

AI+IoT时代渐行渐近 芯片厂商强化“资安”产业布局



本报记者 陈炳欣 顾鸿儒

人工智能(AI)技术加速了物联网(IoT)的发展。目前整个社会逐步进入AI+IoT时代,越来越多的设备开启了智能化进程。同时,预计到2020年,将有超过500亿台设备可以互联互通。随着AI与IoT的快速发展并得到广泛应用,网络攻击现象也表现得更加突出,网络信息安全受到更大挑战。人们需要安全的AI和IoT设备,而不是一个充满风险的AI和IoT设备。

AI+IoT时代，信息安全风险增加

近年来,随着机器学习、计算能力、存储能力以及云计算等技术发展,人工智能技术呈现出“井喷式”发展,家电、移动设备等各种硬件产品中都开始融入人工智能技术,人工智能的发展已成为大势所趋。但是任何新兴技术都是一把双刃剑,AI技术在为人们提供便利的同时,也为网络攻击者提供了新的标的。

360智能安全研究院院长李康表示,智能和安全已经对抗很多年

了,未来还会一直存在,“安全对抗应该是安全领域永恒的一个主题。”而随着人工智能的不断发展,AI技术与安全问题也开始受到关注。人们在享受语音交互功能的方便快捷同时,带语音识别的智能设备可能被黑客变成窃听器,也面临个人数据泄露、非法获取账号信息等安全威胁。

前瞻产业研究院《2018—2023年中国信息安全行业发展前景预测

与投资战略规划分析报告》对权威机构的数据汇总表明,2018年全球安全市场规模在870亿~1000亿美元之间。其中,IIDC的数据显示,2017年全球机构在这方面的投入已经达到创纪录的817亿美元。预计到2020年信息安全方面的投入将达1016亿美元,复合增长率将达8.3%。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(Persis-

tence Market Research)更是预计2025年全球网络安全市场规模会突破2000亿美元。

瑞萨电子产业解决方案中心经理周雄健表示,AI作为一种新型的科技,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是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。

目前终端产品的安全性设计大多处于初级阶段,厂家更关注夺人眼球的炫目功能,却忽视安全保护。

生物特征识别，将成未来发展重点

在升级AI+IoT设备信息安全防护方面,芯片公司有着大量可作的工作。越来越多的芯片公司开始针对这个领域推出“升级版”的芯片技术,实现更为安全的物联网网络。

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,芯片公司既可以采用纯软件的方法,在一个既有的平台上进行数据加密。这种方式的成本最低,但

是防护效能也是最低的。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。只是这种做法,必然会提高成本,并使芯片面积提高。”

作为嵌入式芯片厂商,恩智浦的产品和解决方案在物联网各个边缘计算领域都有着广泛的应用,同时恩智浦对于信息安全也极为重视。“在过去30年间,安全一直是

们恩智浦的立身之本。”恩智浦半导体全球销售与市场执行副总裁史帝夫·欧文表示。恩智浦的信息防护范围也在不断扩展,如语音、生物识别等的信息安全。在日前召开的“恩智浦未来峰会”上,史帝夫·欧文就指出,生物特征识别将是未来信息安全防护方面的重点,如指纹识别、面部识别,以及语音等,都是需要开始有前瞻性考虑的安全问题。

周雄健也表示:“目前终端产品的安全性设计大多处于初级阶段,厂家更关注夺人眼球的炫目功能,

却忽视安全保护。而且很多厂家对成本敏感,无法接受加强安全性带来成本的大幅增加。目前AI和IoT设备的安全需求还没有规范定义。”在这种情况下,芯片厂商需要投入更多力度提供安全的AI和IoT解决方案。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。

人工智能技术可以解决很多应用安全的问题,比如安全分析、广告欺诈监测、隐私分析等。

AI“双刃剑”，守护“资安”作用同样明显

实际上,AI不只是网络攻击的标的,在信息安全防护方面AI技术也可发挥重要作用。由于网络攻击是不断演变的,防御过程中经常需要面临先前未知类型的恶意软件,而人工智能则可凭借其强大的大规模运算能力脱颖而出,迅速排查筛选数百万次事件,以发现异常、风险和未来威

胁的信号。

如今人工智能成信息安全领域的热门应用,越来越多企业也纷纷采用AI技术抵御网络攻击。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。而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,而且还能够自我学习,破解其他AI人工加密算法,人工智能系统在加密通信时甚至都不需要“温习”人类的加密算法!在物理和虚拟世界,人工智能武器的军备竞赛即将打响!

