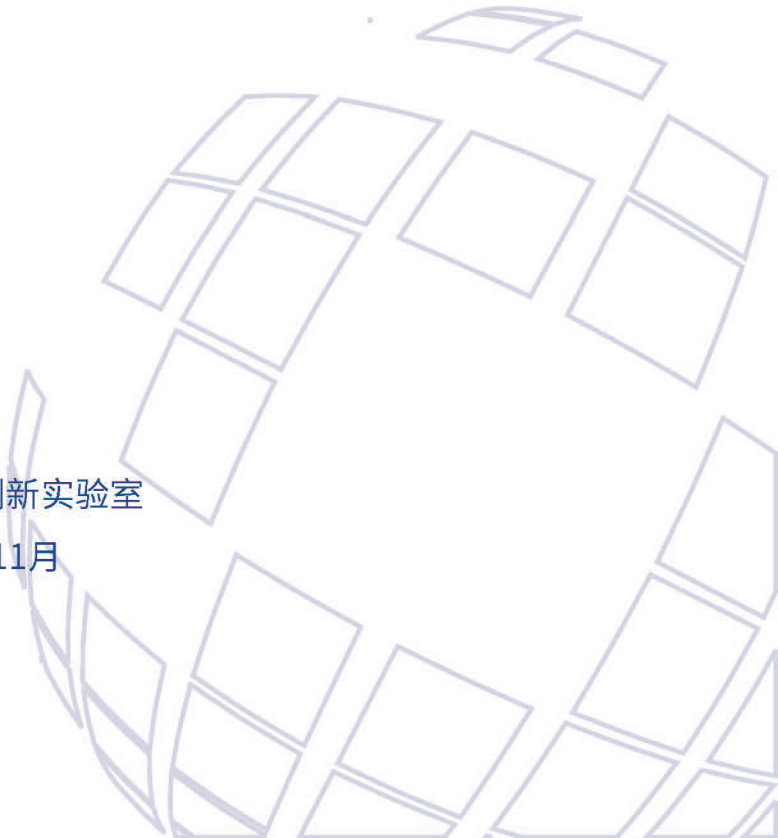
IoT Security Lab
物联网安全创新联合实验室

物联网终端安全白皮书

IoT Device Security White Paper

(2019)



物联网安全创新实验室

2019年11月

版权声明

前　言

随着我国第五代移动通信技术（5G）正式商用，在政策、市场双重驱动下，物联网行业即将进入创新发展期，物联网终端规模也将随之高速发展，物联网卡和物联网终端呈现进一步紧密耦合的发展趋势。

然而，物联网终端安全事件频发，安全隐患凸显，安全形势严峻。物联网终端被破坏、被控制、被攻击，物联网卡被滥用，不仅影响应用服务的安全稳定，导致隐私数据泄露、生命财产安全受损，更会危害网络关键基础设施，威胁国家安全。

为切实承担物联网终端安全管理责任，推动物联网终端安全产业健康发展，履行营造清朗网络空间的责任，物联网安全创新实验室组织，中国信息通信研究院、中国移动研究院牵头，联合中移物联网有限公司、中国移动江苏公司、华为技术有限公司、杭州安恒信息技术股份有限公司、360科技集团有限公司，共同发布《物联网终端安全白皮书（2019年）》。

本白皮书从物联网终端（含物联网卡）和终端安全发展态势出发，梳理物联网终端的普适架构、分析切实存在的安全风险、提出环环相扣的安全保障体系，并结合实际，对物联网终端安全未来发展进行了展望，旨在共商终端安全、共谋管理创新、共创行业发展、共筑产业生态、共话安全未来！

目 录

一、物联网终端概述

（一）物联网终端发展情况

1.应用场景百花齐放，物联网终端呈指数增长态势

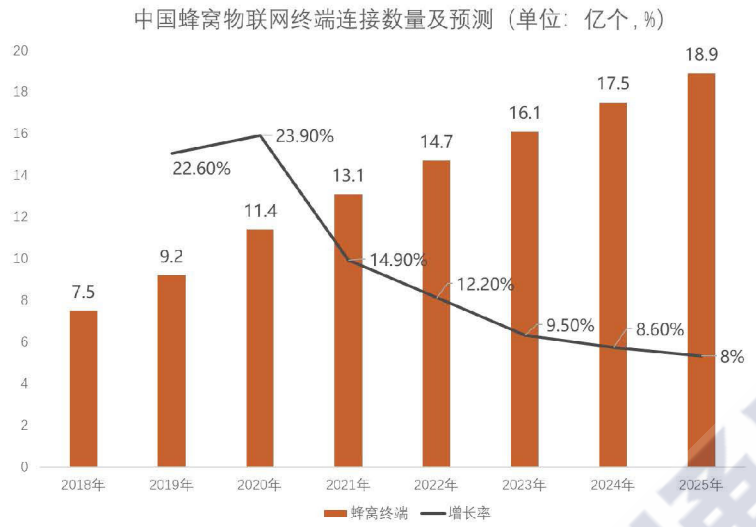
近年来，物联网应用层出不穷、百花齐放，物联网终端渗透进智能交通、智慧医疗、智慧电网、智慧农业等各行各业，走进人民的生产生活，全面推动物联网终端呈指数增长态势。

数据来源：GSMA Intelligence

图 1　全球物联网终端连接数量发展态势图

在全球范围内，物联网终端数量高速增长。截至 2019 年，全球物联网设备连接数量达到 110 亿。其中，消费物联网终端数量达到 60 亿，工业物联网终端数量达到 50 亿。据 GSMA 预测，2025 年全球物联网终端连接数量将达到 250 亿。其中，消费物联网终端连接数量达到 110 亿，工业物联网终端连接数将达到 140 亿，占全球连接的一半以上，具体如图 1 所示。未来，**工业物联网将引领整体连接数量持续增长**，从 2017 年到 2025 年将实现 4.7 倍的增长，年均增

长率达 21%。[1]



