新型基础设施支撑的物联网服务的安全分析

Analysis of the Security of IoT Services Supported by New Infrastructure

刘文懋，雷　新（北京神州绿盟科技有限公司，北京 100191）
Liu Wenmao，Lei Xin（Nsfocus Information Technology Co.，Ltd.，Beijing 100191，China）

摘　要：
随着云计算、物联网和运营商网络的快速发展，可预计未来10年各类新型基础设施的融合会成为一个明显的趋势。首先介绍支撑未来10年内的新物联网应用的基础设施及其关键技术，然后讨论这些基础设施给物联网应用带来的安全挑战，最终给出一些应对策略。

关键词：
物联网安全；5G；边缘计算；云计算
doi：10.12045/j.issn.1007-3043.2019.04.013
中图分类号：TN915.08
文献标识码：A
文章编号：1007-3043（2019）04-0058-05

Abstract：
With the rapid development of cloud computing，Internet of Things and operator networks，it is predicted that the convergence of various new infrastructures will become an obvious trend in the next decade or so. Firstly it introduces the infrastructure and key technologies supporting the new Internet of Things applications in the next decade，then discusses the security challenges brought by these infrastructures to Internet of Things applications，and finally gives some countermeasures.

Keywords：
IoT Security；5G；Edge computing；Cloud computing

引用格式：刘文懋，雷新. 新型基础设施支撑的物联网服务的安全分析[J]. 邮电设计技术，2019(4)：58-62.

1 物联网应用的关键基础设施

1.1 面向物联网应用的云计算基础设施

云计算技术的发展已经超过了10年，无论公有云还是私有云，都具备了提供大规模计算资源、平台服务或应用托管的能力。特别是公有云的平台即服务（PaaS），可为不同的场景下的应用提供诸如AI计算、数据存储、认证和消息队列等服务，通过按需调用这些服务，可组装成云原生（Cloudnative）的物联网应用，支持大规模物联网设备直连云端服务的应用场景。

收稿日期：2019-03-22

如亚马逊AWSIoT平台提供了物联网设备连接、管理和分析功能，并且提供了如FreeRTOS和1-Click等嵌入式操作系统和微服务接口，用于无缝对接AWS的各项云服务。

国内厂商如阿里云在物联网上推出了物联网云平台Link Platform、边缘网关Link Edge和物联网操作系统AliOS Things，同样提供了设备管理和数据分析的功能。在生态合作方面，阿里巴巴与传统厂商合作，开发物联网产品，目前阿里巴巴的产品非常多，截至2018年4月7日，从天猫上搜索“阿里智能”就可以找到4 000多个商品，覆盖环境管家、数码娱乐、全屋智能和运动健康等领域。

表1列出了一些在业界具有代表性的公有云服务商，无一例外地均提供了物联网云平台的服务。这些云服务商或多或少地提供了物联网操作系统或模组SDK，与第三方厂商合作，生产可接入物联网平台的智能物联网终端。

表1　主流公有云服务商的物联网平台

云服务商	云服务	物联网云服务	边缘和终端功能	功能
Amazon	AmazonAWS	AWS IoT平台，AWS Greengrass	AWSIoT设备SDK	设备接入和控制，APP访问与控制，数据分析
阿里巴巴	阿里云	阿里云物联网套件	物联网操作系统AliOS Things边缘网关	设备接入、设备通信、安全能力、设备管理、规则引擎
Google	Google Cloud Platform	GOOGLE CloudIoT	TPU、提供板级SDK接入云平台	连接、管理设备，数据分析
腾讯	腾讯云	微信硬件平台 QQ物联平台 腾讯云物联网套件IoT Suite	物联网套件IoT Suite SDK支持linux和android、RTOS	设备接入、消息转发、消息存储等，机器学习、大数据、云监控服务
百度	百度云	百度天工	百度云智能边缘，设备SDK	数据采集、传输、计算、存储、展现到分析

除了以上云服务商从云端出发自顶向下地建立物联网应用外，还有一些物联网厂商虽然没有云计算的背景，但从物联网芯片和业务入手，为物联网厂商提供了物联网设备SDK，同时建立了物联网平台，自底向上地提出了物联网应用解决方案，如国内的机智云、庆科云等。

此外，在一些工业物联网的场景中，一些云计算服务商直接提供了针对细分领域的物联网云平台服务，例如寄云（neucloud）将工业设备的运行数据保存到云端，并为企业运营者提供直观的运行情况展示，提供运营需要的支撑数据，还可通过计算分析找到运行异常的设备。

