Contemporary advances in multi-access edge computing: A survey of fundamentals, architecture, technologies, deployment cases, security, challenges, and directions

Mobasshir Mahbub, Raed M Shubair

Contemporary Advances in Multi-Access Edge Computing: A Survey of Fundamentals, Architecture, Technologies, Deployment Cases, Security, Challenges, and Directions

Mobasshir Mahbub*, Raed M. Shubair

Department of Electrical and Computer Engineering, New York University (NYU) Abu Dhabi, Abu Dhabi, UAE
Email: mobasshir@ieee.org*, raed.shubair@ieee.org, raed.shubair@nyu.edu

Abstract – With advancements of cloud technologies Multi-Access Edge Computing (MEC) emerged as a remarkable edge-cloud technology to provide computing facilities to resource-restrained edge user devices. Utilizing the features of MEC user devices can obtain computational services from the network edge which drastically reduces the transmission latency of evolving low-latency applications such as video analytics, e-healthcare, etc. The objective of the work is to perform a thorough survey of the recent advances relative to the MEC paradigm. In this context, the work overviewed the fundamentals, architecture, state-of-the-art enabling technologies, evolving supporting/assistive technologies, deployment scenarios, security issues, and solutions relative to the MEC technology. The work, moreover, stated the relative challenges and future directions to further improve the features of MEC.

Keywords – MEC, IoT, Digital Twin, Open-Source MEC, Quantum Computing, AI, Security.

1. Introduction

According to Ericsson's most recent prediction for 2020-2026, worldwide mobile subscribers will increase up to 8.8 billion, and global wireless data traffic will be doubled [1], [2]. This enormous rise in wireless data traffic, vast Internet of Things (IoT) device deployments, and wireless broadband subscribers are being driven by expanded mobile network coverage [3].

With the introduction of beyond 5G connectivity, mobile communications infrastructures, and an ever-increasing number of portable devices (e.g., handsets, wearable devices, unmanned aerial vehicles, and interlinked vehicles), a proliferation of unique services (together with verticals) including intelligent cities, industry 4.0, medical services, and coordinated driving are now feasible. These breakthroughs necessitate the close integration of communication, processing, caching, and control technologies [4]. By 2023, Cisco predicts that approximately 300 billion multimedia applications will have been downloaded [5]. Along with a flourishing spectrum of new and different services, demands for the seamless quality of experiences (QoE) are rising; placing centralized or consolidated cloud computing infrastructures under strain since traditional centralized cloud services are unable to meet linearly expanding computational processing needs. Furthermore, according to Ericsson Mobility Research, worldwide average mobile data consumption will grow up to 164 exabytes (EB) per month in 2025 [6].

These emerging services have considerably diverse priorities, and they often necessitate huge data processing with short end-to-end latency. Across numerous technological solutions at multiple levels (i.e., machine intelligence, millimeter-wave transmissions, network function virtualization), MEC will perform an influential function [7]. MEC's purpose is to relocate cloud features and functionality (i.e., computational and storage services) to the edge or end of a network to reduce the long duration and highly unpredictable delays required to approach centralized clouds. MEC-assisted networking enables user devices (UDs) to transfer computational operations to adjacent processing facilities or edge processing servers, which are often located on the near-user network nodes (i.e., base stations) [8]. Nevertheless, as edge processing units have significantly lower computing capacity than core or central cloud services, the available facilities (radio, computation, and energy) must be effectively handled to offer users a reasonable quality of service (QoS) [9]. Since the end-to-end latency comprises both transmission and processing time, the available resources at the cellular edge of the networks must be managed collaboratively, determining the optimum joint allocation of resources over time in a dynamic and data-driven approach.

The European Telecommunications Standards Institute (ETSI) launched the Mobile Edge Computing (MEC) Industrial Specifications Group (ISG) in December 2014 to encourage and expedite the evolution of edge-cloud computing in wireless networks [10]. The ETSI MEC ISG aimed to establish an accessible ecosystem throughout multi-vendor cloud systems positioned at the RAN's edge, attainable by application/service vendors and third-party stakeholders, to address the issues associated with centrally controlled cloud computing contexts, specifically latency and the expectation of higher speeds [10]. Wireless network operators can decrease traffic congestion in the center of the network and backhaul connections while facilitating the transfer of heavy computational activities from power or resource-restricted user equipment (UE) to the edge servers. This can be achieved by moving data processing workloads to the edge of the network and locally handling data in the vicinity of users. Generally, such distributed cloud architecture serves as a foundational technology for forthcoming 5G and beyond 5G systems, replacing traditional cellular base stations by providing edge-cloud computing capabilities and an IT services ecosystem at the edge of the network. ETSI ISG has decided to drop the 'Mobile' from MEC and changed the name to ‘Multi-Access Edge Computing’ in September 2016 to better reflect its appropriateness in heterogeneous network systems, including storage and computation assistance for end devices over stationary access technologies such as satellite, fiber, wireless, light-fiber, and fiber-wireless [11]. Software Driven Networking (SDN) and virtualized networks have been adopted in MEC development. SDN and Network Functions Virtualization (NFV) are natural extensions to MEC nodes because they enable intelligent network convergence and resource management. MEC nodes use virtualization to accommodate third-party vendor-based Containers and Virtual Machines (VM), resulting in a multi-tenant environment at the edge of the network. Due to the implementation of MEC nodes on the edge of the network, there is a requirement to promote the mobility of services, and VM offloading approaches and Container-based offloading strategies may be identified in the literature [12].

Sixth-generation (6G) [13], [14] network infrastructures are intended to support the Internet of Everything implementations, including brain-computer interplay, multiple sensory extended reality (XR), and self-reliant systems to attain a completely automated and intelligent framework for consumer services and programs in the upcoming years, together with to offer subscribers with an engrossing perception in a virtual environment such as Multiverse. To attain these goals, 6G must meet stringent standards, including ultra-high transmission and dependability, ultra-low latencies, seamless connection, and so on. To that end, it is crucial to include some sophisticated technology into the architecture of 6G wireless environments, such as using Terahertz communication systems [15] and intelligent reflecting surface (IRS) [16] to enhance data transmission efficiency, MEC, and machine intelligence [17] to strengthen data processing performance, and Blockchain [18] to prevent security risks.

MEC is regarded as a possible 6G enabling innovation capable of meeting expanded service needs [19]. For example, by analyzing computation-intensive content or storing ultra-high-definition movies at the edge, MEC may provide ultra-low transmission latency and perfect 4K/8K visual broadcast.

The work reviewed existing literature (survey and review papers) relative to the MEC technologies in section 2. Then it overviewed the fundamentals, relative computing technologies, and MEC in section 3. In section 4 the survey discussed the MEC standardization, reference architecture, and integration of MEC in 5G infrastructure. Afterward, it performed a survey of the state-of-the-art enabling technologies such as Service Function Chaining (SFC), Heterogeneous Cloud-Radio Access Network (H-CRAN), Device-to-Device (D2D) communication, Machine Learning and Artificial Intelligence (ML/AI) in section 5. Further, the work discussed the technical features of MEC, i.e., computation offloading, communications, content delivery and caching in section 6. Supporting technologies such as Rate Splitting Multiple Access (RSMA), Intelligent Reflecting Surfaces (IRSs), Game Theory, Auction Theory, Digital Twins, the open-source MEC framework (for the forthcoming or evolving network, such as 6G), a passive optical network (PON) are discussed in section 7 for improving the features of MEC paradigm. In section 8, the work briefed the deployment scenarios of MEC. Moreover, this work provided an overview of security concerns relative to MEC and state-of-the-art countermeasures in section 9. Furthermore, it described the lessons learned, challenges, and future directions for further work in section 10. Finally, the survey concluded with section 11. Fig. 1 visualizes the structure of the paper.

2. Literature Review

This section of the paper incorporates a review of existing surveys or review works or papers to provide insight into the current progress of the MEC and relative technologies.

Akhlaqi et al. [20] carried out a survey utilizing a mixed-method comprehensive literature review that includes quantitative and qualitative data from literature investigated. The classification of literature based on adopted techniques is described, and significant offloading-related challenges in MEC are explored. The work described possible fields of work, the importance of the methodologies, algorithms, and approaches, and the research directions in MEC for continued future exploration.

Djigal et al. [21] provided an in-depth investigation of Machine Learning/Deep Learning-based resource allocation processes in MEC. The survey started with tutorials that illustrate the benefits of using Machine Learning and Deep Learning algorithms in MEC. The work provided a comprehensive assessment of recent studies that employed Machine Learning/Deep Learning approaches for resource allocation in MEC from three perspectives: (1) task offloading; (2) task scheduling; and (3) joint resource allocation. Ultimately, the work explored the critical issues and potential research objectives of using the Machine Learning/Deep Learning to allocate resources in MEC networks.

Liang et al. [22] performed an extensive survey of prevailing advancements in MEC and explained the MEC principle, structure, and features. The work also discussed MEC’s technological enablers such as NFV, SDN, Information-Centric Networking (ICN), Cloud-Radio Access Networks (C-RAN), Service Function Chaining, Network Slicing, and Fog-computing-enabled access network infrastructures. MEC application scenarios as well as the possible research problems are discussed.

Huo et al. [23] presented an up-to-date and thorough assessment of MEC-enabled vehicular network infrastructure. The work started with outlining MEC's concept, framework, applications, and problems. Following that, the article overviewed MEC’s implementation for vehicular networking services and applications by identifying existing research and potential problems.

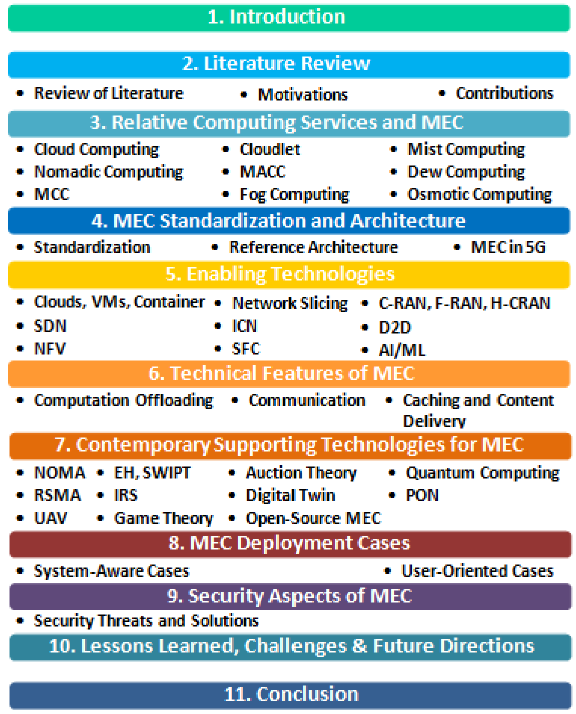

Fig. 1: The structure of the paper.

M. A. Khan et al. [24] provided an in-depth study of recent advancements in MEC-assisted video streaming that have resulted in extraordinary improvements to enable unique use cases. A comprehensive overview of the current advancements is provided, with emphasis on novel cache management techniques, effective computation-task offloading, coordinated offloading and caching, and the utilization of Artificial Intelligence or Machine Learning (i.e., Reinforcement Learning, Deep Learning, etc.) in MEC-enabled streaming services.

The future generation (6G) connectivity systems are designed to support the Internet of Everything and transform client applications and services into a fully autonomous and intelligent system. The Digital Twin-enabled edge network (DITEN) is suggested to do this by combining Mobile/Multi-Access Edge Computing (MEC) with Digital Twin (DT), hence boosting the performance of the network such as capacity, and security while lowering the cost of connectivity, processing, and caching. Tang et al. [25] provided a complete review of DITEN for 6G in this survey. First, the work discussed the essential components of DITEN, such as the principle, structure, and potential. Second, a thorough DITEN design is created, which includes DT modeling/updating, DT implementation, major challenges, and supporting technologies. The Internet of Things (IoT), the vehicular network, the space-to-air-to-ground integrated network (SAGIN), wireless transmission technologies, and other technologies are then discussed, alongside the implementation of DITEN for each domain, such as DT models, DT interaction, incentive strategies, and so on. Finally, limitations and unresolved concerns are addressed.

Gür et al. [26] explored the ICN and MEC integration in this study to give a complete assessment from a prospective view of beyond 5G networks. To demonstrate the practical significance of ongoing standardization initiatives, the work provided a review of active standardization initiatives. Furthermore, the work presented major B5G deployment scenarios and emphasize the importance of ICN and MEC integration in meeting their needs. Finally, the survey outlined research problems and possible research areas. It included a brief review of ICN integration issues and implementation instances as well.

Douch et al. [27] provided a comprehensive and well-structured evaluation of Edge Computing (EC) as well as its associated technologies. The work defined EC from the roots, explaining its architecture and progression from Cloudlet technologies to Multi-Access Edge Computing. Further, the work reviewed current research on the key components of an EC framework, such as resource managing, task offloading, data monitoring, network management, and so on. Additionally, it focused on EC technological solutions, beginning with Edge Intelligence, a subclass of Artificial Intelligence (AI) that incorporates AI algorithms at capacity-constrained edge servers or nodes with substantial heterogeneity and flexibility. Then, the review moved forward onto 5G and its enabling technologies and overviewed how EC and the 5G complement one another. Moreover, it investigated virtualization and containerization as potential hosting Virtual Machines for edge services.

Malazi et al. [28] presented the dynamic resource deployment problem and discussed its connections to other issues, including scheduling tasks, resource allocation, and edge caches. It also provided a thorough analysis of contemporary dynamic resource or service placement strategies for MEC contexts from the viewpoints of communication, middleware, services, and evaluation. At first, it examined several MEC topologies and their supporting technologies from a communication standpoint. Secondly, it reviewed the dynamic service placement approaches from the perspective of middleware. The work also conducted a methodological survey and identified eight research strategies that researchers adopt. The work divided the research aims into six major categories, resulting in a hierarchy of development objectives for the dynamic/flexible service placement challenge. In addition, it evaluated the approaches and developed a solution taxonomy based on six criteria. In the third phase, the work focused on the application level and introduced programs that can benefit from dynamic resource placement. Moreover, in the fourth stage, the work reviewed the evaluation platforms utilized to validate technologies, such as simulators and testing platforms. Finally, the work constructed a list of potential problems and challenges classified by diverse points of view.

Qiu et al. [29] presented a detailed review of current studies that use auction mechanisms in edge computing. Initially, a brief introduction to edge computing is provided, covering three typical edge computing perspectives: cloudlet, fog, and mobile edge computing. Then, the work elaborated on the basics and history of auction techniques that are often employed in edge computing environments. Afterward, it presented a detailed assessment of auction-based methodologies used for edge computing, which is classified by auction methodology. Finally, numerous unresolved issues and intriguing research avenues are highlighted. Decentralized or Distributed Deep Learning (DDL), recently, regarded as one of the facilitators of MEC, helps civilization through dispersed model training and worldwide shared training knowledge.

Sun et al. [30] provided a complete overview in terms of confidentiality, edge variability, and adversarial threats and countermeasures. Furthermore, future DDL developments emphasize themes like efficient utilization of resources, asynchronous connectivity, and completely distributed frameworks.

Arthurs et al. [31] analyzed the concepts of the use of cloud technology with Intelligent Transportation Systems (ITS) and interconnected cars and presented taxonomy as well as implementation scenarios. The work concluded by highlighting areas where more research is required to enable cars and ITS to employ edge cloud technology in a fully controlled and automated manner. In the cloud and edge computing paradigm, effective resource management and pricing is a fundamental problem. In recent times, auction framework design has received a lot of attention as a solution for dealing with this problem.

Jin et al. [32] provided an in-depth examination of cognitive computation offloading, including essential challenges, measurements, and future perspectives.

Ali et al. [33] presented an overview of MEC architecture, application cases, conceptual principles for MEC security infrastructure, privacy and security strategies, and discussed existing and future difficulties, their consequences, and solutions. This study investigated important dangers, defined the MEC framework, identified vulnerable functional layers, and threat groups, and suggested security solutions. To counteract targeted assaults, the study briefed several strategies that MEC providers adopt in various levels of security safeguarding.

Sharghivand et al. [34] provided a complete assessment of the auction-based techniques in the realm of cloud/edge computing.

Jiang et al. [35] performed a complete review of MEC-based video streaming. The associated overview and background information are first evaluated. Secondly, resource allocation concerns have been raised. The enabling mechanisms for video content streaming are described by taking caching, processing, and networking into consideration. Following that, a hierarchy of MEC-supported video streaming services is developed. Finally, problems and prospective research directions are presented.

Ranaweera et al. [36] examined the MEC system's privacy and security aspects. It presented detailed research on threat vector analysis and detection in the ETSI-prescribed MEC architecture. In addition, the work overviewed the vulnerabilities that lead to the detected threat vectors and provided viable security solutions to address the flaws. MEC's privacy concerns are also recognized, and specific privacy objectives are stated. Finally, the work suggested future instructions to improve MEC service privacy and security.

Siriwardhana et al. [37] comprehensively covered the Mobile Augmented Reality (MAR) technology as well as its future possibilities concerning 5G systems and complementing technologies relative to MEC. The research, in particular, presented an instructive analysis of existing and future MAR frameworks in terms of edge, cloud, hybrid, and localized technological possibilities. The study examined significant MAR application domains and their prospects with the introduction of 5G technology. The study also evaluated the importance of 5G technologies and explored the requirements and constraints of MAR technical areas such as connectivity, mobility control, energy governance, task offloading and relocation, safety, and privacy.

Shah et al. [38] examined MEC and the slicing of networks in the context of 5G-focused application scenarios. Modifications to the cloud-native 5G backbone have recently received attention, with MEC application cases enabling network scalability, elasticity, adaptability, and automation or self-orchestration. A cloud-based micro-service framework is envisioned in terms of 5G network slicing. The work also discussed recent breakthroughs allowing end-to-end (E2E) network slicing, as well as the supporting technologies and ongoing standardization initiatives. Finally, this work outlined unresolved research challenges and offered some potential recommendations.

Spinelli et al. [39] started with a review of standardization, with a focus on 5G and NFV, and then moved on to the versatility of MEC intelligent resource utilization and its migration possibilities. Moreover, this survey investigated how the MEC is being utilized and how it may assist industrial verticals.

Filali et al. [40] demonstrated the incorporation of MEC into the design of contemporary mobile networks, together with the transition strategies to a conventional 5G network infrastructure. It also addressed NFV, SDN, and network slicing. Furthermore, the work presented a cutting-edge study on the various ways of optimizing MEC capabilities and QoS factors. The work categorized various techniques based on the optimum resources and QoS factors (i.e., storage, processing, memory, energy, bandwidth, and latency). Ultimately, based on the conventional SDN paradigm, the work offered reference architecture for a MEC-NFV ecosystem.

Mehrabi et al. [41] reviewed the concept of end-user devices-enhanced MEC in depth, i.e., methods that use the capacities of the end device community and the deployed MEC to offer services to end devices. The work divided device-enhanced MEC strategies into two categories: computation offloading techniques and caching strategies. It further subdivided the caching and offloading strategies based on the desired performance requirements, which comprise throughput optimization, latency reduction, energy saving, utility maximization, and increased security. Finally, the work discussed future research possibilities and identifies the key limitations of present device-enhanced MEC systems.

Game theory (GT) is already utilized successfully to construct, develop, and optimize the functioning of numerous typical communication systems and networking contexts. Moura et al. [42] covered the literature on theoretical games deployed to wireless networks, with an emphasis on use cases of forthcoming MEC. Finally, the work described potential trends and research areas for using theoretical games in the emerging MEC services, taking into account both network design challenges and usage scenarios.

Porambage et al. [43] presented a comprehensive overview of the use of MEC technologies for the development of IoT applications, as well as their synergies. The work described the technical considerations of implementing MEC in the IoT paradigm and offered some insight into different integration solutions.

Taleb et al. [44] provided an overview of MEC and emphasized the major facilitating innovations. It discussed MEC orchestration by taking into account both individual applications and a framework of MEC platforms that allow mobility, shedding light on the various orchestration and deployment choices. Furthermore, this paper examined the MEC standard architecture and primary deployment scenarios that provide multi-tenancy for developers, content suppliers, and third parties. Furthermore, this article provided a summary of current standardization initiatives and expands on open research problems.

Shahzadi et al. [45] overviewed the common edge-cloud computing architecture and techniques, along with a quantitative comparison of their classifications using several QoS criteria (relevant to networks' performance and system overheads). Taking into account the knowledge gained, techniques examined, and theories addressed, the study provided a complete review of current research and future research prospects for Multi-Access/Mobile Edge Computing.

Michailidis et al. [46] presented an introduction to Unmanned Aerial Vehicle (UAV)-assisted MEC-enabled IoT as well as a thorough discussion of use instances and application areas where security is paramount. Following that, current research activities on security mechanisms for UAV-assisted MEC-aided IoT are fully overviewed. To that aim, information-theoretic mechanisms for ensuring proper physical-layer security are examined including advanced security measures based on innovations such as Machine Learning and Blockchain. Furthermore, research findings on hardware and software-based approaches for network node recognition and authentication are described. Finally, the work described future possibilities in this research arena, encouraging additional investigation.

Wei et al. [47] provided a detailed literature overview on Reinforcement Learning (RL)-empowered MEC and presented suggestions for further research. Moreover, challenges of the MEC ecosystem linked with unrestricted mobility, interactive channels, and dispersed services are outlined, accompanied by how they might be resolved using RL solutions in various mobile apps or services. Finally, the open research issues are highlighted to give useful direction for further studies in RL retraining and learning.

Li et al. [48] provided a complete evaluation of the progress of the privacy-concerned task offloading in Mobile Edge Computing. Offloading privacy problems, as well as associated metrics and application situations, are examined first. The contemporary privacy-preserving offloading solutions are then categorized into three groups based on their related offloading phases: controlling offloading content and sequence, secure transfer of computation offloading data, and offloading endpoint selection. Finally, future options for privacy-protecting offloading are outlined.

Feng et al. [49] provided a complete analysis of the computational task offloading in MEC systems, including implementations, offloading priorities, and offloading methodologies. It focused on essential difficulties related to different offloading objectives, such as delay reduction, energy usage minimization, profit maximization, and network utility maximization. The existing issues and future possibilities of the task offloading in MEC systems are examined.

Pham et al. [50] started the study by providing a comprehensive review of MEC technologies and their possible use cases and implementation scenarios. Then, it presented the most recent research on the convergence of MEC with emerging technologies that will be employed in 5G and even beyond. The work also summarized edge computing simulation platforms and experimental assessments, as well as open source initiatives. It also highlighted lessons learned from cutting-edge research and explore difficulties and potential future avenues for MEC research.

Huda et al. [51] examined UAV-assisted MEC systems with an emphasis on computational task offloading. To evaluate features and functionality, the work compared the task offloading algorithms holistically. Finally, it discussed open challenges and research objectives in design and execution.

Waheed et al. [52] presented a detailed review of the different vehicular network computing concepts. The study discussed the architectural intricacies, similarities, variances, and significant characteristics of each computing paradigm. Finally, it presented open research issues in vehicular networks as well as prospective research initiatives.

Shakarami et al. [53] provided a comprehensive study on stochastic-based offloading methodologies in diverse computing technologies such as Fog Computing (FC), Mobile Edge Computing, and Mobile Cloud Computing (MCC), within which a standard taxonomy is provided to explore novel mechanisms.

Nikravan et al. [54] presented a rigorous overview of Fog-Edge-Cloud (FEC) trust maintenance schemes. To that aim, selected FEC trust management options are divided into three broad categories: architecture, algorithm, and model/framework. Furthermore, this study reviewed and contrasted the FEC trust managing systems based on their advantages and disadvantages, evaluation methodology, tools and simulation settings, and key trust measures. Finally, certain unresolved concerns and anticipated trends for future investigations are mentioned.

Bréhon–Grataloup et al. [55] studied the deployment issues of MEC in vehicular networks. The study characterized the contemporary Vehicle-to-Everything (V2X) designs to reveal the techniques working behind their enhanced performance: network accessibility and coverage, communication reliability, massive data processing, and workload offloading. Finally, it highlighted unresolved difficulties and obstacles that must be addressed before reaping the full advantages of this paradigm.

Lin et al. [56] offered a detailed review of previous and recent developments in research areas relevant to offloading models in edge computing. Furthermore, the study identified and discussed various research prospects and obstacles in the field of edge computing task offloading models.

Shakarami et al. [57] presented an overview of the ML-based computational task offloading techniques in the MEC ecosystem. In this sense, it studied classical hierarchical structures to identify current mechanisms on this critical topic and identified unresolved challenges. Furthermore, the survey concluded with an argument about unresolved challenges and unexplored or insufficiently addressed future research tasks.

Ray et al. [58] studied the critical role of edge computing technologies in IoT. First, it described the taxonomical categorization and evaluated the industrial elements that can be benefited from both edge computing and IoT, followed by a detailed discussion of each taxonomical element. Secondly, the study described two use cases in which the edge-IoT model recently combined to tackle urban smart living difficulties. Thirdly, it proposed a unique edge-IoT framework for e-healthcare, known as EH-IoT, and created a demonstration testbed. The test findings indicated encouraging benefits in terms of reducing reliance on IoT cloud storage or analytics.

Iftikhar et al. [59] conducted a Systematic Literature Review, also known as an SLR, using standard review methods to examine the function of Artificial Intelligence (AI) and Machine Learning (ML) algorithms and the problems in their application for resource administration in fog/edge computing settings. Several Machine Learning, Reinforcement Learning, and Deep Learning strategies for managing edge AI have been addressed. Furthermore, the work discussed the history and current state of AI/ML-empowered Fog/Edge Computing. Furthermore, a hierarchy of AI/ML-empowered approaches to resource management for fog/edge technology has been suggested, and current solutions have been compared using the proposed taxonomy. Finally, remaining difficulties and intriguing future research topics in AI/ML- empowered fog/edge computation have been highlighted and explored.

Gill et al. [60] explored current research and probable future paths for AI/ML, cloud computing, and quantum computation. Furthermore, the work examined the challenges and potential for exploiting AI and ML for next-generation computation environments such as edge, fog, cloud, quantum computation, and serverless computing.

There are several similar sorts of literature available in scholarly databases such as IEEE Xplore, Science Direct, Springer Link, ACM Digital Library, etc. relative to this survey. However, this work focused on enhancing the existing literature by including an overview of contemporary advanced enabling and supporting technologies. This survey tried to cover notable enabling and supporting technologies for MEC which are not covered or limitedly overviewed in prior works. The work moreover included an overview of security issues and state-of-the-art preventive mechanisms, which is limitedly included in the existing literature. Through this literature review, one can obtain an insight into the MEC and most recent relative technologies. Moreover, the review of existing works will be assistive to figure out the advancements provided by this work. Table 1 includes a comparison between this survey and the mentioned prior survey or review works. Through the table, a better insight of the extended contribution of this survey can be obtained.

Motivations: The motivations behind performing this survey work are mentioned in the following:

- An up-to-date insight into the state-of-the-art advances of MEC technology is frequently required to readily observe contemporary progress.
- Computation and communication resource allocation for MEC is an ever-challenging issue. Therefore, up-to-date improvements relative to these mentioned terms are required. Since, literature on Game Theory and Auction Theory-based computation offloading and resource allocation is limited more and more investigations and discussions on these methodologies should be included in the novel works and literature. As well as, the deployment of open-source frameworks in the context of MEC for the forthcoming networking technologies such as beyond 5G/6G should be discussed. Moreover, novel multiple access schemes such as the adoption of Rate Splitting Multiple Access (RSMA) which is considered to be a significant role player for 6G wireless communications should be examined in terms of MEC.

- A brief overview of modern technologies such as Heterogeneous Cloud-Radio Access Networks (H-CRAN), Simultaneous Wireless Information and Power Transfer (SWIPT), Intelligent Reflecting Surfaces (IRSs), Digital Twins, passive optical networks (PON) and their evolving integration in MEC infrastructure is required since in previous literature the descriptions of such technologies in terms of MEC are limited or even not present.
- Security is one of the significant concerns for the MEC infrastructure; therefore, sophisticated research is required relative to MEC security.
- Evolving challenges and research directions should be devised as per advancement or progress of the MEC services.

Table 1: Comparison table

Survey Topics	This Work	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[27]	[28]	[29]
Fundamentals & Techs.											
Fundamentals	√	√		√	√		√	√	√		√
Relative technologies	√	√					√		√		√
Standards and Archi.											
Standardization	√							√			
Architecture	√			√	√		√		√	√	
MEC in 5G	√	√						√			
Enab. Techs.											
Virtual Machines	√								√		
Container	√								√		
SDN	√			√							
NFV	√			√							
Network Slicing	√										
ICN	√			√				√			
SFC	√			√							
C-RAN	√			√							
F-RAN	√			√							
H-CRAN	√										
D2D	√										
AI/ML	√	√	√			√			√		√
Features											
Computation Offloading	√	√	√	√		√	√		√	√	
Communications	√	√		√			√	√	√	√	
Caching and Content Delivery	√					√				√	
Supp. Techs.											
NOMA	√										
RSMA	√										
UAV	√										
SWIPT & EH	√										
IRS/RIS	√	√									
Game Theory	√										
Auction Theory	√										√
Digital Twin	√						√				
OS MEC for 6G	√										
Quantum comp.	√										
PON	√										
Usage Case	√			√	√		√	√		√	
Security											
Security issues	√	√									
Solutions	√	√									
Issues & Dir.	√	√	√	√	√		√	√		√	√

Table 1: Comparison table (continued)

Survey Topics	This Work	[30]	[31]	[32]	[33]	[34]	[35]	[36]	[37]	[38]	[39]
Fundamentals & Techs.											
Fundamentals	√	√	√	√	√	√	√		√	√	
Relative technologies	√		√			√	√		√		
Standards and Archi.											
Standardization	√									√	√
Architecture	√	√			√		√	√		√	
MEC in 5G	√								√	√	√
Enab. Techs.											
Virtual Machines	√										
Container	√										
SDN	√										
NFV	√										√
Network Slicing	√									√	
ICN	√										
SFC	√										
C-RAN	√										
F-RAN	√										
H-CRAN	√										
D2D	√										
AI/ML	√	√		√							
Features											
Computation Offloading	√		√	√			√		√		
Communications	√						√				
Caching and Content Delivery	√		√				√		√		
Supp. Techs.											
NOMA	√										
RSMA	√										
UAV	√										
SWIPT & EH	√										
IRS/RIS	√										
Game Theory	√										
Auction Theory	√		√			√					
Digital Twin	√										
OS MEC for 6G	√										
Quantum comp.	√										
PON	√										
Usage Case	√		√				√		√		
Security											
Security issues	√	√			√			√	√		
Solutions	√	√			√			√			
Issues & Dir.	√		√	√	√		√	√		√	

Table 1: Comparison table (continued)

Survey Topics	This Work	[40]	[41]	[42]	[43]	[44]	[45]	[46]	[47]	[48]	[49]
Fundamentals & Techs.											
Fundamentals	√	√			√	√	√	√	√	√	√
Relative technologies	√						√				
Standards and Archi.											
Standardization	√					√					
Architecture	√				√	√	√			√	
MEC in 5G	√	√									
Enab. Techs.											
Virtual Machines	√										
Container	√										
SDN	√	√									
NFV	√	√									
Network Slicing	√	√									
ICN	√										
SFC	√										
C-RAN	√										
F-RAN	√										
H-CRAN	√										
D2D	√										
AI/ML	√							√	√	√	
Features											
Computation Offloading	√	√	√				√			√	√
Communications	√	√	√			√	√		√	√	√
Caching and Content Delivery	√	√	√								
Supp. Techs.											
NOMA	√										
RSMA	√										
UAV	√							√			
SWIPT & EH	√										
IRS/RIS	√									√	
Game Theory	√			√							
Auction Theory	√										
Digital Twin	√										
OS MEC for 6G	√										
Quantum comp.	√										
PON	√										
Usage Case	√			√	√				√	√	√
Security											
Security issues	√		√					√		√	√
Solutions	√		√					√		√	
Issues & Dir.	√		√			√	√	√	√		√

Table 1: Comparison table (continued)

Survey Topics	This Work	[50]	[51]	[52]	[53]	[54]	[55]	[56]	[57]	[58]	[59]	[60]
Fundamentals & Techs.												
Fundamentals	√	√		√	√	√		√		√	√	√
Relative technologies	√	√			√	√		√		√	√	√
Standards and Archi.												
Standardization	√											
Architecture	√			√		√		√	√			
MEC in 5G	√	√										
Enab. Techs.												
Virtual Machines	√	√						√				
Container	√							√				
SDN	√	√				√						
NFV	√	√				√		√				
Network Slicing	√											
ICN	√											
SFC	√											
C-RAN	√	√										
F-RAN	√											
H-CRAN	√	√										
D2D	√											
AI/ML	√	√	√					√	√		√	√
Features												
Computation Offloading	√	√	√		√		√	√	√		√	
Communications	√	√	√			√	√	√		√		
Caching and Content Delivery	√	√									√	
Supp. Techs.												
NOMA	√	√										
RSMA	√											
UAV	√	√	√									
SWIPT & EH	√	√										
IRS/RIS	√											
Game Theory	√											
Auction Theory	√											
Digital Twin	√											
OS MEC for 6G	√											
Quantum comp.	√											√
PON	√											
Usage Case	√	√		√			√			√	√	√
Security												
Security issues	√	√	√			√		√				
Solutions	√		√			√						
Issues & Dir.	√		√	√		√	√	√	√	√	√	√

Contributions: The notable contributions of this survey work are highlighted below:

- The work reviewed (41 papers) and briefed up-to-date literature (till 2023) to provide a better insight into the present studies on the MEC paradigm (includes both mobile edge computing and multi-access edge computing, however mainly focused on multi-access edge computing).
- It included a brief overview of relative computing paradigms such as cloud computing, nomadic computing, mobile cloud computing, and edge computing technologies such as cloudlet computing, mobile ad hoc cloud computing, fog computing, mist computing, dew computing, osmotic computing, and MEC.
- Standardization, ETSI MEC reference architecture, and the integration of MEC in 5G network infrastructure (with a brief of 5G-SBA-MEC architecture) are overviewed and briefed.
- State-of-the-art enabling technologies for MEC including clouds, Virtual Machines, Containers, Software Defined Networking (SDN), Network Function Virtualization (NFV), network slicing, Information-Centric Networking (ICN), Service Function Chaining (SFC), radio access control such Cloud-RAN (C-RAN), Fog-RAN (F-RAN), and H-CRAN, Device-to-Device Communication (D2D), machine learning and artificial intelligence approaches are discussed.
- Requirements and recent advances in the computation offloading, communications, caching, and distributed content delivery approaches are described to provide a brief insight.
- Contemporary or advancing supporting technologies for MEC, namely, multiple access techniques such as Non-Orthogonal Multiple Access (NOMA) and RSMA, deployment of UAVs, energy harvesting and SWIPT, implementation of IRSs, Game Theory, Auction Theory, adoption of Digital Twin technologies, open-source framework (open-source MEC), quantum computing, integration of PON, etc. are discussed.
- System-aware and user-oriented vast deployment scenarios of MEC are briefed.
- A brief description of security issues or challenges relative to MEC infrastructure such as edge networking level, access network level, core infrastructure level, edge device level, MEC system level, and MEC host-level threats are provided. Moreover, relevant contemporary threat prevention mechanisms against security issues are overviewed.
- The survey finally mentioned several evolving challenges and research directions relative to the ubiquitous MEC paradigm such as standardization (in terms of forthcoming networks, i.e., 6G), energy consumption, efficiency and scalability of mobility management network functions, MEC service orchestration and programmability, multiple-MEC coordinated collaboration, offloading decision, user experience and bandwidth tradeoffs, security, space-air-ground integrated network (SAGIN) and MEC, edge intelligence, etc.