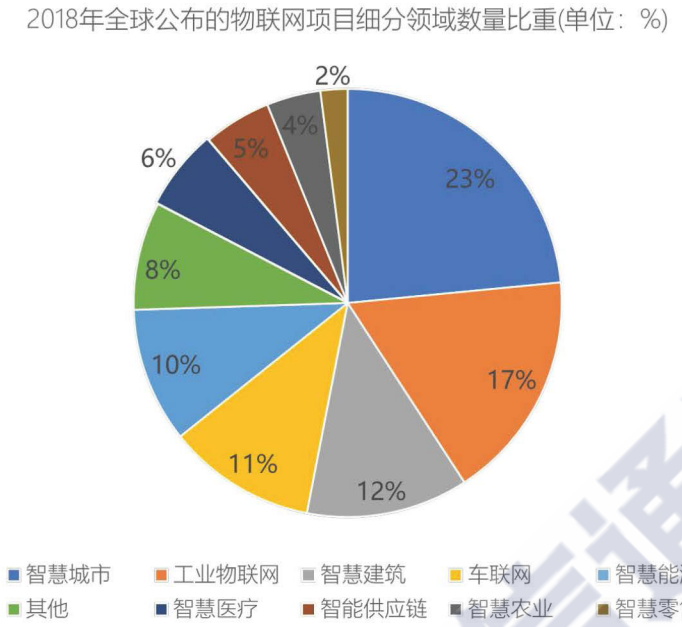
数据来源：GSMA Intelligence

图 2　2018-2022 年中国蜂窝物联网连接数量及预测

在我国，随着信息通信技术的变革发展与创新突破，NB-IoT（窄带物联网技术）、eMTC（增强性机器通信技术）、LoRa（远距离无线电技术）等 LPWA（低功耗广域）技术和应用不断创新突破。目前，我国 LPWA 技术已经形成了以 NB-IoT、eMTC 等为代表的**基于授权频段蜂窝网络技术为主**，以 LoRa 等为代表的**非授权频段技术为辅**的基本格局，共同促进物联网产业快速发展。其中，对于基于授权频段蜂窝网络的技术，三大基础电信企业正加快部署 NB-IoT、eMTC 网络，上中下游产业链已基本形成，网络也已实现了全国覆盖。据 GSMA 统计和预测，截至 2019 年第三季度，我国授权频段蜂窝物联网终端连接数量达到 9.2 亿，预计到 2025 年该数值有望突破 19 亿，具体如图 2 所示。对于基于非授权频段蜂窝物联网的技术，国内 LoRa 阵营力量不断增强，短期内仍将保持快速发展趋势。目前，腾讯、阿里等部分企业已在北京、上海、深圳、杭州等多个城市部署了城域级

[1]数据来源：GSMA（全球移动通信系统协会），物联网安全创新实验室整理分析

LoRa 网络。



数据来源： IoT-Analytics

图 3　2018 年全球公布的物联网项目细分领域数量比重

近年来，物联网应用覆盖的领域也在持续拓展延伸，进一步促进物联网终端数量快速增长。根据 IoT-Analytics 统计数据显示，2018 年，全球范围内公布的 1600 个物联网建设项目中，智慧城市项目占 23%，工业物联网占 17%，智慧建筑、车联网、智慧能源等项目分别占比 12%、11%、10%，具体如图 3 所示。由此可知，当前行业应用市场主要是以企业驱动的应用场景为主，典型应用包括智慧城市、工业物联网、智慧建筑等。

2.蜂窝物联网通信需求迫切，物联网卡快速发展

物联网卡是各类蜂窝物联网终端接入网络的重要媒介。我国三家基础电信企业均已推出物联网卡。截至 2019 年 10 月底，三家基础电信企业物联网卡用户数已近 9 亿左右。其中，中国电信物联网

卡用户数约 1.5 亿，中国移动物联网卡用户数约为 6 亿，中国联通物联网卡用户数约为 1.4 亿。相比于 2018 年底，三家基础电信企业物联网卡用户数达到年度净增 3 亿，同比增长率为 50%。

围绕“功能最小化”要求，物联网卡安全管理逐步收紧。为妥善做好物联网卡安全管理，工业和信息化部陆续出台《工业和信息化部关于贯彻落实〈反恐怖主义法〉等法律规定 进一步做好电话用户真实身份信息登记工作的通知》（工信部网安 2016〔182 号〕）、《工业和信息化部关于进一步防范和打击通讯信息诈骗工作的实施意见》（工信部网安〔2016〕452 号）、《工业和信息化部办公厅关于加强源头治理 进一步做好移动通信转售企业行业卡安全管理的通知》（工信厅网安〔2018〕75 号）等管理政策，要求按照“功能最小化”原则，严格限制物联网卡语音、短信和数据流量功能，并充分利用技术手段加强使用监测及处置。

3. 5G 网络商用部署，促进物联网卡与终端紧密耦合

2019 年 6 月 6 日，工业和信息化部向中国电信、中国移动、中国联通、中国广电发放 5G 商用牌照。2019 年 10 月 31 日，工业和信息化部与中国电信、中国移动、中国联通、中国铁塔共同宣布启动 5G 商用服务，标志着我国正式进入 5G 商用时代。目前，三家基础电信企业已各自在全国十多个城市开展了 5G 组网试验和业务示范，包括北京、上海、成都、武汉、杭州、南京、深圳等，均已开展了 5G 体验用户的招募；中国广电也计划在北京、天津、上海等 16 个城市建设试验网。

5G 网络具备高速率、低时延、广连接等特性，能够更好满足物联网终端连接需求。5G 网络规模商用的快速来临，将极大促进蜂窝物联网终端规模化部署和应用。可以预见，未来使用 5G 网络的蜂窝物联网终端将成为物联网终端的重要形态，**物联网卡和物联网终端将呈现更加紧密耦合的发展态势。**

（二）物联网终端架构及分类

1. 以普适为导向，物联网终端架构轻载且可调整

作为物联网神经末梢，物联网终端主要功能包括：**一是**实现对物理世界真实物体信息的采集、识别和控制；**二是**通过终端的通信接入模块，将采集到的数据信息传输至决策服务端，并接收决策指令。

为实现上述功能，物联网终端通常需具备五个功能模块，分别是**硬件模块、固件系统模块、应用模块、数据模块、通信接入模块。**具体模型架构如图 4 所示。

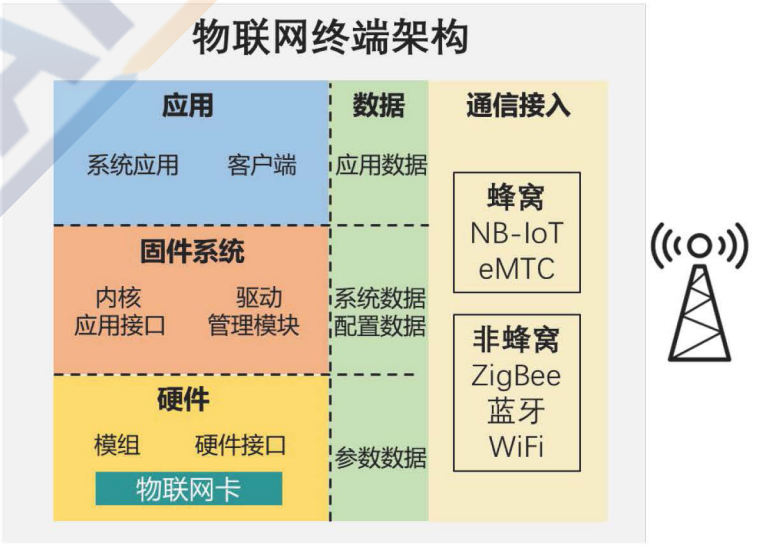


图 4　物联网终端架构

一是硬件模块，是物联网终端的基本模块，涵盖了所有硬件组件和电子元器件。硬件模块为固件系统模块、应用模块和数据模块提供存储的物理介质，也为通信接入模块提供了硬件基础。一般情况下，硬件模块包含物联网终端的主板，以及由主板承载着的处理器、通信模组和调试接口等各个电子元器件。

二是固件系统模块，主要包括系统内核、组件驱动、管理模块等组件。固件系统模块主要提供三种能力：硬件控制能力、软件远程控制能力、计算能力。**硬件控制能力**实现物联网终端可控制不同的硬件设备，实现对物理世界真实物体信息的采集、识别和控制；针对处于无人值守状态的物联网终端，**软件远程控制能力**可实现对固件系统和应用模块的远程升级和远程控制；**计算能力**用于确保物联网终端采集数据和计算结果的精确度。

