。

如我们所知，如埃隆·马斯克、比尔·盖茨、史蒂芬·霍金等名人告诉我们的，人工智能将改变生活。公众对于**人工智能应用带来危害后果**的普遍担忧并非是面对技术变革绝无仅有的反应，只不过是在了解新技术变革并认识到其巨大潜力之前，社会大众通常所表现出的焦虑不安而已。

我们希望以当前争论为契机，传达行业对人工智能及其衍生的机器学习(ML)和深度学习(DL)的观点。我们研究了高性能处理从云端向网络边缘转变如何帮助物联网(IoT)蓬勃发展，以及这一转变范例如何为人工智能展现其真正潜力奠定基础。

我们的眼光不仅局限于当今物联网，而是展望未来：智能互联设备不仅能够相互交谈，它们还可以利用人工智能代表我们彼此交互。有朝一日，这种全新的全球人工智能物联结构将被称为AIoT，即**人工智能物联网**。

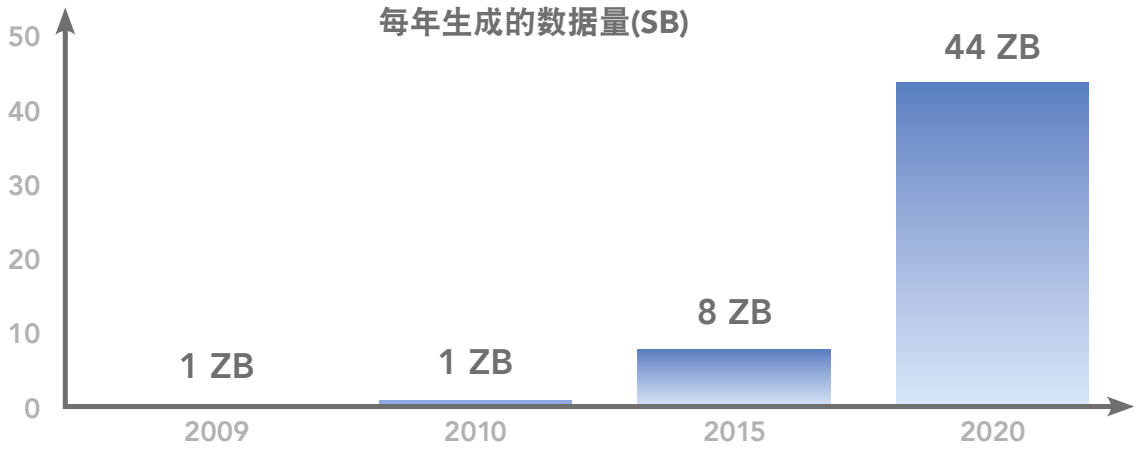
在本文中，我们将讨论这些技术的巨大潜力，同时也将了解其限制性，并思考某些人工智能应用对物联网安全造成的实际威胁，以及如何应对这些威胁。

现状

人工智能作为一门数学学科，在某种程度上也属于哲学范畴，其实在如今突然倍受公众关注之前已默默存在了60多年。现在公开宣传的一个原因在于，长期以来，人们对人工智能应用的认识只停留在理论层面，或者至少是科幻小说中。要在当今物联网环境中真正应用人工智能，必须满足以下三个条件：

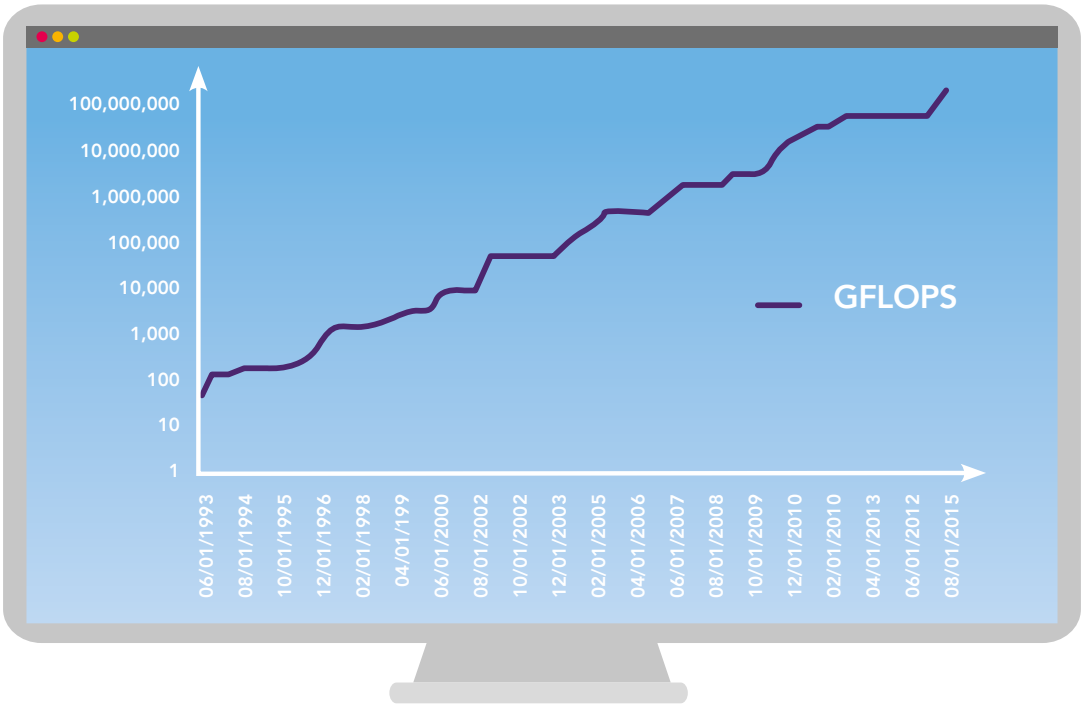
很明显，后两个要求相互依存，如果不能大幅提高处理能力，那么深度神经网络领域不可能取得突破。对于输入而言：越来越多的嵌入式物联网设备，将生成质量参差不齐的大型数据集–视觉、音频和环境数据。如今，数据流以指数级迅猛增长。

事实上，到2020年，每年生成的数据量有望达到44 ZB（1 ZB等于10亿TB），相当于五年内的年复合增长率(CAGR)达到141%。仅五年之后，数据量可能将达到**180 ZB**。



随着全球互联设备、机器和系统日渐增多，非结构化数据量也大幅增长。

大约从2015年开始，多核应用处理器和图形处理单元(GPU)开始普及，我们也通过操作工具来处理这些大量数据。并行处理成为速度更快、成本更低、性能更强大的业务。添加快速、丰富的存储和更强大的算法对数据进行排列和组织，突然之间，出现了一个能够让人工智能繁荣发展的环境。



附图2：从1993年起，全球超级计算机的原始计算性能（用GFLOPs衡量）已成倍提高。Top 500名单上排名第1的全球超级计算机的峰值速度GFLOPS。

尽管如此，在2016年，百度硅谷人工智能实验室的EE Times高级研究员Greg Diamos在评论人工智能要发挥其真正的潜力还缺少什么时说道：

“如今，训练机器学习模型的工作受到计算能力的限制，如果我们拥有更快的处理器，我们会运行更大的模型……实际上，我们使用合理的数据子集进行训练，可在数月内完成，[……]我们可以利用多个数量级的改进 – 100倍或更大。”

- Greg Diamos

2018年，经过神经网络训练的人工智能语音识别软件，成为各种消费类应用和工业应用中不可或缺的一部分。在新型自定义硬件和处理器架构的推动下，计算能力以大约每年10倍的速度提高。计算能力的迅速提升是推动人工智能发展的关键因素，正促使人工智能成为未来的主流技术。

什么是人工智能?

