中国智能家电信息安全发展

白皮书 2.0

前　言

2021 年底，国创中心发布《中国智能家电信息安全发展白皮书 1.0》（以下简称《白皮书 1.0》）以来，人工智能技术飞速发展，为家电行业带来了新的机遇和活力。而家电智能化的发展，也引发了一系列信息安全的新事件新问题，如个人隐私泄露、设备被黑客攻击等，这些问题发生频率越来越高，影响力和危害性越来越大，不仅威胁着用户的安全和隐私，也制约了智能家电行业的健康发展。

随着国内外数据安全和个人隐私保护等各类法律法规要求的不断严格，作为智能家电安全的国家级技术创新服务平台，国创中心深入研究智能家电信息安全的现状、问题及解决方案，结合《白皮书 1.0》，重新修订完善了《中国智能家电信息安全发展白皮书 2.0》（以下简称《白皮书 2.0》）。

本白皮书旨在梳理智能家电信息安全的相关概念、技术、标准和法规，分析当前智能家电面临的安全挑战和风险，总结典型的安全事故和案例，并提出相应的安全需求和建议。在《白皮书 1.0》的基础上，引入了一些新数据、新内容，重塑了逻辑架构；同时引入了新的防护技术与相关标准，为新技术在智能家电中的应用提供了新方向。与《白皮书 1.0》相比主要存在以下不同：

- **普及应用方面。**《白皮书 1.0》主要阐述了家电在技术上的演变与升级，如芯片方面，由原来的单片机升级到系统级的芯片，终端由个体升级到“云、管、端”架构；而《白皮书 2.0》主要从用户需求的角度阐述了智能家电已成为市场的主流，用户需求旺盛，同时详细阐述解析了“端-边”、“边-云”和“端-云”等概念，表达了智能家电技术发展的趋势势不可挡。
- **典型安全事故与需求分析方面。**《白皮书 1.0》主要阐述了近年来由于智能家电存在的安全漏洞和造成的重大损失，分析了其攻击链与风险面；而《白皮书 2.0》主要解析了硬件与芯片、固件与操作系统、通信、应用软件等方面技术安全细节及做好防护的要求；同时更新了近年来发生的重大安全事故，特别是用户隐私安全方面存在的问题与影响。
- **法律法规与认证标准方面。**《白皮书 1.0》主要解析了国内外法律法规与认证标准，如国内的数据安全法、密码法及个人信息保护法，欧洲联盟的通用数据保护条例、加州消费者隐私法，介绍了国内外检测标准与认证机构；而

《白皮书 2.0》主要增加了对 YD/T 4209-2023、GB/T 42015-2022 等《白皮书 1.0》发布后出现的法律法规的解读。

- **信息安全架构方面。**《白皮书 1.0》主要阐述了以“云-管-边-端”体系为主线，聚焦硬件安全、系统安全、通信安全、平台安全、应用安全、数据安全、个人隐私保护等领域的解决方案与措施；而《白皮书 2.0》主要强调了“云-管-边-端”各个环节的关键技术研发与算法创新，以及近年来的新技术，如智慧家居中的人工智能、多方中介计算等技术。
- **安全理念与实践案例方面。**《白皮书 2.0》在《白皮书 1.0》基础上增加了华为——构筑并全面实施端到端的全球网络安全保障体系、中国移动——打造“端边网云”联动的智慧家庭安全运营防护体系两个案例。
- **信息安全技术发展方面。**《白皮书 1.0》主要阐述了物联支付在智能家电安全要求与内生安全可信体系架构的发展，而《白皮书 2.0》增加了隐私计算技术是智能家电信息安全的新导向，强调个人隐私、用户隐私合规是智能家电信息的最为重要的关注点。

通过对智能家电信息安全的全面研究，我们希望能够为政府、企业和用户提供有价值的参考，促进智能家电行业的可持续发展，保障用户的合法权益。同时，我们也期待能够引发社会各界对智能家电信息安全问题的关注，共同推动智能家电信息安全技术的创新和应用，营造一个安全、可靠、智能的家居环境。

本白皮书在编写过程中，也得到了众多政府机构、科研院所、家电企业、安全公司等领导、专家、学者和单位企业的支持和帮助，在此表示衷心的感谢。由于智能家电信息安全领域的技术和标准不断发展，本白皮书可能存在一定的局限性，欢迎读者提出宝贵的意见和建议，以便我们不断完善和更新。

国创中心以智能家电领域卓越的安全引领者为己任，连续发布本白皮书，希望能够在我国家电企业在家电数字化转型中，为智能家电信息安全的发展贡献一份力量，护航我国智能家电行业健康发展，让智能家电更好地服务于人们的生活。

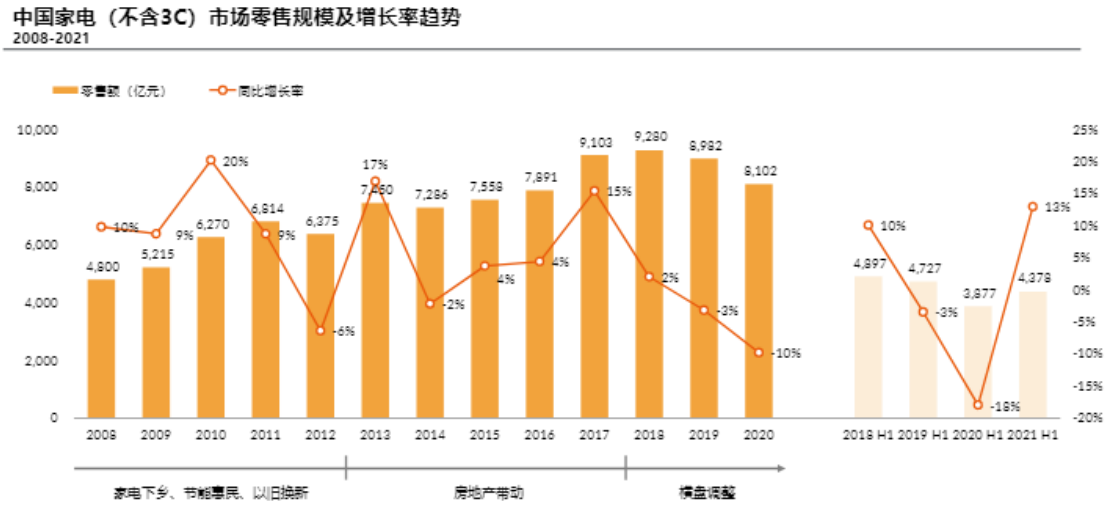
目 录

1. 智能家电的普及应用

1.1 智能家电的应用场景

时至今日，传统家电在逐渐地退出人们的视野，在市场中所占份额，也越来越少,而智能家电则逐渐占据主导地位。与此同时，传统家电的使用风险与弊端仍历历在目，如物理安全防护不足，且缺少智能控制手段的电热毯引发的火灾，又或者是功能单一的传统空调、洗衣机等家电产品，缺少远程控制手段导致的使用不便等实施弊端，已逐渐被迭代迅速的智能家电产品弥补了各项短板。

经历了智能单品的阶段，网络触角不断延伸让万物互联的 AIoT 时代离我们越来越近，我国的家电目前也正向互联互通阶段发展。未来，智能家电将更加人性化、高端化、智能化和人性化，给用户带来更好的消费体验。



（图 1-1）2008-2021 中国家电市场零售规模及增长趋势

2022年8月家电出口商品量值表（人民币值）									
单位：万元									
商品名称	计量单位	8月		1月至8月累积		当月比去年同期±%		累计比去年同期±%	
		数量	金额	数量	金额	数量	金额	数量	金额
电扇	万台	2,007	252,002	27,005	2,810,051	0.4	12.1	-4.1	4.1
吸尘器	万台	1,031	321,811	8,315	2,295,838	-29.1	-19.1	-22.6	-18.7
液晶电视机	万台	905	806,138	6,062	5,477,536	21.2	-20.1	17.1	-16.9
微波炉	万个	459	176,725	4,261	1,593,160	-23.3	-11.4	-7.6	3.1
冰箱	万台	449	414,270	4,043	3,735,539	-23.3	-26.3	-15.9	-14.6
空调	万台	197	247,202	3,715	4,051,059	-16.5	-7.8	-12	-1.9
洗衣机	万台	185	173,061	1,314	1,231,505	8.1	4.5	-11.8	-7.4

（图 1-2）2022 年 1-8 月家电出口商品量值表

结合以上图表数据分析，可以看到在当前国内外家电产品饱和量的情况下，家电市场的国内零售规模仍呈增长趋势，家电出口商品虽然比往年同期有所下降，但总出口量与出口金额仍处于极高水平。不难看出，国内外市场对于家电的需求，已经从增量性需求，功能性需求转向了“焕新”需求。传统家电或者说功能性家电正在被智能家电逐步取代。而智能家电所具备的网络化，智能化，开放与兼容性，以及易用性等特点，结合其具体的通信功能，交互式智能控制以及更为全面的安防功能，已经成为了当今市场的新宠。值得注意的是，智能家电的安全性问题也引起了人们的高度关注。为了避免安全风险，用户应当选择正规品牌的产品，并注意加强设备的安全性保障措施。同时，用户应当定期更新软件和固件，以修复可能存在的漏洞和缺陷。

1.2 智能家电的演变之路

1879 年，美国 T.A.爱迪生发明白炽灯，自此家庭用电这一概念逐步走入人们的视野。在 20 世纪 30 年代，在世界博览会上首次提出了家庭自动化的设想。直到 1984 年，美国联合科技公司将设备信息化，整合化概念应用于建筑，并在美国康乃迪克州出现了首栋智能型建筑，将家用电器，通信设备与安全防范设备各自独立的功能综合为一体的系统，智能家电的概念也从此面世，并随之进入了飞速发展的阶段。

智能家电的发展，离不开芯片的迭代，家电芯片技术的发展演变，实际上是由传统的单片机，到系统级芯片（SOC）的发展演变。单片机出现的历史并不长，

但发展十分快速。1975 年，美国德州仪器公司首次推出 4 位单片机——TMS-1000，标志着单片机正式诞生，而截止到目前，市场上已经出现了 300M 的高速单片机。相比于单片机，SOC 的内涵更为丰富，应用也更为广泛，包含完整的硬件系统及其承载的嵌入式软件。同时它又是一种技术，用以实现确定系统功能，到软/硬件划分，并完成设计的整个过程。SOC 概念的出现意味着在单个芯片上就能完成一个电子系统的功能，这对智能家电起到了举足轻重的支撑作用，也有着不可替代的现实意义。

有基于芯片技术迅猛的创造性革新，我国巨头企业以此为基础战略布局，打通了“云、管、边、端”多层次的管理架构，以此提升资源配置和调度效率。与此同时，以 5G、AI、IoT、区块链、数字孪生等为代表的智能技术，逐步揭开了数据蕴藏的巨大能量，已经成为新一轮技术变革中的最突出变量和推动产业变革的重要生产力，催生了“数据+算力+算法”定义的智能经济，重构了上层应用新体验。

更为具体的说，“云”侧是指计算、存储、网络、算法等一系列资源的集中，以各类智能家电应用场景架设的 PaaS 为例，对“边”侧和“端”侧搜集的用户各类信息。收集信息包含水电气用量、家电操作日志、音视频等，并在“云”侧进行大数据存储、保护、处理、分析和共享。通过大数据、云计算、人工智能等技术，挖掘数据价值，对用户需求、家电操作习惯和喜好等进行学习和研究，为用户提供更为智能的服务以及更为精准的推送，为“边”侧和“端”侧的学习性和智能化提供数据和算法支撑。

“管”侧是整个智能家电系统与云平台之间的通信网络，即“端-边”、“边-云”和“端-云”（部分场景）之间的通信管道。在信息和数据传递过程中，不同的设备、场景、数据类型安全需求不同、安全威胁不同，使用的网络协议也不同。因此，“管”侧需要使用各种不同的通信协议来保障各类数据与信息在传递和流转过程中的机密性、完整性、可用性、可控性和高效性。这些协议包括物联网协议，如 WiFi、蓝牙、红外、ZigBee 以及 NB-IoT 协议等，以及无线通信协议，如 LTE、5G 等。这些协议的选用取决于具体的应用场景和安全需求，以确保信息和数据能够在传递过程中得到有效的保护和管理。“管”侧各类协议就是在智能家电的各类应用场景中，保障各类数据与信息在传递和流转过程中的机密性、完整性、可用性、可控性和高效性。

“边”侧在智能家电的管控和安全中起着重要的作用。它是一个集终端管理、接入认证、安全配置、策略分发与日志处理于一身的智能家电安全中枢，采用网络、计算、存储与控制核心能力为一体的平台，为整个家庭所有智能电器提供近端服务。从智能家电的家庭网络的星型拓扑看，处于中心的位置。它不仅提供终端管理功能，实现智能家电的接入认证，还能对终端进行安全配置，分发策略以及处理日志。因此，“边”侧是智能家电系统中的重要组成部分，为智能家电提供安全、高效的管理和控制服务。

“端”侧是以各类智能家电应用场景为主要构成，典型的智能家电应用场景包括智能娱乐、智能安防、智能控制及智能健康等，场景中由多种智能家电设备组成，目前而言包括智能电视、智能投影仪、AR 设备与智能音响等设备；智能控制场景中的智能窗帘、智能灯泡、智能电饭煲与智能冰箱等设备，家庭智能安防场景中的智能摄像头、烟感报警器、雾感报警器、智能门磁、智能插座与智能门锁等设备，以及家庭智能健康场景中的智能心率检测、智能血压仪与智能穿戴等设备。这些智能家电设备在场景中台的智能控制下，协同构成相对独立的智慧家居应用场景。并且已经实现了每个场景中的每一种智能家电设备，都是以各类功能模块/模组和芯片为硬件基础，架设操作系统，并在操作系统上执行特定的算法程序，实现家电各项功能。同时采集和处理数据，满足用户在娱乐、安防以及智能控制等方面的需求。

结合以上，国内运营商均相继推出自己的智慧家庭解决方案。中国移动推出“和家庭”智慧家庭解决方案，以“宽带+OTT”为切入口，通过家庭娱乐、智能生活与家庭通信渗透全面布局智慧家庭。中国电信形成了以“天翼网关”为基础的智能连接中心、以“天翼高清（IPTV）”为核心的智能娱乐中心以及以“天翼云”为平台的智能数据中心的智慧家庭生态体系。中国联通以“IPTV+OTT”齐头并进的方式为智慧家庭的切入点，全方位构造智慧家庭生态。与此同时，国内各大产业巨头纷纷着眼于建立生态圈进行战略布局。华为发布了 Hilink 连接协议和物联网操作系统 LiteOS，同时联合运营商建立 OpenLife 智慧家庭生态圈。海尔升级自己的智慧家庭方案为 Smart Home，从客厅到厨房，从“黑电”到“白电”，从生活电器到电脑、手机等移动终端，都被紧密联系在一起。阿里巴巴则在打造物联平台“阿里智能”，面向各设备制造商开放协议、云平台和操作系统，并制定了 Alink 协议。此外，腾讯推出 QQ 物联和微信硬件，京东推出 JD+计划。

这些巨头企业在智慧家庭发展中都摆出了开放的姿态，希望能够联合产业链上更多的合作伙伴，从而在行业中形成更大的影响力。

1.3 智能家电技术体系框架

智能家电技术体系框架主要包括 4 层：感知层、网络层、平台层和应用层。

（1）感知层

数据采集主要用于采集物理世界中发生的物理事件和数据，包括各类物理量、标识、音频与视频数据，涉及 RFID(Radio Frequency Identification)、传感器、多媒体信息、二维码/条形码和红外感应等数据采集技术。

传感器网络组网和协同信息处理技术实现传感器、RFID 等数据采集技术所获取数据的短距离传输、自组织组网以及多个传感器对数据的协同信息处理过程。

（2）网络层

网络层也称传输层，实现更加广泛的互联功能，能够把感知到的信息无障碍、高可靠性并且高安全性地进行传送，需要传感器网络与移动通信技术，互联网技术相融合。网络层由各种私有网络、互联网、无线通信网与 M2M(Machine to Machine)无线接入等组成，起到信息传输的作用。该层主要用于对感知层和应用层之间的数据进行传递，它是连接感知层和应用层的桥梁。

（3）平台层

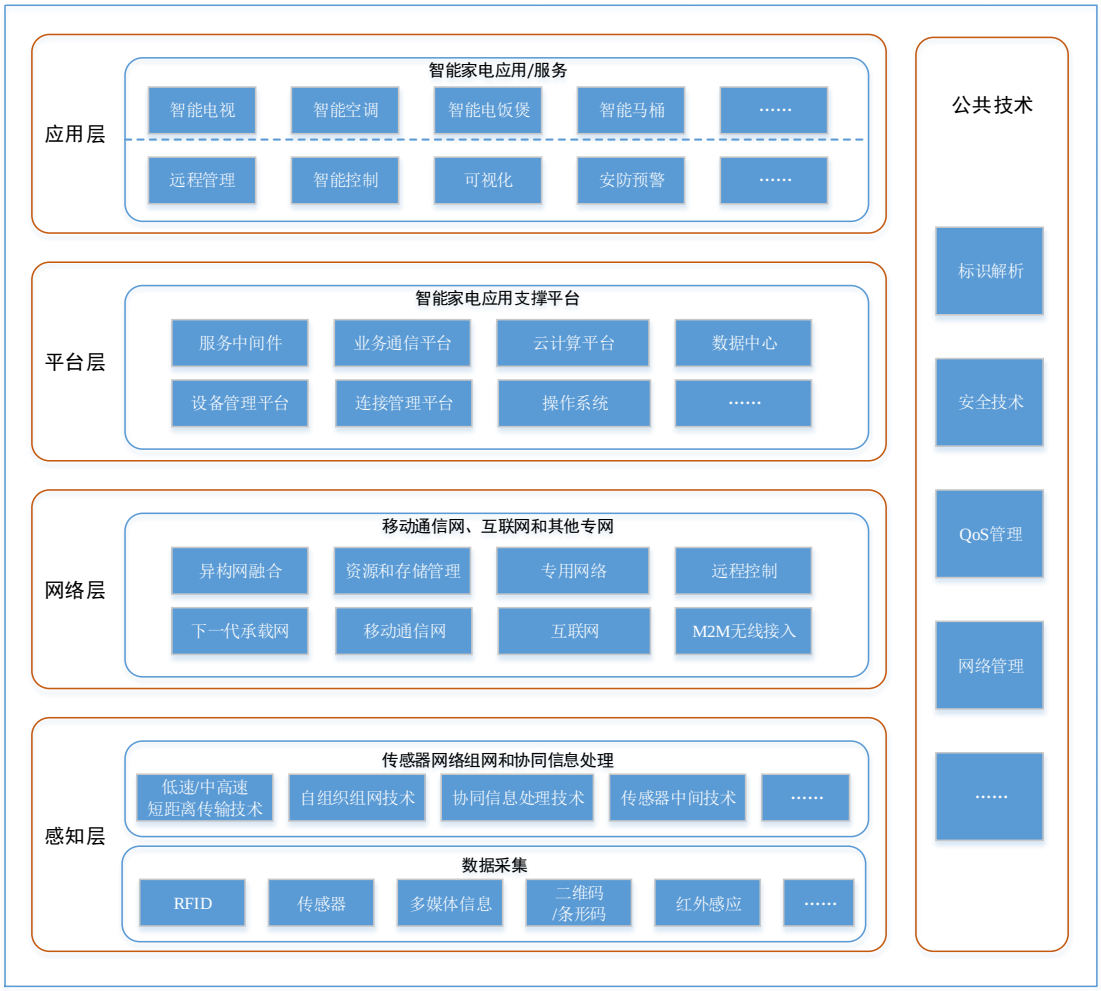
平台层主要是在网络层的基础上，用于支撑跨行业、跨应用、跨系统之间的信息协同、共享以及互通的功能，支撑应用层的服务和程序运行，提供各类应用所需的操作系统和平台。具体包括服务中间件、业务通信平台、云计算平台、数据计算中心、设备管理平台、连接管理平台与操作系统等。

（4）应用层

应用层是智能家电系统的最上层，主要用于实现各种智能家电的应用程序和功能。应用层主要包括智能电视、智能空调、智能电饭煲与智能马桶等智能家电的行业应用，具体功能包括远程管理、智能控制、可视化与安防预警等。

（5）公共技术

公共技术是智能家电信息结构模型的公共技术，具体包括标识与解析、安全技术、网络管理和服务质量(QoS)管理等。



（图 1-3）智能家电技术体系框架

1.4 智能家电发展带来的有益效果与风险

智能家电的蓬勃发展是基于多维的技术革新与进步，相应成果经转化逐步进入市场，实质上是给消费者带来了更多生活方式的选择，不同选择之间的差别甚至可以说是天壤之别。通过远程控制提前开启的空调、通过手机实时监控的摄像头、定时开启的洗衣机以及随时远程控制启停的电饭煲等新型智能家电，所带来的体验感受，是传统家电或者说功能机无法实现，甚至是无法想象的。

智能家电在带来便捷和舒适的同时，也面临着来自信息安全方面的挑战和风险。随着芯片、操作系统、应用程序等各种组件的复杂度和集成度的提高，攻击者可以利用这些漏洞进行攻击，从而威胁到用户的个人隐私和家庭安全。，上层应用多样化，出现了采购商城、物联支付等高安全应用场景，开源和第三方组件的应用扩大了攻击面，安全威胁增加。免费开源的上层应用给了开发者更广阔的

开发空间的同时，也给使用者增加了许多安全风险。应用的安全问题，已经成为整个应用市场发展面临的一个主要问题。各种恶意软件的不断涌现，不仅使得用户的个人信息安全受到威胁，同时也给国家信息安全带来了重大安全隐患。

尤其是用户信息泄露问题频频暴雷，相关新闻屡见不鲜。而信息泄露的风险，以及个人信息的收集、使用、共享在管理以及执行上的混乱，也成为了彼时彼刻用户选择智能家电的最大痛点。

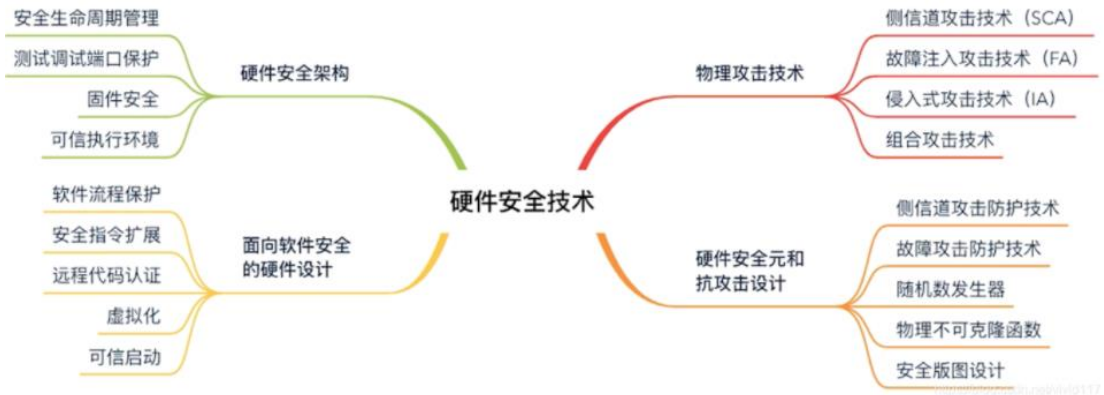
2. 智能家电典型安全事故与安全需求分析

2.1 智能家电存在的安全风险

2.1.1 硬件安全

系统和固件是密不可分的，系统信任由硬件+底层软件共同保护，如果底层有漏洞，那么系统肯定会被破解。因此，硬件安全研究不仅仅局限传统的独立密码芯片研究范畴，在更复杂的、开放的系统中，在硬件安全方面，除了关注秘钥保护，需要注意的防护面还有更多。总起而言，硬件安全的研究内容可分为四个部分，包括硬件安全架构、物理攻击技术、抗攻击涉及以及面向软件安全的硬件设计。

更为具体的说，硬件安全技术包括硬件安全架构、面向软件安全的硬件设计、物理攻击技术以及硬件安全元和抗攻击设计等四个层面。其中硬件安全架构包括安全生命周期管理、测试调试端口保护、固件安全与可信执行环境等；面向软件安全的硬件设计包括软件流程保护、安全指令扩展远程代码认证、虚拟化与可信启动等；物理攻击技术包括侧信道攻击技术(SCA)、故障注入攻击技术(FA)、侵入式攻击技术(LA)与组合攻击技术等；对应的，硬件安全元和抗攻击设计包括侧信道攻击防护技术、故障攻击防护技术、随机数发生器、物理不可克隆函数与安全版图设计等相关技术与设计。



（图 2-1）硬件安全技术思维导图

2.1.2 芯片安全

使用带有读写保护能力的存储芯片确实可以提高设备的安全性，因为硬件级别的保护比软件更难以被攻击者绕过。以 STM32f1 系列单片机为例，设置 RDP（Global Read-out Protection）寄存器的值可以启用读保护选项，从而保护内部 flash 中的固件。