3. Relative Computing Services and MEC

3.1. Cloud Computing

Cloud computing is a paradigm for expanding ubiquitous and on-demand transmission accessibility to shared infrastructure [61]. Cloud data centers (supplied by cloud vendors such as IBM, Google, Amazon, Microsoft, etc.) provide virtual facilities that are widely accessible, extensible, and dynamically reconfigurable; this reconfigurability enables cloud computing to deliver solutions adopting a pay-according-to-usage pricing system. Users may quickly access remote computational facilities and data processing services using the pay-according-to-usage pricing system, and clients are simply charged for the number of services they utilize. The cloud provides Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) functionalities. Developers can employ many different services depending on the needs of the apps they create. The goal of cloud computing at first was to provide users with access to computational resources for ubiquitous computing. Despite cloud computing technology having aided in accomplishing this goal, accessing cloud-based services may take a longer processing time and which is not viable for some vital applications or services demanding very low latency. Because of the expanding growth of mobile devices and the volume of data produced at the edge of the network, cloud services must be located near the place where the data is produced. Due to the increased need for higher bandwidth, reduced latency, spatially dispersed, and privacy-aware content, computing models that may be deployed in the close vicinity of connected devices are required to satisfy the aforementioned demands. Edge computing has indeed been presented as a solution for those requirements. Following that, this work described and compared several computing concepts [62].

3.2. Mobile or Nomadic Computing

The evolution of cloud computing has been impacted by the evolution of mobile computing (MC) [63]. In the case of mobile computing (also known as the nomadic computing [64], [65] paradigm), computing is conducted using mobile and portable equipment. Pervasive context-aware services, for example, location-based reminders, are examples of mobile computing.

The decentralized computing infrastructure of mobile computing is advantageous. Mobile devices may function in dispersed places because of their framework. However, mobile computing has numerous limitations such as inadequate resource limitations, transmission latency, the equilibrium between individuality and reliance or interoperability (common in all decentralized systems), and mobile clients' requirement to seamlessly adapt to frequently changing scenarios. Because of these constraints, mobile computing is generally not suited for programs with low latency or resilience requirements or apps that create, analyze, and store significant volumes of data on devices.

Fog and cloud technology have expanded the extent and accessibility of mobile computing [66]. In cloud and fog computing paradigms, the processing is not restricted to a local networking system. Mobile computing simply necessitates the use of mobile device hardware.

Nevertheless, fog and cloud processing require more powerful hardware as well as virtualization capabilities. Mobile computing integrity should be provided by protecting mobile devices. Mobile computing has limited capabilities than fog and cloud technology; however, recent developments in wireless interfaces and mobile technology have significantly narrowed this gap.

3.3. Mobile Cloud Computing

Mobile Cloud Computing technology (MCC) [67] is the integration of mobile computation with cloud services in which data computation and storing occur in the cloud away from mobile devices. MCC is concerned with the interaction between cloud platform vendors and cloud service customers [68], [69].

MCC allows resource-constrained user devices to access the vast capabilities of cloud computing. The majority of MCC processing has gone from user devices to the cloud. MCC can execute programs with intense computations and extends the battery life of mobile devices. MCC has utilized the advantage of the specifications and capabilities of both cloud and mobile computing. In MCC, computing facilities are highly available due to the use of a mix of cloud computing and mobile computing, as opposed to mobile computing which is resource restricted. This is advantageous for applications requiring a high level of computing, such as mobile augmented and virtual reality. Cloud-based solutions are far more accessible in MCC than mobile computing. Although user devices can do computing in MCC, MCC depends on cloud services to execute high-computation operations. MCC provides privacy on mobile devices as well as the cloud.

MCC is subject to the same constraints as the cloud and mobile computing technologies. MCC is based on a centralized design that may not be suitable for applications that require high prevalence. Moreover, enabling cloud-based capabilities in both cloud technology and MCC requires a Wide Area Network (WAN) connection; hence, applications operating on these platforms must be constantly linked to the Internet, posing connectivity difficulties. Moreover, as previously noted, offloading processing to the cloud causes excessive latency, which is incompatible with delay-sensitive activities.

3.4. Edge Computing

Edge computing [70] has improved storage, supervision, and processing capabilities of data produced by linked devices. Edge computing, contrary to MCC, has now been positioned near the end-devices at the network's edge. Edge computing technology, as per description of OpenEdge Computing, performs processing at the network's edge using tiny data centers near consumers [71]. The primary goal of edge computation is to offer computational and storage facilities in the close vicinity to the users in a ubiquitous manner. Edge computing technology is a critical computing paradigm for end devices in which data is filtered, preprocessed, and aggregated utilizing cloud centers located near end devices. The following are the primary benefits of edge computing [72]:

The Reduction of Latency: Because of its closeness to clients, edge computing has lower latency than MCC and cloud technology. Yet, if the local processing unit is insufficiently powerful, the delay in edge computing might be greater than it is in the cloud and MCC services.

Increased System Performance: Attaining millisecond-level data analysis is the most crucial feature of edge computing. Edge computing minimizes total system latency and transmission bandwidth consumption while improving overall system effectiveness.

Enhanced Privacy and Security: Integrated cloud service providers supply their clients with a complete system of unified data intrusion prevention solutions. Yet, if centrally stored data is disclosed, significant consequences will emerge. The edge computing framework, for instance, enables the deployment of the most relevant security precautions locally (at a local edge computing server). Therefore, the majority of the computation may be conducted on the network's edge, comparatively with a lower volume of data. As a result, it decreases the danger of information leaks during transmissions and the quantity of data retained on the cloud service, lowering security and privacy issues.

Enhanced Service or Resource Accessibility: The accessibility of resources in edge computing is also improved. Edge computing, in comparison to MCC, incorporates tiny data centers, whereas MCC does not comprise a data center. As a result, service availability is greater with edge computing. Moreover, since edge computing may construct hybrid peer-to-peer and cloud services paradigms, it benefits from greater processing capabilities than MCC.

Minimize Operating Expenses: Directly moving data into a cloud system imposes significant operational expenses for data transmission, adequate bandwidth, and latency factors. Edge computing, on the other hand, can minimize data uploading volume; as a result, data transfer volume, bandwidth usage, and latency will be lowered, lowering operating expenses.

Resiliency to Connection Issues: When some computational activities can be performed immediately on the edge, services are not impacted by restricted or inconsistent network connectivity. This is especially useful for executing programs in remote environments with limited network access. It can also help to lower the high expenses associated with networking solutions such as cellular technology.

3.4.1. Cloudlet Computing

Carnegie Mellon University presented the very first edge computing idea in 2009, putting computation/storage near user devices [73]. In certain research, cloudlet is termed as a micro data center (MDC). The cloudlet [74] concept is based on strategically positioning a server or a group of servers with trustworthy high capacities and processing power, as well as a robust Internet connection, near edge devices to offer both storage and computing capacity for such nearby UDs. Cloudlets constitute small-scale data warehouses (miniaturized clouds) that are typically one hop away from user devices. Cloudlet computing offloads computations from user devices to virtualized machine (VM)-based cloudlets located at the network's edge [75].

Cloudlet is a miniature cloud located around user devices. Cloud solution providers who intend to deliver accessible services close to mobile devices might be named as cloudlet technology operators as well. Cloudlets can also be facilitated by telecom operators such as AT&T and others, with virtualization capability positioned close to end or user devices. Cloudlets typically have small-scale hardware sizes in contrast to massive data facilities in cloud computing. Since cloudlets are smaller in size, computational resources are more modest, but energy consumption and latency are lower compared to cloud computing.

One limitation of cloudlet technology is that accessibility is only gained through Wireless Local Area Network (WLAN) connections, and mobile devices need to toggle between the WLAN and cellular network to obtain cloudlet services. Moreover, cloudlets are not necessarily an intrinsic component of the cellular network, and WLAN generally offers local service with restricted mobility support, making it difficult to achieve an acceptable service quality for mobile user devices.

Cloudlets and mobile cloudlets are identical concepts. In the context of mobile cloudlets, the cloudlets are termed as a cluster of nearby interconnected mobile devices. In which they communicate with each other through wireless communication technologies, for example, by Bluetooth or WLAN. These devices can be suppliers or customers of computing services.

3.4.2. Mobile Ad Hoc Cloud Computing

MCC is widespread; however, it is ineffective without centralized clouds. Ad hoc mobile connectivity is a transient and dynamic system of nodes formed by routing and transmission protocols. The most dispersed kind of system is Mobile Ad Hoc-Based Cloud Computing (MACC) [76]. Mobile devices generate a very dynamic network structure in MACC; system adaptation is required for additional devices to often leave/join the system. Ad hoc mobile devices may also form clouds to support communication, storage, and computation. The application scenarios of MACC include unmanned vehicular technology, group live video broadcasting, sensor networks [76], [77], [78], etc.

In the case of cloudlets, virtualized computation by Virtual Machines is necessary, whereas it is not required in MACC. Both cloudlet technology and MACC offer mobility; but, real-time IoT services are not feasible in resource-constrained MACC. Computations in the cloudlet have been distributed among cloudlet nodes located near mobile devices to provide local services to mobile clients.

Since MACC resources are ad hoc in nature [79], it is fundamentally different from cloud services. Mobile devices in MACC serve as storage devices, data or content providers, and computational devices. Due to the confined network infrastructure, they also govern traffic routing among each other. As localized resources (by end devices) have been integrated to form an ad hoc cloud, MACC may provide high computation capacity. In centralized cloud services, these characteristics are distinctive in terms of clients, connectivity, and architecture [80].

3.4.3. Fog Computing

Fog computing is another kind of edge computing [81]. Cisco launched the fog computing framework (termed as "fog" in several researches) in 2012 to facilitate the processing of tasks for user devices at the network's edge [82]. Decentralization of the cloud computing infrastructure deploying fog is done by offering the computation or task processing features between the cloud and edge devices. This brings content, computing, storage, and services near the user devices where the data has to be processed. This enables the formation of fog outside the cloud infrastructure and a reduction of data transmission latency.

The primary distinction between fog and cloud computing is the size of the hardware elements associated with these computing paradigms [83]. Cloud technology provides highly accessible computational facilities with comparatively high power consumption, whereas fog computing offers intermediate accessible computing resources with reduced power usage. With cloud computing, massive data centers are often used, but in fog computing, smaller servers, gateways, routers, switches, set-top devices, or access nodes are used. Since fog computing hardware consumes relatively lesser area than cloud computing hardware, it may be positioned closer to consumers. Fog computing is accessed through linked devices from the network edge to the core of the network, whereas cloud computing is accessed through the network core. Moreover, fog-based services may operate without constant internet access, implying that the services can function independently, with essential updates being delivered to the cloud whenever there is a network connection. In cloud technology, however, devices must be linked to the network while the cloud platform is operating.

Computing, connectivity, storage, management, and decision-process have been dispersed closer to devices in fog, allowing them to supervise, analyze, interpret, evaluate, and respond more effectively. Fog computing has the potential to improve many industries, including energy, industry, transport, healthcare, intelligent cities, and so on.

When fog is contrasted with MACC, MACC is better suited for extremely dispersed and dynamic networks where there is no network connection. Because linked devices in MACC are primarily decentralized, they form a more flexible network.

Cloudlet computing technology, on the other hand, works effectively with the mobile or dynamic cloudlet structure, but fog computing can accommodate massive quantities of traffic; moreover, resources in the fog may be situated anywhere along the device-to-cloud path.

Although both execute storage and computation on the edge of the network near end users, fog computing and edge computing are distinct concepts. The OpenFog Consortium [84], [85] defines this separation by the hierarchical structure. Fog computing allows computation, communication, storage, management, and acceleration anyplace along the cloud server-to-things channel or path; while, the processing is only conducted at the edge of the network in the context of edge computing.

The main disadvantage of the aforementioned edge computing ideas (cloudlet, ad hoc clouds, and fog computing) is that typically, they are not incorporated into the framework of a wireless network; hence, QoS and the quality of experience (QoE) for end users are not assured. The cloud radio or wireless access network (C-RAN) is one notion that can combine cloud services into a wireless network [86]. The C-RAN employs the concept of a dispersed protocol stack, shifting some levels of the protocols to the central baseband unit (BBU) from dispersed remote radio heads (RRHs).

Fog RAN/F-RAN [87] is a type of fog computing framework that may also be integrated with wireless communication technologies. F-RAN and C-RAN are both suitable to be deployed within the base stations of wireless networks; these can be utilized in 5G-related wireless technology implementations and are significantly energy efficient.

3.4.4. Mist Computing

Mist computing [88] is recently introduced, which represents decentralized cloud or computing technology at the farthest edge of linked devices. Mist computation is the first computing step in the IoT-fog-cloud chain; it is colloquially known as "IoT computation" or "things computation." An IoT device might be a wearable smartwatch, a smartphone, an intelligent fridge, or any smart device. Mist computing technology is the extension of computation, storage, and networking over the fog via objects. Mist computation is a subset of MACC because the communication in the mist is rarely ad hoc.

According to research, mist computing technology can minimize the strain in existing WLAN networks for video broadcasting applications, protect users' confidentiality through local processing, and quickly deploy virtualized implementations on single-board computer systems.

Apart from the computing paradigms discussed earlier, the cloud of things and edge clouds are two more related computing paradigms described in various works.

3.4.5. Dew Computing

Dew computing technology is a computing paradigm that first appeared in 2015 [89], [90]. This kind of computing is concerned with the establishment of collaborative connectivity between Cloud Services and end-user devices. This integration enables resources to be transferred between two devices or components based on network circumstances.

3.4.6. Osmotic Computing

Osmotic computation is an emerging computing typology that enables efficient IoT application processing at the edge of the network [91]. Such a paradigm is based on the requirement to connect micro-cloud services provided at the edge with the massive-capacity cloud servers. Osmotic computation is identified by the connection of edge, fog, and cloud computing enabling the smooth and free flow of micro services among them [92].

3.4.7. Multi-Access Edge Computing

As per ETSI standardization, MEC is indeed a platform that provides features for cloud processing and an IT customer experience within RAN (namely at the cellular edge) of wireless networks for users.

In the context of MEC, edge computing capabilities can be integrated into existing base stations by RAN operators besides other available options of edge-level deployments. MEC computing systems are compact and have virtualization capabilities. Due to the nature of hardware (limited capacity), accessible computing capabilities in MEC are limited as compared to cloud computing.

Additionally, MEC can serve low-latency services along with delay-sensitive crucial applications [93]. MEC services provide mobile users with tailored and contextualized experiences because they leverage real-time networking information.

Networking of MEC has been established by WLAN, wide area network (WAN), or mobile networks. MEC mainly focuses on RAN-based communications infrastructure operators. The 5G and beyond communication infrastructure is expected to help MEC greatly since it can handle a wide range of mobile devices with reduced latency and greater bandwidth [94]. Moreover, SDN and NFV as well facilitate MEC capabilities.

Table 2 contains the technical features or brief description, advantages, and disadvantages of the aforementioned computing paradigms.

Table 2: Technical features, advantages, and disadvantages of the computing paradigms

Computing Paradigms	**Technical Features/Description**	**Advantages**	**Disadvantages**
Cloud Computing	• Centralized deployment • Accessible through WAN • SaaS, PaaS, and IaaS functionalities • Data processing happens far away from users • Multiple hops away	• Massive computation capacity • Dynamically reconfigurable • Ubiquitous computing • Massive storage capacity	• Higher latency • Requires higher bandwidth • Threat of massive data loss at the time of security failure • Higher deployment cost
Mobile or Nomadic Computing	• Computing is conducted using mobile and portable equipment • Context-aware services, e.g., location-based reminders • Decentralized deployment • Typically accessible through WAN	• Dispersed computing facilities	• Computational resource limitations • Transmission latency • Equilibrium between individuality and reliance or interoperability • Adaptability for users • Limited storage capacity • Requirements of sophisticated hardware at user end
Mobile Cloud Computing	• Integration of mobile computation with cloud services • Allows access to the vast capabilities of cloud computing • Centralized deployment • Typically accessible through WAN	• Offers capabilities of both cloud and mobile computing • Highly available due to the mix of cloud and mobile computing • Advantageous for mobile augmented and virtual reality	• Higher latency compared to the mobile or nomadic computing (cloud-dependent) • Constant internet link is required • Ineffective without centralized cloud
Cloudlet Computing	• Also termed as micro data center (MDC) • Cloudlets constitute small-scale data warehouses • Typically one hop away • Distributed deployment • Computation/storage near the user devices • Accessible through WiFi/WLAN • Private facility • Offloads computations to virtualized machine	• Latency-awareness • Energy consumption and latency are lower compared to cloud computing • Supports mobility	• Limited mobility since it is only accessible through WLAN/WiFi • Usually not incorporated into wireless networks
Mobile Ad Hoc Cloud Computing	• Decentralized/distributed • Forms device cluster and share computational resources • Mobile in nature • Virtual computation is not required in MACC like cloudlets	• Highly mobile • Transient and dynamic	• Real-time services, e.g., IoT are not feasible in resource-constrained MACC • Usually not incorporated into wireless networks

Table 2: Technical features, advantages, and disadvantages of the computing paradigms (continued)

Computing Paradigms	Technical Features/Description	Advantages	Disadvantages
Fog Computing	• Decentralized/distributed • Private deployments • Accessible through wireless access points • Intermediate accessible computing with reduced power • May operate without constant internet access • One hop away	• Latency-awareness • Lower energy consumption • Accommodate massive quantities of traffic than cloudlets • Low cost	• Flexibility is lower than the MACC • Usually not incorporated into the wireless networks, however, can be integrated via Fog-RAN • Certain security concerns
Mist Computing	• Decentralized/distributed • First computing step in the IoT-fog-cloud chain • Colloquially known as “IoT computation” or “things computation” • Accessible through WLAN	• Latency-awareness • Lower energy consumption • Confidentiality through local processing • Virtualized implementations on single-board computer systems • Highly suitable for IoT and sensor networks	• Limited computational capacity • Typically storage facilities are not readily available
Dew Computing	• Decentralized but dependent on central cloud • Collaborative connectivity between Cloud Services and end-user devices	• Offers certain cloud facilities to the edge	• Limited computation capacity • Dependency on central cloud • Usually requires a reliable connectivity • Typically storage facilities are not readily available
Osmotic Computing	• Decentralized/distributed • Enables efficient IoT application processing at the edge • Connects micro-cloud services with the massive cloud servers • Identified by the connection of edge-fog-cloud enabling the smooth flow of micro services among them	• Suitable for IoT services • Latency-awareness • Lower energy consumption	• Limited computational capacity • Typically storage facilities are not readily available
Multi-Access Edge Computing	• Decentralized/distributed • Mostly accessible through WAN or cellular networks • Typically implemented in RAN. However, there are other few options of implementation. • Offers highly near user computing facilities	• Latency-awareness • Lower energy consumption • End-user friendly • Tailored experiences leveraging real-time network information • Computational and storage facilities near the user premises • Has virtualization capabilities • Reduced threat of information leaks during transmissions due to the lower volume of data	• Computing and storage capabilities are limited than cloud computing • Certain security issues

4. **MEC Standardization and Architecture**

4.1. Standardization

ETSI authored the implementation of MEC technology in the networking functions virtualization (NFV) architecture in February 2018 [95], [96]. Furthermore, ETSI released use instances and requirement standards on MEC in October 2018 which includes an annex outlining sample use cases and associated technical benefits. ETSI has released the MEC frameworks and reference architecture definition, which explain the functional parts and the points of reference amongst them, as well as several MEC services. ETSI released the Proof of Conception (PoC) model in July 2019, which was approved by the MEC ETSI ISG. Moreover, ETSI published a paper regarding MEC-5G integration [97].

MEC allows applications to be implemented as software-only units that operate on the upper end of a virtualized environment placed near the edge of the network. ETSI MEC's infrastructure contains system-, host-, and network-level/tier/layer elements [98]. The networks-level enables connectivity to a range of resources, while the host level offers the virtualized framework and MEC architecture, allowing MEC applications to be executed. The system-level administration offers an overview of the base MEC system, allowing user devices and third-party partners to get access [99].

Moreover, D2D transmission is direct connectivity between two mobile devices that do not require the usage of the network core or access points, or base stations. End devices' resource exchange has been examined using D2D-aided MEC [100]. The combination of MEC and D2D can boost the computation capability of cellular networks by assisting end devices with processing and storage capabilities to interact with traditional MEC architecture. Typically, end devices, small cell base stations, and a macro cell base station comprise the D2D-aided MEC infrastructure. In this instance, the end devices can delegate work to a neighboring MEC or a cluster of D2D nodes.

4.2. ETSI MEC Reference Architecture

Low latency, closeness, position awareness, high throughput, and real-time exposure to radio network parameters are distinguishing properties of the MEC framework. These features enabled expedited content delivery functions and applications to be supplied reasonably close to end users or subscribers at the edge of the wireless network. The satisfaction of mobile subscribers may be considerably increased by more effective network and service management, greater service quality, decreased data transportation expenses, and lowered network congestion. Fig. 2 illustrates the ETSI MEC framework.

The MEC reference model [101], [102] features are briefly described below:

MEC Host and Communications System: The control process of the MEC standard design represents the host layer. It consists of MEC host (MEH) and host maintenance entities. The MEH is made up of the MEC platform, services, and Virtualized Infrastructure. The Virtualized Infrastructure hosts MEC services and applications by providing the computation, communication, and storage resources. The network layer connects the external and internal elements.

MEC Platform: The MEC platform enables MEC services to be hosted as operations on the virtual platform. According to the request of the MEC system controller, the MEC platform is also accountable for the initialization and suspension of MEC applications.

MEC Supervisor: The MEC orchestrator or supervisor is a system-level managing layer that consists of a platform administrator and a Virtualized Infrastructure Manager (VIM). Its core duties include applications and services provisioning using virtualized MEC resources, MEC resource information maintenance, such as topologies, available MEH services and resources, and security and authentication checks for MEC applications. The MEC orchestrator or supervisor is also in charge of policy execution.

Operation Support or Assistance Sub-System: Operation Support Subsystem (OSS) is in charge of providing permission to user subscription queries submitted by User Equipment (UE) through the application-level coordination and management gateway.

Fig. 3 depicts the ETSI MEC reference architecture.

4.3. Integration of MEC in 5G Network Infrastructure

MEC is seen as a crucial enabler, allowing operators to incorporate application-oriented features into their networks. This will enable operators and service vendors to deal with critical latency situations. MEC deployment might be accomplished in a variety of settings where network design and generation have no bearing on the implementation. It is essential to mention that MEC technologies are not confined to 5G, although it is a critical component in enabling and facilitating 5G [103], [104]. MEC is a universal access solution that provides reduced latency wherever necessary, e.g., in situations requiring local interaction, such as automated vehicles [105].

After the introduction of MEC concepts, the ETSI ISG and numerous value chain stakeholders worked hard to formulate MEC standards based on industry agreements. At that moment, the ETSI consortium had 68 affiliates and 35 partners, including not only mobile carriers but also industries, network operators, and institutions such as the University Carlos III of Madrid, Vodafone, Intel, IBM, NTT Corporation, and others [106].

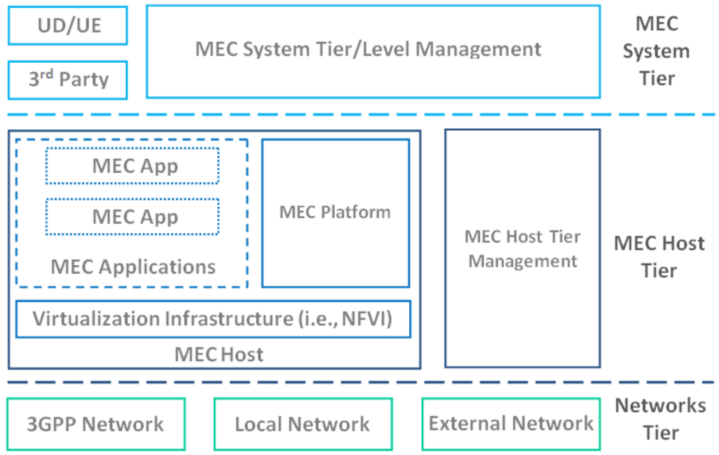

Fig. 2: ETSI MEC framework.

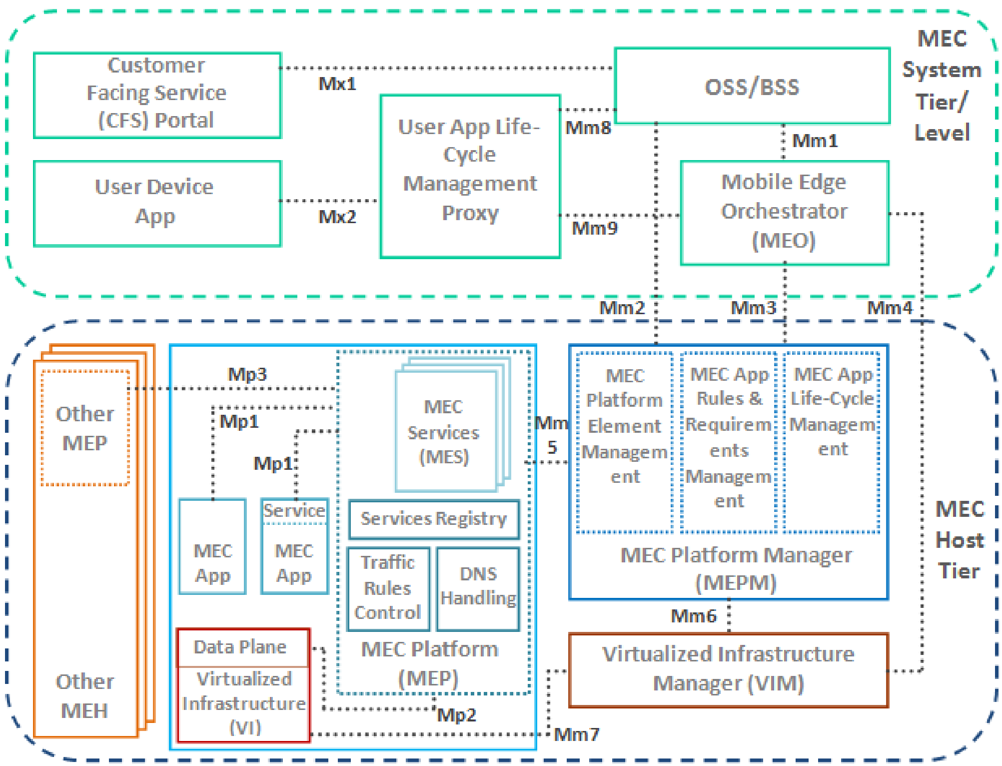

Fig. 3: ETSI MEC reference architecture.

Their participation is crucial for establishing an open and adaptable MEC ecosystem, and MEC benefits a wide range of stakeholder groups, such as mobile network operators (MNOs), developers, over-the-top (OTT) participants, individual application suppliers, network equipment distributors, IT system operators, network operators, and technology companies. The ETSI ISG also released a series of specifications and guidelines focused on topics such as architecture and framework, MEC within the NFV system, and MEC and C-RAN collocation. With the technical framework 3GPP TS 23.501 [107], the 3GPP started introducing MEC in the definition of 5G infrastructure. The 3GPP recently detailed how to install and effectively incorporate MEC into 5G. Fig. 4 visualizes MEC's integration with 5G infrastructure.

One may identify two types of functions in the 5G Service Based/Oriented Architecture (SBA/SOA) suggested by 3GPP [108], [109]: (i) those which utilize one or more services and (ii) others that provide services. The interchange of resources (produce/consume) is dependent on authentication procedures that provide approval or endorsement to the consumers. SBA/SOA enables service access efficiency and flexibility. The request/response paradigm is one of the strategies used for basic and compact service requests. The architecture supports a subscribe/notify approach for lengthy operations to improve the efficiency of sharing services and information across entities. MEC ETSI ISG presents a comprehensive guideline for developing services that facilitate such functions and attributes in MEC. This proposed standard provides the same characteristics for MEC applications that SBA does for network functionalities and related services (enrollment, detection, accessibility, verification and permission, and so on).

The integrated implementation of MEC systems in a 5G environment necessitates the interaction of certain functionalities of MEC in 5G with network functions. Network functionalities and services are recorded within Network Resource Function (NRF) unit, whereas the services generated by requests in MEC are enrolled in the MEC system's service registration portal. For using a service, approval from an orchestrator or authenticator is necessary. Moreover, it allows communications with the network functionality. The Authenticating/Identification Server Function (AUSF) grants this type of permission. The NRF proposes the finding of accessible services. Network Exposure Function (NEF) serves the same purpose as NRF in some circumstances when services need to be reached by exterior and untrustworthy entities. NEF might be viewed as a centralized body for service exposure, approving all types of requests received from beyond the system. Apart from Application Function (AF), NEF, and NRF, there have been a few additional entities or functions worth mentioning. In a 5G system, the Policy Control Function (PCF) unit is in control of policies and regulations such as traffic redirection rules. According to the AF's level of confidence, the PCF might be accessible through NEF or independently. The Unified Data Managing (UDM) function is in charge of several services connected to users and subscribers. It produces credentials to authorize users, manages user recognition, and access controls (such as roaming), records the users' assisting NFs (assisting AMF, Session Maintenance Function (SMF)), and ensures service sustainability through a record for Data Network Name (DNN)/SMF allocations. From the standpoint of the MEC platform, the User Plane Function (UPF) is a decentralized and programmable data plane. As a result, under some deployment circumstances, the local UPF might participate in the MEC implementation [110].

To incorporate MEC in a 5G SBA [111], [112], unique functional facilitators are designed, which may be characterized as follows:

Selection and Re-selection of User Planes: The 5G central network allows UPF selection or reselection for targeted traffic forwarding to the data connection. The UPF preference mechanism parameters are determined by the UPF implementation context and MEC service provider configuration.

Traffic or Packet Forwarding and Steering: In the 5G network, the UPF offers multiple packet routing techniques for MEC operations. Moreover, AFs can influence UPF selection or reselection and provide custom traffic forwarding rules for a single user.

Local Area Packet/Data Network (LAPN/LADN): The adaptability of the UPF placement enables LAPN/LADN functionality. MEC hosts may then be installed on the N6 interface, which connects the UPF to a data connection. Based on LAPN statistics obtained from the AMF, a user adopting MEC facilities may identify LAPN accessibility during the enrollment process.

Sessions and Services Continuity (SSC): SSC functionality is required to facilitate the users' and applications' mobility. The 5G infrastructure enables MEC applications to choose between three SSC configurations. SSC approach 1 in particular offers the user with the consistent network connection, SSC approach 2 may terminate the user's present connectivity before establishing a newer one, whereas SSC approach 3 maintains continuity of service for the subscriber by activating the new user interface before disconnecting the previous one.

Network Capacity Exposure: The 5G framework enables MEC's immediate access to network functionalities as well as indirect accessibility through the NEF. Exposed functionalities include the disclosure of user events, the delivery of user actions to external services, and the disclosure of analytics to third parties.

QoS and Pricing Functions: The QoS and pricing criteria for user traffic or packet directed to the LAPN are defined by the PCF within 5G SBA.

5. Enabling Technologies

5.1. Clouds, Virtual Machines, and Container

Cloud computing delivers large computational capabilities, always-on availability, and easy access while decreasing the necessity for end subscribers to administer, monitor, and facilitate software and hardware. It also features shared pools of resources with dynamic scaling. There are four main technology models available, as well as three service types.

5.1.1. Technology Models

Public Cloud: This type of model is administered by a cloud vendor to give public subscribers access to a set of resources in some kind of pay-per-use manner (i.e., Dell, Microsoft, and Amazon) [113].

Private Cloud: It is entirely owned and administered by a business. To maintain security, privileged access is offered within the corporate network (i.e., Google, Citrix, and RackSpace) [114].

Hybrid Cloud: It is a fusion of both public and private clouds (i.e., IBM, HP, and VMWare) [115].

Community Cloud: It is a cloud resource pool made up of numerous providers that may be shared by a specified group [116].

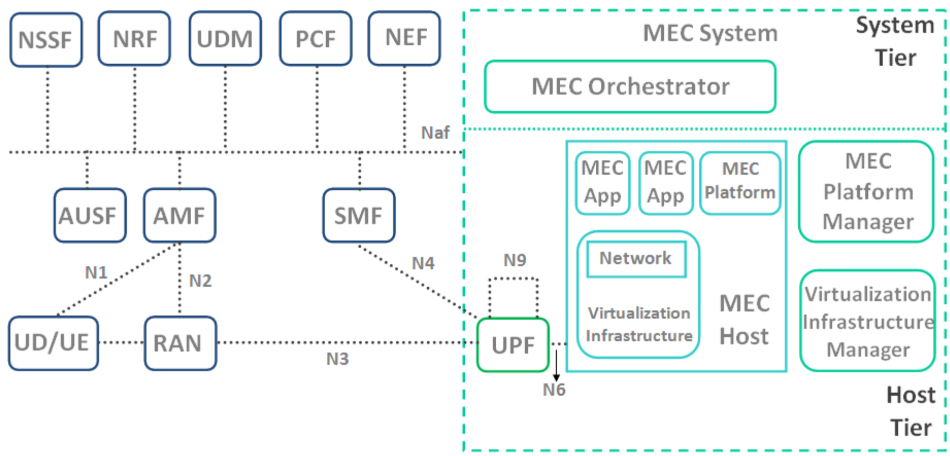

Fig. 4: MEC's integration with 5G network infrastructure.

