国际电信联盟
电信标准化部门

建议书

ITU-T X.1815 (03/2023)

X系列：数据网、开放系统通信和安全性

IMT-2020安全

IMT-2020边缘计算服务的安全指南和要求

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
万维网安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1399
分布式账簿技术（DLT）安全	X.1400–X.1429
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	**X.1800–X.1819**

ITU-T X.1815建议书

IMT-2020边缘计算服务的安全指南和要求

摘要

IMT-2020网络将在网络和计算资源的基础设施上实现各种服务，其中包括增强型移动宽带（eMBB）服务、基于海量机器类型通信（mMTC）的服务和基于超可靠低延迟通信（URLLC）的服务。根据为IMT-2020网络确定的关键特征和要求，它需要更加高效、个性化、智能化、可靠和灵活。

为了支持IMT-2020网络中的典型服务，尤其是eMBB服务和基于URLLC的服务，边缘计算被认为是满足IMT-2020网络的苛刻关键性能指标（KPI）的关键技术之一，尤其是就低延迟和带宽效率而言。

边缘计算使运营商和第三方服务提供商能够在靠近用户接入点的地方部署服务，从而通过减少传输网络上的端到端延迟和负载来实现高效的服务交付。

为了保证边缘计算服务部署和应用的安全性，需要分析边缘计算服务的安全威胁和相关安全需求，建立整体安全框架。

本建议书草案旨在分析边缘计算服务的部署方案和典型应用场景，规定了IMT-2020中针对边缘计算服务的安全威胁和要求，从而为运营商保护其应用建立了安全能力。

历史沿革

版本	建议书	批准	研究组	唯一识别码*
1.0	ITU-T X.1815	2023-03-03	17	11.1002/1000/15113

关键词

边缘计算服务、IMT-2020网络、安全指南

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联未收到实施本建议书可能需要的受专利/软件版权保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列ITU-T网站查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1815建议书

IMT-2020边缘计算服务的安全指南和要求

1 范围

本建议书提供了边缘计算服务的潜在部署方案和典型应用场景，规定了 IMT-2020 中针对边缘计算服务的安全威胁和要求，从而为运营商提供了保护其应用的安全功能指南。

2 参引

下列 ITU-T 建议书和其他参引的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参引均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和其他参引的最新版本。当前有效的 ITU-T 建议书清单定期出版。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[ITU-T Y.3101] ITU-T Y.3101建议书（2018年），IMT-2020网络要求。

[3GPP TS 23.501] 3GPP TS 23.50（2022年），5G；5G系统（5GS）的系统架构（第17版的版本17.4.0）。

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 IMT-2020 [b-ITU-T Y.3100]：（基于[b-ITU-R M.2083]）提供比[b-ITU-R M.1645]所述更多增强功能的系统、系统组件和相关技术。

3.1.2 木马 [b-ITU-T E.800]：一种貌似良性甚至有用的软件，掩盖了软件意图破坏系统或盗取信息的真正目的。

3.2 本建议书定义的术语

本建议书定义了如下术语：

3.2.1 IMT-2020 边缘计算服务：通过 IMT-2020 系统提供的一种服务，它使服务能够在用户设备的接入点附近托管，以便通过减少传输网络上的端到端延迟和负载来实现高效的服务交付。

3.2.2 IMT-2020 系统：由 IMT-2020 接入网（AN）、IMT-2020 核心网和用户设备（UE）组成的 3GPP 系统。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