当 RDP 寄存器的值被设置为启用读保护选项时，单片机的内部 flash 将无法被读出，这意味着攻击者无法通过 JTAG 和 UART 接口读取固件。这种保护机制可以有效地防止攻击者通过软件调试和反汇编来获取固件代码，从而保护了产品的知识产权和安全。

安全启动：是一个计算机系统的启动保护机制，旨在确保计算机系统启动时能够正确验证系统的组件和代码，从而防止恶意软件或篡改系统的启动过程。安全启动通常通过以下方式实现：

篡改保护：加密密钥及账户凭证等核心数据，在独立的执行窗口中解密，防止逆向工程，并对核心数据进行监测，防止篡改。

内存保护：内存实时监测，防止缓冲区溢出，内存保护是一种安全机制，旨在防止恶意代码或错误操作对计算机系统造成损害。

设备 ID：由云平台分配并管理，由制造商生产时写入设备，用于安全识别，防止未经批准的设备访问平台；并用于验证每个设备提供了唯一的证书。

外置硬件加密：是一种通过专门的硬件设备（例如安全芯片）来实现的加密方式，可以用于提高家电等电子产品的安全性。安全芯片是一种专门用于加密和解密的硬件设备，通常与主控 IC（控制家电运行的核心芯片）配合使用，以保护家电的关键代码不被篡改。对安全要求较高的家电，配备安全芯片，比如共享家电。配合主控 IC，防止关键代码被篡改；快速认证身份、认证设备。

内置硬件加密：MCU 集成加密 IC，支持从 AES 到隔离加密子系统，以实现更高效、更安全的加密功能。；这种加密方式通常采用对称加解密、非对称加解密、秘钥存储、唯一 ID、加密库、安全启动管理器等。此外，内置硬件加密还可以用于身份认证、数据签名、秘钥管理等多种安全应用场景。

外置 Flash 防读取：对于外部 Flash，首次启动绑定主控 MCU、FLASH，禁止私自更换 FLASH，防止拆装读取固件。

内置 Flash 防读取：对于内部 Flash，通过编程的方式，把 Flash 区域设置为读保护状态，防止拆装读取固件。

2.1.3 固件与操作系统安全

固件通常有 OTA 升级、本地存储升级两种。无论何种升级方式，都应实现升级包的完整性校验与合法性校验机制，防止升级包被恶意替换、篡改。针对目前应用最广的 OTA 升级，需要保证数据传输通道是安全的。通过 OTA 功能进行设备更新时，设备应拒绝旧版固件更新，以防止历史 BUG 或安全风险重新暴露被利用。特殊需求下（如：测试、维修等）可以通过 SD 卡或线刷等方式对固件验签后刷机。

智能家电操作系统主要分为两类：一类主要面向资源受限的智能家电设备，系统架构多采用可配置、高度模块化的设计。编译后的内核通常小于 10kB，这类操作系统普遍没有用户空间的概念，功能较为单一，如 FreeRTOS、Mbed OS 等；另一类则面向资源丰富的智能家电设备，多采用 UNIX 或类 UNIX 作为系统内核，除了提供进程调度、进程间通信等基础服务外，还提供文件系统、设备驱动、虚拟内存管理、网络协议栈等复杂的服务如 Linux、Android 等。

资源受限型操作系统由于 CPU 性能、存储空间、功耗等硬件资源有限，此类操作系统一般提供轻量级的安全防护措施。如基于 MPU（内存保护单元）实现对存储器和外设的保护，可防止用户应用程序破坏操作系统内核数据，隔离任务间的非法数据访问，防止意外的堆栈溢出和数组越界，从而提高系统的健壮性和可靠性；ARMv8-M 新增的 Trustzone-M 及部分 RISC-V 内核具有的 PMP 功能为智能家电设备带来了 TEE（可信执行环境）功能，可更为灵活地实现软硬件资源的隔离，进一步提高系统的安全级别。典型的 TEE 实现有基于 ARM TrustZone-M 的 Trusted Firmware-M(TF-M)，以及基于 RISC-V 的蓬莱 Enclave 和 Keystone。

资源丰富型操作系统多采用 UNIX 或类 UNIX 内核，一般基于 MMU（内存管理单元）实现多进程，进程间实现软硬件资源隔离。与资源受限型操作系统相比，此类操作系统提供完善的身份鉴别、访问控制、安全审计等机制，与传统的桌面操作系统或服务器操作系统类似。另一方面，由于传统的桌面操作系统或服务器操作系统善于保护某一个用户不受其他用户的影响，而智能家电设备基本只运行在 root（超级管理员）用户下，所以智能家电操作系统更加关注相同用户的不同进程之间的访问控制，也需要创新的访问控制机制。资源丰富型智能家电操作系统常见的安全模型及安全机制有：BLP 模型、Bida 模型、Clark-Wilson 模型

与 Chinese Wall 模型等。

2.1.4 通信安全

智能家电通信安全保障体系聚焦家电设备之间、家电设备与家庭网关之间、家庭网关与智能家电云平台之间等通信安全需求，实现身份认证、数据加密传输等机制。智能家电通信安全保障体系在技术方面，包括终端安全密码模块、密码算法和传输协议等安全关键核心组件与协议，需符合国家相关信息安全标准规范以及国家商用密码主管部门的管理规范；在实施层面，产业链上下游只需要较少的改动就能实现快速、安全地接入平台，具备终端身份可信、数据保密性和完整性保护能力。

通信检测可以通过使用无线通信数据读取、分析和注入等工具，对系统和应用进行安全测试，以发现和修复潜在的安全漏洞。针对不同的无线网络类型和功能，无线安全测试可以分为以下几类：

1.蓝牙安全检测：蓝牙是一种近距离无线通信技术，用于设备之间的数据传输。蓝牙安全检测可以测试设备之间的通信安全性，包括蓝牙协议、加密算法、认证机制等。

2.WIFI 安全检测：WIFI 是一种无线局域网技术，用于设备连接到互联网。WIFI 安全检测可以测试 WIFI 接入点的安全性，包括 WIFI 协议、加密算法、WPS 安全设置等。

3.蜂窝网络安全检测：蜂窝网络是一种广域网无线通信技术，用于移动设备之间的数据传输。蜂窝网络安全检测可以测试蜂窝网络的安全性，包括 3G、4G 和 5G 等不同网络协议的安全性。

4.射频安全检测：射频是一种无线通信技术，用于设备之间的数据传输。射频安全检测可以测试设备之间的通信安全性，包括射频协议、加密算法、认证机制等。

5.NFC 安全检测：NFC 是一种近距离无线通信技术，用于设备之间的数据传输。NFC 安全检测可以测试设备之间的通信安全性，包括 NFC 协议、加密算法、认证机制等。

6.模糊测试：模糊测试是一种测试方法，通过故意引入噪声、错误或不确定的数据来测试系统的鲁棒性和容错性。在无线安全测试中，模糊测试可以测试设

备在遇到干扰、信号丢失等情况下的鲁棒性和容错性。

无线安全测试主要测试的内容包括通信协议、数据与业务逻辑等，以确保系统的安全性、可靠性和稳定性。在测试过程中，可以使用各种工具和技术，如漏洞扫描器、协议分析器、网络仿真器等，来模拟攻击行为并检测潜在的安全漏洞。

2.1.5 应用安全

应用安全，顾名思义就是保障应用程序使用过程和结果的安全。简言之，就是针对应用程序或工具在使用过程中可能出现计算、传输数据的泄露和失窃。

随着智能家电内应用流量的不断增加，敏感数据面临着遭受针对企业应用漏洞的攻击风险，数据丢失与泄露所带来的安全性影响非常严重，应用层存在的漏洞，也更容易遭受黑客的攻击。

更为具体的说，应用安全包括 APP 安全与 AI 安全，对于 APP 安全而言，可以通过多方策略进行保障，如服务器报警策略用户密码策略、用户安全策略、访问控制策略和时间策略来保证服务器的稳定性以及限用户安全访问应用程序的安全设置。与此同时 AI 算法的安全性研究需要业界投入更多的资源进行深入的研究，在智能家电中，人脸识别、指纹识别等基于生物特征识别的人工智能技术得到了广泛的应用，但这些 AI 技术无疑也受到了广泛的攻击。比如通过指模、头像照片等可以仿冒主人打开智能门锁，带来严重的安全隐患。AI 算法的强度要求是智能家电领域的研究重点，在智能门锁等高安全要求场景，需要采取多因子认证技术，来提高攻击成本，确保智能家电、智能安防等设备的安全。

2.1.6 数据安全

数据安全性是指在数字信息的整个生命周期中保护数字信息不受未经授权的访问、损坏或盗窃。这个概念涵盖了信息安全的各个方面，从硬件和存储设备的物理安全到管理和访问控制，以及软件应用程序的逻辑安全。数据安全涉及部署工具和技术，以增强组织对其关键数据所在位置及其使用方式的可见性。理想情况下，这些工具应该能够应用加密、数据屏蔽和敏感文件编辑等保护措施，并且应该自动报告以简化审计并遵守监管要求。

1、数据安全：通过管理和技术措施，确保数据有效保护和合规使用状态。

2、保密性：使信息不泄露给未授权的个人、实体、进程、或不被其利用的特性。

3、完整性：准确和完备的特性。

4、可用性：已授权实体一旦需要就可访问和使用的数据和资源的特性。

5、数据安全能力：组织在组织建设、制度流程、技术工具以及人员能力等方面对数据的安全保障。

6、能力成熟度：对一个组织有条理的持续改进能力以及实现特性过程的连续性、可持续性、有效性和可信度的水平。

7、能力成熟度模型：对一个组织的能力成熟度进行度量的模型，包括一系列代表能力和进展的特征、属性、指示或者模式。

8、安全过程：用于实现某一安全目标的完整过程，该过程包含输入与输出。

9、过程域：实现同一安全目标的相关数据安全基本实践的集合。

10、基本实践：实现某一安全目标的数据安全相关活动。

11、通用实践：在评估中用于确定任何安全过程域或基本实践的实施能力的评定准则。

12、数据脱敏：通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

13、数据处理：对原始数据进行抽取、转换、加载的过程。

14、数据供应链：为满足数据供应关系，通过资源和过程将需方、供方相互关联的结构。

15、规程：对执行一个给定任务所采取动作历程的书面描述。

16、合规：对数据安全所适用的法律法规的符合程度。

2.2 典型案例回顾

2.2.1 智能家电信息安全问题严重威胁用户隐私安全

2016 年的 Defcon 黑客大会上，两个不同的演示报告指出：智能门锁的安全性要跟上其方便性还有很长的一段路要走。来自 Merculite Security 的安东尼·罗斯（Anthony Rose）和本·拉姆齐（Ben Ramsey）展示了一些破解智能门锁的技术，他们所使用的工具是价格不到 200 美元的现成硬件。他们测试了 16 个来自领先制造商的智能门锁，结果其中 12 个被成功破解。Quicklock、iBluLock 和 Plantraco 等公司生产的智能门锁以明文形式传输密码，任何使用蓝牙嗅探器

的人都能轻易破解。Lagute、Vians 和 Ceomate 等其他一些公司出品的智能门锁则容易受到重放攻击，这种攻击是在合法用户开锁或者上锁的时候盗取信号，然后在用户离开之后用于解锁。

据报道,在三星智能 HOME 自动系统中也存在漏洞,并可以利用这些漏洞实施远程攻击,包括从世界上任何一个地方远程打开电子门锁。通过获取该 APP 以及 SmartThings 平台验证合法用户所依赖的 OAuth 令牌,即可实施该攻击。攻击者只需要目标用户点击攻击者构造的一条 HTTPS 链接,然后进入一个长得十分像 SmartThings 平台的登录界面,并输入用户名与密码即可。该应用自身有一个漏洞,它允许 SmartThings 页面的地址被重定向到一个攻击者可控的地址,从那时起,攻击者便与用户一样,具有远程访问门锁的权限了。

PCMag 进行了一项调查，发现 68%的用户认为各种智能家居产品会在他们不知情的情况会监听个人隐私对话，并且这些设备背后的运营商会共享数据。而事实上，以上数据的结果是基于只能家电行业迅猛发展以来，不断暴露出的信息泄露时间导致的。

2018 年，研究人员发现 8 款 sony 智能电视中的 3 个漏洞，其中一个漏洞评级为重大，两个高危。这 3 个漏洞都源于 Sony 的 Photo Sharing Plus 应用，app 允许用户通过手机或平板电脑与 Sony 的智能电视分享媒体内容。同年,Consumer Reports 发现三星和 TCL 的两款智能电视存在安全漏洞，攻击者利用漏洞可以控制目标电视，包括换台、调音量、播放 YouTube 视频等。

时至 2018 年 5 月份,中国国际门业博览会上,一名女子仅用一个“小黑盒”,接连破解了数家品牌商的智能门锁，最快不过 3 秒钟时间。“小黑盒”运用的是特斯拉线圈原理，通过电磁干扰使锁具打开，被打开的智能门锁多数是一些生产规模较小的厂家。

2019 年，据中国消费者协会发布的一份 29 款智能门锁比较试验报告中显示，虽然大部分样品智能门锁对于“小黑盒”攻击都已有所防备,仅有一款无生产企业、无产品型号标志的样品被小黑盒攻击后打开，但是，在 29 款智能门锁样品中，48.3%的样品密码开启安全存在风险、50%的样品指纹识别开启安全存在风险，并且 85.7%的样品信息识别卡开启安全存在风险，这其中包括了凯迪仕、顶固等知名品牌的样品。

2019 年 1 月份，安全研究人员发现沃尔玛和百思买等大型零售商销售的热

门联网和智能家电设备普遍存在严重安全漏洞和隐私问题。送检来自不同制造商的智能相机、智能插头和安防产品等 12 种不同的家电，均存在安全问题，包括缺少数据加密和缺少加密证书验证。其中包括 iHome、Merckry、Momentum、Oco、Practecol、TP-Link、Vivitar、Wyze 和 Zmodo 等产品。

作为智能家居的入口之一，正在走入千家万户的智能音箱也曾被曝出隐私安全问题。据彭博社报道，亚马逊的畅销智能音箱 Echo 被曝出严重内幕，称 Echo 的智能助手 Alexa 正成为亚马逊监听用户的工具。消息称，一个由亚马逊员工和一部分外包人员组成的团队每天会对 Echo 用户与智能助手 Alexa 的对话进行录音并对音频进行分析，然后通过转录、标注等方式反馈给软件，该项工作每天需要进行 9 个小时以上，每人每天分析的音频片段达到 1000 条以上，其中不可避免地会有用户的私密语音。

2022 年 7 月，辽宁本溪的羊女士在民宿房间里使用智能音箱时发现，上方的摄像头拍到很多住客的隐私视频。羊女士表示，这个智能音箱有看护模式，捕捉到了六七段自己和朋友在房间内走动的视频，下面还有很多陌生人的隐私视频。资料显示，小度几乎参与了酒店所有的关键服务，从播报信息、客房设备控制、呼叫客房服务到影音娱乐功能等。即便酒店版去除了摄像头，依然有可能得到用户大量隐私信息，包括顾客的声音记录、生活习惯等等。消费者离开后，相关信息的处理直接关系到消费者隐私安全。

2022 年 9 月份，乐歌股份陷入舆论漩涡，被消费者投诉其旗下智能升降台产品有质量问题。消费者称，在某电商平台购买了乐观 a9 智能升降台产品，到手后发现产品的数码屏内偷偷暗藏了一颗摄像头，但是产品本身没有需要用到摄像头的地方且暗藏摄像头，存在隐私泄露风险。事件经媒体报道后迅速发酵，引发广泛关注，引起上市公司股价连续两日下跌，合计跌去逾 10 个点。

2.2.2 基于智能家电网络攻击事件威胁国家社会安全

随着万物互联时代的到来，越来越多的智能家居设备连接到互联网上，与其他通信设备互联互通。由于智能家电设备网络安全的脆弱性，越来越多的黑客将攻击目标对准了智能家电设备。

2016 年 10 月，美国发生了一起全国性的网络瘫痪事件，这导致 Twitter、Amazon 和 Paypal 在内的多家网站无法登陆，两个半小时后，这些网站才开始陆

续恢复。这起事件主要来自于智能摄像头和智能家电等物联网设备。一款叫做 Mirai 的恶意软件感染了大量存在漏洞的物联网设备。被感染后，这些本来为人们服务的设备瞬间变成了僵尸网络中的肉鸡设备，并被用于大规模 DDos 攻击。

DNS 服务提供商 Dyn 公司托管的全球基础设施遭到了大规模 DDoS 攻击，并攻击了一些互联网的最受欢迎的目的地，如 Spotify 公司，亚马逊公司，HBO，Twitter 公司以及纽约时报等机构。Dyn 公司遍布世界各地的 20 个数据中心遭遇到攻击，其中一部分是名为 Mirai 的软件创建的僵尸网络实现的，安全性比较薄弱的 IoT 设备受到影响，如闭路电视摄像机和录像机。攻击者仅仅通过猜测默认密码就获得了这些摄像头的控制权。

无独有偶，新加坡三大电信公司之一 StarHub（星和）也遭受了两次国际黑客网络袭击，导致了新加坡部分宽带用户网络中断。StarHub 公司对中断的网络日志进行了分析，发现其域名服务器(DNS)遭受了“故意并且可能是恶意的”分布式拒绝服务(DDoS)攻击，黑客所用手段的是控制智能摄像头等终端设备发起 DDoS 攻击。

2020 年底，FBI 在发布的公共服务公告中表示：“黑客正在劫持安全性较弱的智能设备，通过家庭监控设备进行 swatting 攻击。”黑客使用了之前在网上泄露用户名和密码，向执法部门举报，谎称受害者正在进行犯罪活动。FBI 表示当执法部门到达住所时，黑客通过家用摄像头和扬声器监视警察，黑客有时还在共享在线社区平台上直播事件。这类“swatting”事件的数量近年来在美国各地有所增加，更有甚者因警察误射毙命。

时至 2021 年，职业网络巨头领英（LinkedIn）在 2021 年 6 月发现，其 7 亿用户的相关数据被发布在暗网论坛上，影响了其 90%以上的用户群。一名自称为"God User"的黑客利用该网站（和其他网站）的 API，通过数据抓取技术转储了约 5 亿用户的信息数据集。接着，他们夸口说，他们正在出售完整的 7 亿客户数据库。尽管 LinkedIn 辩称，由于没有敏感的个人数据被泄露，该事件只是违反了其服务条款，而不是数据泄露。但正如英国国家网络安全委员会（NCSC）警告的那样，God User 发布的一份抓取数据样本包含电子邮件地址、电话号码、地理位置记录、性别和其他社交媒体细节等信息，这将为恶意行为者提供大量数据，在泄密事件发生后制造令人信服的后续社交工程攻击。

2.3 家电信息安全的需求特点分析

2.3.1 亟待强化的隐私保护

根据市场调研，隐私泄露问题已经成为用户选择智能家电的最大痛点，大数据为人类生活带来了技术变革，但同时也对人们的隐私造成了新的威胁。传统的隐私保护机制受到了冲击，强化对个人信息隐私权的保护显得尤为迫切。

信息安全事件频发也反映了智能家电产业建设初期，安全作为基础建设的重要性。智能家电发展到今天，家电厂商不能再以实现基本功能为制造目标，更不能以华而不实的应用实现为设计主体，而要清本正源，关注市场需求。显而易见的，安全作为家电使用的基本需求，是客户在竞品选择中的重要筹码。提高在智能家电信息安全方面的投入成本，从而得到正向的市场回馈，是每个家电厂商应该意识到的重要问题，也是明智的选择。

同时，随着新基建的加速发展以及 5G 网络的进一步普及，基于 5G 网络的智能家电设备的应用会越来越多，IPv6 的使用也解决了多种接入设备连入互联网的障碍，但是失去了网关的保守，设备可能面临更大的安全维系。将来一定会有更多的黑客组织将目标瞄准各种新型的智能家电设备，利用这些智能家电设备上存在的一些漏洞，在这些物联网设备上植入相应的恶意程序，控制智能家电设备发起 DDOS 攻击行动或者直接利用漏洞盗取智能家电设备中的用户隐私数据，甚至是发起一次影响深远的 APT 攻击行动，都将会造成不可挽回的损失。

概括性的说，个人隐私泄露可能存在的不安全因素包括但不限于以下几种情况：移动设备的信息泄露、收集用户数据的上层应用、网络服务信息泄露以及病毒以及木马的恶意攻击。可以说，窃取用户隐私信息的手段层出不穷，而智能家电为用户带来的便利的同时，信息安全也并不能成为便利的代价。随着大众越来越频繁地使用智能家电产品，公民的数据也大量地被储存在企业、组织的数据库中，再加上技术漏洞以及法律制度的不完善，越来越多的个人信息被滥用、盗取甚至被倒卖，这也带来了严重的隐私泄露问题。因智能家电信息安全问题导致的个人隐私泄露事件频发，消费者对此存在持续的焦虑。

公众对家电信息安全和个人隐私保护的需求是，迫切的，仅依靠有效的法律法规来确保公众的信息安全明显是不足的。这也意味着智能家电制造企业需要负担更多的保护数据安全的责任与义务。

2.3.2 法律法规的合规要求

在智能家电的质量安全及电磁兼容发方面，国内对市场销售的电子电气产品，除依据《产品质量法》与《强制性产品认证管理规定》等规章对产品实施强制性认证以外，鉴于智能家居产品的特殊性，也就是其利用无线网络或有线网络实现信息交互，并以此为主导，实现智能化功能的特点，智能家电还要符合网络信息安全方面的相关法规。

《中华人民共和国网络安全法》于 2017 年 6 月 1 日起实施。2019 年 10 月 26 日，中华人民共和国第十三届全国人民代表大会常务委员会第十四次会议，《中华人民共和国密码法》通过。2021 年 6 月 10 日，第十三届全国人民代表大会常务委员会第二十九次会议通过《中华人民共和国数据安全法》，自 2021 年 9 月 1 日起施行。《中华人民共和国个人信息保护法》于 2021 年 11 月 1 日执行。

GDPR 在2018年5月开始强制实施，仅在 2019 年 7 月，依据 GDPR 对企业的罚款总额累计高达 3.6 亿欧元，其中英国航空因数据泄露罚款高达 2 亿，谷歌也因没有充分履行数据处理原则而被罚款 5000 万。

上述法律法规均从不同层面与角度，对智能家电的信息安全提出了更为细化的要求，做到了有法可依、有法必依、执法必严、违法必究。立法程度的完善，是对制造商与客户的法律约束，同时也是对制造商与客户的保护。义务与权力对等，互为依存约束，也为智能家电行业制造了良好的发展环境。

2.3.3 成本敏感特点对信息安全技术的特殊要求

高端智慧家居是高度数据化、信息化的时代产物。未来智慧家居产品要互联互通才可以为人们带来更多便利，在设计上需要更高的安全意识与思维。人们随身携带并使用着各种智能设备和智能穿戴，家中也安装很多智慧家居设备，这些设备通过物联网技术连接起来，为人们的生活、健康、人身财产安全、各种家庭事务提供各种安全保障和便捷服务。一旦某个环节或设备遭到入侵，将会严重影响整个智慧家居网络的可用性和可控性，对用户信息安全、隐私保护甚至是人身财产安全可能带来不可忽视的巨大风险。

然而，从当前新兴智慧家居产业来讲，家电厂商首先需要的是更多的流量和数据来充实产品销售报表，因此智慧家居产品更多地冠以便捷、智能化的功能和体验，而信息安全作为后发事件往往容易在设计和生产中被忽略。另外，信息安

全本身是一门非常专业的技术，大多数厂商的技术集中于家居设备的生产、制造和应用开发，对信息安全技术与知识了解相对匮乏，一方面缺少防御信息和隐私泄露风险的安全意识；另一方面，即使意识到保护隐私和信息安全，也不知如何下手。若寻求第三方合作，无形中加大了智慧家居产品的成本投入。当然，也有部分厂商不仅意识到智能家电信息安全问题还在技术上进行了研究和开发，但往往采用的是独立协议独立接口，自家产品自成体系，虽然保证了自身系列产品的安全，但严重限制了未来智慧家居设备的扩展与互联互通。用户要么不能随意选择家电产品，要么在家居事务管理中需要操作各厂商搭建的各类平台和程序，违背了智慧家居灵活和便捷的设计初衷。

同时，2021 年 3 月 5 日，2021 年国务院政府工作报告中指出，扎实做好碳达峰、碳中和各项工作，制定 2030 年前碳排放达峰行动方案，优化产业结构和能源结构，家电信息安全的解决方案必须立足于服务该目标，不能顾此失彼，因此增加家电功耗。

2.3.4 企业打造智能家电安心品牌的市场需求

随着智能化水平的提升，智能家电市场规模迅速增长。数据显示，2016-2020 年我国智能家电市场规模不断增长，中商产业研究院预测，2021 年我国智能家电市场规模将达 5760 亿元。

中国是全球最大的家电产能基地之一，2019 年，我国家电行业的出口规模达 3034 亿元，同比微增 0.9%。2020 年新冠肺炎肆虐全球，海外居家生活时间延长，提升了海外市场对家电产品的需求。2020 年我国家电行业的出口量达 338997 万台，同比增长 14.2%;出口额达 661.28 亿美元，同比增长 23.5%。最新数据显示，2021 年 1-4 月我国家电行业的出口量达 120480 万台，同比增长 45.9%;出口额达 310.64 亿美元，同比增长 61.9%。

