物联网安全白皮书

（2018 年）

中国信息通信研究院

中国移动信息安全管理与运行中心

2018年9月

版权声明

前　言

自 2005 年国际电信联盟（ITU）正式提出“物联网”这一概念以来，物联网在全球范围内迅速获得认可，并成为信息产业革命第三次浪潮和第四次工业革命的核心支撑。物联网技术的发展创新，深刻改变着传统产业形态和社会生活方式，催生了大量新产品、新服务、新模式，引发了产业、经济和社会发展新浪潮。

与此同时，数以亿计的设备接入物联网，物联网产业规模不断壮大，针对用户隐私、基础网络环境的安全攻击不断增多，网络安全问题已成为限制物联网服务广泛部署的障碍之一。

为促进物联网及其生态系统的健康发展，控制物联网面临的安全风险，我院与中国移动通信集团有限公司信息安全管理与运行中心牵头，联合中移物联网有限公司联合、360 企业安全集团、北京神州绿盟科技有限公司共同研究编制物联网安全白皮书（2018）。

本白皮书从物联网安全发展态势出发，从物联网服务端系统、终端系统以及通信网络三个方面，分析物联网面临的安全风险，构建物联网安全防护策略框架，并提出物联网安全技术未来发展方向及建议。

目 录

一、物联网安全发展态势

（一）全球物联网市场规模快速增长，安全支出持续增加

一方面，全球联网设备数量高速增长，“万物互联”成为全球网络未来发展的重要方向。据 GSMA 预测，2025 年全球物联网设备（包括蜂窝及非蜂窝）联网数量将达到 252 亿如图 1.1，远高于 2017 年的 63 亿；同时，物联网市场规模将达到目前的四倍。此外，工业物联网设备联网数量在 2016 年至 2025 年间，将从 24 亿增加到 138 亿，增幅达五倍左右[1]，工业互联网设备联网数量也将在 2023 年超过消费物联网设备联网数量如图 1.2。

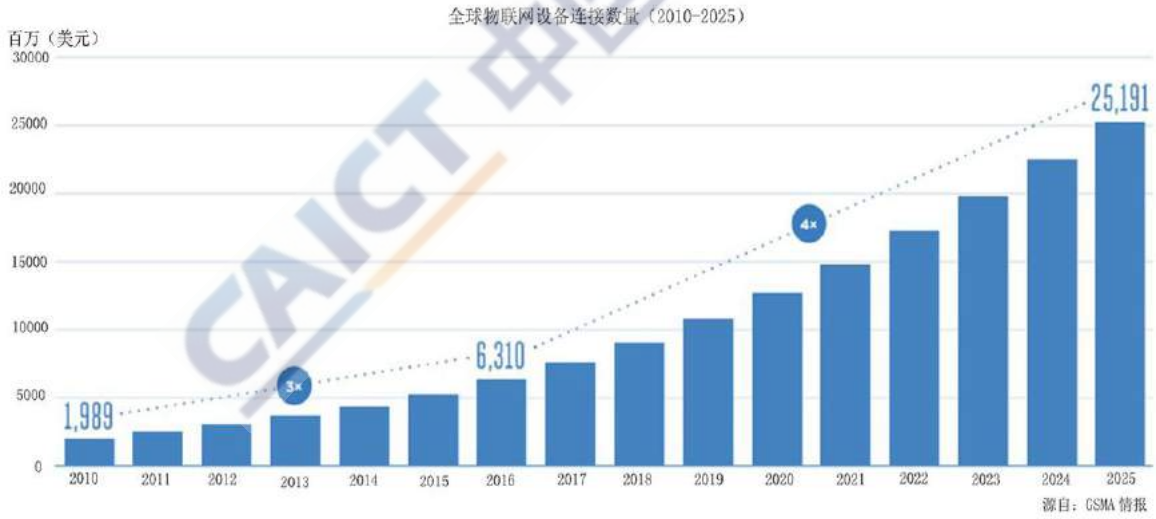

图 1.1 全球物联网设备联网数量

[1] IoT: the next wave of connectivity and services（https://www.gsmaintelligence.com/research/2018/04/iot-the-next-wave-of-connectivity-and-services/665/）

图 1.2 全球消费物联网设备及工业物联网设备联网数量

LoRa、NB-IoT 和 5G 等通信技术的发展让万物互联成为现实。尤其面向低耗流物联网终端的 NB-IoT，作为万物互联网络的一个重要分支，适合广泛部署在智慧城市、智慧交通、智能生产和智能家居等众多领域。

另一方面，物联网安全事件频发，全球物联网安全支出将不断增加。当前，基于物联网（IoT）的攻击已经成为现实。据 Gartner 调查，近 20％的企业或相关机构在过去三年内遭受了至少一次基于物联网的攻击。为了防范安全威胁，Gartner 预测 2018 年全球物联网安全支出将达到 15 亿美元，比 2017 年增长 28％，预计到 2021 年物联网安全支出将达到 31 亿美元[2]如表 1.1。

[2] Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018（https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018）

表 1.1 全球物联网安全支出预测（单位：百万美元）（来源：Gartner）

	2016	2017	2018	2019	2020	2021
终端安全	240	302	373	459	541	631
网关安全	102	138	186	251	327	415
专业服务	570	734	946	1221	1589	2071
总计	912	1174	1506	1931	2457	3118

（二）物联网系统直接暴露于互联网，容易遭到网络攻击

当前，大量物联网设备及云服务端直接暴露于互联网，这些设备和云服务端存在的漏洞（如：心脏滴血、破壳等漏洞）一旦被利用，可导致设备被控、用户隐私泄露、云服务端数据被窃取等安全风险，甚至会对基础通信网络造成严重影响。

