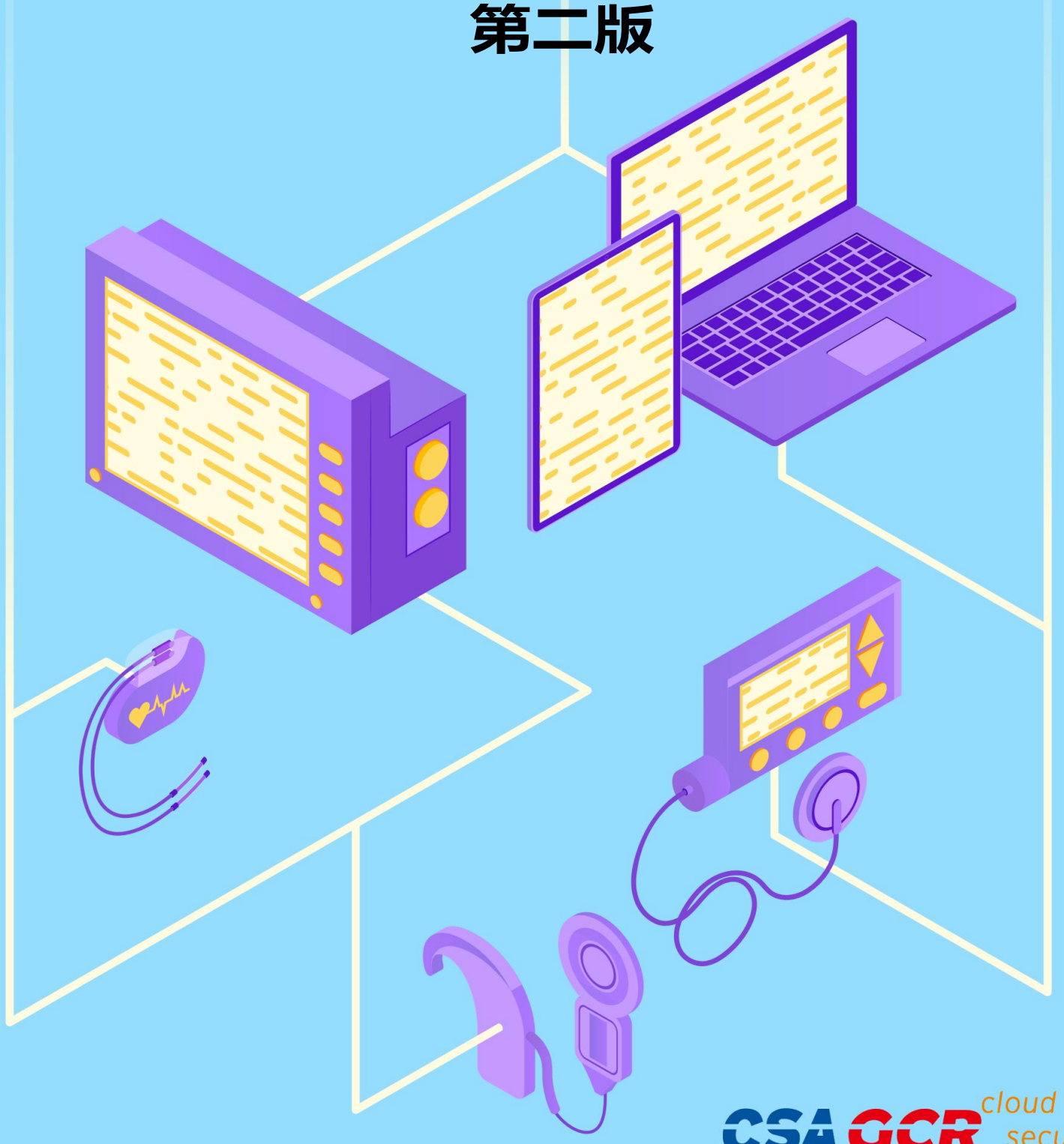
物联网安全控制框架指南

第二版



CSA GCR cloud security alliance®
GREATER CHINA REGION

云安全联盟物联网工作组官方网址：
https://cloudsecurityalliance.org/working-groups/internet-of-things/

