AI+IoT逐步落地 安全芯片面临新商机

本报记者 陈炳欣

人工智能+物联网(AIoT)时代人们的信息安全将受到更大挑战。以人(PC或智能手机)为节点的信息网络,将扩展到人与物、物与物之间,网络结构将变得更加复杂,节点分布更加广泛,设备自主运行长期无人照护。这些都是容易遭受黑客攻击的因素,而且只要攻破一点,就有可能导致整个安全防护系统遭到破坏。随着AIoT应用逐步落地,安全需求将更加凸显,这吸引了越来越多安全芯片厂商的关注,开始向这一领域布局。

AIoT时代信息安全问题凸显

AI需要基于海量数据进行训练,假如数据遭到污染,或被攻击者获取,也会造成严重后果。

AIoT是由"AI""IoT"两大热门词汇结合而成的概念,在融合了互联智能和主动智能之后,近年来,在安防、教育、社区、交通和家居等多个场景逐步落地,市场开始打开。预计到2020年,将有超过500亿台设备可以实现互联互通。然而,随着市场应用的扩大,信息安全问题也开始显现。《2017物联网安全年报》显示,目前具有安全风险的物联网设备中,路由器和视频监控设备暴露在互联网上的数量最多。国内暴露在互联网上的路由器超过1000万台,视频监控设备达到168万台,一旦被攻击,就将遭受多重风险。

对此,百度AI安全技术总监聂科峰表示,AIoT时代的安全生态更加复杂,整个生态面临着系统性的安全问题,涉及智能设备的传感器欺骗、软件缺陷、数据风险、系统风险、网络风险等多个方面。事实上,现在很多智能设备在裸奔,若不防患于未然,将是非常可怕的事情。

瑞萨电子产业解决方案中心经理周雄健也指出,AI作为一种新型科技,发展极为迅速,难免有些不足,包括AI本身,比如模型和算法并不完善,如果其模型和算法遭受攻击,就会失效。另外,AI需要基于海量数据进行训练,假如数据遭到污染,或被攻击者获取,也会造成严重后果。

然而,随着网络信息安全问题的突出,信息安全需求扩大,相关市场也在增长。Gartner统计,2017年全球网络安全支出为891亿美元,到2025年将达到1800亿美元。RMR(Persistence Market Research)预计2025年全球网络安全市场规模会突破2000亿美元。

芯片厂商开始积极布局

原本的智能卡芯片厂商华大电子、同芯微电子、大唐微电子纷纷向物联网安全芯片市场转型。

在应对AI+IoT设备信息安全防护方面,芯片公司有着大量可做的工作。新思科技(Synopsys)亚太区总裁林荣坚指出:"对于信息安全的理解涉及三个层面:信息的保密性、信息的完整性和信息发送方与接收方的真实性。针对这三个层面的需求,芯片公司可以采用纯软件的方法,在一个暨有的平台上进行数据加密。这种方式的成本最低,并且防护效能也最低。其次,芯片厂商可以在CPU上定制安全性模块,由于部分采用硬件加密,这种方案比纯软件的方案安全性更高。当然,最安全的做法是加载一颗专门执行安全算法的芯片。"

在"2018未来科技峰会"上,恩智浦强调了在AIoT时代重点发力的三大平台:处理、互联、安全。恩智浦半导体全球销售与市场执行副总裁Steve Owen表示,AIoT时代信息安全防护的重要性不断增加,比如,所有互联设备,包括数据的安全备份,以及在使用WiFi的过程当中,要确保每个结点敏捷流动的过程都是安全的。如果是一辆车,特别是在自动驾驶的过程当中,安全的连接是极为关键的,必须确保车辆跟云端的连接过程免于黑客入侵。

2018年10月,英飞凌科技大中华区安全芯片事业部更名为数字安全解决方案事业部。事业部负责人程佳钰表示,未来将有两个重点方向:一是IP保护。随着数字化,原来不联网、不智能的设备都将加入这些功能。这也意味着制造厂商的研发团队需要大幅增加。英飞凌提供完整解决方案,可以帮助用户在很短时间里,用安全芯片将他们的产品保护起来。二是云计算让所有智能设备变得更聪明,云端是人工智能重要的赋能渠道,这也意味着会有无数设备转移到云上。英飞凌将与云服务商合作,将安全芯片应用于云端。