按照传统的定义，**人工智能**并不引人注目。在1976年发表的开拓性文章《人工智能：个人观点》中，英国神经系统科学家和人工智能先驱David Marr陈述道：人工智能的目标是识别和**解决有用信息处理问题**，并概述如何解决，即解决方法。

20世纪80年代

执行程序

文字处理软件帮助设置文档格式

21世纪初

基于规则制定决策

软件告诉您某个单词拼写错误

或者句子语法不正确

长期未来

人工智能

您告诉软件您想要写一封信，

它会为您写信

21世纪20年代

机器学习

软件可以根据更多意思帮助您

写出更好的句子

诚然，人工智能计算系统的灵感可能来源于构成大脑的生物神经网络。但是，人工智能借鉴人类大脑的功能以使机器像人类一样解决问题，仍然是一个遥远的神话。神经网络更像是一个框架，能够让许多不同的机器学习算法相互协作共同处理复杂的数据输入。与生物神经网络的主要差距在于，ANN专注于执行具体任务，而非普遍通用的解决问题和计划能力。

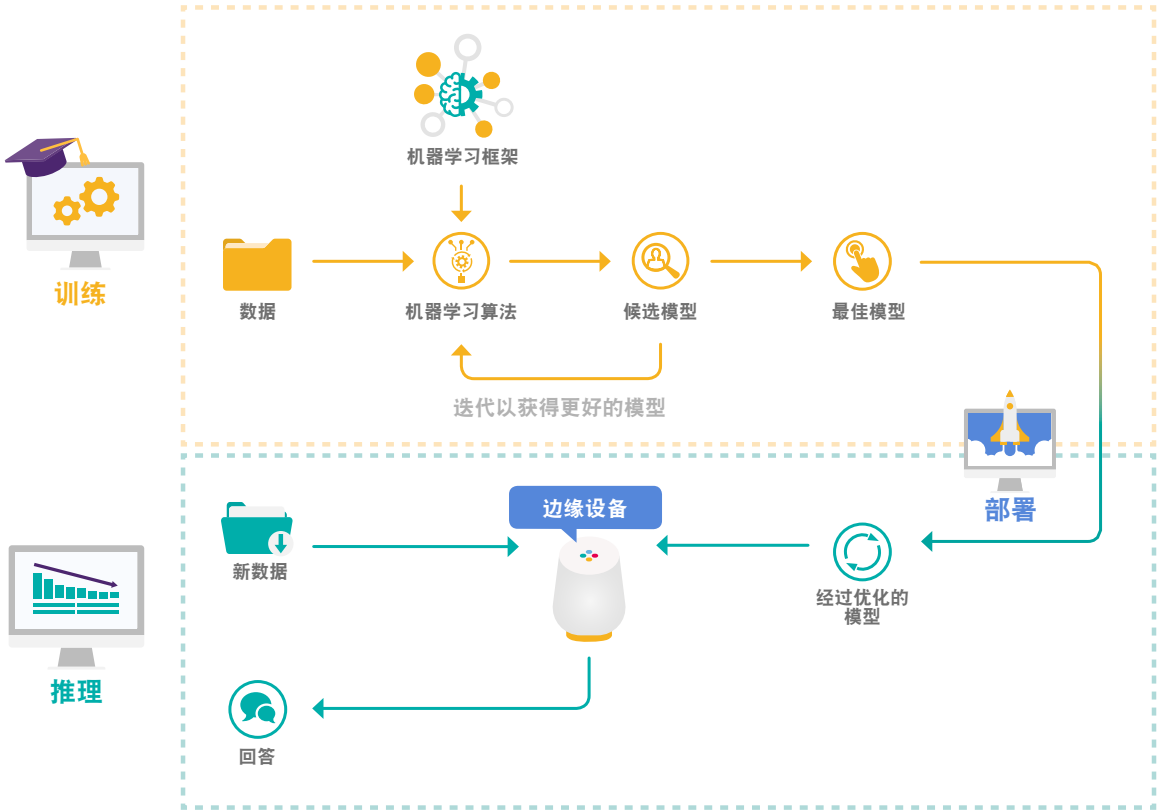
与科研工作相比，如今行业的人工智能方法更加实用。当前人工智能发展以人类推理为指导，以便提供更好的服务或创造更好的产品，而非试图复制人类的思想。但其工作原理是什么呢？我们来看看目前的方法。

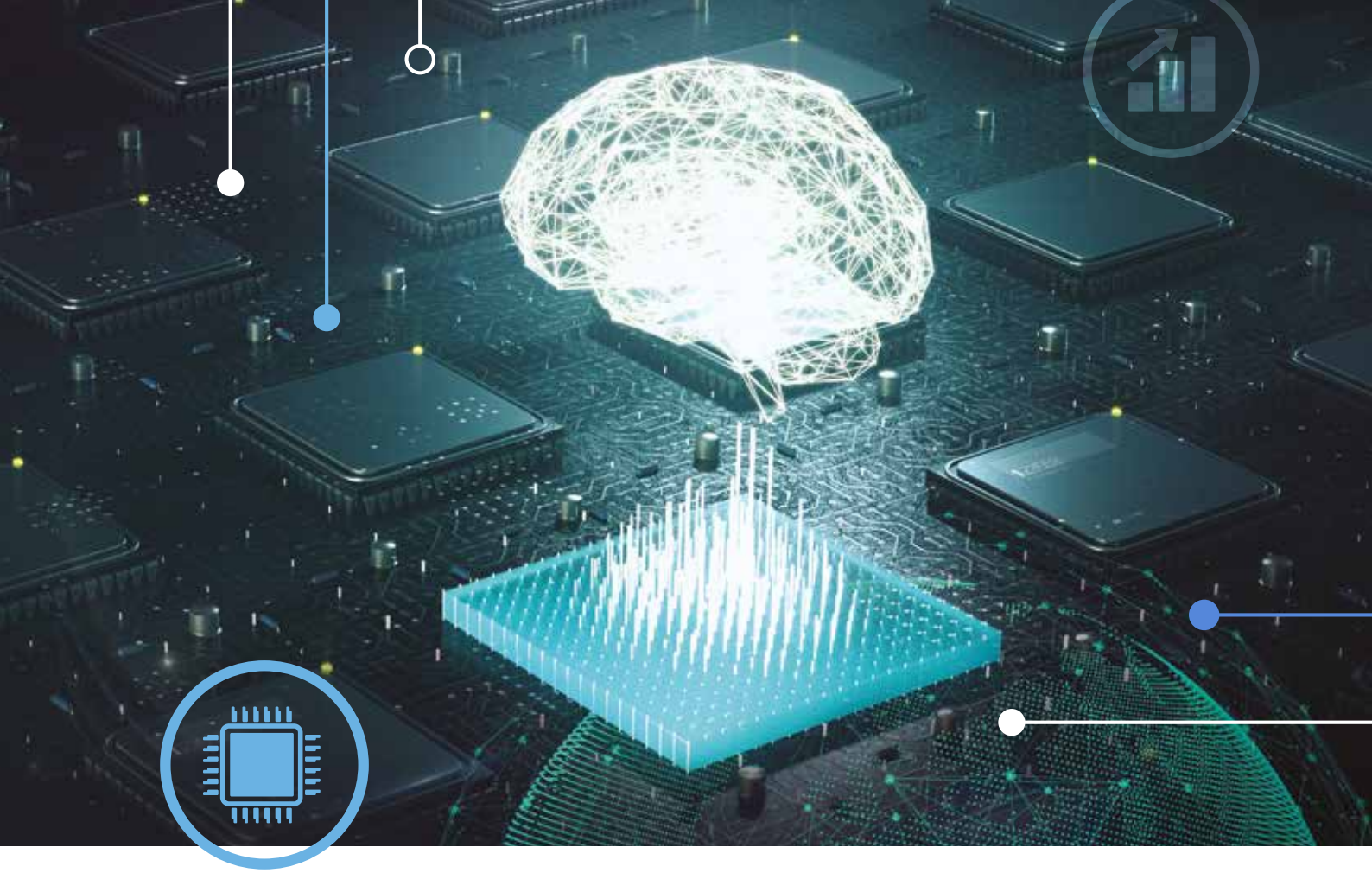
什么是机器学习?

作为人工智能的子集，**机器学习**使用统计学技术赋予计算机学习的能力，而无需明确编程。在其最原始的方法中，机器学习使用算法来分析数据，然后根据其解读进行预测。

关键因素在于，机器经过训练，可从数据中学习，因此它能够执行给定工作。为此，机器学习应用模式识别和计算学习理论，包括概率技术、核方法和贝叶斯概率，这些专业领域技术已成为目前机器学习方法中的主流。机器学习算法并不遵循静态程序指令，而是利用输入示例训练集来构建模型进行运算，以便做出数据驱动型预测并输出表示出来。

计算机视觉是最活跃、最热门的机器学习应用领域。计算机视觉是指从现实世界中提取高维数据，以生成数字或符号信息–最终以决策的形式呈现。然而，就在不久前，为了让机器实现高级模式识别技能，需要进行大量手写代码。操作人员必须提取边缘以定义对象的开始位置和结束位置，应用噪声消除过滤器或添加几何信息，例如提取给定对象的深度信息。事实证明，即使借助先进的机器学习训练软件，让机器真正理解其环境的数字再现并不是一项轻而易举的任务。此时，深度学习派上用场。





什么是深度学习?