@2022 云安全联盟大中华区-保留所有权利。本文档英文版本发布在云安全联盟官网（https://cloudsecurityalliance.org），中文版本发布在云安全联盟大中华区官网(http://www.c-csa.cn)。您可在满足如下要求的情况下在您本人计算机上下载、存储、展示、查看、打印此文档：（a）本文 只可作个人信息获取，不可用作商业用途；(b) 本文内容不得篡改；(c)不得对本文进行转发散布；(d)不 得删除文中商标、版权声明或其他声明。在遵循美国版权法相关条款情况下合理使用本文内容，使用 时请注明引用于云安全联盟。

致谢

本文档《CSA 物联网安全控制框架指南》第二版(CSA Guide to the IoT Security Controls Framework v2)由 CSA 物联网工作组专家编写，CSA 大中华区物联网工作组专家翻译并审校。

中文版翻译专家：

组织者：余晓光

贡献者：余晓光、刘宇馨、陈皓、姚凯、赵锐、何国锋、卢佐华、李腾飞、于继万、任永攀、薛伟佳、雷慧桃、刘洪森、姚博龙

主要审核者：余晓光

贡献单位：华为、奇安信、中国电信、浙江大华、启明星辰

英文版原创作者：

发起人：Aaron Guzman、Michael Roza、Brian Russell

主要贡献者：Renu Bedi、Ramon Codina、 Umesh Jaiswal、Raj Sachdev、Ashish Vashishtha

CSA 员工：Hillary Baron、AnnMarie Ulskey (Graphic Design)

在此感谢以上专家。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！

联系邮箱：info@c-csa.cn；云安全联盟 CSA 公众号

© 2022 云安全联盟大中华区版权所有

序 言

根据全球移动通信系统协会（GSMA）统计数据显示，2010～2020 年全球物联网设备数量高速增长，复合增长率达 19%。随着 5G 的大规模商用，以及云计算、AI 等不断地成熟和应用，万物物联成为全球网络未来发展的重要方向，在工业领域、智慧城市、车联网、智能家居、智慧穿戴等领域发挥重要作用。

在一片物联网蓬勃发展的局面下，我们也不能忽视，物联网安全是物联网能够广泛应用的先决条件。随着越来越多的物联网终端接入到网络中，大量的数据接入点被添加到物联网系统中，这为企业的整体物联网安全防护提出严峻的挑战。因此 CSA 云安全联盟推出了物联网安全关键技术白皮书，旨在帮助广大的企业面对物联网的安全挑战时能够有所参考和依据，本白皮书的内容对于如何做好物联网的安全防护、安全检测有现实的参考作用。在使用中可以根据自己的实际情况进行适配。

本次的编写工作由 CSA 大中华区物联网安全工作组共同完成，在工作过程中如有疏漏、错误等问题，还请读者及时指出。

李雨航 Yale Li
CSA 大中华区主席兼研究院院长

© 2022 云安全联盟大中华区版权所有

目录

介绍 6
目标 6
目标受众 6
版本管理 6
如何使用 IoT 安全控制框架 8
安全控制目标(A、B、C、D、E、F 列) 8
IoT 系统风险影响等级（G、H、I 列） 10
控制指南补充（J、K 列） 11
实施指南（L、M、N 列） 12
设备、网络、网关和云服务（O、P、Q、R） 13
其他参考资料 14

© 2022 云安全联盟大中华区版权所有

介绍

物联网（IoT） 市场随着工业领域在连接和自动化方面的进步在不断扩大。企业对物联网生成的数据和功能的依赖正在迅速增加，要求采用这些新技术的企业不断增多，这些企业组织需要规划可访问、安全和弹性的部署形式。鉴于互联技术的迅速革新和新威胁的持续出现，这些愿景具有很大挑战性。创建安全的物联网环境需要安全工程来解决特定风险，并采用适当的缓解措施。云安全联盟（CSA）物联网安全控制框架为希望更好的理解和实施其物联网体系结构中安全控制项的组织提供了一个起点。框架随附的本指南解释了企业组织如何使用该框架安全的评估和实施物联网系统。