国内厂商也在积极关注这一市场,原本的智能卡芯片厂商华大电子、同芯微电子、大唐微电子纷纷向物联网安全芯片市场转型。目前国内公司的安全芯片已在安防、智能家居、智能表计等领域得到商用。

智能家居市场受到重视

智能家居是数字化转型中非常典型的案例,随着居住升级需求不断增加,智能家居市场将迎来爆发式的增长。

在AIoT逐步渗透各领域的过程中,智能家居正被越来越多的人们看好,有望成为新的高增长点。在去年召开的2018 MIDC小米AIoT开发者大会上,小米宣布升级AI+IoT核心战略,并推出开发者激励计划。由于布局较早,小米IoT平台已经成为当前世界上最大的物联网平台。目前,该平台的智能设备连接数超过1.32亿台,日活跃设备超过2000万台。

相应的,智能家居安全需求也将得到释放。程佳钰表示,智能家居是数字化转型中非常典型的案例,随着居住升级需求不断增加,智能家居市场将迎来爆发式的增长。未来的智能家庭当中,将产生大量数据。而这些数据的闭环上传下达,信息安全非常重要。如果没有相应的安全保护措施,虽然有很舒适的家,但是你不知道哪一分钟就可能会被破坏。

但是,程佳钰也指出,现在智能家居安保市场面临的一大挑战是缺少行业标准。安全防护首先要有标准,没有标准或者没有一个能够真正引领、指导整个行业的标准,很难真正实现保护的目的。程佳钰建议,应当借鉴智能卡、银行卡领域的成熟作法,将传统领域一些好的经验引入新兴应用领域。

人工智能+安全芯片成为技术趋势

中国芯片厂商在积极迈进AIoT安全市场,将人工智能技术融入安全芯片产品当中,这将是一个重要的发展方向。

智能家居乃至整个AIoT都具有应用面广、场景复杂的特点。"作为一个新鲜事物,面对的安全挑战到底是什么样的?很多都是未知的。作为一个企业,如何引入一个具备安全性的方案和产品,如何管理这个系统,也是重要的挑战。"程佳钰表示。

现在有越来越多企业开始将人工智能技术应用于安全产品当中,利用人工智能所具备的认知、学习、推理能力,去解决网络安全问题。日前,IBM宣布人工智能系统"沃森"(Watson)将在网络安全领域大展身手,打击网络犯罪。谷歌则在加密领域取得突破——谷歌大脑成功开发出两个独立的人工智能加密算法,不但能够防范第三方人工智能的破解,也能够自我学习,破解其他AI人工加密算法。

在边缘侧,瑞萨电子推出在嵌入式设备中集成的人工智能技术"e-AI"解决方案,可以将训练好的神经网络模型转换为可在MCU和MPU上运行的C代码。e-AI在为物联网设备提供嵌入式AI技术的同时,也提高产品的安全性。

目前,中国芯片厂商也在积极迈进AIoT安全市场,将人工智能技术融入安全芯片产品当中,这将是一个重要的发展方向。

IC观察

2020年代将见证物联网的实现

物联网缺少合适的环境,难以按照需求增长的速度创造创新和实施机会的状况正在成为过去。现在,一个关键条件逐渐形成:生态系统。由一个个独立应用搭建起来的物联网架构,逐渐发展为成熟、完整的端到端系统,并融入了涉及真实消费者的数据中心和应用场景。这一切得益于推动当前物联网浪潮的四大技术支柱。

传感技术已经相当成熟,现在的传感器拥有超小体积、高效节能、功能全面,因而成为物联网核心的重要资产。按照目前的科技水平,人类世界的任何物理信号都可以转换为电子信号,继而转换为机器能够处理的数字数据,实现任何设想的应用场景。无论是家庭娱乐系统的人类情绪监测,还是智能农业应用中的土壤氮饱和度,抑或是预测性维护场景中的涡轮机震动,数字传感作为人类环境感知不可或缺的一部分,在人类生活和科技之间建立起新桥梁。