AF 应用功能

AMF 接入和移动性管理功能

AN 接入网

CDN	内容分发网络
EASDF	边缘应用服务器发现功能
DDoS	分布式拒绝服务
DC	数据中心
DN	数据网络
DNN	数据网络名称
DNS	域名系统
eMBB	增强型移动宽带
EHE	边缘托管环境
GW-C	网关-控制平面
GW-U	网关-用户平面
IMS	互联网协议多媒体子系统
IP	互联网协议
KPI	关键性能指标
MEC	移动边缘计算
mMTC	海量机器类型通信
NAT	网络地址转换
NEF	网络披露功能
NB IoT	窄带物联网
NFVO	网络功能虚拟化编排器
NRF	网络存储功能
VNFM	虚拟化网络功能管理器
OSS	运营支持系统
PDU	协议数据单元
PSA	协议数据单元会话锚
QoS	服务质量
RAN	无线接入网
SBA	基于业务的架构
SIM	用户识别模块
SMF	会话管理功能
TLS	传输层安全性
UE	用户设备
UPF	用户平面功能
URLLC	超可靠低延迟通信
V2X	车联网

5 惯例

在本建议书中：

关键词“**要求**”表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

关键词“**应该**”表明一项建议的、并非需要绝对遵守的要求，因此声称遵守本建议书并不需要按照该要求行事。

6 IMT-2020边缘计算概述

IMT-2020 网络将在网络和计算资源的基础设施上实现各种服务，其中包括增强型移动宽带（eMBB）服务、基于海量机器类型通信（mMTC）的服务和基于超可靠低延迟通信（URLLC）的服务[ITU-T Y.3101]。根据 IMT-2020 网络中确定的关键特性和要求，它需要成为一个更加高效、个性化、智能、可靠和灵活的网络。

为了支持 IMT-2020 网络中的典型服务，尤其是 eMBB 服务和基于 URLLC 的服务，边缘计算被认为是满足 IMT-2020 网络的苛刻关键性能指标（KPI）的关键技术之一，尤其是就低延迟和带宽效率而言。

IMT-2020 边缘计算使运营商和第三方服务提供商能够通过 IMT-2020 系统在靠近用户接入点的地方部署服务，从而通过降低端到端延迟和传输网络负载来实现高效的服务交付。

6.1 部署方案

3GPP 在 IMT-2020 系统中规定的 IMT-2020 系统架构有两个可用选项，一个是传统的参考点和接口方法，另一个是核心网络功能使用基于服务的架构（SBA）彼此交互。

图 6-1 描述了基于[3GPP TS 23.501]的 IMT-2020 系统架构。

从运营商的角度来看，采用 SBA 的 IMT-2020 边缘计算服务的部署方案可能包括以下 IMT-2020 网络功能：

– UPF（用户平面功能）：UPF是IMT-2020核心网络的网络功能（NF）之一。在IMT-2020架构中，它负责数据包路由和转发、数据包检查、服务质量（QoS）处理以及互连数据网络（DN）的外部协议数据单元（PDU）会话。

– AMF（接入和移动性管理功能）：AMF通过N1接收来自用户设备（UE）的所有连接和会话相关信息，并通过N2接口（见图1）接收来自（无线）接入网（AN）的所有连接和会话相关信息，但仅负责处理连接和移动性管理任务。

– SMF（会话管理功能）：SMF是IMT-2020 SBA的基本元素。它主要负责与分离的数据平面交互，创建、更新和删除PDU会话，以及管理与UPF的会话上下文。

– EASDF（边缘应用服务器发现功能）：EASDF包括一个或多个以下功能：向网络存储功能（NRF）注册用于EASDF发现和选择，以及根据来自SMF的指令处理DNS消息。EASDF具有通过N6接口与PDU会话锚（PSA）UPF的直接用户平面连接（即，没有任何网络地址转换（NAT）），用于传输与UE交换的域名系统（DNS）信令。