三是应用模块，主要为预置在固件系统模块中、用于实现其业务功能的软件程序或指令集，它是业务实现的具体模块。通常来说，嵌入式的业务软件程序一般都会将硬件模块收集到的数据做预处理后或者直接通过通信接入模块与决策服务端或其他物联网终端进行交互。

四是数据模块，该模块贯穿所有的物联网终端模块，它依靠硬件模块进行数据收集，依靠固件系统模块进行数据存储，依靠应用模块进行数据处理和分析，依靠通信接入模块向决策服务端传输和上报数据。数据模块包含硬件部分的硬件参数数据、固件系统的系统数据和配置数据、以及应用模块的应用服务数据等。

五是通信接入模块，主要通过蜂窝移动通信网、非蜂窝移动通信网两大类无线通信手段，直接或通过网关间接连接的方式向决策服务端传输数据。通信接入模块主要负责物联网终端和决策服务端，以及物联网终端间的数据传输。

物联网终端架构虽普适，但灵活可调整。在某些应用场景下，物联网终端架构可随应用需求而有所调整。例如，基于单片机的物联网终端，并不具备固件系统模块，而只有简单的应用模块。

2.以网络为界限，有卡终端与无卡终端共生并存

根据终端的网络接入方式来区分，可将物联网终端分为两类：

一是有卡终端，或称蜂窝物联网终端，主要基于基础电信企业提供的物联网卡作为通信媒介，接入以 NB-IoT、eMTC 等**授权频段技术**为代表的蜂窝移动通信网络。其中，NB-IoT 具有广覆盖、大连接、低功耗、低成本的特性，主要适用于终端数据量多、分布范围广、移动性较低、定位时效性不敏感、数据传输量小等场景，如智能抄表、智能路灯、智能井盖等应用；eMTC 具有广覆盖、低功耗、速率高、可靠性高等特性，且支持语音，适用于终端移动性强、传输速率要求高、定位时效性高等场景，如可穿戴设备、智能物流等应用。

二是无卡终端，主要通过嵌入终端内部的无线通信接入模块，接入以 WiFi、低功耗蓝牙、LoRa、Sigfox、ZigBee 等**非授权频段技术**为代表的行业专网和自组织网络。其中，以 WiFi、低功耗蓝牙、LoRa 技术应用最为广泛。WiFi 具有组网灵活、传输速度快等特性，主要应用于智能家居、电力监测等场景；低功耗蓝牙技术具有短距

离、低功耗、低成本、支持复杂的网络连接等特性，主要应用于智能家居、智慧医疗等场景；LoRa 技术主要适合于小数据量、大覆盖范围、低功耗、低成本等需求的场景，如智慧城市、智能园区、智慧工厂等垂直行业领域。

3.以应用为核心，物联网终端整体分类清晰明确

围绕不同物联网应用场景的具体需求，物联网终端可分为三类：

一是消费性物联网终端，即以提升消费者自身体验为主导，是影响人体感知的舒适度，安全性和效率功能的关键因素。根据 IDC（国际数据公司）预测，2019 年消费物联网有望首次成为全球物联网支出的第二大产业。目前，市场上各种智能设备层出不穷，如可穿戴设备、智能硬件、智能家居、智能出行、健康养老等规模化的消费类应用。行业内，小米、华为、中国移动等企业正积极打造各类可穿戴设备产品，如小米手环、华为智能手表、中移找 TA 等。

二是公共性物联网终端，以 NB-IoT、LoRa 等低功耗广域网络为载体，是以服务智慧城市为主导，基于智能传感器及网络全面实现城市连接与城市感知，准确及时感知城市脉搏。该类终端主要应用于智慧城市、智慧安防、智能交通、智能照明、智能停车、智能井盖、智能垃圾桶等。行业内代表企业为海康威视、海尔、华为等。

三是生产性物联网终端，主要面向供给侧的生产性物联网，以服务工业、农业、能源等传统行业为主导，现已成为传统行业转型升级所需的关键基础设施和关键要素。例如，工业物联网终端主要安装在工厂的大型设备上，用来采集位移传感器、GPS（位置传感器）、

震动传感器、液位传感器、压力传感器、温度传感器等数据，通过有线网络或无线网络传输至决策服务端进行数据的汇总和处理，实现对工厂设备运行状态的及时跟踪，提高工作效率。行业内代表企业为霍尼韦尔、西门子、三一重工等。

二、物联网终端安全发展态势

（一）终端安全能力普遍较低，安全事件频发

近年来，在全球范围内，由物联网终端安全事故引发的安全事件频繁发生。一些不法分子利用物联网终端自身存在的缺陷或漏洞，对其进行主动攻击、恶意控制、窃取数据、篡改数据等，对通信网络的正常运行、应用服务的正常运转造成严重影响。根据攻击类型，可将安全事件划分为以下三类：

一是拒绝服务攻击类事件。2016 年 10 月，攻击者利用摄像头安全漏洞，通过恶意软件对美国西海岸大批量摄像头进行控制，进而对 DNS 服务器（域名解析服务器）发起 DDoS 攻击（分布式拒绝服务攻击），导致大面积通信服务处于瘫痪状态，包括通信网络、公共服务、社交平台等。2017 年 2 月，美国某大学 5000 多台物联网终端遭到恶意软件感染，并被远程操控形成僵尸网络，导致校园网络服务出现异常。其中，绝大多数物联网终端为校园自动售货机。

二是设备被控制类事件。2017 年 4 月，三星 Tizen 操作系统被曝光存在 40 多个安全漏洞，包括权限绕过、信息泄露、命令执行、拒绝服务等，共涉及 3000 万台智能电视、1000 多万台智能手机。不

法分子可利用上述安全漏洞对终端发起远程攻击并控制设备。

三是敏感数据泄露类事件。2017 年 7 月，美国自动售货机供应商 Avanti Markets 遭遇黑客入侵内网，攻击者在终端支付设备中植入恶意软件，造成 160 多万用户个人隐私数据泄露，包括信用卡账户、生物特征识别等信息。

（二）终端安全事件影响较广，覆盖垂直行业

随着物联网应用日益普及，物联网终端也与各垂直行业深度融合。数量庞大、种类繁多的物联网终端逐渐覆盖医疗、交通、电力、农业等行业。物联网终端安全事故更将直接影响各垂直行业应用的正常运转。根据行业应用，典型安全事件包括以下五类：

一是智慧医疗。2018 年 10 月，我国国家药监局发布大批医疗器械企业主动召回公告，召回原因是软件安全性不足，极易遭受黑客控制；召回品牌包括美敦力、GE（通用电气）、雅培等；召回设备包括磁共振成像系统、麻醉剂、麻醉系统、人工心肺机等共计 24 万余台设备。

二是车联网。2018 年 6 月，密歇根大学 RobustNet 团队发现通过控制车载终端，可以篡改实时交通信息造成交通拥堵。如多辆车并发被控制，并篡改数据源，可导致整个区域交通瘫痪。2018 年 9 月，比利时 KU Leuven 大学研究人员发现，Pektron 遥控钥匙系统存在安全缺陷，即通过特定设备可截获并读取附近特斯拉 Model S 用户的遥控钥匙信号，并获取钥匙的秘钥，进而对车辆实施偷盗行为。

