5G数据安全防护白皮书

中国通信学会

2022 年 4 月

中国移动 China Mobile　CAICT 中国信通院　中国通信学会 CHINA INSTITUTE OF COMMUNICATIONS　HUAWEI

版权声明

专家组和撰写组名单

顾问(以姓氏笔划为序)：

陈兴蜀　四川大学网络空间安全学院院长

全国信息安全标准化技术委员会委员及大数据安全特别工作组副组长

撰写组(按单位排名)

单位	姓名
中国移动通信集团有限公司	袁捷、张峰、江为强、王光涛、邱勤、于乐、董航、李文琦、杨亭亭、张弘扬、马禹昇、张鑫月、徐思嘉、王国宇、徐天妮
中国信息通信研究院	张琳琳、庞妹、陈湉、刘明辉、静静、彭志艺、朱纯超、王腾
中国通信学会	张延川、欧阳武、张哲、完欣玥
华为技术有限公司	冯运波、李臣勋、赵宇龙、蒋刚林、罗伯强、陈小利、方亮
中国移动杭州研发中心	叶荣伟、康乾、卢骏
中移物联网有限公司	刘利军、柏洪涛、文远
北京亚鸿世纪科技发展有限公司	瞿宏锋、程治胜、易永波
中国移动通信集团广西有限公司	雷蕾、宁建创、黎峰、
中国移动通信集团浙江有限公司	徐良、胡鸥
中国移动通信集团广东有限公司	任若冰
咪咕文化科技有限公司	金科
北京优炫软件股份有限公司	程志新、黄志军
中国移动通信集团湖北有限公司	彭志文
中国移动通信集团山东有限公司	王海洋
卓望信息技术(北京)有限公司	郭中元
成都思维世纪科技有限责任公司	钟立
中国移动通信集团天津有限公司	刘飞
北京东方通网信科技有限公司	崔婷婷、周春楠、陈乔
中国移动通信集团湖南有限公司	李雁

前　言

5G 作为数字经济发展的重要驱动力，将促进数据要素的集聚和海量增长，5G 网络性能的提升将带来数据流动速度、范围和密集度的变化，5G 通过更广阔的覆盖和更稳定高效的网络连接，将促进多行业、多领域数据应用创新合作，加速垂直行业的数字化转型。5G 与医疗、交通、工业、教育、金融等行业深度融合，5G 数据范围、量级不断增长，数据高度分散化流动，可能带来具有各行业特点的新型数据安全风险，对数据安全防护提出新要求。2020 年 4 月 9 日，国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，首次将数据确定为新型生产要素；2021 年 6 月 11 日，《数据安全法》正式出台，数据安全工作首次提升至国家最高监管层级，意味着 5G 相关技术、业务需要更加谨慎处理数据并保证数据安全。总体看，我国 5G 数据安全治理尚处于初级阶段，亟需加快推进 5G 数据安全保障体系建设，促进 5G 产业和数字经济的健康发展。

为应对和解决 5G 数据安全风险挑战，中国移动通信集团有限公司联合中国信息通信研究院、中国通信学会、华为技术有限公司等各单位共同编制《5G 数据安全防护白皮书》，系统梳理国内外 5G 数据安全政策、动态，全面分析 5G 数据安全面临的风险，结合我国国情提出 5G 数据安全防护体系架构。期待为社会各方提升 5G 数据安全防护能力提供参考。

目 录

一、 5G 数据安全概述

（一）5G 为数据带来新特征

5G 带来数据量级、维度和内容的爆发式增长。5G 作为数字经济全面爆发的新引擎，将促进数据的集聚和海量增长，5G 对万物互联的支持带来传感器、机器臂、无人机、VR 眼镜等海量多种类终端接入，增加数据来源，极大丰富数据内容和数据维度。海量数据的汇聚和获取，将有助于新算法的落地和新技术的研发，促进数据智能处理技术的发展，进一步推动人类社会突破目前的认知瓶颈。

5G 带来数据流动速度和范围的变化。5G 网络性能的提升将极大提高数据流动速度，这对数据处理能力提出了新的要求。在增强移动宽带（enhanced mobile broadband，eMBB）场景下，超大数据流量对现有的数据处理能力带来巨大挑战；在超高可靠与低时延通信（ultra reliable low latency lommunication，uRLLC）以及大规模机器类型通信（massive machinetype communication，mMTC）场景下，工业企业内外网间、人车路间、个人与处理平台间交互频繁，数据流动的范围不断加大。

5G 带来数据应用跨行业、跨领域创新发展。5G 通过更广阔的覆盖和更稳定高效的网络连接，可与各垂直行业应用进行深度融合，数据在边缘侧分析处理需求爆发式增长，将促使各领域打破行业边界，有望突破数据应用垂直化的专业性发展瓶颈，促进多行业、多领域数据应用创新合作，加速垂直行业的数字化转型。

（二）5G 数据安全的研究目标

总的来看，5G 数据安全主要指在 5G 网络特性和融合应用场景下，保障数据全生命周期的安全与处理合规，具体研究目标包括：一是应对 5G 在网络建设、应用场景以及产业生态中面临的数据安全新风险、新挑战。二是促进 5G 数据安全防护体系的部署以及相关安全技术的应用，引导 5G 数据安全产业生态健康发展。三是在现有 5G 及数据安全相关工作的基础上，逐步构建适应我国 5G 发展阶段和基本国情的 5G 数据安全治理体系，形成 5G 数据安全保障能力。

二、 5G 数据安全面临的挑战与风险

（一）5G 数据安全挑战

1、新发展带来挑战

（1）全球博弈加剧

全球新一轮科技革命和产业变革加速发展，5G 作为新一代信息通信技术演进升级的重要方向，正在加快网络部署与应用实践。随着全球 5G 商用初具规模，5G 数据与军事、经济、政治安全加速融合，5G 数据正成为国际竞争的焦点。当前，欧美分别借助实施《通用数据保护条例》（GDPR）、《清澄境外数据的合法使用法案》（CLOUD 法案）等法规强化主体权责、实施长臂管辖，不断加大 5G 数据安全治理范围和力度；其他主要发达国家也已经逐步建立数据治理体系，陆续发布数据安全相关战略措施，以强化主体权责，应对全球数据安全博弈。

（2）安全外延扩展

近年来，各国家、各地区围绕数据安全陆续出台了相关政策、法律法规、标准，从制度层面高度重视数据的保护和利用。国务院发布的《关于构建更加完善的要素市场化配置体制机制的意见》，首次将数据确定为新型生产要素。当前5G数据安全早已打破传统机密性、完整性、可用性，除5G数据载体上的信息安全之外，延伸拓展到5G数据承载的个人权益、产业利益和国家利益的安全，以及通过5G数据安全保护促进数据合法有序开发利用等方面。因此，5G技术业务发展中需要更加谨慎地处理数据并保证数据安全。

（3）融合应用提速

5G融合应用需要运营商、垂直行业企业、第三方服务能力支撑、能力调用企业、应用二次开发服务商等多方参与。各参与方之间如果不能明确数据安全权责划分，将难以保障数据全生命周期安全。近期，工信部发布5G网络安全实施指南，对数据安全责任划分提供了指引，需要各环节加快落实。此外，5G融合应用涉及跨行业数据安全监管，除工业互联网等少数领域外，其它5G应用领域可依据的跨行业数据安全监管制度尚不完备。

2、新特性带来挑战

（1）5G数据量级的增长带来挑战

5G带来海量数据的汇聚，但由于现有安全防护能力还不成熟，数据安全传输、处理、存储的能力面临严峻挑战。同时，由于5G将提供至少十倍于4G的峰值速率，数据流量大幅增加，基于4G网络的数据加密、数据防泄漏等安全防护措施能否有效满足5G网络场景

下的数据安全需求，尚缺乏业务大规模商用的技术验证。

（2）5G 数据流动的变化带来挑战

数据流动与安全保护相互影响，尤其灵活高效的 5G 网络将带来更快、更密集的数据流，传统的通过加密、访问控制、隔离等技术手段保护存储系统的“保险柜”模式已无法满足数据流动安全防护的需求，数据安全保护重点将由原来静态的数据存储系统防护转变为动态的数据流动全生命周期风险管控，需要进一步构建以数据为中心的治理方案。

（3）5G 创新网络架构、应用模式带来挑战

5G 网络架构的升级、多种应用的创新部署带来的 5G 基础能力提升，将会使各行各业受益。其差异化服务能力将真正带来产业互联网的新浪潮，催生新服务、新业态和新模式，同时也对 5G 网络、技术和产品应用部署相关企业的数据安全防护能力提出了新要求。5G 与医疗、交通、工业、教育、金融等行业深度融合，根据其应用形式、应用领域的不同，将带来具有行业特点的数据安全新风险，企业已有的数据安全防护产品需要根据 5G 网络特性及数据流量进行升级换代。

（二）5G 数据安全风险

1、通用数据安全风险

一是 5G 数据采集方面，会涉及更广泛的 5G 终端、物联网终端设备及多接入边缘计算（multi-access edge computing，MEC）设备。这些设备存在管理域下沉、设备自身安全管控能力弱、设备暴露时间