从全球分布来看，路由器、视频监控设备暴露数量占比较高。路由器暴露数量超过3000万台，视频监控设备暴露数量超过1700万台如图1.3。

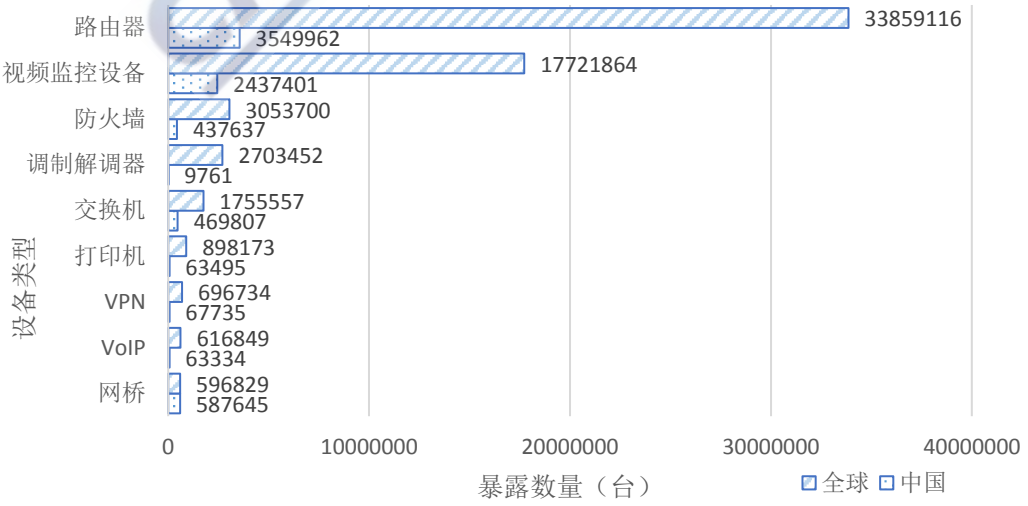

图 1.3 全球和国内物联网相关设备暴露情况

其中，**我国国产设备的暴露占比突出。在路由器方面，**华为暴露设备数量最多，逾 900 万台，AVM、Technicolor、MikroTik、华硕、TP-Link 等 11 家厂商的全球暴露数量超过了百万规模如图 1.4。**在视频监控设备方面，**海康威视和浙江大华的视频监控设备暴露严重，其中，海康威视暴露设备总量超过了 580 万台，浙江大华、D-Link 等厂商的视频监控设备暴露数量也都达到了百万量级如图 1.5。

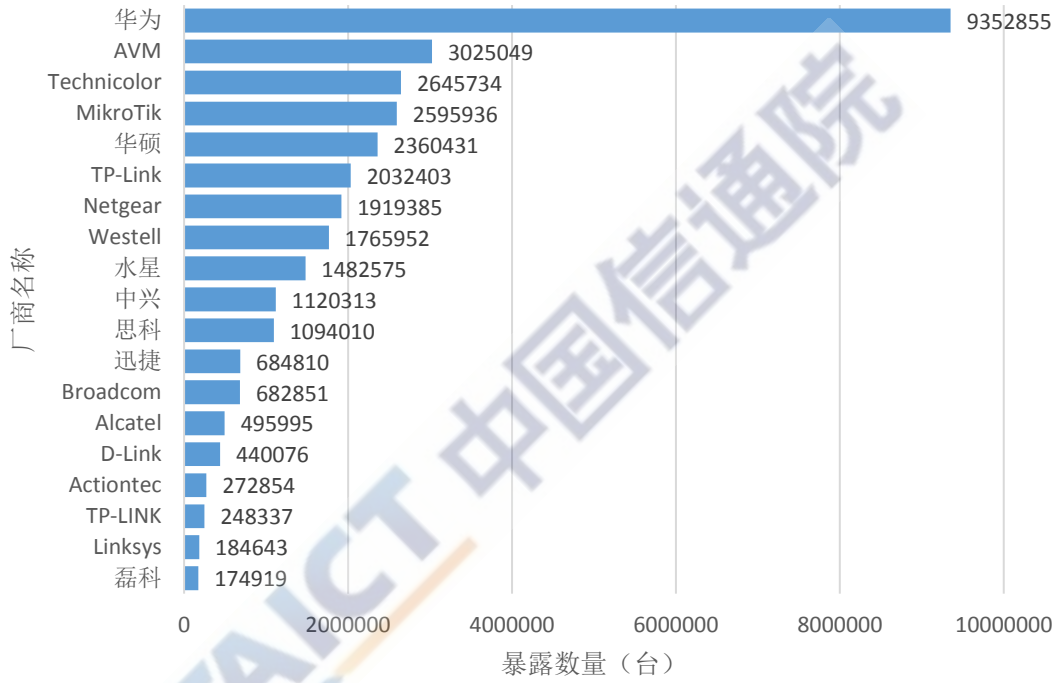

图 1.4 暴露的路由器设备厂商分布（全球）

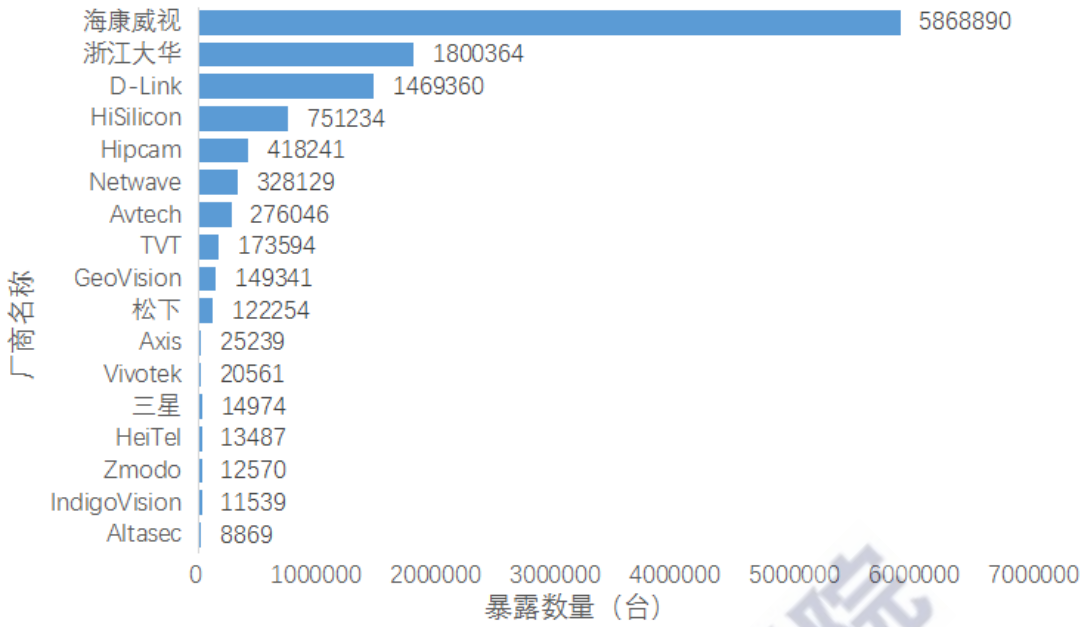

图 1.5 暴露的视频监控设备厂商分布（全球）

同时，**我国暴露于互联网的路由器及视频监控设备数量排名全球前列，路由器数量**超过 350 万台，仅次于美国如图 1.6。视频监控设备数量超过 240 万台，位居第一；其次分别为越南、美国、巴西、印度等如图 1.7。