随着人们生活水平的不断提高，家电智能化的发展，未来智能家电市场将不断加速发展，市场需求持续扩大。特别是近年来随着农村市场的开拓，家电下乡等影响下，农村智能家电市场规模也随之不断扩大。未来几年农村智能家电市场仍有扩大的空间。

与此同时，随着中国消费者收入水平的提升，消费能力逐步提高。在当下，消费者的品牌意识越来越强，对于产品质量和品质的要求也在逐步提升。在良好

的市场前景下，品牌的影响力对于开拓市场、占领市场并获得利润起到了举足轻重的作用。

品牌的影响力来自于消费者的评价与认可，而安全无疑是消费者首要关注的问题，也是企业首要解决的问题。千里之堤毁于蚁穴，品牌的影响力塑造非一日之功，任何有关安全的问题出现，均会为整个品牌带来难以估量的损失。

3. 智能家电信息安全相关法律法规与认证标准

3.1 国内对于智能家电信息安全约束性法律法规

自 2016 年以来，国家先后颁布《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等一系列法律法规，用以规范网络安全、密码使用、数据安全、个人信息保护等，保障公民的网络权益和个人隐私安全。家电作为一个充分竞争的行业，就目前而言，监管仍比较薄弱。但这些法规给智能家电行业的监管提供了充分的依据，让智能家电每个链条中参与者权益的保护实现有据可查、有法可依，对推动智能家电信息安全的正规化、标准化、合法化影响深远。

3.1.1《中华人民共和国网络安全法》

自 2017 年 6 月 1 日起，《中华人民共和国网络安全法》（下称《网络安全法》）正式实施，《网络安全法》明确了网络安全相关的部门、企业、社会组织和个人的权力、义务和责任。规定了国家网络安全工作的基本原则、主要任务和重大指导思想、理念。

《网络安全法》不仅对个人、组织等的网络安全行为做了规定，还明确了相关主体的网络安全责任，这就为企业网络安全保护提出了更高的要求。企业不仅要进行定期的网络安全体检、不断完善网络安全建设，还需要履行网络安全保护义务、保护数据和用户隐私安全等。《网络安全法》加大对“关键信息基础设施运营者”安全合规的责任，这就对构成关键信息基础设施运营者提出了专门的要求。如今的众多智能家电或物联网企业运营管理的联网设备数量众多，达到日均访问量、注册用户数、活跃用户数或数据中心规模的标准或者运营过程中收集存储的个人信息数达到 100 万条以上；或涉及的业务量大，达到数据量或交易额的标准；或涉及关系民生的重要信息系统、控制系统的，就构成了《网络安全法》规定的关键信息基础设施运营者条件。

《网络安全法》还对网络产品、服务做出规定，网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规

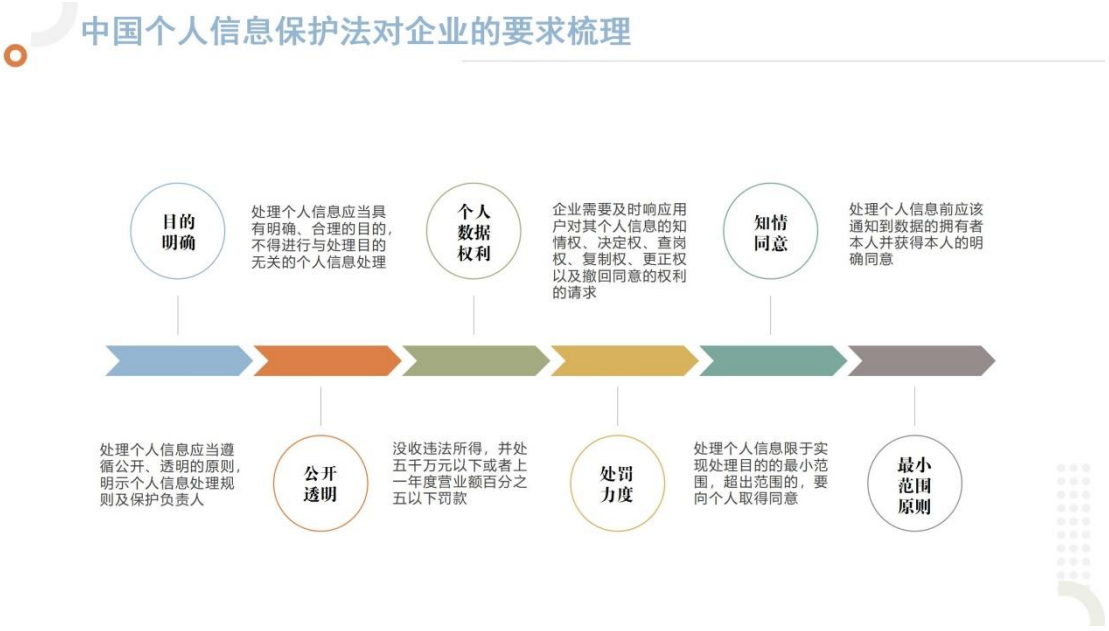
定及时告知用户并向有关主管部门报告；网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

这就对智能家电上层应用的安全提出了更高的要求，厂家通过终端和应用为用户提供更便捷的服务的同时，还要注重上层的应用的健壮性和安全性，纠正智能家电厂商重体验轻安全的认知，督促厂商将安全问题摆上法律的高度。

总体来说，《网络安全法》对智能家电厂商构成关键信息基础设施运营者的，提出了更为具体的要求。收集、使用个人信息，应当遵循合法、正当、必要的原则，注意收集、处理的个人信息及重要数据本地存储义务以及数据安全评估义务，并考虑调整与此相关的网络架构及业务模式；不得设置恶意程序。发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，在约定期限内，持续提供安全维护。

3.1.2《中华人民共和国个人信息保护法》

个人信息的收集、使用、共享等管理混乱，不再匹配个人信息的价值提升，是促进《中华人民共和国个人信息保护法》推出的主要因素。时至今日，《中华人民共和国个人信息保护法》也向企业提出了更严格的要求。



（图3-1）《中华人民共和国个人信息保护法》主要内容梳理

《中华人民共和国个人信息保护法》是一部保护个人信息的法律，自 2021 年 11 月 1 日起施行。个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开与删除等。《中华人民共和国个人信息保护法》涉及法律名称的确立、立法模式问题、立法的意义和重要性、立法现状以及立法依据、法律的适用范围、法律的适用例外及其规定方式、个人信息处理的基本原则、与政府信息公开条例的关系、对政府机关与其他个人信息处理者的不同规制方式及其效果、协调个人信息保护与促进信息自由流动的关系、《中华人民共和国个人信息保护法》在特定行业的适用问题、关于敏感个人信息问题、法律的执行机构、行业自律机制、信息主体权利、跨境信息交流问题以及刑事责任问题。理清了个人信息、敏感个人信息、个人信息处理者、自动化决策、去标识化与匿名化的基本概念，对个人信息处理和敏感个人信息处理等多方面进行了全面规定，建立起个人信息保护领域的基本制度。

《中华人民共和国个人信息保护法》是对于个人信息的保护性法律，对于智能家电厂商而言，尤其需要注意的是，法条指出处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式；收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

相较于以往个人信息保护相关法条分散的局面，《中华人民共和国个人信息保护法》的立法与执行，使个人信息保护进入了真正意义上的“有法可依阶段”。尤其需要智能家电企业注意的是，收集个人信息，应采取对个人权益影响最小的方式，且限于实现处理目的的最小范围，不得过度收集个人信息。

与此同时，所述的个人信息与个人隐私的关系存在着交叉重合，并且在重合的时候优先适用隐私权规则。这对于智能家电厂商对于个人信息的处理，包括个人信息处理规则、个人信息跨境提供规则、个人在个人信息处理活动中的权利、个人信息处理者的义务以及履行个人信息保护职责的部门与法律责任上，均提出了更为严格的要求。

3.1.3《中华人民共和国数据安全法》

《中华人民共和国数据安全法》自 2021 年 9 月 1 日起施行。这是数据安全领域的基础法律，在我国大力发展数字经济、工业互联网的背景下，促进数字经

济健康发展。为数据安全治理有法可依、有章可循奠定基础，明确国家维护数据主权方面的决心，体现了开放数据与数据安全并重的政策。《中华人民共和国数据安全法》是为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益制定的法律。

《中华人民共和国数据安全法》界定了数据、数据处理、数据安全的严格定义，并规定开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

《中华人民共和国数据安全法》加强对向境外司法或执法机构提供存储于中国境内的数据的监管。如第三十六条规定：非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。第四十六条规定，违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

如上述法条所述的《中华人民共和国数据安全法》，其根本目的就是要提升国家数据安全的保障能力和数字经济的治理能力。《中华人民共和国数据安全法》与已实施的《中华人民共和国网络安全法》、《中华人民共和国密码法》及同期实施的《中华人民共和国个人信息保护法》相辅相成，共同构成了中国数据安全的法律保障体系，成为推动我国数字经济持续健康发展的坚实“防火墙”。

例如《中华人民共和国数据安全法》明确提出的数据安全制度，归结而言包括数据分类分级保护制度，也就是根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护；数据安全风险评估预警机制，也就是国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作；数据安全应急处置机制，也就是发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，油除安全隐患，并及时向社会发布与公众有关的整示信息；

出口管制，也就是对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制；以及贸易措施，也就是任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

对家电行业来讲，《中华人民共和国数据安全法》总体而言规范了智能家电产业链条中所有环节对于数据安全的权益和义务，尤其对数据汇聚、处理和利用的厂商行为进行规范，督促数据的开发和利用合规合法。

结合以上，《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等一系列法律法规，从不同角度明确了智能家电行业应尽的责任与义务。与此同时，对应责任与义务，也给出了家电行业在安全性问题上未来进一步发展的方向和指引。在约束家电厂商的同时，实质上也是对家电行业有序发展的有力保护。

3.1.4《中华人民共和国密码法》

《中华人民共和国密码法》自 2020 年 1 月 1 日起施行。《中华人民共和国密码法》是为了规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益制定的法律，是中国密码领域的综合性、基础性法律。

《中华人民共和国密码法》第十二条指出，任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的密码保障系统；任何组织或者个人不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。

《中华人民共和国密码法》规定商用密码从业单位开展商用密码活动，应当符合有关法律、行政法规、商用密码强制性国家标准以及该从业单位公开标准的技术要求；国家鼓励商用密码从业单位采用商用密码推荐性国家标准、行业标准，提升商用密码的防护能力，维护用户的合法权益。

总体来说，《中华人民共和国密码法》对智能家电厂商在密码技术应用方面提出了法律要求，有助于家电行业更好的遵循法律法规，制定相关标准，推动和规范智能家电中密码技术的应用。

3.2 国外信息安全法律法规对智能家电行业的影响

3.2.1《通用数据保护条例》（GDPR）

《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）是欧洲联盟的条例，前身是欧盟在 1995 年制定的《计算机数据保护法》。是欧盟议会和欧盟理事会在2016年4月通过，在2018年5月开始强制实施的规定。

GDPR 罚款总额在 2019 年达到 4.175 亿欧元，仅在当年 7 月，罚款总额就高达 3.6 亿欧元，而当年有 750 家公司收到 GDPR 罚款，平均罚款金额为 50 万欧元，相当于 389 万元人民币。

该条例制定关于处理个人数据中对自然人进行保护的规则，以及个人数据自由流动的规则；条例保护自然人的基本权利与自由，特别是自然人享有的个人数据保护的权利；条例规定不能以保护处理个人数据中的相关自然人为由，对欧盟内部个人数据的自由流动进行限制或禁止。条例规定了约束范围不论企业在不在欧盟，只要在欧盟进行“个人数据处理”、“数据支付对价”、“数据监控”就受 GDPR 限制。后续提出了具体的个人数据处理原则、处理的合法性、同意的条件，以及针对特殊人群和不需要识别的处理的细化处理方式。

值得注意的是，该条例明确规定规定，企业在收集、存储、使用个人信息上要取得用户的同意，用户对自己的个人数据有绝对的掌控权。且明确规定了用户应被允许随时撤销许可或修改授权，且允许用户随时修改个人信息内容。

同时，条例还规定了数据主体的权利、数据主体的访问权，并在后续法条中依次对控制者和处理者、将个人数据转移到第三国或国际组织、独立监管机构、合作与一致性、救济、责任与惩罚、和特定处理情形相关的条款以及授权法案与实施性法案等具体情况，明确、细化约束。

归结而言，GDPR 意义在于推动强制执行隐私条例，规定了企业在对用户的数据收集、存储、保护和使用时新的标准。该标准整体而言更侧重于用于隐私合规保护，对于企业的约束更为明确，且更为严格，相关规定或对我国相关行业标准，尤其是企业制定的相关应对策略具备一定战略意义。

3.2.2《加州消费者隐私法》（CCPA）

《加州消费者隐私法》简称 CCPA。2018 年 6 月，美国加利福尼亚州立法者

通过了《加州消费者隐私法》。该法案在原先公投提案的基础上，于一周内迅速起草并通过。这将为企业理清思绪、成功遵守该法复杂的法律条文带来不少挑战。不过，该法案的出台也为企业建立强大的数据管理体系、确立相关道德准则提供了契机。尊重消费者的选择将成为企业透明度与可信赖度的最佳注脚。

2020 年 1 月，CCPA 正式生效。该法案旨在提高加州居民对个人信息相关问题以及企业对个人信息的收集和所收集之个人信息如何成为其他企业的财产的关注，并切实保护加州居民的隐私权。从更高层面来说，这部新法将要求各机构透明地收集、共享和利用用户数据。凭借显眼的网站标头，加州居民将有权要求知悉企业收集了哪些个人数据、企业是否将这些数据出售给其他企业或与其他企业共享（若存在上述情况，其中涉及哪些个人数据），并有权要求企业停止出售个人数据。

CCPA 第一节明确提出，消费者有权要求收集消费者个人信息的企业向该消费者披露其收集的个人信息的类型与具体内容。收集消费者个人信息的企业应当在收集时或者收集前告知消费者关于其所要收集的个人信息的类型，以及该类型的个人信息的用途。企业在未向消费者提供符合本节规定的通知的情况下，不得收集额外的个人信息或者将收集的个人信息用于额外的用途。

整体而言，CCPA 与 GDPR 的立法逻辑基本一致，但也存在个别差异。同时，CCPA 对个人数据或者说个人信息有着更为全面的定义，对管辖权的规定更为简练与凝聚重点，而在跨境传输的管控上，更为放任，甚至是鼓励。归结而言，CCPA 对用户保障的五个主要权利如下：

用户有权要求企业公开其个人数据收集及出售情况，包括个人可识别信息(PII)的类型、来源、用途以及是否与第三方共享。

用户有权要求企业提供过去 12 个月内收集的个人可识别信息之副本。

用户有权要求企业删除所收集的个人身份信息。

用户有权要求企业不得出售其个人数据。

用户有权不受歧视地行使上述权利。

GDPR 和 CCPA 作为对个人信息保护立法的探索和尝试，对于我国的法律及规定提供了一定的参考作用，对智能家电厂商提出行业标准、个人隐私保护体系等提供参考和借鉴依据。

3.2.3《数据保护法案》（DPA）

英国《数据保护法》(DPA)2018 年 5 月 23 日，英国正式通过新修订的 DPA2018《数据保护法》。该法将废除 1998 年颁布的《数据保护法》，重新建立英国数据保护框架以促进 GDPR 在英国的有效落实，并在 GDPR 框架下对某些条款做出裁剪规定。同时确保英国在脱欧之后与欧盟在个人数据保护方面保持一致，以促进英国与欧盟国家的数据流动。该法主要内容包括：1）加强数据主体对其个人数据的控制权。2）加强数据控制者义务。此外，该法还为刑事司法机构出于执法目的而处理数据设计了专门的执法框架，要求在执法过程中同样需要保护个人数据。

3.2.4《内华达州数据隐私法》(SB220)

美国《内华达州数据隐私法》(SB220)2019 年 5 月 29 日美国内华达州发布 SB 220《内华达州数据隐私法》，该法案涉及互联网隐私，要求互联网网站和在线服务的运营商遵循消费者的指示，不得出售其个人数据。违反 SB 220 可能会导致运营商收到禁令或每次违规最高被处以 5,000 美元的民事处罚。SB 220 已于 2019 年 10 月 1 日生效。

3.2.5《联邦资料保护法》（DPA）

瑞士《联邦资料保护法》(DPA)瑞士是少数未加入欧盟的欧洲国家。在欧盟个人资料保护指令(EU Directive 95/46/EC)实施期间已获得第三国适应性认定，即欧盟认定瑞士关于个人信息保护的相关法规及其保护程度与欧盟个人信息保护指令相当。为应对欧盟 GDPR 新法规，2017 年 9 月 15 日瑞士联邦议会通过修订草案，修正 DPA 相关条文。其目的是配合欧盟 GDPR 的实施，希望在 GDPR 正式实施之后，继续获得第三国适应性认定，而不须在每次跨境资料传输皆遵循 GDPR 规则办理。瑞士 DPA 与 GDPR 区别在于其并未制定数据可携带权、没有领域外效力、对于知情同意的要求较低、认证机制于行为守则及罚则较低。

3.2.6《联邦个人资料保护法》(BDSG)

德国《联邦个人资料保护法》(BDSG)德国联邦议院于 2018 年 4 月 27 日通过《个人信息保护调整和施行法》，其中包含新的德国 BDSG《联邦个人信息保护法》。在这部新的法案中，已实施 40 年的 BDSG 进行了大幅调整以符合欧盟 GDPR

《通用数据保护条例》。在新的 BDSG 法案中德国联邦政府运用了 GDPR 的开放性条款，导致部分新的 BDSG 规范内容超越了 GDPR 的条文规范，与现行欧盟法律不符，很可能被宣布违反欧盟法律。另一方面，旧的 BDSG 仅有 48 条规定，而新的 BDSG 则超过 85 条规定，且更为复杂，提高了法律适用上的难度。

3.2.7 无线电设备指令（RED）补充法规

无线电设备指令（RED）补充法规 2022 年 1 月 12 日，欧洲委员会正式发布了（EU）2022/30 法案，规定相关产品制造商在设计和生产中必须考虑到 RED 指令的三点网络安全要求。规定的适用产品包括大多数可接入互联网的无线终端设备，如路由器，摄像头，智能门锁，智能家电，玩具和儿童看护设备等，但是不包含其他特定指令监管的设备如医疗器械和民航相关的系统。此法案将给制造商留出 30 个月的缓冲期，将于 2024 年 8 月 1 日正式生效，作为 RED 认证的一部份，强制执行。

该法规涉及 REO 指令的第 3（3）条（d）、（e）和（f）三点要求:

3(3)(d)，无线电设备不会对网络或其运行产生有害影响，不会滥用网络资源而导致服务受到严重影响。

3(3)(e)，无线电设备应有安全装置，确保用户和订户的个人数据和隐私得到保护。

3(3)(f)，无线电设备支持特定的反欺诈功能，以确保防止欺诈。

3.3 智能家电信息安全标准与检测认证

3.3.1 国内智能家电信息安全标准

3.3.1.1 GB/T 41387-2022 《信息安全技术 智能家居通用安全规范》

该标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口，规定了智能家居安全通用技术要求和对应测试评价方法，适用于智能家居产品的安全设计和实现，智能家居的安全测试和管理也可参照使用。

智能家居中各类电子设备广泛采用电子器件和软件，除了设备本身由于材料、结构设计、软硬件失效等问题引入安全风险外，还由于设备互联互操作、远程网络操作等带来功能安全和网络安全风险。该标准在定义了智能家居系统的组成以

及对应的安全框架的前提下，对信息安全的通用要求和检测方法两方面进行了规范。智能家居系统主要由智能家居用户、智能家居终端、智能家居控制端、智能家居网关、通信网络和智能家居应用服务平台组成。在该标准中主要针对智能家居终端安全、智能家居网关安全、智能家居控制端安全和智能家居应用服务平台安全提出相应的安全要求和测试评价方法。

3.3.1.2 GB/T 41789-2022《智能家用电器的通用安全技术要求》

该标准由中国轻工业联合会提出，全国家用电器标准化技术委员会（SAC/TC46）归口，中国家用电器研究院牵头，与青岛海尔智能技术研发有限公司、上海奥航智能科技有限公司 、公安部第三研究所、美的集团股份有限公司等单位共同起草制订该标准。该标准已于 2022 年 10 月 12 日发布，2023 年 5 月 1 日起实施。

本标准规定了智能家用电器的通用安全技术要求，包括电器安全要求、信息安全要求、功能安全要求等内容。其中第 6 章信息安全部分的要求包括：通用要求、设备标识与鉴别、物理安全、接口安全、地理位置信息鉴别、环境适应性、固件安全、操作系统安全、应用安全、通信安全、数据安全、密码功能、个人信息保护、审计日志等内容。

3.3.1.3 T/CAS 499-2021《智能家用电器网络安全技术要求和测评方法》

该标准由中国标准化协会（CAS）发布，中国家用电器研究院牵头，与青岛海尔科技有限公司、美的集团股份有限公司、青岛海信日立空调系统有限公司等企业共同起草制订该标准。该标准规定了具备网络功能的智能家用电器（简称网络智能家电）网络安全框架、技术要求、测试评价方法。适用于网络智能家电信息技术安全要求的研发、测试、评估和产品采购。

该标准参考 GB/T 18336 系列标准，将评估对象（TOE）范围限于网络智能家电中的家电通信处理模块，远程管理模块和远程控制模块。其中网络智能家电中的家电逻辑控制模块和传感模块不在 TOE 范围内。远程管理端和远程控制终端中仅与网络智能家电管理、控制和查询相关的功能模块在 TOE 范围内。

该标准给出了网络智能家电的 TSF（评估对象的安全功能）框架图，其中包含的安全功能为：设备网络配置与绑定、身份鉴别、通信保护、固件保护、代码安全、用户管理、访问控制、安全审计和加密存储。同时该标准将网络安全保障

等级分为基本级和增强级，以便于企业及第三方检测机构依据产品的功能职责，选择不同的安全级别，为自评价及测评进行参考。基本级为 TOE 的最低安全要求，通过采用一定的安全功能要求和安全保障要求，使 TOE 能够抵御基本攻击潜力的攻击者的威胁。增强级为通过采用增强的安全功能要求和安全保障要求，使得 TOE 能够抵御中等攻击潜力的攻击者的威胁。

3.3.1.4 GB/T 35273-2020《信息安全技术 个人信息安全规范》

根据国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2020 年第 1 号），由信息安全技术标准化委员会（TC260）GB/T 35273-2020 组织修订的《信息安全技术 个人信息安全规范》已正式获批发布，实施时间为 2020 年 10 月 1 日，并替代 GB/T 35273-2017 版本国标。标准由全国信息安全标准化技术委员会归口。相对于 2017 版标准，2020 版标准进行了针对性修订。

（1）加强标准指导实践

2020 版标准明确了数据安全责任人相关要求，规范了个人信息保护负责人的相应工作职责；规定了定向推送相关要求以及用户可以撤回的权利；提出了平台第三方接入责任相关要求，对第三方接入的监督管理责任进行细化。

（2）支撑 APP 安全认证

规范每条要求的检测评估点，便于认证工作根据标准要求逐条开展；对 APP 中涉及的核心功能、必要信息、必要权限等方面进行展开描述，提出清晰的要求并形成评估点，在标准条款中以 APP 为例进行解释说明，增强其指导性。

此次标准的修订发布，是为了进一步贯彻落实《中华人民共和国网络安全法》规定的个人信息收集、使用的“合法、正当、必要”基本原则，解决人民群众反映强烈的 APP“强制索权、捆绑授权、过度索权、超范围收集”的问题。同时，针对当前 APP 运营管理的一些不合理现象，如告知目的不明确、注销账户难、滥用用户画像、无法关闭个性化推送信息、第三方接入缺乏有效管理、内部管理职责不明等问题，进一步梳理完善条款，指导组织使用标准完善个人信息保护体系。

修订后的标准，将进一步使标准契合我国相关法律法规的要求，增加标准指导实践的适用性，帮助提升行业和社会的个人信息保护水平，推动个人信息保护领域技术产品、咨询服务等方面产业化进一步发展，为我国信息化产业健康发展

提供坚实保障。

3.3.1.5 GB/T 40979-2021《智能家用电器个人信息保护要求和测评方法》

该标准由中国轻工业联合会提出，全国家用电器标准化技术委员会（SAC/TC46）归口，中国家用电器研究院牵头，与青岛海尔科技有限公司、美的集团股份有限公司、深圳 TCL 新技术有限公司、惠而浦（中国）股份有限公司等单位共同起草制订该标准。该标准规定了智能家用电器应用过程中个人信息保护的技术要求、组织管理要求及测评方法。该标准已于 2021 年 11 月 26 日发布，2022 年 6 月 1 日起实施。

该标准主要为规范智能家用电器相关的个人信息保护要求，促进企业良性竞争，为消费者提供更好的消费体验，保障消费者个人信息安全。该标准适用于智能家用电器、智能家用电器系统和智能家居应用过程中相关各类组织的个人信息处理活动，对个人信息收集、存储、使用（公开披露、共享与转让、委托处理及跨境传输）等业务流程，以及个人信息保护的组织管理与评价。