三是智能家居。2017 年 6 月，我国央视报道大量家庭摄像头遭受不法分子入侵，即通过一款扫描软件，可获取用户家中智能摄像头的 IP 地址，并通过应用弱口令密码的方式远程控制摄像头，盗取或截取摄像头中的画面，偷窥用户日常起居生活，泄漏个人隐私信息。并且，破解获得的摄像头 IP 地址、用户名、密码等用户隐私信息甚至被公开叫卖。

四是智慧城市。2018 年 8 月，IBM 研究团队发现 Libelium、Echelon 和 Battelle 3 种智慧城市主要系统中存在多达 17 个安全漏洞，包括默认密码、可绕过身份验证等，可被攻击者利用实现控制报警系统、篡改传感器数据等恶意行为，从而控制或影响整个城市交通。

五是智能电表。2014 年 10 月，安全研究人员发现西班牙所使用的智能电表存在安全漏洞，可被利用实施电费欺诈甚至是关闭整个电路系统，导致发生大面积停电事件。其根本原因是智能电表内部缺少有效的安全保护机制，可轻易被攻击并控制电路系统。

（三）物联网卡较难实名登记，变身诈骗温床

随着移动互联网应用的发展，不法分子逐渐利用较难登记到实际使用人的物联网卡，间接或直接开展网络、电信诈骗。典型手段包括:

一是用于网络注册，间接实施网络、电信诈骗。随着网络实名制的发展，中央网信办陆续发布了《区块链信息服务管理规定》、《互联网用户公众账号信息服务管理规定》等管理规定，均要求“对使

用者进行基于组织机构代码、身份证件号码、移动电话号码等真实身份信息认证”，推动大量互联网应用采用基于移动电话号码进行网络注册和身份认证，如微信等即时通信类应用。事实上，多数互联网应用并未限制使用物联网卡进行注册和身份认证。而物联网卡由于其自身特性，较难登记到实际使用人，给不法分子带来可趁之机。不法分子可利用未登记到实际使用人的物联网卡注册即时通信类等应用。注册成功后，因违规成本小，可利用其开展网络造谣、网络传谣、违规贷款、违规销售、色情服务等不法行为。2019 年 3 月 10 日，山东省日照市公安局查获一个网络刷单诈骗犯罪团伙。该团伙利用未实名登记到实际使用人的物联网卡注册网络账号，并在网络上发布虚假刷单广告，导致受害人遭遇诈骗，财产蒙受巨大损失。

二是直接用于电信诈骗。部分物联网卡未严格落实“功能最小化”要求，仍可正常使用无限制的语音和短信功能。不法分子可利用未登记到实际使用人、未进行功能限制的物联网卡直接进行语音、短信通信，开展虚假销售、恶意诈骗等诈骗行为。

据《第一财经》报道，我国网络黑产直接从业者已超过 40 万人，一张“黑卡”能带来近 100 元的收入。如果按每年有 4000 万张“黑卡”来计算，每年网络黑产从业者可非法获利达到 40 亿元。而目前“黑卡”中有近 80%是物联网卡，即每年物联网卡所带来的非法获利竟高达 32 亿元。

（四）终端安全产业扬帆起步，催生多样生态

物联网终端高速发展，推动国内外各企业愈发重视、加速布局

物联网终端安全产业、积极构建自有生态，促进呈现多生态共存的局面，包括**基础电信企业、互联网企业、通信企业**等。

基础电信企业加速布局联盟生态。国外，美国 AT&T 公司于 2017 年 2 月，联合诺基亚、IBM、高通、赛门铁克、帕洛阿尔托网络、Trustonic 等企业，成立了物联网网络安全联盟，旨在促进联盟内合作伙伴间的交流和合作，发挥各方力量共同应对物联网安全挑战，推动物联网生态系统的安全发展。**国内三家基础电信企业**均已成立专门的物联网公司，并通过建立物联网产业联盟的方式，寻找合作伙伴，达成产业共识，构筑物联网终端安全生态体系。**中国电信**于 2019 年 9 月成立“天翼物联产业联盟安全生态推进组”，开展物联网安全技术和产业研究，推进物联网安全技术、产业与应用研发；**中国移动**打造“移动物联网产业联盟”，现已拥有 928 家会员企业，涵盖芯片、模组、终端、网络、平台、应用等产业链相关企业，并成立了物联网安全执行委员会，推动物联网安全产业链相关产品广泛应用；**中国联通**打造“物联网产业联盟”，设立公共安全委员会，成员包括航天科工集团、电子科技集团等 30 家知名单位。

互联网企业积极布局主导生态。国内，阿里巴巴于 2018 年 3 月宣布全面进军物联网领域，并成立物联网事业部，定位是“物联网基础设施的搭建者”。为主导生态发展，推进标准化建设，阿里巴巴推动成立了“IoT 合作伙伴计划联盟”（ICA），设立安全标准组，聚集设备生产商、安全芯片厂商、模组厂商、测试实验室等物联网安全全产业链合作伙伴，旨在建立安全的物联网连接，实现跨界融

合的安全方案，引领物联网安全行业发展，共建互赢的安全生态。目前，安全标准组积极对物联网安全芯片、物联网卡身份认证、智能门锁安全分级等多领域开展标准化工作，并已发布10项联盟标准。

通信企业前瞻布局平台生态。国外，思科于 2017 年 9 月，联合 Bosch、纽约梅隆银行、区块链服务开发商 ConsenSys 和 Skuchain、信息安全厂商 Gemalto 等企业，致力于以区块链技术为基础，构建安全、可扩展、可互操作、可信任的物联网网络和平台，旨在提升物联网的整体安全性。**国内，华为**于 2017 年 9 月提出了“平台+连接+生态”的物联网发展战略，旨在成为智能平台的搭建者、多种连接方式的创新者和物联网生态的推动者。现已在全球成立多个开放实验室，重点工作方向是为垂直行业提供端到端的物联网安全测试和验证服务，提升整个物联网全产业链的安全能力。**小米**自 2015 年起，全面布局消费级物联网生态，构建“小米生态链”，通过打造小米物联网开发者平台，推动产业合作。目前，平台联网终端数(不含手机和电脑)已达 1.51 亿、终端类型超过 800 种、合作伙伴超过 500 家，已成为全球最大的消费级物联网平台。

三、物联网终端安全风险分析

物联网是互联网的延伸和扩展，最突出的区别是增加了感知层。感知层的核心是数量多、种类多、低成本、低功耗、能感知、能通信的物联网终端。相比传统通信终端，物联网终端安全能力普遍较低，物联网卡难实名登记，已成为物联网整体安全的薄弱环节。如

物联网终端或物联网卡出现安全问题，将影响网络、应用和服务，威害公众生命财产安全，危及网络关键基础设施，危胁社会稳定和国家安全。因此，**物联网终端安全是物联网整体安全的关键环节、重中之重。**

（一）物联网终端安全风险点分析

1. 终端种类多规模大，难统一管理

一是难统一标准化管理。为满足纷繁复杂的物联网应用场景带来的碎片化需求，物联网终端种类繁多，功能、性能、安全需求千差万别、各不相同，较难提出统一适用的安全标准。

二是难统一实时管理。物联网终端规模庞大，所处地理位置一般相对分散、较为广泛，难统一对其进行实时管理，使得普遍长期处于无人看管、无人值守的环境中，即便发生被偷盗、被破坏、被损毁的情况，也较难第一时间发现并及时处置。

