导读：多接入边缘计算 MEC 通过将计算存储能力与业务服务能力向网络边缘迁移，使应用、服务和内容可以实现本地化部署，成为实现 5G 解决不同应用带来的多样化网络需求的核心技术之一，备受业界研究人员广泛关注。运营商在积极实现低层网络节点的边缘能力持续提升的同时，也在不断通过边缘计算技术为垂直行业应用进行赋能。

为了促进 5G 通信技术交流，推动我国 5G 通信技术发展，《电子技术应用》杂志 2020 年第 6 期推出“5G 边缘计算技术与应用”主题专栏，论文内容既涵盖了 5G 边缘计算的资源调度策略、安全策略、能力开放策略等技术方案探讨，同时也提供了边缘计算技术在远程医疗和智能安防等领域的应用实践，期待为 5G 时代的边缘计算技术研究和应用部署提供有益的借鉴。

特约主编：朱雪田，北京邮电大学工学博士，教授级高级工程师，中关村国家自主创新示范区高端领军人才，现就职于中国联通网络技术研究院。长期从事 4G/5G 移动通信技术与业务创新研发工作，作为项目组长先后负责多个 4G/5G 领域的移动通信国家重大项目，发表学术论文超过 80 篇，发明专利 100 余个，个人著作 3 本。

基于 MEC 的能力开放及安全策略研究*

张 蕾，刘云毅，张建敏，杨峰义
（中国电信股份有限公司研究院 5G 研发中心，北京 102209）

摘 要：多接入边缘计算（Multi-Access Edge Computing，MEC）作为 5G 关键技术之一，受到了业界研究人员的广泛关注。MEC 以边缘网络、边缘计算资源为基础，提供连接、计算、能力、应用的积木式组合，为用户就近提供服务，支持网络能力与业务能力的合作引入与统一开放。在 5G 移动通信网络中，如何将边缘计算平台的能力安全高效地开放给第三方，增加网络能力、业务能力的附加值，已成为热点问题。基于此，研究了边缘网络能力开放技术及安全策略。首先介绍了 MEC 的系统架构及可开放的边缘能力，随后给出了边缘网络能力开放架构以及流程，然后介绍了边缘能力开放过程中面临的风险并介绍了相关安全策略，最后介绍了具体的应用实例。

关键词：多接入边缘计算；网络能力；业务能力；能力开放；安全策略
中图分类号：TN929.5 **文献标识码**：A DOI：10.16157/j.issn.0258-7998.200376

中文引用格式：张蕾，刘云毅，张建敏，等. 基于 MEC 的能力开放及安全策略研究[J].电子技术应用，2020，46(6)：1-5.
英文引用格式：Zhang Lei，Liu Yunyi，Zhang Jianmin，et al. Research on capability exposure and security strategy based on MEC[J]. Application of Electronic Technique，2020，46(6)：1-5.

Research on capability exposure and security strategy based on MEC

Zhang Lei，Liu Yunyi，Zhang Jianmin，Yang Fengyi
（5G R&D Center，China Telecom Corporation Limited Research Institute，Beijing 102209，China）

Abstract：Multi-access edge computing(MEC) as one of key technologies of 5G，has attracted wide attention from related researchers. Based on edge networks and edge computing resources，MEC provides a combination of connectivity，computing，capabilities and applications，provides services to users nearby，and supports the introduction and exposure of cooperation between network capabilities and business capabilities. In the 5G mobile communication network，it has become a hot issue that how to exposure the edge capabilities safely and efficiently. Given that，this paper firstly introduces the MEC system architecture，network capabilities and business capabilities，and then studies the capability exposure architecture and procedure. Finally，we give the security strategy and introduce a specific example.

Key words：MEC；network capability；business capability；capability exposure；security strategy

* 基金项目：国家科技重大专项课题(2017ZX03001013-004)

0 引言

多接入边缘计算(Mobile Edge Computing,MEC)是网络能力、业务能力、内容应用的边缘载体/平台,实现各种能力在边缘的合作引入、按需积木式组合、统一接口开放,满足4K/8K/XR高清视频、工业互联网、车联网等行业领域不同场景的差异化需求[1-2]。多接入边缘计算系统是一个具备网络能力开放和业务能力开放的平台,MEC可通过公开API的方式,为运行在平台主机上的第三方应用提供业务控制、无线网络信息、位置信息等多种服务。