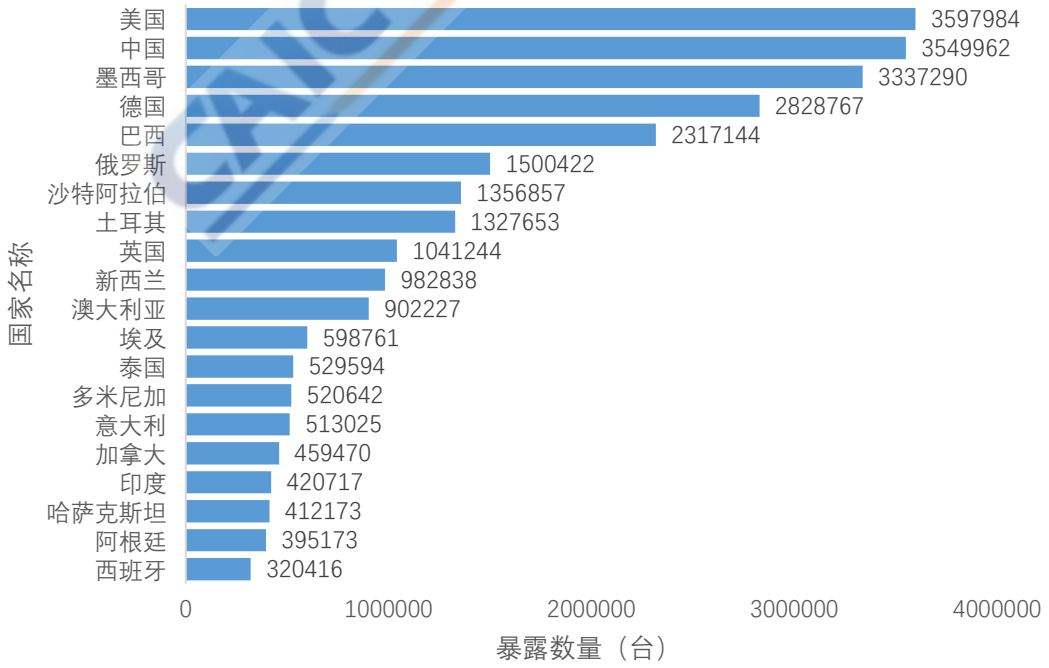

图 1.6 暴露的路由器国家分布

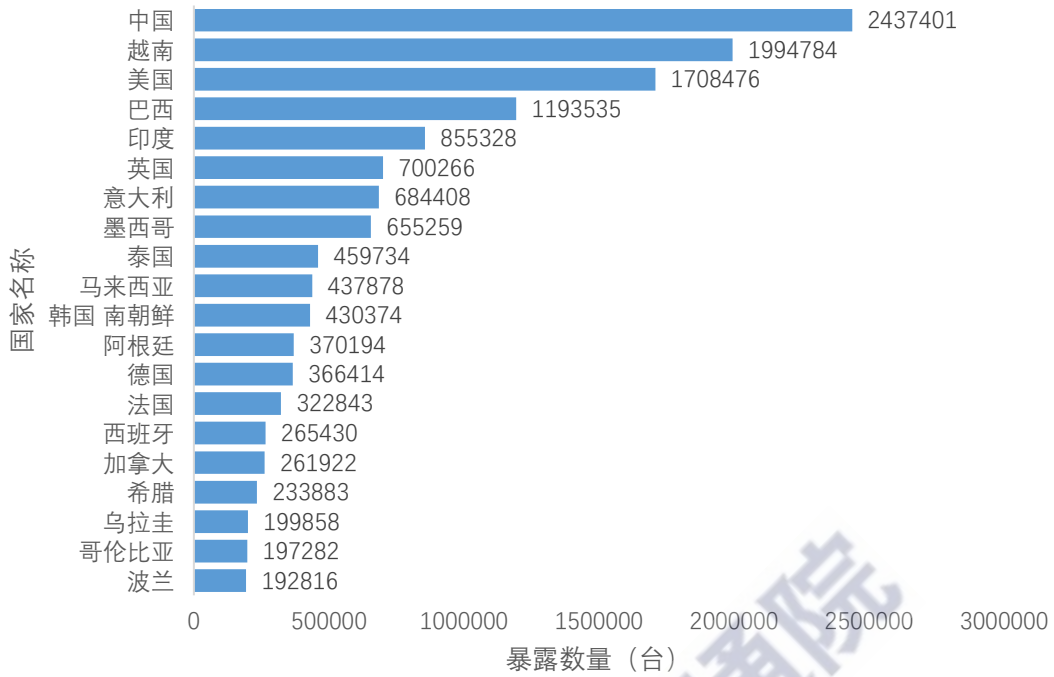

图 1.7 暴露的视频监控设备国家分布

此外，**全球范围内采用 CoAP、XMPP 协议的云服务端暴露数量较高。**暴露数量最多的 CoAP 服务数量接近 45 万个如图 1.8。

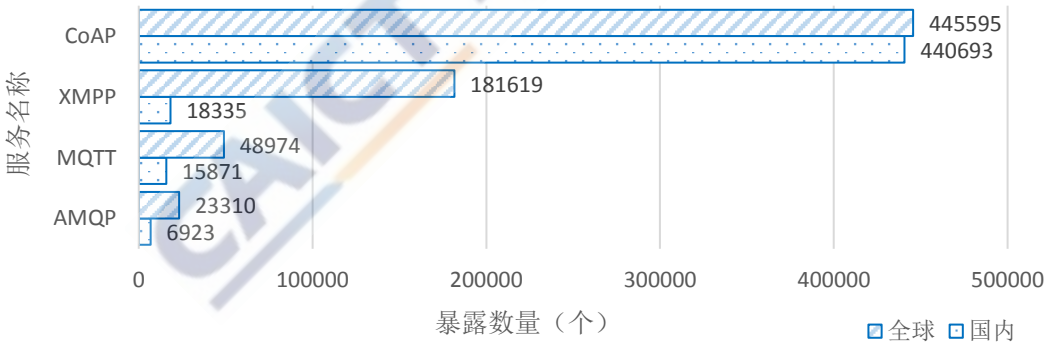

图 1.8 全球和国内物联网服务暴露情况

（三）物联网安全风险威胁用户隐私保护，冲击关键信息基础设施安全

一方面，智能家居设备部署在私密的家庭环境中，如果设备存在的漏洞被远程控制，将导致用户隐私完全暴露在攻击者面前。例如，智能家居设备中摄像头的不当配置(缺省密码)与设备固件层面

的安全漏洞可能导致摄像头被入侵，进而引发摄像头采集的视频隐私遭到泄露。2017 年 8 月，浙江某地警方破获一个在网上制作和传播家庭摄像头破解入侵软件的犯罪团伙。查获被破解入侵家庭摄像头 IP 近万个，获取大量个人生活影像、照片，甚至个人私密信息。2017 年 2 月 28 日安全专家 Troy Hunt 曝光互联网填充智能玩具 CloudPets（泰迪熊）的用户数据存储在一个没有任何密码或防火墙防护的公共数据库中，暴露了 200 多万条儿童与父母的录音，以及超过 80 万个帐户的电子邮件地址和密码。