人工智能技术可以解决很多应用安全的问题,比如安全分

析、广告欺诈监测、隐私分析等。北京大学郭耀教授指出:“应用在访问用户数据前会有一个非常长的条款,利用人工智能技术就可以对此进行聚类分析,然后对比相似功能的应用,如果100个应用做同样的事情,其他的都不需要电话号码,而有一个需要,那肯定是有问题的。”



《物联网与人工智能应用开发丛书》书评一： 电子工程师需要终身学习

本报记者 陈炳欣

现代人们的生活节奏不断加快,工作岗位更迭频率也随之增加,加之电子信息技术革新的脚步加快,终身学习逐渐成为电子工程师的必修课,如手机芯片便经历了由多片到单片的变化,目前的SoC作为系统级集成电路,能在单一芯片上实现信号采集、转换、存储、处理和I/O等功能,将数字电路、存储器、MPU、MCU、DSP等集成在一块芯片上实现一个完整系统的功能。它的制造需要涉及深亚微米技术、特殊电路的工艺兼容技术、嵌入式IP核设计技术、测试策略和可测性技术、软硬件协同设计技术和安全保密技术等。

物联网被认为是继计算机、互联网和移动通信之后信息产业的新一轮浪潮,未来5~10年将会对人们的生产、生活产生深远影响。特别是当人工智能技术蓬勃发展起来之后,物联网与人工智能相结合,让IoT在社会当中所能发挥出的边际效应得到进一步扩展。融合了AI技术和IoT的智能物联网,将产生更多力度提供安全的AI和IoT边缘端,再通过大数据分析,以及更高形式的人工智能,形成智能化的应用场景和应用模式,服务实体经济,为人类的生产活动、生活提供更好的服务,实现万物数据化、万物互联化。集成电路技术亦将伴随应用端的新变化新需求产生新的变革。对于电子工程师来说,了解AI+IoT技术发展脉络,补课“加油”,非常必要。

《物联网与人工智能应用开发丛书》由工业和信息化部人才交流中心、恩智浦半导体合作编著,内容涉及安全应用与微控制器固件开发、电机控制与USB技术应用、车联网与电动汽车电池管理、汽车控制技术应用等物联网与人工智能应用开发的多个方面,对于专业技术人员的实际工作具有很强的指导价值。

物联网和人工智能时代,嵌入式开发模式正在发生变化:传统的寄存器编程方式虽然方案简单、高效,对硬件资源要求低,但无法适应当今MCU系统日趋复杂,开发周期紧迫的要求;而基于SDK的调用函数库编程能够提升开发效率,降低人力成本,改善产品可靠性,已经成为嵌入式固件开发的必然趋势。为了顺应32位MCU固件开发趋势,很多技术厂商推出了集

赛灵思与华为率先推出

云端实时视频流解决方案

本报讯 10月12日,自适应和智能计算的全球领先企业赛灵思公司(Xilinx)、华为和NG-Codec今天宣布开发中国首款云端高效率视频编码(HVEC)解决方案。该解决方案独家采用赛灵思Virtex UltraScale+FPGA和NGCodec的全新H.265视频编码器。该技术将进驻华为云FACS(FPGA加速云服务器)并在年底前投入使用。这将在中国的可扩展云基础设施中实现首个使用FPGA的广播质量级的实时流媒体解决方案。

赛灵思云视频高级市场营销经理Sean Gardner表示:“把赛灵思功能强大、灵活应变的FPGA技术与NGCodec全新HEVC编码器相结合所形成的这种独特组合能实现一系列以往无法实现的解决方案。华为率先把这种解决方案运用在了自己的云基础设施上,并把该技术引进中国——世界上规模最大的实时视频流市场,华为引领了这个行业的发展。”

在中国,视频流是一项主要工作负载,企业正在纷纷努力推出基础设施,以满足强劲视频流快速增长或者高峰需求。传统上,企业采用GPU运行HVEC,但

成式的开发软件和工具,为用户提供嵌入式开发所需的外设驱动、协议栈操作系统、IDE和相关工具。恩智浦半导体推出的MCUXpresso软件和工具开发套件就是具有代表性的一种。《嵌入式微控制器固件开发与应用》以MCUXpresso驱动API为线索,以基于ARM Cortex-M内核的LPC5411X为例,从最基础的上电驱动和时钟控制开始,展示MCU各个外设的编程与应用。

USB作为一种通用的标准通信接口,由于其良好的数据传输性能、低廉的成本和出色的可扩展性,在人工智能和物联网时代,已经成为大量的数据交换和传输的重要通道,被广泛应用。但与其他总线协议相比,由于USB在物理信号和协议上更加复杂,开发难度更大。《微控制器USB的技术及应用入门》和《微控制器USB的信号和协议实现》,一书从USB项目应用角度出发,系统地介绍嵌入式USB接口的硬件、软件和认证方面的技术;一书关注USB底层的信号和协议,从实践出发,结合实际的示波器波形图和USB协议分析仪提供的记录信息对USB的信号和协议进行系统的讲解。