1.2　面向实时物联网应用的边缘计算和5G网络

物联网云服务主要部署在云服务商所在的数据中心，数据流从物联网终端设备经过互联网到达云计算数据中心，整个过程会存在一定的延迟。在一些低延迟近乎实时的应用场景中，如自动驾驶、工业控制，这样的延迟是无法接受的；此外互联网的链路存在不稳定性，一旦到云端的通道延迟或中断，终端就无法进行正常的数据处理，可能引发严重的后果。

所以，在很多物联网云服务商提出的解决方案中，除了云端和终端外，还引入了边缘网关的角色，该网关承担实时决策和部分数据处理工作，边缘侧和云端共同组成完整的设备控制和数据处理机制。例如，表1中的AWS和百度云的物联网解决方案中均包含了边缘网关，最终提供了人工智能处理海量实时数据的功能。客户可在接入互联网的出口处部署边缘网关，在内部网络部署物联网设备，对内组成高速传输的网络。

除了云服务商可以在客户侧或CDN侧部署边缘网关外，电信运营商也积极参与到物联网和边缘计算的建设中。特别是5G标准中，ITU-R将超高可靠与低延迟的通信（uRLLC）作为三大应用场景之一，这就要求运营商了解物联网应用的区域，并在建设和运营时将边缘服务尽可能贴近应用基站。这将改变现在运营商数据中心和部署云服务的模式，给托管云服务提出了更灵活的要求。

需要说明的是上述基础设施将会彼此融合，例如AWS的GreenGrass云服务提供了物联网分析、存储服务。考虑在工业物联网等场景下对实时性、网络中断而业务不断的要求，GreenGrass支持边缘计算，使得物联网设备可以运行Lambda函数处理收集到的数据，这样设备即使在离线状态也可以完成部分功能。

2　新基础设施下的物联网服务的安全挑战

2.1　云计算带来的安全挑战

随着云计算技术引入物联网应用，会出现2类安全挑战：云平台自身的安全问题和使用云服务后的物联网应用的安全问题。

a）云平台数据秘密性。物联网设备的所有者将物联网设备产生的数据传输到了云平台中，并保存在云存储中。与传统的on-premise嵌入式应用平台相比，物联网云平台暴露的攻击面大大增加，如何提高整个云计算系统的安全防护能力，防止恶意攻击者攻破并窃取有价值数据，将是云服务商面临的巨大挑战。

b）云平台可信度。物联网平台上存储的数据的拥有者为物联网设备拥有者或物联网厂商，但数据存放在云端，数据拥有者缺乏物理上的控制权，这会带来潜在的风险。此外，云服务商的内部员工可能恶意窃取或篡改物联网应用数据，云平台的可信度是物联网上云的挑战之一。

c）云服务可用性。物联网应用会管理上百万规

模的物联网设备，所以物联网服务的可用性就显得尤为重要。当云服务出现服务中断或被拒绝服务，则整个物联网应用可能会陷入瘫痪。

d）来自云平台的攻击。如果攻击者攻破了云平台，或内部员工恶意控制了物联网云服务，则可以通过云端指令向物联网设备下发指令，如下载恶意代码、对特定目标发动拒绝服务连接等，从而影响特定或所有的物联网设备的安全性。这将比破解一两个物联网设备的危害性大得多。

总之，当云计算应用在物联网场景下，既要考虑到云计算自身的安全问题，还要考虑物联网在云计算的应用中面临的独特挑战。

2.2 边缘计算带来的安全挑战

边缘计算将远程计算存储拆分成了云端和边缘两级，那么会存在以下安全挑战。

a）认证机制。为了加快认证速度，会在云端和边缘侧实现协同的认证机制。当云端认证通过后，边缘节点会缓存认证信息。但整个过程需要考虑各种因素，例如重放攻击、凭证失效时间等，以防止攻击者绕过云端认证，伪造边缘节点控制物联网终端。

b）由于带宽和实时性要求，业务安全的数据分析会将大量的训练过程放到云端，而将分类过程放在边缘节点，但该计算模型需要考虑数据分析的准确率和响应速度。在业务量巨大的物联网网络中，这将会是一个巨大的挑战。即便误报率降到很小的比例，乘以海量的事件数，也是人力难以处理的量级。

c）运营商网络中的边缘节点尽可能靠近业务位置，该边缘节点除了业务处理外，还需要具备相应的安全能力，那么边缘节点中按需的安全防护能力，安全防护机制是在核心网络部署，还是在边缘节点部署，需要考虑资源约束条件和服务需求，这将考验运营商网络架构和安全体系的成熟度。