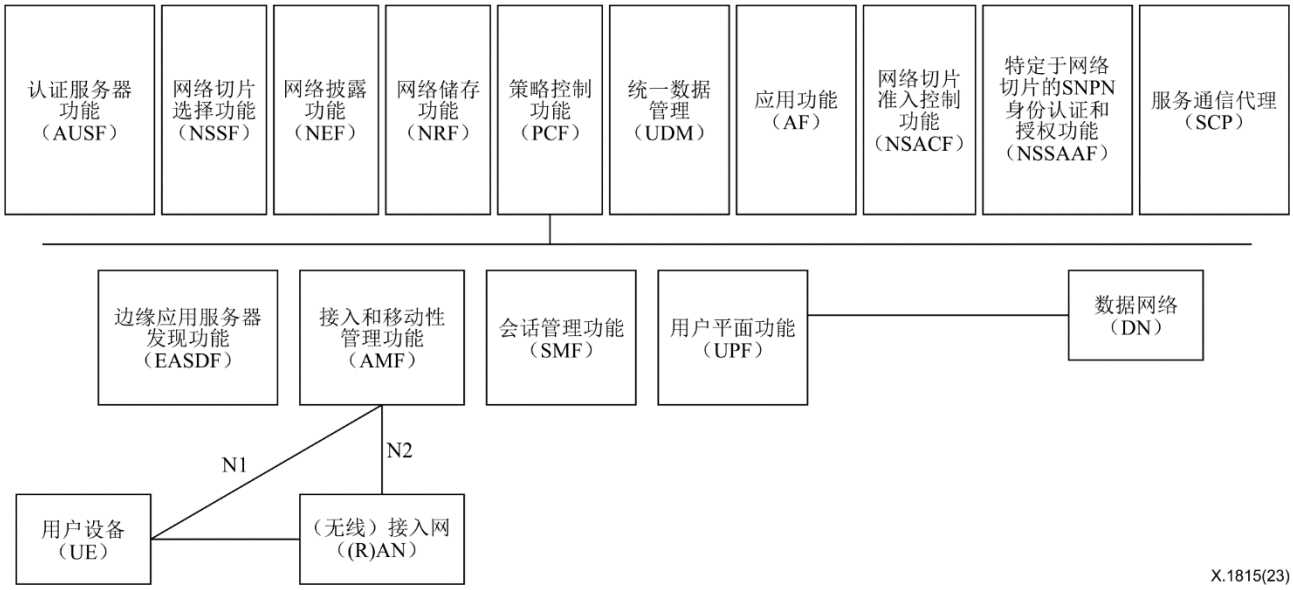

图6-1 – IMT-2020系统架构

图 6-2 描述了 IMT-2020 边缘计算服务的部署方案。

IMT-2020 系统支持部署在 PSA UPF 之外的 DN 中的边缘托管环境（EHE）。EHE 可以在运营商或第三方的控制下[b-3GPP TS 23.548]。部署 EHE 的 DN 的本地部分可以具有与同一 DNN 的集中部署的 PSA 和本地部署的 PSA 的用户平面连接。