2. 终端安全能力较低，难抵御攻击

受限于物联网终端低成本、低功耗、计算资源有限等现实因素，较难将为手机等传统通信终端设计的安全机制直接配置到物联网终端上，如安全策略、加密算法等，导致物联网终端自身安全能力较低，易被利用安全漏洞开展入侵、攻击等行为，且较难抵御。

结合图 4 物联网终端架构，物联网终端安全风险点主要包括:

一是硬件安全风险点，易被破坏。终端长时间无人值守，攻击者可利用其暴露的调试接口或芯片设计缺陷直接捕获相关信息，并

进行攻击，甚至引发大面积攻击事件。另外，攻击者还可通过物联网终端处理数据的时间消耗、功率消耗、电磁辐射等信息推测终端密钥等关键数据，进行侧信道攻击，从而获得更多、更敏感的隐私数据。

二是固件安全风险点，易被攻击。在固件系统设计方面，物联网终端普通存在启动代码未进行合法性/完整性验证和系统等漏洞未及时修补、系统权限开放过多、权限限制不严格等问题，易被攻击者利用进行攻击。**在认证鉴权方面**，物联网终端普遍存在身份认证和授权机制弱、缺乏必要的安全防护能力等问题，易被攻击者利用获取用户的身份认证信息，进而伪造用户身份或通信节点，并向其他终端、接入网关进行入侵和攻击。

三是通信安全风险点，易被控制。物联网终端安全防护能力较弱，且规模庞大，易成为攻击者的突破口，被入侵、控制而形成大规模 DDoS 攻击。例如，若一台物联网终端被入侵、控制，攻击者可通过传播手段感染数以百亿计的物联网终端，最终形成规模化的僵尸网络，向骨干网络或服务系统发起大量服务请求，造成资源过载，导致服务中断甚至瘫痪。

四是应用安全风险点，易被利用。物联网终端的应用程序普遍存在逻辑缺陷或编码漏洞等问题，甚至有些终端设备厂家为节省开发成本直接调用第三方组件，导致应用软件引入了开源漏洞。攻击者可利用软件漏洞，通过植入木马、病毒等方式入侵或控制终端，并最终导致应用服务失效。

五是数据安全风险点，易被窃取、篡改。巨量化物联网终端感知、采集、存储海量涉及个人、家庭、垂直行业的隐私数据。而受限于硬件资源，物联网终端无法直接引入传统数据安全保护机制，导致敏感数据缺少保护机制，甚至是明文传送。一方面，**数据被窃取，泄露隐私。**攻击者利用安全漏洞入侵终端，获取用户隐私数据。例如，攻击者可入侵联网家用摄像头，获取用户生活状态和生活规律等隐私数据，另一方面，**数据被篡改，污染数据源。**攻击者利用安全漏洞入侵终端，篡改数据源并向决策服务端回传伪造的数据，将对应用服务带来巨大影响。如智慧医疗、智能交通等应用数据源遭到污染，将极大危害用户生命财产安全。

（二）物联网卡安全风险点分析

1. 难严格落实实名登记要求，易被滥用

一是物联网卡具备流转链条长、实名登记责任主体多、单次售卡数量大等特点，较难登记到实际使用人。例如，车联网终端中物联网卡的流转链条会依次经过电信企业（包括基础电信企业和移动通信转售企业）、后装市场、车厂、4S 店等多环节，最终才流转到实际使用人。而在此流转链条中，目前只有电信企业需承担实名登记主体责任，剩余流转主体均未承担实名登记主体责任，导致并未登记到实际使用人。且物联网卡单次发卡量大，一方面，提高了切实登记到实际使用人的难度；另一方面，如未严格登记到实际使用人，更给不法分子带来更多可趁之机、扩大影响范围。

二是受限于网络设备能力，较难实现物联网卡流量“功能最小化”。 根据工信部 182 号、452 号文件要求，电信企业在设计、销售物联网卡时，需要严格对其进行功能限制，即实现语音、短信、流量的定向访问。针对语音、短信的定向访问，电信企业可通过在智能语音网、短信网关上设置白名单等方式，有效实现功能限制；针对流量的定向访问，电信企业虽可通过设置专用 APN（接入点）、建设 VPDN（虚拟专用拨号网业务）专线等方式实现，但目前由于网络设备容量不足、增加用户成本等问题，仍缺乏有效的技术手段对物联网卡实现流量定向访问限制，导致部分电信企业未能严格按照实名登记管理要求对物联网卡的使用范围、开通功能进行限制。

2. 难全面监测使用行为状态，及时止损

受限于性能要求，难对计费信息进行全量、遍历访问，判断违规行为。全面实时判断物联网卡违规行为，需通过全量、遍历读取每张物联网卡的计费信息，获得其通信对象、通信时长、所处位置、使用业务等数据，并与功能约束进行比对判断是否发生疑似违规使用行为，如无限制通话、与非白名单用户通信、漫游至诈骗高发地区等。目前，物联网卡规模已近 9 亿，对巨量化计费信息进行全量、遍历访问，对电信企业的物联网卡监测平台性能要求极高。而无法全面、及时了解物联网卡使用情况，未能及时判断违规使用行为，也将导致未能及时提醒处置、及时止损。

四、物联网终端安全保障体系

针对物联网终端安全风险，推动构建“评估安全风险、增加安全能力、全面监测管控”的全过程工作机制，通过“应用新技术、采用新手段、建设新平台”的方式方法，逐个解决安全风险，构筑物联网终端安全保障体系，全面提升物联网终端安全能力。