将边缘网络的能力开放给第三方应用,具有重要意义。基于边缘计算平台提供的网络能力及业务能力,第三方应用可根据其业务需求,获得差异化的网络服务,提高用户体验效果。同时,边缘能力开放可以丰富边缘计算平台API,如既能通过网络能力API提供网络能力,又能通过业务API提供业务能力,有力地促进应用的创新,实现规模化效益[3]。另外,MEC平台上可以集成第三方的多种应用,这有助于增强运营商与第三方客户的合作关系,构建良好的生态合作环境。另一方面,边缘计算平台上的网络能力和业务能力的开放也可能带来安全隐患,如未授权访问和病毒攻击、敏感数据泄漏等[4]。因而如何安全高效地开放给第三方应用、提供合理的解决方案将具有重要意义。

基于以上背景,本文首先介绍了MEC的系统架构及可开放的网络能力与业务能力,随后给出了边缘网络能力开放架构以及流程。同时,考虑到边缘能力开放过程中可能会带来的安全问题,本文还给出了相关安全策略,最后介绍了具体的应用实例。

1 MEC关键技术

本节主要介绍了MEC系统架构以及关键模块的功能,之后介绍了与MEC场景强相关的网络能力和业务能力。

1.1 MEC系统架构

为了更好地研究边缘网络的能力开放架构及关键流程,基于3GPP和ETSI相关5G网络、MEC等相关技术规范[1,5],本文给出了基于微服务实现的MEC系统架构图,如图1所示,具体介绍如下。

MEC系统架构主要包含NFVI、MEC平台、MEC管理平台3部分,可以通过相关接口与IT计费系统、OSS系统等对接实现计费结算、服务开通等功能。

MEC平台主要提供业务应用的部署运行环境,支持网络及业务能力的统一引入、安全防护、统一开放等功能。ME平台管理器(ME Platform Manager,MEPM)主要负责MEC平台的监控、配置等管理工作,ME编排器(ME Orchestrator,MEO)主要完成对边缘应用的编排和管理。虚拟化基础设施管理器(Virtualized Infrastructure Manager,VIM)负责基础设施层硬件资源、虚拟化资源的管理、监控和故障上报。

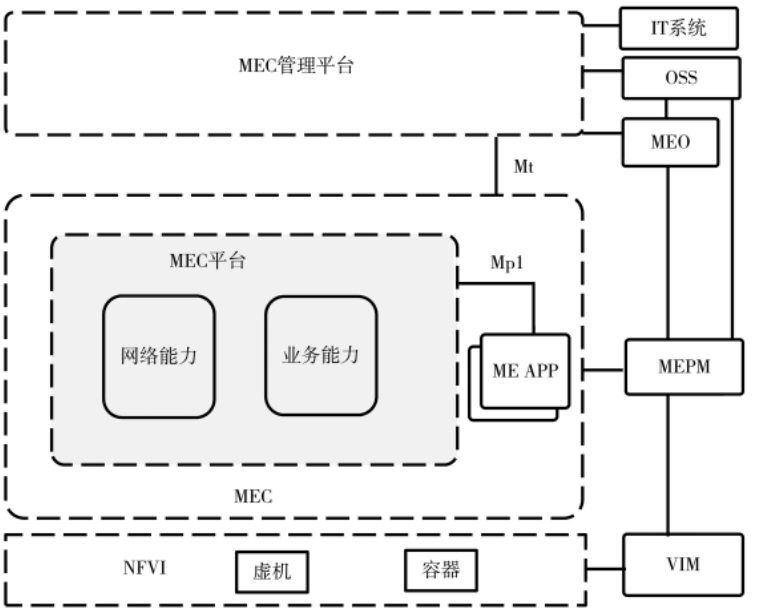

图1 MEC系统架构

边缘应用(Mobile Edge Application,ME APP)通过由MEC平台封装的Mp1接口调用边缘能力,MEC平台生成原始能力调用日志,相关日志通过Mt接口实现边缘向中心同步的云边协同。如客户在MEC管理平台订购了网络能力,可通过边缘MEC平台完成网络能力的调用。

1.2 边缘网络可开放的能力

将网络能力、业务能力集成在MEC平台上,供边缘应用及第三方应用调用,可增加运营商网络能力的价值,接下来将详细介绍各种能力。

1.2.1 网络能力

以下主要介绍了在MEC的场景下和MEC强相关的能力:

(1)位置监控能力:提供用户位置上报手段,通常用于辅助选择应用部署的主机、根据位置进行本地分流决策,以及应用移动性管理;