从运营商的角度来看，IMT-2020 边缘计算服务的部署方案如图 6-2 所示。

– 边缘DC：提供移动边缘计算（MEC）功能，支持IMT-2020边缘计算服务和网关用户平面（GW-U）和UPF功能。

– 本地DC：提供GW-U、内容交付网络（CDN）和UPF功能。

– 区域DC：提供网关控制平面（GW-C）、AMF/SMF、NB IoT和IMS等功能。

– 管理域：包括云管理平台、网络功能虚拟化编排器（NFVO）和虚拟化网络功能管理器（VNFM）。

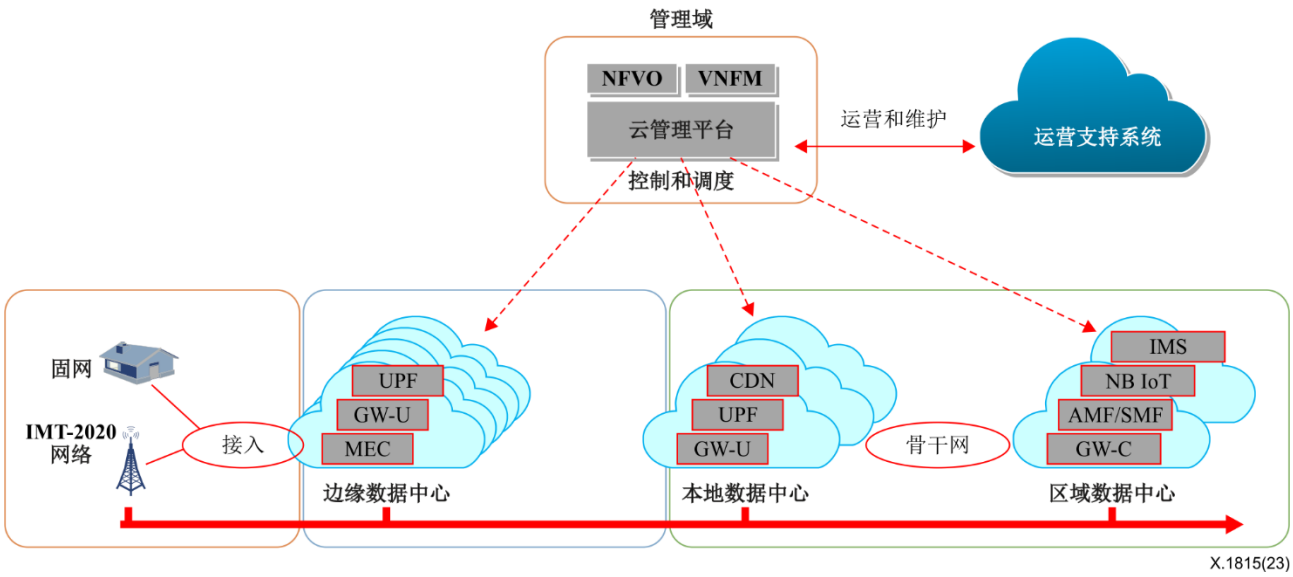

图6-2 – IMT-2020边缘计算服务部署方案

6.2 典型应用场景

6.2.1 车联网（V2X）

在 V2X 的场景中，具有多个应用的连接设备的数量给网络侧带来了不断增加的数据传输需求。网络需要为数据使用和存储提供增强的宽带和计算能力。

通过在 V2X 中应用 IMT-2020 边缘计算技术，可以在边缘节点部署应用，从而减少端到端的延迟，并根据不同 V2X 服务的具体要求来提高可靠性（即，安全驾驶服务在延迟和可靠性方面均需有严格要求），同时受益于更短的传输路径，此外亦会提供更强大的计算和存储资源。

基于 IMT-2020 边缘计算技术的 V2X 中的服务包括但不限于：

– 信息服务：边缘计算服务提供地图加载和更新、音视频娱乐、车辆远程检测等功能。这些功能要求边缘计算服务提供增强的移动宽带能力，例如，至少25 Mbps的4K高清视频服务。

– 安全驾驶服务：边缘计算服务通过车辆信息、行人信息和路边单元信息采集，协助驾驶员做出车辆控制决策（例如，通过发出碰撞警告）。要求边缘计算服务提供低延迟和高可靠性能力（通常，延迟小于20毫秒，电信可靠性至少为99%）。

– 增强的驾驶效率服务：边缘计算服务基于IMT-2020 V2X和大数据分析技术优化交通设施的效率，例如交通灯控制、车辆引导速度。

6.2.2 物联网（IoT）

通过将 IMT-2020 边缘计算技术应用于物联网，可以在边缘节点部署应用，从而减少端到端的延迟，受益于更短的传输路径，并通过本地数据计算提供更高效的服务。

基于 IMT-2020 边缘计算技术的物联网的服务场景包括但不限于：

– 智慧城市；

– 智慧楼宇；

– 智能家居。

6.2.3 工业互联网

IMT-2020 边缘计算技术通过协调 IMT-2020 网络与边缘控制器、边缘网关和边缘云来支持工业互联网服务（特别是对于实时物联网应用，数据处理通常在远离中央数据中心的地方进行，低延迟是强制性要求）。