总体安全解决技术思路如图 5 所示。

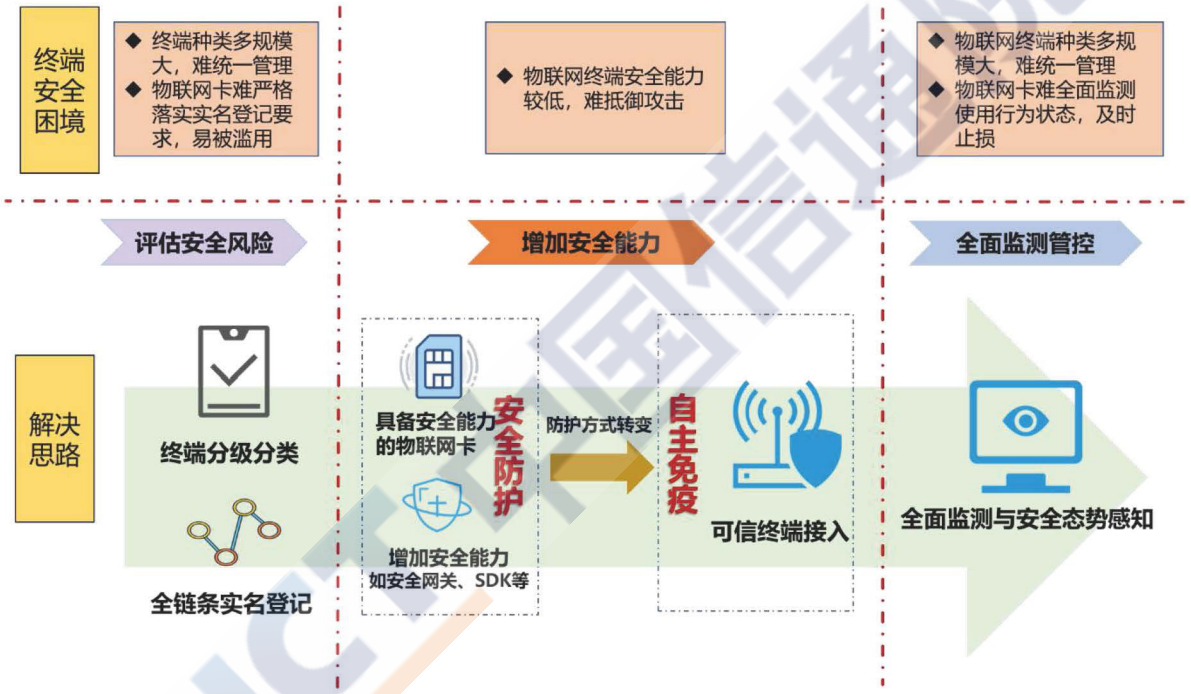


图 5　物联网终端安全解决思路

（一）评估安全风险

针对“物联网终端种类多规模大、难统一管理”和“物联网卡难严格落实实名登记要求，易被滥用”的安全风险，可全面开展安全风险评估。

针对物联网终端，构建分级分类管理机制，开展安全风险评测。

一是分级分类。基于已有安全能力、结合安全需求，有差别、有针

对性提出相应的安全能力要求，因地制宜提升安全能力。**第一步：**基于充分、广泛的调研，结合实际情况，制定评级标准，包括评级指标、评级手段和评估方法等，对物联网终端实行“**分级管理**”，包括高风险、中风险、低风险三类。**第二步：**对应风险等级各不相同的物联网终端，实行“**分类管理**”。针对高风险等级的终端，需提升安全能力，实时监控，并进行安全态势感知；针对中风险等级的终端，需提升安全能力，定期监控；针对低风险等级的终端，可偶尔监控。**二是安全风险评测。**为有效评判物联网终端所处的风险等级，可在终端上线部署前对其进行安全风险评测。即根据评级指标，从硬件模块、固件系统模块、应用模块、数据模块、通信接入模块等方面着手，利用仪表等设备对物联网终端进行安全评测，并对其风险等级进行评估，为决定是否需要增加安全能力或增加何种安全能力提供可靠依据。

针对物联网卡，构建全链条安全管理机制，评估未实名登记风险。基础电信企业可通过技术手段，实现物联网卡流转全链条安全管理，核心解决以下五方面问题：**一是**需多主体相互配合，采集物联网卡流转链条上各环节的流转数据，真实反映物联网卡流转全过程；**二是**信息不可篡改，防止流转过程中，某环节主体因利益因素而发生人为篡改信息的情况；**三是**需有管控中心，解决难以监控各节点交易，容易造成数据不一致或交易记录中断等问题；**四是**不同流转环节对不同数据需具备隐私保护能力，以满足不同企业登记、交易和查询等要求；**五是**从此链条中，可实时、清晰记录物联网卡

的流转情况，对未实名登记风险进行实时判断。**区块链技术天然适用于开展物联网卡全链条安全管理**，可同时实现物联网卡实名登记管理、使用行为监测、信用评估、信用查验四方面功能。管理机制示意图如图 6 所示。

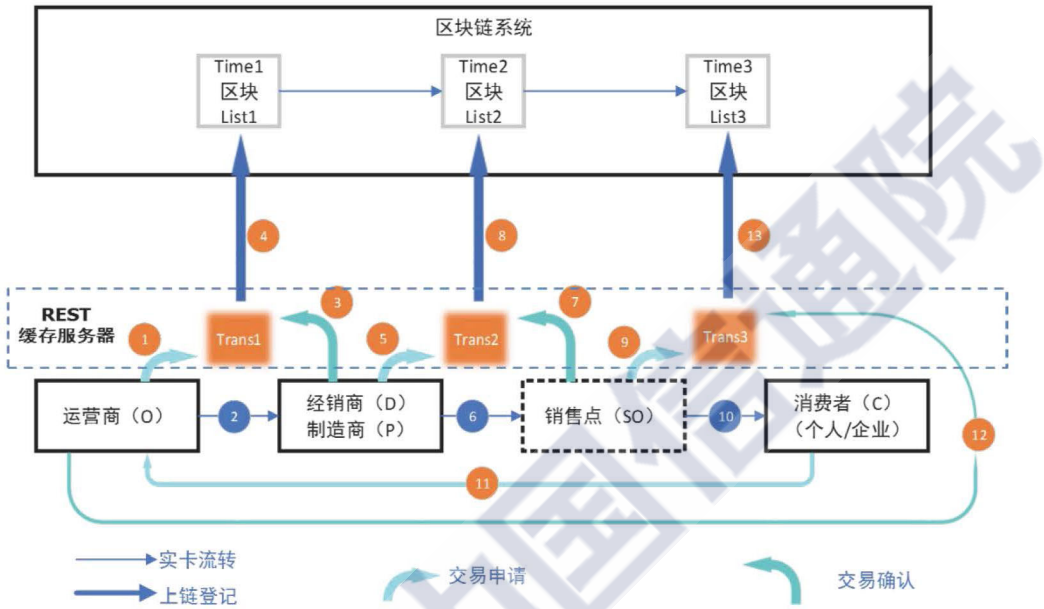


图 6　基于区块链的物联网卡全链条安全管理机制示意图

基于区块链的物联网卡全链条安全管理机制核心在于切实保证数据准确、完整上链，整个数据采集与登记过程包含“电信企业-中间流转企业-面向消费者的销售点-消费者”四个角色，并根据以下三点原则实现各个角色的数据切实上链。**一是**初始登记要求。只有电信企业具备初始登记的权限，负责创建一个区块链上的号卡身份和凭证，并登记相关信息和使用限制，以作为后续交易、流转所传递的载体。**二是**销售资格校验要求。中间流转企业在号卡售出时，必须首先验证该企业是否当前持有号卡。验证成功后方可发起售出申请。**三是**开卡激活要求。面向消费者的销售点在提出号卡售出申请时，必须由消费者向电信企业提供符合相应规定的实名登记材料，

电信企业审核通过、签名确认、激活开卡后，方可作为合法信息登记上链存证。

（二）增加安全能力

针对“物联网终端安全能力较低，难抵御攻击”和“物联网卡难严格落实实名登记要求，易被滥用”的安全风险，根据安全风险评估结果，可通过构建“内生增强、外部赋能、安全可信”的工作机制，有针对性提升物联网终端安全能力。

1. 物联网卡，内生增强安全能力

利用物联网卡内生增强安全能力，为物联网终端提供安全认证等安全服务。以物联网卡安全能力为核心，结合物联网终端、网络、平台能力，建立集安全认证、数据加密、安全存储于一体的物联网终端安全保障体系，技术思路如图 7 所示。