第二个发挥作用的推动因素是连接。已经确立并经过现场验证的标准目前覆盖了整个连接范围,从NFC等超短距离连接到中等距离(WiFi、Thread、Zigbee、V2X),再到广域网和整座城市(Lte、LoRa)。在广域网领域,5G承诺即将兑现。目前,第一批5G基础设施试运行方案已在欧洲、中国和美国推广落实。此外,超宽带(UWB)等更先进而强大的技术也正在实施,进一步缩短连接差距,为全新的应用场景提供支持。

第三大支柱是"边缘":这项根本性创新变革正在将越来越多的智能科技推向边缘。在边缘产生数据并在数据中心处理的旧模式已达到极限。计算将随之迅速转向边缘。实际上,IDC预测表明,仅仅一年之后,就有43%的物联网计算发生在边缘。出现这种趋势的理由十分充分。专用边缘处理可以减少响应时间和网络拥堵。例如,自动驾驶汽车主要依赖于实时处理,以瞬间做出正确的决定。通过专用处理,无需建立低效率和无响应的集中式云数据中心来处理显著增长的数据收集量。专用处理在设备级别更加可靠,更好地保护用户的隐私,因为原始数据不会上传到云端。

一项近期Cisco研究表明,美国只有9%的受访者表示高度信任物联网设备。换言之,在数字时代,如果一个人必须时刻警惕冰箱会不会泄露自己的隐私,又何谈幸福?恩智浦在为安全生态系统提供解决方案方面具有成功经验,例如安全微控制器、NFC、支付、门禁控制、高速网络交换机等,因此我们的工程师和业务人员在创建信任互联网方面发挥了重要作用。这种通过设计确保安全的理念还包含安全制造设计、安全信任配置和安全交付,从而建立起物联网生态系统的第四大支柱。

新的传感技术、跨全球连接、从中心向边缘的转变、通过先进的安全技术保护系统和设备是物联网从探索阶段迈向实际实现的重要推动因素。我们预计到2025年,互联设备将达到750亿台。终端设备可能达到数万亿台,全新的应用和业务模式都围绕着这些设备展开,从中心向边缘的转变将带来巨大的机会。

(恩智浦半导体总裁Kurt Sievers)

(上接第1版)

从冷门赛道的独行者到"AI的珠穆朗玛"

然而,在风口上能够"坚持长期艰苦奋斗"的AI芯片企业犹如过江之鲫,为何地平线能够荣登全球榜单?在接受记者采访中,余凯表示,地平线的核心,即"一核",在于自主研发的嵌入式人工智能芯片。"三翼",即智能驾驶、智慧城市和智慧零售。2017年12月,地平线发布了两款嵌入式人工智能视觉芯片——面向智能驾驶的征程(Journey)1.0处理器和面向智能摄像头的旭日(Sunrise)1.0处理器。

这两款芯片产品是中国最早的一批人工智能处理器。同期,寒武纪3款人工智能处理器推出,面向视觉领域的1H8处理器、面向智能驾驶领域的寒武纪1M处理器以及嵌入到华为麒麟980芯片的寒武纪1H处理器。与之相比,地平线的噱头似乎并没有那么大,但其独有的特点也不容忽视。

余凯认为,站在技术的角度上,硬件一定会成为技术发展瓶颈。为了将软件能力充分发挥,解决更高的计算能力要求,地平线提出了独有的顶层设计——"从软件到硬件一体化"。据余凯介绍,通用的硬件或者通用的算法,效率较低,难以满足客户对终端侧AI芯片及解决方案的"低成本、低功耗、高性能"三大要求。因此,地平线将AI芯片和算法进行深度优化,推出了一体化方案。此外,地平线的"AI平民化"想法同样让人眼前一亮,余凯表示,为了更好地应对性价比要求,地平线选择代替客户去做芯片与算法的整合,这对技术和生态都产生了较高的要求。

"基于芯片,我们将核心能力辐射到不同应用场景,提供针对性的解决方案,也就是三翼——智能驾驶、智慧城市和智慧零售。在这三个业务方向上,做商业化落地,我们希望,基于自主研发的人工智能芯片,打造一个开放的应用生态。"余凯说。