5.1.2. Service Models

Platform-as-a-Service (PaaS): Users are provided with a platform for designing, deploying, and managing apps (i.e., Azure websites and Amazon Beanstalk) [117]-[119].

Infrastructure-as-a-Service (IaaS): Offers scalable virtualized computing infrastructure, including computation, storage, and connectivity (i.e., Azure VMs, EC2, and Amazon) [119].

Software-as-a-Service (SaaS): Provides cloud-hosted software that is readily available (i.e., Dropbox and Google Sheets) [119].

Virtual Machine: A cloud-based system is often comprised of a cluster of physical devices that constitute a single logical object that may be shared among several players doing discrete isolated tasks or jobs. One method is to use a hypervisor that can generate and run Virtual Machines (VMs) that also can host various processes [120]. Virtual Machines segregation provides users with an isolated environment, i.e., a fully working computer, regardless of the foundational equipment [121]. The VM technology provides fine-grained supervision for initializing and terminating activities and services at any moment without impacting the underlying hardware, allowing for more resource provisioning versatility. Virtual Machine, however, is an artificial construct of physical equipment stack (i.e., virtual BIOS, networking interface, storage, RAM, and CPU) that necessitates a complete guest operating system (OS) image as well as extra packages and modules for hosting services and programs. A Virtual Machine wastes a substantial amount of facilities unless a service or application requires or demands such infrastructure, in addition to its delayed starting time due to booting a full operating system.

Container: In the context of the Containers [122], abstractions occur at the operating system level, supporting applications and libraries, as well as systems resources to operate a particular service or application. Containers split the resources of actual computers, resulting in numerous separate user-space instances that are substantially smaller in size than Virtual Machines. This enables several Containers to run under a single operating system, enabling faster implementation with nearly native efficiency in central processing unit (CPU), memory, storage, and networking. A Container often executes a service or application by enabling quick instantiation and rapid migration benefits owing to its lightweight architecture; however, it is less reliable than Virtual Machines, which can also run several applications more effectively. In actuality, a Container may be orchestrated in milliseconds, but a Virtual Machine might take seconds or even minutes, according to the capabilities of the operating system, actual equipment, and the system workload.

Containers provide a lightweight virtualization approach that enables the portable execution of MEC functions, which is very relevant for mobile consumers [123]. Containers can also help MEC services since they provide methods for rapid packaging and deployment across a wide number of linked MEC platforms [124]. Containers outperform Virtual Machines in the domain of MEC in five ways. First, Containers generate layers of images and extend images to develop and create programs, which are then recorded as images ('.img' system image files) in storage. The Container processor or engine later uses this to execute the program on the host. The engine aids in packaging, distributing, and coordinating, allowing for rapid deployment. Second, Container API supports life-cycle management, which includes building, defining, composing, distributing, and executing Containers. Third, storage is given by connecting one or even more data volume Containers with continuous service. Fourth, networking is accomplished by port mappings, which facilitate Container interconnection. Finally, compatibility for micro services-based architecture (i.e., discrete software packages of a loosely connected service that may be easily mapped to construct a business application according to need) makes containerization easier under the PaaS paradigm.

Docker is the most popular Container technology for facilitating an edge computing context [125]. Containers may also be utilized to replace Virtual Machines, resulting in lower resource use concerning both storage and computation. Moreover, Apache Mesos [126] and Google Kubernetes [127] support the Container cluster management inside dispersed nodes, allowing for quicker scalability.

Regardless of the advantages of Containers, which are more visible in settings with user maneuverability, Virtual Machines may host larger applications or programs or services or a collection of applications or programs or services connected with a specific third-party vendor, ensuring a better level of security. The functionality of Virtual Machines can indeed be advantageous in such circumstances, particularly where service flexibility is not essential, as in corporate and residential networks. Containers, particularly Docker Containers, are intrinsically adaptable and can easily operate within a Virtual Machine [128]. Such Containers may be moved from one Virtual Machine to the other or perhaps to bare hardware without needing substantial effort.

Kubernetes: Docker is responsible for the packing and delivery of applications or services, meanwhile the Kubernetes infrastructure is responsible for scaling, running, and monitoring such applications or services. Kubernetes [129] is also known as a Container operator because it automates the installation, scheduling, scalability, and synchronization of containerized workloads. Kubernetes by itself does not directly execute Containers; rather, single or maybe more Containers are encased in a high-level framework known as pods. Containers within the same pod exchange resources and networks, as well as interact with one another. The Kubernetes cluster's overall design comprises a master or controller and nodes or slaves. The master is in charge of providing the Application Program Interfaces (API) to developers and scheduling cluster deployments, such as pods and nodes. The nodes include the Container runtime, such as a single or more Docker Containers operating within pods, as well as a component called Kubelet [130], which handles connectivity between the master and the node.

OpenStack: Due to its adaptability and diversity, is regarded as one of the best possibilities for supporting 5G MEC usage scenarios. It is an open program that is used to construct both public and private clouds and has strong support for Virtual Machine and Container concepts. OpenStack [131] is sometimes known as a cloud operating system since it maintains and controls massive pools of facilities in data centers such as computation, connectivity, and storage. OpenStack seems to be a massively distributed infrastructural software platform that is utilized in hundreds of data centers across the world. The telecom sector has recently introduced it to improve MEC usage scenarios.

5.2. Network Function Virtualization (NFV)

NFV is a virtualized framework that uses virtual hardware abstraction to separate network services from hardware or equipment. As a result, it is advantageous reusing the technology and infrastructure of NFV [132]. Fig. 5 represents ETSI NFV architectural framework.

The NFV is made up of Virtualized Network Functions (VNFs), underpinning NFV Infrastructures (NFVI) [133] and an NFV Management and Orchestration system (MANO) [134] to offer virtualized network services.

A VNF is generally a software execution of a network operation that is independent of the hardware facilities it employs. The VNFs depend on the NFVI, which obtains the required virtualized facilities (processing, storage, and communication) from the physical resources via the virtualization level. A VNF can be distributed over one or more Virtual Machines, with Virtual Machines segmented on the facilities of a physical host by software packages known as hypervisors.

The NFV MANO is made up of three major parts [135]: the NFV Operator, the VNF Management unit, and the Virtualized/Virtual Infrastructure Manager (VIM). The NFV Operator is the topmost structural layer of the NFV Management and Orchestration system and is in charge of network service development and Lifecycle Management system (LCM). Conversely, the VNF Management units are there in charge of the Lifecycle Management of the VNFs, which are handled separately by the Element Maintenance (EM) systems. A VNF Management unit can support one or more VNFs. Lastly, the Virtual Infrastructure Manager supervises and regulates the NFVI facilities (i.e., processing, communication, inventory of software, storage capacity, and network resources, improving energy efficiency, increasing resources for Virtual Machines, planning and optimization, and a collection of infrastructure fault detection and prevention operations). An NFV-based networking service is made up of an ordered list of VNFs that connect two endpoints and route traffic via them. This combination to deliver an NFV-based networking service is comparable to the specifications of Service Function Chaining (SFC).

The architectural modifications are detailed individually for each one of the two levels (of a MEC infrastructure) for consistency and clarity.

MEC Host Tier/Level: Both the MEC services and the MEC Platform are installed as VNFs upon that host side, whereas the virtualized architecture is implemented as NFV Infrastructures [136], [137]. The NFV Infrastructures, or virtualized infrastructure, may be implemented using a variety of virtualization technologies, including Container or hypervisor-based systems, as well as combining virtualization techniques. The MEC Platform Manager is replaced on the host supervisory end by the NFV-MEC Platform Manager and a VNF Management unit. The NFV-MEC Platform Manager is responsible for the same tasks as the MEC Platform Manager. The VNF Management unit is in charge of managing the Virtualized Network Functions' service life. The Virtual Infrastructure Manager retains its identical capabilities.

MEC System Tier: The MEC Orchestrator (MEO) is overtaken by the MEC Applications Operator as well as an NFV Operator in the NFV-MEC framework. The MEC Applications Operator is responsible for the same things as the MEC Orchestrator [138]. Nevertheless, the MEC Applications Operator delegates resource management and MEC program management to an NFV Operator. The other components are unaffected.

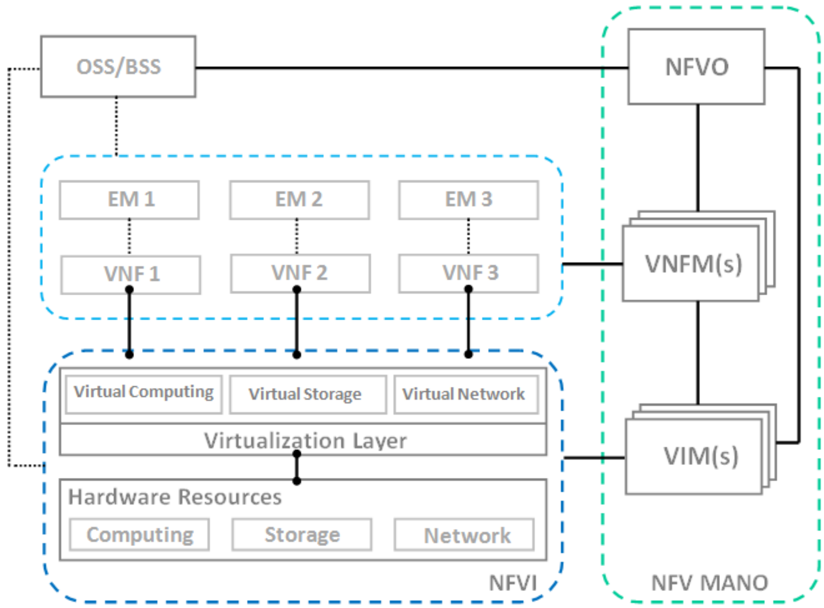

Fig. 5: ETSI NFV architectural framework.

The work identifies the mentioned potential NFV advantages for MEC: (i) reduced OPEX and CAPEX; (ii) more flexibility and rapid implementation of new services.

5.3. Software Defined Networking (SDN)

To install the MEC platform in an NFV context, ETSI proposes a reference design. Also, some alternative designs are presented depending on the SDN framework to enable smooth collaboration across NFV and SDN platforms [139]. Fig. 6 visualizes the SDN-based MEC-NFV architectural framework. While being created for standard NFV infrastructure, these solutions are still applicable in a MEC-NFV context. According to ETSI standards, SDN control strategies can be placed in the MEC-NFV framework in a variety of circumstances (Fig. 6) [140]. An SDN supervisor can be integrated with the virtualized environment supervisor, counted as part of the NFV framework, abstracted as either a Virtualized Network Function (VNF) or integrated into the Base Station Subsystem (BSS)/Operations Support Subsystems (OSS). As a result, SDN control systems are placed in MEC servers to deliver on-demand MEC operations by linking VNFs and managing infrastructure resources interactively (i.e. computation, storage, and connectivity) [140]. MEC enables service operators to provide new sorts of services that necessitate cloud computing resources at the network's edge. SDN improves MEC functionality by recognizing the significance of flexibility in defining policies for where and how data will be processed [141], as well as implementing network services without extra expenditure or hardware change. The work identifies five SDN advantages for the MEC infrastructure: (i) scalability; (ii) accessibility; (iii) resiliency; (iv) interoperability; and (v) flexibility.

5.4. Network Slicing

Network slicing [142], [143] has evolved as a significant idea for delivering an adaptable networking infrastructure that can efficiently serve rising enterprises with different service requirements. It entails dividing a single network into multiple circumstances, each of which is designed and adapted for a particular mandate and/or service/application. According to an important industry statement that explains the network slicing idea, network slicing allows the establishment of several logical, self-contained systems on a single physical infrastructure, providing resource separation and customizable network operations. In other ways, network slicing creates a multi-architecture that supports flexible network resource allocation as well as an adaptive attribution of network services, Radio Access Techniques (RATs), and activities, even with a limited lifespan, allowing for new revenue generation opportunities.
Network slicing facilitates resource sharing across virtual MNOs, processes, and applications by introducing the concept of network slice brokers, which supports network sharing administration and the service exposing capability operation, as detailed in the 3GPP cellular systems [144]. The network slicing, from an infrastructure standpoint, assigns a set of reserved or shared facilities, either real or virtual, to certain occupants by implementing a network hypervisor. To meet the service needs of incoming queries, network slices must integrate a collection of cloud-based and network-based resources, such as bandwidth, networking functions, computing, storage, and accessibility to big data or quantitative analytics, among others.

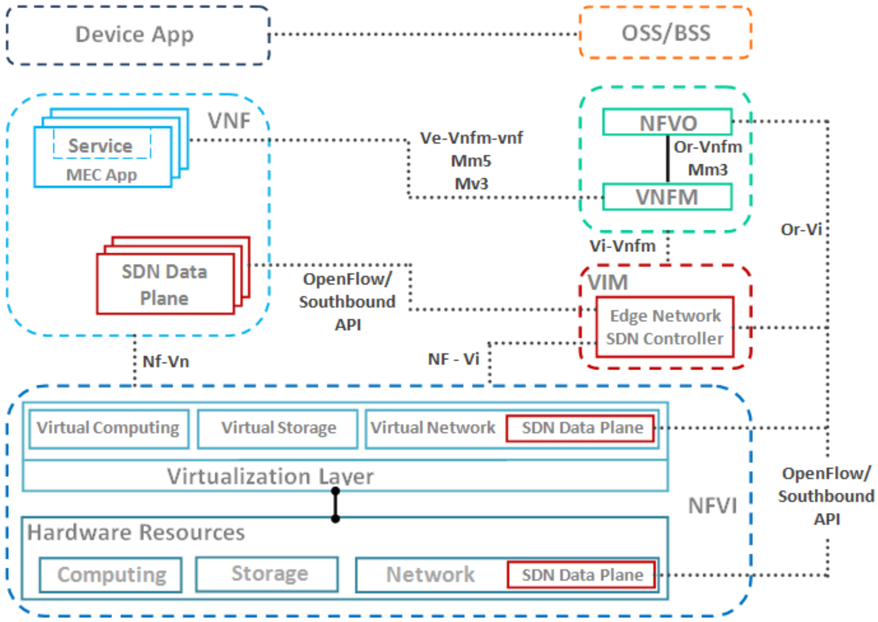

Fig. 6: SDN-based MEC-NFV architectural framework.

Fig. 7 depicts an example of the network slicing on a common network infrastructure considering the potential role of MEC in mobile broadband, automotive, and massive IoT services [22], [44], [145]. Mobile broadband services need significant capacity to ensure that an application achieves adequate efficiency. With traffic forwarding to the localized edge, the MEC system may store content at the edge, boosting the capability of the wireless backhaul and network infrastructure. To assure optimal broadband experiences, MEC may also provide a variety of services such as video accelerators or activity-aware performance optimizations. MEC is a catalytic element that influences the potential of an array of sophisticated operations for the Vehicle-to-Everything/automotive network slicing [146], which must support rigorous latency and extensibility with network functions initialized at the edge. Flexibility is crucial for managing enormous volumes of data quickly and effectively in massive IoT; therefore, MEC can offer storage and processing services for accomplishing signaling improvements.

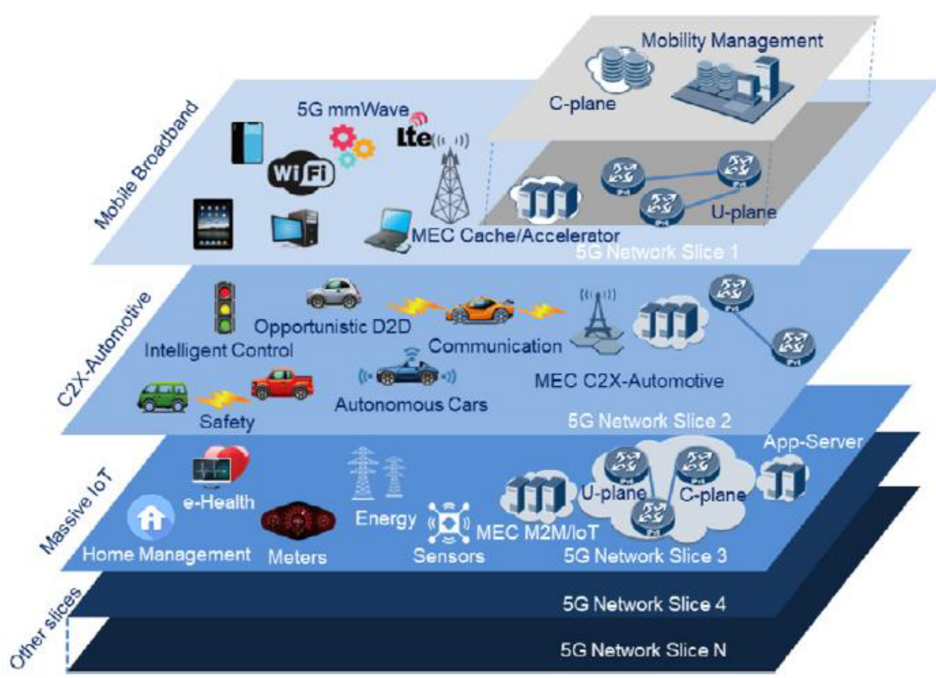

Fig. 7: Network slicing [22].

To enable service modification in slicing, a combo of NFV and SDN solutions is needed, offering a strong synchronization for VNF allotment and service orchestration at the edge server, while offering genuine and flexible service management in real-time operation. Network slicing, as one MEC enabler, delivers two primary advantages to the MEC setting: (i) dynamic infrastructure and (ii) effective resource utilization.

5.5. Information-Centric Networking (ICN)

The Internet, which had been initially intended for host-to-host interactions, is now mostly utilized for content distribution. With continually rising traffic levels, an Information-Centric Networking (ICN) concept tries to bridge the gap between both the original design of the Internet and modern services, including high-definition multimedia on-demand streaming, 3D gameplay, and virtual and augmented reality environments. To improve content transfer, ICN proposes redesigning the Internet framework as a content-centric system that employs two conceptual designs, namely connectivity (instead of hosts) as well as caching, e.g., at MEC computing servers, to alleviate bandwidth congestion and enhance data delivery [147]-[149].

5.6. Service Function Chaining (SFC)

The goal to accelerate the transition to software-defined and configurable networks have prompted network engineering and research organizations to create another technique defined as Service Functions Chaining (SFC) [150]. SFC assists telecom companies and service providers in dynamically creating network services and directing traffic flows across them. Although this description and principles seem similar to those of NFV, SFC deals with the issue of delivering end-to-end solutions throughout a chain or hierarchy of service functionalities [151]. In reality, SFC is an ideal technique for interconnecting two or even more service functionalities in a certain network sequence. Fig. 8 shows the architecture of SFC. Additionally, virtualized service functionalities and physical network elements can be chained. As a result, SFC assures that physical network operations remain in-network and services delivery frameworks are not omitted thereby.

Traffic streams in an SFC infrastructure are categorized and then processed based on this categorization. These procedures are administered in the sequence of the chains, and such procedures may be reclassified, culminating in another sequence. The SFC advisory committee of the Internet Engineering Task Force (IETF) has created SFC architecture for generating, updating, and removing the structured service chains that are related to network data flows. Service Functions (SFs) Classifiers, Services Function Forwarders (SFFs), and the SFC control planes are the core constituents of the SFC framework. The SFC management plane interacts with all of these elements and is in charge of a variety of tasks such as establishing service configuration paths, choosing Service Functions for a demanded SFC, informing classifiers about how to categorize traffic flows, and implementing traffic forwarding guidelines in Services Function Forwarders based on the service configuration path. Classifiers classify traffic flows by comparing them to the policy established by the management plane and then applying the necessary assortment of network service functions. The service function is in charge of specialized processing and can be deployed as a virtual component or as an actual network component. As appropriate, the Services Function Forwarder forwards traffic to the related service functionalities or into the classifier based on service configuration path information.

The MEC application tier is now quite dynamic due to the continuous expansion of end-user activities. Furthermore, because of the large number of virtualization solution ideas in terms of designs, deployments, or implementations, SFC is one of the essential players in the MEC environment. SFC allows MEC to adjust a networking service function to the end user context and deliver end-to-end services [152]. Incorporation of SFC within MEC is an acceptable technique for organizing service function implementation, realizing desired strategies, adapting applications when approaches or policies evolve, and rationally allocating resources to provide needed services.

SFC offers a wide range of MEC applications, which can improve MEC functioning in terms of resource optimization, privacy, and accessibility [153]. The study [154] solves the inter-MEC handover issue by offering the proper option to locate and move SFCs to accommodate subscribers of a 5G infrastructure with MEC regarding service latency. When a user switches cells, the proposed method determines which Virtualized Network Functions of Service Functions Chains should indeed be transferred, which MEC services should be used, and what amount of resources ought to be assigned. These decisions are made to minimize service disruption. To achieve optimal QoS for IoT operations, the researchers of [155] devised a method for carefully placing service functionalities of SFCs in the networks' edge. They presented a probability-based logic programming technique for ranking locations of VNF chains depending on bandwidth, end-to-end latencies, and safety requirements. Leveraging the advantages of the protected service chaining framework, [156] introduces a novel SFC architecture to meet various security needs for Multi-Access Edge Computing. This system attempts to deliver real-time secure service sequencing to mobile subscribers. A fuzzy intelligence system-based technique is used to appropriately arrange the security features and therefore generate the security support chains to achieve a superior level of safety and an optimum sequence of the security mechanisms [157]. Masoumi et al. [158] and Bai et al. [159] investigated the MEC contexts with a focus on VNF failures. To address this issue, they deployed selected VNFs rather than the entire SFC. The procedure of choosing which VNFs are redundant is dependent on available statistics, which are determined by the average interval between problems and the average time necessary to fix the problems. A VNF redundancy solution is built in light of the edge network's restricted resources and depending on this parameter.

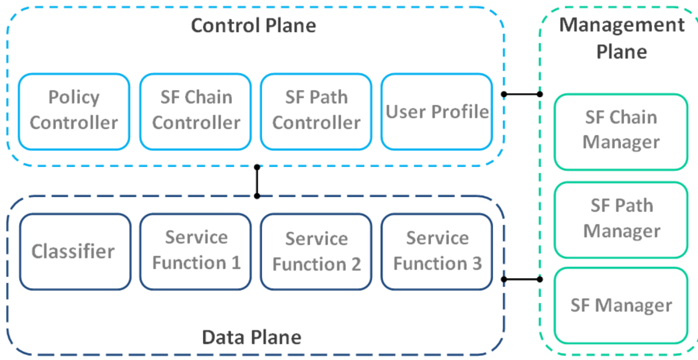

Fig. 8: SFC architecture.

5.7. Radio Access Control

The radio accessibility networks in 4G/5G systems are made up of two primary constituents: the Remote Radio Heads (RRHs), which handle radio spectrum transmission/reception, and the Baseband Units (BBUs), which handle signal processing.

China Mobile presented the Cloud-RAN (C-RAN) network design in 2010 [160]. C-RAN groups BBUs from a detached central workplace, referred to as a BBU controller, distant from their corresponding RRHs; the combined BBUs are identified using private routers that reside within the BBU controller. The C-RAN design allows for lower power consumption, more efficient operation, and increased dependability. One downside of C-RAN is indeed the vast separation between the BBU pool and RRHs, which generates additional delay across the BBU pool and users. This problem spawned a new RAN design known as Fog-RAN (F-RAN), whereby every BBU controller is built by aggregating just a limited number of RRUs, allowing users more alternatives for determining the best BBU venue to operate their services. Similarly, the reference [161] compared F-RAN with C-RAN, indicating that the F-RAN gives a faster service, however, at a relatively higher cost.

5.7.1. Heterogeneous C-RAN

To handle the enormous rise in network traffic, and a vast number of interconnected devices, infrastructure densification has emerged as the crucial component of 5G networks by deploying additional access points and base stations and utilizing spatial spectrum reusing. A heterogeneous network (HetNet) is a merger of higher-power macro cells with lower-power small cells, such as femto cells, pico cells, micro cells, and relay nodes. HetNets were designed because of the following advantages [162]: (i) increased coverage and efficiency, (ii) minimization of the macro cell dependability, and (iii) decreased cost and subscriber turnover. Nevertheless, there are significant problems with deploying dense HetNets: (i) significant interference, (ii) insufficient energy management, and (iii) lack of flexibility and adaptability.

Heterogeneous C-RANs (H-CRANs) [163] are offered as a promising option to deliver excellent energy and spectral efficiency [164]. H-CRANs can also provide broad coverage and good energy efficiency, whereas MEC can provide significant computational facilities for low-latency applications [165]. Combining these two critical technologies will enable 5G to accommodate more applications. H-CRAN may be integrated with MEC to ease the installation of the MEC system, taking into account the computing and storage facilities in the BBU pools [166] as well as the deployment of the RRHs [167]. As a result, the integration of MEC and H-CRANs can provide the following advantages:

By collocating MEC and H-CRAN, the expenditure on MEC implementation can be significantly decreased. Everyone seems to know, deploying a suitably wide MEC network requires a big investment. Re-architecting MEC installation to C-RAN infrastructure is one option to reduce investment costs. The cost of transferring extra task processing over the operating RRHs or BBU pool will be decreased in this situation.

The integration of MEC with H-CRAN can give the operational versatility and infrastructure reconfigurability that the virtualization of H-CRAN may deliver. The H-CRAN can speed up radio deployment by lowering the time required in traditional deployments, such as typical General-Purpose Processing units. Since C-RAN virtualizes many RAN operations, MEC may benefit from H-CRAN's coverage, energy efficiency, network simplification, and high security [168].

H-CRAN MEC may be implemented in a variety of settings. H-CRAN, for example, may interpret task signals from any place, such as a cell tower co-located area. Since H-CRAN implementation necessitates a significant amount of computing power, it may immediately transform into a MEC server to compute workloads from users.

In conjunction with the advantages listed above, various obstacles with H-CRAN MEC platforms can be emerged via H-CRAN and MEC collocation, such as deployment scenario planning. The key problems of H-CRAN MEC technologies are elaborated on below:

The equilibrium of rollout and network effectiveness inside the H-CRAN MEC architecture should be thoroughly examined. Since the H-CRAN provides dynamic capacity, the functionality of MEC systems is affected by the separation distance between the C-

RAN/MEC and cell site, e.g., how effectively it can support activities. For example, while putting the C-RAN/MEC platform in a central facility might greatly save costs, it results in excessive latency. In this instance, use cases must be carefully examined to determine which programs should execute at which locations.

Most MEC capacity management solutions take into account the computational resource on MEC hosts and may therefore be used directly in H-CRAN MEC. Yet, concurrently optimizing computing resources and scheduling network resources in H-CRAN remains difficult. Inter-cell and cross-layer interference must be regarded, specifically in HetNets. Furthermore, the adaptive resource management method based on C-RAN NFV may require being updated to flexibly plan virtual computing resources under variable network capacities and task entry rates.

Another issue that must be addressed with H-CRAN MEC systems is confidentiality. Since MEC service offers a wide range of applications, including third-party apps that are not directly regulated by mobile network carriers. There is a danger that these apps will deplete network resources or allow hackers to disrupt network operations. As a result, executing integrity assurance tests on programs should be considered during installation or upgrade.

Because of the presence of inter-carrier interference (ICI) or disturbance, the resource provisioning issue in H-CRAN MEC systems is significantly more difficult than in standard MEC systems. To counteract this impact, the spectrum resource inside every cell can be separated into orthogonal sub-channels that should be assigned to mobile users effectively (for example, which sub-channel or sub-carrier user device has to use for offloading a task to the host MEC server). To decrease inter-cell interference or disturbance in H-CRAN MEC systems, several types of resources must be orchestrated efficiently, including not just traditional wireless resources (e.g., transmit power, sub-channel, space, and time), but also countervailing expenses (e.g., harvested energy, the backhaul spectrum, caching storage, and computing capabilities). User association, computational offloading, interference reduction, and allocating resources are the key problems of high-density H-CRAN MEC technologies. More significantly, these issues are inextricably linked and must be addressed together.

On one side, it is expected that a large number of MEC systems will be extensively implemented in the coming years, varying in size (processing capabilities) and functionality (computation speeds). The link between subscribers and MEC systems, on the contrary, is highly dependent on the placement sites of MEC systems. Whenever a user device travels within the geographic region served by the unified BBUs, user motion can be disregarded. This type of BBU centralization affects the system performance and user experience.

5.8. Device-to-Device Communication (D2D)-Aided MEC

The exponential expansion of mobile data transmission and context-aware programs necessitates novel techniques to more effectively utilize bandwidth and enhance coverage while reducing latency and energy usage. Since every communication must be transmitted through the centralized control unit, the star configuration of mobile networks with a central control point, such as a base station or access point, suffers from inadequacies. D2D transmission, on the other hand, is a radio technology that allows direct data transfer between two neighboring UDs without the participation of the wireless network's central management point or core network, i.e. without crossing the base station or access point. This direct D2D connection has various advantages, including enhanced spectrum efficiency, higher data rates across devices, lower power consumption, and shorter end-to-end latency. D2D connectivity has been exploited in numerous research works to offload computations to other adjacent users (not utilizing MEC facilities) [169], [170]. Moreover, accessing caches at adjacent users (although not leveraging MEC caches) has been examined in previous research [171], notably audiovisual file caching at some other UEs [172]. Fig. 9 depicts D2D-aided edge computation/MEC scenarios.

Unfortunately, D2D communication has certain implementation issues. One problem is the requirements to acquire exact channel information, for example, channel estimation and transmission control, which introduces overhead.

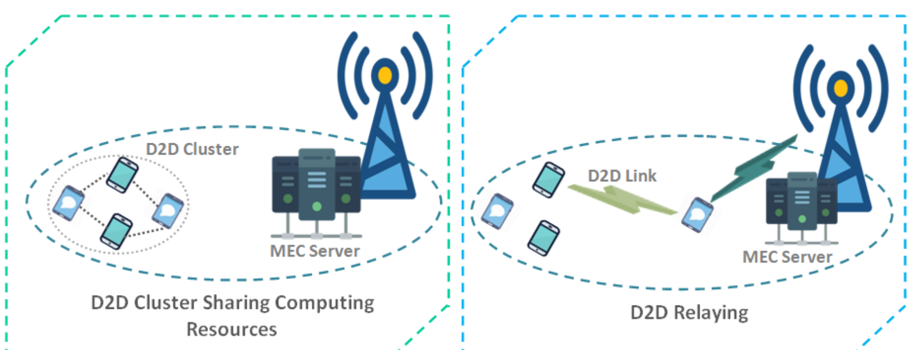

Fig. 9: D2D-aided edge computation or MEC scenario.

Another significant problem in D2D communications is privacy. D2D transmission is inherently vulnerable to security threats since a user's content goes through another user's device [173].

Selfish exploitation activity of user devices is another impediment to cooperative multi-device D2D transmission; since some devices may take other devices' communications resources, i.e., multi-hop D2D connectivity via intermediate relay mobile users and preventing the relay user to assist others [174].

Interference and movement management are also significant issues. As a result, when constructing device-enhanced MEC platforms that incorporate D2D transmission, these D2D communication issues must be carefully examined.

Notwithstanding these obstacles, D2D communication offers great potential for a variety of realistic use case circumstances in forthcoming communication systems. The work next goes over a few sample use-case instances in detail.

National Security and Confidentiality: The wireless cellular communication's dependency on the accessibility of the wireless communications infrastructure causes serious challenges in emergency and catastrophe situations such as flooding and earthquakes. Such calamities frequently destroy the mobile network infrastructure, causing cellular wireless communication to be disrupted. D2D communications, on the other hand, do not necessitate a permanent network infrastructure and may thus continue functioning even if the cellular network architecture is broken. Because of this benefit of direct D2D interaction, for emergency conditions, the United States governing body for the regulation of telecommunications for national and public safety and the European administrative body for Postal and Telecommunications regulations for next-generation state-level security and confidentiality of communication systems [175].

Proximity and Location-Based Services: With a growing emphasis on online gaming, promotional campaigns, and social media platforms (e.g., Instagram, Facebook, and others), there is a greater need for effective quick connectivity to endorse interconnections between adjacent users with reduced latency and battery capacity while maintaining high degrees of user confidentiality. D2D communication can permit such connections between nearby user devices, for example, a cell phone communicating to a computer or other cell phones for storing or exchanging video and photographs [176], [177].

Vehicular Connectivity: Another major use scenario of D2D transmission is vehicular or V2X interaction, which is classified into three types: vehicle-to-network (V2N), vehicle-to-infrastructure (V2I), and vehicle-to-vehicle (V2V). Recent substantial advancements in computing and communication infrastructures, as well as vehicular sensing technologies, have moved focus on V2X communications to strengthen public safety and smart transportation systems, accident avoidance mechanisms, and electric car charging [178], [179].

Authors noticed that the aforementioned use cases, along with a diverse variety of other D2D connectivity use circumstances, have the possibility of benefiting considerably from jointly utilizing MEC computing and caching resources, alongside the facilities of other neighboring mobile end devices, i.e., device-enhanced MEC [41], [180].