2.3 5G网络带来的安全挑战

5G网络存在3种应用场景，其中2个与物联网相关。其中：高可靠性与低延迟通信（uRLLC）可以将延迟降低到1 ms，那么这些实时性很高的应用中就应该将后端的处理时间也压缩到同等数量级，这对整体系统设计和性能优化提出了很高的要求；此外海量连接通信（mMTC）可在每平方公里管理十万台物联网终端，那么也对边缘节点的高并发长连接能力提出了要求。如果这些物联网应用在设计上不考虑通信网络、边缘节点和应用场景，很容易在服务可用性、认证和加密性能上出现瓶颈。

此外，5G网络实现了全网络IP化，即在接入网、汇聚网和核心网都运行了TCP/IP协议，在此基础上可部署基于X86的计算存储资源实现服务编排，那么是否可以利用SDN/NFV技术，在上述网络中部署可快速生效的安全资源，并将安全能力融合进标准的NFV架构，形成可管理、可控制的安全资源池，这将向安全厂商和运营商提出新的挑战。

2.4 合规性的挑战

当物联网服务保存用户终端的数据时，必然会涉及到用户隐私问题，2018年5月欧洲的通用数据保护法案GDPR正式落地，届时会对物联网服务商的方案中的数据存储、数据传输提出了很高的合规性要求。例如车联网应用中需要对车辆标识、PKI等做匿名化处理，以防止被攻击者跟踪行迹。

此外，一些国家考虑到网络空间主权，颁发的法律法规也对服务商数据存储的归属做出了规定。这对于物联网应用的架构、国际化（i18n）和服务承诺（SLA）都提出了挑战。

3 新型基础设施下的物联网服务的安全对策

3.1 云计算平台的安全防护

从云服务商的角度，应在设施、平台和应用层面保证云计算系统的安全性，从而保障运行的物联网平台安全（见图1）。

例如，在云计算系统和虚拟环境建设时，应根据业务的安全需求，事先划分安全域，并在边界侧部署访问控制策略；并分析物联网服务所面临的安全威胁和自身的脆弱性特点，有针对性地部署检测和响应机制，在运行时检查网络流量和终端内部行为，建立正常场景下的基线，分析异常的行为，对恶意攻击进行隔离、响应和溯源取证。

3.2 面向物联网服务的安全云

在用户的角度，除了云服务商的安全机制外，还应该有独立的第三方安全厂商提供专业的安全保证，例如对物联网终端到云端数据流进行安全防护，以及对物联网云服务的安全检查。针对应用即服务（SaaS）的业务，国外较为成熟安全机制为基于云访问的安全代理（CASB——Cloud Access Security Brokers）。