该标准在 GB/T 35273-2020 的基础上，结合智能家电的特点，将智能家电的信息收集方式以及个人信息的流转场景进行了分类，明确了个人信息安全级别的划分。划分出智能家电个人信息分类以及智能家电个人敏感信息分类，并对智能家电个人信息安全级别进行极高、高、中、低四个级别的划分。

3.3.1.6 GB/T 41817-2022《信息安全技术 个人信息安全工程指南》

该标准的标准编制工作牵头单位为中国电子技术标准化研究院，参与编制的单位均为国内头部的高科技企业、律师事务所及信息安全公司。除上文所述的对国内业界工程实践中的业务、法律和信息安全工作的经验总结外，《工程指南》参考了国际和国外有关隐私工程、隐私技术框架的研究成果。

《工程指南》将个人信息安全工程进行了首次定义，也称为隐私工程（privacy engineering），是将个人信息保护关注点整合到系统和软件生命周期过程的工程实践。标准描述了个人信息安全工程目标，给出了在需求分析、产品设计、产品开发、测试审核、发布部署、运行维护等系统工程阶段的个人信息保护实施指南。

标准适用于涉及个人信息的网络产品和服务，为其在需求、设计、开发、测试等系统工程阶段开展个人信息保护实践提供指导。其目标包括：

透明性：确保信息系统中个人信息处理活动达到足够的透明度，其目标是使个人信息主体、控制者和处理者等相关方了解个人信息保护的风险。

可管理性：提供对个人信息的细粒度控制，确保个人信息主体、控制者、处理者等相关方能够适当干预信息系统的个人信息处理过程。

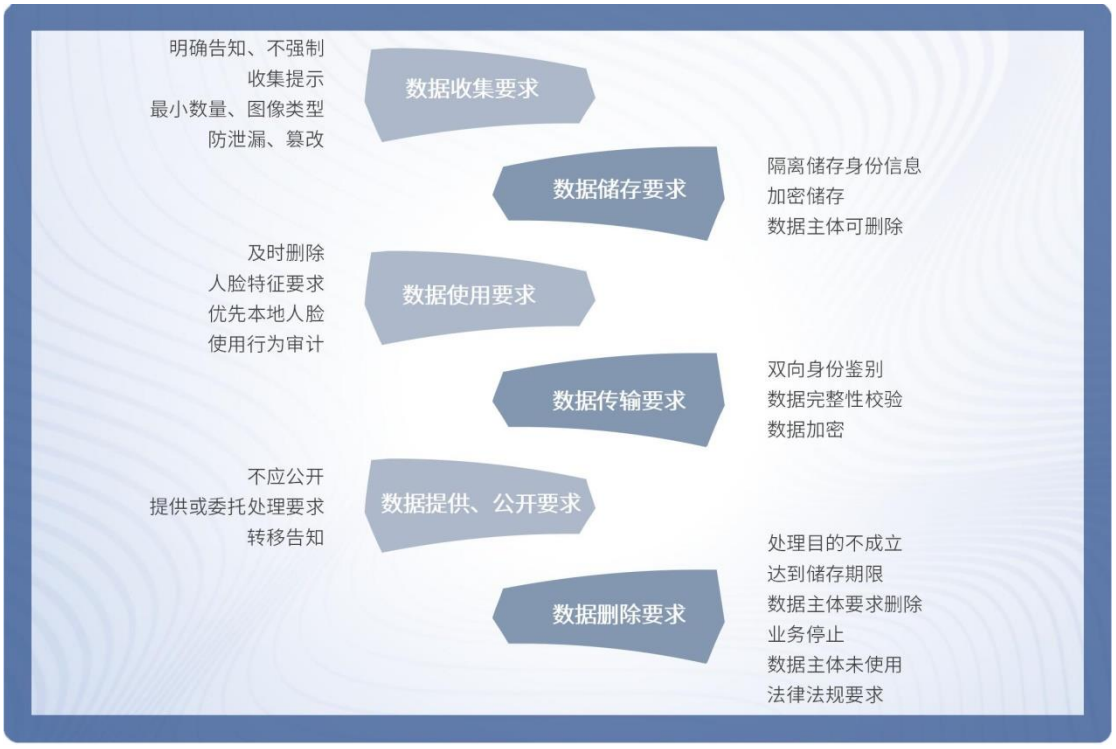
不可关联性：采取措施对个人信息去标识或匿名化处理，减少个人信息链接到个人信息主体引起的安全风险。

《工程指南》的整体逻辑显示其最为重视的工程阶段为产品设计阶段。《工程指南》为此特意在第 7 部分罗列了产品设计阶段的重点设计考虑点，重点设计考虑点显示了《工程指南》对《个人信息安全规范》所关注的重点的落实，对产品的具体设计者而言更具有落地操作的参考性。

3.3.1.7 GB/T 41819-2022 《信息安全技术 人脸识别数据安全要求》

为贯彻落实《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》以及《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》等有关要求，深入支撑人脸识别技术应用过程中的数据安全保护，重点围绕个人信息处理的最小必要原则，针对人脸数据滥采、泄露或丢失、过度存储和使用等突出问题，结合当前人脸识别技术应用现状，中国电子技术标准化研究院联合 30 家单位，共同研制了国家标准 GB/T41819-2022《信息安全技术人脸识别数据安全要求》。

该标准实施对象为人脸识别数据处理活动，包括收集、存储、使用、传输、提供、公开与删除等，主要内容包括规定了数据处理者开展人脸识别数据处理的安全通用要求，并进一步明确了收集、存储、使用、传输、提供、公开、删除等处理活动的安全要求。标准应用于人脸识别数据处理者，也就是帮助人脸识别数据处理者规范人脸识别数据处理活动，防范人脸识别数据安全风险。



（图 3-2）《信息安全技术 人脸识别数据安全要求》核心内容

3.3.1.8 GB/T 41807-2022《信息安全技术 声纹识别数据安全要求》

由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口，该标准贯彻落实《中华人民共和国网络安全法》、《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等有关要求，对声纹识别数据的收集、存储、使用、传输、提供、公开、删除等活动提出安全要求，规范数据处理者的声纹识别数据处理行为。标准的发布和实施为提升声纹识别产品和服务安全性，为防范个人信息和隐私信息安全风险提供了重要支撑。

通过声纹识数据处理活动中常见安全风险的分析，如：数据的滥采滥用、数据提供给未获授权同意的第三方、数据传输过程中被监听和攻击导致语音样本泄露等，提出通用要求以及面向声纹数据全生命周期的安全防护要求，保护声纹数据的全生命周期安全。

3.3.1.9 GB/T 42012-2022《信息安全技术 即时通信服务数据安全要求》

为贯彻落实《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》以及《国务院办公厅关于促进平台经济规范健康发展的指导意见》等有关要求，强化平台企业数据安全责任、保障平台经济安全健康发展，针对即时通信服务的常见数据安全风险，结合行业应用现状，中国电子技术标准化研究院等

18 家单位共同研制了国家标准 GB/T 42012-2022《信息安全技术 即时通信服务数据安全要求》。

标准实施对象为即时通信服务，包括个人即时通信服务(面向个人用户的即时通信服务)、组织即时通信服务(面向组织办公场景的即时通信服务)。非商业服务不包含在内，如:组织内部自建或自用服务不包含在内。

即时通信服务涉及的相关方主要包括：

1.即时通信服务提供者:利用即时通信服务平台，提供即时通信服务的企业法人。

2.个人用户:自然人形式的用户，存在于个人即时通信服务和组织即时通信服务。

3.组织用户:组织形式的用户(如企业、政务机关)，存在于组织即时通信服务。

4.第三方:提供资讯信息、广告服务、应用集成等服务的相关方。

本标准规定了即时通信服务收集、存储、传输、使用、加工、提供、公开、删除、出境等数据处理活动的安全要求，并给出了即时通信服务典型场景数据安全保护要求。

该标准的应用为即时通信服务数据安全监管工作提供参考，促进即时通信平台规范健康发展。帮助即时通信服务提供者规范数据处理活动，建立数据安全治理体系，保障用户个人信息权益。为即时通信服务相关的数据安全评估、认证等工作提供依据。

3.3.1.10 GB/T 42015-2022《信息安全技术 网络支付服务数据安全要求》

为贯彻落实《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》与《国务院办公厅关于促进平台经济规范健康发展的指导意见》等有关要求，强化平台企业数据安全责任、保障平台经济安全健康发展，针对网络支付服务处理用户数据和业务数据的突出问题结合行业应用现状，中国电子技术标准化研究院等 18 家单位，共同研制了国家标准 GB/T42015-2022《信息安全技术网络支付服务数据安全要求》。

网络支付服务涉及的相关方主要包括:网络支付服务平台，网络支付服务用户，网络支付服务账务平台网络支付服务提供者。本标准规定了网络支付服务收

集、存储、使用、加工、提供、公开、删除以及出境等数据处理活动的安全要求，并给出了网络支付服务典型场景下的数据安全要求。为网络支付服务数据安全监管工作提供参考，促进网络支付平台规范健康发展。帮助网络支付服务提供者规范数据处理活动，建立数据安全治理体系，保障用户个人信息权益。为网络支付平台相关的数据安全评估、认证等工作提供依据。

（图 3-3）《信息安全技术网络支付服务数据安全要求》所提出的基本要求

3.3.1.11 YD/T 4209-2023 《智能家居终端安全 智能电视安全能力技术要求和测试方法》

本标准由中国通信标准化协会提出并归口（行业标准）。

本标准规定了智能电视硬件，操作系统，预置应用，第三方应用，网络通信和人工智能服务 6 个方面的安全能力，并从基本的安全保障、实现难度、安全能力等层面对智能电视安全能力进行分级，制定相应的测试方法。

本文件仅提出智能电视安全能力技术要求和测试方法，对具体技术实现方式不作规定。

3.3.1.12 T/CCSA 288-2020《智能家居终端安全 智能音箱安全能力技术要求和测试方法》

本标准由中国通信标准化协会提出并归口（团体标准）。

本标准规定了智能音箱安全能力技术要求和测试方法，包括硬件安全能力、操作系统安全能力、应用层安全能力、网络通信安全能力和人工智能服务安全能力，并对安全能力进行了分级，制定了相应的测试方法。

本标准适用于具备人工智能能力、提供互联网内容服务的智能音箱设备

3.3.2 国外智能家电信息安全标准

3.3.2.11ETSI EN 303645 消费物联网网络安全：基线要求

EN 303645 由欧洲电信标准化协会（ETSI）基于其编写的 TS 103645 之上主导编写，是欧盟发布的首个针对消费类 IoT 设备的网络安全基线，该技术标准主要规定消费类物联网产品及其相关服务的网络安全标准。内容涵盖设备软件、通信、管理后台、流程制度等 13 个安全要求及个人隐私数据保护。同时，ETSI 开发出了测试用例参考标准 ETSI TS 103 701,消费类物联网产品评估指南，旨在为消费类物联网产品建立安全防线，保护用户隐私。

EN 303645 标准自 2020 年发布以来，不仅在欧盟内开始被广泛使用，在全球 IoT 行业影响范围也很广，已被十余个政府机构、IoT 行业安全联盟及第三方安全认证机构所采纳吸收。

3.3.2.2 NISTIR 8259 物联网设备制造商的基础网络安全活动

美国国家标准与技术研究院（NIST）于 2020 年发布网络安全指南 NISTIR 8259：《物联网设备制造商的基准网络安全活动》，该指南描述了制造商在将其物联网设备出售给客户之前应考虑的与网络安全相关的建议活动。这些基础网络安全活动可以帮助制造商减少客户所需的网络安全相关工作，从而降低物联网设备危害和使用受损害设备实施的攻击的普遍性和严重性。

NISTIR 8259A：《物联网设备网络安全能力核心基准》，从基本的风险评估，网络安全测试,软件安全开发基本要求，以及用户信息告知均有所覆盖。网络安全测试包括设备标识、安全配置、数据保护、逻辑接口接入授权、软件/固件升级、安全事件日志等，为物联网设备网络安全能力提供了最低基准线。

3.3.2.3ANSI/UL 2900-1 网络连接产品软件信息安全标准

该标准由美国 UL 主导编写，经 ANSI 审核成为美国国家标准。

ANSI/UL 2900-1 标准提出了可联网产品的通用软件网络安全要求，它包含以下三方面的内容：

①有关软件开发商（供应商或其他供应链成员）产品风险管理流程的要求。

②评估和测试产品是否存在漏洞、软件弱点和恶意软件的方法。

③关于在产品的架构和设计中存在安全风险控制的要求。

3.3.2.4IEC 60335-1:2020 家用和类似用途电器安全

IEC 60335-1:2020 是由 IEC（国际电工委员会）发布的第 6 版家用和类似用途电器的安全通用要求。此次修订在规范性附录 U 中引入了网络安全要求，以避免未经授权的访问以及通过公共网络进行远程通信的传输故障的影响。

上一版本的 IEC 60335 系列标准不能处理新兴的无线技术和公共网络内器具之间的远程通信。标准 Annex U APPliances intended for remote communication through public networks（附录 U 通过公共网络进行远程控制的设备）针对上述问题提出。

但是，该附录不涉及与数据保密和消费者隐私方面保护要求。

3.4 国内外认证机构及认证服务

3.4.1 国内认证机构

认证机构介绍：中国网络安全审查技术与认证中心（英文缩写为：CCRC,原为中国信息安全认证中心）于 2006 年由中央机构编制委员会办公室批准成立，为国家市场监督管理总局直属正司局级事业单位。依据《中华人民共和国网络安全法》《网络安全审查办法》及国家有关强制性产品认证法律法规，承担网络安全审查技术支撑和认证工作；在批准范围内开展与网络安全相关的产品、管理体系、服务、人员认证和培训等工作；同时设有国家信息安全产品质量监督检验中心（北京）。

认证服务介绍：依据 CCRC-TR-088-2018《智能家居产品安全技术要求及测试评价方法》和《IT 产品信息安全认证实施规则 智能家居产品》，CCRC 推出了针对智能家居的信息安全检测和认证，认证的范围为智能家居产品，包括智能家居设备、控制端应用、智能家居应用服务平台（软件系统）。智能家居设备包括智能家居网关设备、控制设备以及应用设备。

认证机构介绍：中家院（北京）检测认证有限公司成立于 2014 年 12 月，是中国家用电器研究院旗下的检测认证技术服务平台，是国家家用电器质量检验检测中心、国家智能家居质量检验检测中心、中国家用电器检测所和中家院认证中心的所在单位。在原有检测资质的基础上，完善扩充自愿性产品认证机构资质，成为“检测认证一体化”机构。

认证服务介绍：中家院（北京）检测认证有限公司经国家认监委批准，开设了产品认证服务。中家院２０１６年就推出了针对智能家电的检测认证规则，用于网络智能家用电器（简称网络智能家电）的信息技术安全认证。涉及的网络智能家电信息安全方面的检测认证范围包括家电设备端(家电产品)种类(空调器、冰箱、洗衣机、热水器、吸油烟机、厨房机械、微波炉、电饭煲等）、远程控制端（手机 APP 等）、远程管理端（远程服务平台）的不同划分申请单元。目前，依据 T/CAS 499-2021《智能家用电器网络安全技术要求和测评方法》开展检测认证。

3.4.2 国际认证机构

认证机构介绍：Intertek 电子电气业务始于 1896 年爱迪生创建的电气试验室，即后来的 ETL。通过其遍布全球的授权实验室网络，Intertek 可以为客户提供快速专业的产品测试、检验与认证解决方案。集团于 2002 年 5 月在伦敦证券交易所上市，是支持性服务行业 FTSE 公司之一。同时 Intertek 是第一家进入中国的国际商业检验机构，自 1989 年以来，已在全国建立 20 多个分支机构及国际水准的实验室。

认证服务介绍：Intertek 在电子电气质量与安全领域拥有广泛的能力和资质，全球 100 多位专家活跃在超过 200 家标准和符合性组织，包括 ANSI、AHAM、ASHRAE、CSA、IEC、NFPA、UL、VCCI、IECEE 等。

其实验室受 30 多家主要的认证机构认可，包括美国职业安全与卫生管理局（OSHA）国家认可测试实验室（NRTL）、加拿大标准委员会（SCC）、国际电工委员会电工产品合格测试与认证组织（IECEE）、美国实验室认可协会（A2LA）、联邦电信委员会（FCC）、英国授权服务中心（UKAS）等。Intertek 以差异性的高附加值服务，为客户提供包括安全、性能、电磁兼容、能效、绿色及环境等在内的一站式解决方案。

认证机构介绍：1901 年，由英国土木工程师学会(IEC）、机械工程师学会(IME)、造船工程师学会(INA）与钢铁协会(ISI)共同发起成立英国工程标准委员

会(ESC 或 BESC)，并于同年 4 月 26 日在伦敦召开第一次会议。这是世界上第一个全国性标准化机构。1902 年电气工教师学会(IEE)加入该委员会，英国政府开始给予财政支持。1929 年 BESA 被授予皇家宪章。1931 年颁布补充宪章，协会改用现名(BSI)。BSI 是在国际上具有较高声誉的非官方机构。

认证服务介绍：“风筝”标志是 BSI 特有的注册商标，国内外厂家均可申请使用。使用这种标志的企业不仅其产品必须符合有关的 BS 标准的要求，而且必须具有符合 BS-5790 的质量保证体系（ISO9000 族的质量保证模式标准也可），在认证过程中，还要对该体系进行评定。使用安全标志的产品，必须符合 BS 标准的安全要求或其它的安全规定。申请及认可办法与“风筝”标志的办法大体相同，同样适应于国内。外企业。

认证机构介绍：TrustArc 是一家位于美国的全球知名隐私合规技术公司。该公司提供帮助企业更新隐私管理流程的软件和服务，从而使其符合政府法律和最佳实践。他们的隐私印章或合规证明受到全球的普遍认可。

认证服务介绍：TRUSTe 企业隐私认证框架标准认证是基于 TrustArc 隐私和数据治理问责框架标准和程序的独特监管要求开发的一套隐私认证，通过该认证可使收集或处理个人信息的组织能够展示符合监管期望和隐私责任标准的证明。

该框架基于全球公认的法律和监管标准，例如：欧盟通用数据保护条例(GDPR)、ISO 27001、美国健康保险流通与责任法案 (HIPAA)、经合组织隐私准则、APEC 隐私框架等。

认证机构介绍：ePrivacy 是一家欧洲权威隐私认证机构，为全球企业及其产品提供隐私咨询和认证服务，涵盖移动应用、电信、车联网、健康产品及各类广告服务等行业。

认证服务介绍：ePrivacyseal 数据保护印章由欧洲权威隐私认证机构 ePrivacy 对在线和移动产品进行深入审核后授予，该认证涵盖了通用数据保护条例(GDPR)对数字产品的法规和技术要求。认证标准目录不断调整以适应 GDPR 和其他数据保护法律的解释。该认证在欧盟乃至全球都具有权威性和广泛影响力。

认证机构介绍：TÜV（德国技术监督协会）是总部在德国的全球知名第三方检测和认证机构，协会内在 IoT 安全认证领域影响力较大的成员机构有德国莱茵 TUV、南德 TUV。

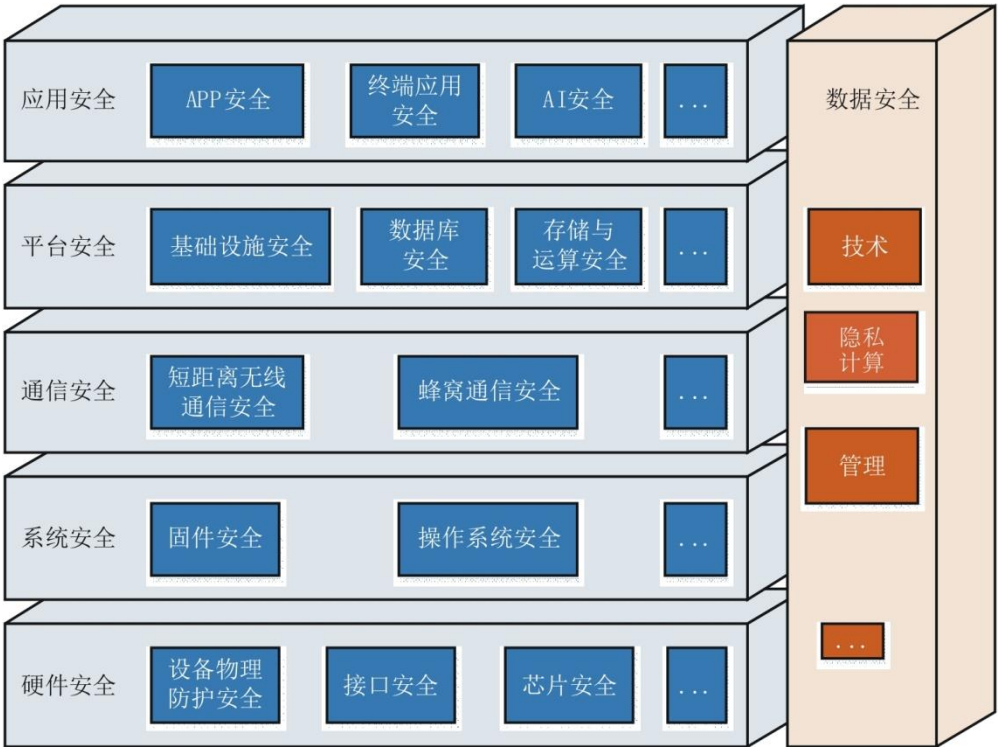
认证服务介绍：TÜV 提供基于欧盟 ETSI EN 303645、GDPR 的 IoT 产品、控制应用及云服务的安全隐私认证服务，服务内容包括产品安全能力评估、代码分析、渗透测试和问题验证，产品在通过认证后可获得 TUV 认证证书及产品安全认证标签。莱茵及南德均为认证申请厂商提供基础、中级和高级的认证等级供选择。

自 2017 年起，TUV 莱茵陆续为国内的诸多 IoT 设备的行业头部品牌提供咨询服务或颁发证书，提供针对 IoT 设备、App 和云服务的三大类咨询及认证服务，并基于技术和法规的进步而不断更新检测标准。相关企业通过 TUV 莱茵的认证后，不仅可以获得相关证书，还可获准使用其独有的认证标识，用于市场宣传和增强消费者信心。

4. 智能家电信息安全架构的实施与转化

4.1 智能家电信息安全体系架构

针对智能家电面临的安全风险与智能家电各环节的安全需求，需构建完善的智能家电信息安全保障体系架构，这对于指导产业链各环节的生产制造、全面提升智能家电信息安全水平具有重要意义。高端智能家电安全技术体系架构将以“云-管-边-端”体系为主线，聚焦硬件安全、系统安全、通信安全、平台安全、应用安全、数据安全、个人隐私保护等领域，为高端智能家电提供实用、有效的信息安全解决方案，为智能家电产业健康发展提供信息安全理论和技术支撑。

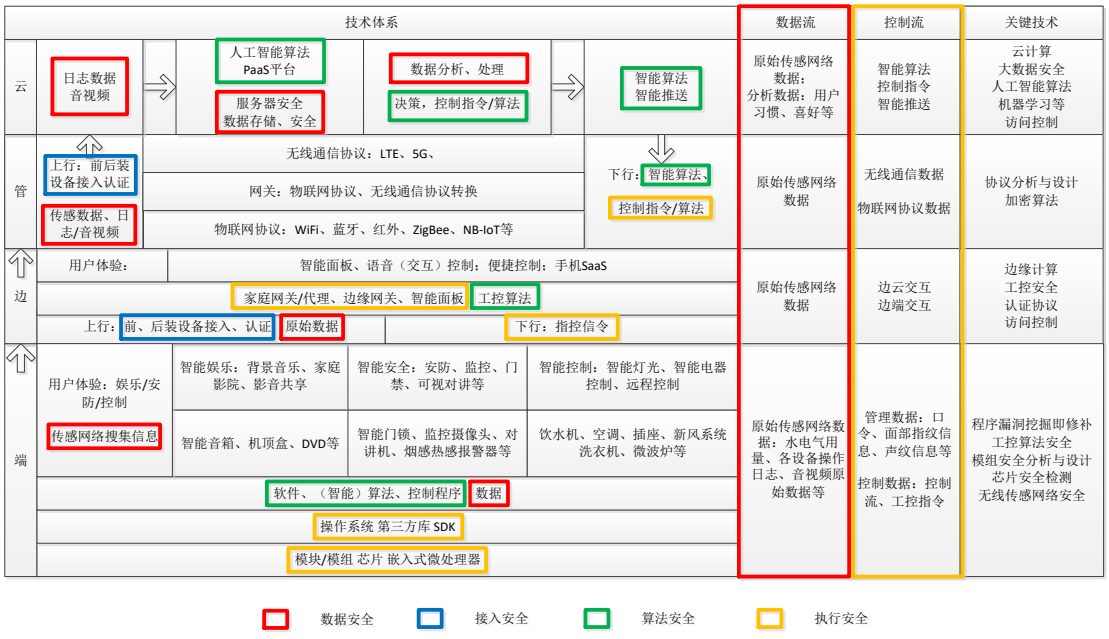


（图4-1）智能家电安全体系架构

4.2 智能家电信息安全体系架构的实施

4.2.1 高端智能家电安全技术体系架构设计

高端智能家电安全技术体系架构将以“云-管-边-端”体系为主线、以数据流和控制流为信息对象，以数据安全、接入安全、算法安全及执行安全为核心环节，聚焦智能家电的信息安全基础理论和基础架构、信息安全关键技术、基本信息安全模组和协议、信息安全标准和检测研究等，结合重大课题、专项课题的联合集中攻关，实现体系安全、数据安全、通信安全、终端安全、业务安全和管理安全等多维安全，为高端智能家电行业提供安全、可靠、高效、实用的信息安全技术、方案、产品、检测及标准，为智能家电产业健康发展提供信息安全理论基础与技术支撑。