物联网安全控制框架用于部署各种互联设备和相关云服务、网络技术和应用软件的企业物联网系统。该框架在许多物联网领域都具有效用，从只处理影响力有限的“低价值”数据系统到支持关键服务的高敏感系统。系统所有者根据存储和处理的数据价值以及各种潜在的物理安全威胁影响对组件进行分类。

该框架帮助用户确定适当的安全控制项，并将其分配给特定的体系架构组件，包括:

- 设备
- 网络
- 网关
- 云服务

在这个架构中，分配给每一层的控制项代表最佳情况的安全布局。在某些情况下，架构组件无法实现此框架中实现建议的某些控制项。在这种情况下，系统安全架构师应识别这些缺陷，并制定计划，使用替代措施降低剩余风险。

目标

物联网安全控制框架提供了一个工具，用于评估实施在贯穿开发生命周期的安全性，以确保他们符合行业指限定的最佳实践。

目标受众

物联网安全控制框架是系统架构师、开发人员和安全工程师的一个资源，用来设计安全的物联网生态系统。物联网系统评估人员（如审计师和渗透测试人员）可以利用该框架来验证控制及其部署的实施情况。

版本管理

- **物联网安全控制框架第 1 版**

© 2022 云安全联盟大中华区版权所有

引入了 155 个基本级别的安全控制措施，以减轻物联网系统在各种威胁环境中面临的许多风险。

- **物联网安全控制框架第 2 版**

改进了第 1 版框架，以便更好地将控制措施归类到一组全新的域中，并最大限度地减少了分配给物联网架构内的组件的控制措施。重要的变化包括开发了全新的域结构和基础设施，后面会予以解释。

- 更新的控制:为了保证技术清晰，所有的控制措施都经过了审核和更新。
- 全新的域结构:审查和更新了控制域，以 更好地分类控制措施。
- 新的法律领域:引入相关的法律控制措施。
- 新的安全测试域:引入架构分配的安全测试。
- 简化基础设施分配:将设备类型合并到一个单一类别，简化对架构组件分配控制措施。

- **未来的变更-第 3 版将包括以下值得注意的改进:**

- 物联网框架的共享责任矩阵
- 安全所特定的控制措施
- 受损指标
- 物联网框架到欧盟网络和信息安全局(European Union Agency for Network and Information Security, ENISA)制定的物联网安全指南的映射
- 物联网框架到美国国家标准与技术研究所(National Institute of Standards and Technology, NIST)网络安全框架(CSF)和 800-53 的映射