CASB一般部署在终端到云端之间的某个位置，对经过的数据在业务层面进行分析和处理，CASB通常有3种部署方式。

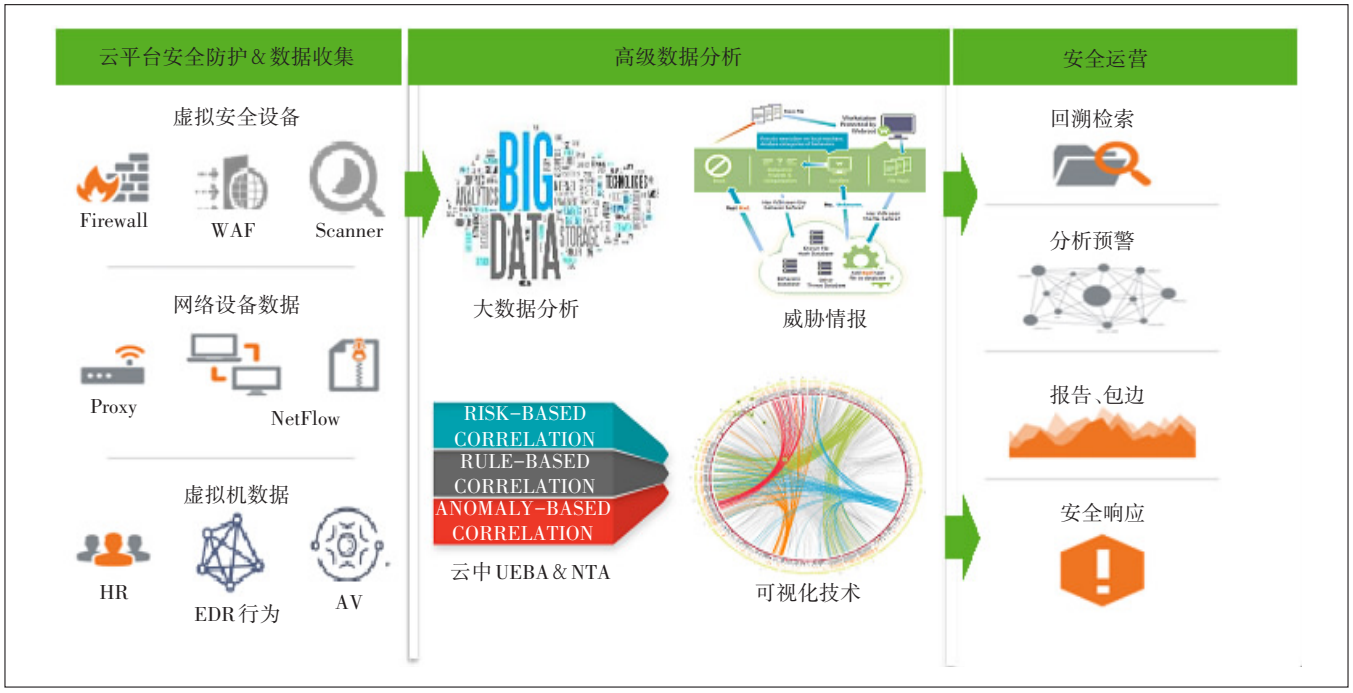

图1　云计算平台的安全防护示意图

a）云端代理，即通过反向代理设置数据流经过CASB云。在物联网场景中，安全厂商会构建一个面向物联网应用的安全云。

b）企业侧，即CASB网关。在物联网场景中，该网关会演变为边缘网关，但有处理物联网业务的能力。

c）云端API模式。用户在CASB云端和业务云平台设置订阅监控操作，当业务云端发生事件时，CASB云会收到回调通知，进行处理。在物联网场景中，要求物联网云平台提供开放的接口，向第三方安全平台提供事件订阅通知的功能。

总之，安全厂商可建立面向物联网应用的安全CASB机制，从业务角度分析物联网设备或物联网服务运行状态，找到潜在的异常和恶意攻击。

3.3 借助SDN/NFV构建管道侧快速响应能力

4G网络在核心网利用通用的x86服务器部署资源池，利用SDN/NFV技术实现按需的网络服务链，5G网络则更进一步，在接入网、汇聚网和骨干网均具备了SDN/NFV的资源池能力。安全作为业务的一部分，自然也能成为服务链中的一环。

当物联网的业务数据经过运营商网络时，运营商可根据业务特点和威胁态势，在最靠近业务层调用安全资源，进行防护。例如当运营商的态势感知系统发现某地大量的物联网僵尸主机连接C2时，则可动态向SDN网络设备下发阻断指令；当发现有僵尸网络针对某个目标发动DDoS攻击时，则可快速在近源侧准备好虚拟化清洗设备资源池，通过SDN控制器将流量调度到清洗资源池进行缓解。

可见，运营商可充分利用物联网设备和服务的威胁情报，构建针对物联网的知识库，利用SDN和NFV技术按需构建安全资源池，在此基础上针对多个物联网威胁或脆弱性场景提供安全增值服务，在管道侧实现全面的安全防护。

3.4 充分利用边缘计算提高安全服务质量

如前述所，运营商网络中可部署安全资源池，提供按需的安全服务；从物联网云服务商的角度看，也可以在云端侧部署相应的CASB安全机制。但考虑到安全检测机制的实时性和安全数据分析所花费的带宽资源，如果物联网服务商或运营商支持边缘计算，则可将上述安全机制一部分卸载（offload）到边缘侧，提高安全服务的质量（QoS）。

第3.3节提到运营商用靠近物联网设备侧的接入层安全资源池对DDoS流量进行清洗，就是一个典型的边缘侧提供的安全服务。此外，基于代理的物联网CASB服务在一些实时性要求较高的异常检测应用中，也需要在边缘侧部署一些偏分类功能的检测节点，当发现异常行为时实施阻断，而不需要考虑与CASB云服务的延迟开销或网络状态。

3.5 改进的认证方式和密码算法

借助新型基础设施和新的技术发展，很多实时性要求很高的物联网应用成为可能，例如智能交通中的协同驾驶、工业互联网下的业务控制。这些应用场景下必然会存在安全攻击，例如在V2V无线网络中，恶意攻击者伪造身份实施女巫攻击；在工业互联网中，攻击者伪造或重放控制指令，那么身份认证和通信加密就成为了物联网应用的必选项。