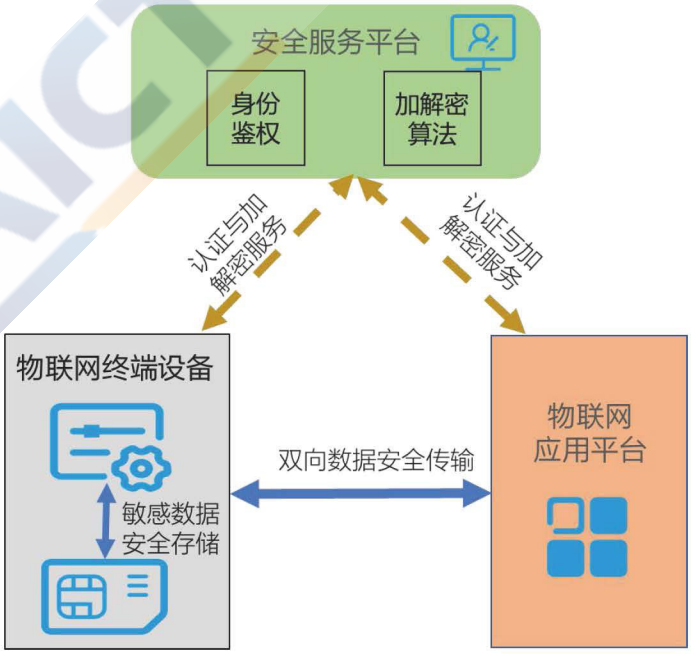


图 7　利用物联网卡内生安全能力，增强物联网终端安全能力技术思路

利用物联网卡内生增强安全能力，可实现以下三方面功能：

一是身份认证。作为物联网终端接入蜂窝网络必须的身份标识模块，物联网卡是物联网终端上的天然硬件。可利用物联网卡进行身份认证，实现对终端的身份认证，确保物联网终端的身份合法性。在物联网终端与物联网应用平台通信交互过程中，可通过物联网卡的身份认证能力对平台身份进行校验，确保物联网终端只接收来自合法平台的数据和指令。

二是数据加密传输。物联网终端与物联网平台间传递敏感数据时，可通过物联网卡和安全服务平台对敏感数据实现双向的数据加密传输，确保数据传输过程中不会被恶意窃取或篡改。

三是敏感数据存储保护。可利用物联网卡内部的安全存储空间，存储物联网终端内部的敏感数据，避免发生终端敏感数据泄露、篡改等情况。

目前，中国移动 SE-SIM 已具备上述能力。另外，部分厂家的芯片也已具备类似硬件安全环境能力，如高通、海思等。

2. 物联网终端，外在赋予安全能力

针对“物联网终端安全能力较低”和“物联网卡难实现流量定向访问”的安全风险，可通过外在赋予安全能力的方式进行解决。

为终端赋予安全能力，并配套建设安全管理平台，可同时实现物联网卡流量定向访问、物联网终端安全管控，同步做好物联网终端和物联网卡的安全管理。技术思路如图8所示。

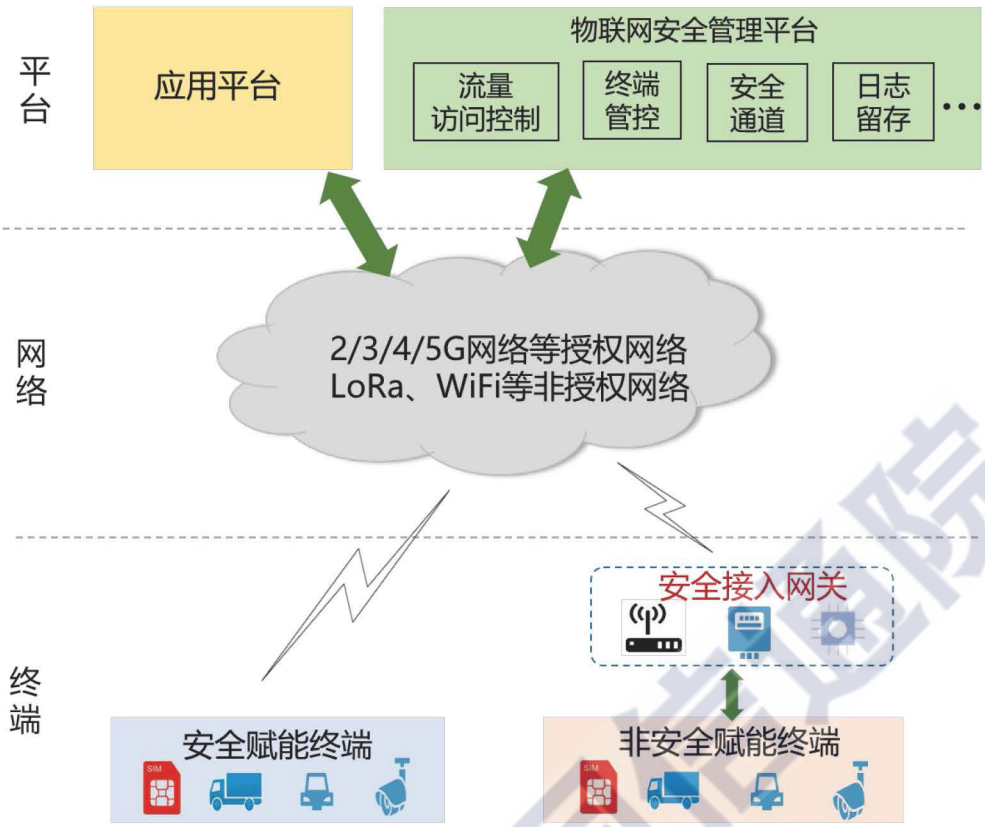


图 8　外在赋予安全能力技术思路

外在赋予安全能力是指：在终端或网关中增加集成安全能力的模组、SDK（软件开发包）等套件，使得终端或网关具备接收、执行安全策略，以及上报访问行为数据等能力。其中，安全策略包括设置黑白名单列表、限制访问能力等。

物联网安全管理平台通过以下技术思路实现对物联网卡流量的定向访问控制：承载物联网卡的终端直接、分别连入安全管理平台和应用平台，安全管理平台将安全策略直接下发至终端。终端访问应用平台时，自身安全能力将执行安全策略，判断目的IP地址、URI 等是否在黑白名单中。如在白名单中，则正常访问；如在黑名单中或不在白名单中，则拒绝访问。对于承载物联网卡未具备安全能力的物联网终端，以及未承载物联网卡和安全能力的物联网终端，均需通过连入

的、具备安全能力的物联网网关，间接实现流量定向访问。具体是，终端需通过网关，间接、分别连入安全管理平台和应用平台。安全管理平台需将每一个终端的安全策略下发给网关。终端向网关发起流量访问请求时，网关通过自身安全能力执行安全策略，判断目的 IP 地址、URI 等是否在黑白名单中。如在白名单中，则正常接续访问；如在黑名单中或不在白名单中，则拒绝接续访问。

物联网安全管理平台通过以下三方面功能实现对物联网终端的安全管理：一是事前预警，安全管理平台向具备安全能力的终端下发安全策略，限制访问功能，通过大数据分析与数据挖掘技术，获取安全事件的特征信息，进行发展类、安全类统计分析，及时预警终端所发生的异常情况。**二是事中监测，**安全能力在执行安全策略的同时，将执行结果和访问流量特征上报给管理平台，实时监测终端访问行为；定期对新入网行业用户实名登记情况进行监督检查，建立定期通报机制。**三是事后管控，**遇重大安全事件发生，或通过预警判断有违规访问行为发生、将发生重大突发安全事件时，安全管理平台可快速直接管控终端的异常行为。