5.9. Machine Learning and Artificial Intelligence

Machine Learning (ML) has been used in a wide range of applications, including digital assistants, video monitoring, social media platforms, email spam and virus screening, search engine result refinement, and product suggestion. There are various reasons why machine learning algorithms are becoming more popular [181]: (i) ML facilitates mechanisms that can automatically adjust and configure themselves to legitimate users, (ii) ML can explore new information from massive database systems, (iii) ML can resemble human and substitute certain strenuous tasks, that necessitates some cognition, (iv) ML can develop programs those are challenging and costly to build manually because they contain specialized comprehensive abilities or expertise synchronized to a specific project, and at last (v) massive rise in computing capabilities. In general, ML is classified into three fundamental types: Unsupervised Learning, Supervised Learning, and Reinforcement Learning (RL) with Deep Learning (DL), presented as a breakthrough approach and a big step forward toward ML, capable of achieving higher-level abstractions based on simple elements. The International Telecommunication Union (ITU) Telecommunications Standardization Division [182] recently suggested a uniform framework for ML in forthcoming networks, in which MEC would play critical roles as a producer, pre-processor, collector, modeler, strategist, distributor, and sink. MEC, for example, may receive data from users and subsequently preprocess the data by running an ML algorithm to extract the required information before delivering the outcome to the centralized cloud for any further training. Furthermore, various surveys and tutorials covering ML, DL, and related implementations in networking and communications have been published, and readers can resort to these publications for further information [183]. Fig. 10 visualizes a graphic demonstration of the incorporation of AI/ML and analytics in a MEC server.

Because of the fast expansion of wireless communication systems and infrastructures, it is expected that Artificial Intelligence (AI) or machine intelligence generally, and ML in particular, may have crucial functions in 5G, 6G, and beyond [184], [185]. In general, ML can offer the following benefits:

The capacity to learn from massive data to enhance system operations and efficiency is the most obvious benefit of ML, which may be done without additional hand-crafting functionality. Because (i) mobile data traffic is extensive, (ii) mobile traffic raises at unprecedented rates, (iii) mobile traffic is non-stationary (i.e., the timeline for reliability and validity can indeed be comparatively short), (iv) mobile data effectiveness is not retained (i.e., data accumulated can sometimes be low-quality as well as disruptive), and

(v) mobile data is diverse, the significance of learning emerges inherently in wireless systems (i.e., data traffic can be produced by various types of devices and services).

Due to huge state and action domains, varied network devices, and varying QoS objectives, joint communication, caching, computing, and control (4C) management in 5G as well as beyond is enormously challenging [186]. In such cases, ML can provide instantaneous and/or completely distributed approaches. Furthermore, model-free wireless communications raise difficulties such as channel estimation, problem statements, and closed-form solutions, all of which may be easily tackled by ML [187].

Finally, since edge computing will serve an essential role in enabling low-latency operations and the bulk of intelligent services will be placed at the edge of the network, edge intelligence will develop. Using edge intelligence to extract usable information from huge amounts of mobile data might increase the capabilities of tiny IoT devices and allow the implementation of computationally intensive and lower-latency edge services [188]. Edge learning, on the contrary, can avoid the limitations of cloud intelligence and on-device intelligence by balancing learning design complexity and training duration [189].

Optimizing MEC confronts various issues, including cache placement, communications and computing resource planning, computational task allocation, and combined 4C optimization. A variety of difficulties in MEC systems have been investigated in research [190], including computing offloading, caching, combined 4C optimization, safety and confidentiality, big data analyses, and the mobile crowd.

AI fosters technological innovation by improving data analysis insights, particularly in time-varying and complicated networks. In this setting, stretching AI advances to the edge of the network has generated an entirely novel field known as edge cognition or intelligence. It is not only a combination of MEC with AI [191], but a whole new and complementary strategy for employing AI at the edge of the networks [192]. Nonetheless, edge intelligence adoption remains in the early stages. Edge hardware can use edge intelligence to execute model training and inferences locally, minimizing the need for frequent contact with cloud services. Reinforcement Learning and Deep Learning approaches have increasingly become the most prevalent AI techniques in edge intelligence. Reference [193] asserts that the convergence of Artificial Intelligence and MEC is indeed an unavoidable trend, and provides justification for this assertion:

- Reduced latency and bandwidth use
- Adaptation to changing environments
- More diverse edge applications and services
- MEC facilitates pervasive AI
- AI features can facilitate MEC.

AI has the potential to significantly improve the cognitive efficiency and effectiveness and competence of the vehicular Internet of Things (IoV) to adapt to frequently developing dynamic environments, as well as provide numerous task specifications for the allocation of resources, data processing task scheduling, and traffic prediction forecasting. By introducing AI technologies to edge access nodes, edge intelligence has demonstrated exciting potential for handling various intelligent vehicular scenarios. The work [194] developed a Double-Deep Q-network algorithm-based solution for minimizing the cost of transmission, storage, and computing in a vehicular network. Nevertheless, there are still issues that must be addressed before edge intelligence can be widely used, such as

- System dynamics and transparency
- Infrastructure and network design
- Models of lightweight training
- Privacy and security.

6. Technical Features of MEC

6.1. Computation Offloading

Since user devices are capacity restricted, they must offload some of the resource-intensive activities (e.g., video analytics or processing) to certain other resource-rich terminals to conserve capacity, energy, and time. It is also one of the inspirations behind the MCC paradigm, which enables cloud services for mobile users. Nevertheless, MCC imposes several constraints, i.e., escalation of the traffic load (backhaul and radio) and latency. To solve these restrictions, offloading computations in edge cloud computing/MEC are presented, which consists of three components [195]. The very first aspect, termed as application/task splitting, is in charge of selecting between three ways based on different performance metrics: localized processing, complete offloading, or partial offloading [57]. While making this determination in a versatile and complicated network infrastructure is difficult, the partitioning technique (either automated application assessment or programmer-specified segmentation) adds further challenges. The second component, which consists of three actions, is concerned with task allocation. Step 1 is to identify resource-rich endpoints (for example, edge servers) which may be utilized for offloading. Step 2 is task sequencing, which involves assigning partitioned tasks or workloads to found nodes for optimal performance. The final step or step 3 is task allocation. The last component maintains several categories of resources.

The in-practice offloading strategies are described below:

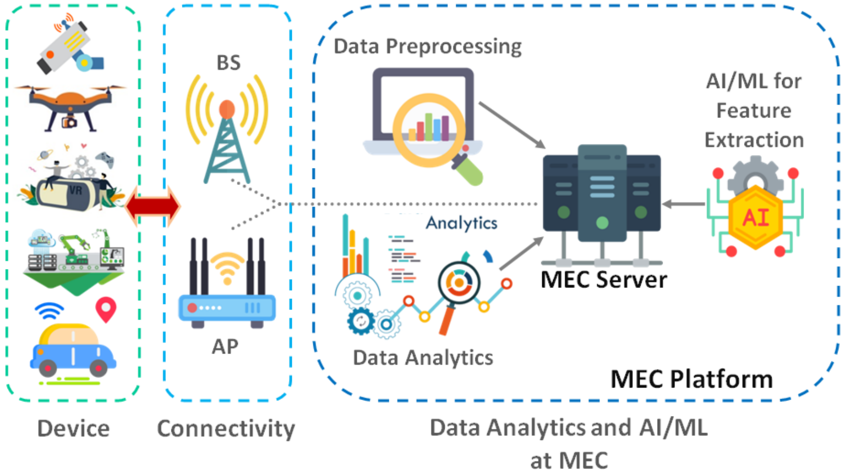

Fig. 10: Incorporation of the analytics and AI/ML in an MEC server.

Full Computation: (i) Local Computation: All computing activities are executed in local devices (UDs) rather than transferred directly to the MEC infrastructure, resulting in substantially lower latency than offloading computing workloads to the servers. Unfortunately, this technique throws significant constraints on the device's battery performance and energy usage. This will also impose special demands on the computing capacity of the end devices. (ii) Edge Computation: Unlike local computation, edge computation sends all compute-intensive operations to MEC nodes for processing. Afterward, there are three forms of latency to consider: a) the time it takes to transfer content to the MEC; b) the time it takes for the MEC hosts to analyze content; and c) the time it takes for the device to obtain the processed data. Let's anticipate that the total of such three delays will be less than the local computational latency. The devices' energy is also conserved in this manner.

Partial Computation: Partial computation typically divides processing into two sections: offloaded and non-offloaded segments, which tend to be more adaptable than the binary choice of local computation or edge computation. The non-offloaded data segments will be processed locally by the user device, while the offloaded data segments will be processed on the edge side. Nevertheless, precisely distinguishing two factors and balancing the limitations is difficult. Moreover, offloading decisions are made by taking into consideration a variety of factors such as energy usage, latency, and communication bandwidth.

Li et al. [196] studied a novel joint optimization approach for caching and computation offloading in a MEC infrastructure for vehicular networks. Ke et al. [197] constructed an adaptive deep reinforcement learning-based strategy for computation offloading in a MEC-based heterogeneous or collaborative vehicular infrastructure. Researchers jointly examined the system's reliability, energy usage, and execution delay.

The offloading selection is an important aspect of the MEC since it decides where the computation needs to be performed. While making the selection, one ought to take into consideration not just the power consumption of the end devices as well as the energy consumed by the MEC hosts. Consider the scenario of a single user device transferring computation to several servers (e.g., under very tight latency constraints) as well as the scenario of numerous devices offloading. Most studies, however, consider that the user device remains immobile when making offloading decisions. Users can frequently move, and in some cases, they may relocate from one location to another. In this scenario, the preference to minimize the expense relative to user mobility is a reason for concern.

Cyber foraging provides compute offloading, strengthening mobile device capabilities while significantly improving the energy economy. CloneCloud partitions code automatically at the thread layer. Cuckoo examined component-level partitioning, and a related mechanism was built in MAUI. Yet, the transaction state may be extended because of an unbound delay in computation offloading to a faraway cloud. In certain circumstances, this may use more energy than local computations.

MEC consumes less energy due to lower latency and closeness to the RAN edge. As a result, consumers benefit from speedier execution and improved performance. Encoding represents the most computationally intensive element for video services. Whenever a mobile device wants to initiate a video chat during teleconferencing, a negotiation process is undertaken to pick the kind of encoding accessible before the content is encoded within the mobile device and afterward uploaded. Such a procedure requires power and may take some time. Tusa et al. [198] suggested a communication mechanism to transfer the encoding function to an edge computing server as a solution. Offloading the encoding portion will conserve energy and reduce delays in connectivity, providing excellent video quality.

Machine-to-machine (M2M), wearable tech, or other IoT devices may shift compute-intensive programs to the edge. This may be accomplished by dividing the program and transferring only the data-intensive portions to the edge. Abdelwahab et al. [199] presented REPLISOM, a computation offloading paradigm for IoT services in which the edge cloud submits a demand to the respective IoT devices, obtaining information relating to the connected service, i.e., generally a memory replication of the VM. REPLISOM is built along the Long-Term Evolution (LTE)-evolved memory replicating mechanism, which uses D2D connectivity to combine numerous memory copies from the surrounding user devices into a unified compact form, which is subsequently fetched from the device. Compressed sample-building techniques are employed to administer such memory replicas, lowering the effort required by typical devices to push for saving energy and money by minimizing the number of repeated requests at once.

The work [200] considered the idea of a hybrid cloud, which splits applications flawlessly in core and edge cloud services, enabling delay responsive and user-interactive features at the edge, thereby preserving a configurable cloud approach, and this is an edge-cloud cooperative scheme focused on IoT applications. The goal is to make two new types of applications more efficient: extremely accurate indoor localization which relies on reduced latency and flexible and robust video surveillance that preserves bandwidth. Another sector that needs a substantial amount of computational power is mobile games. Mobile gaming may become more interactive owing to lower reaction times by transferring the rendering portion from handheld devices. In the context of multiplayer gaming, the trade-off around offloading and cloud service efficiency should be evaluated to prevent overloading a specific cloud platform. In this regard, Hu et al. [201] and Qin et al. [202] suggested a distributed computational offloading model based on game theory. The model takes into account a multi-channel radio network and a multi-user offload strategy, with the equilibrium state attained by taking into account the number of users who can gain from edge computing. RAN-aware content optimizer, a complementing service that harnesses the features of MEC, can improve the effectiveness of computational offloading. Obtaining information on RAN performance and user context before offloading can help both the devices and the network. Magurawalage et al. [203] suggested a network-aware and energy-efficient architecture for application offloading depending on network accessibility, radio signal performance, and surrogate computational resources that are available. It deconstructs applications into their constituent parts and develops an offloading online approach according to the previously mentioned optimization factors. Wu et al. [204] presented computation architecture from the standpoint of IoT applications. It then analyzed cutting-edge concepts for AI-empowered cloud-edge coordination for IoT. Lastly, a list of prospective research problems and open queries is presented and addressed. To solve the tradeoff between low computing power and substantial latency, while also ensuring data integrity throughout the offloading process Wu et al. [205] proposed a Blockchain-based cloud-edge-IoT computing framework that takes advantage of both MCC and MEC, with MEC servers providing reduced latency computing services and MCC servers providing more computational capability. Furthermore, the work designed an energy-efficient dynamic computational task offloading (EEDTO) algorithm that chooses the appropriate computing location live, either on the MCC server or the IoT device, or the MEC server to jointly optimize energy usage as well as task response time. Xue et al. [206] presented an efficient offloading system for DNN Reasoning Acceleration (EosDNN) within a cloud-edge-local cooperative context, where DNN reasoning acceleration is primarily employed in task migration delay optimization as well as real-time DNN query realization. Xue et al. [207] investigated DNN model segmentation and offloading and proposed a unique optimization strategy for parallel task offloading of substantial DNN models in a cooperative cloud-edge-local setting with restricted resources. To acquire the DNN offloading method, an enhanced Double Dueling Prioritized Deep Q-Network (DDPQN) technique is suggested in conjunction with the coupling cooperation level and node balancing degree. Fig. 11 depicts the notable and evolving algorithms for computational task offloading [208]-[225].

6.2. Communications

Communication links between mobile users and cloud services are generally characterized as bit-stream or bit-pipe with either fixed rates or arbitrary rates with specified distributions in MCC research. Such coarse designs are used for adaptability and may be appropriate for the architecture of MCC platforms where the focus is on mitigating latency in core networks and managing large-scale clouds but not wireless communication delay. In the case of MEC systems, the situation is distinct. Considering the small-scale nature of edge clouds and the concentration to latency-critical activities, the key design goal is to reduce communication latency by creating a highly improved air interface. As a result, the bit-pipe or bit-stream concepts discussed above are unsuitable since they miss several essential aspects of wireless transmission and are overly simplified to allow for the deployment of sophisticated communication mechanisms. To be more explicit, wireless networks differ from their wired equivalents in the following fundamental ways:

(i) In wireless transmission medium multipath fading arises due to reflections, environmental disturbance, and refractions or dispersions of signals from scattering elements in the surroundings (for example, walls, trees, and buildings), rendering the channels extremely time-varying and causing significant inter-symbol interference (ISI). In trustworthy transmissions, effective ISI reduction methods like spread spectrum and equalization are required.

(ii) The broadcast aspect of wireless transmissions causes a radio wave to be affected or disrupted by other radio waves in the same spectrum, potentially lowering their respective reception signal-to-interference plus noise ratio (SINR) and increasing the likelihood of signal loss during the time of detection (at the receiver end). To deal with performance deterioration, interference control has emerged as one of the most critical design concerns for wireless communication systems, attracting significant research efforts.

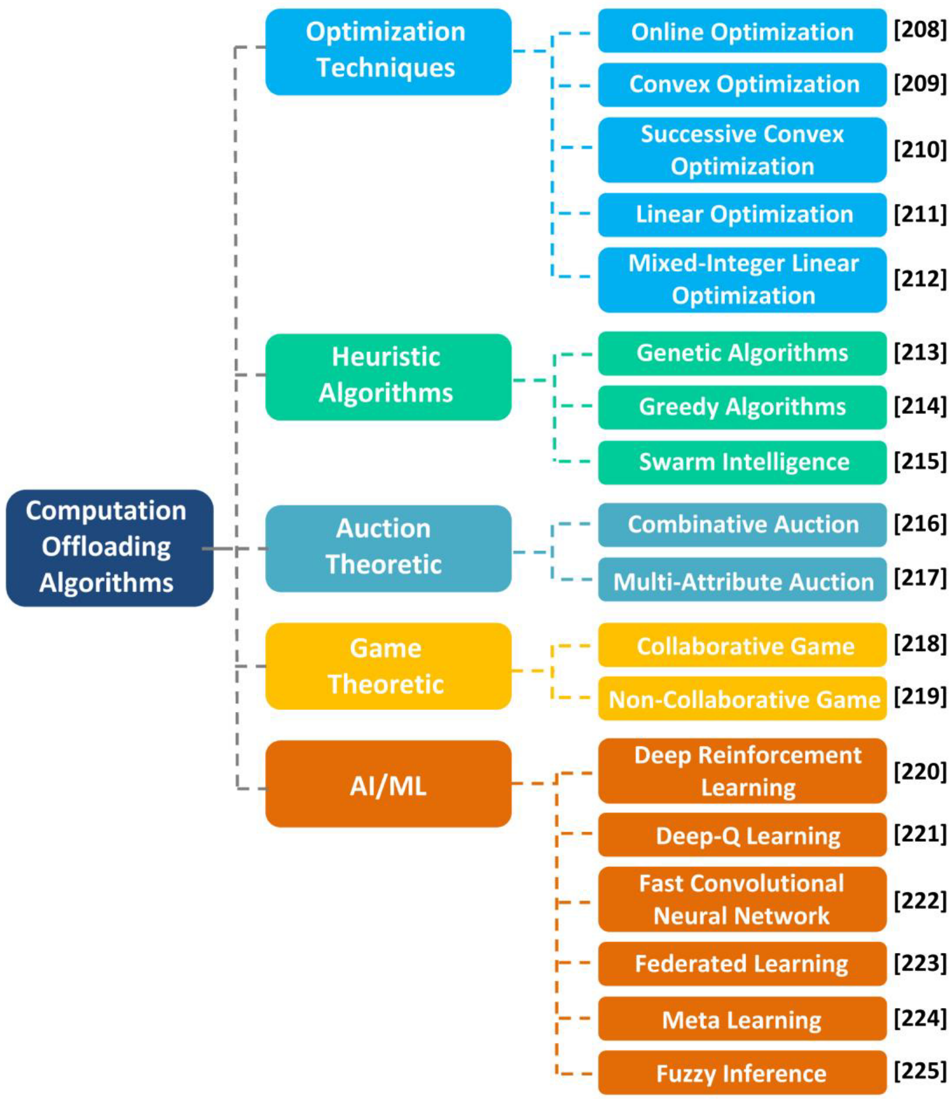

Fig. 11: Computational task offloading algorithms.

(iii) The spectrum scarcity has been a major impediment against incredibly high-rate radio access, encouraging extensive research into exploiting unique spectrum resources, formulating novel transceiver configurations and network frameworks such as novel multiple access techniques to enhance spectrum efficiency, and constructing spectrum sharing and accumulation strategies to facilitate effective use of segmented and underexploited spectrum resources.

Since wireless channels vary randomly in time, frequency, and space, it is vital to building efficient MEC systems that smoothly combine control of computational offloading with radio resource management. For example, if the wireless channels are under severe fade, the decrease in task execution delay during remote computing may not be adequate to substitute for the increment in transmission latency caused by the severe decrease in transmission rates. In these kinds of instances, it is preferable to postpone offloading until the channel gain is acceptable or to transfer to a different frequency/spatial communications channel having higher quality for offloading. Additionally, boosting transmission power can boost data rates while also increasing data transfer energy usage. The foregoing concerns imply the collaborative design of offloading or transferring and wireless transmissions that are adaptable to time-varying channels based on precise channel-state information (CSI).

Communications in MEC systems are primarily between base stations or access points and user devices, with the potential of direct D2D connections [226]. MEC systems are small server facilities installed by cloud computing/telecom vendors that may be co-located with radio access points, such as public WLAN hotspots and base stations, to save expenditure (for example, transmission site rents). The radio access points not only offer a wireless channel for the MEC workstations but also allow access to the faraway data center over backhaul networks, allowing the MEC server to offload some computing workloads to other MEC workstations or large-scale cloud computing facilities. D2D connections with surrounding devices give the option to transmit computing tasks or workloads to MEC servers for mobile devices that cannot interact directly with MEC servers owing to limited wireless interfaces. Moreover, D2D transmissions allow the peer-to-peer sharing of resources and computing load management within a group of user devices.

There are several commercialized wireless transmission technologies available currently, including Bluetooth, radio frequency identification (RFID), near-field communications (NFC), WLAN, and mobile networks such as LTE, 5G, beyond 5G, and 6G networks (planned to be deployed within 2030). With varied data rates and communication capabilities, these technologies can facilitate mobile offloading from user devices to access points or peer-to-peer wireless collaboration. In terms of operating frequencies, maximum transmission range, and data throughput, conventional wireless communication systems differ greatly. Since the transmission or coverage area and transmission rate in NFC are so limited, it is best suited for purposes that involve little information transmission, such as e-payment and physical access verification. RFID is identical to NFC in a sense that it permits only one-way transmission. Bluetooth represents a more powerful method for enabling short-distance D2D connectivity in MEC platforms. WLAN, LTE, 5G (and forthcoming 6G) are key technologies facilitating long-distance connectivity between user devices and MEC servers, which may be dynamically switched based on connection stability. The networking and communication protocols must be modified for the implementation of wireless technology solutions in MEC systems to encompass both the communications and computing facilities and efficiently enhance computational efficiency, which is more complex than data transfer.

Hu et al. [227] developed a MEC architecture and accompanying communication protocols for content delivery and processing in vehicular connectivity networks that include IEEE 802.11p, licensed sub-6 GHz spectrum, and millimeter wave (mmWave) communications. Liu et al. [228] presented a unified heterogeneous networking system for MEC and fiber-wireless accessibility networks that employ network virtualization to accomplish dynamic coordination of networking, storage, and computational resources to accommodate various application requirements. Peng et al. [229] provided an adaptive spectrum management approach to improve spectrum resource usage during the communication with the MEC server for a self-driving vehicular network. Song et al. [230] developed a novel MEC architecture for satellite-terrestrial integrated IoT systems leveraging Low Earth Orbit (LEO) satellites. Li et al. [231] presented a multi-relay aided computation offloading architecture for MEC with energy harvesting (MEC-EH) infrastructure. A computational operation may be conducted in this system by transporting it to the MEC host via multiple neighboring relay units.

6.3. Caching and Distributed Content Delivery

Since content, particularly video constitutes the most popular wireless network services, thousands of visual content elements are transmitted regularly to content providers' systems. Such content is kept in huge quantities in the providers' data warehouses before being transcoded from originating version to the final delivery version and disseminated to various streaming servers across many network locations for continued distribution. Despite attempts to distribute material, certain users may encounter service disruptions owing to buffering issues and jitter, particularly in mobile contexts. By expanding Content Delivery Network solutions to the cellular edge, consumers' QoE may be improved while backbone and core network utilization are reduced. Many study findings support this conclusion. Studies [232]-[235] particularly provided several architectural styles for supporting parallel and distributed edge servers able to execute audiovisual caching and broadcasting to improve QoE for content distribution. In terms of the influence on backhaul, caching contents can reduce bandwidth needs by up to 35% [236].

Recently, Media Cloud, a system for effectively distributing adaptive streaming services for video, has been presented, which provides an elastic virtualized content delivery infrastructure at the edge. MNOs and OTT vendors may fully leverage the MEC system by pre-caching popular material at the edge based on analytics and user/service predicting data. A context-aware networking with edge caching features, relying on big data analysis is examined, whereas a content positioning and delivery technique based on content recommender systems and wireless environment features are detailed in [237] and [238].

Caching may be implemented in a hybrid fashion for networked cloud edges, in which each edge server distributes the cached resource metadata in the format of a portfolio. When users request contents for the very initial time in a traditional cloud computing system, the request is forwarded to a distant cloud platform to retrieve the needed material. Unlike traditional cloud operations, hybrid caching allows users to request material from other local edge platforms rather than retrieving content from faraway clouds. Besides video, augmented reality is another sort of material that is extremely dependent on round trip length and network availability. MEC can offer optimal QoS, particularly for 3D picture files and other large or complex contents, by storing those locally rather than relying on central cloud facilities and core network infrastructure.

Zhong et al. [239] intended to reduce the average task executing time in the MEC system by taking into account the variability of task requirements, caching of distributed applications, and access point or base station cooperation. Ugwuanyi et al. [240] presented and examined a novel system Predictive-Collaborative-Replacement (PCR) for managing content caching within MECs that incorporates proactive prediction, coordination across MECs, and a substitution algorithm. Tefera et al. [241] investigated a decentralized adaptable resource-aware communication, computation, and the caching system based on Deep Reinforcement Learning (DRL) that can orchestrate varying network settings. MEC's capacity limits its ability to cache all versions of popular streaming. Video transcoding alleviates this issue to some extent by transforming the higher attainable video bit rate to such a required lower one; nonetheless, transcoding a significant amount of videos simultaneously might soon exhaust the accessible edge processing capacity. As a result, caching adequate video bit rates which can serve the greatest number of network subscribers is a difficult task. To tackle this challenge and make better use of network edge facilities (processing and storage), Kumar et al. [242] developed a non-traditional strategy for video caching that makes use of network information offered by MEC's Radio Networking Information (RNI) Application Program Interfaces (API). Ding et al. [243] presented an edge content distribution and update (ECDU) mechanism. The researchers implemented a variety of content hosts in the ECDU architecture to store raw content gathered from mobile users, as well as cache pools to preserve content that is often queried at the network's edge.

7. Contemporary Supporting Technologies for MEC

7.1. Multiple Access Technologies

7.1.1. Non-Orthogonal Multiple Access (NOMA)

NOMA is a potential multiple access technology for forthcoming wireless communications technologies. NOMA enables several users to utilize the single resource block by utilizing successive interference canceling (SIC) [244] and superposition coding (SC) [245] at the transmitting and receiving ends, respectively. As a result, the advantageous qualities of NOMA concerning the allocation of resources and interference reduction have been thoroughly examined in numerous situations that are tempting to cope with the aforementioned issues of combining connectivity, sensing, and computational functionalities. As a result, assessing the potential advantages of the NOMA scheme in multi-functional communication systems is quite valuable.

Because of its greater spectral efficiency, NOMA has been regarded as a major enabling innovation in next-generation communication systems. On one aspect, the NOMA principle fundamentally alters the layout of potential multiple access systems. In particular, unlike traditional orthogonal multiple access (OMA), which assigns orthogonal bandwidth spectrum resources to user devices or subscribers, NOMA facilitates users to utilize the same spectrum, with multiple access interference managed by advanced transceiver configurations. As a result, as opposed to OMA, NOMA provides greater flexibility for effectively utilizing finite bandwidth resources [246].

NOMA is broadly categorized in two variants [247]: code-domain NOMA (CD-NOMA) and power-domain NOMA (PD-NOMA). CD-NOMA employs user-specific sequences to share the total available radio spectrum, whereas PD-NOMA takes use of user channel gain variances and multiplexes subscribers in the power domain. Another notable newly developed variant of NOMA is cognitive radio-NOMA (CR-NOMA) [248]. Sparse code multiple access (SCMA), orthogonal frequency-division multiple access (OFDMA), code division multiple access (CDMA), and multi-user shareable access (MUSA) are instances of code-domain oriented access techniques [249]. NOMA can handle more subscribers than available sub-channels, which contributes to a variety of benefits such as huge connectivity, lower latency, improved spectral efficiencies, and improved channel feedback.

With the provision of unique possibilities, the integration of NOMA and MEC may considerably increase user satisfaction and system performance. While NOMA has several benefits in terms of improving bandwidth efficiency and cell-edge connectivity, soothing the channel feedback demand, and lowering transmission latency, MEC provides significant benefits not just for subscribers, but also vendors and third-party providers, and allows for improved overall network performance.

NOMA and MEC together can offer low-latency connectivity. Since the 5G and beyond communications infrastructure will not be entirely constructed around one technology, it is critical to manage the infrastructure from a variety of viewpoints, including air interface, network design, and enabling techniques. NOMA and MEC seem to be two potential options for dealing with latency needs. MEC relocates cloud services and processes to the edge of the network, where the majority of data is created and managed. As a result, MEC enables edge applications to better fulfill end users' reduced latency needs as opposed to cloud computing. Similarly, flexible scheduling as well as grant-free accessibility in NOMA offer decreased communication delays for 5G and beyond network users.

NOMA and MEC may be coupled in a variety of ways with various current wireless technologies, including mmWave connectivity [250], multi-input multi-output (MIMO), massive MIMO, and so on, to improve connection, spectrum efficiency, energy consumption, and computing capabilities [251]. Massive MIMO, as an example, may dramatically boost the spectral performance of wireless networks by extensive spatial multiplexing; hence, massive MIMO-NOMA can allow vast connectivity while maintaining excellent spectral efficiency. MmWave frequencies can be utilized for wireless communication systems to provide gigabit-per-second data speeds. The substantial gains produced by massive MIMO can compensate the severe path loss induced by mmWave. As a consequence, NOMA MEC may be used in conjunction with the mmWave-based massive MIMO scheme to permit numerous devices to offload computational workloads at higher data rates.

Since communication speed is vital in a ubiquitous computation scenario, the use of NOMA to assist work offloading has drawn considerable interest. In particular, the effect of NOMA on workload offloading was assessed in [252] using several asymptotic performance evaluations. In [253]-[255] authors investigated and showed the benefits of NOMA in diverse MEC systems and cache-aided MEC systems, correspondingly. The authors of [256] and [257] investigated communication and computational resource management of NOMA-MEC systems, demonstrating the benefits of NOMA in improving energy efficiency. The authors of [258] made a new contribution by devising a unique hybrid offloading strategy for MEC systems considering the perspective of energy efficiency.

7.1.2. Rate Splitting Multiple Access (RSMA)

RSMA is developed as a kind of multiple access approach for forthcoming wireless communication systems for non-orthogonal transmissions, interference mitigation, and rate optimization. RSMA has been viewed as a possible key enabler for the 6G wireless communication due to its high spectral/energy efficiency, dependability, and resilience for both uplink and downlink multiple-user communications. Inter-user interference is being partially decoded and handled as noise in the downlink or downward RSMA, and this not only optimizes decoding efficiency and complication, but also allows flexibility to connect NOMA and space division multiple access (SDMA). Using channel second-order characteristics, [259] suggested a more generic downlink rate-splitting scheme for the MIMO technology with imperfect or insufficient CSI at the transmitters. As opposed to NOMA and SDMA, message prioritization is advantageous for successfully controlling power-domain distortion and achieving a better spectral efficiency for downlink communication. The work [260] deployed an intelligent reflecting surface (IRS) to support the downlink RSMA technology, which outperformed the IRS-assisted downlink NOMA scheme in terms of outage performance. [261] suggested the RSMA-aided downlink transmission architecture for cell-free enormous machine-type connectivity. Contrary to the downlink or downstream RSMA, the split signal streams or radio waves from multiple devices in the uplink or upstream RSMA are completely decoded at the base station receiver utilizing SIC [262]-[265]. The advantage of using uplink RSMA over uplink NOMA using SIC processing is that it achieves the complete capacity range of multiple access channels or streams [265]. Yet, RSMA implementations for uplink media access control (MAC) remain in their early stages. Because the split data streams of multiple uplink users greatly increase detection complications at the receivers, the optimal effectiveness of uplink RSMA is heavily dependent on rate-splitting settings as well as the SIC decoding sequence at the receiver end [266], [267]. [268] presented a rate-splitting strategy for an upstream CR-NOMA system to decrease user scheduling complexities, in which the divided signal streams may be decoded sequentially even with the identical received power level. Reference [269] proposed a rate-splitting strategy for an upstream NOMA system to increase user integrity and outage performance. Taking into account the partial rate limitations across subscribers, [270] optimized the sum rate in the case of uplink RSMA. With the assistance of minimum mean squared error (MMSE)-based SIC, [271] utilized an upstream RSMA to assure max-min user integrity in single-input multi-output (SIMO) NOMA systems. The work [272] utilized uplink RSMA for physical-level network slicing to provide ultra-reliable and lower-latency (URLLC) and enhanced or improved mobile broadband connectivity (eMBB). References [273], [274] utilized uplink RSMA in aerial networks to improve communication reliability, reduce interference, and improve weighted sum-rate effectiveness. Moreover, the research [275] utilized the utility of RSMA for satellite communications by integrating beamforming and uplink RSMA. Reference [276] introduced a collaborative RSMA for uplink user collaboration. The work [277] examined outage behavior for a two-user upstream RSMA system taking into account all potential SIC decoding orders.

Although NOMA-MEC allows several users to transfer their computing workloads to a base station at the same time, the implemented NOMA with SIC may not attain the entire capacity domain of uplink multiple access streams, limiting the system efficiency of NOMA-MEC systems. To reach the full capacity domain of uplink multiple access streams extensive research is necessary to establish the appropriate SIC decoding sequence and transmit power assignment. The works [278], [279], therefore, analyzed the deployment of uplink RSMA in latency-aware MEC scenarios. To use RSMA for uplink MACs, efficient interference control, and low-complexity SIC handling are on the horizon. The work [280] proposed a CR-inspired rate-splitting scheme to maximize the achievable rate of a secondary user (SU), meanwhile maintaining the primary users' (PU) outage performance the same as orthogonal multiple access (OMA).

Inspired by the capability attained by uplink RSMA as well as CR-inspired rate-splitting the work [281] envisioned an RSMA-assisted MEC (RSMA-MEC) strategy to boost the successful computing probability (SCP) and minimize offloading delay in a MEC mechanism. A single MEC host and many randomly deployed users comprise the network. Since user or device geo-positions have a substantial influence on channel conditions, acceptable and realistic location modeling is required to assess system efficiency. As a result, the work considered that the positions of randomly dispersed users pursue a uniform Poisson Point Process (PPP) [281]. Recognizing the impact of user geo-positions and related inter-user interference, it separated users into a centralized and an edge or periphery cluster to construct a paired-user CR-based RSMA and utilized it to facilitate MEC.

7.2. Unmanned Aerial Vehicle (UAV)-Assisted MEC

Typical grounded infrastructure-based MEC systems are inapplicable in dense urban or non-rural regions or environmental disaster zones since establishing network services in these hostile conditions is typically inefficient. Admittedly, aerial edge computation mechanism, namely, UAV-enabled airborne MEC paradigm obtained increased research interest from both business and academia [282]. Because of UAVs' inherent characteristics such as on-demand implementation, relatively inexpensive, configurable maneuverability, line-of-sight (LoS) communication, high gliding altitude, etc., UAVs exerting as aerial MEC stations can be used in a variety of scenarios ranging from civilian to military for important tasks. When the servers integrated with base stations are overcrowded or inaccessible, aerial or UAV-aided MEC systems may often act as a supplement to terrestrial MEC networks. The LoS communication and mobility of UAVs, in particular, can considerably minimize task offloading latency as well as energy usage for MEC platforms. Fig. 12 depicts UAV-assisted MEC infrastructures.