另一方面，利用设备漏洞控制物联网设备发起流量攻击，可严重影响基础通信网络的正常运行。物联网设备基数大、分布广，且具备一定网络带宽资源，一旦出现漏洞将导致大量设备被控形成僵尸网络，对网络基础设施发起分布式拒绝服务攻击，造成网络堵塞甚至断网瘫痪。2016 年 10 月 21 日，美国域名服务商 Dyn 遭受到来自数十万网络摄像头、数字录像机设备组成的僵尸网络高达 620G 流量的 DDoS 攻击，导致美国东海岸大面积断网，Twitter、亚马逊、华尔街日报等数百个重要网站无法访问。同年，德国电信遭遇网络攻击，超 90 万台路由器无法联网，断网事故共持续数个小时，导致德国电信无法为用户提供正常网络服务。

二、物联网安全风险分析

（一）物联网应用系统模型

物联网应用涉及国民经济和人类社会生活的方方面面，典型应用如：车联网、智能家居、智能监控、智能物流、智能穿戴、智慧

医疗和智慧能源等。通过对各应用系统业务流程及实现原理进行分析，总结物联网应用系统模型如图 2.1:

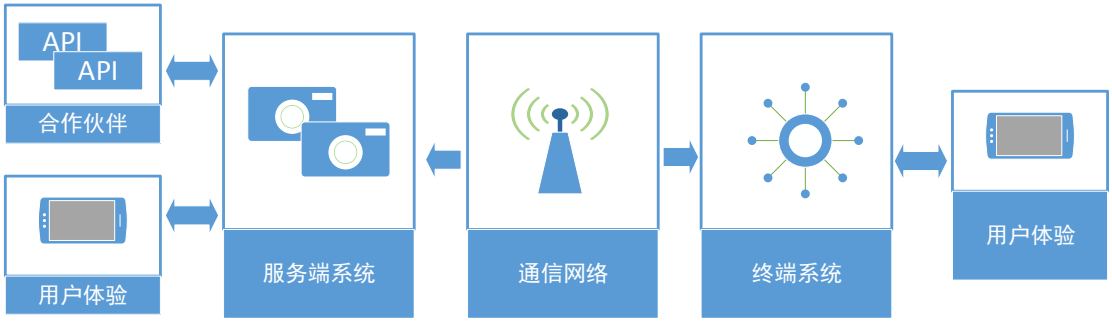

图 2.1 物联网应用系统模型

上述模型主要包括三部分：服务端系统、终端系统和通信网络。各部分功能主要如下:

1. 服务端系统：主要功能是从物联网终端系统收集数据信息存储至服务器中，并通过业务功能模块处理后，将处理结果通过不同业务接口反馈给用户界面显示，用户可以通过 API 接口或者 UI 界面获得数据结果。

2. 终端系统：主要包括低复杂性设备、复杂设备和网关，它们通过有线及无线网络将物理世界和互联网彼此相连。常见的终端系统设备包括：运动传感器、数字门锁、车联网系统、工业控制传感器等。终端系统从周围真实物理环境中收集数据，并将数据格式化后通过蜂窝或非蜂窝网络传输至服务端系统，并在接收到服务端反馈时将信息显示给用户。

3. 通信网络：主要包括有线和无线通信网，负责连接服务端、终端，并为其间数据传递提供通道（电信网、互联网、卫星通信

等），同时也承担终端设备与用户终端之间的信息交互（蓝牙、WIFI、近场通信等）。

基于模型分析可知，物联网安全风险主要也集中在服务端、终端、通信网络三个方面。

（二）物联网服务端安全风险

物联网服务端是整个物联网业务系统的功能核心。终端传感器数据收集处理、处理结果向用户界面接口反馈等基本功能都由服务端实现；此外，用户分级认证、系统维护管理、可用性监控等系统运行所必须的关键任务都由服务端完成。不同行业物联网业务系统虽然业务功能、拓扑结构大相径庭，但其设计原理、架构方式彼此类似，如图 2.2 所示：

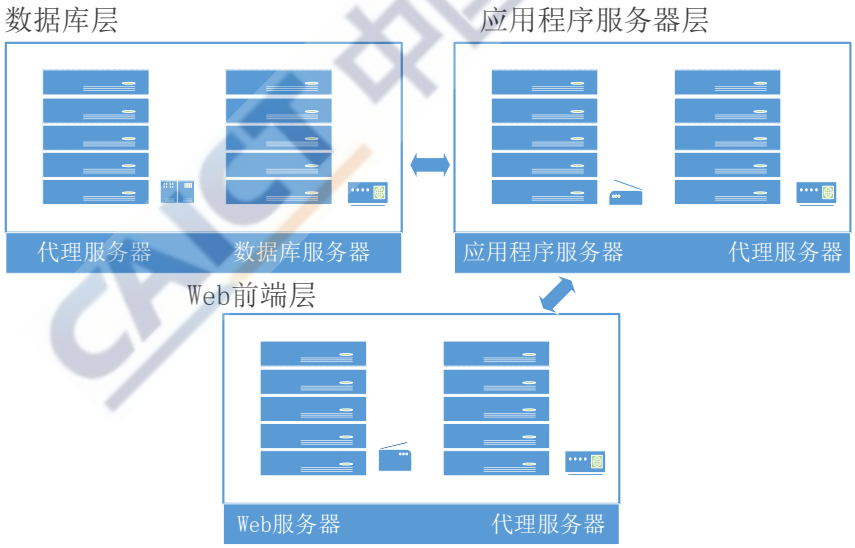

图 2.2 物联网服务端模型

终端传感器采集的数据及用户请求通过通信网络发送到 web 前端层并由其处理后转发至应用程序服务器层进行业务处理，处理过程中涉及数据存储部分功能会与数据库层进行数据交互。从模型分析物联网服务端安全风险如下：

1.服务端存储大量用户数据，成为攻击焦点。物联网业务系统的各种应用数据都存储在数据库层，由于用户数据高度集中，容易成为黑客攻击的目标，一旦遭受到攻击或入侵将导致数据泄露、系统业务功能被控制等安全问题。

2.虚拟化、容器技术提高性能同时带来安全风险。目前大多数物联网业务系统都搭建在虚拟化云平台之上以实现高效的计算及业务吞吐，但虚拟化和弹性计算技术的使用，使得用户、数据的边界模糊，带来一系列更突出的安全风险，如虚拟机逃逸、虚拟机镜像文件泄露、虚拟网络攻击、虚拟化软件漏洞等安全问题。

3.系统基础环境及组件存在漏洞，易受黑客攻击。物联网业务系统自身的漏洞，如云平台漏洞、大数据系统漏洞等都会导致系统受到非法攻击。通常物联网业务系统中会设计很多组件，如操作系统、数据库、中间件、web 应用等，这些程序自身的漏洞或设计缺陷容易导致非授权访问、数据泄露、远程控制等后果。

4.物联网业务 API 接口开放、应用逻辑多样，容易引入新风险。业务逻辑漏洞通常是由于设计者或开发者在设计实现业务流程时没有完全考虑到可能的异常情况，导致攻击者可以绕过或篡改业务流程。比如绕过认证环节远程对物联网设备进行控制；通过篡改用户标识实现越权访问物联网业务系统中其他用户的数据等。物联网业务系统 API 接口开放则可能会造成接口未授权调用，导致批量获取系统中敏感数据、消耗系统资源等风险。