© 2022 云安全联盟大中华区版权所有

如何使用 IoT 安全控制框架

下面图 1 详细说明用户使用 CSA IoT 安全控制框架对独特的环境进行评估和实施安全控制时应遵循的流程。图中的字母对应于框架（电子表格）中的列。

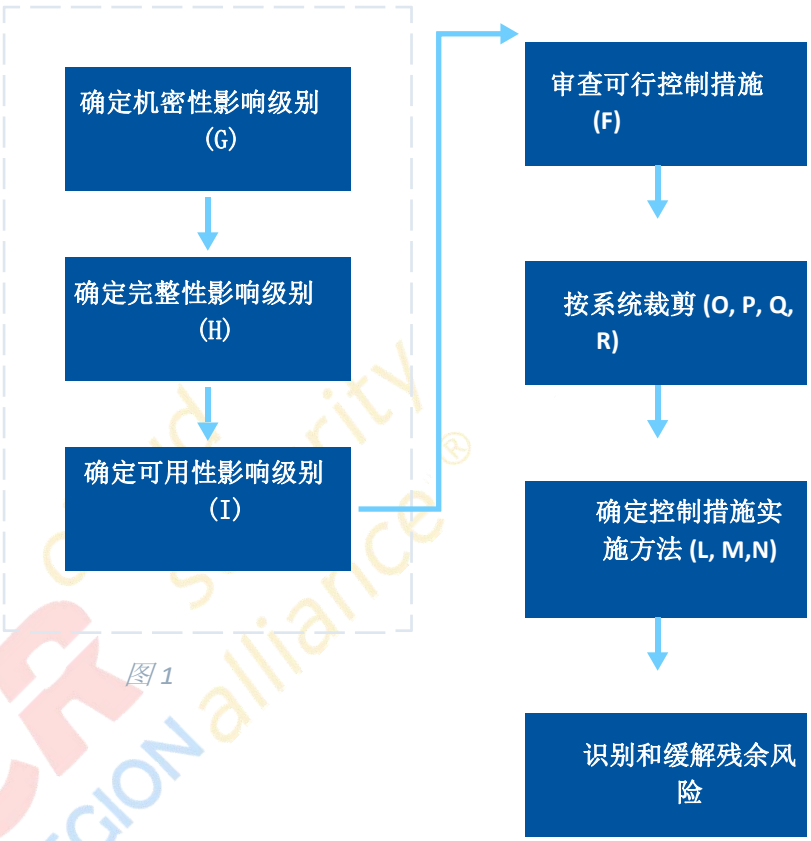


图 1

评估始于对系统架构安全性和数据影响级别的了解。他们的特点是基于标准过程，如美国联邦信息处理标准出版(FIPS) 199。一旦确定了系统机密性、完整性和可用性的影响级别，就可以对框架进行筛选，仅显示适用于这些影响级别的控制措施。

审查 F 列中的每个结果控制措施，并查看 J 列中的任何附加指南。O、P、Q 和 R 列包括用于将控制措施分配给不同架构组件的工具。

这些列允许用户根据控制措施是用于设备、承载设备的网络、网关还是云服务进行筛选。

用户还可以了解如何使用 L、M 和 N 列实现控制措施。这些列提供了控件类型的建议，控制措施应该是手动的、自动的和两者结合，以及控制措施的执行频率。

遵循这一初始流程，该框架提供了为物联网系统架构量身定制的安全基线的理想版本。物联网架构中的某些组件可能无法满足部分控制措施。在这种情况下，安全架构师必须了解残余风险并确定补偿性控制措施以缓解风险。

安全控制目标(A、B、C、D、E、F 列)

图 2

控制域（A 列）：由各个安全控制措施的逻辑分组（请参见下表）组成，并在 F 列（控制）中进行了详细说明，每个控制规范的名称均在“控制域”类别下用斜体字表示。

控制域（B 列）：按域进行分类。

© 2022 云安全联盟大中华区版权所有

控制子域（C 列）：子域以更细的粒度进行分类。

#	控制域名称	缩写	子域
1	资产管理	ASM	命名约定，库存资产，监控资产
2	配置管理	CCM	配置文件、固件更新、配置控制、报废计划
3	通信安全	COM	可信通信，消息队列遥测传输（MQTT）安全，加密通信
4	数据安全	DAT	数据分级和分类，数据清理，静态加密数据
5	治理	GVN	治理框架，法规和法律要求，合规管理，隐私权，业务连续性，安全性
6	身份与访问控制	IAM	口令管理、身份验证，授权，访问控制，证书管理，密钥管理，信任锚管理，引导程序，账户审核
7	事件管理	IMT	事件响应
8	物联网设备安全	IOT	认证的设备，安全平台，安全配置
9	法律	LGL	法律评估，法律实施计划，法律目的，条款和条件以及隐私政策的文件措施，合同，免责声明，披露，通知弃权，责任，数据传输
10	监控和记录	MON	威胁情报，威胁搜寻，自动恶意软件日志管理，分析，事态定义，射频（RF）监控
11	运营可用性	OPA	维护，故障恢复，分布式拒绝服务（DDoS）保护，服务水平协议
12	物理安全	PHY	物理访问控制
13	政策	POL	策略定义、采集安全策略、安全处置
14	风险管理	RSM	风险管理策略、风险管理执行、限制责任

© 2022 云安全联盟大中华区版权所有

15	安全应用	SAP	移动应用程序、云服务、自治系统
16	安全系统 开发生命周期	SDV	流程安全、供应链/采购、安全开发实践、安全测试
17	安全网络	SNT	安全发现、网络强化、零信任、网络可视化
18	安全无线网络	SWS	RF 架构、蓝牙安全、近场通信 (NFC) 安全、Zigbee 安全
19	培训	TRN	管理员培训、用户培训
20	漏洞管理	VLN	负责任的披露计划、漏洞扫描、更新和补丁
21	安全测试	SET	评估范围和规划，渗透测试， 红队、第三方评估、漏洞赏金、物联网 应用程序和服务（内部开发）