AIt并不是什么新鲜事物，这个观点已出现了数十年，它是指软件可以在人工“神经网络”中模拟生物大脑皮层的神经元阵列。**深度学习**算法尝试执行该工作，即模仿人类神经元网络的多层结构和功能。从实际意义上来说，深度学习算法学习识别声音、图像和其他数据的数字表示模式。但如何识别呢?

借助算法的最新改进和不断提高的处理能力，现在我们可以对更多层虚拟神经元进行建模，从而运行更深、更复杂的模型。长期以来，贝叶斯方法行不通的原因是，为了计算证据，必须手工执行概率整合。如今，贝叶斯深度学习应用于多层神经网络，以解决复杂的学习问题。

但是现在，我们的工作仍主要集中在“窄”或“弱人工智能”概念领域，即能够和人类一样，或者比人类更好地执行具体任务的技术。例如，用于图像分类或面部识别的人工智能技术可执行人类智能的某些方面，但不是全部智能，或者甚至是多项人类能力的组合。能够执行多项复杂任务的机器，也就是表现出的行为至少像人类一样熟练灵活的机器，被视为“强人工智能”。虽然专家对于强人工智能是否能实现这一问题的意见不统一，但他们并未停止探索的脚步。

自2013年以来，人工智能领域的投资额增长了三倍

现在，随着相关数据量成倍增加，对能够解决数学和计算问题的更高效系统的需求变得至关重要。因此，IT行业的主要公司已将重心转到开发IC和应用方面，他们的目标是**使人工智能成为市场上下一代软件技术的核心**。

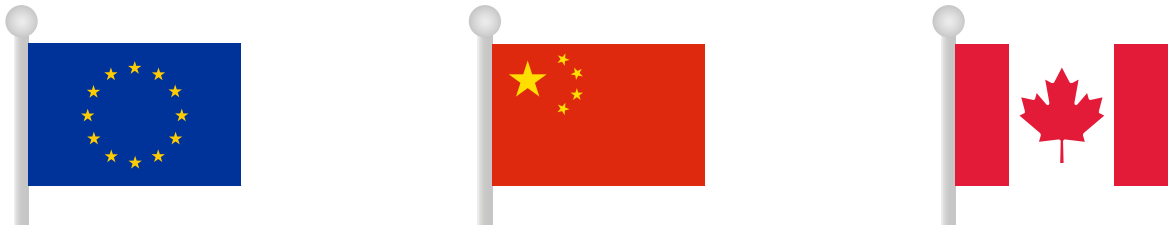
对于技术的颠覆潜力，我们所采用的有效指标是目前对人工智能的投资规模。据麦肯锡表示，2016年对人工智能的投资金额为260亿至390亿美元，其中大部分投资来自Google™和Baidu™等科技巨头。从2013年起，人工智能领域的外部投资额已增加两倍。在中国，人工智能投资额年增76%。中国高科技公司Alibaba™将在未来五年内投资150亿美元，打造全球人工智能技术网络。

在未来5年，阿里巴巴将在**人工智能**领域投资**150亿美元**

2016年，在**人工智能**领域投资了**260亿至390亿美元**

很明显，人工智能初创公司对投资者的吸引力越来越大。对这些企业的投资已从2014年的26.7亿美元增加至2016年的50.2亿美元。从2016年到2017年，全球人工智能初创公司的数量增加了大约141%，从2016年以来，超过1,100家新创办的人工智能公司发起股权融资。

全球政府也开始看到人工智能行业的关联性。欧盟委员会想要使欧盟跻身人工智能行业前列，并宣布提供17亿美元用于这些技术的研发，而中国的计划更加宏伟，中国国家集成电路产业投资基金计划投资470亿美元用于人工智能技术的开发。多个其他国家/地区也制定了国家人工智能计划。美国于2016年5月实施全面人工智能研发计划；英国发起一项计划，旨在改善对数据、人工智能技能和人工智能研究的工作；加拿大宣布为泛加拿大人工智能战略投资1.25亿美元。



17亿美元
用于研发

470亿美元
用于人工智能技术开发

1.25亿美元
人工智能战略

经济前景一片光明

因此，经济预测师看好**新兴人工智能市场**。来自普华永道的研究显示，得益于人工智能，2030年全球GDP可继续提高14%，这相当于额外增加**15.7万亿美元**。“其中，6.6万亿美元可能来自更高的生产力，9.1万亿美元可能来自消费方面的影响。”

得益于**人工智能**，
2030年全球GDP可**提高14%**

相当于**15.7万亿美元**

具体来看不同国家/地区，预计中国（2030年GDP提高26%）和北美（提高14.5%）将获得人工智能的最大经济收益，总计相当于10.7万亿美元，其中7万亿美元将收入中国囊中，而北美只获得3.7亿美元的收益，共占全球影响的约70%。

在北欧，人工智能对区域经济的影响较小，但仍有望占到GDP的9.9%，相当于1.8万亿美元。在英国，到2035年之前，预计人工智能将为经济额外带来8140亿美元（6300亿英镑），使GVA的年增长率从2.5%增加至3.9%。

考虑到对强大计算硬件的依赖性，毫无疑问对经济的最强烈影响预计将出现在IC行业。仅在半导体行业，到2025年，支持人工智能的组件将实现600亿美元的全球销售份额。一个潜力巨大的领域是健康保健市场，从2017年到2027年，人工智能将贡献大约40%的增长，到2027年预计将达到500亿美元。

到2027年，人工智能将为**健康保健市场**带来**近40%的增长**

到**2020**年，德国各行业的人工智能可使德国**GDP提高4%**。

在过去两年间，人工智能在各个行业达到超过26%的复合增长。从战略角度来看，其最大的潜力在于其与物联网互补的特性：虽然物联网可确保持续提供相关数据，但人工智能能力充当系统的推理引擎，可解读端点生成的数据并驱动其功能。