窗口长等问题，在采集阶段面临着数据被非法采集、篡改、泄露等风险。

二是5G数据传输方面，和4G网络一样面临着接入侧含漫游接入的安全传输风险，同时需要关注5G网络MEC功能下沉导致核心网传输路径拉长以及服务化架构下网络功能间的数据传输的安全风险。5G网络具有数据传输量更大、数据传输涉及设备组件更多、传输路径协议更加丰富多样等特点，涉敏数据传输加密管控难度大，面临着数据被窃取、伪造、篡改以及数据传输中断的风险。

三是5G数据存储方面，主要涉及基站、接入和移动性管理功能等控制面网元的5G控制数据，存储在深度包检测（deep packet inspection，DPI）系统或其他应用系统的用户数据（经过处理后的数据），分布在网元/网管、切片管理系统中的管理数据等，若存储数据的设备/系统数据安全防护机制不到位，如敏感数据未加密存储等，存在敏感数据泄露、丢失等安全风险。

四是5G数据处理方面，5G在新技术架构下可以分为用户面数据、控制面数据、管理面数据处理，处理过程面临着鉴权机制不完善，访问权限范围控制不合理，数据处理过程中缺少监控机制，审计内容记录不全或缺失等风险。

五是5G数据共享方面，5G环境下数据归属域更加复杂，行业数据、通信数据相互交融，使得共享场景多样复杂。数据共享过程中面临着敏感数据泄露、共享保密措施不合规等风险。另外，为了更好地提供服务，5G网络支持网络能力开放，主要包括网络及用户信息

开放、业务及资源控制功能开放。网络能力开放带来好处的同时也引入了数据及隐私泄露等安全风险。

六是 5G 数据销毁方面，数据销毁不规范、数据销毁不彻底将带来数据被转移泄露、违规恢复等风险。特别是在软件定义网络（software defined network，SDN）架构下，5G 云环境、虚拟化环境中数据有效销毁的难度将大幅增加。

2、核心网数据安全风险

（1）NFV/SDN 数据安全风险

网络功能虚拟化（network functions virtualization，NFV）/SDN 技术由于解耦了设备的控制面和数据面，为基于多厂家通用 IT 硬件平台建立新型的设备信任关系创造了有利条件。与此同时，基于 SDN 集中控制架构下的入侵和攻击风险也愈发严峻。数据安全风险主要包括：

一是传统封闭管理模式下的安全边界和保障模式被打破，业务的开放性、用户的自定义和资源的可视化应用给云平台的安全可信带来前所未有的挑战，包括数据跨域泄漏、密钥和网络配置等关键信息缺少足够的硬件防护措施等问题。

二是计算、存储及网络资源共享化，会引入虚拟机安全、虚拟化软件安全、数据安全等问题，包括虚拟机逃逸、虚拟机流量安全监控困难、问题虚拟机通过镜像文件快速扩散、敏感数据在虚拟机中保护难度大等问题。

三是部署集中化，通用硬件漏洞被利用会导致攻击在集中部署区

域迅速传播，易导致大规模数据安全事件，造成较大社会或经济影响。

（2）网络切片数据安全风险

网络切片潜在的安全风险点集中体现在切片中共享的通用网络接口、管理接口、切片之间的接口、切片的选择与管理中。一旦非法攻击者通过接口访问业务功能服务器，滥用网络设备，非法获取包括用户标识在内的隐私数据，将给用户标识安全性、数据机密性与完整性带来危害。

用户标识安全方面，若直接使用真实的用户标识进行用户与用户或者用户与应用平台之间的通信，一旦系统的网络切片或切片之间的接口被非法程序访问，用户的标识、真实身份以及其它关联的隐私信息容易遭到泄露，甚至导致其通信活动与内容受到攻击者的非法窃听或拦截。

数据机密性方面，网络切片技术使得网络边界相对模糊，若网络切片管理域与存储敏感信息域没有实现隔离，一旦网络切片遭到攻击，切片中存储的敏感信息将会遭到泄露；

数据完整性方面，网络切片基于虚拟化技术，在共享的资源上实现逻辑隔离，若没有采取适当的安全隔离机制和措施，当某个低防护能力的网络切片受到攻击，攻击者可以之为跳板攻击其他切片，进而访问或破坏其数据。

（3）MEC 数据安全风险

MEC 在靠近无线接入侧增加边缘节点，使应用、服务和内容本地化、近距离、分布式部署，进一步减少业务时延，节省回传带宽。

边缘计算可满足垂直行业云化扩展现实、辅助驾驶等低时延要求类业务以及工业物联网厂内通信等高安全等级业务要求，同时也引入数据安全风险。

一是物理安全条件受限，数据面临被破坏、窃取的风险。MEC节点涉及大量的控制数据和用户数据，然而根据不同业务场景，MEC节点可部署在边缘数据中心、无人值守的站点机房，甚至靠近用户的现场，处于相对开放的环境中，相比在运营商核心机房部署的网络设备，MEC 节点设备更容易被入侵，导致 MEC 节点存储数据被破坏或窃取。

二是 MEC 敏感信息暴露面增加，数据泄露风险增加。MEC 定义了网络和第三方应用的双向 API 通信机制，可以把用户位置、无线网络负荷、无线资源利用率等网络信息通过 API 直接开放给第三方 APP，第三方 APP 也可直接运行在 MEC 节点上。MEC 节点成为新的数据暴露节点，若节点访问控制措施不严或被外部入侵，网络敏感数据存在被非授权访问等风险。

三是边缘计算数据隔离风险。在多个第三方边缘计算应用的托管、入驻的情况下，应用与应用、应用与网元，以及多用户应用下用户与应用间的隔离不当，可能导致用户访问权限越界、数据丢失和泄露等安全风险。

3、无线接入数据安全风险

无线接入数据安全风险包括针对以无线信号为载体对信息内容篡改、假冒、中间人转发和重放等形式的无线接入攻击等风险。

一是 3GPP 接入方面。无线环境中可能存在伪基站，这些伪基站可以干扰无线信号，令 5G 终端降级接入，连接到更加不安全的 2G、3G、4G 网络中从而盗取数据或发送伪造数据。此外，无线环境中广泛分布的安全性较低的物联网设备，在遭受攻击后，很可能会对基站和核心网发起分布式拒绝服务攻击（distributed denial of service attack，DDoS），造成大规模数据安全事件。

二是 NON-3GPP（如 WIFI、zigbee 等）接入方面。5G 所支持的 NON-3GPP 网络接入是未来异构网络融合的重要基础，但同时意味着接入大量、多种类的、未知的终端设备。由于设备种类的多样性带来的接入鉴权复杂性，以及设备移动或者频繁加入/退出网络，造成网络拓扑结构急剧变化，带来的数据安全问题异常复杂。

4、终端设备数据安全风险

一是硬件方面，5G 终端因设备资源受限，无法支撑较为复杂的安全策略，防护能力较弱。因为成本原因，很大一部分终端结构简单，安全能力薄弱，甚至不具备基本的身份校验、加密完整性保护等基础安全能力。

二是软件方面，5G 终端设备系统开源以及第三方软件引入的固有缺陷，使其要面临漏洞利用等传统系统攻击，导致数据存在被非法访问的风险。一些终端出厂以后从入网到报废整个周期始终没有操作系统补丁升级、软件升级的操作；针对开源的操作系统，容易被黑客利用系统本身存在的漏洞；此外，操作系统一些接口(Telnet、SSH、FTP 等) 没有默认关闭，也容易被攻击者利用进行非法数据操作。

三是安全策略方面，5G 应用场景下终端设备移动或者频繁加入/退出网络，造成网络拓扑结构急剧变化，缺少授权检测机制，安全问题异常复杂。很多恶意的终端设备试图接入网络对数据进行信息窃取、篡改以及破坏，这对移动通信网络的安全通信造成了很大威胁。同时，终端缺乏有效检测手段，对终端的安全态势进行评估和判断，造成终端设备存在各类安全问题，例如：终端设备往往采用简单文件传输协议同步数据，该协议容易被中间人攻击，导致会话中的通信数据被窃听，对数据的机密性构成威胁。

由于终端数量庞大，多数终端无人值守，一旦被攻击者非法控制，容易造成 DDoS 攻击、数据被非法窃取、伪造等风险。部分类型终端例如智慧家居由于与公众直接接触，一旦被攻破易直接造成公众的隐私泄露、财产损失等。

5、5G 业务数据安全风险

5G 技术的发展带来了丰富的应用场景，在极大地推动了千行百业发展的同时也带来了新的数据安全风险。从应用场景角度看，总体上存在以下数据安全风险：由于参与方较多导致数据安全权责划分困难；由于跨行业、跨地区、跨部门导致数据安全监管难度加大；由于 5G 技术架构复杂，融合行业众多且应用庞杂，导致数据保护困难。下面从 5G 三大应用场景角度分析相关数据安全风险。