控制 ID（D 列）：控制标识（ID）是特定安全控制的官方标识符。 ID（例如，“RSM-01”）允许通过控件在框架中的位置在别处引用控件。

CCM ID（E 列）：框架中的安全控制在此列中关联或映射到来自 CSA 云安全控制矩阵（CCM）的标识符。当 IoT 安全控制衍生或链接到 CCM 控制时，将识别一个或多个条目。相关控制涉及部分或全部覆盖每个框架中的控制规范。

控制规范（F 列）：规范被编写为解决物联网系统特定风险领域的缓解或对策。为了可用性，每个控件都被分成一个简化的操作，以解决独特的 IoT 环境。

IoT 系统风险影响等级（G、H、I 列）

从第 G 列到第 I 列：这些信息允许根据用户的独特环境对安全措施进行初始裁剪，在开始定制单个安全控制措施之前，用户应参阅两份美国商务部的出版物：《联邦信息和信息系统安全分类标准》（FIPS 199）1 和《联邦信息和信息系统最低安全要求》（FIPS 200）2。FIPS 199 和 FIPS 200 这两份出版物从机密性、完整性和可用性三个安全目标方面，将风险影响级别划分为“低”、“中”或“高”三个水平。

G	H	I
物联网（IOT）系统影响级别		
机密性	完整性	可用性

图 3

© 2022 云安全联盟大中华区版权所有

机密性（G 列）：物联网（IoT）系统中的某些数据，比如个人隐私和专有信息，需要通过各种安全控制措施进行限制访问，以保持适当的机密性。为了评估物联网（IoT）系统内各组件的机密性风险，有必要估计系统数据被公开或被某些攻击者泄露的潜在影响（低、中或高）。

完整性（H 列）：为了保护数据的完整性，企业必须防止数据被不适当修改或破坏，确保信息的真实性。要评估物联网（IoT）系统的完整性方面的风险，需要评估系统数据被破坏或不适当修改时的影响（低、中或高）。

可用性（I 列）：为了确保及时可靠地获取和使用系统信息，需要评估系统在任何一段持续时间内不可用时的潜在风险。

评估系统数据的机密性、完整性和可用性的特定风险是低风险、中风险还是高风险，请参阅出版物 FIPS 199 第 6 页表 1“安全目标的潜在影响定义”。

在确定这些风险影响级别后，物联网（IoT）安全控制框架就可以识别特定环境所需的所有安全控制措施。

请注意，当风险影响级别较高时，应当选用所有可用的安全控制措施，包括低、中、高风险级别的所有安全控制。当风险影响水平为中等时，应当选用中等和低风险水平的所有控制措施。下表是三种影响等级和所需的安全控制措施示例。

安全风险类别	风险影响级别	所需安全控制措施
机密性	高	高、中、低
完整性	中	中、低
可用性	低	低

图 4

控制指南补充（J、K 列）

图 5

额外指导（J 列）：在评估或实施物联网安全控制框架中的任何单个安全协议时，请务必查看这份详细说明了特殊需求、术语解释、以及相关操作提示的补充信息。

© 2022 云安全联盟大中华区版权所有

参考（K 列）：本列提供了专业来源的信息，包括政府出版物、法律法规信息和其他便于充分理解和实施控制规范所需的参考资料等。

实施指南（L、M、N 列）

当为企业实施安全计划时，请使用框架中的“实施指南”部分来帮助确定企业特有环境所需的控制类型（L 列），该组织将如何实施控制措施（M 列），以及每项安全控制措施的实施频率（N 列）。