通过在集成技术组合中将物联网与人工智能合并，将创建全新的强大平台，以实现数字业务价值。

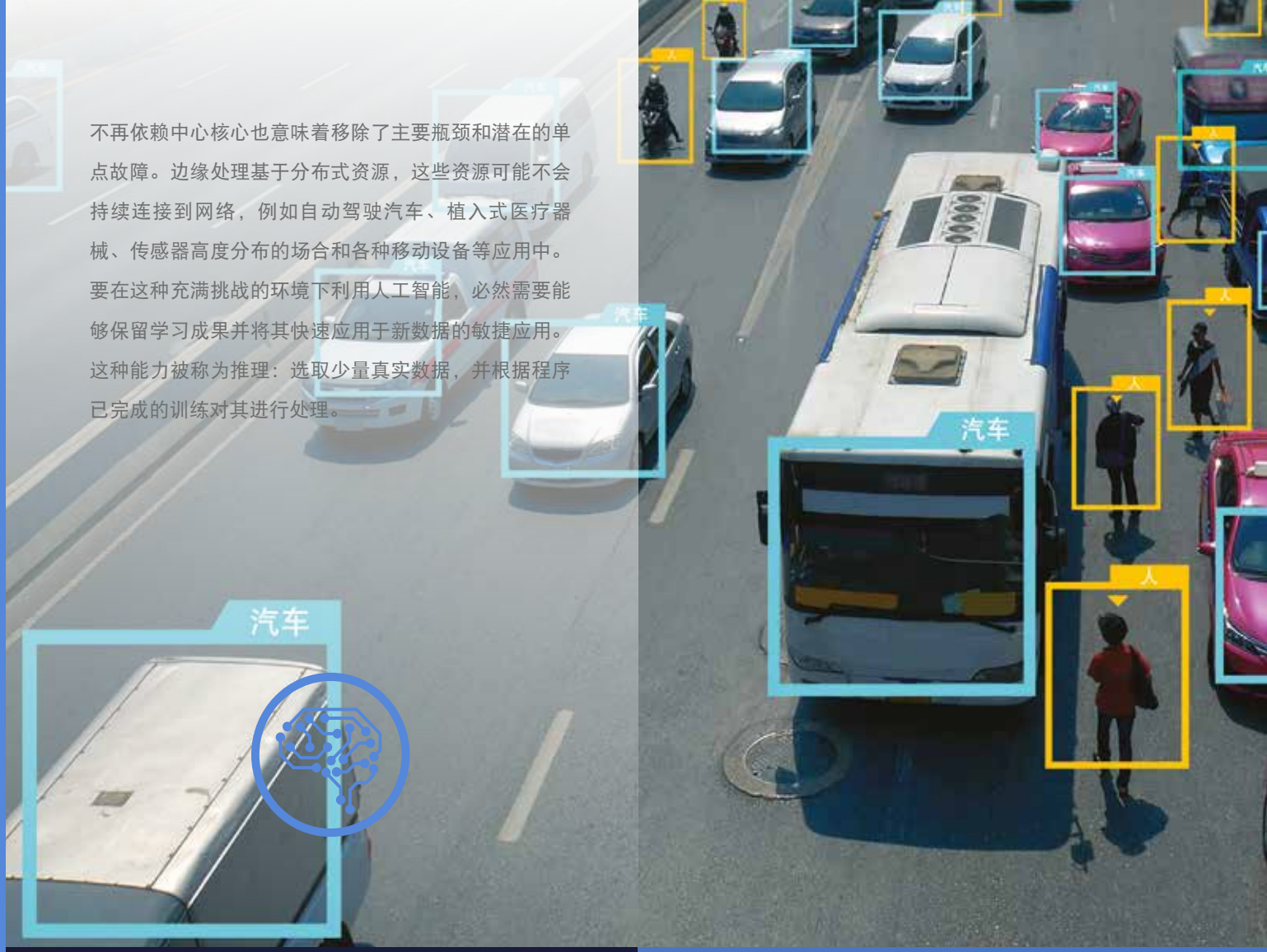
将人工智能技术推动到物联网的边缘节点应用1：高性能处理完成工作

我们已经了解到，要使人工智能发挥巨大潜力，这在很大程度上依赖于恰当的硬件。特别是机器学习，需要巨大的**处理和存储能力**。例如，对于百度的其中一个语音识别模型，一个训练周期不仅需要4 TB的训练数据，还需要20 EFLOPS的计算能力，相当于每秒2000亿亿次($2x10^{19}$)数学运算。由于其对强大硬件的需求，现在人工智能仍主要局限于数据中心。

通过分离人工智能与数据中心并将其推动到物联网的端点，我们将能够充分发掘其潜力。这正是恩智浦的工作。

我们来详细了解一下要求。如今的物联网生态系统已亲眼见证其带来的颠覆，即，数据处理从互联系统中心到网络边缘的转变。边缘处理已取得控制权，将计算应用、数据和服务从一些中心节点（“核心”）转移到互联网外围。物联网设备在外围通过各种传感器（例如，视觉、语音、环境）与现实世界建立联系并输入数据。通过在边缘处理该数据，要移动的数据量大幅减少，从而提高隐私性、减少延迟并改进服务质量。

不再依赖中心核心也意味着移除了主要瓶颈和潜在的单点故障。边缘处理基于分布式资源，这些资源可能不会持续连接到网络，例如自动驾驶汽车、植入式医疗器械、传感器高度分布的场合和各种移动设备等应用中。要在这种充满挑战的环境下利用人工智能，必然需要能够保留学习成果并将其快速应用于新数据的敏捷应用。这种能力被称为推理：选取少量真实数据，并根据程序已完成的训练对其进行处理。



要在边缘环境中支持推理工作，需要经过优化的处理架构和硬件，对处理容量、能源效率、安全性和连接性的特定要求随之而来。恩智浦开发的高级IC产品组合可解决现代边缘环境的挑战，在边缘机器学习领域树立了领导地位，尤其是在处理推理任务方面。事实上，我们位列全球人工智能芯片公司的前三名。

对于边缘的人工智能应用，关键设计目标是平衡系统成本与最终用户体验。例如，基于机器学习的人工智能微波炉可在1-2秒内识别食物。但是，停车信号识别、正在过马路的行人或检测车内手握方向盘的司机是否打瞌睡，则需要更快的处理速度。企业若要增强其人工智能应用组合，可扩展处理器和软件支持是关键，因为它们可以帮助开发人员为一系列广泛的特定人工智能应用部署理想IC。

恩智浦的产品组合涵盖现代人工智能应用所需的几乎所有MCU和应用处理器产品组合：

产品名称		人工智能应用
	i.MX 8M系列	用于高级音频、语音和视频、语音控制、语音协助
	i.MX 8X系列	安全性经过认证，性能高效，适用于汽车、工业和消费类市场
	i.MX 8系列	用于高级图形、图像和高性能计算，适用于汽车、工业和消费类市场
	跨界的i.MX RT	用于音频子系统、消费类和健康保健、家居和楼宇自动化、工业计算、电机控制和电源控制
	i.MX 6、7和8	用于消费类市场和智能家居、物联网云集成
	具有低功耗Arm® Cortex内核的Kinetis®和LPC MCU	具有出色的性能效率的内核、可扩展存储器和集成安全功能。适用于对称加密的片上硬件加速可减少CPU负荷、简化实施、削减软件开销，并允许系统更高效地执行
	Layerscape®产品	QorIQ®通信处理器产品组合提供无与伦比的深度和广度。基于Arm内核技术的下一代QorIQ Layerscape系列处理器，将我们的产品组合将高性能集成到更小的尺寸 - 从功耗受限的网络和工业应用，到需要高级数据路径和网络外围接口的全新虚拟化网络和嵌入式系统
	S32 MCU和微处理器单元	用于汽车和工业应用，为实现高性能和高能效提供最佳架构。旨在解决当前及未来的连接和安全挑战。用于辅助驾驶和自动驾驶的汽车系统是人工智能的主要部署领域。对于传感器信号处理，S32 IC系列提供特定领域的推理解决方案，如雷达、光学传感器和动力传动、车辆动力和车辆网络连接解决方案

量子计算：创建强人工智能的灵丹妙药?

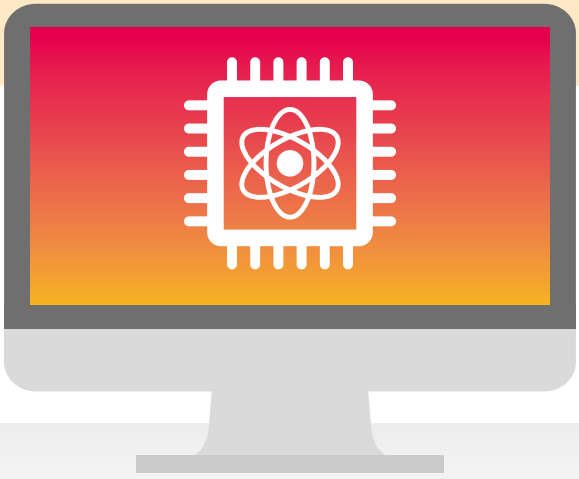
为实现加速计算，量子计算机直接呈现了一个难以想象的巨大的**应用空间** - 奇异的量子力学世界。量子计算机并不像传统数字计算机那样使用由0或1表示的位来存储信息，而是使用量子比特(qubit)，将信息编码为0和/或1。