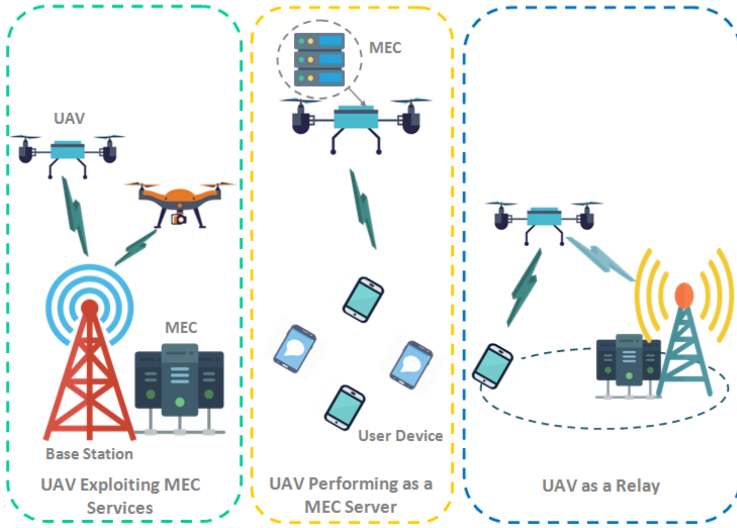

Fig. 12: UAV-assisted MEC infrastructures.

As a result, the merging of UAVs with MEC is considered to be a win-win solution for next-generation communication systems, playing a critical role in delivering flexible and omnipresent communication and computing services in a variety of circumstances [283], [284].

When compared to traditional ground infrastructure-based MEC solutions, UAV-aided MEC has demonstrated significant benefits, owing mostly to the unique characteristics of UAVs [285]. Some of the primary benefits of UAV-aided MEC are stated below:

Ad-Hoc and Cost-Effective Implementation: Due to UAVs' better scalability and ease of deployment, UAV-aided MEC frameworks can be rapidly dispatched at reasonable costs in response to real-time requirements and offer computation offloading potentials to users with constrained local computing capacities, particularly in areas where connectivity facilities are infrequently distributed or even completely destroyed.

Coverage and Computational Performance Optimization: Since UAVs often fly at a higher altitude; a vast region may be successfully served with a small subset of UAVs. More crucially, with the use of inter-UAV linkages, a swarm of UAVs, i.e., a flying ad hoc network (FANET) may collectively accomplish activities in large-scale locations. While performing as an auxiliary computational service vendor, MEC servers enabled by UAVs can also considerably increase computation capacity in hotspot locations, allowing more users to be supported through powerful computational services.

Consistent LoS Offloading Connectivity: Besides increased coverage, another advantage of greater cruising altitudes for UAVs in airborne MEC is the increased likelihood of LoS connections. As compared to terrestrial fading mediums, LoS connections can provide more dependable wireless connections for workload offloading and computational outcome downloading, meeting MEC's rigorous QoS criteria.

Energy Usage and Delay Reduction: Controllable mobility of UAVs offers an extended technical dimension of freedom (DoF) for airborne MEC as compared to ground infrastructure-based MEC platforms. Better channel characteristics can be achieved by UAV trajectory adjustment. The offloading energy usage and task delay for UAV-aided MEC may thus be greatly decreased when combined with suitable resource allocation algorithms.

UAVs are classed into numerous categories based on their size, weight, wing design, flight time, and altitude [285], such as higher altitude platforms (HAPs) vs. lower altitude platforms (LAPs), rotary-wing vs. fixed-wing, big vs. small or miniature UAVs, and so on. Depending on the specific application circumstances, many varieties of UAVs can indeed be operated for UAV-assisted MEC. Fixed-wing UAVs, including small airplanes, have faster flight speeds, longer ranges, and can carry heavier weights than rotary-wing UAVs; however, they must constantly move forward to stay aloft. Hence, fixed-wing UAVs often fly ahead indefinitely and are utilized to cover a broad region while providing computing facilities. Rotary-wing UAVs, on the other hand, like quadrotor drones, may hover over a specified spot. Furthermore, loads of rotary-wing-based UAVs are generally tiny because of their tiny shape and weight. The main advantage is that they can land and take off vertically without the need for an airfield or launcher, allowing for faster and more flexible deployment. HAPs typically fly up to 17-22 km altitude and are intended for long-term services (days or months) over wide geographic regions [286]. The advantage of LAPs is their inexpensive cost and quick deployment or replacement, notwithstanding their limited computing capacity.

As previously stated, UAVs can function as airborne base stations incorporating MEC workstations to deliver computational services to wireless users in places where network infrastructures are unevenly dispersed or even completely destroyed. Furthermore, while infrastructure-based MEC implemented within a preset territory may be unable to adjust with time-varying configurations of service demands, UAVs can be quickly deployed to designated locations to address temporary or unanticipated demands. UAVs, on the other side, can operate as relays to help users offload tasks to more capable distant MEC nodes with two or even more hops. Since UAVs may modify their placements to experience optimal channel conditions, UAV relays provide additional options for a performance increase when compared to traditional static relaying. Owing to a single UAV's limited processing capacity, numerous UAVs can collaborate to enhance the coverage area and computational capability, where extensive design is needed for cooperative computing procedures. Additionally, using inter-UAV linkages, a swarm of UAVs may be built as a FANET. In this context, task bits produced by small UAVs can be transferred to a lead UAV with rich computational power for real-time computing. Moreover, workloads from ground users can be assigned among numerous UAVs within the FANET. LAPs can potentially be combined with HAPs and ground infrastructure to establish an information network. Since HAPs own a broad outlook on the entire system, they are accountable for offering omnipresent connectivity and computing services, whereas LAPs complement the terrestrial MEC systems and ensure high QoS standards [287], [288].

Inspired by the great versatility of UAVs Jiang et al. [289] investigated a multi-UAVs-aided MEC platform in which UAVs perform two roles, contributing to facilitating computation or functioning as relays, to minimize total usage of time and energy. As a result, an optimization approach is devised to reduce the total power utilization of the MEC unit. The problem is then defined as a Markov process of decision-making. Afterward, two reinforcement learning approaches, Q-learning as well as competitive Deep Reinforcement Learning are suggested to find the best policies for computational offloading as well as resource allocation. Diao et al. [290] investigated a UAV-assisted MEC platform with a multi-antenna base station. The work explored offloading optimizations and scheduling solutions for energy consumption reduction. Apostolopoulos et al. [291] proposed a unique data-offloading decision-making paradigm in which users can partially offload their content to a sophisticated MEC system comprised of both terrestrial and UAV-mounted MEC workstations. Zhang et al. [292] presented and analyzed UAV-assisted MEC system in which a hovering UAV as well as a terrestrial base station endowed with computational capabilities serving a variety of ground UDs. The system intended to reduce the weighted expense of time delay and energy usage while keeping offloading selections and resource competition in mind.

7.3. Energy Harvesting, Simultaneous Wireless Information and Power Transfer (SWIPT), and MEC

The modern industrial environment is more conscious of its obligation to optimize energy consumption and management across all areas, including communications. Energy harvesting [293], often referred to as power harvesting or energy scavenging is a viable technology for 5G networks as it provides a viable alternative to standard energy supply sources [294]. The primary idea behind energy harvesting is to harvest various accessible energy sources and use them to power energy-constrained devices to extend their lifetime. Energy harvesting, in conjunction with the conventional power grid, can assist in meeting the energy demands of the different layers of 5G and beyond 5G networks, such as sensing devices in IoTs, portable devices, base stations in HetNets, helping relays in D2D networks, and computing servers. Furthermore, new advancements in sophisticated materials and equipment designs aid in the realization of energy-harvesting circuitry for tiny portable consumer electronic devices, accelerating the use of energy harvesting for IoT devices. Energy harvesting is simple in principle but complex in execution, which is heavily influenced by the sort of energy harvesting source. Harvestable energies can be derived from environmental or man-made sources that are either controlled or uncontrolled. To exploit the respective energy sources, several energy harvesting technologies (e.g., pyroelectrics, electrostatics, photovoltaic conversion, piezoelectrics, thermoelectrics, and radio frequency (RF)-based energy harvesting) can be used. Moreover, various devices may harvest varying amounts of energy; for instance, wearable devices [295], intelligent footwear [296], etc. RF transmissions are less impacted by climate or other ambient environmental variables than conventional natural energy resources. As a consequence, these signals may be easily managed and planned, and radio frequency-based energy harvesting has a high potential to offer steady energy to low-energy systems such as IoT devices, wireless sensing networks (WSNs), and remote geographical area connectivity scenarios in 5G and beyond networks. Radio frequency-based energy harvesting can scrounge wireless energies from (i) ambient resources (e.g., FM, AM, and WLAN) that can be predictable or sometimes uncertain, or (ii) specialized sources that are placed to perform as an energy supply. Radio frequency-based energy harvesting from ambient sources generally necessitates an intelligent mechanism that monitors communication frequency ranges and time frames for harvesting possibilities. Wireless Power Transfer (WPT) may be regarded as radio frequency-based energy harvesting with effective management of specialized energy sources between emitters and harvesters.

SWIPT works in the same way as a standard wireless telecommunications network that consisted of a base station and several mobile user devices. Antenna arrays are installed upon that base station. The radio frequency signal resource provided by the base station may be utilized to transport both energy and information. Every mobile station changes communication modes randomly to capture information, energy, or perhaps both. In particular, under the D2D scenario, power and information can be delivered in both bi-directional orientations between smart devices.

SWIPT technology combines WPT with Wireless Information Transmission (WIT). Nicola Tesla introduced the WPT technique in 1914 [297]. It is currently transformed into two primary branches: far-field WPT-based electromagnetic (EM) emission and near-field WPT-based EM interaction, all of which are gaining popularity due to their safety, versatility, and environmental friendliness. For quite a long time, academics have been interested in near-field WPT transmission systems because of their close to 90% power transfer efficiency (PTE) and tens of kilowatt transmission capacity [298]. The failure to fulfill mobility, on the other hand, is a fatal flaw. When compared to cable charging, the advantage of near-field WPT appears to be minor. Neither the issue of battery scarcity nor the hassle of recharging can be alleviated. Far-field WPT, particularly when paired with WIT technologies, on the other hand, presents a viable solution to the dispute between the high rate of transmission and extended lifespan of battery-powered devices in 5G and beyond communication systems while satisfying wireless charging standards for mobility.

To date, most manufacturers have focused solely on WPT technology, particularly near-field WPT systems, which have seen significant commercial success in recent years. Some prominent handset manufacturers have announced the availability of smartphones that feature coupling-based WPT, while electric vehicle (EV) manufacturers are eager to file patents enabling coupling-based wireless recharging. The advancement of distant range WPT is not being considered. As a result, this survey intended to present the commercialization development of far-field WPT. Unlike the Wireless Power Consortium (WPC) which focuses solely on magnetic inducing or resonation technique the Air Fuel Alliance (AFA) [299], the main global institution on WPT standards and technologies includes not only magnetic technologies but also radio frequency technologies to address a variety of circumstances. In the year 2019, Air Fuel Alliance Development Forum occurred in Shenzhen, China, on March 12th and 13th [300]. On the forum, a few RF-based WPT devices were exhibited. These systems are developed based on a power emitter, a harvesting unit, and a charging station; with a maximum transmission power of up to 100 kW [301]. Powercast has the greatest charging distance among these items or devices, reaching 24 m at a 915 MHz frequency [302].

This section introduces four common resource allocation schemes. Most academics concentrate on various allocation algorithms, whereas other antenna developers are interested in new antenna structure designs.

Power Splitting (PS): Power splitting is the best approach to achieve simultaneous information and power transmission. The radio frequency signal captured by the antennas is segregated by the power splitting architecture with a specified power splitting ratio β, whereby β % of such signal goes to the decoder circuitry and (1- β) % passes to the battery circuitry at the same time [303].

Time Switching (TS): Time Switching is a low-complexity design that only requires a switching module ahead of the receiver structure. The equipment is in the phase of information transfer whenever the switching circuit is switched to the decoder circuitry. When it changes to the battery circuitry, the state of the transfer of power is activated [304].

Antenna Switching (AS): Antenna Switching is a simple construction with several antennas. It is comparable to a split antenna arrangement, with the exception that the receivers cannot collect information and power at the same time. When the energy-collecting antennas are activated, the entire RF signal resources are utilized to charge the batteries. While the information-collecting antennas are engaged, the RF resources are utilized for decoding [305].

Antenna Separated: Multi-antennas are used at the transmitters to realize the segregated transmission structure. Certain antennas are employed for power transfer, while others are utilized for data communication. Apart from that, the inside architecture of the antenna has gained recognition. A dual-band antenna configuration is developed in the paper [306] to broadcast mmWave signals at two separate frequencies. Furthermore, high frequency is utilized for power transfer while low frequency is employed for transmitting information. A comparable dual-band antenna may be installed equitably on terminal devices.

Scientists and engineers have suggested SWIPT-based MEC systems to enable all devices to experience real-time and high-throughput facilities [307].

SWIPT technology enables networks to deliver the computation result and energies to the device through the downlink at the same time. Moreover, this method can compensate for the issue of high attenuation in typical long-distance wireless power transmission [308], [309]. Typically, the two most common SWIPT transmission mechanisms are Power Splitting and Time Switching. Although the MEC server's energy transmission is adequate for devices near the base station (BS), it is insufficient for devices that are perpetually outside of the MEC service range. Insufficient power causes the equipment to go out of operation abruptly, which is deleterious for human-embedded devices or safety detecting systems. To compensate for this weakness, several researchers proposed SWIPT-based D2D networking [310]-[312]. This network enables devices with adequate energy to send energy to devices that have limited energy capacity.

Among the foregoing radio frequency signal resource provisioning schemes, there is a typical and crucial difficulty that exists throughout the SWIPT framework, i.e., the radio frequency-energy harvesting tradeoff [313], [314]. How much radio frequency signal resources ought to be dedicated to information processing to maintain excellent communication performance, and how much should be dedicated to energy harvesting to extend the device's lifetime? Regardless of whether additional antennas are allocated for information transmission, the radio wave power passing to the decoding unit is increased, thereby, the amount of information harvesting is increased and all of these procedures result in the insufficient radio frequency signal remaining for battery charging. Consequently, in most circumstances, finding a suitable allocation mechanism to maximize the tradeoff is critical to the SWIPT mechanism.

Cooperative task offloading or transferring and resource distribution in energy harvesting-enabled small cell network systems is discussed in [315], [316] to optimize the number of workloads or tasks executed by edge computing nodes while minimizing their latency and energy costs. The researchers presented a Deep RL-based methodology for online transferring to minimize computing complexities in large energy harvesting-driven systems in their papers [317]-[319]. The works [320], [321] applied DL approaches which learn binary offloading selections based on previous offloading experiences and suggested techniques successfully improve workload offloading behavior. A decentralized implementation of suggested techniques, on the other hand, is still required to allow users to determine offloading selections in a distributed way through a learning process. Furthermore, [322] presented a privacy-aware offloading technique based on the RL algorithm for a medical IoT device powered by energy harvesting. The policy for task offloading implemented by the edge device may be established by considering the degree of privacy, energy usage, and computational delay through each time slot. The authors investigated computational offloading and resource management for energy harvesting in [323]-[325]. These mobile devices first gather energy from RF transmissions, which they may utilize to conduct local activities or transfer (tasks) to a MEC host. Several alternative offloading techniques can also attain self-sufficiency. State-of-the-art approaches for task transporting in MEC and radio power transmission to end terminals are reported in [326]. The authors proved the efficacy of the WPT approach in charging high-end cell devices, which have become increasingly prevalent in MEC. Yet, when computational resources become limited, MEC's performance may suffer. As a result, they emphasized the impact of deciding across task-offloading solutions and offloading positions on the energy consumption of MEC systems.

7.4. Intelligent Reflecting Surface (IRS)-Assisted MEC

An IRS can adjust the wireless network intelligently to optimize signal strength obtained at the destination. This is in stark contrast to previous strategies that improved wireless communications by improvements at the transmitter or recipient. An IRS is made up of numerous IRS components, each of which may reflect the incoming signal at a different angle. The transmitted message in such IRS-assisted connections flows from the sender or transmitter to the IRS gets enhanced at the IRS, and then goes from the IRS towards the receiver or recipient. This type of communication technology is especially beneficial when the transmitter and receiver are separated by a weaker wireless channel caused by barriers or bad environmental circumstances, as well as when they do not share a line-of-sight link. Fig. 13 illustrates an IRS-assisted MEC transmission paradigm.

IRSs are expected to play a major function in 6G networks due to their capacity to configure wireless environments, according to numerous wireless communications specialists. In November 2018, a Japanese network operator named NTT DoCoMo and MetaWave, a startup, showed the application of IRS-like innovation for supporting radio transmission in 28GHz frequency [327]-[329]. IRSs have also been compared to 5G communication systems' massive MIMO technique. IRSs reflect radio signals and hence use less (active IRSs) or even no power (passive IRSs), but massive MIMO emits signals and requires significantly more power [330]-[332]. In just the same sense, researchers of [333] contrasted the energy consumption of IRS-assisted systems with amplify-and-forward (AF) relay networks, while the researchers of [334] evaluated the effectiveness of IRS with decode-and-forward (DF) relays.

IRSs have already been presented and widely researched in recent times as a viable technology for forthcoming wireless communication networks [335], [336]. An IRS, in particular, is a vast array of passive elements or components. By adaptively regulating the mirrored EM waves' phase-shift that impact upon the surfaces, it can provide a desirable wireless propagation scenario between transmitting and receiving devices [337], [338]. By applying IRS in communication networks, channel power gain may be successfully increased and transmission QoS can be optimized without consuming substantial additional power.

Recent breakthroughs in configurable meta-materials make it easier to build IRSs [339] for improving the spectrum and power consumption of wireless communications. An IRS, in particular, is made up of IRS supervisor (typically a microcontroller) and a huge number of passively reflecting components. According to the IRS controller's directives, each IRS reflective element is susceptible to altering both the phase and amplitude of the mirrored waves, thereby, cooperatively modifying the data transmission environment.

IRSs achieve gain by combining virtual array-generated gain and reflection-assisted beamforming gain. These virtual array gains are generated by integrating both the LoS and IRS-reflected radio waves, whereas the reflection-assisted beamforming gains are acquired by actively regulating the phase shift generated by IRS components. By integrating both of these distinct advantages, the IRS obtains the ability to increase the offloading likelihood of success of devices, hence enhancing the capacity of MEC frameworks.

Minimizing execution latency and minimizing energy usage are two legitimate goals in the context of task or workload offloading in MEC platforms.

Existing works (e.g., [340], [341]) on IRS-aided MEC mechanisms have demonstrated that properly implementing an IRS next to the offloading subscribers or devices and efficiently constructing the passive beamforming can assist the reconfiguration of the computation-load dispersion among users. Moreover, it can improve the device-to-MEC data transmission rates, thus significantly minimizing their computation-offloading latency, particularly when the device-to-MEC LoS links are blocked.

If the primary LoS link connecting the wireless user devices and MEC stations is obstructed, the data can indeed be transferred via the IRS-assisted mirrored channel. Reflection-based beamforming may be implemented explicitly by concurrently adjusting the reflection parameters of IRSs. That includes both the enhancement of the transmission rate for cell edge user devices and strengthening physical-level security. Consequently, with the assistance of IRSs, MEC's overall performance may be significantly enhanced [342]. Additionally, unlike traditional transceivers, IRSs require just low-complexity control circuitry rather than a high-power-based radio-frequency chain. As a result, they may be densely placed at a low expense and use of energy to facilitate ubiquitous MEC. Moreover, integrating IRSs into current MEC platforms does not need the development of unique conventions or MEC hardware [343].

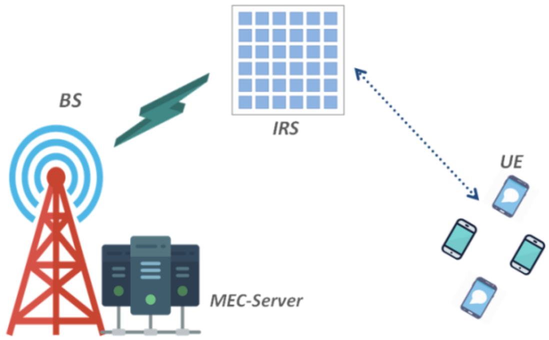

Fig. 13: IRS-assisted communication in an MEC paradigm.

Zheng et al. [344] explored the latency reduction challenge by developing IRS-assisted MEC networks. Chen et al. [345] proposed a unified dynamical beamforming approach to enhance the total computational rate of an IRS-assisted MEC infrastructure, whereby each device adopts a binary offloading strategy. Zhou et al. [346] investigated a collaborative task computing architecture in which the source node transfers some of its computational tasks to multiple user devices with the support of double IRSs. Chen et al. [347] designed and analyzed the IRS-aided wireless-powered MEC system in which each device's computational workload is separated into two sections for local processing and offloading to MEC servers. Both Time Division Multiple Access (TDMA) and NOMA techniques are studied for offloading. Ha et al. [348] studied the effectiveness of an IRS-assisted uplink NOMA-based MEC system considering a Nakagami-m fading channel.

7.5. Game Theory for MEC

Game Theory has already been utilized successfully to develop, design, and improve the functioning of numerous representative telecommunications and networking systems. The games in such situations, as usual, contain a diverse set of participants with competing objectives.

Game theory [349] is a mathematical application that is employed in the analysis of the tactics used by various participants while making decisions, resulting in an increase in reward among them as well as an increase in the reward for a specific player. O. Morgensterns and J. von Neumann were the initial researchers to employ games in zero-sum contests, which are games with just one participant [350]. Cooperative game theory refers to a type of game whereby a set of players' activities and formation impact the outcome of the game. Non-cooperative plays or games, on the opposite hand, do not need players to work together to decide the game's conclusion. Each participant can perform their actions, and the ultimate consequences are determined by their activities [351]. Furthermore, in non-cooperative games or plays, each participant can pick from a list of rules.

In simple words, Game Theory is a field of practical mathematics that explores how rational individuals may interact amongst themselves to acquire stable management of system facilities to satisfy the service objectives (of those players) when faced with a combination of common and finite network resources. Game Theory investigates the interactions of self-interested and autonomous actors. There has been a significant amount of studies in wireless network technology over the past few years, as well as at the present moment, there is a great interest in applying Game Theory in wireless communications [352], such as cognitive radio or spectrum sensing [353], sensor networks [354], [355], and multimedia social networks [356].

Game Theory can provide helpful recommendations for administering wireless data connections to handle the rising MEC issues, such as energy consumption, storage, virtualization, and computation at the edge of the network.

Game theory, which is augmented with the assistance of learning algorithms [357], contributes significantly to the management of parameter configuration, as well as their modeling and evaluation. Initially, the work will go through the benefits that non-cooperative (NC) Game Theory may utilize in a variety of wireless network domains. In network resource distribution, non-cooperative Game Theory helps to improve the strategy of using a shared pool amongst a group of customers that wish to use a limited number of resources fairly. This means that non-cooperative Game Theory enables elastic and scalable resource management. The fundamental issue in power control is distinguishing and reducing signal interference. Without non-cooperative Game Theory, energy usage is enormous in this case, and non-cooperative Game Theory assisted in resolving this issue. Non-cooperative Game Theory improves the management of a specific communication link that will be shared by multiple users in the context of MAC. Multi-rate adaptive forwarding with non-cooperative Game Theory is used to direct traffic across a network to maximize end-user performance. For security, non-cooperative Game Theory is employed to maximize network longevity while allowing low-power computing and IoT connectivity. Together with this, wireless nodes stay competitive against one another for a constrained shared resource. Previously an algorithm is utilized that overcomes the problem of adaptability as opposed to the centralized model. Moreover, MEC delivers computing capabilities within close proximity, to provide the optimum user experience [358].

Li et al. [359] proposed a Game Theoretic approach for power management in interference-aware multiple-user MEC systems. The research [360] investigated relative delay minimization in MEC-enabled UAV clusters. The optimization issue is described as an offloading game to address the challenge in dispersed UAV networks. Wang et al. [361] examined the topic of computational offloading in MEC systems in the case of vehicular communications and presented two algorithms: the game-based computational offloading (GBCO) algorithm and the optimum offloading algorithm. Li et al. [362] presented a Game Theory-based method for task/workload offloading and resource management in the MEC framework to minimize energy consumption and delay. In [363] game theory and DRL are utilized to offload computational tasks in a dynamic edge computing paradigm. Xia et al. [364] proposed Game Theory-based mobility-aware computation offloading and resource management strategies for MEC systems.

7.6. Auction Theory and MEC

Despite its many advantages, MEC exhibits significant resource management challenges. Edge servers in MEC, in particular, often have constrained storage, computing, and network resources, but end users or subscribers have rapidly increasing processing needs. As a result, one difficulty is determining how to optimally distribute services to users. Furthermore, the MEC invites new service providers or vendors into the computing market. Since both vendors and users are inherently selfish [365] motivating vendors and users to engage in the market is a different challenge.

Auction Theory, a prominent economic technique, has been frequently employed to handle similar challenges, for example, in wireless communications [366]. Auction-based systems, in particular, are promising because they may fairly and effectively allocate sellers' constrained resources to purchasers in a transactional form at competitive pricing. Trustworthiness, trade balance, independent rationality, and economic productivity are all desired qualities of an ideal auction-based system [367]. Auction-based processes ensure that resources are distributed to the purchasers who place the most worth on them. Considering these benefits, various works have lately utilized Auction Theory to tackle the resource management problem in MEC. It is based on previous research that different sorts of auction techniques are appropriate for various kinds of issues in certain application contexts.

7.6.1. Terminologies of Auction Mechanisms

The following are the standard terminologies and classifications of auction mechanisms used in auction literature [368]:

Auctioneer: An auctioneer is often an executor who implements the auction mechanism and decides the champions and payments including both bidders (purchasers or in this sense users) and sellers (in this context MEC service providers) based on the auction guidelines. The auctioneer in the MEC marketplace might be a resource provider or a trustworthy third party.

Bidder: A bidder is indeed a purchaser who wants to buy products or services from vendors. In the MEC marketplace, user devices often operate as buyers looking to acquire a variety of resources (e.g., computing, caching, content delivery resources, etc.) to complete compute-intensive and latency-sensitive computational workloads. Auction participants include both bidders as well as sellers.

Seller: A seller is the proprietor of the auction items or services who wish to sell those at a specific price to maximize profit. Edge servers often operate as merchants (or sellers) in the MEC marketplace, owning a variety of commodities like computation and storage facilities, networking bandwidths, and so on.

Price: Typically, the price was determined by competitiveness during an auction procedure. It might be an initial price at which a seller consents to sell the product or resource, a bidding price, it is the price at which a buyer consents to pay for the resource, or a closing price (the transaction price), which is the ultimate purchasing price in the event.

Commodity: A commodity is a trade object between a supplier and a purchaser in an auction. Sellers compete with buyers to sell a valuable product at the best possible price. Products in the MEC market might be computational services, caching services, or network services.

Auctions can be classified in a variety of ways, both in theory and in practice [369], however, they are frequently classed according to the following characteristics [370]:

Single- vs. Two-Sided Auctions: Only one party (buyers or sellers) can put bids during a single-sided (i.e., forward and reverse) auction. In the context of a two-sided auction, both sides can put bids.

Uni- vs. Multi-Attribute: Allotments in uni-attribute bidding or auction are defined only by one characteristic (e.g., bid price). On the other hand, under a multi-attribute auction, additional qualities (for example, QoS) are also taken into account.

Open-Cry vs. Sealed-Bid: At open-cry bidding, each bidder screeches out his bid, but in a sealed-bid context, each bid is placed discreetly.

Single- vs. Multi-Item (Combinative) Auctions: A single-item bid trades only one kind of product on the marketplace, whereas a combinative auction trades numerous sorts of things.

Single- vs. Multi-Unit: In the context of a single-unit bid, just one unit of every item may be traded; however, many units can indeed be marketed or traded throughout a multi-unit auction.

An auction process can be characterized further according to the periods at which the marketplace is cleared [370].

Offline Auction or Bid: Once all bids have been received, the marketplace is cleared.

Online Auction: Buyers come and leave without notice, and the auctioneer eliminates the market in real time as soon as an updated request is received or a new option becomes available.

Sequential Auction: Buyers can place several offers, as well as the auctioneer eliminates the marketplace regularly within a selected time constraint.

The primary purpose of auction technique design is to establish auction guidelines so that a targeted objective is attained in the convergence of selfish actors' behavior. As a result, with an auction mechanism that is properly built, the necessary auction aims will be easily attained while selfish actors pursue their motivations and preferences. The following portion describes a few of the desired qualities in auction mechanism development.

Trustworthiness: Guarantees that participants' fairness is within their best interests, and hence they cannot gain from dishonesty [371].

Independent Rationality: By applying the technique, any participant can raise his or her benefit [372].

Trade Balance: The market neither builds surpluses nor runs deficits [373].

Economic Productivity: The maximization of value across all individuals (social welfare) entails a socially optimal distribution of resources. Furthermore, if the utility loss tends to be null as the highest social benefit approaches indefinitely, the mechanism is referred to as Asymptotically Efficient [372].

Computational Tractability: The auction process clears the marketplace by discovering commodity allocation and price within a tractable calculation time [372].

7.6.2. Auction Approaches for MEC

In general, the MEC trade consists of several sellers or vendors and numerous buyers or user devices, with buyers requiring sellers' resources to complete computational-intensive and latency-sensitive activities. Because of its many-to-many structure, multi-item auction or bidding is widely used to handle resource trade in the MEC trade [373]. Furthermore, in the MEC trade, user devices often bid for a combination of resources (e.g., computation, storage, networking, energy, and so forth), and combinative bidding [374] is an appropriate method. As a result, the next sections introduce combinative [375] and multi-attribute auctions [376], [377].

Combinative Auction: A combinative or combinatorial auction is a type of auction whereby each buyer bids on a variety of commodities. In contrast to typical auction systems, purchasers can acquire a package of combinative commodities, including many sorts of commodities.

Each bidder or purchaser puts a bid to the auction house or vendor in the combinative bidding, indicating the demand for a group of products instead of a single item. The auctioneer provides an efficient allocation system over purchasers after accumulating bids/asks given by buyers/sellers. Contemplate a combinative bidding in a MEC trade for computing service provision. The market consists of three purchasers (bidders) and one vendor (auctioneer). Purchasers place a bid to vendors that describe the computational resource requirements. Each offer, in particular, reflects the need for computing and energy resources. The challenge then becomes determining who the winners are and how much each winner must pay. Certain optimization methods, such as greedy algorithm [378], dynamic programming [379], and graph neural network algorithm [380], can be used to tackle this problem.

The combinative auction is ideal for trading a package of complementary products and may effectively increase the auction effectiveness of allocating multiple commodity combinations.

Multi-Attribute Auction: It is commonly used to solve optimum resource allocation issues in MEC. Unlike traditional auctions (for example, Dutch auction [381], English auction [381], first-price and second-price-based sealed or enclosed-bid auction [382]), a multi-attribute auction is a many-to-many framework, meaning that the number of vendors and purchasers is even more than one. For a multi-attribute auction, vendors and purchasers submit their inquiries and bidding prices to an auction house, which acts as the auctioneer's agent. The auctioneer then organizes the asks (retailer's prices) and bids (bidder's prices) in ascending and decreasing order. The auctioneer then computes the transaction price. Eventually, the successful bidder obtains the product and pays the associated seller. Repeating the preceding procedure will reveal the matching association between the remaining purchasers and vendors, as well as related hammer prices.

7.7. Digital Twin-Enabled MEC

Digital Twin is an effective method of connecting the real and digital worlds [383]. Digital Twin has undergone four development cycles as a result of enhanced communication and computing technologies, including information emulating, digital simulations, value systems chain interaction, and linked operational and industrial activities. To that aim, there are three types of Digital Twins, with specific definitions as follows:

Monitoring Digital Twin: In this context, Digital Twin is employed to monitor a physical item [384]. The physical item has no interaction with its virtual environment, and modifications to the physical entity do not influence its virtual form after it has been generated and vice versa.

Simulation Digital Twin: Digital Twin is characterized in this context as a simulation tool or program [385]. Physical things may be understood, anticipated, and enhanced by computer simulation, allowing their effectiveness to be enhanced. The virtual model evolves alongside the actual thing, but the physical item does not alter in response to the virtual model's dynamism.

Operational Digital Twin: The data flow between physical items and the respective twins is bilateral in this situation [386]. Specifically, physical things broadcast information and updates to their twins, which are formed and updated depending on that knowledge, and the actual object's circumstances may be anticipated. Conversely, the twin will transmit back information, including ideal remedies for a specific issue, to direct physical object actions.

Based on the preceding criteria, Digital Twin is now commonly referred to as "*an intelligent and developing system that correctly and digitally copies a physical thing across several granularity layers and monitors, regulates, and improves the physical object throughout its life cycle*" [387]. Digital Twin is made up of three parts: (i) tangible items, such as a car, a robot, a complicated system, or a human; (ii) digital twins of physical items; and (iii) connections between physical items and their digital twins. The physical items convey their status and produced sensing data to the interactive twins for Digital Twin modeling and updating via the link, and the interactive twins offer feedback towards physical objects. As a result, dynamic interactions and the synchronized evolution of the actual item and its virtual duplicate are possible. To that purpose, Digital Twin is an effective method for simulating, analyzing, forecasting, and optimizing the physical model throughout its entire life cycle. Fig. 14 shows the evolution of Digital Twin.