图 6

安全控制措施的类型（L 列）

物联网框架的安全控制措施根据这些措施在何时、何地，以及如何提高安全性分为三种类型。

预防性控制：阻止某些安全事件发生，例如：通过锁门或使用更高级别的生物识别来限制进入房间的权限。

检测性控制：识别并提取事件特征。如通过盘点发现库存差异、录制视频、并使用运动传感器检测非法入侵。

纠错性控制：减轻安全事故造成的损害。例如：灭火器可以减少火灾的潜在影响，或者在主数据中心发生故障时可以切换至备用的数据中心。

控制实施指南（M 列）

安全控制措施根据自动化程度，可以分成三种方式进行实施。

手动控制：手动控制由人员执行。例如在风险管理流程审核中，通过人员评估来确认流程是否按照策略进行执行。

自动控制：自动控制由系统进行执行，无需人员干涉。例如在用户访问检查中，用户使用用户名和密码进行登录。系统在验证其组合正确后授予访问权限。

控制频率（N 列）

一些组织需要根据内部风险优先级或监管合规要求进行更频繁的控制。针对不同情况推荐以下频率（视个别企业需求而定）。

- 每年
- 季度
- 每月

© 2022 云安全联盟大中华区版权所有

- 每周
- 日常的
- 事件：不规则执行的控制（例如，软件更新）
- 连续：每天执行多次控制（例如，用户访问）

设备、网络、网关和云服务（O、P、Q、R）

物联网框架指导物联网系统中架构元素控制的应用。这些架构元素代表物联网架构中的标准层，如下图所示。

图 7

实施者应查阅这些文档部分以确定控制是否适用于每一层。每列都描述了在 IoT 架构中创建信任边界的机会。应在每一层应用离散控制。

设备（O 列）

直接应用于设备层的控件，专注于设备处理、存储和/或生成的数据。通用物联网设备将包含传感器、执行器和可能的最小用户界面。该设备还可以使用必须受到完整性保护的配置文件来收集和存储事件或安全日志。

网络（P 列）

在网络层面上，通信模组是最常见和必需的构成模块之一，帮助设备实现入网连接功能，如无线访问接入点（WAPs）类模块，可支持设备实现 WiFi 入网连接。其他网络构成模块还包括密钥管理服务器，常和特定网络协议绑定着，用于保障网络协议实现的安全性。 此外，为加强网络安全控制，零信任设计，虚拟局域网（VLAN）划分，防火墙和入侵检测设备等技术都可被使用，用来加强网络安全层面的访问和接入安全。数据保护层面，建议采取机密性和完整性保护措施，保障业务传输过程中的数据安全性。

网关（Q 列）

网关作为 IoT 设备入网前的汇聚接入点，经常被视为攻击者的潜在物联网网络入口点。 与普通 IoT 设备相比，由于其本身计算、存储能力较强，网关通常应用了更多的安全控制措施，如链路 AES 加密、访问控制措施等。

© 2022 云安全联盟大中华区版权所有

云服务（R 列）

大多数物联网设备需要云环境才能运行。设备可以将数据直接发送到云，也可以通过云服务进行管理。传输到云的数据必须在传输过程中受到保护，并且必须在云提供商的存储中永久保存。在某些情况下，必须在云中应用匿名保护，以确保身份不能被关联到相应 IoT 数据，造成隐私泄露。