（三）物联网终端安全风险

物联网终端系统由传感器及网关组成，主要功能是实现对信息的采集、识别和控制。从技术特点上可分为以下几种类型设备，部署示例如图 2.3:

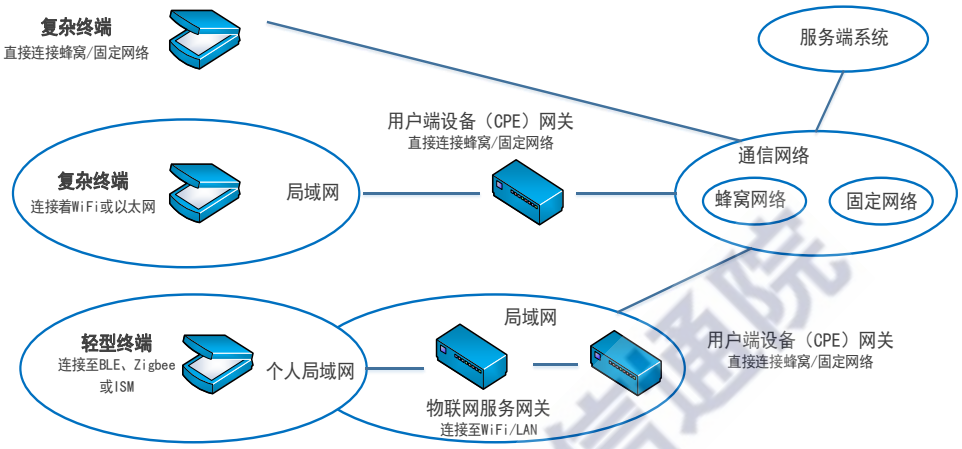

图 2.3 物联网终端示例

1. 轻型终端。轻型终端用于单一的物理用途，如照明开关、门锁等，通常采用成本较低的元器件并使用低功耗近距离通信（如 RFID、BLE 或 Zigbee 等），轻型终端通常通过网关或者用户终端设备与物联网服务端进行数据交互。常见的轻型终端有可穿戴设备、家庭安防传感器、NFC 标签等。

2. 复杂终端。复杂终端可以实现更多功能，通常内置基本处理器，可运行本地应用程序或处理音视频数据等。可通过蜂窝等长距离通信链路或通过 WIFI、以太网经由用户终端设备与物联网服务端进行数据交互。常见的复杂终端有智能家电（如冰箱、洗衣机等）、工业控制系统（如 SCADA）、智能汽车跟踪监测设备（如联网的 OBD2 设备）。

3. 物联网网关。网关具备更强大的处理能力，用于管理长距离通信链路，例如蜂窝、固定通信网、以太网等，它接受服务端系统发出的命令并将其转换为轻型、复杂终端可以解析的信息传递给终端，并将终端收集的信息处理后发送至服务端系统。因此网关在物联网业务系统中起到网络汇聚接入的作用，让终端之间及终端与服务端之间可以互相通信。常见的物联网网关例如物联网服务网关、用户端设备网关。

综上，物联网终端侧可能面临的安全风险如下：

1. 终端物理安全。由于感知终端或节点处于不安全物理环境，有可能被偷盗，非法位置移动、人为破坏以及自然环境引发的威胁，可能造成感知终端或节点的丢失、位置移动或无法工作。

2. 终端自身安全。感知设备通常无法拥有完备的安全防护能力，缺乏相应的安全防护体系，这使得感知设备易遭到攻击和破坏，其次许多物联网设备由于未及时更新，或者缺乏相应的更新机制导致物联网终端设备存在的软件漏洞风险极高。

3. 网络通信及结构安全。目前许多适用于通用计算设备的安全防护功能由于计算资源或系统类别的限制很难在物联网上实现，因此物联网通信机制存在较大的安全隐患。例如：许多物联网设备都是部分或全部明文传输，缺乏加密的通信机制。许多物联网都未对代码或配置项变更进行权限限制，缺乏成熟的授权或认证机制，容易发生恶意敏感操作或数据未授权访问。一些家庭内网络很少进行

网络分段隔离或防火墙设置，使得物联网设备极易遭受同网段病毒感染、恶意访问或操控。

4. 数据泄露风险。物联网系统泄露用户隐私数据的风险较高。主要存在云端、物联网终端设备本身两个来源的泄露风险。一方面，云端服务平台可能遭受外部攻击或内部泄密，或者由于云服务用户弱密码认证等原因，均有可能导致用户敏感数据泄露;另一方面，设备与设备之间也存在数据泄露渠道，在同一网段或相邻网段的设备可能会查看到其他设备的信息，比如屋主名字，精确的地理位置信息，甚至消费者购买的东西等。

5. 恶意软件感染。一旦感知终端、节点被物理俘获或逻辑攻破，攻击者可利用简单的工具分析出终端或节点所存储的机密信息；同时，攻击者可以利用感知终端或节点的漏洞进行木马、病毒的攻击，使得终端节点被非法控制或处于不可用状态，获取未授权的访问，或者实施攻击。例如引发大规模 DDoS 攻击的 Mirai、BASHLITE、Lizkebab、Torlus、Gafgyt 等。除了被用于拒绝服务攻击，被这些病毒感染的物联网设备还可用于窥探他人隐私，勒索所劫持设备，或者被利用作为攻击物联网设备所连接的网络渗透入口等。

6. 服务中断。可用性或连接的丢失可能会影响物联网设备的功能特性，一些情况下还可能降低安全性，例如楼宇警报系统一旦连接中断的话，将会直接影响楼宇的整体安全性。

（四）物联网通信网络安全风险

物联网的通信网络系统主要用于将感知层获取的信息在网络中进行传递和处理。由于物联网涉及的网络多种多样，从感知层的无线、红外线等射频网络，通过无线接入网，例如窄带物联网络、无线局域网、蜂窝移动通信网、无线自组网等，经过互联网，到达物联网应用层平台，因此物联网面临的网络安全威胁更为复杂，具体有四方面安全隐患。

1. 无线数据传输链路具有脆弱性。物联网的数据传输一般借助无线射频信号进行通信，无线网络固有的脆弱性使系统很容易受到各种形式的攻击。攻击者可以通过发射干扰信号使读写器无法接受正常电子标签内的数据，或者使基站无法正常工作，造成通信中断。另外无线传输网络容易导致信号传输过程中难以得到有效防护，容易被攻击者劫持、窃听甚至篡改。

2. 传输网络易受到拒绝服务攻击。由于物联网中节点数量庞大，且以集群方式存在，攻击者可以利用控制的节点向网络发送恶意数据包，发动拒绝服务攻击，造成网络拥塞、瘫痪、服务中断。