Subsequently, a new approach called the Digital Twin-enabled MEC network has been developed to bridge the gap between the physical MEC facility and digital systems [388]. Digital Twin models are developed and managed by Digital Twin-enabled MEC network with the help of the networks' edge [389]. The Digital Twin-enabled MEC network is made up of three technical segments: the edge layer, the device/physical layer, and the Digital Twin network. Local computations and connectivity are handled just at the physical level, as well as the physical layer's real-time state and modeling parameters are transferred to the edge layer through physical-to-physical communication. Real-time Digital Twin models and modifications are handled at the edge of the network. Edge units, such as base stations, can gather physical elements' functioning status information and evolve their behavioral model depending on the acquired data in time-varying surroundings. Furthermore, edge nodes continually check the status of physical components to ensure compatibility with the respective twins. Digital Twin may be installed on any edge computing server, and indeed the edge tier is invisible to users. Conversely, all users are capable of exchanging edge services (with each other). Using twin-to-twin connectivity, Digital Twins are virtually joined to form connectivity with shared infrastructure in the Digital Twin network. Digital Twin-enabled MEC network can capture real-time network characteristics and utilize them to make optimum network decisions instantly from a centralized standpoint. In this purpose, the desired Digital Twin-enabled MEC network may be used to directly develop and optimize network strategies such as workload offloading, allocation of resources, caching, and so forth, and the connectivity schemes' effectiveness and affordability can be improved. In reality, without a Digital Twin-enabled MEC network, continual connections among edge computing servers and devices under their coverage are necessary to collect real time feedback for task transferring and resource allocation choices. As a result, the deployment of Digital Twins aids in getting optimal resource provisioning solutions while reducing communication costs. Digital Twin-enabled MEC network can enable computationally intensive applications like Metaverse [390] and automated vehicles [391], [392]. Fig. 15 depicts the structure of a Digital Twin service-based MEC platform.

The Digital Twin-enabled MEC network framework is separated into three tiers: the physical layer or level or tier, the virtual tier, and the application tier. In a MEC framework, the physical tier includes all physical equipment, such as end-user devices and edge computing servers, as well as the wireless connectivity infrastructure. End devices have limited computing and storage capabilities, therefore tasks must be offloaded to one or even more edge computing platforms for cooperative computation. Twin mappings exist in the virtual tier such as identical or twin-end devices, twin edge computing hosts, and twin communication environments (networked physical items and wireless communication environments of the physical tier). Metadata such as the actual entities' real-time status are captured in the physical tier and then transmitted to the virtual tier twins through physical-to-twin connections [393], [394].

The virtual layer includes the Digital Twins that completely replicate the physical items and govern and regulate the physical layer through simulations, predictions, and optimizations [394]. The Digital Twin system records original data of physical things, such as hardware configurations, user details such as geo-location and available resources, statistical facts, and real-time MEC server operating status, and it also monitors the system's dynamism. This information is vital for building high-precision Digital Twin models of physical things and communication environments in the virtual tier. In reality, however, it is difficult to mimic a physical phenomenon/entity virtually which will be absolutely equivalent to its physical counterpart. Moreover, several critical aspects must be considered, such as reliability, fault tolerance, reduced latency, and security. To address these difficulties, sophisticated enabling technologies like connectivity, data processing, management approaches, Machine Learning, and Blockchain may be deployed to Digital Twin modeling techniques and making decisions while safeguarding user privacy. Relying on the various developed concepts and big data, Digital Twins may aid in finding intelligent approaches to application layer challenges including task transferring and allocation of resources in IoT [395], [396], vehicular communications systems [397], [398], the space-air-ground integrated network (SAGIN) [399]-[401], health services [402], wireless infrastructure [403], and so on.

Additionally, effective interconnections between Digital Twin-enabled MEC network system levels are necessary to connect physical things, twins, and services [404]. The twin-to-physical entity interface, in particular, allows real-time interactivity between both the Digital Twin tier and the physical tier. The system's broad information may be retrieved by communicating between twins via twin-to-twin integration. Moreover, services such as IoT, transportation networks, and healthcare seek a function from the Digital Twin-enabled MEC network platform via twin-to-application interactions, and the virtual tier feeds back the ideal selections to the application tier.

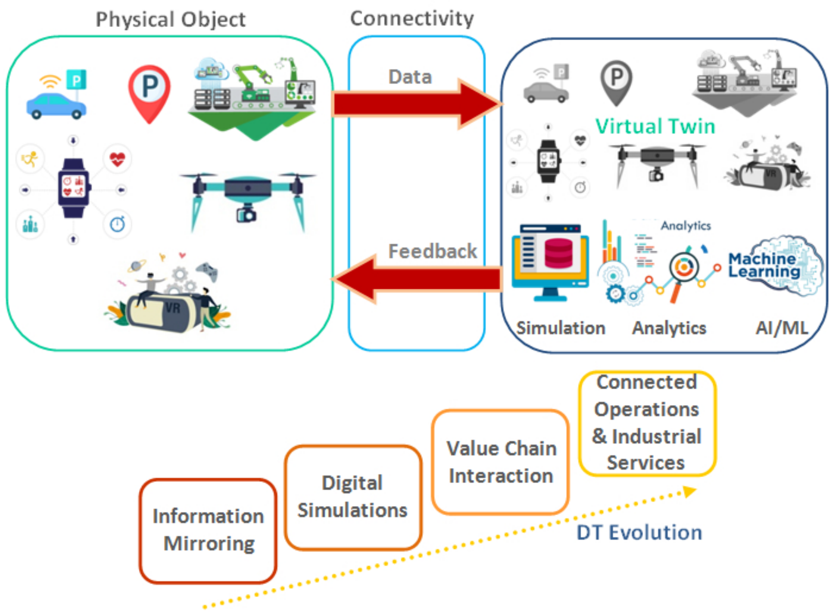

Fig. 14: The evolution of Digital Twin.

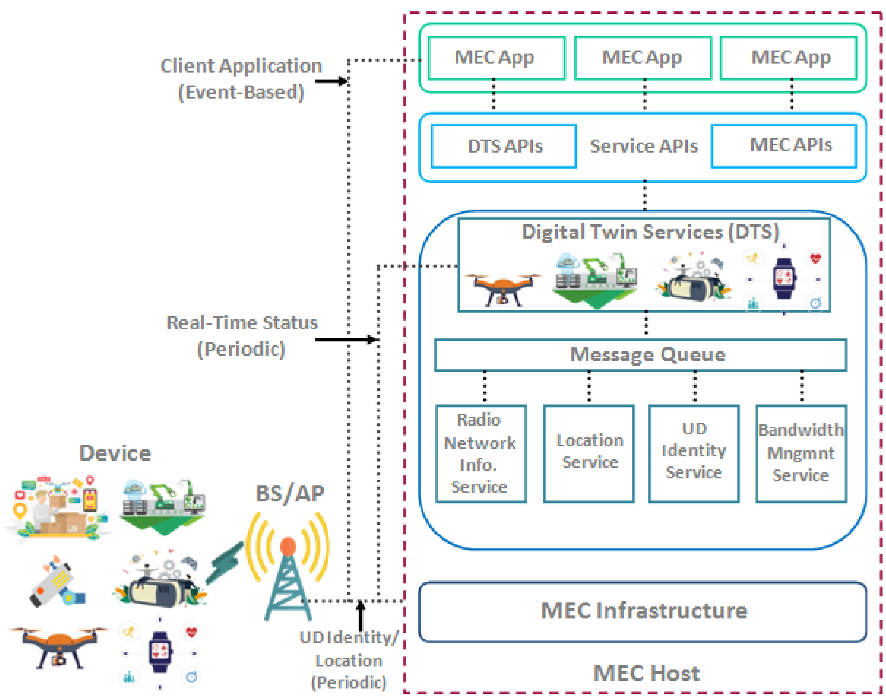

Fig. 15: The structure of a Digital Twin service-based MEC platform.

Communications are essential for interconnectivity and have a direct influence on system performance, particularly throughput, transmission delay, security, and so on. A network's connectivity resources are typically limited or constrained. Attempting different decisions in a real-time network is quite difficult. Admittedly, one can execute various communication activities in a virtualized edge network using a Digital Twin-enabled MEC network, and then acquire the ideal operation characteristics to report the actual network to achieve optimal system performance, including transmission rate, bandwidth utilization, security, and so on. Numerous studies are concentrating on employing Digital Twin to enhance the network system performance. In [405], the Digital Twin-enabled MEC network is used to determine the best transmission resource allocation to reduce traffic congestion.

MEC may be utilized to process some computing activities and ease the strain on network computational resources. However, networks' computational resources are constrained; therefore, it is still challenging to handle intensive computing tasks to serve upcoming programs including Metaverse, Augmented Reality (AR), Virtual Reality (VR), XR, etc. Sophisticated edge computing has recently evolved as a result of combining MEC with AI, whereby multiple AI models are built using various ML approaches, including DL, RL, and Transfer Learning, which demand a large amount of computational resources to train as well as update the model. Digital Twin-enabled MEC network can be used to boost computing performance [406]. By building Digital Twin-enabled MEC networks for such a cloud infrastructure, the physical component and AI algorithms are integrated with the virtual realm to conduct task computations and model training or construction, and indeed the results are subsequently given back to the respective physical components. To that aim, the Digital Twin-enabled MEC network enables resource-constrained user devices and servers to process intense computational workloads and AI model construction or training [407]. [408] suggested a novel Blockchain-based Digital Twin-enabled 6G edge networking infrastructure recovery system.

7.8. Open-Source MEC for 6G

The primitive MEC design is based on specialized hardware, and its unique software functions are tightly interwoven with the hardware, making it too stiff to accommodate fast-developing situations accelerated by 6G. As a solution, a dynamic mechanism described by open-source software operating on general-purpose technology platforms combines open-source mobile networking with MEC.

7.8.1. The Fundamentals of an Open-Source Network

Open-source network [409] architecture is comprised of four key components: the cloud entity that includes the core network (CN); the edge context that includes decentralized MEC hosting; the diversified terminal aspect; and the network context that includes a RAN attaching the edge as well as terminal realms (users) and a transport interface joining the cloud as well as the edge realms [410].

The open-source core network framework is widely described in the cloud sector. SBA, for example, has been defined as a fundamental component of the 5G core network infrastructure in the third-generation partnerships Project (3GPP) specifications, demonstrating a substantial degree of versatility and adaptability [411]. SBA divides the initially connected network functions into numerous independent system components, each of which provides one or even more services that may be utilized by the other system components [412]. As a result, all functional blocks may communicate with one another to provide users with customized services, just like they were linked to a single service interface. Nevertheless, due to the increasing real-time complexity requirements, the OS RAN framework [413]-[415] has yet to be specified in the network realm. Several viable options, including RAN decoupling and reconfiguring, have been proposed to do this. To begin, traditional network’s tightly connected RAN parts, functions, and resources must be entirely separated. These might then be dynamically reconstructed to meet the needs of the user, resulting in personalized virtual RANs. Simply to be said, the OS idea enables the easy formation of 6G RANs using LEGO blocks [416]-[418].

RAN Decoupling: A strict closed operating system underpins the tightly connected 4G wireless networks. As a result, at least four distinct RAN decoupling strategies, notably hardware/software detaching or decoupling (HSD) [419], the user plane and control plane separating (UCPS) [420], [421], the central unit and decentralized unit partitioning or segregation (CDUS) [422], [423], and downlink and uplink detaching (DUD) [424], [425], have been proposed for coordinating a beneficial level of accessibility in 6G. There is no universal consensus on the ideal open-source RAN design since they all offer various advantages and disadvantages. It should be noted that HSD and UCPS provide the foundation of open-source wireless networks or cellular network systems, while CDUS, as well as DUD, extend the versatility and accessibility of wireless networks.

HSD decouples services and resources from physical infrastructure. Because of the competent variety of NFV technological advances, network resources may be generalized and redistributed among multiple users, and distinct services can be provided by the same architecture, thereby decoupling functionality from the underlying architecture.

UCPS is inspired by SDN, which isolates control signals from data transport. The user plane and control plane are formed by installing database stations within higher frequency bands and controlling stations within the most favorable lower frequency spectrum, accordingly.

From the standpoint of the open-source protocol layer, CDUS constitutes one of the fundamental technologies utilized in the next-generation or evolving cloud RAN [426], [427] that focuses on splitting the typical evolved node base station (eNB) into the wirelessly distributed unit and the central unit [428].

Tightly connected downlink and uplink transmissions limit a user's connectivity versatility. A dynamic user association with high energy efficiency may be accomplished by using DUD through the dual connection, in which a user attaches to a small base station and a macro base station for its uplink and downlink transmission, respectively.

RAN Reconfiguration: Traditional RANs have indeed been softwarized and separated into distinct virtual network functions utilizing RAN decoupling technology. Consequently, to serve a variety of applications, just the appropriate detached network functions will be selected and combined to build RANs on demand. Currently, at least two proposed ways are in practice for the efficient reconfiguration of 6G RAN, notably MANO and RAN slicing or splitting [428]-[430]. RAN slicing [431]-[433] enables the dynamic allocation of virtualized network functions and radio capacities in RAN to multiple services. RAN slicing explicitly picks the appropriate network functions by using allocated resources and afterward wraps them to construct a tailored virtual network whenever a specified service request arises.

MANO is another successful method for establishing RAN reconfiguration, which is more adaptable to varied network perspectives than RAN splitting or segmentation. The management section is in charge of comprehensive RAN monitoring [434]-[436], such as life cycle management [434], defect detection [435], auditing [436], and security management [437], [438]. The orchestrating component [439] assists the network functions and leverages the underlying resources to reassemble the RAN, and it consists primarily of two sub-components: selecting the proper network functions and properly scheduling those for a particular service.

RAN Capability Enhancement: MEC enables local computation and storage resources that may be connected well with open or accessible RAN to provide customers with low-latency applications while also decreasing the stress on the transmission network [440]-[442]. Even though the open-source RAN framework is yet to be fully specified, an open-source MEC system [443], [444] based on the aforementioned decoupling and reconfiguration techniques will be explained in this survey work. Additionally, to support its attractive applications, varied networking architecture, and various resources, 6G will become increasingly complicated. As a result, traditional network management approaches involved with human-controlled ideologies will become insufficient, necessitating the use of advanced artificial intelligence (AI)-based solutions [445] inside the RAN for achieving self-organizing, autonomous operation, and capital expenditure or operational expenditure savings [446]-[448].

7.8.2. Open-Source MEC

In this part, the work mentioned the use of decoupling and reconfiguring to incorporate the essential notions of open-source networks into MEC and presented the open-source MEC concept to improve the accessibility and flexibility of upcoming MEC systems [449]. Specifically, open-source MEC splits the closely connected service functions into numerous separate NFs and supports them flexibly via a simpler service-based interface (SBI) by establishing a service-based MEC layer. After that, network functions' MANO is designated for customizing MEC by presenting the handy template and instance idea, in which the open-source templates for MECs are specified and then instantiated as needed.

Open-Source MEC Framework: The applications layer and MANO layer comprise the complete structure, in which the former (applications layer) is primarily accountable for data handling and delivery, involving the infrastructure tier, virtualization tier, service-based MEC tier, and applications or services tier from down to up. On the other hand, the latter (MANO layer) is made up of MANO and Virtualized Infrastructure Manager, and that accomplishes the open-source MEC platform's coordinating and resource administration. The neighboring layers are connected via standard interfaces and collaborate to provide MEC services sought by users [450], [451]. Fig. 16 depicts the open-source MEC framework.

The infrastructure tier is the lowest, encompassing the whole systems computational, caching, and connectivity facilities. The processing unit in particular provides high-performance computational capacity for such service-based MEC tier, which is located directly beneath the applications or services tier. The major elements of the caching services at the infrastructure tier are storage devices, i.e., the solid-state drive/hard drive. This layer's connectivity resources comprise bandwidth along with access points and next-gen base stations (gNBs) [452].

In the virtualization tier the underpinning three-dimensional facilities may be detached from the specialized hardware and aggregated into a pool of resources, relying on the NFV principle, and shared by many network functions at the service-oriented MEC tier. Next, as shown in the virtualization tier, open-source MEC builds many Virtual Machines or Dockers that function on the inherent resource pool and may concurrently support various network functions for offering customized services [451]. The main aspect of open-source-MEC is the service-oriented MEC layer [453], which contains a uniform SBI and varied network functions, with the SBI connecting different network functions jointly based on the uniform stateless hypertext transmission protocol (HTTP) to ensure that they may interact directly with one another if needed. The work also presented the detached centralized service functionalities into distinct network functions. The user plane function (UPF) of the service-oriented MEC tier is specifically taken from the 5G core network for open-source MEC to offer open-source MEC-5G new radio (NR) features [454]-[456]. After that, to improve open-source MEC, the work grabbed numerous more network functions from the 5G core network control plane and constructed several new network functions. These network functions are accessible to one another and may be merged at any time, allowing all users to activate and deactivate them quickly in recognition of specific customized services.

Indeed, the subscriber does not need to rely on open-source-specifics. Instead, customers will access customized services through numerous applications at the application tier. For the sake of convenience, only two applications are studied in this article, which are relative to the caching and computation queries, i.e., the application tier's high throughput and intense computational situations. Furthermore, the MANO layer or tier is in charge of controlling these network functions alongside applications, as well as ordering the Virtualized Infrastructure Manager to assign resources. As previously stated, MANO is responsible for MEC reconfiguring, in which open-source MEC templates and implementations are suggested for executing flexible reconfiguration as needed. The MANO plane's Virtualized Infrastructure Manager maintains virtualized resources following the directions of MANO and ensures that suitable computing, caching, and networking resources are available for the top levels.

MEC Decoupling: To separate MEC functionalities, research works envisioned the open-source MEC platform's service-based MEC tier, which developed from the classic MEC tier, which is mostly built of SBI as well as service-oriented network functions. Studies extracted and depicted a service-based MEC tier's precise structure.

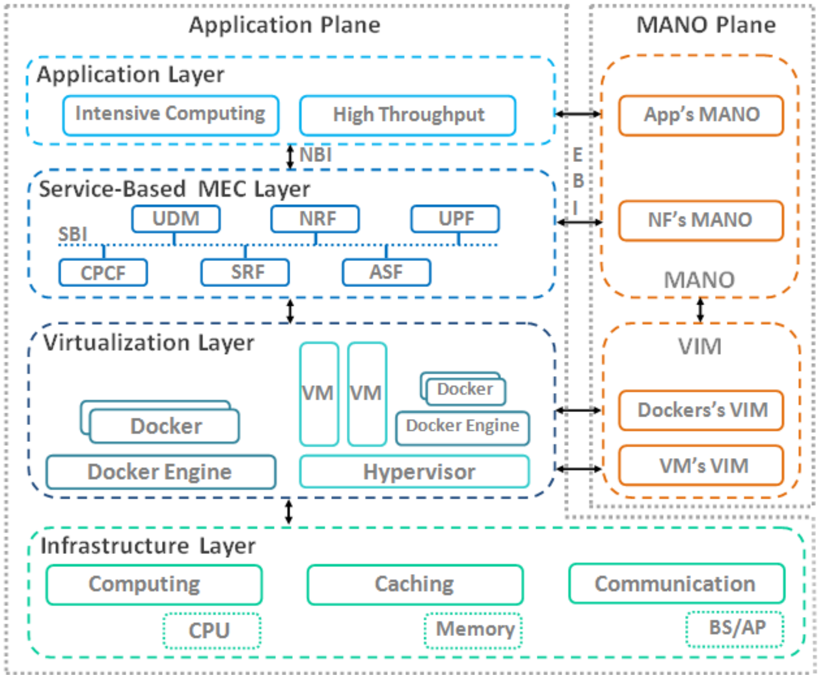

Fig. 16: Open-source MEC framework.

The SBI links all of the NFs to facilitate interface design and deployment. The north-bound functionality interface is indeed an application programs interface (API) that allows the application tier to communicate well with the service-based MEC Tier to receive services. The east-bound functionality interface is an API that allows the network functions' MANO to communicate well with service-based MEC Tier, which is primarily used to control and organize network function resource management and life phase. The work [457] presented an integrated Representational State Transfer-ful (RESTful) API for such SBI/south-bound functionality interface, north-bound functionality interface, and east-bound functionality interface based on the identical HTTP, which itself is lightweight and readily read by both humans and computers. Hence, the service-based MEC tier enables direct connections between network functions, MANOs and network functions, and network functions and applications, minimizing interface complexity and protocol inconsistencies in the conventional MEC design [458].

MEC Reconfiguration: While MEC administration is not directly tied to open-source MEC realignment, the ETSI-proposed combined monitoring of MEC and NFV may still be employed in open-source MEC; however, the idea of service-based MEC tiers is certain to offer issues to the orchestration approach. As a result, the study briefed open-source MEC templates [451], as well as the implementations of network functions, through Kubernetes, which enables the flexible ordering of network functions and any future MEC reconfiguration [451]. Further, specifically, certain templates, such as a computation-heavy template, are pre-prescribed for related specific applications. Nevertheless, if no user requests such a specific service or application, the framework will not allocate the necessary resources for the template, therefore the template is void. If a subscriber requests (such a service or application), the framework will activate it by allocating computational, caching, and networking facilities as an instantiation [459].

7.9. Quantum Computing-Inspired MEC

In contrast to traditional MEC employing classical information technology [460], the intrinsic qubit noise in adaptable quantum computers will degrade qubit integrity as the number of qubits, gates, and tests rises [461]. Configurable quantum computers may run quantum processors with sophisticated cryogenic equipment and fault-tolerant techniques to enable fault-tolerant quantum computation [462]. Quantum computers operate at exceedingly low temperatures to reduce the entropy of quantum components. Quantum distortion, on the opposite side, is combated by the employment of fault-tolerant systems, such as those that utilize surface codes, concatenated codes, and bosonic qubits [463]. In error codes, for example, information is dispersed among many physical qubits that comprise a logical qubit. Ultimately, even fault-tolerant quantum computation at cryogenic temperatures may provide enormous increases in processing and energy efficiencies of configurable quantum computers.

As scalable quantum computing achieves the needed capacity and quality, Multi-Access Edge-Quantum Computing (MEQC), in conjunction with the remote access provided by numerous edge servers, will strive to push the bounds of quantum advantage [464]. Users throughout the world may have access to and profit from cloud/edge quantum technology vendors, including Amazon Braket, IBM Quantum, and Azure Quantum by offloading computing activities to quantum systems in edge servers. This increases the possibility of identifying novel usage for quantum computation and addressing current challenges, hence accelerating the practical deployment of quantum processing. MEQC, by dramatically boosting the attraction of quantum computation to mobile consumers, can present users with a variety of potentially dangerous applications, including quantum ray tracing [465]. MEQC differs significantly from standard edge cloud computation in terms of processing power and energy usage. To begin, quantum computing employs quanta accumulation, distortion, and entanglement to speed computational processes in novel ways. Secondly, quantum computers typically perform at extremely low temperatures. As contrasted with traditional computers, the majority of quantum computers' power consumption is utilized to sustain the ultra-low temperature enclosure. Finally, to ensure the dependability of computing outcomes, quantum computers identify suitable error-correcting codes and the level of error correction convolution based on respective energy and latency restrictions. As a result, empowering devices (i.e., edge user devices) to effectively offload workloads to quantum edge computing nodes or servers remains a difficult topic.

Xu et al. [466] proposed a unique mobile edge quantum computation concept that extends quantum computing capabilities to mobile edge infrastructures that are closer to mobile consumers (i.e., edge devices). Passian et al. [467] proposed a quantum-edge simulator in their research work to simulate sensing and quantum-edge computing. Li et al. [468] proposed a quantum ant colony-approach-based mobility-aware service deployment in the context of SDN-empowered MEC. Masdari et al. [469] proposed a quantum-based arithmetic optimizing algorithm for energy-efficient computation offloading in MEC.

7.10. Passive Optical Network (PON)-Assisted MEC

Current MEC, 5G as well as beyond 5G research have emphasized the advantages of employing optical fiber networking to handle the growing number of connected devices and associated QoS-aware services. Optical fiber has a large capacity and minimal propagation latency. The cost-effective and extended-capacity passive optical network (PON) has emerged as a natural alternative for backhauling and fronthauling of 5G and beyond networking infrastructure, using the advantage of optical fiber which has already been installed in the majority of metropolitan or residential areas as well as commercial premises [470]. The PON's design, hardware, efficiency, capacity, and underlying standards and algorithms have all developed over time [471]. These advancements, together with optical fiber implementations that have already reached residential and commercial premises, have facilitated the transmission of latency-sensitive as well as bandwidth-hungry applications to a significant number of consumers.

Such services characterize 5G and 6G features since they demand millisecond-level latencies, ultra-reliable networking capabilities, and a considerable quantity of computation. The fusion of MEC and PON systems is a promising option for delivering latency-sensitive but task-intensive services to meet such demanding QoS requirements [472].

Wang et al. [473] examined the latency-aware network designing of a Wavelength Division Multiplexing (WDM)-PON-based MEC-enabled fiber optic wireless access network under architectural and management restrictions. Das et al. [474] proposed a hybrid analytical-iterative approach for estimating optimal virtual PON segment allocation in evolving MEC-based C-RAN, resulting in mesh access connectivity with ultra-low-level end-to-end delay. Wang et al. [475] proposed a joint optimization approach to minimize the deployment cost and latency for a Time Division Multiplexing (TDM)-PON network-based MEC-empowered C-RAN. Das et al. [476] proposed a unique PON-based mobile fronthaul transport infrastructure focused on PON virtualization which permits EAST-WEST connectivity in addition to standard NORTH-SOUTH connectivity. Hu et al. [477] proposed an application-aware MAC scheduling approach for MEC-enabled TDM-PON fronthaul.

8. MEC Deployment Cases

The survey has categorized the deployment cases into two separate categories: (i) system-aware deployment cases and (ii) user-oriented deployment cases. System-aware deployment cases are indicating the system-aware/specific/sophisticated deployment and orchestration cases that are offered by the MEC service provider to a certain host or platform which provides specific service to the users and such services are video streaming, gaming services, edge intelligence-aware image/fingerprint processing for recognition, etc. In this circumstance, users will get a service through a platform or host and the platform or host will be the orchestrator of the MEC service or facilities. User or user devices here in this context are only service consumers. User-oriented deployment cases are indicating the end-user level services such as IoT services and other related ones. These types of MEC services will be readily available directly to the end-users. In this circumstance, users can demand the vendor or have some capabilities to orchestrate certain of the MEC facilities or services as per their needs or requirements, i.e., different IoT services have different requirements (enabled by the vendors under the supervision of regulatory entities if required).

8.1. System-Aware Deployment Cases

8.1.1. Applications Hosting

An Application Service Provider (ASP) can deploy services at a MEC node to give a quick response. Such services may be useful in emergencies such as healthcare services, disaster tackling, and so forth. It can be beneficial for local services needed by the regional communities inside the MEC host's region since it reduces network bandwidth and operating expenses. Yang et al. [478] presented an enhanced video streaming service hosted by a MEC server. The most popular programs on PCs, tablets, and cell phones are games.

The devices on which they are featured are linked through LAN and/or cellular connectivity. Because games demand low latency, which typical cloud services cannot provide, they may be served on a MEC server near users [479]. While the game or program is running, the user may travel outside the base station's coverage area, making it difficult to remain connected to the MEC server.

8.1.2. D2D Communications

MEC is required to minimize latency in real-time vehicle-to-vehicle (V2V) [480], machine-to-machine (M2M) [481], [482], or device-to-device (D2D) supervising. Due to significant latency, M2M, D2D, and V2V communications are not viable over the cloud. D2D transmissions have a wide range of applications, including media downloading, peer-to-peer (P2P) file transfer [483], online interactive gaming, streaming services, mobile social networking (MSN), and so on. A D2D link allows users in close proximity to interact with one another. Individuals who participate in MSNs share a shared interest. As opposed to the client-server model, they can get material from one another. Rivera et al. [484] proposed a blockchain-enabled peer-to-peer secure task sharing through the assistance of a MEC server. MEC hosts can be useful in enabling real-time communication for automobiles via D2D communication, therefore avoiding the incidence of an undesirable road collision by the delivery of immediate warning messages [485].

8.1.3. Edge Intelligence

Pervasive computing incorporates computation and networking capabilities into ordinary things, resulting in massive amounts of heterogeneous content. MEC server may do data analytics to limit the amount of data delivered to the cloud platform. A traffic tracking app, for example, only transmits the data of aggregate speed as opposed to the particular speed. A further example is a “kid missing crowd program,” in which only images with a kid in the frame are sent to the data center. This use case presents an application operating on a MEC server near the radio network which gets a huge volume of data from sensors and devices linked towards the MEC host's wireless node(s). The program then evaluates the data and extracts vital information such as kid photos for the “kid missing crowd apps” [486] and aggregated speed for the “traffic monitoring platform,” [487] which it then transmits to a centralized cloud service. Bellavista et al. [488] presented a MEC framework for mobile crowd monitoring, with data analytics conducted on the MEC server. To preserve backhaul bandwidth, data undergoes filtering at the MEC server before being sent to the cloud server in this scenario.

8.2. User-Oriented Deployment Cases

8.2.1. Smart Cities

Smart cities are a complicated Internet of Things (IoT) paradigm that intends to manage public affairs by implementing Information and Communication Technology (ICT) viable alternatives. Smart cities may employ public resources more efficiently, which improves the degree of services offered to customers while lowering operating costs for public administration. For example, one realistic smart city project, Padova smart city, has been accomplished in the Italian city of Padova, which may pick open data with ICT technologies for public administration as soon as possible to make the optimal utilization of public resources [489]. Neom smart city is another example of a smart city that is planned to be developed in Saudi Arabia [490].

As a sophisticated cyber-physical system (CPS) implementation, smart cities may include various sub-applications or features such as smart grid, smart traffic, smart buildings, waste treatment, environmental sensing, smart health, intelligent lighting, and so on. The aforementioned sub-applications or facilities should be endorsed by a unified connectivity/communications infrastructure or communications systems developed for such sub-applications or facilities should be integrated to form a large-scale interrelated network model for CPS application areas, to make the best utilization of public resources in city areas. The deployment of MEC will improve the utility or features of a smart city to make it more suitable for living [491]-[493].

8.2.2. Smart Agriculture

Smart agriculture or precision farming utilizes the most modern and advanced ICT technology to increase agricultural profitability and environmental sustainability. Smart farming focuses on operating actuators (motors, pumping, illumination regulators, and so forth) according to sensor data (humidity, temperature, brightness, etc.). Furthermore, UAV-aided computation is a sort of application-oriented edge computing that is now popular in agricultural advancement [494]. The UAVs, which are equipped with cameras and computation capacity, are dispersed in the formation of a swarm and hover over enormous agri-fields to monitor grain or drop conditions. Besides crop yield, MEC may be used to study farm animal behavioral patterns, which is important for animal health and well-being.

Nevertheless, one of the issues that agricultural lands experience is geographic isolation as well as a lack of robust and consistent data network connectivity. To resolve this problem, private edge computing as well as communication architecture, provides a significant alternative for enriching agricultural regions. Another reason to use edge computation (MEC) is to preserve the main network from overload as sending all video recordings and sensor data from several farm fields to the centralized server will create significant latency in the network [495], [496].

8.2.3. Smart Vehicular Network or Transportation

The deployment of MEC improves the safety and intelligence of modern smart city roadways and transit systems. Smart roads help to disseminate awareness amongst road elements by utilizing an advanced traffic control system, in which cars assisted by the MEC services may interact with each other to preserve road traffic safeness and balance. It is also feasible to address particular road scenarios more effectively by using vehicle-to-thing interaction, such as in the event of a collision or the case of the movement of emergency automobiles (police car, ambulance), when cars are directed proactively to clear up specific road lines [497].

Traffic collision detection [498] constitutes one of the services that will be housed in the MEC server dependent on data acquired from the driving environment; underneath MEC server may instruct and adjust real-time vehicular speed and trajectory, in addition to lighting controls to minimize collision incidents. MEC is also used to augment road cameras with features, including vehicle tracking and recognition [499]. The road surface condition seems to be another concern in road safety; the project [500] envisioned deploying a congested surface sensor module having the capability of vehicle supervision, wherein data is gathered and processed utilizing edge computing nodes.

8.2.4. Smart Grid

A smart grid framework is an electrical system that includes energy efficiency-assuring resources, renewable energy resources, and smart appliances. Intelligent meters located across the network are employed to receive and send energy usage estimation. The intelligent meter's data is overseen through supervisory control and data acquisition (SCADA) technologies that regulate and stabilize the electricity grid. Furthermore, SCADA systems may be supported by dispersed intelligent meters and miniature grids that are interconnected with MEC. For example, MEC can balance as well as scale, the load based on information supplied by certain microgrids and intelligent meters [501]-[503].

8.2.5. Smart Industries

MEC has been completely linked with the most prevalent industry 4.0 standards; this integration is often referred to as industrial edge computation. Proactive maintenance is a strategy used by emerging industries to decrease capital expenditure and operational expenditure. The machine is fitted with numerous IIoT (industrial IoT) sensors, such as heating, vibrations, and pressure sensors that collect data and send it to edge computing nodes and the data will be analyzed for forecasting machine faults and mistakes [504].

Furthermore, the fourth industrial revolution wants to include AI in its production processes. Since industrial enterprises cannot send private information to a public cloud (for example, recordings from production areas), companies have to depend on edge computing [505]. Several instances are available at present stating how industrial revolution 4.0 is employing edge intelligence for object identification with machines, autonomously guided vehicles (AGV), and human position estimation.

Apart from the aforementioned sectors, E-commerce businesses are in serious need of real-time connection with their consumers, as delivering promptly with MEC represents one of the finest browsing perceptions they can give to their clients. Similarly, by improving their recording devices with computer vision features, MEC may assist protect in-store payment terminals [506].

8.2.6. E-Healthcare

Several scholars are interested in technological advancements in the health sector. Healthcare, like other sectors, can benefit from MEC [507]; for example, patients afflicted with strokes may fall. As per stroke stats, someone in the United States gets a stroke every 40 seconds [508]. Falls are prevalent in stroke victims, who typically have hypoglycemia, hypertension, muscular weakness, and other symptoms. According to current studies, one-third of strokes might be avoided by preventing falls as soon as possible [509]. A substantial amount of study has been conducted in an attempt to detect and avoid falls, for instance, by integrating human-computer interface devices like smartphones, smartwatches, and Google Glass, however some limits persist.