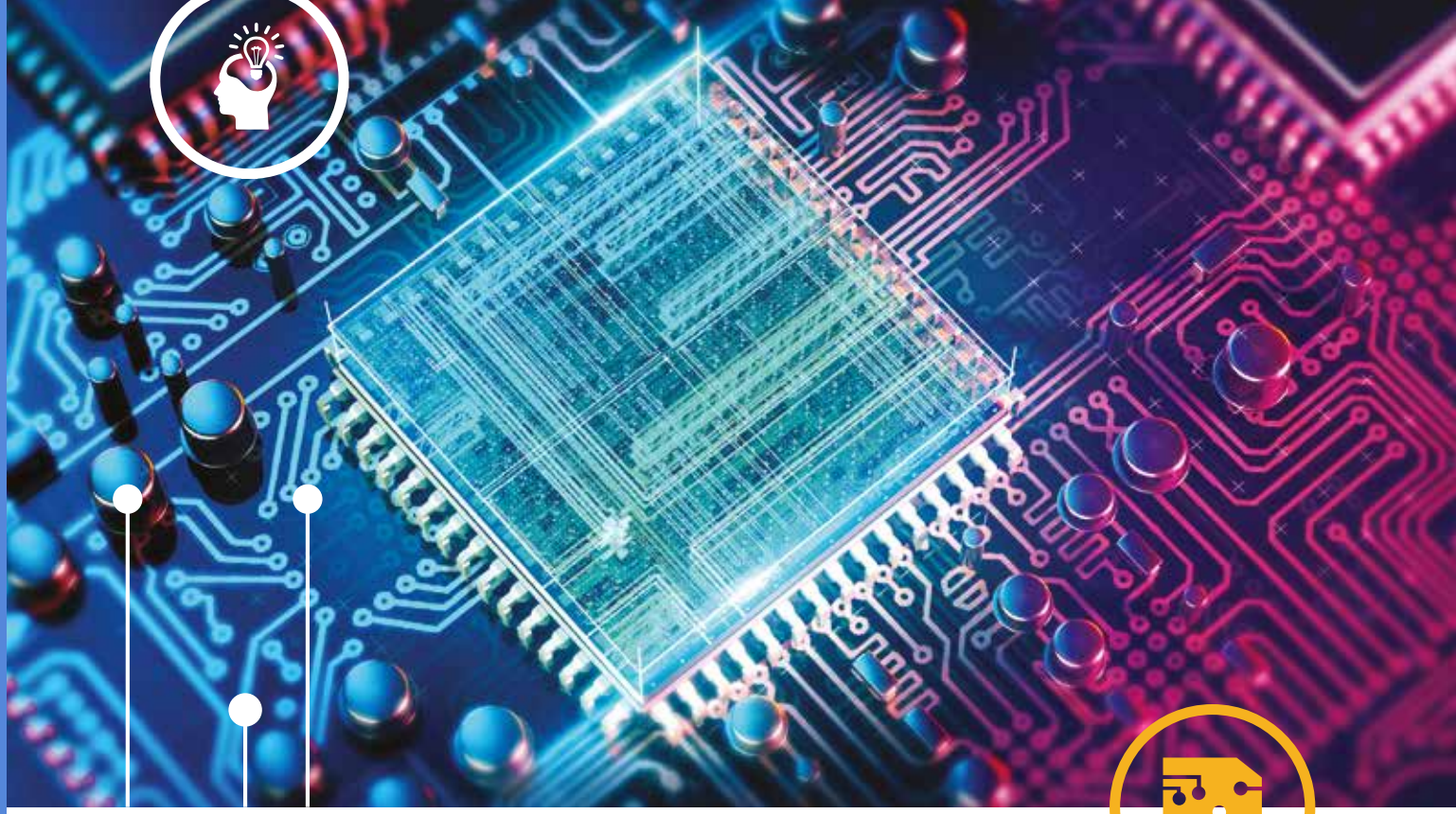
这种叠加态以及纠缠和隧穿等其他量子力学现象，使得量子计算机能够同时操控大量的状态组合。人工智能极需快速处理能力，而量子计算能否为实现强人工智能铺平道路？答案既肯定，也否定。

其实，在过去十年里，量子计算已经从有关其真实性的猜测和争论发展到小型的原型演示。概念不仅得到验证，使用数十量子比特构建的计算机器也已投入运行。然而，对于量子计算机，这种扩展能否继续保持下去以达到或超越经典计算机的功能，这一点仍是未知数。与量子计算机扩展相关的根本问题，导致科学家们无法明确判断是否可以构建出更大的计算机。

量子计算机的一个本质特征是，它们只适用于特定类型的计算问题。普通计算机使用的所有任意算法并非全都适合量子计算机。到目前为止，只开发出了少量能在量子计算机上运行的算法。其中就包括Grover算法，这种算法可显著加速超大量数据的非结构化搜索，在人工智能领域具有巨大潜力。如果量子计算机有朝一日能够广泛部署，预计它们将与普通计算机相互补充，而不会取代普通计算机。

也有人猜测并认为量子计算机会破坏传统加密系统，如公共密钥算法（RSA、Diffie-Hellman、椭圆曲线）和对称加密（如3DES和AES）。撇开关于对这种说法的严重质疑（来源于量子计算机的概率特性），即使它真的能够破坏加密系统，那也是很久以后的事了 - 2030年左右。





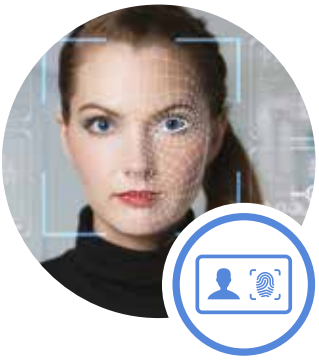
将人工智能技术推动到物联网的边缘节点应用2：专用机器学习环境

为构建具有先进功能的**创新人工智能应用**，开发人员通常需依赖一种能够将专用功能轻松集成到消费电子、工业环境、车辆及其他嵌入式应用的机器学习软件环境。但是，若要大规模推出基于人工智能的业务模型，并使所有垂直市场的数十亿最终用户都能用上人工智能应用，行业首先必须**克服过去的限制**。

为此，恩智浦开发了机器学习硬件和软件环境，使推理算法得以在现有架构内运行。借助其机器学习环境，恩智浦为其众多设备提供了大量易于实现的机器学习功能 - 从低成本MCU到突破性的跨界i.MX RT处理器和高性能应用处理器。该机器学习环境提供全套即用型方案，允许在宽广的范围内选择最佳计算元件：从Arm® Cortex M和A内核到高性能GPU与数字信号处理器(DSP)和用于执行高级数据处理的自定义加速器架构。

恩智浦机器学习环境有助于机器学习在视觉、语音、路径规划和异常检测领域的应用快速增长，并支持集成平台和工具，以便在这些引擎上部署机器学习模型，包括神经网络和经典机器学习算法。

恩智浦机器学习环境支持：



视觉

语音

路径规划

异常检测

对于将机器学习集成到应用的客户，机器学习环境所包含的软件工具，允许他们导入自己预先训练的机器学习框架。对于高性能数值计算，通过从他们自己的首选开源软件库中导入，如TensorFlow™或Caffe模型，设计人员可以将这些模型转换为经过优化的推理引擎。利用工具，客户可以在云端训练模型，导出这些模型，并在集成到边缘应用的恩智浦芯片内进行部署。

为了满足广泛的客户需求，恩智浦还创建了一个不断扩大的机器学习合作伙伴生态系统，将客户与配套技术联系起来，通过经过验证的机器学习工具、推理引擎、垂直应用和设计服务，加快获利周期。

这只是第一步，因为恩智浦已经开始在其设备中集成可扩展的人工智能加速器，此举将使机器学习性能至少提高一个数量级。作为加密加速技术领域的领导者，对恩智浦而言，为人工智能功能执行相同工作，将进一步巩固恩智浦作为机器学习领域领导者的地位。

人工智能：对物联网安全的意义

每秒钟**发现五个新的恶意软件变体**。全球各个机构每小时遭受100次未知恶意软件攻击。每天有100万个新恶意文件出现在互联世界。

随着越来越多的设备和系统连接到网络，网络犯罪对技术资源和整个社会带来的安全威胁不断增大。

在恩智浦，我们构建了世界上最复杂的一些安全设备。我们在设备内部创建反制措施，以保护设备免遭广泛的逻辑和物理攻击，如旁路攻击或模板攻击。总有一天，黑客将依靠人工智能从安全系统中提取机密和关键信息，这只是时间问题，因为人工智能会增强它们的“学习”能力。我们必须思考并检查我们的防御机制，以对抗这些即将到来的威胁。