3. 非授权接入和访问网络。用户非授权接入网络，非法使用网络资源，或对网络发起攻击；用户非授权访问网络，获取网络内部数据，如用户信息、配置信息、路由信息等。

4. 通信网络运营商应急管控风险。对于通信网络运营商来说传统的短信、数据、语音等通信功能管控主要依据单一设备、单一功能、单一用户进行。但物联网设备终端规模大，且不同业务的短信、

数据等通信功能组合较多，若不能在网络侧通过地域、业务、用户等多维度实施通信功能批量应急管控，则无法应对海量终端被控引发的风险。

（五）各典型应用场景风险分析

随着物联网技术产品不断成熟，其潜力和成长性逐步凸显。物联网应用已经渗透到生产和生活的各个环节。本文选取了全球物联网发展较快、应用较成熟的典型场景进行安全风险分析，具体如下:

1.消费物联网：消费物联网是以消费为主线，利用物联网智能设备极大的改善或影响人们的消费习惯为目的生产、打造的智能设备网络。智能家居（包括智能家庭、家电等）是消费物联网最主要的消费级产品，同时智能穿戴设备如手环、眼镜、便携医疗设备也是消费物联网的主要应用。**消费物联网的应用场景贴近数量众多的终端销售者，容易催生黑色产业链。**

近期，针对消费物联网的安全威胁事件日益增多，如英国某医疗公司推出的便携式胰岛素泵被黑客远程控制，黑客可以通过控制注射计量威胁使用者的生命安全。2017 年，日本国内出现多起针对智能电视的勒索病毒事件。我国国内也爆发了多起黑客利用漏洞入侵并控制家用摄像头，并非法获取用户敏感视频对用户进行敲诈的安全事件。

目前，针对消费物联网的主要威胁有:

（1）利用漏洞或者自动安装软件等隐秘行为窃取用户文件、视频等隐私;

（2）传播僵尸程序把智能设备变成被劫持利用的工具;

（3）通过控制设备反向攻击企业内部或其后端的云平台,进行数据窃取或破坏。

2. 车联网：车联网是以车内网、车际网和车载移动互联网为基础，按照约定的通信协议和数据交互标准，在车与车、车与路、车与行人及互联网等之间，进行无线通讯和信息交换的大系统，是能够实现智能化交通管理、智能动态信息服务和车辆智能化控制的一体化网络，是物联网技术在交通系统领域的典型应用。车联网对促进汽车、交通、信息通信产业的融合和升级，对相关产业生态和价值链体系的重塑具有重要意义。

智能车联网通过车载智能设备同时实现与云端服务通讯和与本地总线通讯，实现通过手机应用对车辆进行远程控制的智能化需求。因此，接入车联网的车辆内部信息架构至少包括了行车信息总线和物联网/互联网两部分通讯网络，这使得网关类组件安全也成为了影响车联网安全的重要因素。伴随车联网智能化和网联化进程的不断推进，车联网安全已成为关系到车联网能否快速发展的重要因素。

目前，针对车联网安全的主要威胁包括:

（1）传感器数据合法性难以判断，基础数据篡改引发误响应;

（2）核心控制组件存在漏洞，控制权外泄存安全隐患;

（3）接口身份认证缺失，存在非法设备接入的安全隐患;

（4）OTA 通道存在供应链威胁植入风险;

（5）智能应用存在被利用可能。

3. 工业互联网：工业互联网在工业生产中的应用使工业生产活动开始呈现“数字化、智能化、网络化”的发展趋势，各个生产环节的互联互通成为新常态。这使得工业生产部分环节网络与外部网络互通，在提高效率的同时，可能引发并导致严重的安全事件。

据不完全统计，我国工业互联网联盟 82 家工业企业的 ICS、SCADA 等工控系统中，28.05%都出现过漏洞，其中，23.2%是高危漏洞。总体来看，我国工业互联网安全态势比较严峻，工业控制系统和平台的安全隐患日趋突出，工业网络安全产品和服务适应性不高，工业互联网安全保障意识及能力亟待强化。

目前，针对工业互联网的安全威胁主要有:

（1）网络和系统资产庞杂，资产和网络边界识别困难，资产直接暴露在互联网，安全风险很大。

（2）系统和设备的服役年限较长，软硬件无法及时升级更新，存在大量安全漏洞;

（3）网络隔离措施、主机安全防护措施等技术手段缺失，无法阻止病毒和攻击的漫延，无法应对脆弱性安全风险;

（4）威胁感知能力不足，当发生入侵攻击、恶意破坏、误操作等事件发生时，用户无法即时定位和有效溯源;

（5）安全运营能力不足，缺乏专业安全人员和安全运营能力，缺少对安全风险的发布、跟踪、响应的闭环管理。

4. 产业物联网：产业物联网是指连接工业产品、流程、服务等各环节的全球化网络。它实现了人、数据和机器间自由沟通。产业

物联网的特点是使用“智能设备+互联网”技术对已有的产业行业进行改进，解决以前无法解决的问题并大幅提高工作效率。例如：铁路运输系统使用智能闸机检票后，将以往需要多人检票的工作缩减为只需 1、2 名引导员在旁指引旅客正确使用闸机。并且闸机的智能验票和一票一过机制，有效解决了逃票问题。

虽然产业物联网发展的初衷是为了解决行业痛点、提升运营效率。但是由于部分设备厂商缺乏安全经验，重视业务和成本而忽视安全，导致部分新设备投产后向已有业务系统引入了大量安全隐患。

目前，针对产业互联网的安全威胁主要有：

（1）传感器状态直接影响生产流程，如出现安全问题后果严重；

（2）新型智能设备接入原有生产环境，冲击既有安全手段；

（3）数据安全依赖持续运维，难以做到安全和成本兼顾；

（4）云安全经验不足导致云主机和数据安全完全依赖云平台的基础安全能力；

（5）移动端 APP 开发外包，分发途径难以控制，易被不法分子利用。

三、物联网安全防护策略

（一）物联网安全防护策略框架

物联网应用系统由服务端、终端和通信网络等三部分构成。物联网安全防护体系架构涵盖物联网的感知层、传输层、应用层，涉及服务端安全、终端安全和通信网络安全等方面问题。由于物联网终端数量巨大、类型多、业务差异大、计算能力薄弱，无法部署传

统的防火墙、杀毒软件等安全防护手段，因此可以在连接终端与服务端的通信网络部分增加流量分析、态势感知等安全策略。物联网安全防护策略框架如图 3.1，通过采取被动防御、积极防御的技术策略，在兼顾物联网研发设计、上线运行以及报废等生命周期安全需求的基础上，最终可实现威胁情报驱动的智能感知乃至智能反制，自主应对物联网时代复杂多样的潜在网络安全威胁。