目前，市场上已有多种类似产品，包括中国移动安连宝、360安全管控SDK、安恒信息物联网安全心等。

3. 安全可信环境，实现终极安全目标

传统增加安全防护手段的安全管理机制较为被动。因终端缺乏应对未知安全威胁的能力，导致较难从根源上避免安全风险、杜绝安全

隐患。**而通过构建端到端安全可信体系架构的方式，可使得网络具备自身免疫的安全防御能力，变被动防护为主动免疫，实现终极安全目标。**

物联网安全可信体系是指在物联网终端、网关、安全管理平台中引入可信技术，构建完整的可信体系架构，打造安全可信的网络和应用环境，使得物联网网络能够及时识别“自己”和“非己”成分，并主动对“非己”成分采取必要的隔离和预防。

物联网安全可信体系架构由接入可信、连接可信和平台可信三部分组成。其中，**接入可信**是利用物联网可信网关与海量、异构物联网终端设备连接，作为物联网的可信边界；**连接可信**是指在网关与平台间传递数据时，采用可信连接等方式对网关和平台进行身份认证，确保数据能够发送到正确的终端或平台，防止数据在传输过程中被截取、窃听和篡改；**平台可信**为可信网关和终端提供安全可信的管理平台，具有安全管理、策略制定、策略下发等功能。

通过构筑安全可信环境，可使得从物联网终端开始，通过可信链传递将终端的可信度逐渐扩展、延伸到网络、应用中，并能对终端进行行为监测、异常行为评估、恶意攻击溯源和阻断，建立主动防御和自我进化的高可信物联网可信环境，实现物联网安全的全链条可信。

近年来，可信计算已成为国内外研究和应用的热点。**国外**已较早启动可信计算领域研究。2003 年，以美国为首正式成立了全球可信计算组织（TCG），并在 2014 年发布了 TPM2.0（可信平台模块）标准。目前，已有多个芯片厂商商业化生产和应用符合该标准的安全芯片，

包括英飞凌、意法半导体(ST)、Atmel、华邦电子等。**国内**，中国工程院沈昌祥院士指出，安全是发展的前提，发展是安全的保障。没有网络安全，整个信息社会、智能社会将成为黑暗中的废墟，为此应提倡主动免疫的可信计算，在计算运算的同时进行安全防护，为网络信息系统培育免疫能力。

（三）全面监测预警

针对“物联网终端种类多规模大，难统一管理”和“物联网卡难全面监测使用行为状态，及时止损”安全风险，可推动构建统一监测平台，实现对物联网终端和物联网卡的全面监测预警。

全面监测，实现安全态势感知。一是全面获取物联网终端、物联网卡的在线使用行为信息，包括物联网终端在线状态、业务访问情况等，以及物联网卡基础数据、通信业务使用情况等，实现全面监测。**二是**充分利用大数据深度挖掘技术，实现安全态势感知，对物联网卡、物联网终端异常使用行为进行预警，如机卡分离、需稳定在某一固定位置的终端高频移动、终端被入侵、数据被篡改等。

基于态势感知，及时进行预警，降低影响范围和程度。结合物联网卡、物联网终端安全态势感知情况，在发生安全事故预警时，及时对相关企业、设备厂家、应用服务提供商进行提示，为物联网终端管控提供参考依据，降低安全威胁对网络或应用等关键基础设备造成的影响。

五、物联网终端安全未来展望

（一）明确要求，推动健康发展

一是从国家层面，提出物联网终端安全管理要求，推动发展。一方面，国家要求可有效促进全社会、各行业、多产业切实提升物联网终端安全意识，推动从主观上充分认识到做好物联网终端安全管理的重要性和必要性，增强主观能动性，切实发力做好物联网终端安全相关工作。另一方面，物联网发展涉及多行业，物联网终端安全管理涉及多行业主管部门，需从国家层面进一步明确各部门的职责分工，促进分工有序、各司其职、相互合作，共同做好物联网终端安全管理。

二是从行业层面，出台物联网终端安全管理政策要求，指引发展。各行业可从行业自身需要出发，结合本行业内物联网终端安全管理的痛点和难点，制定出台专门的安全管理政策要求，促进行业内相关终端安全工作规范发展。

三是从产业层面，建立健全物联网终端安全标准体系，规范发展。以从源头提升物联网终端安全能力为导向，围绕芯片、模组、硬件、数据等终端关键模块，研究物联网终端安全核心技术，制定相关标准，推动落地实施，规范产业链有序发展。

（二）以卡促端，创新管理模式

一是5G网络部署商用，促进物联网卡和物联网终端进一步耦合。5G 网络在速率、覆盖范围、可靠程度等方面的优势，将有效推动物

联网应用服务提供商采用 5G 网络作为传输中介。5G 网络正式商用部署，将推动蜂窝物联网终端规模持续增速发展，促进物联网卡和物联网终端进一步紧密耦合。

二是物联网卡安全管理势在必行，迫切需要物联网终端增加安全能力。面对未实名登记的物联网卡易被滥用的严峻形势，做好物联网卡安全管理迫在眉睫、势在必行。而做好物联网卡安全管理，落实“功能最小化”要求首当其冲。因此，迫切需要提升物联网终端安全能力，满足功能管控需求。

三是以物联网卡安全管理为契机，同步做好卡和终端的安全管理。以满足物联网卡安全管理需求为导向，增加物联网终端安全能力，可同步做好物联网卡和终端的安全管理，甚至还可将监管范围扩展至网络和应用，全面做好物联网安全管理。

（三）鼓励创新，促进产业革新

物联网终端安全问题属物联网安全特色问题，传统信息通信安全技术手段无法全面满足物联网终端安全需要。对此，鼓励应用新技术，创新思维思路和方式方法，探索物联网终端安全新的解决方案，助力提升物联网终端安全核心竞争力。

一是应用新技术探索新思路。区块链、边缘计算、可信接入等新技术新理念快速发展，鼓励从物联网应用发展趋势着眼，以满足物联网终端安全需要、解决安全问题为导向，研究提出新的解决方案，创新安全防护思维思路和方式方法，着力推动物联网终端安全

产业发展。

二是推动新思路落地实施，谋求革新发展。针对新思路，鼓励基于物联网应用产业园区，以创新示范应用为抓手，推动落地实施新方案。在落地实施过程中，评估效果，判断是否推广应用，为革新发展奠定应用基础。

（四）产业聚力，构筑共识生态

物联网终端安全的健康可持续发展，离不开产业链的鼎力支持、合力推动和全力配合。迫切需要物联网终端产业链达成共识、形成合力，共筑物联网终端安全新生态、共谋新发展，形成多赢局面。

聚力共建产业联盟。产业链相关单位可以成立物联网终端安全产业联盟的方式，包括物联网应用服务提供商、基础电信企业、物联网终端厂商、模组厂商、芯片厂商、安全厂家等，推动在安全需求、解决方案、标准规范、测试认证、应用示范等方面达成共识，形成产业合力，共建产业生态化、规模化发展模式，切实提升物联网终端安全能力。

MEMBERS OF THE UNIT

物联网安全创新联合实验室（成员单位）

CAICT 中国信通院

中国移动 China Mobile

中国信息通信研究院

中国移动通信有限公司研究院

中国移动通信集团江苏有限公司

中移物联网有限公司