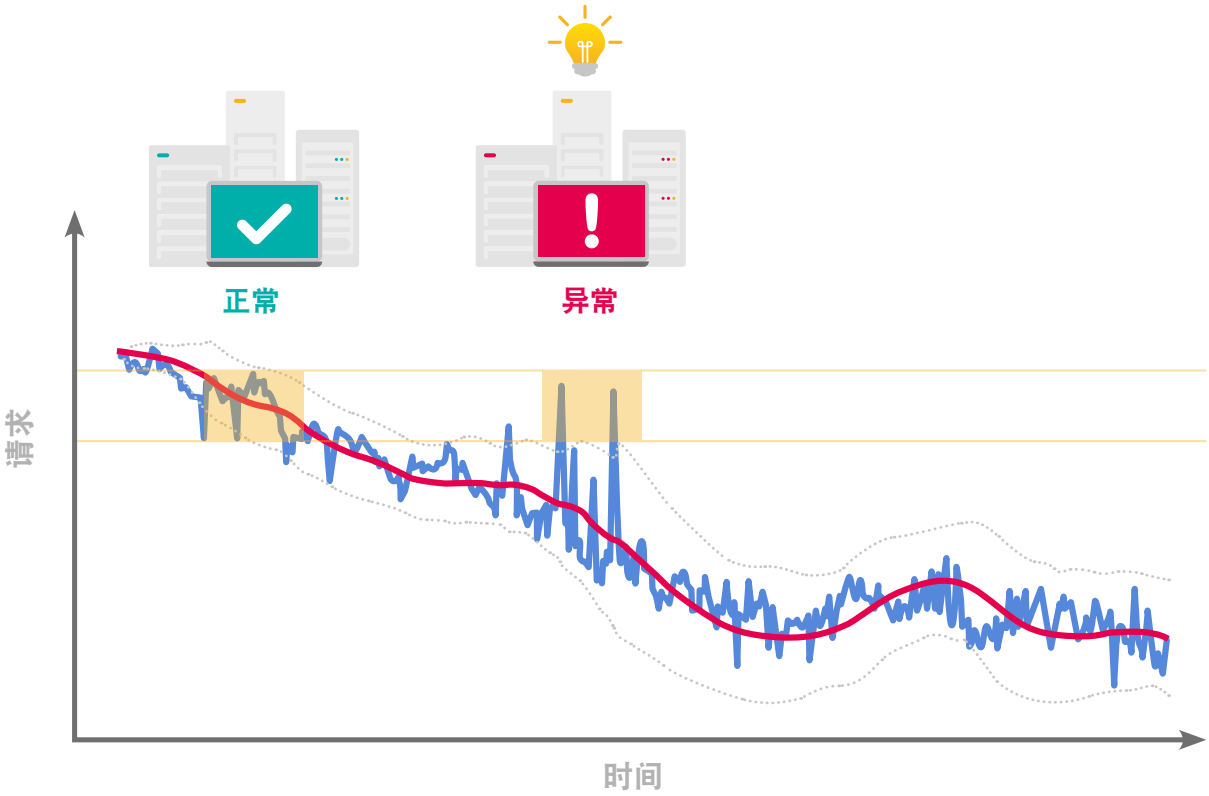
人工智能的进步与网络威胁的发展密切相关。机器学习是一把双刃剑：虽然机器学习可使行业级恶意软件检测程序更高效地工作，但很快，居心不良者也会利用机器学习来增强其攻击能力。事实上，来自阿姆斯特丹大学的一组研究人员近期证实了这一工作原理。白帽黑客通过旁路攻击将信息泄漏到CPU的转译后备缓冲器(TLB)之外，然后使用新型机器学习技术来训练其攻击算法，以提高算法的性能水平。他们相信，机器学习技术将提高未来旁路攻击的质量。

为了防止新型高效人工智能和机器学习技术的出现改变势均力敌的现状，我们必须重点关注如何利用人工智能来提高系统安全性和数据隐私。

机器学习可以增加系统安全性

基于机器学习安全性的一个良好示例是异常检测，即系统“检测”数据流中的异常行为或模式。

以前异常检测通常用于垃圾邮件和恶意软件检测，但通过机器学习可以扩展为在系统中寻找更隐蔽、更复杂的异常行为。虽然监控和防范外部威胁对于实施高效的系统防御至关重要，但很少有组织意识到内部威胁。在埃森哲于2016年开展的一项调查中，他们发现，三分之二的受访组织曾遭遇过来自组织内部的数据失窃。其中，91%的受访组织表示他们不具备识别此类威胁的高效检测方法。机器学习可协助开发高效的实时分析和异常检测功能，以便从系统内部识别并消除基于用户的威胁。



异常检测

异常检测，即系统“检测”数据流中的恶意行为或模式，以前通常用于垃圾邮件和恶意软件检测。通过机器学习，可进一步扩展为在系统中寻找更隐蔽、更复杂的异常行为。

机器学习有助于物联网安全 –
但机器学习本身必须获得安全保障。

安全与机器学习

机器学习用于保障安全

- 用于防御
- 入侵检测
- 欺诈检测
- 控制流保护

在产品中应用机器学习，以帮助击退安全攻击

- 用于攻击
- SCA
- API/协议

抵御机器学习支持的攻击

机器学习的安全性

- 保密性
- 对抗示例
- 完整性与真实性
- 隐私

提高机器学习系统的安全性

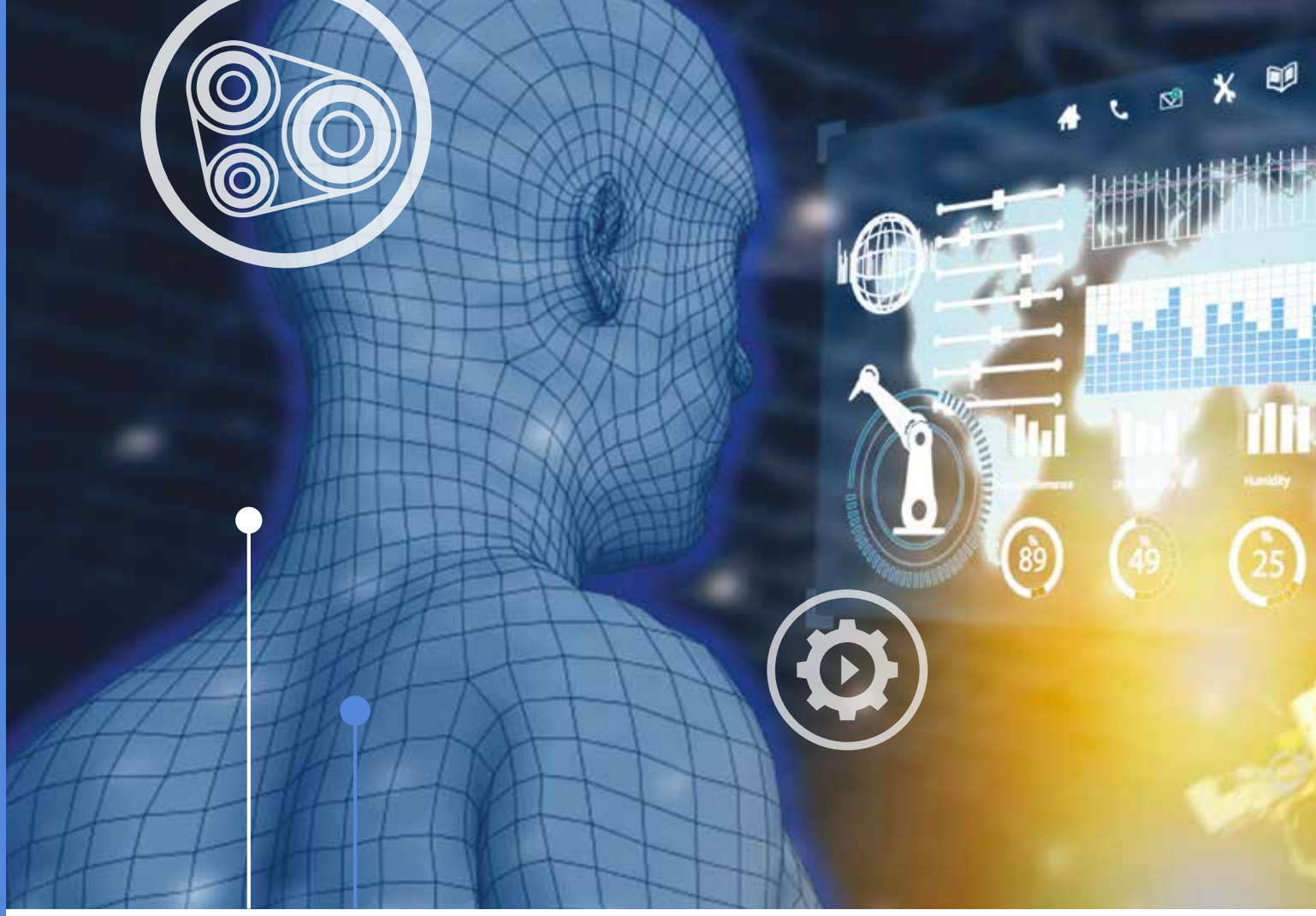
隐私保护机器学习

此类应用很容易识别：人工智能数据提供者（无论是训练阶段，还是推理阶段）不希望在不受保护的情况下提供其数据。随着新的欧盟通用数据保护条例(GDPR)于2018年5月25日生效，处理欧盟公民数据的任何企业必须提供隐私保护，否则将遭受高额罚款。

处理欧盟公民数据的任何企业必须提供隐私保护

如不遵守，将遭受高额罚款

例如，在医疗和金融应用中，企业负责保护提供数据信息用户的隐私。一个典型应用场景是使用患者的病历训练诊断模型。当机器学习模型可公开获取时，相关威胁便随之而来，例如，在之前的场景中，医院执行诊断时。对该模型具有访问权限的恶意用户也许能够分析其参数，并恢复用于训练模型的一些数据。



在工业环境中，数据隐私对系统提供商至关重要的情况也不胜枚举。例如，在预测性维护中，机器数据用于确定现役设备的状况，以精确预测何时应执行维护。与例行或基于时间的预防性维护相比，由于只在需要时执行任务，而且很有可能在系统故障前执行，因此可显著节省成本。相关服务机器的所有者明确希望能够利用生成的数据获益，但同时非常关注自身利益，不愿与使用相同机器的竞争对手分享数据。这样一来，维护服务提供商进退两难。

关键问题在于：企业如何能够继续尊重隐私问题，同时仍允许使用大数据带来商业价值?