(2)流量引导能力:提供应用定制用户面路由的手段,应用可通过PCC策略体系,请求SMF选择本地UPF,实现本地分流;

(3)QoS能力:边缘应用通常对网络传送性能要求较高,通过QoS能力调用可提升应用对应的数据流的服务质量;

(4)计费能力:MEC提供的边云协同的服务环境,主要面向应用提供方提供服务。计费能力可指配收费方,灵活适配2B的商业模式。

1.2.2 业务能力

通过边缘平台将业务能力的能力开放给出去,第三方应用根据实际需求接入,可获得差异化的网络服务,进而提升用户满意度。以下主要介绍了目前几个较受关

注的业务能力：

(1)视频转码能力：支持分片转码和动态扩容，弹性扩展转码资源，覆盖主流格式并支持多种分辨率和码率，满足各种场景的定制化需求。智能转码可分析视频元信息，根据结果智能选择最优的转码模板并将转码结果及时回调给用户。

(2)视频 AI 能力：构建 MEC 平台上的智能视频边缘分析能力引擎，为视频安防、智能交通等场景提供视频的边缘识别、结构化分析等处理以及边缘与云端间的通信交互，用通用、标准的方式为视频业务提供云边协同的 AI 分析处理能力，丰富 MEC 平台的能力，促进 5G+视频+AI 的发展。

(3)vCDN：虚拟内容分发网络(Virtual Content Delivery Network，vCDN)可为业务提供包括存储、计算、网络等基础资源服务；也可以提供缓存、加速、函数计算、组播等 CDN 能力服务；vCDN 边缘服务可以通过 MEC 运营管理平台以及 MEC 边缘应用编排管理功能下发，基于容器/虚拟化封装并在边缘节点执行。

(4)虚拟现实云端渲染：将云端计算、云端渲染的理念以及相关技术引入到 VR 应用中，借助高速稳定的网络，将云端的显示输出和声音输出经过编码压缩后传输到用户终端，实现 VR 业务内容上云、渲染上云。

2 基于 MEC 的能力开放架构及流程

本节将重点介绍边缘能力开放架构及相关流程，包含封装编排、访问鉴权、路由转发、边缘能力调用等流程。

2.1 边缘网络能力开放架构

图 2 给出了边缘网络能力开放逻辑架构图[6-7]，其中 5G 网络能力、业务能力及基础设施资源组成了能力层；能力提取与编排层根据用户对网络能力的需求，将提取到的能力借助能力编排器进行封装、编排及组合，最终满足行业客户对差异化服务能力的需求；边缘能力开放层北向与边缘能力应用层互通，南向与能力连接，支持边缘网络能力的安全开放，并提供可调用的统一 API 接口和网关；边缘能力应用层位于最高层，是能力开放的需求方。客户可根据实际需求订购网络能力或业务能力，按照服务协议对边缘网络能力进行安全的调用。