边缘控制器负责来自边缘网关的任务协调、应用部署和生命周期管理，并控制工业设备等。

边缘网关实现来自边缘云的任务协调、工业设备注册、应用部署和生命周期管理，并分析边缘数据等。

边缘云负责边缘网关的任务协调、工业设备注册、应用部署和生命周期管理，并协调边缘服务器和分析边缘数据等。

7 安全威胁

从分层的角度来看，提供 IMT-2020 边缘计算服务涉及基础设施层、网络层和应用层，因此必须从所有这些角度考虑安全威胁。需要注意的是，虽然 MEC 具有安全和隐私保护的特性，且由于数据传输直接发生在 MEC 服务器上，而不是通过中央服务器，因此降低了数

据在网络传输过程中的数据泄露风险，但大量移动设备的利用和边缘云服务器的部署却导致了新的安全挑战。具体来说，传统的云计算安全解决方案可能不适合 MEC，原因是边缘的物联网设备环境会遇到许多新的威胁，而这些威胁与传统的云管理中的威胁截然不同。实际上，不可能在边缘设备上应用当前的数据安全方法，原因是大多数边缘设备是资源受限的，并且由于 MEC 的高度动态环境，网络变得易受攻击。ENISA（欧洲网络和信息安全局）根据 3GPP 第 16 版审议了 5G 规范，并对 MEC 进行了详尽的漏洞评估[b-ENISA]。因此，在为未来的 5G 应用开发 MEC 环境的同时确保安全性仍然是在不久的将来需要进一步研究的问题。

7.1 基础设施层

7.1.1 云管理平台

IMT-2020 边缘计算服务的部署可能需要云管理平台。除了对这种平台的一般安全威胁之外，攻击者还可以使用云管理平台和 IMT-2020 网络之间的接口来对 IMT-2020 网络发起进一步的攻击。

7.1.2 虚拟化基础设施

如果物理资源受到攻击或损坏，虚拟化基础设施可能不可用。攻击者可能会利用这一潜在的系统漏洞，对虚拟资源管理系统进行未经授权的管理访问，并修改配置信息。

7.1.3 恶意硬件/软件注入

被称为木马的未经授权的软件和硬件组件可以被注入到基础设施中，以降低现有边缘服务器和设备的效率，甚至允许利用服务提供商[b-Daniel]。这可能允许那些为边缘计算服务提供软件和硬件解决方案的实体代表攻击者无意地执行恶意活动。

7.1.4 设备的物理篡改

由于边缘计算架构中的计算资源离潜在攻击者更近，因此对设备进行物理篡改的可能性更大。攻击者可能会破坏边缘节点，进而危及整个网络的效能。

7.2 网络层

7.2.1 分析网络流量

攻击者可以监控和/或窃取链路数据，并分析流量特性以获得关于服务的信息，从而进一步攻击网络。

7.2.2 嗅探网络拓扑

攻击者可能危害可能部署在开放环境中的服务节点，以发起嗅探网络拓扑的攻击。

7.2.3 DDoS攻击

攻击者可能危害开放环境中部署的订阅用户和/或服务节点，从而发起 DDoS 攻击。当 DDoS 攻击发生时，现有网络资源被来自网络内其他受损资源的流量淹没，这是另一个边缘计算安全风险。

7.2.4 窃听或操纵通信数据

使用 IMT-2020 边缘计算的服务基于开放的无线网络。攻击者可能窃听或操纵通信数据；在一些场景中（例如工业和制造业以及智慧城市），通信数据可能包括极其重要的信息，例如用户标识符和凭证、商业信息和公共安全信息。

7.2.5 跨域攻击

由于 IMT-2020 网络中的边缘计算服务需要协调接入网、核心网和云管理平台之间的功能，单点妥协可能会招致跨域攻击，从而导致网络和服务不可用。

7.2.6 未经授权的接入

为了使 UE 能够连接到最佳边缘计算服务，UE 和 IMT-2020 核心网络之间的信令交互是必要的。如果信号被攻击者篡改，可能会导致对边缘计算服务的未经授权的接入，甚至可能导致 DDoS 攻击。