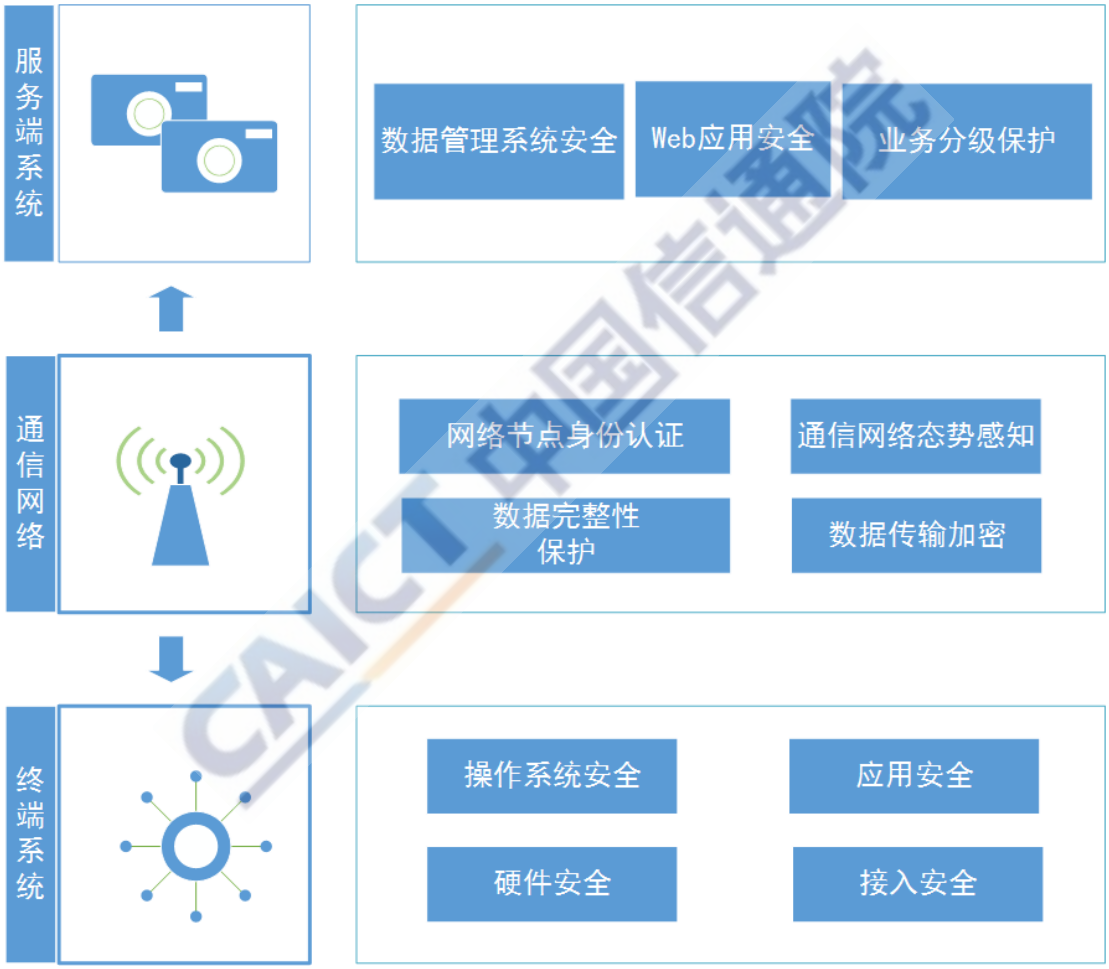

图 3.1 物联网安全防护策略框架

（二）物联网服务端安全防护策略

物联网服务端安全防护主要针对数据管理系统、基于云计算的 Web 应用、业务分级保护等方面的安全问题。

1. 分布式数据管理系统安全防护策略

物联网系统中包含大量设备，相应会产生海量数据，因此物联网中需要配备大量服务器资源，组成一个分布式、去中心化的数据管理系统，以对网络中海量数据进行有效的存储、管理、分析等。首先，该数据管理系统必须满足分布式数据库安全相关需求，包括身份验证、数据加密、数据备份与恢复机制等方面。其次，由于物联网中部署大量服务器，物联网服务端的数据管理系统也需要做到系统加固、漏洞检测与修复、防黑客、抗 DDoS 攻击、安全审计、行为检测等服务器安全防护，以防发生由于主机被攻破导致的数据泄漏、数据篡改等安全问题。

2. 基于云计算的 Web 应用安全防护策略

物联网智能设备业务系统通常会配备与云端服务相对应的基于云计算的应用，通过浏览器界面为用户提供业务相关的数据统计、展示及智能设备远程管理能力。这种应用本质上属于 Web 应用，因此物联网服务端也需要着重解决 Web 应用存在的安全隐患。在物联网安全防护体系中，针对 XSS、CSRF、SQL 注入、命令行注入、DDoS 攻击、流量劫持、服务器漏洞利用等典型 Web 应用攻击方式，按照“事前防范、事中防御、事后响应”的原则，可采取以下措施，最大程度减轻 Web 应用安全隐患，确保物联网服务端 Web 应用系统符合安全要求，维持系统稳定运行:

（1）设置安全基线，制定防篡改、防挂马安全规范，提出监测、防护与处置机制和要求;

（2）辅助以自动检测工具、检查列表定期开展检查工作;

（3）不定期进行 Web 威胁扫描、源代码评价及渗透测试，查找系统漏洞、研判是否挂马，及时对系统进行更新升级;

（4）对收集的数据进行统计、分析，定期形成系统安全态势分析报告;

（5）安装防病毒、通讯监视等软件。

3. 业务分级保护策略

近年来，物联网业务和应用爆发式增长，遍及智能交通、环境保护、公共安全、智能消防、工业监测、水系监测、食品溯源和情报搜集等多个领域。一旦这些业务和应用被攻击、相关信息和数据被窃取或伪造，都可能对国家安全、社会秩序、公众利益造成不同程度的侵害。因此，在实际应用中，需要对物联网业务和应用实施监测，并根据物联网具体业务和应用所可能涉及到的数据、对象以及对国家、社会和个人的影响程度，建立物联网应用和业务分级保护制度。针对不同的业务和应用，制定不同等级的安全防护技术要求和管理要求，采取不同防护及管控策略和措施，以满足不断提升的物联网网络安全防护要求。

（三）物联网终端安全防护策略

物联网中的终端设备种类繁多，如 RFID 芯片、读写扫描器、温度压力传感器、网络摄像头、智能可穿戴设备、无人机、智能空调、智能冰箱、智能汽车等，体积大小不一，功能复杂程度多样。这些终端所面临的安全威胁，除传统计算机病毒外，还包括木马、间谍

软件、劫持攻击、钓鱼邮件、钓鱼网站等。综合考虑物联网终端本身及其所面临的安全威胁特点，需从硬件、接入、操作系统、业务应用等方面着手，采取适当的安全防护措施，确保物联网终端安全乃至物联网整网安全。