（1）eMBB

eMBB 场景方面，由于 5G 数据速率较 4G 增长 10 倍以上，网络边缘数据流量大幅提升，数据安全防护往往需下沉前置到边缘进行。

5G 应用场景的下沉需求，涉及到例如用户面功能、MEC 等全新的节点/功能，这将给安全设备的接入、管控、处置流程引入新的风险。此外，eMBB 场景下还存在隐私数据管控风险，如增强现实/虚拟现实、高清视频直播、大视频等对带宽有极高要求的业务场景衍生的海量数据往往涉及个人隐私，需要专门的规章及标准进行严格管控与指导。

（2）uRLLC

uRLLC 场景方面，低时延需求造成复杂安全机制部署受限的困境。安全机制的部署，例如接入认证、数据传输安全保护、终端移动过程中切换基站、数据加解密等均会增加时延，过于复杂的安全机制不能满足低时延业务的要求。如在 5G 车联网应用场景下，为保证时延要求，应用场景往往采用简单的加密标准，但无法保证数据在传输过程中的机密性和完整性。如何平衡安全与传输效率仍是该场景亟待解决的问题；此外，在端到端的直连通信场景下，车联网终端间通过广播方式在专用频段上进行直通链路短距离信息交换，攻击者将可能利用直连通信无线接口的开放性，进行假冒身份、数据窃听等攻击行为，给用户带来经济损失甚至人身伤害。

（3）mMTC

mMTC 场景方面，在泛连接场景下的海量多样化终端易被攻击利用，对网络运行安全造成威胁。5G 时代将有海量物联网终端接入，其中大量功耗低、计算和存储资源有限的终端难以部署复杂的安全策略，一旦被攻击易形成僵尸网络，成为攻击源，进而引发对用户应用

和后台系统等的网络攻击，造成数据泄露、损毁。此外，不少终端设备负责采集、存储、传输位置、光电等关键数据，一旦因防护不当导致数据被非法劫持、获取，可能造成大规模个人隐私数据甚至国家重要数据泄漏事件。

三、 5G 数据安全发展动态

（一） 相关政策

1、国际

美欧 5G 安全战略侧重供应链安全，强调供应链安全对数据安全的基础性影响。美欧 5G 发展处于网络建设与应用探索的初期，对 5G 数据安全的关注聚焦于数据传输环节安全，以及信息系统与设施的数据存储安全。由此将保障网络通信安全、信息系统与设施的供应链安全作为重中之重。2020 年，美欧接连发布 5G 安全相关战略与政策文件，反复强调要保障 5G 基础设施和供应链安全，并将其作为数据安全的基础。特别是在近期美欧发布的指导本国或本地区强化 5G 基础设施安全的政策文件中，进一步强调了 5G 供应链安全对保障 5G 数据安全的重要性。例如，2020 年 8 月，美国国土安全部网络安全和基础设施安全局发布《5G 安全战略》，明确指出 5G 设备的不安全组件是影响传输数据与信息安全的重要因素，并提出将扩大对 5G 供应链风险的感知和推广安全措施作为其 5 大战略措施之一；2020 年 12 月，欧盟发布《5G 补充——欧盟电子通信规范安全措施指南》，其中，系统与设施安全作为 8 个重点领域之一，被视为保护数据安全的关键基础。

近年来，美欧陆续发布数据安全、5G 安全战略和法律政策，并持续完善 5G 安全治理措施，相关数据安全和 5G 安全策略均适用于 5G 数据安全保护。美国通过《美国国家安全战略》和《开放政府数据法》等一系列的国家战略、法律政策等对数据全生命周期安全做出了详细的规定。欧盟通过《非个人数据自由流动框架条例》和《欧盟数据战略》逐步建立起欧盟框架下的数据安全跨部门治理机制，为欧盟数据自由流动提供了安全保障。在 5G 数据安全保护方面，美国 2020 年发布《5G：不断发展的网络能力及挑战》，提出要对 5G 用户数据采取统一的保护措施；2020 年 12 月，美国国防部发布《5G 技术实施方案》，提出要关注和应对 5G 漏洞，进一步强化 5G 数据安全保护；欧盟 2020 年相继发布《5G 网络安全风险缓解措施工具箱》及后续进展报告，通过督促成员国完善 5G 网络功能、加强应急响应和跟进 5G 标准中安全措施的实施保障 5G 数据安全。

2、国内

《网络安全法》《民法典》《数据安全法》《个人信息保护法》等法律法规的出台为 5G 网络安全、数据安全以及个人信息保护提供了法律基础。中央网信办发布了《网络数据安全管理条例（征求意见稿）》《个人信息出境安全评估办法（征求意见稿）》《儿童个人信息网络保护规定》，中央网信办、工信部、公安部、市场监管总局联合制定了《常见类型移动互联网应用程序必要个人信息范围规定》《App 违法违规收集使用个人信息行为认定方法》，为 5G 应用发展中可能涉及到的个人敏感信息收集使用、广告精准推送、数据出境等

问题提供治理依据。公安部发布《网络安全等级保护条例》（等保2.0），为5G网络运营者数据安全保护提出要求。工信部出台《5G网络安全实施指南》，强化5G网络技术和应用数据安全保护，将5G网络安全保障要求和措施融入5G网络规划、建设、运行的各环节。

5G垂直行业应用涉及多部门监管职责，工信、医疗、交通、公安等多部门联合或在各自职责范围内制定5G融合应用数据安全保护规范。工信部发布《关于推动5G加快发展的通知》《“5G+工业互联网”512工程推进方案》《车联网（智能网联汽车）产业发展行动计划》，强化5G网络以及工业互联网、车联网等融合应用领域数据安全保护，落实各环节主体责任；工信部和卫健委联合发布《进一步加强远程医疗网络能力建设的通知》，提出加强5G远程医疗网络质量监测管理，保障医疗大数据资产全生命周期内合规和可信；交通运输部发布《推进综合交通运输大数据发展行动纲要(2020—2025年)》，提出推进5G在交通运输领域的应用，着力完善数据安全保障措施，保障国家关键数据安全。

（二）标准现状

1、国际

国际标准聚焦5G整体安全规范，侧重5G关键技术和垂直领域数据安全研究，但未专门为5G制定数据安全标准，数据安全通常作为5G安全标准中的权衡因素提出。第三代合作伙伴计划（3GPP）冻结的R15、R16标准中均包含数据机密性和完整性保护以及用户隐私保护等数据安全内容；全球移动通信系统协会（GSMA）携手3GPP

形成的网络设备安全保障计划（NESAS）机制中包含数据可用性和完整性保护以及认证和授权等数据安全测试内容。同时，各标准组织在5G关键技术数据安全标准方面开展一系列研究，国际电信联盟电信标准分局（ITU-T）、国际标准化组织（ISO）、欧洲电信标准化协会（ETSI）、电气与电子工程师协会（IEEE）等标准组织对边缘计算、网络功能虚拟化等技术提出了数据保护和隐私保护等方面的要求和建议。针对智慧城市、物联网、车联网等5G垂直应用领域，相关标准中已涉及隐私保护和分类分级等方面的数据安全要求。此外，数据生命周期安全管理、数据主体隐私保护、隐私保护能力评估等数据安全通用标准，也可为5G网络部署及业务应用中数据安全和个人信息保护工作提供参考。

2、国内

我国积极正制定5G数据安全专用标准，多数数据安全通用标准可适用于5G数据安全治理。全国信息安全标准化技术委员会（SAC/TC260）、全国通信标准化技术委员会（SAC/TC485）、中国通信标准化协会（CCSA）、IMT-2020（5G）推进组等标准组织积极推进5G数据安全标准化工作。工信部发布的《电信和互联网行业数据安全标准体系建设指南》明确提出建设5G数据安全标准体系。SAC/TC260发布的《5G网络安全标准化白皮书》提出了数据安全类标准需求及框架；CCSA推进了一批5G专用或相关基础类标准项目研制，已发布和在研的相关标准包括YD/T3813-2020《基础电信企业数据分类分级方法》《5G数据安全总体技术要求》《互联网新技术

新业务安全评估要求 基于5G场景的业务》《工业互联网数据安全分类分级指南》《物联网业务数据分类分级方法》《5G数据安全评估规范》等，其中数据安全类标准主要出自 CCSA TC8 数据安全工作组；此外，我国目前已发布的个人信息保护、全生命周期各环节等数据安全相关标准如GB/T 35273-2020《信息安全技术 个人信息安全规范》、GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》、YD/T 3628-2019《5G移动通信网安全技术要求》等适用于5G网络、技术和应用的数据安全保护。