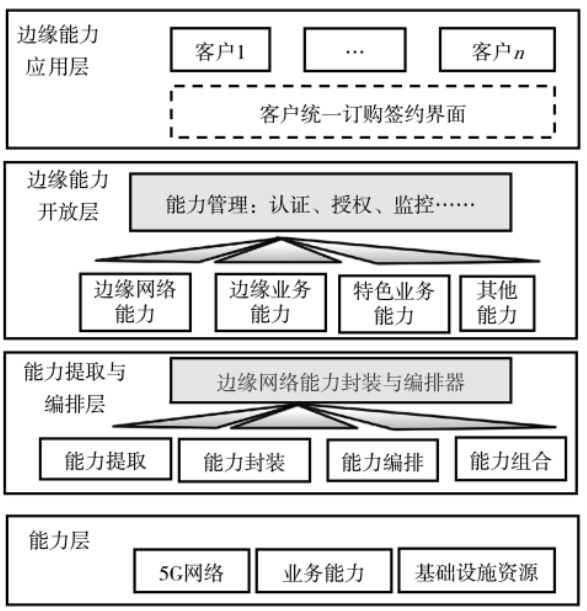

图 2 边缘网络能力开放逻辑架构

2.2 能力开放流程

边缘网络能力开放主要是实现边缘能力的对外开放，主要包含能力封装与编排、访问鉴权、负载均衡、限流流控、路由转发的功能。图 3 给出了边缘能力开放的主要流程。

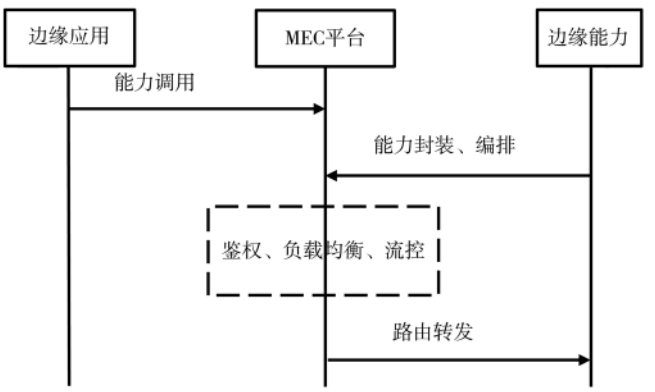

图 3 能力开放流程图

2.2.1 能力封装与编排

边缘计算平台可以提供各式各样的原子能力 API，并以原子能力 API 为基础，对 API 进行实时在线的封装、编排和组合，为行业客户提供各种场景化、差异化的复合能力 API。同时，为了满足应用对多个能力 API 快速、灵活地调用，边缘计算能力开放支持对能力 API 调用的优先级、顺序等进行设置。另外，边缘计算能力开放还支持对多个能力 API 调用的嵌套检测，以及多个能力 API 编排组合的冲突检测[2]。

2.2.2 访问鉴权

访问鉴权是指为边缘应用(ME APP)调用边缘能力提供签名认证、请求鉴权服务并最终根据鉴权结果生成能力调用日志。

(1)身份签名认证

边缘应用根据 MEC 管理平台签发的签名密钥对 APP ID 及其他参数进行签名加密，并在调用边缘能力时携带签名结果和其他业务参数。

MEC 平台根据签名密钥对业务参数进行签名加密，并与请求的签名结果进行比较，两者一致则认证通过。

(2)接口权限鉴权

MEC 平台根据边缘应用调用边缘能力时携带的 APP ID 参数及请求地址，判断该应用是否有权限使用该边缘能力。

当该应用鉴权通过后，MEC 平台将请求路由至相应

的能力，并记录能力调用日志。

2.2.3 路由转发

能力开放为边缘应用的能力调用提供路由转发服务。主要根据边缘应用请求地址中的路由信息从路由表中获得请求能力的 IP 与端口号进行转发服务。

2.2.4 能力调用流控

流控是指在一段时间内，系统接收到的请求数量高于其所设置的处理阈值时，将超出阈值的请求拦截过滤，以此来保障系统应用的正常运行。

MEC 平台能力开放的流控可以分为 3 种场景：

(1)当 MEC 平台节点内的整体业务并发量超出 MEC 平台能力开放设置的阈值时，对所有能力调用请求进行限流，保障 MEC 平台能力开放正常可用；

(2)当某个能力的请求量超出该能力集群设置的并发承受量时，对该能力的请求进行流控；

(3)对某个边缘应用调用方进行一段时间内的调用请求阈值设置，对单个调用方进行流控。

3 基于 MEC 的安全策略研究

边缘网络能力开放过程中，可能带来安全隐患，如未授权访问和病毒攻击、敏感数据泄漏等。本节主要介绍了安全隐患和相关解决方案。

3.1 安全隐患

3.1.1 基础设施风险

MEC 虚拟基础设施通过计算、存储、网络，虚拟化层所暴露出的漏洞可能受到黑客的攻击，破坏硬件和服务的可用性，甚至通过漏洞控制系统与业务，窃取关键敏感数据。同时，MEC 应用大多采用基于容器的微服务架构，各容器共用宿主机内核资源，所以容器与宿主机之间、容器与容器之间隔离方面存在安全风险，如进程隔离、进程间通信隔离等。