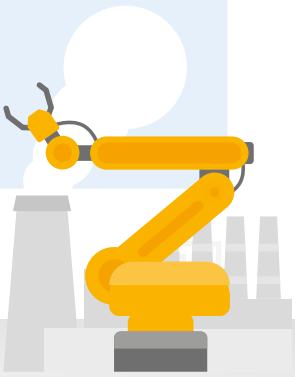
由此产生了同态加密这一研究领域，这是一种能够增强隐私保护的技术，可将数据加密成可计算的加密文本。计算中使用的任何数据仍保持加密形式，只对目标用户可见。加密后的计算结果与同样应用于纯文本计算的结果匹配。在机器学习环境中，如果公司希望将数据传入外部提供的基于云的机器学习模型，则可以利

用同态加密，以避免提供对未加密数据的访问权限，同时仍允许对其数据应用复杂计算。恩智浦继续在该领域引领发展。

基于属性的加密是另一种隐私保护技术，允许按照严格的数据保护和隐私规则运行机器学习程序。恩智浦使用的基于属性的身份验证以IBM® Research开发的Identity Mixer协议为基础，可同时提供强大的身份验证和隐私保护。该技术依赖于灵活公钥（“假名”）与灵活凭据的组合，用户只需分享特定交易所需的信息，无需提供任何其他属性。此外，外部方可以只根据用户的假名来创建用户简介。

优势显而易见：

> “互联网就像是月球表面 - 走过的脚印永远不会消失。借助Identity Mixer，我们可以将其变成沙滩，定期清理所有痕迹，”密码学家兼Identity Mixer联合发明者**Jan Camenisch**说道。



攻击机器学习：训练时攻击

如果攻击者追求**机器学习本身的安全性**，会出现什么情况？

在介绍该领域的潜在威胁之前，我们来简单回顾一下机器学习的工作原理。所有机器学习从训练数据开始。输出是一组参数，其实就是一个模型。在第二个阶段（推理），为模型提供新样本后，模型会推断相应输出。例如，如果机器学习算法是图像分类器，则输入新图像后，模型会返回其类别（例如，图像代表一只猫）。该流程的所有步骤，从训练到推理，都有可能遭受攻击。

甚至在收集训练数据并将数据传入机器学习模型时，也可能发生攻击。虽然窃取数据可能是攻击者的一个目标，但他们的目标也可能是更改数据或操控机器学习模型的结果。要让人工智能模型根据物理现实做出预测，值得信任的训练数据至关重要。这一点有时难以实现。举个典型的例子，使用用户发送的数据对异常检测工具进行训练。如果用户故意发送错误的信息来“影响”训练数据，则可能会导致推理性能不佳，或者甚至机器学习模型在推理时出现故障。

推理时攻击：对抗示例

在推理阶段，用户的隐私也必须得到保证。当推理在隐私或**敏感数据**中完成时，这一点尤为重要。

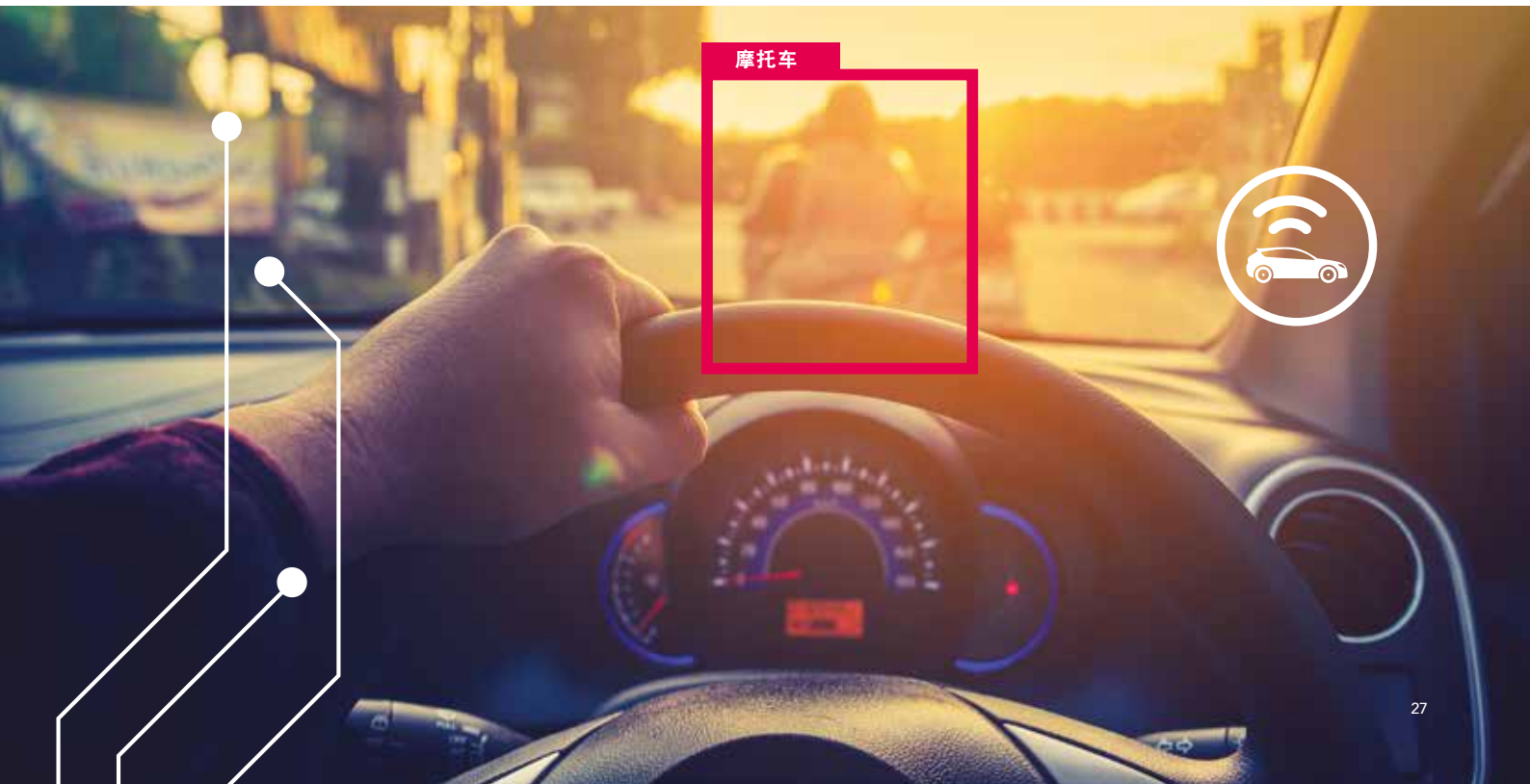
用户也可能是攻击者。作为一种攻击手段，用户可能会采用对抗示例。对抗示例是有效的输入数据，但会导致机器学习模型错误解读该数据。这种看似良性的攻击可带来灾难性后果，举个例子，想一下安全危急时刻的道路标志分类。

研究人员发现，通过在停车标志上粘贴一种特殊的贴纸，可以欺骗图像分类器错误解读或根本不识别该标志。虽然该标志在人眼看来是一个常见的停车标志，但机器学习模型看不到。对抗示例的概念并不陌生。人们所不知道的是其后果的严重性，如在停车标志对抗示例中，可能会导致自动驾驶汽车发生碰撞。

知识产权保护

机器学习模型的价值主要在于相关数据集。训练数据的收集成本可能非常高昂，或者难以获取。当机器学习作为服务提供时，用户只能访问模型的输入和输出。例如，在图像分类器的示例中，用户提交图像，作为交换，用户将获得类别。对用户来说，复制模型本身以避免未来使用付费，这可能相当具有吸引力。一种可能的攻击是，在所选输入数据上查询服务，获取相应输出，并训练获取的数据集，以获得功能相同的模型。