自动化、联网化、电动化成为汽车行业发展的三大趋势,《智能网联汽车的网络安全技术及信息安全》关注智能网联汽车的网络技术及信息安全,通过对汽车网联技术的需求与技术分析,提出相应的网络安全解决方案和建议。《电动汽车电池管理系统的设计开发》立足三重维度与全产业链视角,解析整车系统、动力电池系统,及BMS系统的国内外产业及技术发展现状与未来的发展趋势。智能网联汽车的智能、节能与驾驶安全,目标的实现都需落地在车用电机执行器上。《车用电机控制与实践》从最基本的电机运行原理开始,包括工作原理、电路原理和程序原理,然后深入介绍涉及各种电机的算法和实现。

智能物联时代,电子信息技术更新速度不断加快,涉及基础性的,与应用更加贴合的的知识,同时涉及大量碎片化信息。为了应对挑战,电子工程师几乎需要随时充电,保持所学知识的不断更新换代,《物联网与人工智能应用开发丛书》则提供了一个相对系统全面的资料库,它同时也是“工业和信息化领域专业技术人才知识更新工程”培训用书。

赛灵思与华为率先推出 云端实时视频流解决方案

赛灵思FPGA能以相同的视觉质量将比特率降低35%-45%,从而带来了带宽和存储成本的巨大改善。

华为云商业计算服务域项目的FPGA加速云首席架构师赵刚表示:“为了在这个生气勃勃、迅速发展的市场里扩大我们的份额,服务提供商必须提供一流的最终用户体验。其他技术无法满足我们的这个标准。如今,我们的高性能流解决方案让它变为了现实。”

华为云HEVC解决方案能以每秒60帧的速度实现1080p画质,未来将实现每秒120帧的速率。它能迅速与现有视频工作流程集成,为核心视频功能提速。和赛灵思所有技术一样,用户可以通过更新解码器来提高性能。此外,赛灵思使用开源Ffmpeg媒体框架实现了其技术,从而为所有用户打开了FPGA应用的大门,让更多的开发者可以受益于赛灵思灵活应变异构硬件加速的优势。

2018年10月10日至12日在中国上海世博展览馆举行的华为联接大会上,华为云HEVC解决方案进行了演示。

DRAM与NAND Flash第四季度至明年价格双双走跌

本报讯 根据集邦咨询半导体研究中心最新调查数据,虽然下半年是产业旺季,但市场持续供过于求,DRAM第三季度合约价格季涨幅缩小到仅1%~2%,第四季度可能反转下跌5%,也不排除跌幅持续扩大的可能性,终结价格连九季度上涨的超级周期(super cycle)。而NAND Flash均价在第三季度下跌约10%之后,第四季度因受中美贸易摩擦波及,预估跌幅将大于第三季度,扩大至约10%~15%,渠道市场主流3D TLC颗粒合约价跌幅甚至将超过15%。

DRAMeXchange指出,下半年削弱DRAM需求的主要原因,包括智能手机硬件规格已难以吸引换机需求,导致旺季出货表现平淡;服务器市场出货动能出现杂

音,以及PC/NB市场因Intel平台供货不足而受到冲击等。

而观察下半年的供给状况,虽然各大原厂都意识到2019年供过于求的态势确定,因此试图延后或放缓增加资本支出以及新产能扩产计划。但由于1X/1Y制程的比重持续增加以及良率稳定提升,使得今年第三、四季度的产出持续增加,尤其以1Gb获利能力最佳的服务器内存为最。因此,服务器内存的价格恐怕很快将开始走弱,连带使得整体DRAM平均销售单价下跌。

展望2019年,虽然各家对后续新增产能的计划较为保守,但投片量仍逐渐上升,再加上明年也将持续受惠于1X/1Y制程进入成熟期,DRAMeXchange预计整

体供给位元年产出将成长近22%。明年DRAM价格跌幅仍取决于需求端的变化,尤其是服务器的出货以及单机搭载量是否有足够的成长动能。目前预估2019年DRAM价格年均价将下滑约15%~20%,但如果服务器以及智能手机需求出现重大修正,价格恐怕会有进一步下滑的风险。

NAND Flash市场同样受消费性电子产品需求不如预期影响,而服务器/数据中心对于Enterprise SSD需求虽然稳定成长,但由于产品毛利较高,成为NAND Flash原厂的必争之地,导致Enterprise SSD价格不断走跌。从供给端来看,2018年下半年由于64/72层3D NAND Flash的良率持续提升与产能扩增,主要供应商皆

纷纷上修产出预测。

DRAMeXchange也预期,2019年上半年因处于传统淡季,加上中美贸易摩擦风暴持续发酵,因此对智能手机、笔记本电脑以及平板电脑等主要消费性产品的出货量预估都不乐观,价格持续走跌的可能性偏高。2019年下半年NAND Flash原厂是否放缓各自96层转进速度与新产能扩充的脚步,将是影响届时供需缺口的关键因素。以目前各厂商初步规画来看,2019年第四季NAND Flash整体产能会比2018年第四季增加5%,其中,3D产能将会较2018年第四季大幅增加20%。因此,DRAMeXchange认为,NAND Flash业者未来很可能下修原先对于2019年资本支出的规画。