3.1.2 MEC 应用安全风险

边缘应用对接 MEC 主机提供的服务，接受 MEC 管理平台的纳管，提供行业应用服务。可能面临以下安全风险：

(1)由于不同应用之间的安全等级和防护能力并不相同，如果隔离不当，可能发生某一应用由于自身漏洞被恶意利用而向其他应用进行恶意攻击的安全风险；

(2)不同应用共享资源，可能存在某一应用由于外部攻击或者自身运行异常，导致占用资源过高，从而影响其他应用的正常运营；

(3)由于应用能力可以对外开放，如果权限控制不当，可能存在能力被滥用、恶意使用的风险；

(4)如果第三方应用安全管控能力不足，可能存在应用镜像本身存在安全漏洞，增加风险。

3.1.3 MEC 平台风险

MEC 平台负责提供 MEC 系统功能服务、服务注册、APP 权限控制、流量规则控制等能力，可能面临以下安全风险：

(1)如果 MEC 平台的权限设置存在漏洞，可能导致 APP 越权访问其他服务；

(2)如果 MEC 平台遭受 DDOS 攻击，可能影响 MEC 平台的可用性，进而影响整个 MEC 节点的可用性；

(3)如果 MEC 平台被非授权访问，攻击者可能进行恶意配置，影响 MEC 主机以及 APP 的正常运行。

3.1.4 MEC 编排管理安全风险

MEC 编排管理是实现 MEC 节点灵活部署应用的枢纽，主要面临被非法控制、编排管理失效等风险。

(1)如果网络连接发生故障，可能导致编排管理通道不可用，无法下达编排管理指令，或者编排管理通道被中间人截取，导致编排管理指令被恶意篡改；

(2)如果编排管理权限被滥用，可能导致用户越权对其他 APP 进行生命周期运维；

(3)如果编排管理系统被仿冒，则假冒者可以对 MEC 节点进行恶意编排管理操作，对整个 MEC 节点带来极大的安全威胁；

(4)如果 MEC 编排管理系统被入侵，攻击者可以非授权获取资源控制权限或者获取相关管理信息，从而可以非法控制 MEC 资源。

3.2 安全解决方案

针对前边介绍的安全隐患，本小节提出了对应的安全解决方案。

3.2.1 MEC 应用安全

(1)可对运行在 MEC 平台上的应用进行安全防护，包括镜像安全、MEC 应用的用户权限和访问控制、应用监控等；

(2)MEC 内部按照 MEC 平台及自有应用、第三方应用划分不同的安全域，可以通过防火墙实现域间隔离。

3.2.2 MEC 平台的自身安全防护

安全方案示意图如图 4 所示。

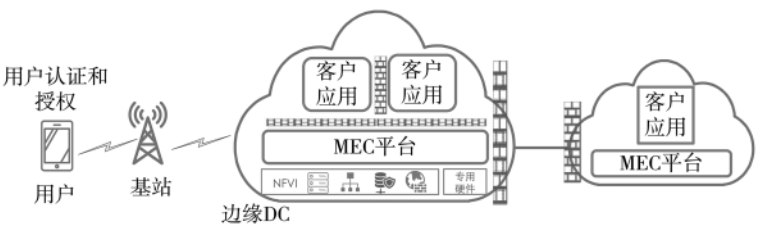

图 4 安全方案示意图

(1)在平台上线、升级时，对 MEC 平台进行安全扫描与评估，保障安全平台。根据漏洞库对平台的各类服务、文件进行扫描。

(2)部署 MEC 平台的安全基线核查系统，针对平台的运行环境参数、自身配置等进行安全基线管理，按制定的安全基线标准进行基线核查，发现不满足基线的问题及时整改。

(3)具备 MEC 平台日志审计能力,及时发现 MEC 应用违规、越权和异常行为,提供事后追溯。

(4)部署防火墙,防止外来网络对于 5G 网络以及 MEC 平台的攻击。

3.2.3 能力开放 API 的安全防护

(1)对 APP 的认证授权管控。对各类 APP 应用进行安全规范设置,降低安全风险,包括为避免第三方直接获取密码,授权方式采用授权码模式;认证请求 URI 中应添加 state 参数,以防范跨站请求伪造攻击;授权服务器在颁发令牌时,应遵循最小授权原则,并对令牌进行生命周期管理。

(2)对 API 接口的安全管控。对 API 接口调用应采用证书等方式进行认证与鉴权。启用 API 白名单,并对发往 API 网关的请求应进行数据包的合法性校验。针对 API 调用操作进行监控,及时切断敏感操作,保护 API 开放安全。

(3)应规范 API 开放接口的安全调用,例如:重定向 URI 中应设置一次有效的 code 参数,避免产生回调域名欺骗风险而造成 code 泄露;code 参数应在使用或过期后删除,避免产生重放攻击。