图（4-2）智能家电安全技术建设内容架构

数据安全分为动态数据保护和静态数据保护。具体体现在“端”侧传感器按要求搜集环境数据、用户家电操作习惯、家庭生活中产生的音视频数据等，数据通过“管”侧上传至“边”和“云”侧，在“边”和“云”侧进行汇聚、存储，通过云计算、人工智能算法对原始数据进行处理和分析，得到结论性信息，形成新的智能算法、控制指令并推送，通过下行通道反馈至“边”侧和“端”侧。数据安全要保证这些数据在传输、存储和使用过程中的机密性、完整性、可用性、

可控性和不可抵赖性。需要适用的密码算法和密码协议。动态数据保护主要用于保护数据在传输过程中的机密性、完整性、可用性和不可抵赖性，常采用加密算法和加密协议来实现，例如 SSL/TLS 协议、IPSec 协议等。静态数据保护主要用于保护数据的机密性、完整性、可控性和不可抵赖性，常采用加密算法和加密协议来实现，例如 AES 算法、RSA 算法等。同时，还需要采取数据备份、数据加密、访问控制、安全审计等措施来保障数据的安全性。

接入安全是指智慧家居设备接入过程的身份认证、权限管理、安全管控、接入审查等。实现前、后装智能家电设备与“边”侧和“云”侧的双向身份认证和访问控制，保障智能家电环境安全、所有设备的受控使用，不存在身份仿冒攻击、中间人攻击、并行会话攻击，降低内部用户或设备攻击的潜在风险。

具体而言，实现接入安全需要采取以下措施：

1. 身份认证：对设备的接入进行身份认证，确保只有合法的设备可以接入网络。一般采用密码认证、数字证书认证等方式进行身份认证。

2. 权限管理：对不同用户的权限进行管理，确保只有授权的用户才能访问和使用设备。需要根据用户的角色和权限设置相应的权限和操作范围。

3. 安全管控：对设备进行安全管控，确保设备的安全性和稳定性。可以采用安全软件、防火墙等措施进行安全管控。

4. 接入审查：对设备的接入进行审查，确保不存在身份仿冒攻击、中间人攻击、并行会话攻击等问题。需要及时监控和拦截可疑的连接行为。

5. 定期更新：对设备和系统的补丁和更新进行定期检查和安装，以修复漏洞和安全问题。

算法安全主要包含加密算法安全和功能算法安全。加密算法安全方面，当前用于保护数据安全的传统加解密算法设计通常基于计算安全性，其安全性证明通常规约到数学难题的求解上。在场景多样、信息种类多样、通信手段多样的智慧家居网络中，不同的应用场景、数据类型、设备算力、安全需求，要适应性地选择加密算法，兼顾安全和效率。因此算法安全需要各类数据和场景下，进行多种加密算法的研究和选择。功能算法安全方面，为给用户提供智能化、自动化的使用体验，智慧家居网络的“云”、“边”、“端”侧都运行着各类程序和算法，主要体现在“云”侧的人工智能算法、机器学习算法、数据挖掘算法等，“边”侧的用户手机、电脑、平板、智能面板等终端设备的控制程序、数据搜集和处理

程序等，以及“端”侧智能家电设备的指令接收和执行程序等。这些程序和算法在设计或编写过程中，可能存在后门或者漏洞，在数据调用、处理和分析过程中可能会产生信息泄露，还可能在算法运行过程中存在数据的恶意拷贝、篡改、删除等非法操作，特殊情况或畸形数据可能造成系统混乱或宕机等等。功能算法安全需要对整个智慧家居网络中功能算法进行安全检测、漏洞挖掘和修补，确保这些功能算法的安全性和鲁棒性。

执行安全一方面是要保障控制流信息的机密、正确和完整，包括“端”侧的口令、指纹、面部、声纹等认证信息、“边”侧和“云”侧发送的下行控制指令及智能算法以及“端-边”交互和“端-云”交互的接入、认证信息等；另一方面是保证硬件底层模组/模块、芯片、操作系统和上层应用程序等的安全性和健壮性，避免软硬件漏洞和后门对家电执行及执行过程中的信息安全产生影响，主要体现在“云”侧服务器设备、“边”侧软硬件和“端”侧智能家电设备的底层硬件、操作系统和应用软件，研究对象主要包括模块/模组、芯片、操作系统和第三方库、各种应用层软件等等。

数据安全、接入安全、算法安全及执行安全有各自侧重的内涵，它们既相互独立，更相互关联，安全技术研发中心的建设内容就是要从这四个方面入手，形成高端智能家电整体信息安全体系。

4.2.2 安全可信关键技术研发及公共服务能力构建

智能家电信息安全问题的具体研究和技术研发过程中，将按照安全技术体系中的数据安全、算法安全、接入安全和执行安全进行课题划分。通过各课题组持续性的理论研究和技术更新，保留各子课题的独立性，便于技术特点和研究技巧的讨论和深入。配合重大课题、专项课题的联合攻关，各子课题可以迅速形成合力、建立关联，聚焦智能家电的信息安全基础理论和基础架构、信息安全关键技术、基本信息安全模组和协议、信息安全标准和检测等研究，协力构建综合、全面的智慧家居信息安全体系。具体课题划分和关键技术如下表。

	数据安全	接入/通信安全	算法安全	执行安全
端	感控信息数据新鲜性、完整性、机	敏感数据访问控制/越权访问	算法漏洞检测修补	固件逆向、固件刷写、升级更新校

	密性、可用性、可控性、不可否认性等 文件、日志保护 设备重用数据清洗 终端/设备数据加密 身份信息管理 数据访问权限	身份信息管理/认证/控制权限管理 非法接入/控制/数据劫持/数据重放 设备 API/网络/人机交互接口安全 口令（生物特征）登录安全	入侵检测算法安全 病毒查杀算法安全 信息处理算法安全 工控算法安全安全 加密算法安全安全	验绕过 设备系统存在密码硬编码、弱口令 旁路攻击、物理渗透、芯片攻击 卡软硬件安全/逻辑安全/内容安全 隐私信息物理安全存储 防盗防破坏防逆向防异常环境
边	网络恶意流量避免 接入和上传信息数据新鲜性、完整性、机密性、可用性、可控性、不可否认性等	网络接入入侵、终端仿冒认证 干扰信号中断通信 信号劫持、窃听、篡改数据 通信延时和中断处理机制	终端设备算法安全 边缘计算算法安全 人工智能算法安全 安全传输算法安全	终端设备的软硬件安全 操作系统安全 网关设备硬件安全 网关设备的管理/设置/运维安全
管	网络数据泄露、篡改 通信完整性校验实现数据传输的完整性保护 网络传输数据新鲜性、完整性、机密性、可用性、可控性、不可否认性等	终端木马网络传播 认证密钥协商安全 信号劫持、窃听、中断、篡改数据等风险 提供通信加密和认证，避免窃听、篡改、伪造以及发送者抵赖等 通信延时和中断的处理机制	WiFi、ZigBee、LoRaWAN、NB-IoT、蓝牙、2/3/4/5G 无线通信协议安全 跨网认证算法 网络协议算法安全（TLS/SSH）	DDOS 攻击 运营商网络致瘫 管两侧信息处理安全/算法健壮性
云	云存储数据被拖库、数据泄露 云信息存储、处理过程的数据新鲜性、完整性、机密性、可用性、可控性、不可否认性等	越权操控 身份伪冒 核心网络堵塞	人工智能算法安全 可信计算 云计算安全 大数据存储、处理、分析等算法安全	云平台本身的安全 服务器安全 入侵检测/防火墙病毒查杀等 可信计算

表（4-1）高端智能家居信息安全关键技术总览

数据安全：1）密码算法研究，如（轻量级）加密算法、完整性验证算法（消息验证码 MAC）、（轻量级）签名算法、无线传感网络加密等算法的分析、应用和设计；2）数据采集安全，如传感器精度、异常数据处理、采集数据可靠性、真实性研究；3）数据调用安全：同态加密、可信计算等研究。力求各层次、各

环节敏感数据的完整性、机密性、可用性、可控性和不可否认性。4）隐私计算，如多方安全计算、联邦学习、可信执行环境以及多方中介计算的研究。

算法安全：1）在“云”侧，可信人工智能研究、智能算法安全、云计算任务调度算法、资源分配算法等安全性分析与设计、算法程序和服务器的漏洞挖掘和修补研究、密码算法安全性分析和设计等研究；2）“管”侧协议软件库包的安全性分析和设计、协议程序安全性、模糊测试技术研究等；3）“边”侧手机、主机、智能控制面板中的程序安全、二进制分析技术研究等；4）“端”侧家电设备执行算法、工控算法、各类轻量级算法安全研究等。力求各层次各算法的鲁棒性、普适性和可解释性。

接入安全：1）“端”侧智能家电设备即插即用、合法性检测、双向身份认证技术、生物特征与经典密码结合、轻量级可重构认证算法、轻量级加密算法、SOTP 技术等研究；2）“边”侧访问控制、安全代理技术、（轻量级）认证协议等技术研究；3）云接入安全研究，如服务器安全、防火墙技术、安全代理、网络攻防技术；4）协议安全性分析与设计研究，如无线传感网络协议、认证密钥协商协议、无线网络协议、物联网协议、OAuth2.0 等接入认证协议安全性研究等。

执行安全：加密芯片检测和设计、加密模块/模组设计、旁路攻击检测、冗余控制/多路控制技术、特定条件下的（轻量级）可信计算、各类操作系统安全性检测与设计等技术的研究。

4.2.3 关键技术研发

4.2.3.1 身份认证技术

设备认证

智慧家居信息安全中的身份认证主要针对接入设备的身份认证，常用的设备身份认证主要通过设备的标识信息进行认证，常用的有 802.1X 接入认证技术，Portal 接入认证技术和 MAC 地址认证技术。MAC 地址认证技术与其它两种技术的区别在于用户不需要安装任何客户端软件就可以对设备进行认证，且 MAC 地址的唯一性也为接入安全提供了重要保障。在智慧家居信息安全中，MAC 地址认证技术是一种简单易用的身份认证技术，可以确保只有授权设备才能访问网络，从而

提高接入安全性。

云平台认证

国外比较成功且已经被广泛使用的物联网智慧家居开放平台是 MiOS 平台。平台允许用户远程地控制、监听以及自动控制家庭和办公室中的智能设备。作为一个开放平台，采用了一种简单的认证机制：在第三方应用向服务器发送的所有控制请求的中加入用户的用户名、口令以及网关的序列号作为用户认证信息。为了加强安全性，采用发送所有含有用户信息的控制请求，对于不支持的应用在发送请求时将口令域置为空，当服务器接收到不包含口令的请求时只响应那些没有安全要求的设备。目前国内还没有基于物联网的智慧家居开放平台的实现，而 MiOS 平台的认证机制显然不适应具有更高开放性的智慧家居平台。

开放平台已渗透到互联网的每个角落。纵观这些开放平台，主要采用两个安全机制：OpenID 和 OAuth 协议，通过它们的使用为开放平台提供规范、简洁、安全的认证授权管理机制。其中，OAuth 协议正逐渐成为公认的互联网开放授权标准。传统的身份验证模型中，客户端使用资源拥有者的身份证书（通常是一个用户名和口令）来访问服务器上的资源，这就产生了访问资源的安全和隐私问题。协议在这个模型的基础上引入了第三个角色：资源拥有者，即将客户端与用户分开。在模型中，客户端已不再是资源的真正所有者，它通过资源拥有者而不是所属的服务器来控制资源的请求。为了让客户端访问资源，它必须先从资源拥有者那里获得访问许可，这个访问许可以以令牌或者共享密钥的形式表示。令牌的目的是使资源拥有者不需要与客户端共享其证书。与用户名密码方式不同，令牌以一定的受限范围和生命周期被分发，并且可以独立地撤销。

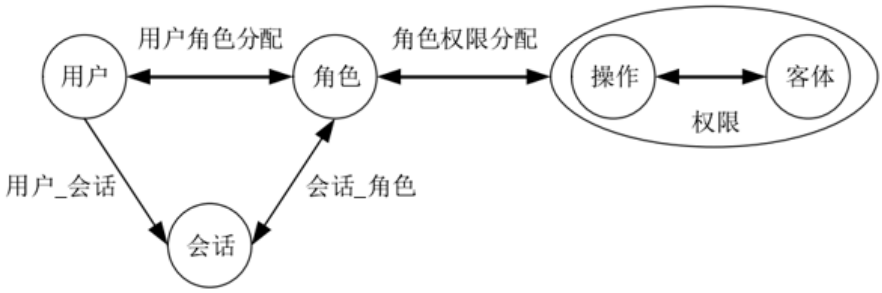
访问控制技术

访问控制技术自上个世纪 60 年代被提出以来得到了广泛的关注和研究，并依据其实际应用在不同阶段提出了针对不同问题的访问控制模型，主要包括：自主访问控制（Discretionary Access Control, DAC），强制访问控制（Mandatory Access Control，MAC）、基于角色的访问控制（Role Based Access Control，RBAC）和基于属性的访问控制（Attribute Based Access Control，ABAC），不

同的访问控制模型根据其不同的访问控制策略拥有各自的授权方式。

基于角色的访问控制技术是在用户与权限中加入角色，使得用户与权限实现逻辑分离，极大的方便了权限管理，减少了整个系统复杂程度，符合智慧家居信息安全需求的简单化和高效性。目前智慧家居访问控制中使用的模型主要是RBAC，其他模型的应用研究还不成熟。该技术的基本思想是将用户划分成与其在组织结构体系相一致的角色，角色直接拥有权限而不是主体，主体则通过角色的分配来实现对客体权限的授权。在系统中角色具有直观性与稳定性，减少了权限管理的复杂程度，从而降低了权限管理带来的工作量。

基于角色的访问控制包括用户（USER）、角色（ROLE）、许可（PERMISSION）等要素。用户是访问系统资源的主体。角色是一种“职位”，用户只有坐在这个位置上，才能实现对客体的访问。许可就是对允许对客体权限的操作。用户可以“担当”多种角色，一个角色也可以让多个用户同时“担当”，每种角色拥有很多种许可，每个许可也可以授权给许多不同的角色。



图（4-3）RBAC 模型框架

4.2.3.2 数据安全技术

终端数据安全

从安全属性角度来看，终端数据安全包括数据的机密性、完整性、来源真实性、时效性等安全属性。

a）通常采取加密算法来保护数据的机密性。采用的加密算法包括对称密码算法、非对称密码算法，对称密码算法相对于非对称密码算法的优势在于高效的加解密效率，计算开销较小。常用的对称加密算法有：分组对称加密算法（如SM4、AES）、序列对称加密算法 ZUC 等。

b)通常采用数字签名/验签或消息鉴别码（MAC）等机制来保护数据的来源真实性。其中数字签名/验签采用非对称密码算法实现，常用的非对称加密算法有：SM2、SM9、ECC、RSA（2048 以上）等；消息鉴别码（MAC）可以采用 HMAC、CMAC 等组合算法实现。

c)通常采用杂凑算法（即密码散列算法）或数字签名/验签等机制来保护数据的完整性。其中常用杂凑算法包括 SM3、SHA2、SHA3 等。

d)通常采用带数字签名的时间戳或序列号来保证数据的时效性，避免防重放攻击。

另外还可以利用已有的安全通信协议对通信数据的安全属性进行保护，如针对 IP 层的 IPSec，针对传输层以上的的 TLCP/TLS（TCP 传输）、DTLS（UDP 传输）等。

在智能家电采用不同的具体通信方式时需要考虑以上的安全机制：无线通信相比于有线通信更容易遭受监听、中间人以及重放等攻击，IEEE 802.15.4 标准在设计时充分考虑了安全问题，其在链路层提供了加密、认证以及重放保护等安全服务。为抵御窃听攻击，ZigBee 协议工作在 2.4GHz 频段，传输率为 250kbps，并支持 128bitAES GCCM 加密模式。Z-Wave 作为另一种流行的通信协议，在 900MHz 频段附近工作，具有 40kbps 与 100kbps 两种传输速率，并通过为每个设备赋予唯一的 PIN／QR 码标识其身份保护数据安全。在 CoAP 应用层协议安全方面，标准版的 DTLS 协议可以提供端到端的安全传输，但其需要双向认证，存在开销过大的问题。

云平台数据安全

当前云平台大数据数据安全保障措施，主要有如下几种：

a）加密技术，为了保障数据的安全，云计算可以根据数据类型通过加密技术来制定加密算法。加密技术一般分为两种：对称加密技术与非对称加密技术。数据在通过网络进行传输之前，对数据采取必要的加密措施，然后再将其上传至云数据中心。

b）隔离技术，由于云平台数据库里储存着大量的数据，所以为了区分不同用户的数据和便于出现问题后对数据进行恢复，采取在数据库里建设隔离数据构架的办法。

c）容灾技术，可能引起数据服务停止的所有防范和保护技术，主要包括数据备份、数据复制、系统迁移等措施。

d）反病毒与入侵检测技术。

智慧家居中的人工智能技术

机器学习和取证分析在工业和商业环境中已经很普遍，在智慧家居环境中也有较好的应用。机器学习可被用于确定系统的行为模式，如网络上的流量、正在运行的应用程序、设备之间建立的通信。机器学习系统将追踪在设备、本地网络或云端中的模式。

在设备层面，本地机器学习系统将通过查看存储器、任务、IP 地址等一系列参数来确定设备的正常运行模式，并确定在正常条件下的运行方式。在只有一种或两种功能的智能家用电器中，通过嵌入能增强机器学习引擎的神经网络加速器（NNA），可实现对行为模式的良好建模。设备可以将其元数据报告给网络级或云级系统，该系统将接收所有这些信息并在众多的设备群中进行分析。

在网络层面，路由器可以查看所有的流量，并可以运用自己的智能来确定联网中的设备何时与外界进行通信。通过使用机器学习引擎，它们可以评估何时出现异常通信，可以检测到从网络到外界的异常数据流，可以将其作为一个问题来报告。反之亦然，它们可以识别针对本地设备的异常流量来源。

在云端，应用程序的主机可以看到非常广泛的设备和网络，并且借助它们大型的计算资源，它们可以追踪整个环境中的实时活动。它们应用了与设备层面或网络层面相同的机器学习概念，但是由于其计算能力，它们可以处理更多的数据，并可以查看庞大生态系统的更加具体的信息。

机器学习在消费领域中的应用是非常广泛的。从检查隐私参数是否已被正确设置并定期追踪，到观察设备的运行、保护消费者的数据和私人信息，机器学习系统成为消费环境的守护者。它被置于设备内、路由器和托管应用的云端中，这些信息安全层共同协作，为设置设备和保护消费者提供指导。

4.2.3.3 隐私计算技术

多方安全计算

多方安全计算（Multi-Party Computation，MPC）是指在无可信第三方的情况下，多个参与方共同计算一个目标函数,并且保证每一方仅获取自己的计算结果，无法通过计算过程中的交互数据推测出其他任意一方的输入数据(除非函数本身可以由自己的输入和获得的输出推测出其他参与方的输入)。就智能家电而言，这种计算的方式可以通过逻辑电路完成，并植入多方安全计算协议。实现多方安全计算的关键技术包括多方安全协议、加密算法、逻辑电路设计等。其中，多方安全协议是用来确保各方之间的交互符合安全要求的协议;加密算法是用来保护数据的机密性和完整性的算法;逻辑电路设计则是用来实现目标函数的电路设计。这些技术的综合运用可以实现多方安全计算的目标，同时保证计算的正确性和效率。

联邦学习

联邦学习,又名联邦机器学习、联合学习、联盟学习等。联邦学习是实现在本地原始数据不出库的情况下,通过对中间加密数据的流通与处理来完成多方联合的机器学习训练。联邦学习参与方一般包括数据方、算法方、协调方、计算方、结果方、任务发起方等角色,根据参与计算的数据在数据方之间分布的情况不同,可以分为横向联邦学习、纵向联邦学习和联邦迁移学习。其现实意义在于进一步的保护智能家电在数据传递环节中的信息安全性。

可信执行环境

可信执行环境(TrustedExecutionEnvironment,TEE)通过软硬件方法在中央处理器中构建一个安全的区域,保证其内部加载的程序和数据在机密性和完整性上得到保护。TEE 是一个隔离的执行环境，为在设备上运行的受信任应用程序提供了比普通操作系统更高级别的安全性以及比安全元件更多的功能。

多方中介计算

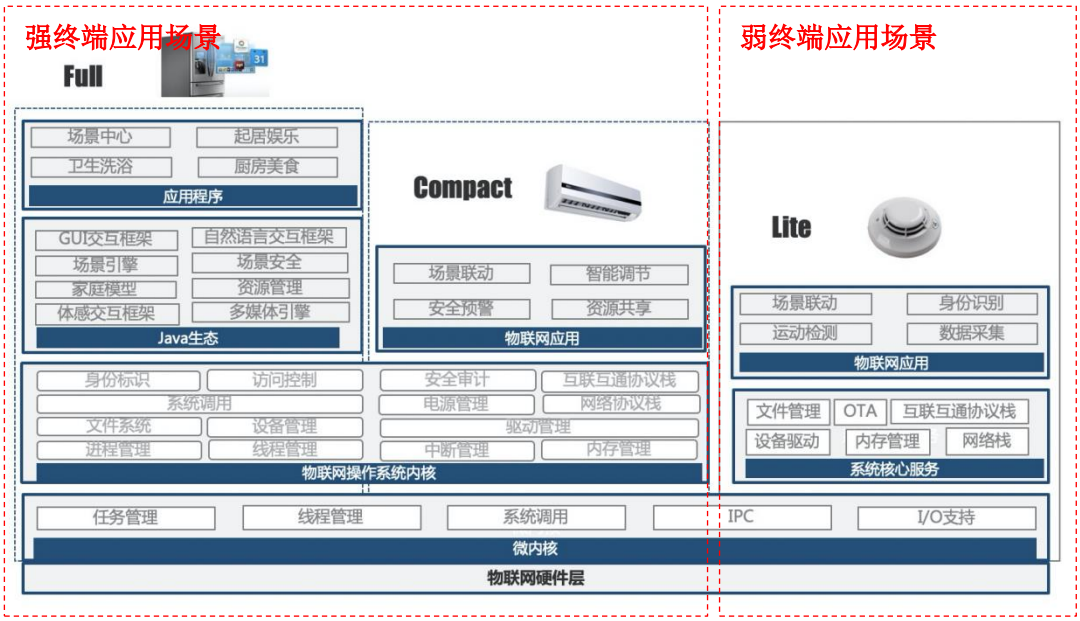
多方中介计算是指多方数据在独立于数据方和用户的受监管中介计算环境内，通过安全可信的机制实现分析计算和匿名化结果输出的数据处理方式，是一个计算管理系统。在 MPIC 中，数据方的原始数据由其去标识化后输入中介计算

环境或平台参与计算，完成计算后立即被删除，匿名化结果数据经审核后按指定路径输出。在 MPIC 的特定环境和规则下，信息数据的身份标识经过加密和标识化的处理，因其算法具有不可逆性，故无法恢复为原始数据，满足了匿名化的一个要求，即不能原复；同时，由于这些去标识化的信息数据被封闭在特定受监管环境或平台中，客观上达到了匿名化的另一个要求，即无法识别特定自然人。故被处理的数据实质可视同匿名化，不再属于个人信息，无需征得个人同意就可进入中介计算环境或平台参与计算。相关技术可以应用于“云管边端”中的各个环节，就关键加密信息，信息交互过程中，尤其是涉及到隐私安全层面，应该得到更为深层的应用于开发。

4.2.4 感控家电终端类安全标准

智能家电终端安全标准

鉴于此各个家电企业的联网化终端产品底层安全技术就可以根据不同产品的功能丰富程度和实际应用场景相结合，呈现模块化趋势。在共享底层关键安全芯片、安全模块或安全 OS 的前提下搭建上层应用平台，支持从繁到简的应用场景。不同企业的规划策略有所差异，但总体上智能网联家电终端产品可从大趋势上划分为强终端和弱终端两个主要分类：其区分主要依据为是否拥有操作系统，或可解读为是否拥有一定运算能力。强终端与之相匹配的底层硬件在强终端中多为 MCU 处理器，或性能处理器，以支撑上层微内核安全可信操作系统，如 TEE 等，或安卓等富操作系统，功能丰富具备一定可扩展性；而弱终端底层硬件多为单片机或 SE 安全芯片，集成嵌入式软件，功能相对简单扩展性差。