（三）产业动态

1、国际

当前国家5G产业竞争与市场拓展重点向行业应用倾斜，数据安全关注度持续提升。5G市场蓬勃发展，竞争加剧，数据安全成为维护产业优势的切入点。美欧通过成立技术联盟、伙伴关系、数据协议签署等形式来保障本国在国际间的数据流通安全，如2020年北美、欧盟、日本等运营商合作建立“Open RAN”政策联盟，倡导有助于推动“Open RAN”技术发展的政府政策，希望通过软硬件解耦和接口开放化，打破传统电信设备软硬件一体化、接口高度集成化式架构，从而从供应链安全的角度提出保护数据安全的建议。欧盟于2020年11月发布《欧盟数据治理条例》针对基于数据的产品和服务的共享模式提出要求，这也将影响欧洲各国5G网络建设与部署。行业应用方面，面向5G欧洲市场的数据安全态势，德国在2020年12月修订《信息技术安全法》，旨在为德国通信技术供应商提出统一的安全标

准，为供应商 5G 网络建设与行业应用的数据安全监测提出建议。

2、国内

我国 5G 及数据安全均在发展过程中，数据安全相关产业对于 5G 数据安全保护供给不足。一方面，我国 5G 网络仍处于发展导入期，当前产业发展政策主要以网络建设、生态示范为重点，我国各省市区出台的 5G 政策文件包括发展规划、行动计划、实施方案、基站规划建设支持政策等，主要致力于推进 5G 网络建设、应用示范和产业发展。另一方面，国内数据安全技术产业发展方兴未艾，数据安全产品、解决方案、服务体系尚未成熟，存在数据安全保障基础薄弱、数据安全产品类型与解决方案单一等问题，针对 5G 应用的数据安全技术产品防护水平有待提升。此外，5G 产业联盟企业开放共享的同时，也面临保障数据安全后续投入的压力，包括相关基础设施部署、服务运营成本等。

四、 5G 数据安全防护体系参考架构

（一）参考架构

5G 数据安全技术防护体系从 5G 通用数据安全、5G 网络数据安全、5G 业务数据安全等多维度进行建设，适用于 5G 各种业务场景的数据安全防护。

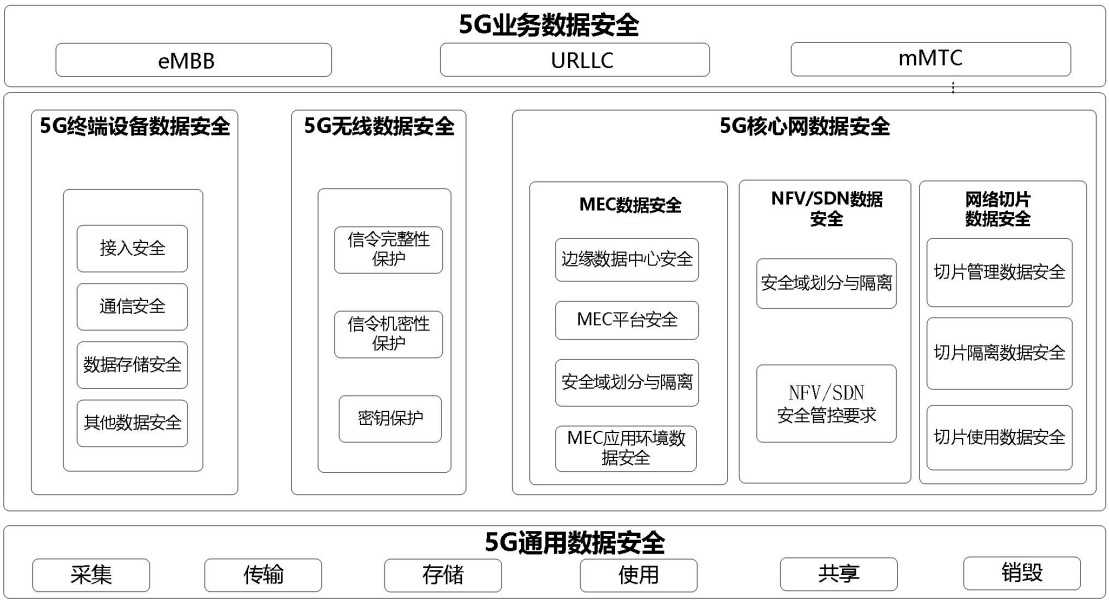

图 1　5G 数据安全防护体系架构

5G 数据安全防护体系架构包括:

✧5G 通用数据安全：数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据共享安全、数据销毁安全。

✧5G 基础设施安全：物理安全、云平台安全、网络安全。

✧终端设备数据安全：接入安全、通信安全、数据存储安全、其他数据安全。

✧无线数据安全：信令完整性保护、信令机密性保护、密钥保护。

✧核心网数据安全：MEC 数据安全、NFV/SDN 数据安全、网络切片数据安全。

✧5G 业务数据安全：车联网、工业互联网等 5G 垂直行业数据安全。

（二）5G 数据安全防护

为有效应对典型的 5G 数据安全风险，根据各行业及运营商实践

经验，给出相应的防护建议以供参考。

1、5G 通用数据安全

按照数据采集、数据传输、数据存储、数据处理、数据共享、数据销毁等各维度进行防护，同时对各个阶段的数据安全风险进行集中监测与预警处置。

（1）数据采集安全

在数据采集阶段，对人、设备、接口强化认证鉴权机制，同时加强人员管理，设备定期进行安全检查和漏洞修复。针对采集到的数据，根据相关标准要求做好分类分级，并采用适当的形式进行防护。针对敏感数据，根据相关规范进行数据内容加密。针对各采集通道做好流向控制和区域隔离，确保数据不出网的同时做到相互不干扰。采集缓存区域也应纳入安全管控范围，采集行为进行必要的详细日志记录以便进行监控、审计。

（2）数据传输安全

在数据传输阶段，可根据业务流程、职责界面等情况合理划分安全域，并在安全边界上配置相应的访问控制策略、部署安全措施。加强安全可靠性保障及分类分级管控，满足 5G 网络传输数据量大、传输路径协议丰富等新型场景下的安全问题。针对跨安全域传输，通常应对敏感信息的传输通道和数据内容进行加密保护和完整性校验，并对传输过程进行详细日志记录以便进行监控、审计。

（3）数据存储安全

在数据存储阶段，可根据数据涉敏级别，参考相应标准规范进行

差异化安全存储，差异化措施包括脱敏、加密、访问控制、备份要求、容灾要求等。对存储数据的设备及基础设施做好访问控制、安全基线、风险评估。针对多租户数据的共享存储需求，建立安全策略，提供多租户数据安全管控机制。

（4）数据处理安全

在数据处理阶段，坚持最小分配原则，使用者仅访问必要数据，除非获得授权，否则无权访问数据。此外，针对数据的高风险操作，建议由两人或以上授权人员共同完成，通过分权制约、互相监督确保涉敏数据安全性。针对接口调用数据的场景，做好接口鉴权和使用监控。对数据处理行为进行详细日志记录，以便进行监控、审计。对于数据处理方为外部单位的情况，可参考第（5）条“数据共享安全”。

（5）数据共享安全

在数据共享阶段，严格落实内部审批，通过保密协议等方式明确数据共享双方应承担的安全责任。对可接触敏感数据的员工，签订个人安全保密承诺书，明确安全责任。数据共享坚持最小分配原则，并根据相关规范对数据做相应保密处理。数据共享设备、接口做好鉴权管理、账号管理。共享使用过程进行详细日志记录，以便进行监控、审计。共享结束后及时关闭共享接口，使用方及时删除获取的共享数据。此外，建议数据提供方对数据处理方进行安全评估，确保数据处理方的安全防护水平不低于本方，有条件的，可定期检查数据处理方的安全防护水平。

（6）数据销毁安全

在数据销毁阶段，建立针对各种数据销毁场景下的数据销毁管理制度、办法和机制，涉及国家秘密的，需符合《涉及国家秘密的载体销毁与信息消除安全保密要求》；落实安全销毁措施，保证被销毁数据不可被还原（包括副本、备份），并做好效果验证；针对物理销毁操作做好存储介质的的安全管理，避免数据被违规留存、非法拷贝、还原；现场销毁场景建议安排内部工作人员进行现场监督，做好销毁过程操作记录，以便进行监控、审计。

2、5G 核心网数据安全

（1）NFV/SDN 数据安全

5G 基于 NFV 和 SDN 技术在云计算平台上构建网络，提升了网元功能和网络连接的灵活性、可编程性，为 5G 电信业务提供了资源可弹性伸缩、流量可全局调度的新型服务环境。NFV 引入了虚拟化管理层、虚拟机、容器、虚拟交换机及路由器、管理编排等功能，改变了 5G 数据的流转环境，同时引入大量 NFV 管理数据，拓展了 5G 数据安全保护的范畴。NFV/SDN 建议从以下四点做好数据安全防护：一是通过系统安全加固、安全隔离、安全管控等技术手段保障好虚拟化平台安全；二是通过数据加密存储、完整性校验、数据加密传输等技术手段保障数据传输和内容安全；三是由于云计算平台的运维特性，需在迁移或弹性扩缩过程中采用分布式杂凑算法等网络数据分布式存储的销毁策略与机制，实现对数据的有效销毁，确保数据不可恢复，防止滥用误用；四是做好各种操作的详细日志记录，以支持安全审计。