在地平线成立之前,余凯是百度自动驾驶的创始人。在地平线成立之后,余凯将智能驾驶开向了另一个高潮。2019CES国际消费电子产品展上,地平线Matrix自动驾驶计算平台获得了CES创新奖,并首次展出了基于该平台的两款最新自动驾驶解决方案——地平线NavNet高精地图采集与定位方案,以及地平线激光雷达感知方案。

据余凯介绍,2015年,刚刚进入自动驾驶领域之时,地平线是在这条冷门赛道上独行的唯一一家中国AI芯片公司。"之后,行业入局者才慢慢多起来。目前,在自动驾驶领域,地平线已经有征程系列处理器、基于地平线AI芯片技术的Matrix自动驾驶计算平台、驾驶员行为监测系统(DMS)等系列产品和方案。"余凯说。

智能驾驶、智慧城市和智慧零售是人工智能芯片目前最火的应用大方向。其中,以自动驾驶智能芯片最为艰难,交通环境复杂,车辆运行安全性要求较高,余凯曾将自动驾驶智能芯片比喻为"人工智能产业的珠穆朗玛"。但地平线却选择扎根于此,余凯表示,L5自动驾驶的实现不能一蹴而就。"从车联网、ADAS到高精度地图,或者说,从L3/L4到更高级别自动驾驶,这是一个漫长的过程。但每一个环节都需要处理器,自动驾驶汽车其实就是'四个轮子上的数据中心'。"余凯说。

在笔记本电脑时代、手机时代之后,自动驾驶智能芯片将会成为各大科技公司竞争的"第三时代"。因此,地平线在自动驾驶智能芯片领域布局,起跑线上再次体现"视野"。目前,地平线已同韩国SK电讯达成合作,拓展海外市场,推动地平线自动驾驶处理器及方案落地。

从淡化"摩尔定律"到为客户主动赋能

谈到地平线未来发展,余凯表示将沿着既定的发展规划,推动AI芯片和算法的不断迭代升级以及落地应用。目前,地平线已有明确的发展路线图,例如地平线BPU芯片研发路线图。余凯表示,为了顺应AI芯片的发展趋势,地平线将致力于提升产品性能,重点看好三大方向:"软硬结合""边缘计算",以及"场景落地"。

余凯表示,随着摩尔定律加速度的减小,对于芯片工艺制造来说,5纳米的物理制程已接近极限。2018年,联电宣布停止12nm以下先进工艺的研发;格罗方德宣布止步于7nm工艺;就连巨头台积电,5nm的研发也尚未有好消息传出。"物理制程牵绊摩尔定律发展缓慢,单位集成度提升滞后。"余凯说。

如何解决物理制程止步不前成为了地平线关注的重点。余凯介绍,目前业内普遍的做法,即提高其并行度,进入"新摩尔时代"。提高并行度是否真能解决问题还值得商榷,因为并不是所有的计算,均能进行并行操作。"即使可以支持并行计算,那也意味着,硬件构架和软件设计要进行深度结合。"余凯说。

"软硬结合"助力并行计算,而并行计算,简单来说是为了增加算力。余凯表示,计算是智能化的核心,而算力将是第一生产力。"由于实时性、可靠性、数据安全性等要求,计算下沉到边缘终端是时代必然趋势,人工智能时代的到来,要求越来越多的终端设备具备强大的本地计算能力。边缘的人工智能处理器将是未来科技竞争的主战场,是一个科技制高点。"余凯说。

很明显,想要占领这个制高点的前提,是要具备规模性商用。余凯认为,AI芯片的大规模商用需要产生围绕AI芯片的杀手级应用,新的应用能够为客户带来巨大的、前所未有的价值。

"聚焦场景,软硬结合、深度优化、协同设计,将最大程度地提升性能、为客户创造最大的价值。同时,AI应用场景非常丰富,构建开放的平台,在AI芯片上提供丰富的软件、有力的服务,赋能客户在AI芯片上开发出来更多、更丰富的应用,则可以在更广大的场景上为AI落地创造机会。"余凯说。

社长:卢山 社址:北京市海淀区紫竹院路66号赛迪大厦18层 邮编:100048 每周二、五出版 周二8版 周五8版 零售4.50元 全年定价294元 手机报全年定价126元 广告部:010-88558848/8808 发行部:010-88558777 京昌工商广登字第20170004号 经济日报印刷厂印刷