图（4-4）终端应用场景

由此强终端安全标准可涵盖安全模块标准（含密码模块应用推广），安全 MCU 标准，安全操作系统 TEE 标准（含安全可信应用标准），基于富操作系统的 APP 安全性标准，安全外设标准。弱终端安全标准可包括安全 SE 芯片标准（含密码芯片应用推广），安全嵌入式软件标准。

身份识别安全标准

实现云端对终端的身份识别功能，主要是提供网联家电设备接入开放通信网络的设备身份标识，这类安全标准应侧重于载体内信息的不可篡改、完整性和可用性，而且由于身份信息载体可能为强终端或弱终端，且计算存储能力受限，其安全机制应尽量轻量化，减少安全负担。

安全网关标准

安全网关是感知层安全能力的“重机枪”，起到承上启下的作用，大量数据由此转发，包括上行数据和下行数据。安全网关安全能力一般包括:设备安全接入能力、数据安全转发能力、安全存储能力、安全协议转换能力、敏感数据过滤能力以及自身安全，其安全标准可以按照安全能力进行分级。

平台安全标准

本类标准主要为物联网生态系统中业务运营使用的通用业务服务平台提出

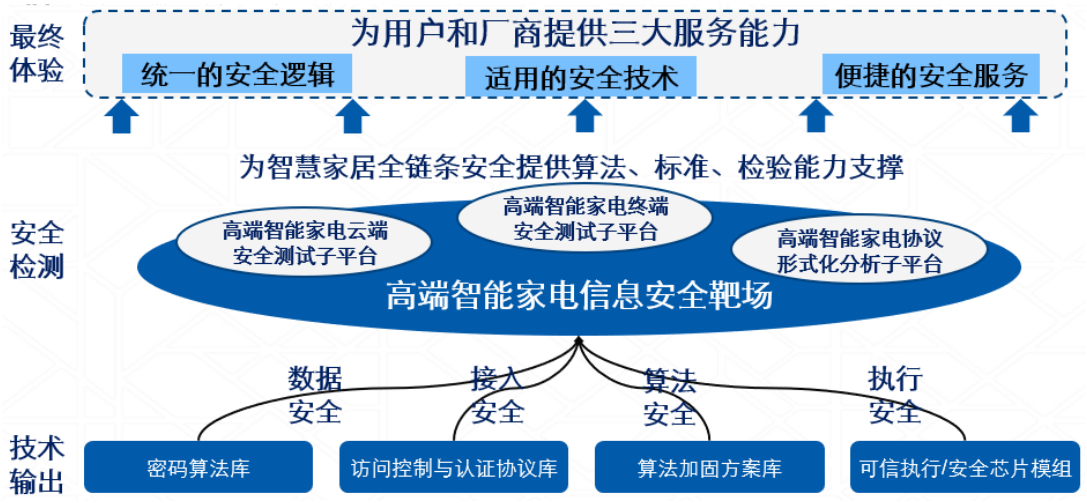
规范要求，包括但不限于数据安全防护、身份认证、访问控制等，引导相关安全技术、产品、及产业的健康发展。

应用安全标准

区别于终端侧的 APP 应用安全，专门针对安装于智能手机中的智能家电控制入口客户端 APP 应用安全性标准，主要包括隐私数据保护，白盒加密，控制接口 API 安全交互，用户身份识别等。

公共服务能力构建

针对高端智能家电的数据安全、接入安全、算法安全和执行安全四个环节，推出高端智能家电安全可信技术平台，包含高端智能家电密码算法库、智能家电公钥基础设施服务子平台、访问控制算法与认证协议库、可信执行/算法加固方案库、专用安全模组/芯片产品等，为智能家电静态信息与动态数据全链条安全提供算法和方案支撑。此外，架设智慧家居信息安全测试靶场，综合协议形式化检测子平台、智能终端信息安全测试子平台、云端安全测试子平台，为智慧家居全系统信息安全提供检测标准、方案、工具和能力。



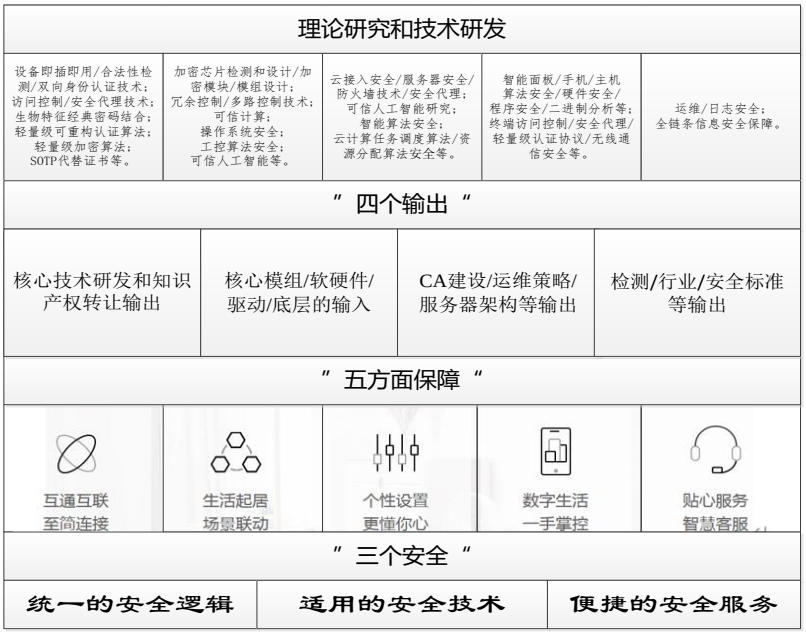
图（4-5）公共服务能力构建

以智能家电公钥基础设施服务子平台为例，采用 PKI 公开密钥基础架构技术，提供面向高端智能家电的身份认证服务，签发和管理数字证书。为智能家居设备提供统一的唯一可信标识，有效统计、管理、分析智能家居设备的状况，建立健全智能家居信息安全体系，保障智能家居厂商业务的信息安全，涵盖智能家居远

程控制、远程 OTA、设备间的指令交互、用户个人隐私数据的存储、用户支付和交易、设备流转等场景下的信息安全。提供密钥管理服务，生成和管理用户主密钥，创建、删除和管理加密密钥以保护数据，对关键信息进行加密，使高端智能家电生产企业和应用开发企业专注于开发加密/解密功能场景。构建起智能家电安全根服务体系。

最终建设目标

通过对智慧家居信息安全需求、关键技术的调研、整理和研究，智能家电安全技术研发中心拟围绕数据安全、算法安全、接入安全和执行安全四个环节，覆盖智慧家居提供的全服务的全链条，着眼智慧家居信息系统的可用性、机密性、可鉴别性与可控性，在课题划分的基础上，聚焦轻量级加密算法、安全通信协议、隐私保护、安全审计、授权认证等信息安全关键技术，着力理论研究和技术研发，通过实现“四个输出”，即核心技术研发和知识产权转让输出、安全核心模组/软硬件/驱动/底层的输入、CA 建设/运维策略/服务器架构等输出、以及检测、行业、标准输出，为用户提供“五方面保障”，即“互通互联/至简连接”、“生活起居/场景联动”、“个性设置/更懂你心”、“数字生活/一手掌控”、“贴心服务/智慧客服”全链条安全，最终在智慧家居信息安全方向实现“三个安全”，即统一的安全逻辑、适用的安全技术和便捷的安全服务。



图（4-6）智能家电安全技术研发中心建设目标

4.3 检测体系构建

4.3.1 可信众测能力构建

传统渗透测试大多以扫描和简单人工检测为主，借助于特征库匹配和扫描；众测服务全部采用数十位专家手工检测，借助于灵活的手法组合、基于业务、社会工程等方式，测试出技术和业务流程的漏洞。智能家居设备众测存在成本问题、过程监管和固件泄露几大问题，在智能家居设备进行众测就要具备可信众测的环境。

可信众测靶场需要具备防止文件泄露的功能，可以根据研究、测试和业务需要，为每位用户分配独立、完整、相同的众测环境，且互不干扰，真正实现软硬件资源“人人独享”，同时还可以创建传统“共享式”众测环境，支持外联安全设备进行大靶场搭建和测试智能家电产品。

4.3.2 云端检测能力构建

智能家居云端服务架构包含 Web 应用、服务器、数据库、中间件四大部分，涉及的安全问题主要分为安全漏洞、配置缺陷及弱口令几大方面。云端检测能力构建主要针对智能家居相关的云端管理平台、OTA 平台等云端相关的平台快速识别资产并发现分析漏洞及安全配置的能力构建。能力构建主要为 Web 应用、系统及数据库漏洞扫描设备、配置核查扫描设备及弱口令扫描设备。

4.3.3 固件检测能力构建

智能家电设备中的固件就是系统文件，系统所有的功能都在固件中，通过对固件进行解密和解包就可以获取系统文件信息，安全人员通过对关键文件进行逆向分析可以进行漏洞挖掘。固件检测能力构建需要具备安全可信及自动化检测智能家电设备固件安全隐患的服务平台。该平台通过自动化的方式从固件自身信息、敏感信息、代码安全、配置风险、CVE 漏洞等多个检测维度，识别和分析车联网设备固件可能存在的风险漏洞，提前发现安全问题，提升车联网设备的安全强度，避免固件漏洞被恶意利用导致信息泄露、设备功能故障等，也降低厂商的更新、回收和升级成本。

固件升级确认

a)安全要求：固件应具备通过升级方式修复安全漏洞的更新机制，且更新前应得到用户确认。

b)测评对象：智能家电的固件。

c)检测方法：1、查看操作系统是否具有自动和手动更新功能；2、如果具有自动更新功能，检查是否可以自动更新操作系统；3、手动更新功能，检查是否可以手动更新操作系统，并在更新前是否具有用户确认提示。

d)预期结果：如果以上测评方法内容 1、2、3 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

固件来源和完整性验证

a)安全要求：对于远程下载升级固件的场景，应对固件更新文件的来源和完整性进行验证，验证通过才可升级。

b)测评对象：智能家电的固件。

c)检测方法：1.在升级服务器中添加用于测试的新版本固件，尝试启动固件升级，验证固件升级前是否对固件升级包验证来源可靠性； 2.尝试修改固件升级文件的内容，进行系统更新，验证是否可以通过完整性校验完成更新。

d)预期结果：如果以上测评方法内容 1、2 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

固件传输安全

a)安全要求:固件下载传输通道应采用安全机制,防止中间人劫持或者嗅探。

b)测评对象：智能家电的固件。

c)检测方法：检查固件下载链路是否可防止中间人劫持或者嗅探。

d)预期结果：如果以上测评方法内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

固件断点续传

a)安全要求：若固件升级失败，应保持升级前原有版本且可以再次升级。

b)测评对象：智能家电的固件。

c)检测方法：尝试推送不正确的固件给智能家电，使升级失败，验证智能家电是否恢复到之前可用的版本。

d)预期结果：如果以上测评方法内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

固件安全保护

a)安全要求：应对固件进行安全保护，确保固件不能通过串口读取等手段被提取出来。

b)测评对象：智能家电的固件。

c)检测方法：尝试通过串口读取固件，验证是否能够读取成功。

d)预期结果：如果以上测评方法内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

固件代码防篡改

a)安全要求：固件中的关键代码及重要数据应具备防篡改、防逆向等功能。

b)测评对象：智能家电的固件。

c)检测方法：通过逆向分析方法，验证固件中的关键代码及重要数据是否具备防篡改、防逆向等功能。

d)预期结果：如果以上测评方法内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

安全启动

该检测项包括如下内容：

a)安全要求：智能家电芯片应支持安全启动，启动时对固件（uboot、kernel、

rootfs)或 Flash 关键分区进行完整性验证,确保验证通过后系统才能正常启动。

b)测评对象：智能家电硬件内置安全模块芯片。

c)检测方法：1.查看是否具备基于密码算法保护的安全启动（SecureBoot）硬件保护能力；2.通过激光、电磁、电压毛刺等错误注入手段对这一启动过程进行侵扰，验证是否有效。

d)预期结果：具备安全模块的芯片应具备安全启动功能。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

服务裁剪

a)安全要求：对操作系统进行服务裁剪时，应符合模块最小化原则，仅保留必需模块。

b)测评对象：智能家电操作系统。

c)检测方法:审核开发文档或相关技术文件,查看操作系统进行服务剪裁时,是否满足模块最小化原则，且仅保留必要的模块。

d)预期结果：如果以上检测方法内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

服务端口

a)安全要求:操作系统应仅开放产品说明书或技术文件中明确必需开放的服务端口，关闭非必需服务端口。

b)测评对象：智能家电操作系统。

c)检测方法:检查操作系统是否已关闭对应产品说明书或技术文件所要求的非必需端口服务。

d)预期结果：如果以上检测方法内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

系统加固

a)安全要求：操作系统应进行安全加固，具备防止逆向工程的能力。

b)测评对象：智能家电操作系统。

c)检测方法：利用检查工具，核查操作系统是否进行安全加固，具备了防止逆向工程的能力。

d)预期结果：如果以上检测方法内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

用户权限分配

a)安全要求：对于支持多个用户账号的系统，用户权限分配应遵循最小化原则，普通用户只拥有系统赋予的最小权限，禁止越权操作。

b)测评对象：智能家电多用户操作系统。

c)检测方法：1.创建多个用户账户，验证用户权限分配是否遵循最小权限原则；2.检查普通用户是否只拥有系统赋予的最小权限；3.尝试越权操作，该越权操作是否被禁止。

d)预期结果：如果以上检测方法内容 1、2、3 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

默认配置修改

a)安全要求：对于可配置服务的系统，应具备修改默认配置的功能，具体功能要求包含但不限于修改默认身份和认证信息、服务启用和禁用、应用访问控制等。

b)测评对象：智能家电操作系统。

c)检测方法：查看对于可配置服务的系统，是否具备修改默认配置的功能，具体功能要求包含但不限于修改默认身份和认证信息、服务启用和禁用、应用访问限制和应用后台刷新、数据上传、数据下载限制及监控。

d)预期结果：如果以上检测方法内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

4.3.4 移动端检测能力构建

智能家电 APP 包含智能家电系统中的 APP 及手机 APP 应用两大类，涉及移动端 APP 分为 Android 和 ios 两大平台。移动端检测能力构建需具备深度静态检测技术、动态检测技术和源代码扫描等能力，可以全面评估应用的安全问题，准确定位问题根源，呈现详细的安全问题详情，并提供代码修复示例。

不但具有强大的安全检测能力，能够检测第三方 SDK 的安全问题和应用权限使用情况，还具有检测结果自主验证与编辑、批量应用安全统计及版本安全管理等丰富的平台功能。在平台的管理系统中，可自主实现白名单库、第三方 SDK 库、敏感词库等的添加和管理。

APP安全

智能家电 APP 一般用于远程管理设备，用户通过无线协议连接设备，向设备下发配置信息，获取设备状态等。由于 APP 开发人员设计不当，部分智能家电相关的敏感信息，可能会以硬编码的形式存储在 APP 中，通过对 APP 就行安全分析可以获取到这些敏感信息。智能家电是由多个应用组合而成的，而安全遵循木桶定律，任何一个应用的安全性不足都会拉低整个设备的安全性。应采取以下措施建设应用安全：

1）避免对外开放端口研发应用程序时，应尽量避免对外开放端口，对本地提供服务的端口应绑定本地回环地址（127.0.0.1），从而减小攻击面。

2）启用安全编译选项在编译应用程序时，应使能编译器安全相关的选项，如不可执行栈（NX）、栈溢出检测（Stack Canary）、地址随机化（PIE、ASLR）、RELRO 保护等。

3）安全加固核心代码逻辑应进行加固混淆，提升第三方进行逆向分析的门槛，如使用安全编译器进行编译，或使用二进制加固工具对可执行文件进行加固。

4）避免 WEB 漏洞当智能家电内置 WEB 服务时，应注意避免出现常见的 WEB 漏洞类型，如 SQL 注入、命令注入、越权等。

AI安全

机器学习和取证分析在工业和商业环境中已经很普遍，在智慧家居环境中也有较好的应用。机器学习可被用于确定系统的行为模式，如网络上的流量、正在运行的应用程序、设备之间建立的通信。机器学习系统将追踪在设备、本地网络或云端中的模式。

在设备层面，本地机器学习系统将通过查看存储器、任务、IP 地址等一系列参数来确定设备的正常运行模式，并确定在正常条件下的运行方式。在只有一种或两种功能的智能家用电器中，通过嵌入能增强机器学习引擎的神经网络加速器（NNA），可实现对行为模式的良好建模。设备可以将其元数据报告给网络级或云级系统，该系统将接收所有这些信息并在众多的设备群中进行分析。

在网络层面，路由器可以查看所有的流量，并可以运用自己的智能来确定联网中的设备何时与外界进行通信。通过使用机器学习引擎，它们可以评估何时出现异常通信，可以检测到从网络到外界的异常数据流，可以将其作为一个问题来报告。反之亦然，它们可以识别针对本地设备的异常流量来源。

在云端，应用程序的主机可以看到非常广泛的设备和网络，并且借助它们大型的计算资源，它们可以追踪整个环境中的实时活动。它们应用了与设备层面或网络层面相同的机器学习概念，但是由于其计算能力，它们可以处理更多的数据，并可以查看庞大生态系统的更加具体的信息。

机器学习在消费领域中的应用是非常广泛的。从检查隐私参数是否已被正确设置并定期追踪，到观察设备的运行、保护消费者的数据和私人信息，机器学习系统成为消费环境的守护者。它被置于设备内、路由器和托管应用的云端中，这些信息安全层共同协作，为设置设备和保护消费者提供指导。

4.3.5 硬件检测能力构建

智能家居设备相对传统 IT 面临类型众多、ECU 的硬件形态多样的挑战。家居终端普遍应用嵌入式操作系统，其对实时性要求较高，运行有大量代码的终端硬件，是与外界无线通信并实现实际控制的核心器件。单件的终端不仅实现控制设备动作的具体执行，还负责整个系统的数据交互。因此家居控制器的信息安全至关重要。家居控制器的信息安全取决于控制器所采用的硬件系统是否满足信息安全要求。硬件系统导致的固件信息泄露给不法分子深入分析控制器提供了便利。智能终端硬件在接触式场景中，面临着通过 USB、SD 卡接口、外壳中暴露的调试

接口获取高权限 shell 或者低权限提取后再注入命令，更换关键配置数据的问题。

对于更深层次漏洞项的挖掘和利用，往往需要拆解终端硬件，通过硬件调试接口、拆解芯片、读取存储的方式得到终端硬件中运行系统的固件和关键的配置信息以及个人的隐私信息，在得到如上信息后，不法分子可以通过逆向、模糊测试、静态测试、动态调试的方法，找到更深层次的漏洞点。

NAND Flash 固件提取工具 艾普全功能 NAND Flash 烧写器 NPR4000B 支持 8MByte(44Mbit)到 128GByte(1024Gbit)的 NAND Flash 的快速烧录,具有 4 个高速烧写通道,适合具有预装资料的车载导航电脑,网络摄像头,网络摄像机,手持智能设备,学习机,数码相框,网络播放机,高清机顶盒,蓝光 DVD 机,游戏机,电子书,点读机,语音地图机,监控类等产品在大规模生产中使用,加密 CF 卡,加密 U 盘,加密 SD 卡,固态硬盘等存储工具的 Flash 原始数据复制。

eMMC 固件提取工具 RT809H 编程器为维修行业通用编程器，拥有智能识别、高速读写、高速传输、性能稳定、过流保护、支持芯片广泛的特点。

NOR Flash 固件提取工具艾普 PRO3000A 烧录器可烧录 8MB(44Mbit)到 128GB(1024Gbit)的 NAND Flash 支持封装 TSOP48、SOP40、FBGA43、LGA52、LGA42；可烧录 512KB(4Mbit)到 128MB(1Gbit)的 NOR Flash,支持封装 TSOP48、TSOP54、BGA44、TSOP40;支持文件烧写和母片烧写两种方式：采用单座结构设计,可对 NAND 及 NOR Flash 芯片进行烧录,烧录过程实时校验写入数据,绝对保证数据的正确,支持目前市面上多种软硬件平台的 NAND Flash 芯片的管理方式。

AVR 仿真器模块 采用金滩电子科技 AVR JTAG ICE 仿真器，仿真器提供 USB 口和标准 JTAG 接口，兼容性较好，仿真器主要用于 AVR 芯片的调试仿真。可以与 Atmel 公司的 AVR Studio + iccavr 或者 WINAVR 相配合的一套完整的基于 JTAG 接口的片上调试工具，支持所有 AVR 的 8 位 RISC 指令的带 JTAG 口的微处理器。JTAG 接口是一个 4 线的符合 IEEE 1149.1 标准的测试接入端口(TAP)控制器。IEEE 的标准提供一种行之有效的电路板连接性测试的标准方法(边界扫描)。AVR 仿真器可以用来进行芯片硬件仿真，如程序单步执行、设置断点，通过硬件仿真可以了解芯片里面程序的详细运行情况。AVR JTAG 仿真器主要用来对芯片进行仿真操作，支持 debugWIRE、JTAG 和 PDI 接口的 AVR 芯片，同时也可以通过 JTAG 接口对芯片编程（将程序写入芯片)。设备提供 USB 口和标准 JTAG 接口，兼容性较好。支持芯片 ATmega128、ATmega128L、ATmega14、ATmega142、ATmega142V、

ATmega145、ATmega145V、ATmega149、ATmega149V、ATmega14L、ATmega32、ATmega323、ATmega323L、ATmega32L、ATmega44、ATmega44L 等，针对产品需要可以实现单步、连续、断点、变量具有数据或程序空间断点，对 Flash、EEPROM、熔丝位、加密位进行编程。支持仿真器固件可无限升级，向上向下都兼容，支持 AVR STUDIO 软件 4.12/4.14/4.14/4.17/4.18。设备有 3.3V-5V 宽电压支持、过流保护，具有 0.5A 可恢复保险丝和数据缓冲电路。

SPI FLASH 烧录器模块 采用西尔特 410p，设备支持 242 个厂商 3.5 万个型号芯片实现存储器数据读取、修改、擦除。使用 USB2.0 通讯接口，全面支持 WinXP/Vista/Win7/Win8/Win10，完美兼容 32/44 位系统，具有量产烧录模式，一旦芯片正确插入插座 CPU 即自动启动批处理命令，无需人工按键，同时满足 SPI 传输的以下方式：1.时钟极性(CPOL-Clock Polarity)：空闲时的极性高（polarity high）或者低（polarity low）。2.时钟相位(CPHA-CLock Phase)：在上升沿还是下降沿采样数据。具有过流和 ESD 保护，有效保护编程器和电脑 USB 口不致因意外损坏,支持 93/24/25/BR90 系列 SPI NORflash 存储器和 4.2-5V 各种电压器件，支持过流、短路保护和最大 512M 存储。

串口工具模块 DTool 功能 USB 转 UART 串口模块 使用 CP2102 核心芯片作为芯片主控，性能好，高速可靠稳定，使用 USB2.0 接口，通过 50mA 自恢复保险丝提供过流保护，有对应的电源和信号传输指示灯，支持 windows 系统 32 位、44 位系统驱动支持,实现 3.3V 和 5V 切换开关,USB->UART 支持通讯波特率 50bps～2Mbps 可配置非常规波特率，支持 5、4、7 或者 8 个数据位，支持奇校验、偶校验、空白、标志以及无校验。

STLink 下载器模块 采用 HWA YEH ST-LINK V2 支持全系 STM32 SWD 接口调试支持全系列 STM8 SWIM 下载调试仿真。采用 USB2.0 接口进行仿真调试，单步调试，断点调试，通过高速 USB2.0 与 PC 端连接，支持 STM32/STM8 满足高性能、低成本、低功耗的特性，支持 JTAG/SWD，从而满足再接口上调试程序，并使用接口来实现与目标板的通信的需求，支持 ST-LINK Utility v2.0 及以上版本和固件升级，提供 5V 电源输出，提供 I/O 口保护和 LED 状态提示灯。

ULink 下载器模块 采用世讯 ULINK2 仿真器，设备即插即用、支持基于 ARM Cortex-M3 的串行调试、支持程序运行期间的存储器读写、终端仿真和串行调试输出、支持 20-pin 连接线。具备无限的 RAM 断点，在 Cortex-M3 上最多 4 个断

点，JTAG 时钟<=10MHz，Memory R/W 约为 28K，Flash R/W 约为 25K，支持 USB2.0、JTAG RTCK、Single-Step(Fast)、Real-Time Agent，支持 ST、Texas Instruments (ARM7/ARM9/Cortex Family)，支持程序运行期间的存储器读写、终端仿真和串行调试输出。

调试功能接口安全

该检测项包括：

a)安全要求：具备调试功能的接口，应在出厂时设置为默认关闭输入接口。

b)测评对象：智能家电硬件接口。

c)检测方法：1.判断调试接口的依据：（a.电路板上存在引脚（有无插针都算）b.电路板上有引脚功能标记 c.依据芯片技术手册，使用万用表确定对应引脚功能）（注：业务功能接口不算调试接口，但不应有引脚功能标记）2.判断调试接口是否默认关闭（根据调试接口的类型，选择使用“usb 转 ttl”、“jlink”，“stlink”等工具连接调试接口查看是否有数据）

d)预期结果：审查智能家电技术文档并检查具备调试功能的接口，如存在则默认关闭输入接口。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