7.2.7 边缘应用的网络暴露

IMT-2020 网络可以将网络信息披露给本地应用功能（AF），可能的情况例如本地 PSA UPF 通过本地网络披露功能（NEF）或直接将网络信息披露给本地 AF。

7.2.8 路由信息攻击

路由信息攻击或简称为路由攻击发生在边缘网络的网络层。路由攻击会干扰网络中流量的传输方式，从而影响吞吐量、延迟和数据路径。

7.2.9 会话劫持

黑客拦截并劫持用户会话，以获得对用户数据和服务的接入。

7.3 应用层

7.3.1 技术框架的脆弱性

在 IMT-2020 边缘计算服务中，由于大量节点在不同场景和垂直行业中使用相同的技术框架，如果一个节点受到损害，将会影响其他节点。

7.3.2 未经授权的使用

当非法或未订阅的用户通过伪装成授权实体获得对 IMT-2020 边缘计算服务的接入时，就会出现未授权使用的威胁。

7.3.3 木马和病毒

当恶意 IMT-2020 边缘计算服务或攻击者冒充合法服务提供商并将木马或病毒注入到可能对用户设备和数据有害的应用中，甚至对移动电信网络发起进一步攻击时，使用木马和病毒的攻击就会发生。

7.3.4 数据披露

在边缘计算服务的应用数据迁移、传输、存储、共享和销毁过程中，当攻击者冒充合法实体来获取数据时，就会发生数据泄露。

8 安全需求

8.1 基础设施层

云管理平台的安全要求应包括：

a) 云管理平台支持数据平面网关、边缘计算平台管理和边缘计算应用的认证和授权。

b) 保护敏感数据，以防止未经授权的接入和数据篡改（例如，在工业场景中，敏感的生产数据需要得到保护，以正确执行工业流程并避免因网络攻击而造成的任何中断）。

c) 云管理平台应与IMT-2020核心网络元素（如UPF NEF）安全隔离。

d) 进行旁路分析，使用时间、功率和空间温度分析来检测硬件木马。基本上，这种方法通过识别异常的系统行为，如执行时间和功耗的增加，来检测安装在边缘节点上的恶意固件或软件。