下图提供了这些体系结构层的直观描述。

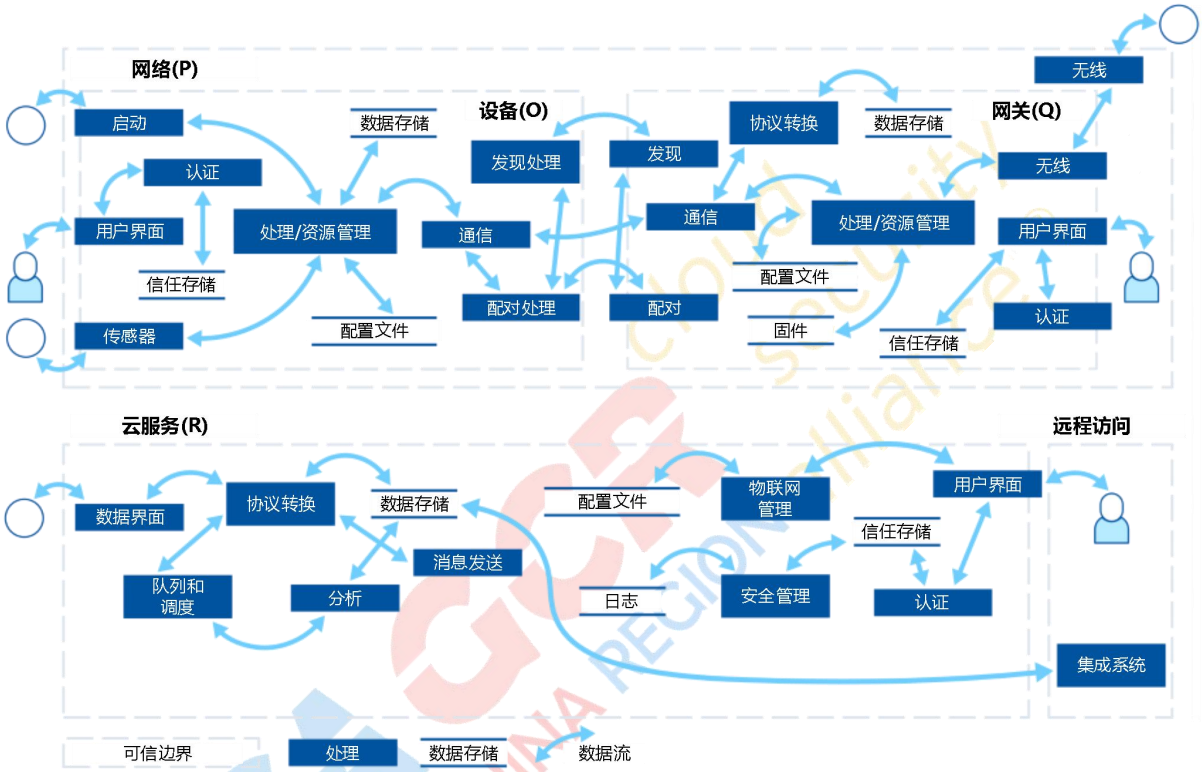


图 8

其他参考资料

Fagan, Michael. Megas, Katerina N. Scarfone, Karen. Smith, Matthew. “物联网设备制造商网络安全指南”, 2020-05, NISTIR 8259, 美国国家标准与技术研究所.
https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf

Fagan, Michael. Megas, Katerina N. Scarfone, Karen. Smith, Matthew. “物联网设备网络安全能力核心基准”, 2020-05, NISTIR 8259A, 美国国家标准与技术研究所.
https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf

Boeckl, Katie. Fagan, Michael. Fisher, William. Lefkovitz, Naomi. Megas, Katerina N. Nadeau, Ellen. Piccarreta, Ben. Gabel O’Rourke, Danna. Scarfone, Karen. “管理物联网网络安全和隐私风险的注意事项”, 2019-06, NISTIR 8228, 美国国家标准与技术研究所.
https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST. IR.8228.pdf

© 2022 云安全联盟大中华区版权所有

Iorga, Michaela. Feldman, Larry. Barton, Robert. Martin, Michael J. Goren, Nedim. Mahmoudi, Charif. “雾计算概念模型：美国国家标准与技术研究所的建议”, 2018-03, NIST SP 500-325, 美国国家标准与技术研究所.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf

机构间国际网络安全标准化工作组. “关于物联网（IoT）国际网络安全标准化现状的机构间报告”, 2018-11, NISTIR 8200, 美国国家标准与技术研究所.
https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8200.pdf

Voas, Jeffrey. Kuhn, Richard. Laplante, Phillip. Applebaum, Sophia. “物联网（IoT）信任问题”, 2018-09, NISTIR 8222, 美国国家标准与技术研究所.
https://csrc.nist.gov/publications/detail/nistir/8222/draft

欧盟网络与信息安全局（ENISA）. “物联网安全的良好实践：安全软件开发生命周期”, 2019-11.
https://www.enisa.europa.eu/publications/good-practices-forsecurity-of-iot-1

欧盟网络与信息安全局（ENISA）. “关键信息基础设施背景下的物联网基线安全建议”, 2017-11.
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

ISO/IEC JTC 1/SC 41. “物联网参考架构”, 2018-08.
https://www.iso.org/standard/65695.html

Microsoft Azure. “物联网（IoT）安全最佳实践”, 2018-10.
https://docs.microsoft.com/enus/azure/iot-fundamentals/iot-security-best-practices

© 2022 云安全联盟大中华区版权所有