调试接口口令安全

该检测项包括如下内容：

a)安全要求：对于具有调试接口的智能家电，需配置用户名、口令等方式进行认证授权，禁止用户直接登录；应符合口令复杂度要求，字符长度不少于八位，由大小写字母、数字、特殊符号中的两种或两种以上类型组成。

b)测评对象：智能家电硬件接口。

c)检测方法：1.通过访谈，了解调试接口位置，询问用户名和密码，验证是否符合口令复杂度要求。2.尝试弱口令，验证是否可以进入调试接口。

d)预期结果：审查智能家电技术文档并检查具备调试功能的接口，如存在则应满足口令复杂度要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

USB接口安全

该检测项包括如下内容：

a)安全要求：对于具有 USB 接口的智能家电，应保证做好智能家电数据的相关安全隔离和保护，防止智能家电连接到计算机或其它智能家电时，造成数据泄露。

b)测评对象：智能家电硬件的 USB 接口。

c)检测方法：1.找到 USB 接口，可利用 USB 连接线，通过 adb 连接家电，查看是否能获取家电的 shell。2.找到 USB 接口，查看是否能利用此接口获取敏感数据

d)预期结果：审查智能家电技术文档并检查具备 USB 接口，如存在则应满足安全隔离和保护要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

硬件防拆涂层安全

该检测项包括如下内容：

a)安全要求：应在调试功能的接口处添加环氧树脂涂层，防止逆向工程。

b)测评对象：智能家电硬件接口。

c)检测方法：1.查看表面是否添加了环氧树脂涂层（表面有一层透明薄膜）2.再使用万用表测试是否能导通来验证。

d)预期结果：审查智能家电技术文档并检查具备调试接口，如存在则应存在防拆涂层。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

物理测试接口安全

该检测项包括如下内容：

a)安全要求：应取消物理测试接口、测试点和测试焊盘。

b)测评对象：智能家电硬件接口。

c)检测方法：检测终端智能家电是否已取消物理测试接口、测试点和测试焊

盘。

d)预期结果：不存在任何测试接口、测试点和测试焊盘。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

芯片读写安全

该检测项包括如下内容：

a)安全要求:芯片应具备固件读写保护功能,防止固件被未授权读取或篡改。

b)测评对象：智能家电硬件内置芯片。

c)检测方法：尝试通过 swd、jtag、串口等对芯片上固件进行读取，验证是否能够提取成功。

d)预期结果：固件应无法被正常读出，或读出的固件为加密态。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

侧信道安全

该检测项包括如下内容：

a)安全要求：对于支持安全模块的芯片，应具备侧信道攻击防护能力。安全模块所支持的各种密码算法，在运算时，运算时间、能量消耗和电磁辐射三者与密钥等敏感信息之间没有明显的相关性。

b)测评对象：智能家电硬件内置安全模块芯片。

c)检测方法：1.检测安全芯片运算时运算时间、能量消耗和电磁辐射三者与密钥和敏感信息之间是否存在明显的相关性。2.是否能够抵抗计时攻击、能量分析攻击和电磁分析攻击三种不同的侧信道攻击方法。

d)预期结果：具备安全模块的芯片应具备侧信道攻击防护能力。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

芯片物理安全

该检测项包括如下内容：

a)安全要求：对于支持安全模块的芯片，应具备数据的物理保护能力，防止攻击者通过去除芯片表面封装层而获取存储器数据。

b)测评对象：智能家电硬件内置安全模块芯片。

c)检测方法：1.对安全芯片工作环境进行监控，尝试通过激光或化学开封智能家电去除芯片表面封装层后并试图获取存储器数据时，验证模块是否会产生警告信息，或主动擦除敏感数据和密钥，使芯片进入不可用状态；2.借助微探针台核查是否对芯片内部总线以及存储器等重要敏感电路部分添加物理保护层。

d)预期结果：具备安全模块的芯片应具备数据的物理保护功能。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

安全域隔离

该检测项包括如下内容：

a)安全要求：应具备安全域隔离功能，提供可信执行环境，具备硬件真随机数发生器、密钥生成和加解密、签名验签等运算引擎，加解密运算仅在可信执行环境内部执行。

b)测评对象：智能家电硬件内置安全模块芯片。

c)检测方法：1.查看芯片是否具有安全域隔离功能；2.查看是否具备硬件真随机数发生器和加解密引擎，并通过采集端口采集其生成的随机数种子；3.借助随机数检测工具检查其数据是否为真随机，并满足我国商密或美国 NIST 相关随机数随机性标准；4.核查加解密运算是否只在可信执行环境内部执行。

d)预期结果：具备安全模块的芯片应具备安全域隔离功能。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

4.3.6 通信检测能力构建

通信检测能力系统可通过使用无线通信数据读取、分析和注入功能等工具，对系统、应用进行安全测试。针对不同的无线网络类型和功能，无线安全测试子系统分为蓝牙安全检测模块、WIFI 安全检测模块、蜂窝网络安全检测模块、射频安全检测模块、NFC 安全检测模块和模糊测试模块。无线安全测试子系统主要测试的内容包括通信协议、数据、业务逻辑等。

蓝牙检测 蓝牙检测主要针对车载蓝牙协议的风险进行安全检测，主要检测模块分为蓝牙扫描模块、加密测试模块、蓝牙流量嗅探模块、流量重放模块、拒绝服务攻击模块以及 CVE 检测模块。

Wi-Fi 检测 Wi-Fi 检测主要针对六大方面进行安全检测，WIFI 热点探测模块、WIFI 弱密码破解模块、WIFI 端口扫描模块、WIFI 拒绝服务攻击模块、WIFI 中间人攻击模块以及 WIFI 协议栈漏洞模块。

远程请求验证

a)安全要求：系统应具备对远程控制的请求身份验证和接入认证的能力，避免非法用户或应用对系统进行控制。系统应对不同的应用进程及数据之间实施访问控制管理措施，不同应用程序的进程及数据不能非授权访问。

b)测评对象：智能家电多用户操作系统。

c)检测方法：申请远程控制，验证系统，1.是否具有身份验证和接入认证的能力；2.是否可以禁止非法用户或应用控制系统。当不同的应用进程或数据之间进行访问时，1.验证系统是否具有访问控制机制，2.不同应用程序的进程及数据是否禁止随意互访。如果以上检测方法内容 1、2 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

d)预期结果：如果以上检测方法内容 1、2 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

未公开账号

a)安全要求：系统不应预留任何未公开帐号，所有帐号应可被操作系统管理。

b)测评对象：智能家电多用户操作系统。

c)检测方法：1.查看系统是否禁止预留任何的未公开帐号；2.查看所有帐号是否都可被操作系统管理。

d)预期结果：如果以上检测方法内容 1、2 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

隐秘通道

a)安全要求：禁止存在绕过正常认证机制直接进入到系统的隐秘通道，如：

特定接口、特定客户端、特殊 URL 等。

b)测评对象：智能家电多用户操作系统。

c)检测方法：通过渗透测试方法，探测是否存在绕过正常认证机制直接进入到系统的隐秘通道，如：特定接口、特定客户端、特殊 URL 等。

d)预期结果：如果以上检测方法内容为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

默认口令

a)安全要求：用户首次登录智能家电系统，智能家电应提示用户修改默认口令。

b)测评对象：智能家电多用户操作系统。

c)检测方法：通过首次登录智能家电系统，核查智能家电是否具有修改默认口令的提示功能。

d)预期结果：如果以上检测方法内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

系统API访问控制

a)安全要求：对于能够安装外部应用的系统，应提供对系统 API 的访问控制机制，防止应用对系统接口的非授权调用。

b)测评对象：智能家电操作系统。

c)检测方法：查看对于能够安装外部应用的系统，是否提供对系统 API 的访问控制机制，防止应用对系统接口的非授权调用。

d)预期结果：如果以上检测方法内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

口令复杂度

a)安全要求：系统登录口令应满足复杂度要求，字符长度不少于八位，由大小写字母、数字和特殊符号中两种或两种以上类型组成。

b)测评对象：智能家电操作系统。

c)检测方法：1.将少于八位的弱口令设置为系统登录口令，验证是否设置成功；2.验证登录口令是否由大小写字母、数字和特殊符号中两种或两种以上类型组成。

d)预期结果：如果以上检测方法内容 1 为否定，2 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

通信协议安全

a)安全要求：对于支持远程连接的智能家电，系统应使用安全的通信协议保障通道安全，包括具备建立通道时的身份鉴别和传输数据的机密性与完整性保护能力。

b)测评对象：智能家电操作系统。

c)检测方法：对于支持远程连接的智能家电，检查系统所使用通信协议是否可保障鉴别信息、用户个人信息等敏感数据传输的保密性和完整性；1.是否未使用 SSL2.0.0、SSL4.0 和 TLS1.0 等已曝存在高危漏洞风险的协议版本；2.在建立通道时，是否进行身份鉴别；3.在传输数据时，是否对数据进行机密性与完整性的验证。

d)预期结果：如果以上检测方法内容 1、2、3 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

日志记录

a)安全要求：对于通过 Web 进行远程管理的智能家电，对其进行管理和配置时，必须经过登录认证，其登录/退出过程需有日志记录。日志内容应至少包括登录使用的账号、登录是否成功、登录时间以及远程登录发起方的 IP 地址等信息。

b)测评对象：智能家电操作系统。

c)检测方法：通过 Web 进行远程管理的智能家电，对其进行管理和配置时：1.验证是否须经过登录认证；2.检查在登录/退出的过程，是否有日志记录；3.日志记录内容是否至少包括登录使用的账号、登录是否成功、登录时间以及远程登录发起方的 IP 地址等信息。

d)预期结果：如果以上检测方法内容 1、2、3 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

e)判定原则：测试结果应与预期结果相符，否则不符合要求。

4.4 典型企业智能家电信息安全理念与最佳实践

4.4.1 海尔-安全态势感知平台助力安全系统构建

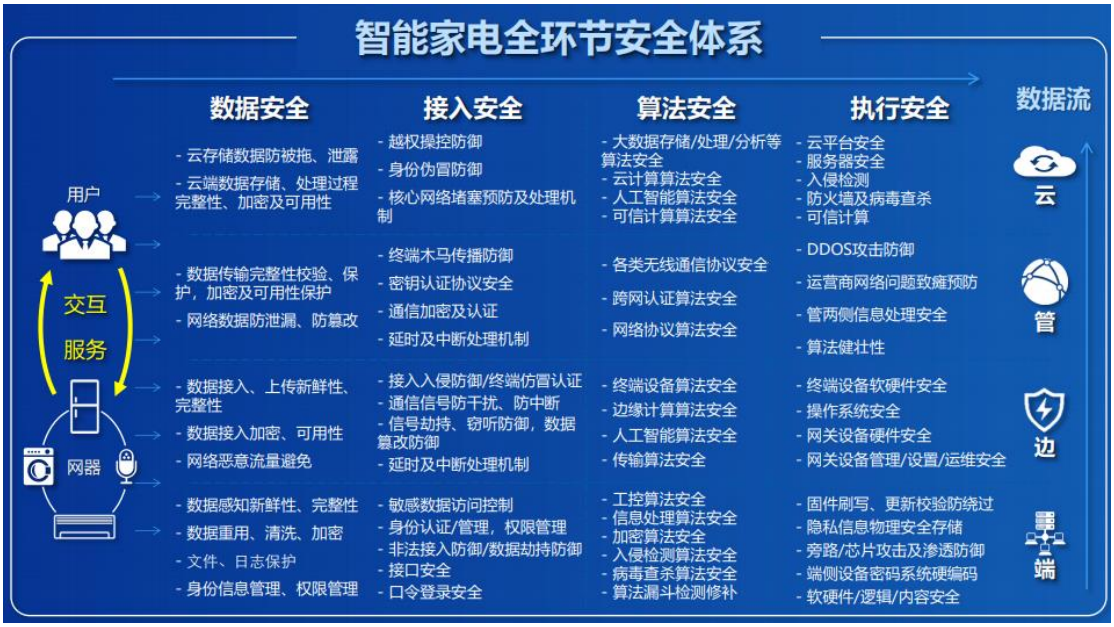
海尔物联网智能家居业务提供基于物联网智能设备的通信、人工智能、数据处理等服务，是智能家电、智能语音、手机 APP、设备及应用数据的接入与业务处理平台，是提供智慧家庭领域全开放、全兼容、全交互的智慧生活平台服务。系统的核心业务包括基础设施平台、开放平台、IoT 网关服务、用户管理、大数据、AI 智能等服务。通过海尔物联网平台提供物物互联服务，实现了 3C 产品、智能家居系统、安防系统等的智能化识别、管理以及数字媒体信息的共享。海尔智能家居使用户在世界的任何角落、任何时间，均可通过打电话、发短信、上网等方式与家中的电器设备互动，目前拥有几千万用户数量。

海尔通过技术和管理对业务进行全面安全防护，有完善的安全组织与内外安全合规制度，通过边界安全、风控安全、应用安全、设备安全、通信安全、数据安全、边缘安全 7 个维度对平台与业务安全进行立体防护。

此外，海尔物联网平台积极落地实施国家网络安全等级保护 2.0 三级要求以及《中华人民共和国个人信息保护法》的要求，从管理到技术对平台进行了积极的安全防护工作，对个人隐私数据进行了有效保护。海尔云平台通过安全的架构，将预测、防御、监控和响应融为一体，构建出安全态势感知平台，为用户提供持续的安全监控、分析和快速响应能力，实现安全的统一策略管理，有效预测风险，精准感知威胁，提升响应效率，全方位保护物联网资产的安全与业务的高效开展。

海尔安全技术研发中心重点开展安全技术、核心芯片与核心软件、集成模组

和智能技术方面的研发工作。研究轻量级算法、通讯协议、隐私保护、授权认证、安全框架与审计系统；研发安全 MCU、加密芯片、可信计算、同态芯片、WIFI 芯片、SOC 芯片等；研究轻量级物联网 OS、开发环境与系统框架；研制传感器、IOT 模组、6LoWPAN 模块；研究海量数据采集与分析、场景联动与推理、图谱挖掘与关联等智能数据处理与交互技术，并建立了完备的智能家电全环节安全体系，获得了相关成果基础。



（图 4-7）海尔智能家电全环节安全体系

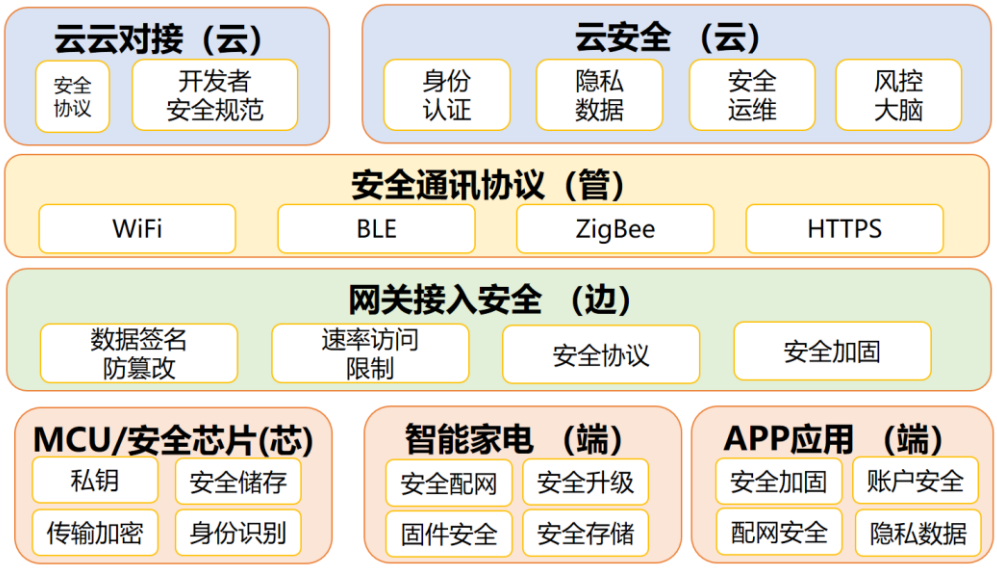
（图 4-8）海尔安全技术成果基础

4.4.2 美的-4S 云管端+风控大脑+1M 隐私管理体系

美的 IoT 隶属于全球领先的家电巨头美的集团，致力于构建面向智能家居、智能安防、人工智能等领域为用户提供全路径、全场景、全触点的以智能家电为核心的安全、便捷的物联网解决方案，为客户提供优质的智能服务，同时不断优化智能家居和相关服务的使用体验。目前，美的智能家居全线布局，融合美的数字化 MES(Manufacturing Execution System)优势，已经形成「4S 云管端+风控大脑+1M 隐私管理体系」，成为美的构筑智能家居安全体系的基座，为智能家电产品上市与使用等安全问题提供了一套完整的解决方案，切实保障用户隐私和数据安全。

图（4-9）美的智能家居使用场景

美的 IoT 在智能家电领域，使用美的美居 APP，微信小程序，鸿蒙操作系统原生应用等入口，依托全球范围内部署的美的物联网平台，为 300 个产品品类超 5000 万产品提供智慧的互联、互动服务。温馨智能家庭来自安全的保障，美的 IoT 以智能互联为驱动，在科技智能连接家居的同时，我们把保障用户个人数据的安全作为美的产品与服务的核心生命线，让用户随时随地享受智能便利、安全舒适的智能家居服务。为此美的 IoT 按照 4 Security （风控安全、云安全、数据传输安全、智能家电安全)+1M(安全管理)的原则进行智能家电安全体系建设，确保“云-管-边-端”全链路的安全与隐私得到充分的保护。



图（4-10）美的智能家电系统安全与隐私保护体系

美的 IoT 一直致力于遵循各国的数据安全与隐私保护法规的要求，如我国的《网络安全法》、《欧盟通用数据保护条例(GDPR)》以及《加州消费者隐私法(CCPA)》等保护用户的隐私安全。美的作为消费者信赖的全球化科技集团，严格遵守我国《消费者权益保护法》，并依据我国权威部门发布的《App 违法违规收集使用个人信息行为认定方法》、《GB/T-2020-35273 信息安全技术-个人信息安全规范》、《工信部 APP 侵害用户权益专项整治 8 项要求》的要求提升美的美居在 App 端的合规性及个人信息保护能力。同时美的 IoT 落实国际权威的安全标准及行业最佳实践，如 ISO27001 信息安全管理体系及 ISO 27701 隐私管理体系，建立并形成了具有美的特色的智慧家居隐私管理与安全体系。

美的 IoT 在遵循全球数据安全及隐私保护法规的前提下，持续提升自身的隐私保护能力，致力将美的 IoT 打造成消费者信赖、行业认可的隐私安全标杆品牌。为确保信息安全与隐私保护策略的贯彻执行，美的 IoT 在 2019 年正式成立隐私保护办公室，通过流程制度、技术防护、审查和评估机制等建立完善的安全管理体系。同时，美的聘请全球知名律师事务所和咨询机构作为数据合规供应商，确保美的符合各国法律合规要求。截至目前，美的 IoT 已经具有较为成熟的数据安全及隐私保护管理制度，以及相对应的隐私保护能力，美的的智慧家电产品、APP、云平台、SDK 等通过了全球多个广受认可的信息安全与隐私合规领域的认证。以下是一些重要的信息安全认证的例子。

- ETSI 303645 消费者物联网信息安全:基准要求

- CCRC IT产品信息安全认证证书（智能家居产品）
- CCRC移动互联网应用程序(App)安全认证
- CCRC 物联网设备互联互通组件EAL4+认证
- ePrivacyApp个人数据保护技术认证
- UL物联网安全评级证书
- NISTIR 8259安全要求
- 物联网安全联盟ioXt认证
- TRUSTe企业隐私体系认证
- PCI DSS 认证
- CSASTAR云安全国际认证
- APEC 跨境数据合规
- ISO 27001 信息安全管理体系认证
- ISO 27701 隐私信息管理体系认证

通过这些国内外的信息安全认证表明美的的智慧家电安全和隐私体系已经达到较高的安全水准，能为用户提供安全放心的智慧家电产品与服务。美的 IoT 始终坚持“科技尽善，生活尽美”的公司愿景，始终坚持通过科技创新提升产品品质和服务质量，专注于持续技术革新，并以此贡献人类，提高人类生活质量，促进人类生活更舒适、更轻松、更安全、更美好，让每个人和家庭享受到智能家居带来的美好生活。

4.4.3 小米-隐私保护理念与默认安全基本原则

图（4-11）小米已获得的安全与隐私认证

截止 2022 年 3 月 31 日，小米在全球范围内的 AIoT 连接设备数达 4.78 亿（不包括智能手机、平板及笔记本电脑）。小米将保护全球每一位用户的安全与隐私融入整个业务流程中，始终秉承从设计着手的隐私保护理念（Privacy by Design）和默认安全基本原则（Security by Default）。早在 2016 年，小米就通过了国际权威安全机构 TrustArc 的隐私认证，在 2019 年，小米通过了 ISO27001 和 ISO27018 安全体系认证，代表了国际标准组织对小米安全隐私保护能力的认可。此外，近年来，小米的多款 AIoT 产品还分别获得了英国标准局（BSI）、美国 UL、德国莱茵等国际第三方权威认证机构颁发的数据安全证书。特别值得一提的是，2022 年上半年，小米公司成功获颁美国国家标准技术研究院（NIST）的数据安全框架注册证书。

标准规范：小米为所有生态链企业提出统一的安全基线要求，并定期为其提供专业培训，安全基线基于小米 AIoT 安全实验室的内部&外部安全测试漏洞库，并结合国内外法律法规和标准规范。意在帮助国内物联网企业，在应对以上安全挑战时，可以有一个开放，便捷，落地的知识库，让企业在设计和开发消费级物联网终端产品时，可以对照此指南，规避一些基本的安全与隐私保护风险，以快速提升产品的安全与隐私保护能力。

流程制定：小米非常重视 IoT 产品的网络安全保护能力，集团规定所有小米产品在设计、研发、测试等阶段均需要纳入安全环节。在设计&研发阶段，集团安全 BP 会对产品进行安全需求评估，帮助业务团队发现产品设计、开发方案是

否满足安全要求；在测试验证阶段，AIoT 安全实验室也会负责验证产品是否满足相应的安全要求。最终，会由 AIoT 安全实验室出具安全测试报告，根据所发现漏洞的影响程度和可利用性，帮助业务综合判断产品安全风险。

技术实现：为了高效的为 IoT 产品提供快速，准确的安全评估和技术测试工作，小米自主研发了 AIoT 安全评估和测试平台，平台集成了合规评估，技术测试，提测审查和自动化报告等一系列功能，可以大大提升安全测试效率，保障在大量的产品上线需求下，仍能确保其安全问题及时被发现和解决。与此同时，平台具备持续监测能力，可以时时监控在售设备是否有安全问题，影响哪些产品，并及时告警。同时，小米对外 SRC 和 hackerone 平台及时接收白帽子提交的安全漏洞，并进行验证和确认，及时修复 IoT 产品的安全漏洞，确保其在统一的安全水平内。

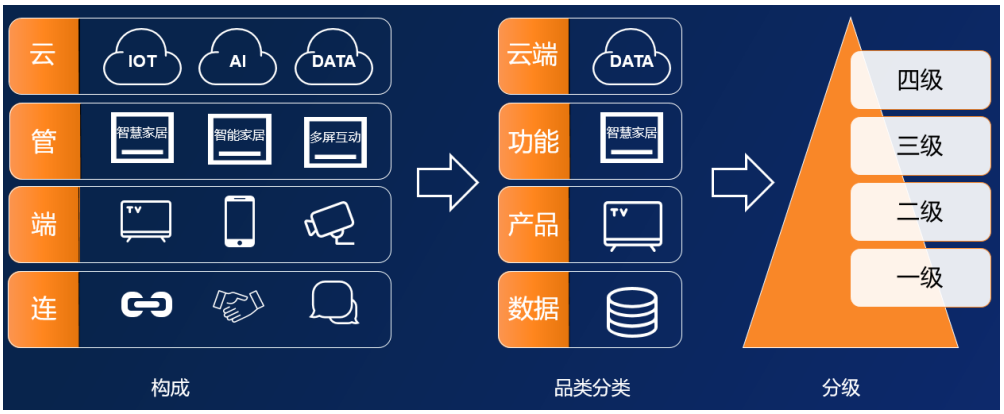
除了统一的安全基线，小米定制化提供统一的安全芯片，WI-FI，BLE 等定制模组供生态企业使用，尽最大程度的减少生态公司产研人员安全水平参差不齐可能导致的通信协议上的问题，减少攻击面。

为了更少的上传用户数据，小米一直在努力研发端侧执行算法模型，如 MACE micro 将在更多的应用到端侧语音识别，端侧行为检测等等产品上，并将一直努力致力于新兴安全与隐私技术的研究和实践，更多的应用到 IoT 产品中去，减少安全和隐私风险。

4.4.4 TCL-全品类智能家居产品定制安全策略

图（4-12）TCL智能家电安全管控架构

用户对智能家居的依赖，使得智能家居设备成为了人们的必需品。而智能家居设备的安全性则成为用户日益关注的话题。对于智能家居产品的信息安全理念和安全实践，TCL 采用了分类分级、全流程管控、全品类覆盖的方法，来治理 AIOT 发展下各类智能家电的安全管控。从安全设计、安全事件和安全测试三方面作为抓手，结合产品安全等级分级标准，对不同型号的智能家居产品采取不同的安全治理策略，以求达到覆盖全品类产品从设计、开发、测试、生产到售后的全流程安全管控，打造全品类智能家居产品的安全底座。