但在车联网场景下，高速运行的车辆通常交互时间不会超过数秒，在此间隔内完成身份认证、密钥交换、数据加密等操作，就要求在设计认证和密码算法时考虑到时延。

此外，在涉及到隐私的物联网场景下，密钥生成还需要考虑到匿名性、可管理的不可回溯性等属性。在弱终端的场景下，加密算法还需要考虑能耗和处理性能等问题。

总之，实现安全的物联网应用必须考虑认证和加密机制，设计或选择适合相应场景的认证和加密机制尤为重要。

3.6 设想的物联网安全架构

综上所述，在新型基础设施支撑下的物联网安全架构将是层次化、复合的体系。

在终端或边缘侧，应内置安全SDK或Agent，除了安全加固外，还可接收安全云端的安全处置指令。

此外，边缘侧应具备安全分析的部分能力，对流经的数据进行在线实时的分析识别；同时，具有根据云端指令按需准备虚拟化安全资源的能力。

在运营商骨干网侧，可利用SDN和NFV技术实现快速、按需和灵活的威胁感知、安全检测、应急响应的安全能力，提供定制化的安全服务。

在云端，安全厂商部署安全SaaS服务，在业务层面提供海量、细粒度的物联网业务安全分析和物联网威胁情报服务。物联网云服务商提供完备的云安全防护机制，应对针对应用平台的种种攻击。

图2给出了物联网安全架构，需要说明的是图2中只给出了主要功能组件的关系，要实现前述的物联网安全防护，还需关注2个核心控制应用：CASB云服务和边缘侧业务分析的整体检测机制；运营商整体的安全防护决策和调度应用，涵盖了骨干网和边缘侧的所有资源池管理。设计好这2类应用的架构，是构建灵活有效物联网安全体系的重要前提。

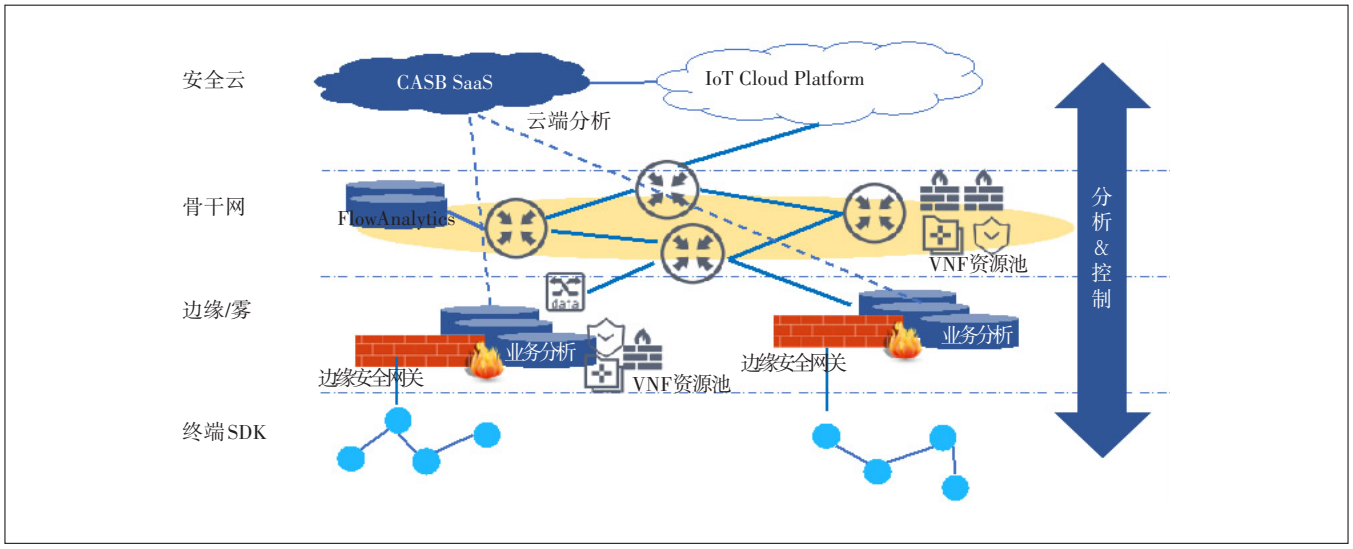

图2　物联网安全架构

参考文献：

[1] AWS IoT Service[EB/OL].[2019-01-22]. https://aws.amazon.com/iot/.

[2] 武传坤. 物联网安全关键技术与挑战[J]. 密码学报，2015(1)：40-53.

[3] 陈彦宇. 物联网安全威胁及应对策略探析[J]. 信息安全与技术，2017，8(4)：17-20.

作者简介：
刘文懋，绿盟科技创新中心总监，博士，主要研究方向为云计算安全以及物联网安全等领域；雷新，高级安全顾问，硕士，主要负责运营商领域安全解决方案。