Recently, researchers introduced a DL-based fall detection mechanism utilizing MEC technologies [510], [511]. U-fall is built on a fall detection system that employs acceleration magnitude measurements and non-linear time-series analysis. U-fall detects motion using smart device sensors including gyroscopes and motion sensors. To provide real-time identification, U-fall smartly maintains the integrity between both the smartphone as well as the MEC server. Furthermore, the suggested infrastructure is capable of producing correct findings, making it more trustworthy and dependable [512]-[514].

8.2.7. Smart Banking

Blockchain, invented in 2008 is an electronic trading system that is independent of any third-party operator (banks, government, etc.). Transaction verification in Blockchain is performed by miners, who focus on solving a theoretically and computationally difficult challenge known as the verification of work. One of the main role players behind intelligent banking is Blockchain technology. In IoT devices, Blockchain typically cannot be directly implemented due to the computation-intensive nature of mining tasks. As a result, outsourcing mining jobs to the MEC server is a viable option. Furthermore, a notable Blockchain issue is pricing cooperative miners, since there is a requirement to boost MEC service providers’ revenue while simultaneously safeguarding miners' investment benefits from transferring to the MEC server [515], [516].

8.2.8. Infotainment

Internet Protocol Television (IPTV) [517], [518] over Wireless to the Everything/x (WTTx) delivers wireless broadband services via wireless broadband communication systems (e.g., cellular networks) [519], [520]. At the moment, network connectivity and television (TV) infrastructure are distinct. IPTVoWTTx enables operators and over-the-top (OTT) broadcasters to replace TV infrastructure while saving money on infrastructure expenditure. IPTV through WTTx will enable OTT providers to deliver content swiftly by utilizing the existing mobile networks. IPTV has a three-tier-based design. The IPTV's centralized cloud server or data center acts as a repository for Video on Demand material, which is the first tier. The second tier is just the IPTV edge server, which offers users with Electronic Program Schedule as well as Video on Demand features. Consumers are represented by the third layer. The IPTV central hub is often implemented on a regional basis, such as in a big city or significant metropolitan area. To deliver the finest user experience, IPTV edge servers are installed closer to users [521]. However, high mobility creates issues in dealing with the frequent switchover of operations and services to offer end customers uninterrupted service.

8.2.9. Video Analytics

In the past, security cameras are employed to send data to a centralized server. Because of the increasing prevalence of security cameras, the conventional client-server design may be unable to transmit footage from millions of devices, putting a strain on the network. In this instance, MEC will be advantageous by including cognition at the device directly, which is configured to transfer information through the network whenever motion is detected. Moreover, MEC-enabled video surveillance might be useful for a variety of systems, such as traffic control applications that can identify road congestion or an accident based on traffic patterns. The program can also aid facial recognition; for instance, if an individual commits an offense, his image (captured by the sophisticated cameras) may be sent to the edge computing server to help track down the perpetrator [478], [522]-[528].

8.2.10. Immersive Audiovisual Streaming (AR/VR)

A live either indirect or direct representation of a tangible, real-world situation whose attributes are augmented (or replaced) by computer-generated sensory stimuli such as music, video, animations, or Global Positioning System (GPS) data is referred to as augmented reality (AR). AR apps can deliver extra information in real-time after processing such data. AR applications are extremely localized and need both low latency and extensive data computation. The exhibition video guide is a portable electronic device that gives thorough information on certain artifacts that cannot be readily exhibited. AR plays a crucial role in online gaming, like Pokémon Go, Ingress, Minecraft Earth, Jurassic World Alive, Angry Birds AR: Isle of Pigs, The Walking Dead: Our World, etc. By precisely evaluating the raw data, MEC enables AR service ought to have the capacity to differentiate the desired contents and subsequently transfer AR data to its intended subscriber. MEC-enabled AR devices have recently received a lot of interest [529].

AR platforms such as Junaio, Layar, Wikitude, and Google Goggles have recently incorporated mobile technology [530]. AR provides a real-world user experience by merging actual and virtual items that exist concurrently. Modern AR services, such as news, TV shows, sports, object detection, games, and so forth, have become adaptable in their audio as well as visual components. Metaverse is a prominent instance of such advancement of AR [531]. Yet, AR systems typically require high computational power for task or workload offloading, low latency for improved QoE, and high throughput to support indefinite IT services.

MEC platforms have been identified as a potential for latency-sensitive AR technologies [532]. They enhance AR systems, for instance, by increasing throughput by moving cognition to the network's edge rather than depending on the main network. Transferring computation-intensive activities to the closest cloudlet is thus more optimal and efficient, improving user experience.

Brain-computer interface is one instance of AR functionality that works by recognizing human brain signals [533]-[535].

The work [536] reviewed the escalation of mobile augmented reality (MAR), i.e. Web AR with the advancement of networking and computing technologies such as 5G and beyond networks and MEC.

9. Security Aspects of MEC

9.1. Edge Networking-Level Threats

The edge network provides computing power, data storage, and administration services [537]. It facilitates application and service delivery by sharing infrastructures, platforms, and supervisory planes [538]. Nevertheless, some components, such as isolation [539], [540] may not provide an equivalent to cloud security needs. In a MEC integrated edge network context, applications or functions may not be created utilizing trusted computing techniques, which raises risk [541].

Privacy Leak: Unapproved accessibility to MEC nodes may jeopardize data confidentiality [542]. The MEC concept restricts the breadth of privacy breaches by splitting data and limiting access [543]. Edge network infrastructures, on the other hand, may exfiltrate confidential material and rich network contextual information, including client status details, traffic data, and local network circumstances, which are used by different services to provide context-aware management [544]. The work [545] presented a deep deterministic privacy-preserving mechanism.

Privilege Escalation: When a malicious party takes advantage of a design flaw, bug, or configuration issue in an application or operating system, he or she gains elevated privileges on restricted elements that would normally be limited to that individual [546]. The malicious attacker can then utilize the newly obtained unauthorized rights to steal sensitive data, conduct administrative operations, or distribute malware, thereby causing catastrophic damage to server operations [547]. The works [548]-[550] proposed prevention mechanisms against this type of attack.

Service Manipulation: Service manipulation assaults, unlike cyber-criminals who aim to steal information or grab it as hostage through ransomware, can be difficult to detect. Hackers can make erroneous alterations to data, which might have disastrous consequences [551]. A device in a cluster placed around an edge network that participates in service delivery can operate as a decentralized computing system, and if the device is hacked, the entire group can be affected [552]. An internal aggressor with proper rights can not only alter information exchange, but also launch rogue services that really can send misleading management information including historical data to third parties [553], [554]. The references [555] and [556] presented prevention mechanisms against this kind of attack.

Rogue Data Center: The edge network seems to be more difficult to maintain and protect than traditional cloud computing settings [557]. In this threat scenario, an attacker might take control of a whole edge network by installing malicious equipment pretending as an edge networking unit (i.e., access point, routers, switches, network cards) that lies between a cloud server situated in the core infrastructure and user devices to affect connections with external devices [558]. Several works have proposed multiple prevention mechanisms against this sort of attack [559]-[561].

Physical Damage: Cyber-physical security combines numerous technological disciplines, such as physical, computer, and connectivity resources on various spatial scales, all of which are regulated by computational models [562]. Systems are frequently linked to an IP network. Throughout the event of an invasion, the entire ecology might be disturbed or brought to a standstill by physical disruption [563]. Monitoring the computational capabilities for unexpected usage or load [564] becomes a possible security check to protect the internal structures of the MEC servers against this attack. Several prevention mechanisms are presented in these works [565]-[567].

Resource Misuse: Malicious actors may attack consumers, companies, or other service vendors using MEC resources [568]. For instance, the malicious attackers can be massive-scale mechanized click fraud, for "mining" electronic currencies, or brute-force computer threats on credential databases [569]. A third type of attack is resource usage, for example, a rogue VM might scan the regional network for susceptible IoT devices as well as host botnet nodes [570]. The works [571]-[573] proposed several prevention schemes against this cyber attack.

VM Manipulation: The host layer or tier or level is a significant functional aspect in MEC. It contains the MEC Platform Manager, Virtualized Infrastructure Manager, and MEC hosts that deploy resources and deliver functions to MEC users utilizing virtualization approaches including VNF and VM. Nevertheless, when deployed in MEC infrastructure, virtualization methods create various security concerns such as VM tampering, VM escaping, Domain Name System (DNS) escalation, VNF placement shift, security-log inspection, and surveillance [574], [575]. The attack vectors influence the host tier activities of orchestration elements [576]. Trusted Platform Manager (TPM) and Virtual Machine Introspection (VMI) are two approaches recommended for dealing with virtualization-related security issues [577].

Injection Attacks: Injection attacks remain one of the most common and dangerous web application threats [578], [579]. They can cause data loss, data breaches, data integrity failure, denial of service (DoS), and the compromise of a system or device. Injection attacks are a broad class of threat vectors that allow adversaries to inject malicious code into a system, which is then processed by a mediator as an element of a request or instructions, causing the affected program's execution pattern to be altered [580]-[582]. Prevention mechanisms against this attack are mentioned in the reference works [583]-[585].

9.2. Access Network-Level Security Threats

Access network safeguarding is essential for MEC platforms' efficiency which provides a framework for safe connectivity with user devices and cloud infrastructure [586], [587]. Failing to deploy adequate access network security rules exposes hostile parties to exploit important vectors, resulting in significant network risks [588]. Infrastructure for access networks includes network components and systems that support information flows across devices connected towards the access network infrastructure, MEC host, as well as core networks. An attacker may attempt to compromise the access network infrastructures, associated devices, or communication links [589]. Vulnerabilities to MEC services and applications include applications or services misuse [590] and the distributed denial of service (DDoS) attack attempts [591].

Denial of Service: Access networks are subject to DoS assaults, which might take the form of DDoS attacks [592] or radio jamming [593]. The persistence of Virtual Machines distributed across numerous MEC hosts raises the possibility of exploited Virtual Machines coordination in a substantial assault, such as DDoS [594]. Whenever a service or application is hacked, the infected service or application uses MEC resources, i.e., network bandwidth, processing power, or memory. The attack causes a delay in an applications' or services' response or destroys the MEC node's operation, resulting in service interruption. Security orchestrating, automating, and response (SOAR) mechanisms are available in the security sector to give an autonomous and preemptive security strategy to this sort of serious threat [595]. Sophisticated DoS/DDoS prevention architectonics are described in the reference works [596]-[601].

Man-in-the-Middle: The MitM attack is typically distinguished by the existence of a malevolent third party across two or more interacting parties, surreptitiously relaying or intercepting their conversation [602]. A MitM attack is classified as an infrastructure assault in the MEC scenario, in which the malicious attacker attempts to seize a specific network section and proceeds to perform attacks, including phishing and eavesdropping, on linked devices [603]. Since MEC services and applications rely heavily on virtualization, conducting a MitM attack attempt on many Virtual Machines may have an impact on both parties or sides or victims of the assault [604]. Reference [605]-[607] works proposed MitM prevention mechanisms.

Rogue Gateway: The decentralized MEC architecture enables an environment in which hostile attackers might design and install illegal gateways to undertake unauthorized actions. Unauthorized gateways can constitute a substantial hazard by enabling backdoor access to critical resources if they have access to networking equipment, programs, and edge services. Solution mechanisms against this issue are described in these works [608], [609].

Inconsistent Execution of Security Policies: The synchronization and uniform compliance of security functionalities during the time of mobile devices' switch from one operator to another poses a difficulty for the providers of mobile networks. This activity demonstrates the necessity for telecom operators to share security policies on an adaptive scale to ensure that subscriber traffic across networking devices is safely managed, especially when devices' connection shifts from the MEC of one operator to the MEC of another operator [610].

Communication Channels: The radio channels of a wireless communication network are formed through a wireless transmission medium, which constitutes the most vulnerable connection in a communication network. Man-in-the-middle attack, eavesdropping, Sybil, replay attack, smurfing attack, spoofing, and DoS are all mobile telecommunications threat vectors [611]. There is a danger of unauthorized intrusion to offloaded information during the offloading procedure [612], [613]. Risk considerations emphasize interoperability and compatibility issues with the user devices' connectivity to the base station. Advanced researches are ongoing to offer a secure communication channel for MEC services [614]-[620].

As a threat prevention or security assuring mechanism for access network safeguarding and establishing secure access from anywhere Secure Access Service Edge (SASE) emerged as a notable security solution. SASE represents a cloud architectural concept that integrates network with security as a service capability into a single cloud-based service [621]. SASE, in theory, expands safety and networking features beyond what is generally provided. This enables individuals to make use of secure web gateway, zero-trust network access, firewall as a service, and a slew of threat detection services. SASE is made up of two components: Security Service on the Edge as well as SD-WAN.

When correctly deployed, a SASE strategy enables enterprises to ask for secure access regardless of the location of their users, tasks, devices, or applications. This constitutes a major benefit in ensuring the security of distant workers. SaaS applications are fast gaining traction, and data is rapidly moving between data centers, regional offices, multi- and hybrid-cloud, and edge-cloud settings. SASE offers secure surfing, business application accessibility, and SaaS application accessibility from anywhere.

9.3. Core Infrastructure-Level Security Threats

Access and edge network activities for MEC are supported and managed by core infrastructure [622]. The trustworthiness of the core architecture can have a knock-on effect on other systems, such as the cloud. Under this setting, it is vital to examine the credible threats against the fundamental or core infrastructure [623], [624].

Privacy Leak: Accessibility to core infrastructure raises the chance of attackers obtaining information held on edge infrastructure, raising worries about privacy leaks. In the case of edge network breaches the potential impact of a privacy violation is confined to the type of content the adversary has achieved access to [625]. "Privacy by design" represents a unique MEC security technique. The principles comprise privacy functionality protection built into the design, preemptive action instead of a reactive response to privacy breaches, and data confidentiality throughout the lifespan [626]. References [627], [628] mentioned several prevention mechanisms against this sort of attack on core infrastructure.

ICT Intrusions: An ICT intrusion is defined by the attacker intending to breach into a system or device to purposefully modify data and manage the hardware it relies on [629], [630]. Data manipulation [631], background information [632], collusion [633], outside forging [634], eavesdropping [635], likability [636], Sybil [637], and identity attacks [638] are examples of such attacks. Security assurance mechanisms against these attacks are proposed in these works [639]-[644].

Software-Based Attacks (on Virtual Infrastructure): NFV security raises serious issues regarding its flexibility and the protection of the underlying telecommunications infrastructure [645]-[647]. It has the greatest influence on system resilience in addition to the entire quality of available services. The bulk of security risks target NFV infrastructure's fundamental architectural features, such as VNF modification, VNF location change, and information exfiltration as well as damage [648]. Fawcett et al. [649] offered an SDN-based conceptually centralized control solution that allows dynamism in networking security systems by collecting intelligence from networking devices via configurable APIs and using virtualization. In the network periphery, virtual security mechanisms can be used to detect possible threats, isolate vulnerable network devices, and prevent them from jeopardizing system security [650]. [651] proposed an advanced prevention mechanism against the attack on virtual infrastructure.

Rogue Infrastructure: This threat implies that attackers target specific components of the core infrastructures, and a successful assault might enable control of services and applications found in MEC servers. Even though the possibility of an adversary effectively launching this attempt is extremely low, effective security controls and procedures for critical MEC systems are still required. Security and privacy assurance mechanisms against this issue are proposed in these works [652], [653].

9.4. Edge Device-Level Security Threats

The sensitivity of user-controlled device material is considered while defining security and privacy needs [654]. Users sometimes become active contributors who develop data and engage in the sharing of information in addition to obtaining services. Unfortunately, there will be fraudulent users who will seek to disrupt functions and negatively impact the performance of edge devices [655].

Information Injection: An attacker can insert malicious data onto any hacked device to spread misleading information [656]. Poisoning [657] is a hostile operation in which attackers insert bogus information into an electronic system. Outside forging [658] happens when misleading messages containing fabricated information are created to jeopardize the confidentiality of victim modules. In the intelligent manufacturing arena, for example, an attacker injects erroneous pressure readings to delay valve activation to cause malfunctions [659]. Prevention mechanisms against these sorts of attacks are prescribed in these works [660]-[662].

Eavesdropping: Adversaries intercept communications across communication channels (through which the user devices are communicating), obtaining access to sensitive information [663].

Side-Channel Attacks: The goal is to obtain sensitive private information by gaining unauthorized access to user devices. Passcodes, login information, email, and geo-location information are the primary targets of this sort of cyber-attack [664]. An efficient intrusion detection system or intrusion prevention system with ML mechanisms could be a viable solution for detecting malware in a user device [665]-[669].

9.5. MEC Level Security Challenges

9.5.1. MEC System-Level

Global Defenses: The administration and orchestration of many security features is a difficult topic, and activating security methods separately on several entities does not always imply that the entire system is safe. It is necessary to strike a balance across local (decentralized) as well as global (centralized) defensive systems, as well as assuring accountability and flexibility. A central surveillance system should be put in place to provide insight into the MEC infrastructure, and all aspects ought to be verifiable. The end-to-end protection mechanism is required whenever possible to ensure privacy [670]-[672].

MEO Security: Virtualization attacks are possible against MEO [673]. A compromised MEC orchestrator (MEO) might have a significant influence on the whole MEC system's operation. Examples include the suspension of MEC critical programs, the enrollment of malicious application bundles, and uneven resource utilization of the MEC hosts. Self-analysis methods for hypervisors must be used; for Linux-based systems, Security Enhanced/Extended Linux (SELinux) may be useful [674], [675]. Nevertheless, given the quickness with which technology and assaults develop nowadays, it is deemed more appropriate to approach through software-programmable solutions rather than inflexible hardware (to allow for updates, changing targets, reactive attacks, and so forth). The issues of privacy and confidentiality in softwarization as well as virtualization do not only pertain to MEC, since adaptable solutions are necessary to safeguard 5G and beyond networks in general. Within the MEC-in-NFV infrastructure, solutions to virtualization challenges and security frameworks have been examined [676], [677]. They comprise Trusted Platform Manager (TPM)-based attestation and validation of MEC applications and VNFs, in addition to the Customer Facing Service (CFS) portal queries. Auto-configurable security features, as well as approaches to safeguard VNF in NFV settings, are suggested [678], [679]. Ideally, a security facilitator relying on softwarization (VNF/SDN) might eliminate the requirement for manual configuration, which is no longer practicable under present conditions. Yet, it is unclear how such a cybersecurity orchestrator should be designed and incorporated into the MEC architecture.

Interconnection Security: OSS is subject to attacks outside the MEC infrastructure at the MEC system level because of its interaction with the CFS interface and user applications through the LCM proxy. It creates security vulnerabilities; for instance, the CFS interface is vulnerable to DDoS assaults [680]. OSS can be used to disguise adversaries that claim to have valid access. In the absence of suitable security controls, a large volume of queries from the OSS towards the MEC orchestrator may harm the performance of the MEC orchestrator [681].

9.5.2. MEC Host-Level

Physical Security: MEC hosts are placed near the network's edge, near user devices, and in open surroundings. As a result, the physical placement of the MEC hosts gets insecure with host-level devices being even more susceptible to physical intrusions than system-level equipment, which is often located in a more physically safe region. Moreover, the desire to deploy a large number of MEC hosts to encompass a whole region creates concerns about maintaining a high degree of physical security [682]. This raises the danger of unwanted physical accessibility and, as a result, physical degradation or manipulation of devices, with direct repercussions for accessibility (e.g., DoS attack attempts) and secrecy (e.g., data leakage via both active as well as passive assaults) [683]. The equipment may lack the hardware security of generic servers [684], however, the MEC equipment should include anti-theft as well as anti-damage procedures as a kind of protection. Tamper protection is unquestionably a strong security method for preventing the reading of secret data (e.g., cryptography keys) and ought to be implemented in the context of MEC hardware as well. The well-known notion of the weakest point applies in this situation: the protection of the total system is guaranteed by the safety of the weakest point (the attackers usually target weak points.). MEC hosts with inadequate security can quickly become targets [685]-[688].

Privacy of User Location: Location tracking facilitated by MEC might be viewed as both a benefit and a concern. Unauthorized exposure to the Location Application Program Interface (API) can pass sensitive data concerning user navigation and tracking over time [689], [690], comparable to unauthorized entry to radio network data in mobile communications (i.e., access to user recognition mechanisms, which may jeopardize the users' confidentiality) [691], [692]. MEC hosts (and hence users) are thus directly vulnerable to location privacy problems [693]. To mitigate such dangers, API privacy and highly synthesized location records or processed/encrypted data play a significant role. Nevertheless, when GPS services are unavailable or in the case of emergencies, the MEC geo-location service can be useful. Reference literature performed research on location privacy [694]-[697].

Local Defenses: Because of their local nature, host-level assaults have a geographically limited impact on the end users. This enables MEC to impose security procedures and minimize assaults in the local networking segment [698]. MEC is appropriate for deploying a defense perimeter, such as against DDoS assaults where the attacker only targets a tinier traffic stream, and the edge may inform the core network well about the source of risk, resulting in overall improved reliability. MEC's remote or localized aspect can further improve confidentiality by preventing data from approaching centralized servers and therefore eliminating a threat to centralized infrastructure. For example, the processing of photographs of vehicle registration plates at the edge server and recognition of the registration number to just pass the number to the central server (this prevents the possibility of location leaks) [699]. Conversely, at the same moment, it is considered that local information transfer (as opposed to, say, transferring information via the internet) decreases data exposure [700], but can raise security threats when the volume of data traversing nodes is large, due to heavy traffic and location near the network's edge [701]. The works [702], [703] presented several security enhancement techniques for MEC-assisted IoT context.

Virtualization Security: Malicious Virtual Machines might try to take advantage of their hosting [704]. Malicious insiders having adequate permission to access as well as harm a Virtual Machine or even a suspicious Virtual Machine with advanced privileges [705], [706] might be used in Virtual Machine manipulation attempts. If a Virtual Machine is operating on many servers, a typical DoS attack or assault may cause harm to all servers at the same time [707]. As a defense against DoS assaults, Virtual Machines' resource usage should be controlled, and resource usage should be balanced between servers [708], [709]. In terms of data privacy, subscriber information is preserved at the MEC server level, which means it might be exposed. Moreover, the possibility of data alteration necessitates proper backup and recovery capabilities, which are strongly linked to dependability prevention. Virtualization attacks may disrupt orchestrating on the host side, and an exploited Virtualized Infrastructure Manager can cause MEC services to fail [710]. Another kind of contamination is service manipulation, which can have serious effects including DoS or data leaking attacks [711]. If a system got corrupted (not only through virtualization assaults, but in a broad sense), the adversary may intervene at multiple levels (e.g., applications, services, resource usage) and launch a variety of attacks.

Constrained Resources: The use of computationally complex security techniques, such as heavy encryption, can be an issue. For example, edge devices may have restricted connection and resources, limiting the security standards that may be implemented and facilitating the vulnerability of attacks. This might lead to limitations in the adoption of high-security systems, such as authentication. The employment of public-key cryptography, particularly, public-key infrastructure (PKI) may be problematic due to high computational expense and maintenance [712]. The adoption of lightweight encryption can be considered in this sense [713], [714]. Data deduplication technologies at the edge (detecting and deleting duplicate data or even preventing recomputations) would improve performance on resource or capacity-constrained devices. Nevertheless, doing this while retaining security is generally attainable with Fully Homomorphic Cryptography, which involves extremely high computation overhead [715]. The European Authority for Cybersecurity (ENISA) recognized the complexity of implementing security approaches in 5G and beyond networks (because of the combination of technologies like cloud computing, fog computing, and edge computing), and the necessity of efficient cryptographic algorithms (due to resource constraints on nodes) as major aspects in 5G and beyond security studies and developments.

10. Lessons Learned, Challenges, and Future Directions

This section of the paper includes lessons learned through the survey. Moreover, this section described the open issues and future research scope relative to MEC technology.

10.1. Lessons Learned

The lessons learned through this survey work are enlisted below:

- 5G Service Based/Oriented Architecture (SBA/SOA) suggested by 3GPP can enable a higher degree of service access efficiency and flexibility for the MEC framework.

- Softwarization/SDN can provide enhanced scalability, accessibility, resiliency, and interoperability for MEC services.
- Virtualization of the network can minimize the OPEX and CAPEX and can ensure more flexibility and rapid implementation of new services.
- Network slicing, as one MEC enabler, can deliver the dynamic infrastructure and effective resource utilization.
- ICN employs two conceptual designs, namely connectivity and caching, e.g., at MEC computing servers, to reduce the bandwidth congestion problem and enhance data delivery.
- SFC can allow MEC to adjust a networking service function to the end user context and deliver end-to-end services. Incorporation of SFC within MEC is an acceptable technique for organizing service function implementation, realizing desired strategies, adapting applications when approaches or policies evolve, and rationally allocating resources to provide needed services. SFC offers a wide range of MEC applications, which can improve MEC functioning in terms of resource optimization, privacy, and accessibility.
- H-CRAN can assure ease of the installation of the MEC system, taking into account the computing and storage facilities in the BBU pools as well as the deployment of the RRHs. By collocating MEC and H-CRAN, the expenditure on MEC implementation can be significantly decreased. The integration of MEC with H-CRAN can give the operational versatility and infrastructure reconfigurability that the virtualization of H-CRAN may deliver.
- D2D-aided MEC can provide ad-hoc computation resources as per demand for scenarios such as IoT, V2V, V2X, etc.
- AI/ML-based computation/communication resource allocation schemes can help to improve the efficiency of the MEC system.
- NOMA and RSMA multiple access techniques can improve the communication resource utilization for MEC services.
- The implementation of UAVs in MEC communication for content offloading can enable the possibility of ad-hoc implementation, reduces energy consumption and communication delay, and provides better coverage and therefore computational performance optimization.
- The integration of SWIPT technology with MEC can enable networks to deliver computational services and energies to the device through the downlink and uplink at the same time.
- The deployment of IRSs can improve the device-to-MEC data transmission rates, thus significantly minimizing their computation-offloading latency, particularly when the device-to-MEC LoS links are blocked. Since IRSs establish LoS links and/or introduce scattering and beamforming gains and improved communication channel/s can be obtained which improves energy efficiency.
- Game Theory and Auction Theory can be utilized for improved computation and communication resource orchestration in the MEC framework.
- Digital Twin-enabled MEC network can establish a bridge between the physical MEC facility and digital systems. It can capture real-time network characteristics and utilize them to make optimum network decisions instantly from a centralized standpoint. Therefore, it may be used to directly develop and optimize network strategies such as workload offloading, allocation of resources, caching, and so forth, and the connectivity schemes' effectiveness and affordability can be improved. It can enable computationally intensive applications like Metaverse and automated vehicles.
- Open-source MEC can improve the accessibility and flexibility of the evolving MEC systems. Specifically, open-source-MEC splits the closely connected service functions into numerous separate NFs and supports them flexibly via a simpler service-based interface (SBI) by establishing a service-based MEC layer. The open-source MEC framework will be highly assistive to embrace the evolving network infrastructures.
- Scalability, computational, and energy efficiency can be achieved by incorporating quantum computing in MEC. However, the research on quantum computing for MEC is still in its early stage, therefore, further research is required.
- The fusion of MEC and PON systems can be a promising option for delivering latency-sensitive but task-intensive services to meet such demanding QoS requirements.
- Applications and services such as smart cities, smart agriculture, smart industries, the e-healthcare, smart vehicular network, video analytics, etc. can be benefited from the escalated computational facilities of MEC.
- State-of-the-art security or privacy-preserving mechanisms should be researched and analyzed continuously since threats against the MEC framework are ever-evolving and maintaining security and privacy is a significant challenging task. Especially, the security and privacy of the Virtual Machines should be strictly maintained otherwise confidentiality of the system and user data can be threatened.

10.2. Challenges and Future Directions

Standardization: Edge computing has evolved as an enticing and critical paradigm for scientific and industrial endeavors. Various standardization organizations have worked hard to develop suggestions and references for attempting to incorporate MEC from either the edge of the network or the MEC-5G standardized network level [716]. The International Electro-technical Commission (IEC) and ISO have worked hard to define cloud infrastructure, software packages, the Virtual Machine and Container maintenance, and orchestration. ETSI is a major participant in the 5G-MEC industry, and its various white papers have contributed to the standardization of MEC systems. A versatile standardization approach for the MEC paradigm is required to embrace beyond 5G, i.e., 6G networks. In this context, frameworks like open-source MEC should be appropriately analyzed and enhanced to incorporate versatile 6G networking infrastructure.

Energy Consumption: Environmental change has become one of the major urgent challenges of the twenty-first century. Global warming has forced the world to concentrate more on clean, renewable energy. Yet, with today's growing electricity usage owing to revolutionary frontier applications, there is a greater than ever necessity for utilizing renewable sources of energy as the major driver of MEC infrastructure. Whereas MEC promises to minimize energy consumption, there has been a growing demand for MEC servers to be powered by clean energy and recovered energy sources. Nonetheless, significant attempts are being made to reduce MEC servers' energy use while simultaneously making offloading decisions that promote MEC powered by renewable energy [717].

The MEC deployment moves storage and computing facilities that were previously in the data center to the network's edge. On the other side, the network edge may react to user requests while also decreasing the unnecessary use of returning services. One of the primary areas of attention in MEC network enhancement is energy efficiency. Media caching, processing, and connectivity between MECs and subscribers or user devices can all result in high energy usage in the MEC transmission scheme. As a result, it is critical to design an effective resource optimization method to minimize system energy usage to adequately plan caching, processing, and communication resources.

Moreover, there are three types of energy usage for the combined optimization of MEC-based media caching and encoding/decoding: caching, encoding/decoding, and signal propagation energy consumption. As a result, determining ways to enhance total energy efficiency while simultaneously considering caching, encoding/decoding, and transmission is a significant problem for future research.

Efficiency and Scalability of Mobility Management Network Functions: During handovers, packets or data payloads may be delayed at the originating base station for improved mobility control [718]. The queued packets are sent from the originating base station to the replacement base station when the user device is switched over to another base station. Any shared anchoring switch linked to the source continues to multicast payloads to all potential recipient base stations. MEC hosts connected to base stations can cache packets, and just a high-capacity MEC server can serve as the anchoring switch. Further study is needed to improve the efficiency and scalability of mobility management networking functions with the help of MEC hosts. In addition to the foregoing, when a device is going to be handed over, observing the interactions of MEC features, such as the functionality of the targeted MEC host and position management, is an unexplored field. Handover may be conducted while taking MEC factors into account: for instance, a handover to a MEC server must be executed only when it has adequate resources [719].

Studies concentrating on mobility management, notably Virtual Machine migration, have largely assumed that each user device's computational task/s is computed by a single computing station. As a result, the difficulty is to manage the Virtual Machine migration method effectively when the operation is offloaded to multiple computational nodes. Furthermore, Virtual Machine migration places a heavy burden on the backhaul and therefore causes significant latency, which renders it inappropriate for real-time operations. As a result, more improved methodologies for highly rapid Virtual Machine migration in millisecond range need to be devised. Nevertheless, because of the communication issues between computing servers, this approach is quite difficult. As a result, a more practical task is finding ways to pre-migrate the computations in advance (e.g., using certain prediction techniques) such that no service interruption is apparent to users. Although solutions above may reduce the Virtual Machine migrating period, stand-alone Virtual Machine migrating may indeed be inappropriate for real-time applications. As a result, it is crucial to direct the majority of studies on the collaboration of independent mobility management strategies. Dynamic management and joint integration of all strategies (including power management, Virtual Machine migration, compaction of migrated content, and/or route planning) should be explored more extensively in this respect to improve the user experience for user devices and improve the entire system performance for migrating users.

MEC Service Orchestration and Programmability: Service orchestration and reconfigurability concerning distinct levels of the MEC system (i.e., application platform, infrastructure, and services offered on the system) remain unresolved concerns that pose substantial obstacles. Service orchestration must be undertaken in tandem with network resource portability, taking potential and Virtualized Network Function allocation into account, particularly the stretching of functions across a collection of edge-cloud systems. Edge-cloud systems located across separate management domains present additional impediments for service orchestration when considering interoperable resources, where further studies are needed for resource aggregation as well as service mapping mechanisms, in addition to the specification of the associated APIs.

This article discusses various service attributes of edge-cloud coordination and reconfigurability, such as (i) service operational activities, i.e., allocating resources, service alignment, platform selection, and trustworthiness, (ii) continuity of service and flexibility within a cluster of MEC/edge computing stations, and (iii) cooperative optimization of Virtualized Network Functions as well as MEC services on pervasive edge computing systems to achieve effective utilization of resources and cross-layer or inter-tier optimization or improvement among edge-cloud services. Moreover, it provides an overview of the diverse MEC system architecture scenarios and specifies the prospective MEC orchestrator deployment alternatives while taking into account various SDN/NFV convergence opportunities that enable diverse edge-cloud resource management varieties.

The development and standardization initiatives for providing effective MEC services are currently underway, with several hurdles remaining [720]. One of the main areas is the establishment of enhanced APIs that will allow third parties to purchase and coordinate resources on MEC systems simply and efficiently, including the related data models. Several APIs and data formats are still being discussed in ETSI-MEC in light of evolving usage cases, such as leveraging the mmWave scientific breakthrough to aid the MEC platform. Similar APIs should additionally be extended to give RAN-relevant or network-related information, allowing the application to observe the network.

Multiple-MEC Coordinated Collaboration: MECs are often deployed in a dispersed fashion in edge networks, with MEC-based caches and computing capabilities scattered across the network. An individual MEC has limited storage capacity and computational power. Unnecessary caching and computation operations will cause the MEC server to become overloaded. When these activities are forwarded to the data center within the cloud, the expenses will rise. As a result of multi-MEC in decentralized mode, nearby MEC servers can work together to execute caching and computational activities. Other inactive MEC systems can be utilized to minimize network expenses and enhance the performance of the network when the present MEC server lacks caching or processing resources [721], [722]. Also, resource sharing across MEC servers becomes a significant study topic. For example, how to choose a desired server among several other MEC servers that cache related material when the target multimedia content demanded by the subscriber is not cached by a native MEC host. The transfer of local computational activities to other MEC servers whenever the native MEC server's processing demand is preoccupied is a notable research issue as well. The resource-sharing strategy based on decentralized multi-MEC collaboration has to be investigated further in the future to increase resource usage and QoE.