（2）网络切片数据安全

网络切片是建立在共享资源上的虚拟化端到端 5G 专用网络，承载了各类垂直行业业务。切片包含 5G 网络管理数据、控制数据、业务数据、切片管理数据。建议从以下两点做好数据安全防护：一是加强切片管理组件的身份认证、权限管控、数据访问控制等安全措施，防止数据非授权访问；二是做好切片安全隔离，对于安全要求高的行业实施物理隔离，采用专用服务器和网络设备部署切片网元，对于普通场景要做好切片与多切片共享网元间的网络隔离。此外，针对不同安全需求的业务和不同敏感级别的数据传输，网络切片选取各种切片隔离机制，包括 RAN 隔离、承载隔离和核心网隔离。其中 RAN 隔离重点针对无限频谱资源和基站处理资源；承载隔离则通过软隔离和硬隔离实现在时隙层面的物理隔离；核心网隔离实现网络切片间、功能间、用户间隔离。

（3）MEC 数据安全

根据不同敏感级别的数据，针对 MEC 部署差异化的安全策略，通过身份认证、安全隔离、第三方 APP 安全监管、细粒度授权、数据备份、数据加密和脱敏等技术手段实现数据安全防护及管控。在 MEC 运行时，需要针对 APP 上流转的数据进行分析，特别是使用者的 ID 和位置。特定业务包含的敏感数据可选用加密算法进行加密存储。对安全要求高的数据，建议采用安全传输层协议（transport layer security，TLS）/互联网安全协议（internet protocol security，IPSec）等加密传输的方法，防止通信过程中数据泄漏。在数据使用过程中，

应关注当地的数据安全要求，且建议针对具体的流转行为进行审计，特别地，当数据属于隐私数据时，可采用脱敏方式对数据进行处理。

3、5G 无线数据安全

对于 5G 终端无线接入过程中用户数据和信令数据的安全，可从信令完整性保护、信令机密性保护、密钥保护和抗重放保护等方面进行防护。基于密钥技术在 5G 终端与 5G 基站之间以及 5G 基站与业务管理功能之间进行数据传输加密保护，保障重要信息（用户数据、信令数据等）的机密性、完整性，并可抗重放攻击。对于无线接入侧的个人敏感信息及重要数据可运用加密算法进行传输加密，避免敏感数据泄露风险。

4、5G 终端设备数据安全

在终端接入环节，可通过认证和密钥协商机制完成设备的接入鉴权，提高终端接入过程的安全性。用户数据机密性、完整性保护能力及终端所能支持的最大数据速率依赖于终端能力，终端建立通信会话时，在能力范围内采用加密方式最大限度地保护数据的机密性和完整性，对于敏感数据，可运用祖冲之算法或 AES 算法等加密技术进行加密。针对终端数据存储，可通过数据加密和容器隔离等技术，运用加解密和完整性检测等手段进行数据安全防护，针对特定业务可设定加密存储区域，未经授权的任何实体不能从该区域的数据中还原出用户隐私数据的真实内容。此外，针对终端遗失及弃用等场景，建议提供可有效、彻底销毁数据的手段。

5、5G 业务数据安全

5G 业务数据安全主要包含通用数据安全和承载在 5G 网络上的垂直行业特定的数据安全两部分内容。5G 业务可明确自己的关键数据清单，针对关键数据清单，做针对性的数据安全防护；5G 垂直行业除参考 5G 通用数据安全要求外，还可参考特定行业的数据安全要求。部分 5G 垂直行业数据安全实践案例详见附录 A。

（1）eMBB 业务应用场景

在面向公众的 eMBB 业务场景下，建立业务流量数据内容监控与识别能力，在特定情况下可暂停违规或者涉及数据泄漏的 eMBB 业务。MEC 上部署第三方应用，需要进行软件、资源、系统和 API 接口的安全隔离及采取恰当的安全措施，保证应用之间的数据隔离；对集成第三方 APP 的合作方进行约束管理（认证和测试），避免第三方恶意 APP 带来的数据安全风险。

eMBB 业务应用场景安全要综合考虑终端与 eMBB 业务服务平台的认证以及传输安全，保障网元间的用户数据传输安全。在终端与 eMBB 业务服务平台之间采用二次认证和密钥管理机制，确保终端与业务平台身份的真实性及业务使用的合法性，同时，在两者之间协商并管理业务层密钥，对用户数据进行加密保护，防止攻击者窃听。对高安全要求业务场景，保证网元之间用户数据传输安全性，可通过物理隔离或加密手段确保 5G 用户面安全，如核心网与 eMBB 业务服务平台之间可使用数据专线建立安全的数据传输通道，保证用户业务数据传输安全性。

（2）uRLLC 业务应用场景

可从接入认证、数据传输、本地处理和移动切换过程进行优化，建立面向低时延需求的安全机制，统筹优化业务接入认证和数据加解密等环节带来的时延，尽可能在低时延条件下提升数据安全防护能力。

URLLC 业务应用场景要保证 5G 端到端传输路径在可控的时延范围内，就需要考虑降低以下过程中所产生的时延，包括身份认证、数据传输、安全上下文切换、网络节点的数据加密与解密等过程。针对身份认证的时延，可通过就近部署认证服务器、降低认证协议的复杂度、提高认证效率来降低；针对数据传输的时延，可通过优化安全算法以减少数据传输安全保护所带来的额外开销、对数据实施端到端的加密等来降低；针对 5G 终端在移动网络切换的时延，可通过采取异构多层接入网络的统一认证机制、把各网络节点间的安全上下文传送降低到最小程度等来降低；针对网络节点间数据加密与解密的时延，可通过使用轻便的加密算法，实现并行的加解密操作来降低。

（3）mMTC 业务应用场景

在 mMTC 场景中划分专有切片，并在相应切片上进行单独用户业务体验质量设置和安全配置，针对不同设备和数据敏感级别提供差异化安全传输能力，降低潜在的数据泄漏风险。

针对 5G 终端本地的关键数据，在采集、传输和存储等数据处理环节，采用数据加密等安全手段，防止数据泄露。考虑到网络负载能力有限，可以采用分布式身份管理和接入认证缩短认证链条实现快速

安全接入，降低认证开销，同时缓解核心网压力，规避信令风暴以及认证节点高度集中带来的瓶颈风险和单个网络节点被海量终端同时攻击的风险。针对海量连接特性，采用轻量级的安全算法、简单高效的安全协议来实现终端与网络间的双向认证和数据加解密，避免传统方案的沉重开销。

五、 发展建议与展望

（一）明晰5G数据安全与发展并重的防护思路

一是统一思想提高认识，坚持鼓励与规范并举的发展思路。贯彻落实党的十九届五中全会精神,统筹兼顾5G安全与发展。5G网络和应用发展仍处于建设推广期，党中央以及地方出台的相关政策文件以鼓励扶持应用创新为主，多数领域暂时还未形成可复用推广的行业应用模式。在此背景下，建议5G数据安全治理要采取包容审慎策略，持续推进5G网络建设、产业应用的同时，推进数据安全防护体系的完善，在发展中解决安全问题。

二是将数据安全贯穿网络规划建设和应用发展全过程。把握5G网络建设和应用发展导入期时间窗口，在网络部署和应用推进的同时，同步落实数据安全管理措施。结合信息通信行业5G和数据安全有关工作部署，建立健全5G数据资产分类分级、重要数据目录、权限管理、合作管理、安全评估等制度规范。强化5G行业应用数据安全保护，针对5G典型应用场景和数据特性，梳理形成数据资产清单，明确各方数据安全管理措施。

（二）完善5G数据安全法律法规和监管手段

一是《数据安全法》的出台标志着数据安全建设及监管工作进入有法可循、有法可依的新时代，但5G数据安全相关法规制度仍不完善。建议在5G网络安全实施指南的基础上，结合5G在不同领域应用中的特点，进一步完善跨行业跨领域数据安全规则，提出对所属领域的5G网络部署、应用产品等相关数据安全保护要求。

二是建立差异化的数据安全保护机制。依托网络数据安全合规性评估等有关工作机制，针对5G融合应用类型数据流转涉及的核心环节，督促数据相关方各自梳理和识别业务数据，明确涉及的数据类型、重要程度、流转路径以及责任归属，建立符合应用类型的数据安全保护机制，强化数据安全风险评估和问题处置。

三是开展5G融合应用数据安全检测认证。依托行业协会以及第三方机构，发动垂直行业应用方、运营商、第三方应用开发商以及科研机构等多方力量，围绕“5G+智慧城市”、“5G+工业互联网”、“5G+智慧能源”等典型应用领域和场景类型，共同研讨数据安全风险及应对策略，探索开展5G融合应用数据安全认证，逐步提高各应用领域数据安全的标准化、规范化水平。

（三）推进5G数据安全标准研制和技术攻关

一是加强5G数据安全国际标准体系布局。强化5G数据安全国际标准化相关工作，及时跟进国际标准组织工作动态，提前开展5G、6G等新技术数据安全研究，提升我国在5G国际标准化领域话语权。