3.2.4 MEC 编排管理安全

(1)对编排和管理系统实体进行安全基线配置,实现安全服务最小化原则;对重要配置文件进行安全配置核查,确保配置文件的安全;定期进行安全扫描和加固。

(2)对编排管理双方网元实施双向认证或者白名单接入方式;对组件或设备(包括软件、硬件和固件)进行检测,检测到非授权的组件或设备时应支持禁止其网络访问。

4 应用实例

多接入边缘计算平台支持实时转码、VR 渲染、人脸识别等业务能力的统一开放。本节以基于 MEC 的人脸识别能力开放为例,阐述边缘网络能力开放在行业应用中的探索。

该业务场景中,将人脸识别能力下沉到“边缘侧”,MEC 集成人脸识别的能力,采集摄像头数据,进行人脸识别;MEC 通过能力开放接口,将识别能力开放给第三方应用;第三方应用可以经过注册、认证、鉴权等流程,调用 MEC 平台的视频分析数据接口,获取人脸识别的分析结果。图 5 给出了基于 MEC 的人脸识别能力开放示意图。

可以将边缘平台上的人脸识别能力开放给企业园区、公安等行业,有助于加强园区安防维护社会治安,具有良好的发展前景。

5 结论

MEC 是一个具备无线网络能力开放和运营能力开放的平台,MEC 可通过公开 API 的方式,为运行在平台主机上的第三方应用提供 AI 识别、VR/AR 视频渲染、位置信息等多种服务。本文首先介绍了 MEC 系统架构及 MEC 平台集成的网络能力和业务能力;随后描述了边缘网络能力开放架构及相关流程,包含封装与编排、访问鉴权、路由转发、能力调用等流程;然后分析了边缘能力开放过程中的安全隐患,主要介绍了 MEC 应用和平台面临的风险,并给出了 MEC 平台的安全防护及能力开放 API 的安全防护策略;最后介绍了基于 MEC 的人脸识别能力开放实例,将人脸识别能力开放给第三方应用,可以加强园区安防和社会治安等。

参考文献

[1] ETSI GS MEC 003:Mobile edge computing(MEC);framework and reference architecture,V1.1.1[S].2016.

[2] 张建敏,杨峰义,武洲云,等.多接入边缘计算(MEC)及关键技术[M].北京:人民邮电出版社,2019.

[3] 中国多接入边缘计算开放实验室.中国多接入边缘计算技术白皮书[Z].2019.

[4] 黄嘉,聂炜玲,王丽秋,等.5G MEC 关键技术及安全隔离措施研究[J].互联网天地,2019(10):29-33.

[5] 张建敏,谢伟良,杨峰义,等.5G MEC 融合架构及部署策略[J].电信科学,2018,34(4):115-123.

[6] 张蕾,夏旭,朱雪田.基于 5G 确定化网络的行业应用研究[J].电子技术应用,2019,45(12):20-24.

[7] 李红祎,赵一荣,李金艳,等.基于能力开放的 5G 网络切片管理研究[J].电子技术应用,2020,46(1):1-5,11.

(收稿日期:2020-05-11)

作者简介:

张蕾(1993-),女,硕士,主要研究方向:网络架构、边缘计算等 5G 关键技术。

刘云毅(1993-),男,硕士,主要研究方向:5G 边缘计算技术。

张建敏(1983-),男,博士,高级工程师,主要研究方向:移动通信、边缘计算等 5G 关键技术。

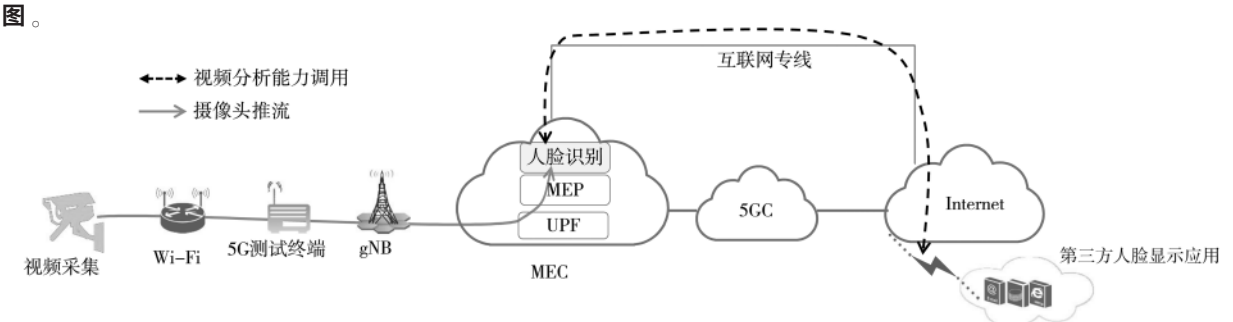

图 5 基于 MEC 的人脸识别能力开放示意图

版权声明