1. 硬件安全。通过实现物联网终端芯片的安全访问、可信赖的计算环境、加入安全模块的安全芯片以及加密单元的安全等，确保芯片内系统程序、终端参数、安全数据和用户数据不被篡改或非法获取。

2. 接入安全。利用轻量级、易集成的安全应用插件进行终端异常分析和加密通信等，实现终端入侵防护，从而避免发生借助终端攻击网络关键节点等行为。同时需要轻量化的强制认证机制，阻止非法节点接入。

3. 操作系统安全。在安全调用控制和操作系统的更新升级过程中，通过对系统资源调用的监控、保护、提醒，确保涉及安全的系统行为始终是可控的。另外，操作系统自身的升级也应是可控的。

4. 应用安全。保证终端对要安装的应用软件进行来源识别，对已安装的应用软件进行敏感行为控制，同时确保终端中的预置应用软件无恶意吸费行为，无未经授权的修改、删除、窃取用户数据等行为。

（四）物联网通信网络安全防护策略

目前物联网中采用了现有的多种网络接入技术，其中包含窄带物联网络、无线局域网、蜂窝移动通信网、无线自组网等多种异构

网络，使得物联网在通信网络环节所面临的安全问题异常复杂，需要通过多重方案对整个网络层进行安全防护。主要可采取以下四方面措施:

1. 引入网络节点身份认证机制。在物联网通信网络中引入身份认证机制，利用关键网络节点对边缘感知节点的身份进行认证，从而防止和杜绝虚假节点接入到网络中，以确保通信网络节点安全。

2. 强化终端数据完整性保护。通过在物联网终端和通信网络之间建立安全通道，建立信息传输的可靠性保障机制，在保证用户通信质量的同时，对终端数据提供加密和完整性保护，防止数据泄露、通讯内容被窃听和篡改。

3. 加强数据传输加密操作。在杜绝明文传输的基础上，进一步加强数据过滤、认证等加密操作，确保传送数据的正确性。同时，还可进行设备指纹、时间戳、身份验证、消息完整性等多维度校验，最大程度保证数据传输的安全性。

4. 通信网络安全态势感知。由于物联网终端数量庞大、性能受限，无法部署传统的防火墙、杀毒软件等安全防护手段，而运营商拥有骨干网流量，具备对物联网设备进行监控的先天优势。运营商可通过网络空间搜索引擎进行公网物联网设备的主动识别以及通过流量特征进行局域网物联网设备的被动检测。在了解网络中目前连接的物联网设备基本状况后，可以对这些设备的流量进行分析并跟踪，对安全攻击实时监控，对物联网安全风险进行趋势预测，为后续的物联网安全风险治理奠定基础。

四、物联网安全未来发展展望

近年来，物联网在蓬勃发展的同时，也暴露出了许多安全问题。服务端、终端以及通信网等物联网应用模型各主要环节，仍然**存在网络安全**管理和**检测工作不规范、传统的安全防护技术不能适应当前的网络安全新形势、尚未建立起有效的安全防护防御体系和安全生态等诸多问题**。**下一步**，我们应**着眼于物联网未来发展**和安全需求，**针对物联网**未来发展**可能面临的网络安全新形势**和**新需求**，需要**从规范行业安全管理、制定行业安全检测标准、构建新型有效的安全防护体系、探索和研究新技术新应用等多个维度**着手，联合政府和行业力量，共同打造物联网安全生态，积极**推动物联网安全健康发展。**

（一）推动物联网安全技术标准落地及合规性检测

推动物联网安全技术标准落地实施，全面推广技术合规性检测，促进物联网产业良性发展。目前，国内已发布《物联网参考体系结构》《物联网术语》《网络安全等级保护基本要求 4：物联网安全扩展要求》《信息安全技术 物联网安全参考模型及通用要求》等系列国家和行业标准，为设备厂商、服务提供商、安全企业等开展物联网相关工作提供了技术要求和参考规范。下一步要健全完善物联网安全标准体系，加快推动相关技术标准落地实施，全面推广技术合规性检测，进一步促进物联网产业健康良性发展。

（二）以攻促防推进物联网安全技术发展

密切关注物联网攻防技术发展趋势，以攻促防，建立适应物联网环境的安全防护机制。当前，针对物联网业务系统的攻击手段已经超出传统网络攻击范畴，攻击形式更加多样化，传统的防御手段难以满足日益增长的安全保护需求。为此，可从攻击的角度出发对物联网系统进行安全风险分析及检测评估，深入研究物联网应用系统可能存在的安全漏洞，以及针对这些漏洞的新型攻击手段，攻防结合，在完整攻击链条中寻找最佳防御点，采取针对性的防御技术，构建有效的物联网安全防护体系。

（三）构建物联网全生命周期立体防御体系

加强物联网全生命周期安全管理，构建覆盖物联网系统建设各环节的安全防护体系。在物联网业务系统规划、分析、设计、开发、建设、验收、运营维护以及废弃等各环节，明确安全管理规章制度并严格执行安全管理，使安全融入到物联网系统建设全生命周期中。在开发阶段，严格依据要求和规范进行系统软硬件开发及测试，并阶段性开展安全测试；在建设、验收阶段，严格执行安全管理，在系统建设完成后进行安全风险评估，保障安全防护的有效性和合规性；在运营维护阶段，定期进行安全风险评估，持续跟踪威胁情报和信息，改进安全管理和防护措施；在系统废弃阶段，做好残余信息清理工作，形成全生命周期安全防护管理体系。

（四）联合行业力量打造物联网安全生态

联合物联网产业链各方力量，共同打造物联网安全生态。物联网产业具有高度融合、应用多样、发展迅速等特点，其生态覆盖传感器元器件制造、设备集成生产、网络服务提供、软件服务提供、系统集成开发及销售等环节，安全问题更是涉及传感器、芯片、硬件，通信技术、网络服务以及相关行业领域应用等方面，因此构建开放、合作、共赢的安全生态圈是产业发展的必然趋势和要求。未来，我国需要从整机设备、核心芯片、安全运营服务等板块入手加快产业布局，形成产业链上下游协同创新的局面，推进产业转型升级，提升我国物联网安全产业核心竞争力。

（五）探索新技术在物联网安全领域的应用

加快探索物联网安全新技术新应用，满足不断发展的物联网安全防护新需求。随着物联网技术的发展和应用的创新，未来物联网在服务系统、终端、通信网络等方面都将面临巨大挑战，例如如何有效管理百亿级别的多源异构终端设备、如何解决海量数据对网络带宽带来挑战等，同时也给物联网安全提出了更高要求。下一步，我们要着眼于物联网未来发展趋势，加快对去中心化认证、边缘计算、终端安全轻量化防护技术、软件定义边界等新技术新应用的研究和探索，将其应用于物联网安全防护中，满足物联网未来发展的安全保护需求。

中国信息通信研究院

地址：北京市海淀区花园北路 52 号
邮政编码：100191
联系电话：010-62304839
传真：010-62304980
网址：www.caict.ac.cn