二是推进5G融合应用数据安全标准研制。完善与垂直行业的合

作机制，结合医疗、交通、工业等行业数据安全保护各环节典型风险及各行业对数据分类分级的不同要求，共同推进 5G 融合应用安全标准化工作。

三是加强 5G 数据安全技术攻关。以重点项目和课题研究为牵引，鼓励企业加强漏洞挖掘、数据保护、入侵防御、跟踪溯源等数据安全技术研发，增强数据安全技术自主创新能力。通过建立人才培养基地、制定人才培养计划等方式，加强 5G 数据安全高端融合性人才储备与团队培育。

（四）加速 5G 数据安全生态共建和国际协同

一是打造 5G 数据安全产品供给支撑体系。加速培育数据安全相关技术产业，开展数据安全类产品与服务示范试点与推广，积极建立并参与开源社区，鼓励建立、资助、参与开源社区项目，推进通信行业与垂直行业间的数据共享与协同服务，通过投融资以及管理模式等机制创新，促进产学研对接与合作，缩短数据安全技术创新至商业化的发展周期，尽早发挥我国 5G 数据规模优势，加速形成数据安全产业生态。

二是在《全球数据安全倡议》的基础上，加强同东盟、二十国集团（G20）、金砖国家、亚太经合组织及一带一路等相关国家地区 5G 数据安全沟通交流，充分重视各方对 5G 数据安全问题的正当关切，秉承共商共建共享理念，协调更多有着相近立场主张的国家共同推进 5G 数据安全治理体系建设。

三是基于我国 5G 数据规模和发展优势，组织企业、高校、研究

机构等深入研究 5G 技术应用场景以及 5G 产业生态数据安全防护，开展数据安全和个人信息保护及相关规则、标准的国际交流合作，推动符合《联合国宪章》宗旨的个人信息保护规则国际互认，通过规则外溢效应，提升数据空间国际影响力。

附录 A 5G 融合应用数据安全实践

（一）5G+交通行业数据安全实践

1、背景

随着城市汽车保有量的不断增加，道路交通运营管理面临的压力与挑战日益增加，“治危”、“治堵”和“治乱”成为摆在交通管理部门面前的一道难题。5G+交通行业充分发挥 5G 网络高带宽、低时延的特点，融合 4K 视频+边缘计算+AI 等技术，有效提升交管部门对道路卡口车辆车型实时监控统计、车流转向统计的能力，为推进实现事故预防“减量控大”工作、实现事故数量和死亡人数“双下降”以及较大道路交通事故“零发生”的工作目标提供了强有力的支撑。5G+智慧交通行业场景的多样性以及网络的开放性，使用户隐私信息从封闭的平台转移到开放的平台上，接触状态从线下变成线上，5G 网络能力开放架构可能会面临网络能力的非授权访问和使用、用户和网络敏感数据泄露等安全风险。

2、数据安全解决方案

针对 5G+AI 智慧交通行业，梳理行业数据资产清单，完成数据分类分级，构建行业数据安全风险标准化评估模型，通过评估模型，发现行业潜在的数据安全风险；基于 DPI、大数据清洗分析、AI 风

险建模等技术，对采集到的交通流量数据内容进行自动化安全评估监测，动态发现数据安全风险。

（1）数据分类分级

交通行业数据包含公安交通管理数据、交通运输数据、城建数据、大型活动数据、诚信数据等业务系统数据，交通流量流据、车联网数据等维护管理数据，以及道路环境监测数据、机动车号牌监测数据、交通视频监控数据等运营监控数据。不同类别数据敏感级别差异大，对数据进行分类分级，形成数据资源清单，准确掌握数据的分布情况后，可为数据保护方案提供参考依据。

（2）数据安全风险评估

5G 数据安全风险评估模型以 5G 技术架构、5G 终端安全、通用安全管理、数据全生命周期、隐私保护等为核心评估点，从防止敏感数据信息泄露的角度出发，分析可能对数据安全造成影响的各类威胁和隐患。

由于 5G+AI 智慧交通业务中的数据包含了个人数据、生物特征、车辆信息等敏感信息，根据相关合规要求，对这些类型的数据有着严格的数据安全管控措施；从数据全生命周期的安全管理视角，重点对 5G 数据安全审计手段、审计独立性职能、数据共享安全等方面进行评估。

（3）自动化数据安全风险识别

针对 5G+AI 智慧交通业务所采用的边缘计算架构中网络功能虚拟化的边界资产，以资产指纹识别为核心，配合 MEC 下的虚拟服

务器的商业及开源软件，针对性开发攻击样例插件库；对 MEC 被划为不同的功能域，如管理域、核心网域、基础服务域、第三方应用域等，基于边缘分布式的特点，引入各种虚拟资产识别能力，通过构建基于聚类算法的无监督学习、多维建模及智能分析模型，对采集到的应用系统数据流量中的数据内容（用户轨迹、车牌、驾驶员信息）、数据传输信息（源/目标 IP 地址、接口等信息，即数据从流向）进行监控，对风险点进行预警，实现自动化识别监测能力和数据处理过程可视化。

（二）5G+智慧港口行业数据安全实践

1、背景

港口的作业效率和自动化水平是决定港口未来竞争力和经济效益的重要因素。5G 及 MEC 技术与港口深度融合，将对港口基础设施、运输组织模式、商业治理模式等产生深远影响。在此应用场景下，确保其高安全性和高可靠性至关重要。然而，5G 与港口 ICT 基础设施结合密切，甚至使得企业分布式内网通过运营商 5G 网络实现了互联互通，同时边缘计算技术也使得 5G 网络核心网网元下沉到港口侧，港口应用安全将对 5G 网络产生很大的影响。因此 5G 智慧港口应用场景不仅需要保障 5G 网络自身安全和边缘计算安全，还需为港口应用提供新型安全能力特别是数据安全防护能力。

2、数据安全解决方案

通过数据分类分级、5G 无线数据安全防护、5G 客户终端设备（customer premise equipment，CPE）接入终端数据安全防护、MEC

数据安全防护等维度保障港口数据安全。

（1）数据分类分级

港口行业数据包括运行状态数据、控制指令数据等设备数据，物流信息、船舶数据、码头资料、锚地资料、航道资料、码头平面图、生产调度管理信息等业务系统数据，以及身份信息、鉴权信息、日志信息、内容信息等用户个人数据。港口行业数据安全关系到生产商、服务提供商、用户个人等各方利益，特别地，敏感级别较高数据的安全性将极大影响港口运行安全及工作人员生命财产安全，因此，需针对港口数据进行分类分级，针对不同类别不同敏感级别的数据采取相应的防护措施。

（2）5G 无线数据安全防护

5G 无线数据安全主要是指 5G 终端 CPE 和 5G 基站之间无线接口(空中接口)的机密性和完整性。一是通过对空口数据（包括信令和用户数据）开启加密保护加密算法将明文数据转换为密文数据，保证数据不被泄露，并且支持 128 位加密算法。二是 5G 网络支持对信令消息和用户面数据提供完整性保护，5G 终端和 5G 基站通过完整性算法能够检测信令消息和用户面数据是否被篡改。

（3）5G CPE 接入终端数据安全防护

部署支持 IPsec 功能的路由器，结合部署在园区内网边界的智能防火墙（含安全网关），实现 CPE 与港口园区内部网络间的端到端加密。

（4）MEC 数据安全防护

从物理安全、平台安全、网络安全、运维管理安全等多方面加强数据安全保护。

✧物理安全：由于处于相对开放的环境中，MEC 设备更易遭受物理性破坏。评估和保障基础设施的物理安全，引入门禁、环境监控等安全措施，加强自身防盗、防破坏方面的结构设计，防止数据损毁。

✧平台安全：保障平台虚拟化带来的数据安全风险。引入可信计算技术，从系统启动到上层应用，逐级验证，构建可信的 MEC 平台，防止 MEC 平台的软件被篡改；通过虚拟机隔离提升虚拟化安全，对于部署在 MEC 的虚拟机（virtual machine，VM），通过微分段等技术，对 VM 和不同应用实施严格隔离；另外，通过实时监测 VM 的运行情况，有效发掘恶意 VM 行为，避免恶意 VM 迁移对 MEC 造成感染。

✧网络安全：MEC 连接了多个外部网络，在港口 MEC 中，使用传统的边界防御、内外部认证、隔离与加密等防护技术，对 MEC 接口数据安全进行防护。

✧运维管理安全增强：为了确保 MEC 节点中资产与数据的安全，对使用 MEC 的各方的行为执行认证、授权、审计。此外，在平台层面、网络层面、业务层面等多个维度，对数据资产的所有权、使用权和运维权进行分权分域的管理。当 MEC 与核心域之间涉及到管理、计费等关键性通讯时，充分利用 PKI 以及 TLS/IPsec 等协议，实施认证授权与传输加密。

（5）切片接入安全

网络切片选择辅助信息（network slice selection assistance information，NSSAI）可以区分不同类型、不同用途的切片。在园区终端初始接入网络时，NSSAI 指示基站及核心网网元将其路由到正确的切片网元。切片选择辅助信息对于港口属于敏感数据，5G 网络可对 NSSAI 进行保护。