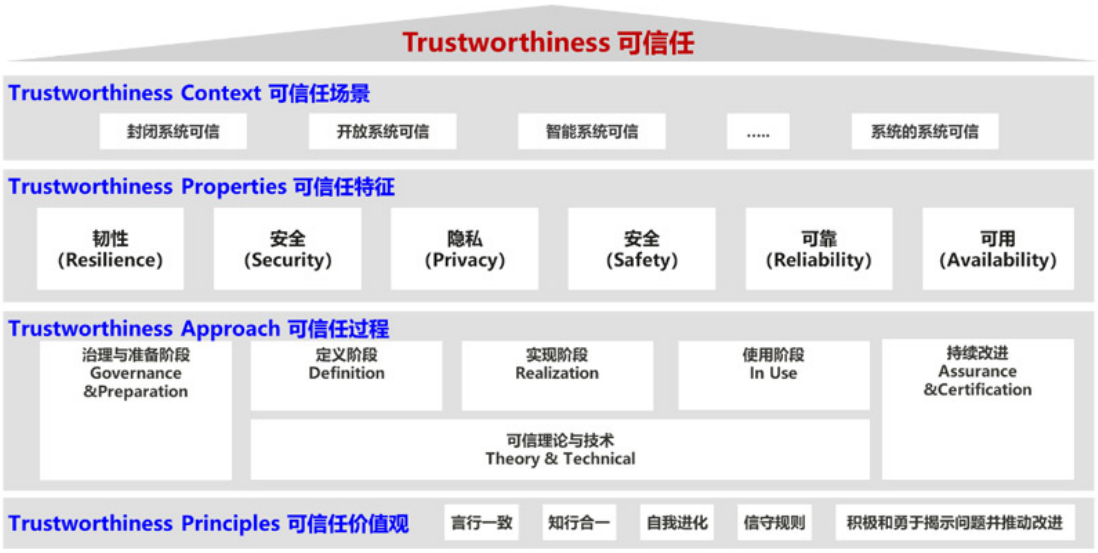


图（4-13）TCL安全分级

随着 AIOT 技术的发展，互连互通技术也在逐步覆盖用户家庭的各类设备，接入网络的家居设备也在逐步增加。对于庞大的家居设备，TCL 采用分类分级的策略来统一管理各个产品。智能家居的构成分为了云管连端，“云”代表业务云，如 IOT 云、AI 云等，负责处理智能家居设备的业务请求；“管”代表云端与终端的管道，打通云端与终端，为用户提供综合服务；“端”代表智能家居设备和智能家居应用；“连”代表终端之间的连接协议，是智能家居互联互通的基础。TCL 依据云端、功能、产品、数据等信息进行评估，对“云管端边”进行安全分级。不同安全分级的“云管端边”也将采取不同的安全措施来保障网络安全和用户数据安全。

2021 年 6 月，TCL 的 RT51 电视通过了德国 TüV 的 ETSI EN 303645 认证。ETSI EN 303645 “物联网消费品的网络安全”是由 ETSI（前身为欧洲电信标准协会）开发，该欧洲标准详细介绍了广泛接受的有关物联网消费设备安全性的“最佳实践”。

4.4.5 华为-构筑并全面实施端到端的全球网络安全保障体系



图（4-14）华为可信任框架

华为坚持独立的商业精神，全力为客户网络和业务的安全运营提供保障支持。为客户服务是华为存在的唯一理由。无论是面临自然灾害、社会冲突、还是网络攻击，都全力与客户共同维护网络的稳定、可靠、安全运行。

为了持续交付高质量产品和服务，需要有先进的业务流程保障。华为自 1997 年起聘请了世界知名公司，为华为提供业务流程咨询。基于网络安全的要求，华为在公司标准流程、基线、政策和规范中融入了所需要的最佳实践。这种方式使网络安全成为华为日常经营的标准动作，而不是亡羊补牢。华为将网络安全规范嵌入到 12 个公司流程与业务模块。早在 1999 年，华为就开始了网络安全旅程，发布了首批安全技术规范，以增强产品与解决方案的安全性。

今天，ICT 正在从一个垂直行业演变成全社会的平台性产业，使能各行各业的数字化、智能化转型，驱动新一轮工业革命，推动人类社会迈向万物互联的智能世界。全面云化、智能化、软件定义一切等发展趋势，对 ICT 基础设施产品的可信提出了前所未有的要求。可信将成为客户愿买、敢买一个产品的基本条件。可信不仅仅是产品外在表现的结果，更是产品内在实现的过程，是结果和过程的双重可信的高质量。

华为认为，网络安全是数字化转型的基础，数字化程度越高，安全事件危害越大。为了应对持续增加的网络威胁，政府监管机构、安全产业、企业客户逐步形成以“正向建、反向查”为基础的网络安全建设框架。正向建包括基础设施可

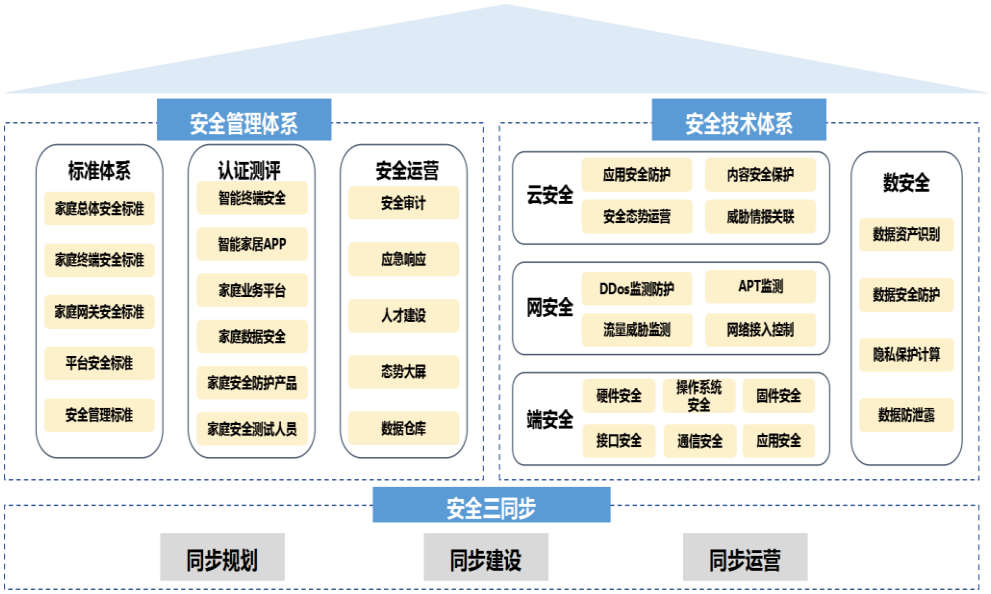
信、网络可信和身份可信。反向查则包括全域监测、智能防御和一体安全。华为安全推出的 HiSec 3.0 安全解决方案体系正是该安全建设框架的落地，具备智能分析、动态检测、全局防御、内生可信四个特征，为客户提供准、快、稳的安全防御，构筑韧性网络。

华为公司把网络安全和隐私保护作为公司的最高纲领。华为将在遵循 ISO9000 的质量管理体系、遵循 ISO/IEC/IEEE 15288 和 12207 的系统工程和软件开发过程之上建设更加强壮的管理系统，使每一位具备可信价值观的员工，基于华为可信任过程相互协作创新，开发出具备可信特征的产品，给客户提供可信的高质量产品，并持续改进。

华为对业界主流安全标准、流程规范、指导书，以及法规指令、白皮书、学术论文等 150+篇文档开展研究,我们发现每一个标准不一定都是完备的，或者关注点各自有侧重。未来在电信行业、在 ICT 社会里面构建全联接的基础底座，需要什么样的可信标准？为了在设计和信任之间建立起桥梁,便于产品定义者和设计者、以及产品的使用者和运营者对如何可以达成可信形成一致地理解，我们结合华为自身大规模的研发、网络部署和运维经验，有设计大型复杂产品的系统知识和系统架构能力。我们从系统工程的行业共识出发，基于可解释、可落地、可验证和有相当业界共识基础的四个原则定义华为可信框架。

4.4.6 中国移动-打造“端边网云”联动的智慧家庭安全运营防护体系

中国移动以“连接+算力+能力”服务体系为底座，依托运营商算网为基础，融合接入安全、隔离安全、基础安全机制等安全能力，面向智能家居场景、用户、设备、生态等实现网络安全防护“三重境界”和“一体化全程可信”愿景。即实现智能家居“资产不可知”、“威胁不可达”、“系统不被控”的一体化安全防护效果，推动家庭网络从单点防控迈向全程可信。



在安全三同步的基础上，构建管理体系、技术体系一体化安全架构，为家庭领域用户提供安全服务。

安全管理体系：标准体系构建方面，在 TC260 牵头制定 GB/T 41387—2022《信息安全技术 智能家居通用安全规范》国家标准，并在 ISO SC27 将国家标准成果转化成 ISO 27403 国际标准，将中国的先进理论带入国际视野、先进实践与国际接轨，为提升全球家庭物联网安全水平贡献“中国方案”。在 CCSA TC11 立项《智能家居设备安全分级要求》行业标准，深度参与 OLA 联盟系列标准《智能家居互联互通 通用安全技术要求》的研制工作；成立智能家居安全实验室，开展常态化智能家居安全测评服务，累计检测设备 980 款，消除安全风险 3885 个，挖掘上报 CNVD 智能家居设备原创漏洞 10 项。并在测评基础之上，联合中国网络安全审查技术与认证中心，推出业界首个智能家居安全认证服务。建立健全的智慧家庭安全应急工作体系，组建安全运营专家团队。

安全技术体系：打造“Andsec 智慧家庭安全运营防护体系”，在端侧，突破智能家居终端的性能局限，研发低功耗、轻资源的嵌入式安全 SDK，提供基于异常检测、漏洞扫描的终端威胁监测能力，依托“智家 ID”、“一机一密”的终端安全认证与数据安全加密能力，实时保护智能家居终端设备安全，规避设备被控所导致的规模性安全事件发生风险。用户体验上，实现零配置，免安装，一键授权即可实现快捷入网绑定及账号登录。在网络侧，打造智能安全网关，并形成全流量安全检测、内容安全审核、应用安全防火墙、数据安全海关等多项安全能力，实现暴露面隐藏、上网行为管控、隐私数据保护、不良信息拦截等防护效

果。在云侧，打造基于家庭安全大脑的集中化安全威胁态势感知体系，对家庭网络中存在的诈骗网站、恶意行为、网络攻击等安全风险进行全面的监测。防护 2.26 亿家庭，赋能 246 家智能家居厂商。

5. 智能家电信息安全技术发展的新展望

5.1 物联支付是智能家电的新场景

物联网支付诞生是市场供需两面互相作用催生的产物。在供给侧，若干新技术出现及与成熟技术的整合推动物联网规模商用，为物联网支付的可行性打下基础。比如物联网技术的快速发展促使设备日趋联网化，智能化，单一设备可承载的计算能力大大提升，从而使设备具备支付处理的能力。同时，传感器技术结合人工智能和云计算为设备填上“眼睛”与“大脑”，物联网设备可以具备自动化地根据用户状态获取支付验证信息或发起支付交易的能力。在需求侧，物联网时代的到来，也促使物联网产业链的相关各方积极寻求一种新的解决方案。对于用户，“懒”是推动生产的核心动力，用户希望简化支付流程，借助物联网设备的感知能力实现无感支付，支付发起由现有的用户主观驱动转变为设备的事件化驱动。

对于高端智能家电而言，单一的家电终端创新竞争力逐渐弱化，终端生产厂商急需向链条化服务进行转型，围绕智能家电终端打造生态链，深度参与智能家电所在生态的每一环节。支付作为实现生态闭环的重要一步，智能家电终端需要构建自有物联支付能力的家电终端。对于终端产业链上的服务商，物联网支付可使服务融于场景，缩短用户触达渠道，增加用户粘性及服务忠诚度。同时自动化的物联网支付可与供应链进行结合，结合支付发起条件，预判用户需求，实现货物智能制造，服务智能生成，降低供应链压力。然而支付安全作为关系到用户切身利益的重要环节，是保证用户财产安全、厂商信誉可靠的命脉技术。支付过程须涉及金融数据，安全等级要求较高，智能家电终端支付需满足设备认证、交易保护、交易可追溯，可证伪三大要求，这就需要在终端设备硬件、操作系统、上层应用、通信协议、接入认证、数据保护等全维度上，对提供物联支付的智能家电解决方案提出了更高、更严苛的安全要求。

5.2 隐私计算技术是智能家电信息安全的新导向

在“云管边端”体系下的各个环节，合作计算变得日益常见。所谓的合作计算是指一群分布在各地的参与者为了一个共同问题进行相互合作求解的过程。合作计算可能在彼此信任的用户之间发生，此情形下的合作计算容易实现。然而当在彼此不完全信任甚至是处于竞争的用户之间需要进行合作计算时，处于自己的隐私或数据的安全考虑，用户往往希望合作计算的过程中其余任意的合作者都无法获得也无法推导出自己的秘密输入信息。

隐私计算是在保护数据本身不对外泄露的前提下实现数据分析计算的技术集合，达到对数据“可用、不可见”的目的；在充分保护数据和隐私安全的前提下，实现数据价值的转化和释放。隐私计算是面向隐私信息全生命周期保护的计算理论和方法，是隐私信息的所有权、管理权和使用权分离时隐私度量、隐私泄漏代价、隐私保护与隐私分析复杂性的可计算模型与公理化系统。

详细的说，隐私计算技术是指在处理视频、音频、图像、图形、文字、数值、泛在网络行为性信息流等信息时，对所涉及的隐私信息进行描述、度量、评价和融合等操作，形成一套符号化、公式化且具有量化评价标准的隐私计算理论、算法及应用技术，支持多系统融合的隐私信息保护。隐计算涵盖了信息搜集者、发布者和使用者在信息产生、感知、发布、传播、存储、处理、使用、销毁等全生命周期过程的所有计算操作，并包含支持海量用户、高并发、高效能隐私保护的系统设计理论与架构。隐私计算是泛在网络空间隐私信息保护的重要理论基础。

显而易见的，与传统数据使用方式相比，隐私计算的加密机制能够增强对于数据的保护、降低数据泄露风险。因此，包括欧盟在内的部分国家和地区将其视为“数据最小化”的一种实现方式。同时，传统数据安全手段，比如数据脱敏或匿名化处理，都要以牺牲部分数据维度为代价，导致数据信息无法有效被利用。就智能家电信息安全问题而言，智能家电用户不希望自己的隐私数据被泄露，要求对自己的数据使用有知情权与控制权；与此同时，智能家居设备厂商希望尽可能多地采集用户数据，以提供更好的智能服务。而隐私计算则提供了另一种解决思路，保证在安全的前提下尽可能使数据价值最大化。

从技术角度出发，隐私计算是涵盖众多学科的交叉融合技术，隐私保护方案不仅有效利用了边缘设备的数据，还避免了用户的隐私数据流出，是非常具有潜

力的研究方向。但目前而言，在智能家居现实场景使用联邦学习技术保护用户隐私的相关研究少之又少，难以在现实场景中落地应用。有基于此，结合智能家电对于用户信息的采集应用与用户对于隐私安全保护需求，隐私计算技术或成为智能家电行业发展过程中一把无可替代的“钥匙”。

5.3 家电行业对于信息安全重要性的新认知

相比仅在物理传统家电仅需要考虑物理层面的安全而言，联网运行的智能家电不仅要保证自身的使用安全，更时刻面临网络安全、数据安全、隐私安全等风险：如网络传输信息被窃听、智能门锁被破解、用户家庭信息数据被泄露利用等。另外，智能设备内生安全系统的不完善，存在信息泄露的安全性性风险，或信息安全构架被恶意攻击，从而导致用户暴露隐私或信息泄露。对应智能家电或智慧家居场景，人民追求舒适便捷的生活服务的同时，追求个人隐私保护和信息安全的需求日益迫切，个人隐私泄露事件将不再以简单的道歉或赔偿而结束，可能上升到法律范畴。结合最新销售数据分析与市场调研，智能家电在信息安全方向的保障已经成为了用户最新要求。

新的消费主力的崛起，必然引起新消费变革。每一个消费群体都有着其明显的消费习惯和喜好。随着 80、90 后消费力量的崛起，如何适应 80、90 后的消费习惯，成为家电行业的课题。物质资源丰富的生活环境，使得 80、90 后在家电消费方面更注重品质和个性化。家电智能化、个性化已经成为一种必然趋势。在分工越来越细的市场趋势下，高端智能家电和智能家居的发展必定是专业化和个性化的。通用场景下的解决方案将逐渐因无法响应用户个性化需求逐渐退出历史舞台。AI 技术的诞生与飞速发展，帮助智能家电对用户产生精确画像，生成用户定制化习惯模型，再此基础上提供精确的服务反应，实现人与家居的共同进步、和谐共处。

然而，个性化的设定对信息安全和隐私保护的带来极大挑战，用户对隐私信息的界定不同、生活习惯不同、产生的画像数据不同，这将导致通用的信息安全解决方案无法兼容和普适。另一方面，如何哪些数据可见、哪些数据可用、哪些数据的可用且不可见，也将成为在安全条件下为用户提供个性化服务首要解决的问题。因此，智能家电种类必将针对不同的应用场景呈现前所未有的多样性，通

用的、大包大揽式的信息安全解决方案面对不同场景的种类繁多的家电终端必将拙荆见肘，个性化的信息安全和隐私保护方案将成为未来高端智能家电的发展必然。

5.4 智能家电信息安全是市场竞争的新指标

广大人民群众对个人隐私和信息安全的需求不断提升，为智能家电产品提供了一个全新赛道：信息安全或隐私安全保护与功能体验俱佳才是未来智能家电产品的核心竞争力。从当前新兴智慧家居产业来讲，家电厂商首先追求的是更多的流量和数据来充实产品销售报表，因此智慧家居产品更多地冠以便捷、智能化的功能和体验，而信息安全作为后发事件往往容易在设计和生产中被忽略。另外，信息安全本身是一门非常专业的技术，大多数厂商的技术集中于家居设备的生产、制造和智能化应用开发，对信息安全技术与知识了解相对匮乏，一方面缺少防御信息和隐私泄露风险的安全意识和技术团队，况且信息安全问题带来的额外成本并不能在丰盈财务报表方面产生立竿见影的效果，再者安全技术或模块对轻量级的家电产品带来额外的开销是否会影响用户的体验的论证无从下手。这种重应用、重体验、轻安全、轻隐私的理念将不断被改善，并且从技术角度看，轻量级低成本的内生可信安全将成为智能家电信息安全未来发展的重要方向。

另一方面，许多厂商即使意识到保护隐私和信息安全，或因为构建安全团队成本过高、研发安全技术难度较大而不知如何下手，若寻求第三方合作，无形中加大了智慧家居产品的成本投入。当然，也有部分厂商不仅意识到智能家电信息安全问题并在技术上进行了研究和开发，但往往采用的是独立协议独立接口，自家产品自成体系，虽然保证了自身系列产品的安全闭环，但严重限制了未来智慧家居设备的扩展与互联互通。用户要么不能随意选择家电产品，要么在家居事务管理中需要操作各厂商搭建的各类平台和程序，违背了智慧家居灵活和便捷的设计初衷。因此，显然易见，信息安全无疑将成为智能家电万物互联的基础底座。

然而白璧微瑕，层出不穷的信息安全与隐私泄露问题成为家电厂商在全新赛道上醒目警示牌。《孟子》有云，人必自悔然后人悔之，家必自毁然后毁之，国必自伐然后人伐之。隐私泄露和信息安全所产生的问题，或能亡羊补牢，但问题为家电厂商带来的负面社会影响，则无法一言蔽之。智能家电信息安全水平将成

为产品竞争力的基本指标。

5.5 共建全面家居生态安全是智能家电行业的新目标

智能家居是综合运用物联网、云计算、移动互联网和大数据技术，结合自动控制技术，将家庭设备智能控制、家庭环境感知、家人健康感知、家居安全感知以及信息交流、消费服务等家居生活有效地结合的生态环境，其飞速发展为家电行业带来了新的窗口，全面安全的家居生态是未来家电行业需要携手共建的新目标。

目前而言，智能家居的功能性还存在诸多空白，或者说不足之处。智能家居首先要创建和运营一个健康、可管理的室内环境系统，结合以上，涉及到住宅财产与生命安全的，更是需要重视问题中的重中之重。如华为推出的 HarmonyOS 3，在不断的促进更多生态产品加入超级终端，实现自由连接。然而如何构建系统的兼容性，也就是不同品牌智能家电单品与系统之间的互联互通、兼容后的全面安全防护以及设备更新等问题，也是智能家居难以普及的主要原因之一。

现实生活中经常会出现这样的情况，消费者买回如 A 品牌的音箱、B 品牌的空调，尽管都是智能单品，但是几乎每个品牌都要在手机上下载一个单独的 APP，并在使用时需要操控多个 APP，极度影响用户对于智能家居产品的新体验。与此相比，国外许多智能厂家约定俗成地采用共同的开放协议，即使不同厂家的产品都可以兼容，很多智能产品消费者只需要购买安装即可同步使用。解决兼容性问题会极大的提高了用户的体验感受，同时对于安全性问题的协同防护，所消耗的资源也会更低。

目前而言，阿里智能、腾讯、海尔、美的等头部家电企业，都在致力于推出自己的互通协议，在这些平台的努力之下，越来越多智能产品互相兼容，这是国内智能家居发展的必然趋势。

结束语

随着人工智能、隐私计算等新技术的快速出现与广泛应用，智能家电为人们的生活带来了极大的便利，但同时也带来了新的信息安全挑战。

在这份白皮书中，我们深入探讨了智能家电信息安全的相关问题，包括智能家电的普及应用、典型安全事故与安全需求分析、相关法律法规与认证标准、信息安全架构的实施与转化以及信息安全技术发展的新展望等方面。呼吁在“产业高质量发展”的国家战略的指引下，通过加强产学研合作，对信息安全始终保持严苛的标准和极致的追求，始终坚守安全底线，创造用户更安心放心的智慧生活体验，为用户提供安全高效的个性化场景服务。正如本白皮书所提出的，要让安全成为了智能家居中“看不见”的“基础设施”。提供从底层芯片、操作系统到云端的立体安全保护能力，构建可信的基础架构，更高的安全性与良好的计算性能，打造安全和用户体验兼顾的安全体验。

我们通过研究认识到，智能家电信息安全是一个综合性的问题，需要政府、企业、用户等各方共同努力。政府应加强法律法规标准的制定和监管，为智能家电行业的发展提供良好的政策环境；企业应加大在信息安全方面的投入，提高产品的安全性和可靠性；用户应增强信息安全意识，选择安全可靠的智能家电产品，并注意保护个人隐私。

未来，随着智能家电技术的不断发展和应用场景的不断拓展，信息安全问题将变得更加复杂和严峻。我们需要持续关注智能家电信息安全的发展动态，加强技术创新和研究，不断完善信息安全保障体系，以确保智能家电行业的健康、可持续发展。

共建全面家居生态安全是智能家电行业的新目标，让我们携手共进，为实现这一目标而努力。相信在各方的共同努力下，智能家电将为人们带来更加便捷、舒适和安全的生活体验。

编委会

编委主任：郑建华、王　晔

编委委员：曲宗峰、林美玉、顾　健、赵宇波、李京春、叶晓虎、罗　蕾、杜　磊、桂志辉、洪焕健、张志亮、杨永清

主　　编：王　凯、李红伟、刘婧璇、陆思奇

主要参编单位及执笔代表：（排名不分先后）

国家高端智能化家电创新中心	王　凯、丁召杰、王绪方、胡栾莎
中国家用电器研究院	李红伟、时　雨
中国电器科学研究院	曾　博、胡　欣
中国信息通信研究院	刘婧璇、王　宁
山东产业技术研究院（青岛）	张　冬
中国质量认证中心青岛分中心	王伟伟
河南省网络密码技术重点实验室	陆思奇、王永娟
浙江大学	胡蕊丹、付　杨
中国海洋大学	李景圣
中国石油大学（华东）	石乐义
中国移动通信集团	鲁　青、赵　帅
青岛移动公司	张　昕
海尔集团股份有限公司	陈启龙
TCL 科技集团股份有限公司	林舜大
海信集团有限公司	陈　健
山东小鸭集团家电有限公司	张守章
长虹电子控股集团有限公司	黄德俊
小米科技有限责任公司	黄宗新
北京智慧云测科技有限公司	安　涛
纬领（青岛）网络安全研究院有限公司	李彦江

启明星辰信息技术集团股份有限公司	王常久
郑州信大捷安信息技术股份有限公司	刘献伦、刘为华
广东为辰信息科技有限公司	赵焕宇、代舒婕
博智安全科技股份有限公司	王路路
北京网藤科技有限公司	赵西玉
海恒数字科技（青岛）有限公司	于祺越