这里罗列的攻击当然并不详尽。多种攻击可以结合，带来更大的损害。例如，模型在被盗后可用于恢复训练数据或制作对抗示例。为了做好充分准备以应对这些不断演变的威胁，人工智能必须成为物联网系统安全中不可或缺的一部分。如果不希望未来的敌人随意使用人工智能机器学习模型的训练和推理，那么必须从一开始就思考“通过设计确保安全”和“通过设计确保隐私”原则。幸运的是，人工智能领域现在汲取物联网安全的经验教训还不算太晚。



展望未来：
人工智能物联网

通过设计具备智能属性的事物并将其连接到**物联网**，我们创建了一个全球资产网络，不仅提高了我们的生活质量，还使我们的生活更方便、更安全。物联网赋予我们眼睛和耳朵，甚至还包括双手，让我们从网络边缘接触到物理现实，在这里我们收集原始数据，将数据流式传输到云端，数据在云端经过处理，获取卓越价值：**适用知识**。

通过增加高性能处理，我们在数据中心和云端执行的信息处理和分析逐渐变少，现在我们更多地在边缘执行这些操作，于是，奇迹出现了。我们亲眼见证了基础设施、行业、个人设备等的神奇变化，这些变化使我们的生活更加多姿多彩：通过所有这一切，我们的生活变得丰富多彩。

智能交通基础设施

智能供应链工厂

移动设备

前端商店

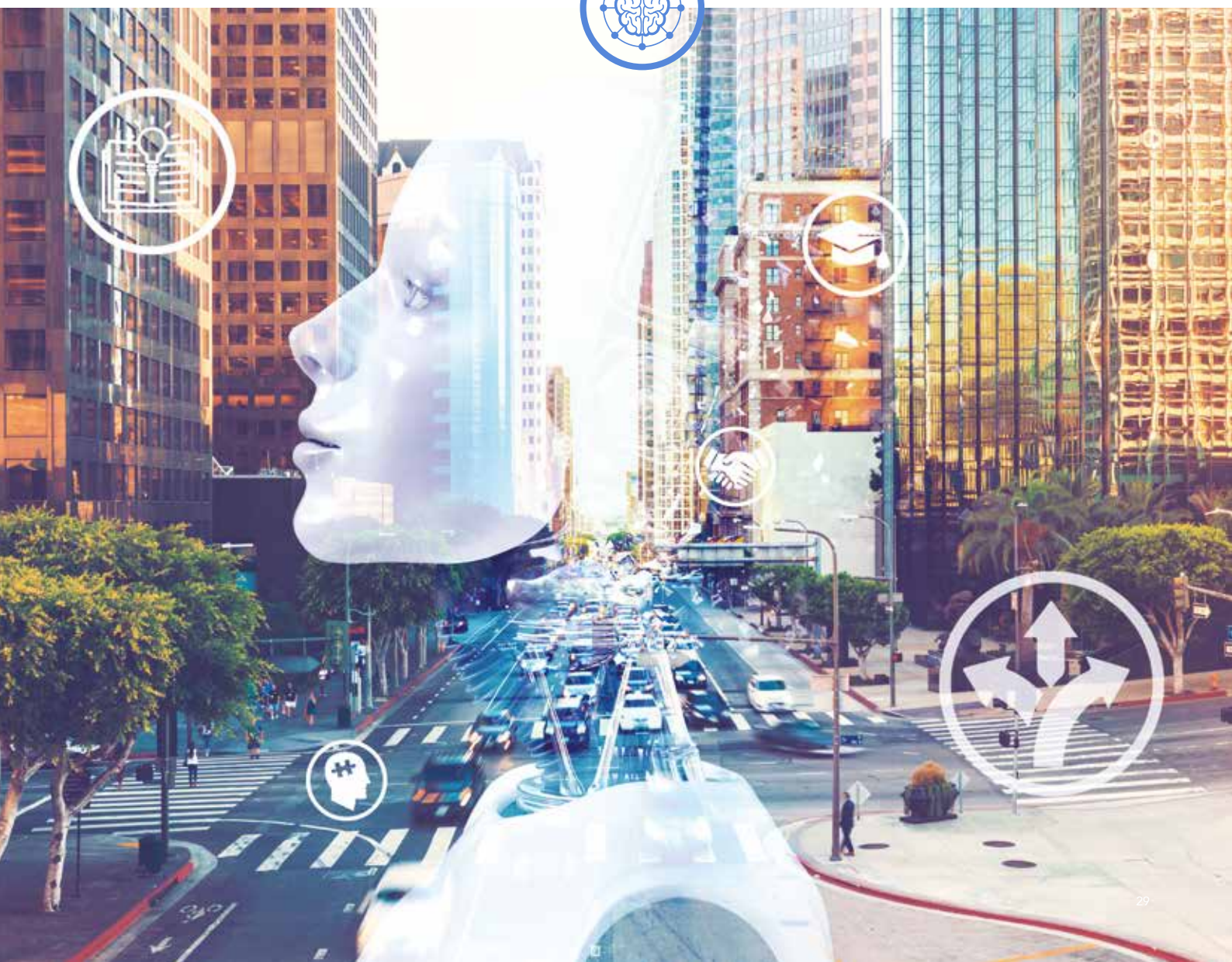
实时

目前，物联网为我们带来了前所未有的机会，让我们能够丰富自己的生活。但是，在实现更强大、更具影响力的目标的道路上，这只是其中一步。我指的是人工智能物联网。

如今的智能物体虽然可以流式传输数据、学习我们的偏好并且可通过应用控制，但它们并不是人工智能设备。它们相互“通信”，但它们不能共同协作。监控疫苗供应冷链的智能集装箱不是人工智能系统，除非它能够“执行操作”，如预测集装箱内的温度变化并自动调节冷却。

自动驾驶汽车或可在海上自主导航的搜索救援无人机其实是人工智能系统。如果它能代表您驾驶或飞行，那么您可以相信，这其中包含一些重要的人工智能能力。通过算法完成语言的读/说/译、预测物体的质量和速度、代表您购买股票、识别面部或诊断乳腺癌都是人工智能的特征。

现在，想象这样一个世界，所有人工智能设备相互连接。通过认知功能（如学习、问题解决和决策制定）扩展物联网的边缘，将使如今的智能物体从纯实用工具实现真正的自我延伸，使我们与现实世界交互的可能性成倍增加。

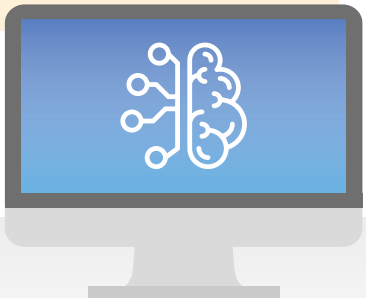


作为物联网的重要组成部分，人工智能是全新应用和服务的基础。例如，Siemens®使用人工智能改善燃气涡轮机的运转。通过从操作数据中学习，系统可以大幅减少有毒氮氧化物的排放，同时提高涡轮机的性能和使用寿命。西门子还利用人工智能系统自动调整下游风力涡轮机的叶片角度，以提高工厂产量。

GE开发了一项基于无人机和机器人的工业检查服务，并使用人工智能自动导航检查设备，从设备采集的数据中自动识别缺陷。在医疗护理领域，位于费城的托马斯杰斐逊大学医院寻求通过自动语言处理改善患者体验，自动语言处理将允许患者通过语音命令控制房间环境并请求各种信息。Rolls-Royce®正在开发支持物联网的飞机引擎维护服务，利用机器学习帮助其发现模式并识别将出售给航空公司的运营见解。在消费类市场中，谷歌的Duplex告诉我们未来是什么样的：这个虚拟助手可通过电话执行“真实”任务，完成安排牙医预约或晚餐预订等功能。这些任务通常需要双方人际互动，但以后不需要了。Duplex的人工智能语音听起来十分自然，以至于接电话的人可能根本没有意识到他们在与机器交谈。

现在，这对未来意味着什么？事实上，即使大量方兴未艾的人工智能物联网应用逐渐兴起，但我们仍然无法揣测未来还会出现什么。有一点是肯定的 - 当今数字时代社会正在发生根本变革。与个人计算机或手机出现时相比，伴随人工智能与物联网融合出现的范式转变将更大。恩智浦正通过边缘的安全互联处理解决方案推动这一转变，从而在未来人工智能物联网中实现无数应用。

要消除其中蕴含的风险，基于“通过设计确保安全”和“通过设计确保隐私”原则的高效安全性将成为关键。如果我们在设计未来基础设施和设备时牢记这一点，那么人工智能物联网必将改变我们的生活。而我们也有责任为人类带来光明灿烂的未来。



www.nxp.com