（6）切片隔离安全

5G 智慧港口针对切片建立了三级立体化安全隔离体系，如图 2 所示。

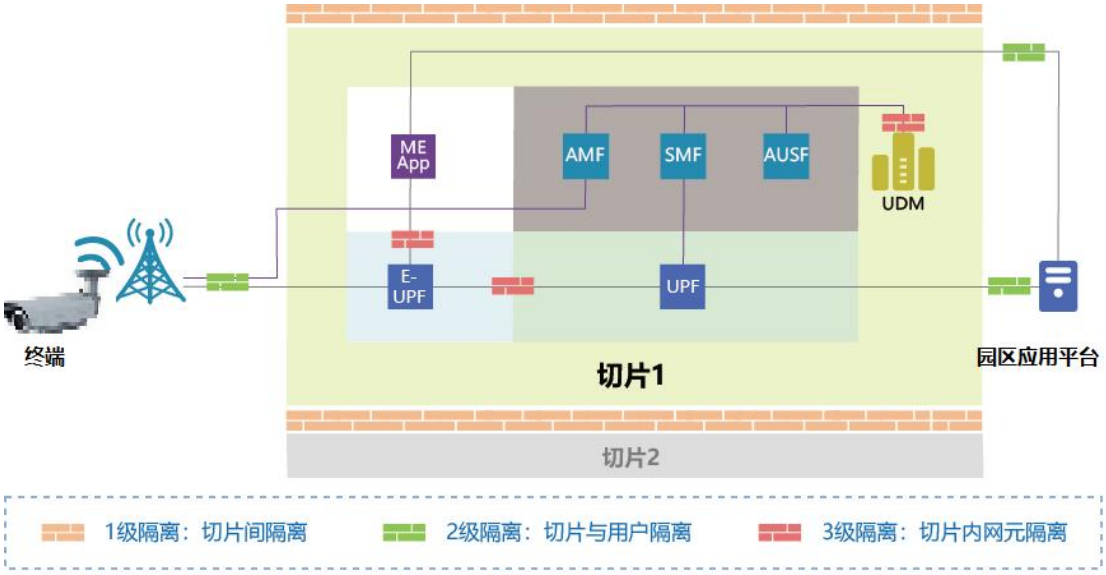

图 2 网络切片的三级立体化隔离体系示意

切片隔离体系包括：

✧切片间隔离：依据园区业务类资产和数据资产的重要性，进行切片间的有效隔离，保障每个切片具有对应安全级别；

✧切片网络与用户隔离：为保障 5G 网络切片的安全、高可靠运

行，在切片网络设计时，在最终用户侧、园区应用侧设置隔离机制，再按照服务级别协议向不同应用提供高可靠切片服务，保证切片网络自身安全边界清晰，确保切片网络自身的安全可控；

✧切片内网元间隔离：在切片网内划分出安全域，提供网元间安全隔离；

上述的三级立体化安全隔离体系中，每个层级的隔离实施方案均可从网元、网络、数据三个层面实施，使用成熟的虚拟化隔离方案，借助 NFV、SDN 等技术，与虚拟机编排、切片编排功能协同，实现精准、灵活的切片隔离。

（7）数据传输安全

✧ 传输隔离：将智慧港口园区网络与其他普通公网划分为不同的虚拟局域网/虚拟专用网络（virtual private network，VPN），使得无法路由通信，即非智慧港口授权的设备无法访问企业私有网络及授权设备及其数据。

✧ 传输安全：借助 5G 技术自身已具备的空口数据机密性和完整性保护能力，保障从行业终端到基站的空口安全。从行业终端到 5G 控制面核心网、从基站到 MEC、从 MEC 到企业，全面保障整个园区的数据传输安全。

✧ 端到端数据安全:企业网络也可建立从终端到企业私有网络的 VPN 传输隧道确保应用层的行业数据安全。

（三）5G+智能制造行业数据安全实践

1、背景

5G+智能制造将新一代信息技术与先进制造技术深度融合，贯穿设计、生产、管理、服务等制造活动各个环节，具有自感知、自决策、自执行、自适应、自学习等特征，旨在提高制造业质量、效益和核心竞争力。随着 5G 技术的发展，为了满足数据传输高可靠低时延、增强移动宽带、海量机器类型通信等需求，各类行业应用逐渐被迁移到 5G 边缘云上，这些应用共享相关资源和数据共享接口，一旦某个应用被攻击，将会影响其他应用的安全运行，造成数据泄露甚至服务中断；同时 5G 网络能力开放将用户个人信息、网络数据和业务数据等从内部的封闭平台开放出来，网络运营商对数据的管理控制能力减弱，加大数据泄露的风险。

2、数据安全解决方案

为解决 5G 边缘云数据安全风险，针对业务的敏感数据分类分级管理、业务数据风险智能发现、风险态势与预警三大应用场景提出解决方案。

（1）数据分类分级

针对边缘云上的各种应用进行敏感数据识别和梳理，智能化分类分级，形成数据资源清单，准确掌握数据的分布情况，为数据保护方案提供参考。数据分类分级参考《工业数据分类分级指南（试行）》，结合智慧工厂研发设计、生产制造、运维、管理等环节，对数据进行分类识别并形成数据分类清单，数据类型包括研发设计数据、开发测

试数据等研发域数据，控制信息、工况状态、工艺参数、系统日志、监控视频、监控图像等生产域数据，物流数据、产品售后服务数据等运维域数据，系统设备资产信息、产品供应链数据、业务统计数据等管理域数据及与外部单位进行交换、共享、交易等外部域数据。

（2）数据安全风险智能发现

针对边缘云的业务应用，采集和分析 HTTP、HTTPS、FTP、SMTP 等协议的流量，针对加密流量采用非监督学习和监督学习结合的方式，从网络流量特征、协议、流量大小、业务时间、业务操作行为等多维度建立合规基线模型，然后实时对比、分析从而发现数据安全风险事件；针对非加密协议可对操作数据内容、传输文件内容进行还原，利用大数据分析、机器学习等技术建立用户画像、业务画像、数据安全合规基线等，实现批量传输敏感数据、数据跨境传输、接口异常访问敏感数据、接口未授权等安全场景的实时监测与风险事件溯源分析，确保 5G 边缘云上智能制造行业的应用与数据安全。

（3）数据安全态势可视化

平台通过多重维度进行数据的可视化展示。针对数据安全风险事件，展示访问用户、风险类型、风险级别、发生时间、关联业务等；结合历史风险数据、业务数据，进行数据关联分析，实现风险事件的趋势预测。

（四）5G+医疗行业数据安全实践

1、背景

5G 医疗是 5G 技术在医疗健康行业的一个重要应用领域。随着

5G 正式商用以及与大数据、互联网+、人工智能、区块链等前沿技术的充分整合和运用，5G 医疗行业越来越呈现出强大的影响力和生命力，对推进深化医药卫生体制改革、推动医疗健康产业发展，起到重要的支撑作用。

当前，我国 5G 医疗发展尚处于起步阶段，在顶层架构、系统设计和落地模式上还需要不断完善，但 5G 医疗前期探索已取得良好应用，实现了 5G 在医疗领域包括远程会诊、远程超声、远程手术、应急救援、远程示教、远程监护、智慧导诊、移动医护、智慧院区管理、AI 辅助诊断等场景的广泛应用。5G 医疗场景涉及海量、多样的医疗终端，在医疗系统与系统之间、系统与检测设备之间，存在大量的医疗数据和用户个人数据的传输交换、分析需求，给 5G 医疗行业数据安全带来新的挑战和安全需求。

2、数据安全解决方案

由于医疗数据多涉及患者隐私方面的问题，在数据存储和使用方面具有更严格的要求与限制。为有效防范数据安全风险，参考《中华人民共和国数据安全法》《GB/T 3925-2020 信息安全技术 健康医疗数据安全指南》，通过数据分类分级、网络切片安全防护、MEC 边缘计算安全防护和 5G 医疗专网大数据安全防护等方面来保障 5G 医疗行业平台数据安全。

（1）医疗数据分类分级

医疗行业数据包括自然人身份标识、网络身份标识、患者基本资料、实体身份证明、患者私密资料、用户密码及关联信息等患者身份

相关数据，患者分诊建档/等级信息、患者体征数据采集信息、患者病情等级数据等患者服务内容数据，仪器服务数据、服务记录和日志、服务设备资料等患者服务衍生数据，以及项目管理数据、急诊科统计指标、急诊科统计信息等医院系统管理数据。不同类别数据敏感级别不同，需对数据进行分类分级，针对不同类别不同敏感级别的数据采取有针对性的安全防护措施。

（2）切片安全防护

5G 网络切片支持在统一基础设施平台上提供逻辑隔离、定制化的专用网络，并提供完备的安全机制与功能。5G 应用平台提供切片选择辅助信息 NSSAI 区分不同类型、不同用途。在内网终端初始接入网络时，NSSAI 指示基站及核心网网元将其路由到正确的切片网元，从而对 NSSAI 进行隐私保护。