e) 将受木马影响的硬件与未受木马影响的硬件进行比较的木马硬件检测方法用于检测恶意攻击。

f) 加强未放置在高度安全的边缘数据中心的任何边缘节点的物理安全性，例如通过在制造期间采用额外的物理保护技术或在现场实施锁定机制和其他物理保护措施。

g) 独立于上述内容，边缘系统中处理加密材料的部分须使用例如加固的、抗攻击的SIM卡进行保护，以防止旁路攻击。

虚拟化基础设施的安全要求包括：

a) 如果IMT-2020边缘计算服务的基础设施由虚拟机部署，则虚拟机的vCPU、内存和I/O需要安全隔离。

b) 虚拟化基础设施支持容器之间的安全隔离。

c) 虚拟化基础设施支持存储库和签名的镜像。

d) 使用网络切片进行分段，以分离流量并隔离计算资源[b-ENISA]。

8.2 网络层

网络电信的安全要求应包括：

a) 它支持数据传输的机密性和完整性保护。

b) 它使用安全协议（例如TLS v1.2）在网络元件之间建立安全通道。

c) 通过使用安全的端到端传输协议对各方之间的数据流量进行加密，使用长随机数或字符串作为会话密钥，并在每次成功登录后重新生成会话id。

d) 它通过仔细过滤流量来支持DDoS保护功能，从而不允许不合法的请求通过，而合法的请求通过而没有明显的延迟。

网络管理的安全要求包括：

a) 运营支持系统（OSS）支持与云管理平台交互的认证和授权。

b) 安全隔离边缘计算服务管理和OSS之间的功能。

c) 持续监控网络是否缓慢或有故障，并及时发出网络攻击和问题的警报。

d) 建立可靠的路由协议。

8.3 应用层

边缘应用的安全要求应包括：

a) 实施安全评估，其中包括安全合规性检查、资产管理、病毒扫描等。

b) 边缘应用支持云管理平台和其他边缘应用之间交互的认证和授权。

c) 它保护敏感数据，以防止未经授权的接入和数据篡改。

d) 它支持边缘应用的集成验证。

e) 它在边缘应用加载和实例化期间验证管理员的身份和权限。

f) 支持数据迁移、传输、存储、共享和销毁过程的机密性和完整性保护。

g) 它支持基于程序语言安全扩展和静态程序分析的自动识别和安全加固功能。

h) 它支持对应用性能、流量、源信道和客户端环境的实时监控、分析和警报功能。

i) 支持应用审计，定期收集边缘设备和应用的安全日志，存储并分析它们，然后报警并追踪违规、越权和异常应用行为。

9 边缘计算服务的安全功能指南

9.1 基础设施层

为了满足基础设施层的安全要求，应提供以下必要的安全功能：

a) 数据安全风险监控和预警，防止数据篡改和泄露。

b) 数据安全存储，其中包括敏感数据的加密存储和封装能力。

c) 针对虚拟化平台的安全保护能力，通过系统安全加固、安全隔离、安全控制、数据加密等能力来保证虚拟化网络中的数据安全。

d) 确保虚拟化NF安全性的安全功能，其中包括：

- 认证控制；
- 接入控制；
- 系统安全性的远程验证；
- 通信安全；
- 证明；
- 镜像；
- 签名；
- 安全隔离；
- 硬件介导的执行飞地；
- 基于硬件的信任根；
- 硬件加密；
- 可信执行环境；
- 自加密存储；
- 直接访问内存；
- 硬件安全模块；
- 软件完整性保护和验证。

9.2 网络层

应该提供的网络层安全功能包括但不限于：

a) 保护数据传输的机密性和完整性的能力，如时间戳、序列号、链接加密和其他机制。

b) 支持防止会话劫持的功能，例如加密各方之间的数据流量，使用长随机数或字符串作为会话密钥，以及在成功登录后重新生成会话id。

c) 边缘节点的数据安全控制，其中包括身份认证、安全隔离、持续监控和预警、数据加密、数据脱敏和备份。

d) 可靠的路由协议。

9.3 应用层

应该为应用层提供的安全功能包括但不限于：

a) 控制不同用户和场景的应用权限，以保证应用层数据和服务的机密性、完整性和可用性。

b) 抵御病毒攻击，及时更新病毒库，防止数据泄露或被盗。

c) 识别和评估敏感数据，其中包括脱敏授权、加密存储、监控跟踪、异常报警、审计管理、销毁等能力。

d) 身份认证、持续监控和预警。

参考文献

[b-ITU-T E.800] Recommendation ITU-T E.800 (2008), *Definitions of terms related to quality of service*.

[b-ITU-T X.1811] Recommendation ITU-T X.1811 (2021), *Security guidelines for applying quantum-safe algorithms in IMT-2020 systems*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-ITU-R M.1645] Recommendation ITU-R M.1645 (2006), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*.

[b-ITU-R M.2083] Recommendation ITU-R M.2083 (2015), *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*.

[b-3GPP TS 23.548] 3GPP 23.548 (2021), *5G system enhancements for edge computing (version 17.2.0 release 17)*.

[b-Daniel] B. Daniel, *Is edge computing secure? Here are 4 security risks to be aware of* 9 December 2020. https://www.trentonsystems.com/blog/is-edge-computing-secure.

[b-ENISA] ENISA (European Union Agency for Cybersecurity), *ENISA Threat Landscape For 5G Networks*, December 2020. Available to: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2023年，日内瓦