（3）MEC 安全防护

采用入驻方式部署的 MEC 是医疗业务处理的核心，它由 MEC 边缘计算平台、MEC 编排系统、移动边缘应用（ME APP）等部分构成。各部分的安全漏洞都可能被利用发起攻击。MEC 边缘计算节点在部署时支持如下安全机制与能力，保障 MEC 系统的数据安全。

✧NFV 系统安全：包括网络功能虚拟化基础设施解决方案、业务通信系统和管理系统的安全方案。MEC 上同步部署 VM，并通过微分段等技术对 VM 和不同应用实施严格隔离。

✧MEC 平台安全：通过实时监测 VM 的运行情况，有效发掘恶意 VM 行为，避免恶意 VM 迁移对 MEC 造成感染；对敏感

数据进行加密和完整性保护，防止 MEC 边缘计算平台存储的敏感数据被泄露；对 ME App 进行身份认证、授权访问，防止非法访问、数据泄露及拒绝服务攻击；使用传统的边界防御、内部分域、内部认证、隔离与加密等防护技术实现隔离和访问控制。

✧MEC 编排管理系统的安全：对管理系统的网元进行安全加固，对管理系统内部接口和管理系统与外部其它系统之间的接口上的数据进行加密、完整性和防重放保护。

✧ME App 安全：对 ME App 软件进行安全加固、使用 HMAC 等机制对 ME App 软件或者镜像进行完整性保护、对敏感数据加密存储和完整性保护，对访问 ME App 的用户进行认证等，从而防止 ME App 软件本身的漏洞被利用、ME App 软件或者镜像被篡改、敏感数据泄露，用户非法访问 App 等。

（4）5G 医疗专网大数据安全防护

根据《中华人民共和国网络安全法》和网络安全等级保护制度 2.0 标准，需要从数据收集、数据传输、数据存储和数据处理等方面对医疗数据进行相应的安全管理。数据安全管理具体场景如图 3 所示。

图 3 5G 智慧医疗数据安全管理具体场景

5G 网络中隐私保护所采用的主要技术措施有：

✧数据加密技术：数据加密是 5G 网络中保证数据隐私安全的最有效手段之一，也是隐私保护过程中采用的最常见技术手段之一。按照实现思路，可以将其划分为静态加密技术和动态加密技术。从实现的层次上，可以分为存储加密、链路层加密、网络层加密、传输层加密等。采用加密技术可以有效保证 5G 网络隐私数据的机密性、完整性和可用性。

✧基于限制发布的隐私保护技术：在 5G 网络数据发布过程中，限制发布技术即是有选择地发布原始数据、不发布或者发布精度较低的敏感数据,以实现隐私保护。当前此类技术的研究集中于数据匿名化:即在隐私披露风险和数据精度间进行折中,有选择地发布敏感数据及可能披露敏感数据的信息,但保证对敏感数据及隐私的披露风险在可容忍范围内。

✧访问控制技术：访问控制技术也是 5G 网络隐私保护采用的最

常用技术手段之一。访问控制可以通过策略和技术手段保证隐私数据不被非法使用和窃取。传统的访问控制技术包括用户口令、数字证书、USB KEY、生物识别技术等。这些技术同样可以应用到 5G 网络之中。

✧ 虚拟存储和传输保护技术：为保证隐私信息在 5G 虚拟化网络存储过程中的隐私安全，可采用用户数据库的动态迁移和随机化存储技术。动态迁移技术可以在保证虚拟机上服务正常运行的同时，将一个虚拟机的数据从一个物理主机迁移到另一个物理主机。这使得攻击者即使成功入侵用户数据库也无法锁定要窃取的用户数据。

（五）5G+采矿行业数据安全实践

1、背景

5G 智慧铜矿项目是探索利用 5G 技术实现矿山设备智能管控，满足矿山管控系统对高带宽及低时延要求，实现控制精度达到厘米级的无人驾驶矿用大车、远程遥控推土机的真实作业场景实践。

5G+智慧矿山体系架构的改变和新技术的应用，改变了传统业务流程和价值链，使得矿山安全防护的重心转移，行业的安全防护手段亟需改进。

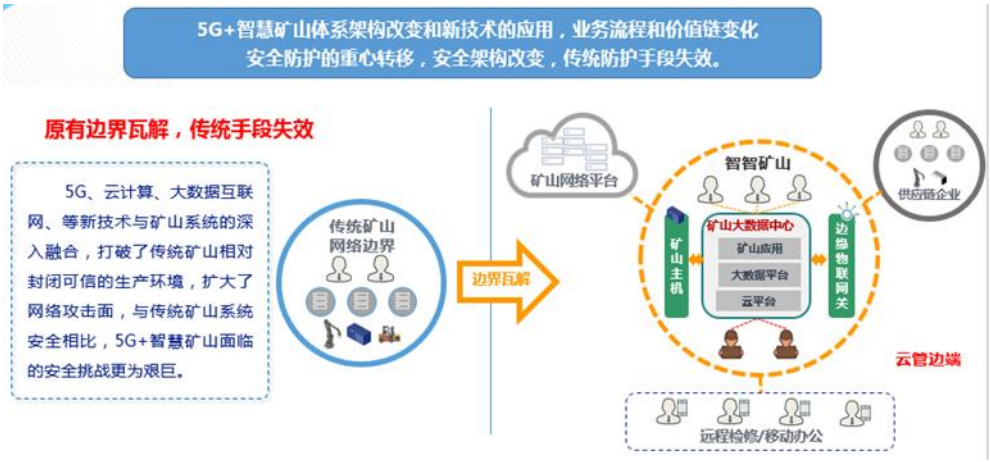

图 4 5G+智慧铜矿安全防护体系演变图

5G 智慧铜矿提高了铜矿的生产效率、降低了设备故障率、节约了人工成本。但随着铜矿企业的信息化，由于缺少统一监管平台，信息孤岛和安全防护矛盾突出，通用能力存在缺陷等问题，也使相关系统面临越来越多的外部安全威胁，智慧铜矿对 5G 智慧园区数据安全解决方案需求迫切。

2、数据安全解决方案

监测生产内网部署区、5G 边缘采集节点等重点节点安全设备数据，结合 5G 智慧铜矿安全防护平台，开展 5G+智慧矿山数据安全风险监测和数据安全事件追踪核查，实现 5G 终端识别和特征协议分析，管理 5G+终端和数据资产，及时发现 5G+智慧网络潜在的数据泄露风险和系统漏洞隐患，并溯源泄露源和数据最终流向，全方位进行数据安全管理态势分析。

（1）数据分类分级

结合行业的生产制造模式对该行业的工业数据进行梳理和分类分级，为数据安全防护提供依据。采矿行业数据包括运行状态数据、控制指令数据等设备数据，矿区传感感知数据、矿区工业自动化数据、

生产计划与执行管理数据等生产运营收据；经营管理数据、综合调度指挥数据等管理数据；标准文件数据、计算模型数据、环境数据等知识模型库数据；以及身份信息、鉴权信息、日志信息、内容信息等用户个人数据。

（2）生产内网部署区

铜矿生产内网部署区部署防火墙、堡垒机、网闸等安全设备，补充 VPN、入侵检测、抗 DDoS、安全审计、安全管理等功能，实现铜矿生产内网的入侵防御。矿区监管平台可主动探测、汇聚日志信息、核心交换机镜像的生产网和办公网流量等，形成安全防护事件报告，经 VPN 或专线传送给 5G 智慧铜矿安全防护平台。

（3）5G 边缘采集节点

铜矿 5G 边缘采集节点部署边缘安全监测设备，负责采集 MEC 边缘网关卸载用户面流量和移动边缘平台/移动边缘平台管理器关于 5G 应用 APP 管理的日志信息。边缘安全监测设备分析流量，形成安全事件报告，通过 VPN 或专线传送给 5G 智慧铜矿安全防护平台。

（4）5G 智慧铜矿安全防护平台

针对智慧铜矿应用场景建设 5G 智慧铜矿安全防护平台，平台部署在核心网机房，系统由采集集群、分析平台等组成，负责接收铜矿生产内网和 5G 边缘采集节点上报的数据，实现 5G 智慧铜矿安全防护平台整体应用功能分析呈现。

利用平台对矿区网络侧和企业侧网络流量数据的探测扫描能力，全面盘点矿山企业在线资产，梳理监测应用层接口和业务访问地址，

实现帐号访问行为审计监测和轨迹识别，分析风险业务系统敏感数据调用情况和数据跨境风险；依托平台网络数据安全威胁监测与处置机制，全面评估智慧矿山安全风险，针对存在风险及时预警、整改，有效提升 5G 智慧矿山网络数据安全态势感知和应急响应能力。

中国通信学会

地址：北京市海淀区万寿路 27 号院 8 号楼

邮政编码：100840

联系电话：010-68203021

传真：010-68203004

网址：https://www.china-cic.cn/