Offloading Decision: The offloading approach selection is critical since it decides whether the task computing is executed locally, remotely, or concurrently in both places. All current researches on the offloading selection consider solely the user device's energy usage into account. Nevertheless, to be consistent with forthcoming green networking, overall energy usage at the MEC (such as computation and associated communication) should be considered further throughout the offloading decision-making process. Furthermore, all studies working with the offloading decisions assume completely static circumstances, in which the user devices do not move before or during offloading. Yet, the energy required for data transmission might be drastically altered even during offloading when channel quality degrades owing to fading or uneven mobility. Therefore, offloading potentially increases energy usage and/or execution time as compared to local computing. As a result, it is required to provide more sophisticated ways for offloading decision-making. Such as the deployment of prediction approaches for the improvement of transmission quality in the context of user mobility (at the time of task offloading).

Moreover, recent works that focus on the partly offloading decisions ignore the prospect of offloading particular pieces to various edge computing nodes. Many edge computing nodes provide greater flexibility and raise the likelihood that offloading towards the MEC will indeed be advantageous for the end device (in terms of energy usage and task execution time). A fundamental problem, in this case, is the aspect of backhaul connectivity between the interacting MEC systems and the capacity to accommodate their fluctuating load and characteristics during the offloading selection.

User Experience and Bandwidth Tradeoffs: User experience is a metric of a user's satisfaction or dissatisfaction with a service that focuses on the full service experience. The advancement of adjustable bitrate is a crucial motivation for investigating an effective way to improve user experience, consequently providing consumers with a distinct service to improve user satisfaction [723]. Furthermore, research on the balance between bandwidth efficiency and user experience optimization in MEC-dependent caching and encoding/decoding techniques is an important area of study. From the standpoint of video content suppliers, two critical variables must be addressed for system optimization: (i) the requirement to lower the expenses of caching and computation; (ii) assuring an improved user experience to consumers (especially, meeting the requirement of computation and communication latency). As a result, how to optimize the expenditure of bandwidth capacity for MEC-dependent caching and encoding with user experience is an essential future research path.

Security: In every network, privacy and safety are always key concerns. As a result, data and edge infrastructure security and privacy are critical for computational offloading. Privacy and confidentiality problems for security setup, threat detection, threat mitigation, and system verification remain unresolved. To limit the security vulnerabilities on the server level, software-defined segregation, and trust management verification are viable alternatives [724]. While running Secure Sockets Layer (SSL) or Transport Layer Security (TLS) guidelines on the UE is prohibitive in some contexts [725], identifying lightweight security standards for the MEC system that may be utilized for user identification, access regulation, password, and credential management is still challenging. In the application segmentation approach, the trade-off between computation for encrypting data and the requirement to use security certificates should be addressed.

Unlike standard cloud computing, MEC exhibits substantial security vulnerabilities, particularly when placed within the ground base stations, or in places where it is exposed to physical assaults. As a result, MEC installations increase security measures against on-site threats. MEC also necessitates stricter security rules since third-party partners can obtain access to the service and retrieve information regarding user geographic location and radio statistics. Authentication based on third-party platform access credentials should be evaluated. One such possibility is to use strategies focused on public-key infrastructure (PKI).

Another significant issue is isolation between various stakeholders, namely, between hosted programs. A security assault on one program should not impact other apps that are running, and isolation should offer privacy while ensuring bidirectional trust among collaborating parties. To provide safe cooperation and interoperability across diverse resources and multiple operating parties, fine-grained authorization with suitable encryption should be considered. In [726], a cutting-edge examination of security and privacy concerns related to edge cloud is undertaken, whereas [727] offers preliminary research on MEC security. With cloud computing, several intrusion detection approaches are in existence, but massive-scale geographically-distributed setups remain a concern for the forthcoming ultra-dense networks.

Space-Air-Ground Integrated Network and MEC: UAVs have superior coverage and can deliver stable and smooth services utilizing LoS connections since they fly at higher altitudes. Yet, in some adverse conditions, UAVs may be unable to conduct vital duties on their own. As a result, help from other networks, such as satellite networks, is required [728]. Since satellites often have extensive coverage areas, they may transport data and control instructions between UAVs and distant ground networks. Moreover, the MEC workstations can indeed be integrated with satellites to improve the edge computing capacity.

The space-air-ground interactive MEC system has various obstacles. Satellites' most prominent drawbacks are propagation loss as well as latency. Nevertheless, the high operational costs of satellite connectivity may preclude widespread use. Thankfully, recent advances in satellite technology have decreased the cost of LEO satellites significantly, and the transmission delay may be dropped to 1-4 milliseconds because of the low orbit height [729], [730]. Yet, the rapid mobility of satellites as well as UAVs frequently alters the channel state, therefore, resulting in rapid handover, making management of space-air-ground unified MEC systems problematic. More significantly, operating satellites and UAVs in heterogeneous systems to provide reliable signaling exchanges and data transfer among many stakeholders is difficult. To address interoperability challenges and accomplish the promised advantages of space-air-ground interoperable MEC systems, more research into a complete mechanism for collaborative communication and computation, resource allocation, and cost-effective protocol design is required [731], [732].

Edge Intelligence: Edge intelligence is gaining traction, allowing user devices to execute the pre-trained DL algorithm from the edge of the network natively. Federated Learning (FL) seems to be a potential distributed Deep Neural Network (DNN) training approach to enhance confidentiality. The author of [733] recommended leaving the raw information on the user device and developing a common framework on the edge computing server by combining locally computed or processed updates. As a result, FL is a viable future option to deploy edge intelligence to improve MEC functioning.

The Accessible Business Rules Framework (ABR)-based caching solution, which is based on the DRL algorithm, is an important research avenue for video streaming systems [734]. Every video block throughout the adaptable bitrate streaming system includes numerous bitrate variants.

Caching multiple bitrates can result in a loss in caching resource usage and an escalation of network expenses due to the capacity constraint of the MEC-based caching system. With the assistance of MEC, network information, such as network link conditions and user activity, may be observed in real-time. Furthermore, this data may be examined and processed utilizing a DRL-based approach, which predicts the popularity of media content as well as the bitrate level for user reactions. As a result, for audiovisual caching with the relevant bitrate variant, the resource allocation technique may be determined in advance, which can increase the cache hit percentage and caching resource usage.

When ML methods are deployed on resource-limited MEC workstations, there is a discrepancy between computational capacity and learning performance. As a result, efficiently implementing an ML algorithm on a MEC server with such a huge number of subscribers and a massive quantity of training data is difficult. Whereas an Artificial Neural Network (ANN) has several layers (e.g., input/output and hidden layers), the optimizer and the stratified MEC architecture are intended to function together. An instantaneous layer of the complete ANN model can indeed be transferred to and handled by multiple MEC workstations (e.g., MEC at macro and small cells), and the outcome of edge training is then relocated to higher-tier cloud computing for further processing. The shrinking of training dataset size, the utilization of pervasive computing, and the protection of user data confidentiality altogether provide significant benefits to cooperative learning. Moreover, DL techniques may be used at MEC servers to identify tainted and/or fabricated data, hence enhancing data quality. In [735], Ming et al. investigated Graph-Assisted Reinforcement Learning for video surveillance using IoT devices. Adaptive video functionality and edge processing have been developed to increase accuracy and minimize latency with constrained capacity.

Traditional ML techniques are ineffective in protecting data confidentiality. Federated Learning distributes training data among individual users, allowing them to develop a shared model jointly while maintaining their unique data locally. Furthermore, Federated Learning can address serious disadvantages of Distributed Learning [736], such as (i) a scarcity of training data and time, (ii) poor performance because of diverse user functionality and network connectivity states, (iii) an inconsistent quantity of training dataset, and (iv) data that is not autonomous and identically dispersed among subscribers. Federated Learning is projected to be a powerful solution for addressing a variety of issues in MEC. Consider the computation offloading issue, in which large numbers of users attempt to offload their operations to a MEC server for external processing. Traditionally, to decide the offloading decision, users must send information to the MEC server along with channel conditions, current battery status, and computation capabilities; nevertheless, this information can be exposed to eavesdroppers and unlawfully utilized to anticipate the user location. With Federated Learning, every user downloads the master template from the MEC system and then determines the offloading preference based simply on its local features, where the MEC is only responsible for refreshing the master template in response to specific user variations. Federated

Learning may ensure data privacy while also providing distributed offloading choices, making it suited for large-scale MEC infrastructures [737].

11. Conclusion

The work performed a survey on the concurrent advancements of the MEC paradigm. Under this circumstance, it reviewed the existing survey or review works to provide an insight into the present state of research and development progress relative to MEC technologies. The work then illustrated an overview of the relative cloud technologies and fundamentals of MEC and hereafter discussed the architectural aspects of MEC. Afterward, the survey stated the contemporary state-of-the-art enabling technologies for MEC, including Virtual Machines, Containers, SDN, NFV, network slicing, ICN, SFC, radio access control, such as C-RAN, F-RAN, H-CRAN, D2D, machine learning/artificial intelligence, etc. Further, the advancing supporting technologies such as NOMA and RSMA, deployment of UAVs, energy harvesting and SWIPT, implementation of IRSs, Game Theory, Auction Theory, Digital Twin technologies, open-source framework (open-source MEC), quantum computing, PON, etc. are discussed. Then, system-aware and user-oriented deployment scenarios of MEC technologies are stated. Moreover, a brief description of security issues to MEC infrastructure and relative prevention mechanisms are briefed. Finally, the work provided a brief description of the lessons learned through the survey and mentioned challenges and future scope for the further improvement of MEC technologies. Hopefully, this survey will be highly supportive to enthusiasts from academia and industry.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The authors would like to express their gratitude to the Department of Electrical and Computer Engineering, New York University (NYU) Abu Dhabi, Abu Dhabi, UAE.

Appendix

Table 3 represents the list of acronyms.

Table 3: List of Acronyms

Acronyms	Definitions
3GPP	Third Generation Partnership Project
4C	Joint Communication, Caching, Computing, and Control
5G	Fifth Generation
6G	Sixth Generation
ABR	Accessible Business Rules
AF	Application Function
AFA	Air Fuel Alliance
AGV	Autonomously Guided Vehicle
AI	Artificial Intelligence
AM	Amplitude Modulation
ANN	Artificial Neural Network
AP	Access Point
API	Application Program Interfaces
AR	Augmented Reality
AS	Antenna Splitting
ASP	Application Service Provider
AUSF	Authenticating/Identification Server Function
B5G	Beyond 5G
BBU	Baseband Unit
BS	Base Station
BSS	Base Station Subsystem
CAPEX	Capital Expenditure
CDMA	Code Division Multiple Access
CD-NOMA	Code-Domain NOMA
CDUS	Central Unit and Decentralized Unit Segregation

CFS	Customer Facing Service
CN	Core Network
CPS	Cyber-Physical System
CPU	Central Processing Unit
C-RAN	Cloud-RAN
CR-NOMA	Cognitive Radio-NOMA
CSI	Channel-State Information
D2D	Device-to-Device
DDL	Distributed Deep Learning
DDoS	Distributed DoS
DDPQN	Double Dueling Prioritized Deep Q-Network
DDQN	Double-Deep Q-Network
DITEN	Digital Twin-Enabled Edge Network
DL	Deep Learning
DNN	Data Network Name/Deep Neural Network
DNS	Domain Name System
DoS	Denial of Service
DRL	Deep Reinforcement Learning
DT	Digital Twin
DUD	Downlink and Uplink Detaching
E2E	End-to-End
EB	Exabytes
EBI	East-Bound functionality Interface
EC	Edge Computing
ECDU	Edge Content Distribution And Update
EEDTO	Energy-Efficient Dynamic Computational Task Offloading
EH	E-Healthcare/Energy Harvesting
EM	Element Maintenance/Electromagnetic
eMBB	enhanced Mobile Broadband
ETSI	European Telecommunications Standards Institute
EV	Electric Vehicle
FANET	Flying Ad Hoc Network
FEC	Fog-Edge-Cloud
FM	Frequency Modulation
F-RAN	Fog-RAN
GBCO	Game-Based Computational Offloading
GPS	Global Positioning System
GT	Game Theory
HAP	Higher Altitude Platform
H-CRAN	Heterogeneous-CRAN
HetNet	Heterogeneous Network
HSD	Hardware/Software Detaching Or Decoupling
HTTP	Hypertext Transmission Protocol
IaaS	Infrastructure-as-a-Service
ICI	Inter-Carrier Interference
ICN	Information-Centric Networking
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIoT	Industrial IoT
IoT	Internet of Things
IoV	Internet of Vehicles/Vehicular Internet of Things
IPTV	Internet Protocol Television
IPTVoWTTx	IPTV over WTTx
IRS	Intelligent Reflecting Surface
ISG	Industrial Specifications Group
ISI	Inter-Symbol Interference
ITS	Intelligent Transportation Systems
ITU	International Telecommunication Union

kW	Kilo Watt
LAN	Local Area Network
LAP	Lower Altitude Platform
LAPN/LADN	Local Area Packet/Data Network
LCM	Lifecycle Management
LEO	Low Earth Orbit
LoS	Line-of-Sight
LTE	Long Term Evolution
M2M	Machine-to-Machine
MAC	Media Access Control
MACC	Mobile Ad Hoc-Based Cloud Computing
MAR	Mobile Augmented Reality
MCC	Mobile Cloud Computing
MEC	Mobile Edge Computing/Multi-Access Edge Computing
MEH	MEC Host
MEO	MEC Orchestrator
MEP	MEC Platform
MEQC	Multi-Access Edge-Quantum Computing
MIMO	Multi-Input Multi-Output
MitM	Man-in-the-Middle
ML	Machine Learning
mMIMO	Massive MIMO
MMSE	Minimum Mean Squared Error
mmWave	Millimeter Wave
MNO	Mobile Network Operator
MSN	Mobile Social Networking
MUSA	Multi-User Shareable Access
NBI	North-Bound functionality Interface
NC	Non-Cooperative
NEF	Network Exposure Function
NFC	Near-Field Communications
NFV	Network Functions Virtualization
NFV MANO	NFV Management and Orchestration
NFVI	NFV Infrastructures
NFVO	NFV Operator
NLoS	Non Line-of-Sight
NOMA	Non-Orthogonal Multiple Access
NRF	Network Resource Function
OFDMA	Orthogonal Frequency-Division Multiple Access
OMA	Orthogonal Multiple Access
OPEX	Operational Expenditure
OS	Operating System/Open-Source
OSS	Operation Support Subsystem
OTT	Over-The-Top
PaaS	Platform-as-a-Service
PCF	Policy Control Function
PCR	Predictive-Collaborative-Replacement
PD-NOMA	Power-Domain NOMA
PKI	Public-Key Infrastructure
PON	Passive Optical Network
PPP	Poisson Point Process
PS	Power Splitting
PTE	Power Transfer Efficiency
PU	Primary User
QoE	Quality of Experiences
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technique/Technology
RESTful	Representational State Transfer-ful

RF	Radio Frequency
RFID	Radio Frequency Identification
RIS	Reconfigurable Intelligent Surface
RL	Reinforcement Learning
RNI	Radio Networking Information
RRH	Remote Radio Head
RSMA	Rate Splitting Multiple Access
SaaS	Software-as-a-Service
SAGIN	Space-to-Air-to-Ground Integrated Network
SASE	Secure Access Service Edge
SBA	Service Based Architecture
SBI	Service-Based Interface/South-Bound functionality Interface
SC	Superposition Coding
SCADA	Supervisory Control and Data Acquisition
SCMA	Sparse Code Multiple Access
SDMA	Space Division Multiple Access
SDN	Software Driven Networking
SELinux	Security Enhanced/Extended Linux
SF	Service Function
SFC	Service Function Chaining
SFF	Service Function Forwarder
SIC	Successive Interference Canceling
SIMO	Single-Input Multi-Output
SINR	Signal-to-Interference Plus Noise Ratio
SLR	Systematic Literature Review
SMF	Session Maintenance Function
SOA	Service Oriented Architecture
SOAR	Security Orchestrating, Automating, and Response
SSC	Sessions and Services Continuity
SSL	Secure Sockets Layer
SU	Secondary User
SWIPT	Simultaneous Wireless Information and Power Transfer
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
THz	Terahertz
TLS	Transport Layer Security
TPM	Trusted Platform Manager
TS	Time Splitting
UAV	Unmanned Aerial Vehicle
UCPS	User Plane and Control Plane Separating
UD	User Device
UDM	Unified Data Managing
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable and Lower-Latency
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VIM	Virtualized Infrastructure Manager
VIM	Virtualized/Virtual Infrastructure Manager
VM	Virtual Machines
VMI	Virtual Machine Introspection
VNF	Virtualized Network Function
VNFM	VNF Management
VR	Virtual Reality
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WIT	Wireless Information Transmission

WLAN	Wireless Local Area Network
WPC	Wireless Power Consortium
WPT	Wireless Power Transfer
WSN	Wireless Sensing Network
WTTx	Wireless to the Everything/x
XR	Extended Reality

References

1. M. Vaezi et al., "Cellular, Wide-Area, and Non-Terrestrial IoT: A Survey on 5G Advances and the Road Toward 6G," in IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 1117-1174, Secondquarter 2022.
2. Ericsson. Ericsson Mobility Report. June 2021. [Online]. Available: https://iotbusinessnews.com/download/white-papers/ERICSSON-june-2021-mobility-report.pdf. Accessed: February 2023.
3. Ericsson. Ericsson Mobility Report: Global 5G growth amid macroeconomic challenges. November 2022. [Online]. Available: https://www.ericsson.com/en/press-releases/2022/11/ericsson-mobility-report-global-5g-growth-amid-macroeconomic-challenges. Accessed: February 2023.
4. Y. Qian, "Beyond 5G Wireless Communication Technologies," in IEEE Wireless Communications, vol. 29, no. 1, pp. 2-3, February 2022.
5. Cisco. Cisco Annual Internet Report (2018–2023) White Paper. March 2020. [Online]. Accessible: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Accessed: February 2023.
6. U. Singh et al., "Coalition Games for Performance Evaluation in 5G and Beyond Networks: A Survey," in IEEE Access, vol. 10, pp. 15393-15420, 2022.
7. M. Liyanage, P. Porambage, A. Y. Ding and A. Kalla, "Driving forces for Multi-Access Edge Computing (MEC) IoT integration in 5G," ICT Express, vol. 7, no. 2, pp. 127-137, June 2021.
8. M. A. Ebrahim, G. A. Ebrahim, H. K. Mohamed and S. O. Abdellatif, "A Deep Learning Approach for Task Offloading in Multi-UAV Aided Mobile Edge Computing," in IEEE Access, vol. 10, pp. 101716-101731, 2022.
9. Y. Wang, H. Wang, S. Chen, and Y. Xia, "A Survey on Mainstream Dimensions of Edge Computing," 2021 the 5th International Conference on Information System and Data Mining (ICISDM 2021), New York, NY, USA, 2021, pp. 1-9.
10. ETSI. New ETSI Mobile-Edge Computing Industry Specification Group starts work. December 2014. [Online]. Available: https://www.etsi.org/newsroom/news/852-2014-12-news-new-etsi-mobile-edge-computing-industry-specification-group-starts-work?jjj=1680708097216. Accessed: February 2023.
11. Light Reading. ETSI Drops 'Mobile' From MEC. September 2016. [Online]. Available: https://www.lightreading.com/mobile/mec-(mobile-edge-computing)/etsi-drops-mobile-from-mec/d/d-id/726273. Accessed: February 2023.
12. B. Blanco et al., "Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN," Computer Standards & Interfaces, vol. 54, no. 4, pp. 216-228, November 2017.
13. C. D. Alwis et al., "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research," in IEEE Open Journal of the Communications Society, vol. 2, pp. 836-886, 2021.
14. S. Elmeadawy and R. M. Shubair, "6G Wireless Communications: Future Technologies and Research Challenges," 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, United Arab Emirates, 2019, pp. 1-5.
15. H. Elayan, O. Amin, B. Shihada, R. M. Shubair and M. -S. Alouini, "Terahertz Band: The Last Piece of RF Spectrum Puzzle for Communication Systems," in IEEE Open Journal of the Communications Society, vol. 1, pp. 1-32, 2020.
16. R. Alghamdi et al., "Intelligent Surfaces for 6G Wireless Networks: A Survey of Optimization and Performance Analysis Techniques," in IEEE Access, vol. 8, pp. 202795-202818, 2020.
17. T. B. Ahammed, R. Patgiri and S. Nayak, "A Vision On The Artificial Intelligence for 6G Communication," ICT Express, May 2022.
18. H. Guo and X. Yu, "A Survey on Blockchain Technology and Its Security," Blockchain: Research and Applications, vol. 3, no. 2, June 2022.
19. M. Banafaa et al., "6G Mobile Communication Technology: Requirements, Targets, Applications, Challenges, Advantages, and Opportunities," Alexandria Engineering Journal, vol. 64, pp. 245-274, February 2023.
20. M. Y. Akhlaqi and Z. B. M. Hanapi, "Task offloading paradigm in mobile edge computing-current issues, adopted approaches, and future directions," Journal of Network and Computer Applications, vol. 212, March 2023.
21. H. Djigal, J. Xu, L. Liu and Y. Zhang, "Machine and Deep Learning for Resource Allocation in Multi-Access Edge Computing: A Survey," in IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2449-2494, Fourthquarter 2022.
22. B. Liang, M. A. Gregory and S. Li, "Multi-access Edge Computing fundamentals, services, enablers and challenges: A complete survey," Journal of Network and Computer Applications, vol. 199, March 2022.
23. L. Hou, M. A. Gregory and S. Li, "A Survey of Multi-Access Edge Computing and Vehicular Networking," in IEEE Access, vol. 10, pp. 123436-123451, 2022.
24. M. A. Khan et al., "A Survey on Mobile Edge Computing for Video Streaming: Opportunities and Challenges," in IEEE Access, vol. 10, pp. 120514-120550, 2022.
25. F. Tang, X. Chen, T. K. Rodrigues, M. Zhao and N. Kato, "Survey on Digital Twin Edge Networks (DITEN) Toward 6G," in IEEE Open Journal of the Communications Society, vol. 3, pp. 1360-1381, 2022.
26. G. Gür et al., "Integration of ICN and MEC in 5G and Beyond Networks: Mutual Benefits, Use Cases, Challenges, Standardization, and Future Research," in IEEE Open Journal of the Communications Society, vol. 3, pp. 1382-1412, 2022.

27. S. Douch, M. R. Abid, K. Zine-Dine, D. Bouzidi and D. Benhaddou, "Edge Computing Technology Enablers: A Systematic Lecture Study," in IEEE Access, vol. 10, pp. 69264-69302, 2022.
28. H. Tabatabaee Malazi et al., "Dynamic Service Placement in Multi-Access Edge Computing: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 32639-32688, 2022.
29. H. Qiu, K. Zhu, N. C. Luong, C. Yi, D. Niyato and D. I. Kim, "Applications of Auction and Mechanism Design in Edge Computing: A Survey," in IEEE Transactions on Cognitive Communications and Networking, vol. 8, no. 2, pp. 1034-1058, June 2022.
30. Y. Sun, H. Ochiai and H. Esaki, "Decentralized Deep Learning for Multi-Access Edge Computing: A Survey on Communication Efficiency and Trustworthiness," in IEEE Transactions on Artificial Intelligence, vol. 3, no. 6, pp. 963-972, December 2022.
31. P. Arthurs, L. Gillam, P. Krause, N. Wang, K. Halder and A. Mouzakitis, "A Taxonomy and Survey of Edge Cloud Computing for Intelligent Transportation Systems and Connected Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 6206-6221, July 2022.
32. H. Jin, M. A. Gregory and S. Li, "A Review of Intelligent Computation Offloading in Multiaccess Edge Computing," in IEEE Access, vol. 10, pp. 71481-71495, 2022.
33. B. Ali, M. A. Gregory and S. Li, "Multi-Access Edge Computing Architecture, Data Security and Privacy: A Review," in IEEE Access, vol. 9, pp. 18706-18721, 2021.
34. N. Sharghivand, F. Derakhshan and N. Siasi, "A Comprehensive Survey on Auction Mechanism Design for Cloud/Edge Resource Management and Pricing," in IEEE Access, vol. 9, pp. 126502-126529, 2021.
35. X. Jiang, F. R. Yu, T. Song and V. C. M. Leung, "A Survey on Multi-Access Edge Computing Applied to Video Streaming: Some Research Issues and Challenges," in IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 871-903, Secondquarter 2021.
36. P. Ranaweera, A. D. Jurcut and M. Liyanage, "Survey on Multi-Access Edge Computing Security and Privacy," in IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1078-1124, Secondquarter 2021.
37. Y. Siriwardhana, P. Porambage, M. Liyanage and M. Ylianttila, "A Survey on Mobile Augmented Reality With 5G Mobile Edge Computing: Architectures, Applications, and Technical Aspects," in IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1160-1192, Secondquarter 2021.
38. S. D. A. Shah, M. A. Gregory and S. Li, "Cloud-Native Network Slicing Using Software Defined Networking Based Multi-Access Edge Computing: A Survey," in IEEE Access, vol. 9, pp. 10903-10924, 2021.
39. F. Spinelli and V. Mancuso, "Toward Enabled Industrial Verticals in 5G: A Survey on MEC-Based Approaches to Provisioning and Flexibility," in IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 596-630, Firstquarter 2021.
40. A. Filali, A. Abouaomar, S. Cherkaoui, A. Kobbane and M. Guizani, "Multi-Access Edge Computing: A Survey," in IEEE Access, vol. 8, pp. 197017-197046, 2020.
41. M. Mehrabi, D. You, V. Latzko, H. Salah, M. Reisslein and F. H. P. Fitzek, "Device-Enhanced MEC: Multi-Access Edge Computing (MEC) Aided by End Device Computation and Caching: A Survey," in IEEE Access, vol. 7, pp. 166079-166108, 2019.
42. J. Moura and D. Hutchison, "Game Theory for Multi-Access Edge Computing: Survey, Use Cases, and Future Trends," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 260-288, Firstquarter 2019.
43. P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila and T. Taleb, "Survey on Multi-Access Edge Computing for Internet of Things Realization," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 2961-2991, Fourthquarter 2018.
44. T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta and D. Sabella, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," in IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1657-1681, thirdquarter 2017.
45. S. Shahzadi, M. Iqbal, T. Dagiuklas and Z. U. Qayyum, "Multi-access edge computing: open issues, challenges and future perspectives," Journal of Cloud Computing, vol. 6, December 2017.
46. E. T. Michailidis, K. Maliatsos, D. N. Skoutas, D. Vouyioukas and C. Skianis, "Secure UAV-Aided Mobile Edge Computing for IoT: A Review," in IEEE Access, vol. 10, pp. 86353-86383, 2022.
47. P. Wei et al., "Reinforcement Learning-Empowered Mobile Edge Computing for 6G Edge Intelligence," in IEEE Access, vol. 10, pp. 65156-65192, 2022.
48. T. Li, X. He, S. Jiang and J. Liu, "A survey of privacy-preserving offloading methods in mobile-edge computing," Journal of Network and Computer Applications, vol. 203, July 2022.
49. Feng et al., "Computation offloading in mobile edge computing networks: A survey," Journal of Network and Computer Applications, vol. 202, June 2022.
50. Q. -V. Pham et al., "A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art," in IEEE Access, vol. 8, pp. 116974-117017, 2020.
51. S. M. A. Huda and S. Moh, "Survey on computation offloading in UAV-Enabled mobile edge computing," Journal of Network and Computer Applications, vol 201, May 2022.
52. A. Waheed et al., "A Comprehensive Review of Computing Paradigms, Enabling Computation Offloading and Task Execution in Vehicular Networks," in IEEE Access, vol. 10, pp. 3580-3600, 2022.
53. A. Shakarami, M. Ghobaei-Arani, M. Masdari and M. Hosseinzadeh, "A Survey on the Computation Offloading Approaches in Mobile Edge/Cloud Computing Environment: A Stochastic-based Perspective," Journal of Grid Computing, vol. 18, pp. 639–671, August 2020.
54. M. Nikravan and M. H. Kashani, "A review on trust management in fog/edge computing: Techniques, trends, and challenges," Journal of Network and Computer Applications, vol. 204, August 2022.
55. L. Bréhon–Grataloup, R. Kacimi and A. Beylot, "Mobile edge computing for V2X architectures and applications: A survey," Computer Networks, vol. 206, April 2022.

56. Lin et al., “A survey on computation offloading modeling for edge computing,” Journal of Network and Computer Applications, vol. 169, November 2020.
57. A. Shakarami, M. Ghobaei-Arani and A. Shahidinejad, “A survey on the computation offloading approaches in mobile edge computing: A machine learning-based perspective,” Computer Networks, vol. 182, December 2020.
58. P. P. Ray, D. Dash and D. De, “Edge computing for Internet of Things: A survey, e-healthcare case study and future direction,” Journal of Network and Computer Applications, vol. 140, pp. 1-22, August 2019.
59. S. Iftikhar et al., “AI-Based Fog and Edge Computing: A Systematic Review, Taxonomy and Future Directions,” Internet of Things, vol. 21, April 2023.
60. S. S. Gill et al., “AI for Next Generation Computing: Emerging Trends and Future Directions,” Internet of Things, vol. 19, August 2022.
61. F. Fatemi Moghaddam, M. Ahmadi, S. Sarvari, M. Eslami and A. Golkar, "Cloud computing challenges and opportunities: A survey," 2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN), Kuala Lumpur, Malaysia, 2015, pp. 34-38.
62. S. Kamboj and N. S. Ghumman, "A survey on cloud computing and its types," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2016, pp. 2971-2974.
63. D. Barbara, "Mobile Computing and Databases-A Survey," in IEEE Transactions on Knowledge and Data Engineering, vol. 11, no. 1, pp. 108-117, January-February 1999.
64. S. A. Ahson and I. Mahgoub, "Research issues in mobile computing," 1998 IEEE International Performance, Computing and Communications Conference. Proceedings (Cat. No.98CH36191), Tempe/Phoenix, AZ, USA, 1998, pp. 209-215.
65. H. -F. Yu, C. -J. Hsieh, H. Yun, S. V. N. Vishwanathan and I. Dhillon, "Nomadic Computing for Big Data Analytics," in Computer, vol. 49, no. 4, pp. 52-60, April 2016.
66. L. Bittencourt et al., “The Internet of Things, Fog and Cloud continuum: Integration and challenges,” Internet of Things, vol. 3–4, pp. 134-155, October 2018.
67. H. W. van der Westhuizen and G. P. Hancke, "Mobile cloud computing and application program interfaces — A review," 2017 IEEE AFRICON, Cape Town, South Africa, 2017, pp. 1569-1574.
68. S. S. Qureshi, T. Ahmad, K. Rafique and Shuja-ul-islam, "Mobile cloud computing as future for mobile applications - Implementation methods and challenging issues," 2011 IEEE International Conference on Cloud Computing and Intelligence Systems, Beijing, China, 2011, pp. 467-471.
69. A. S. Bale et al., "Mobile Cloud Computing - Enabling Technologies and Applications," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 2021, pp. 491-496.
70. K. Cao, Y. Liu, G. Meng and Q. Sun, "An Overview on Edge Computing Research," in IEEE Access, vol. 8, pp. 85714-85728, 2020.
71. K. Cao, S. Hu, Y. Shi, A. W. Colombo, S. Karnouskos and X. Li, "A Survey on Edge and Edge-Cloud Computing Assisted Cyber-Physical Systems," in IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7806-7819, November 2021.
72. F. Shirin Abkenar et al., "A Survey on Mobility of Edge Computing Networks in IoT: State-of-the-Art, Architectures, and Challenges," in IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2329-2365, Fourthquarter 2022.
73. M. Satyanarayanan, P. Bahl, R. Caceres and N. Davies, "The Case for VM-Based Cloudlets in Mobile Computing," in IEEE Pervasive Computing, vol. 8, no. 4, pp. 14-23, October-December 2009.
74. M. Babar, M. S. Khan, F. Ali, M. Imran and M. Shoaib, "Cloudlet Computing: Recent Advances, Taxonomy, and Challenges," in IEEE Access, vol. 9, pp. 29609-29622, 2021.
75. G. Lewis, S. Echeverría, S. Simanta, B. Bradshaw and J. Root, "Tactical Cloudlets: Moving Cloud Computing to the Edge," 2014 IEEE Military Communications Conference, Baltimore, MD, USA, 2014, pp. 1440-1446.
76. I. Yaqoob et al., “Mobile Ad Hoc Cloud: A Survey,” Wireless Communications & Mobile Computing, July 2016.
77. C. Zhu, V. C. M. Leung, L. T. Yang and L. Shu, "Collaborative Location-Based Sleep Scheduling for Wireless Sensor Networks Integrated with Mobile Cloud Computing," in IEEE Transactions on Computers, vol. 64, no. 7, pp. 1844-1856, July 2015.
78. M. Chowdhury, “Time and Energy-Efficient Hybrid Job Scheduling Scheme for Mobile Cloud Computing Empowered Wireless Sensor Networks,” International Journal of Ad Hoc and Ubiquitous Computing, vol. 37, no. 1, pp. 26-36, May 2021.
79. M. Conti and S. Giordano, "Mobile ad hoc networking: milestones, challenges, and new research directions," in IEEE Communications Magazine, vol. 52, no. 1, pp. 85-96, January 2014.
80. A. Khalifa, M. Azab and M. Eltoweissy, "Towards a Mobile Ad-Hoc Cloud Management Platform," 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, London, UK, 2014, pp. 427-434.
81. M. Mukherjee, L. Shu and D. Wang, "Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 1826-1857, thirdquarter 2018.
82. P. Habibi, M. Farhoudi, S. Kazemian, S. Khorsandi and A. Leon-Garcia, "Fog Computing: A Comprehensive Architectural Survey," in IEEE Access, vol. 8, pp. 69105-69133, 2020.
83. M. R. Raza, A. Varol and N. Varol, "Cloud and Fog Computing: A Survey to the Concept and Challenges," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-6.
84. M. Yannuzzi et al., "Toward a converged OpenFog and ETSI MANO architecture," 2017 IEEE Fog World Congress (FWC), Santa Clara, CA, USA, 2017, pp. 1-6.
85. P. -H. Kuo et al., "An Integrated Edge and Fog System for Future Communication Networks," 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Barcelona, Spain, 2018, pp. 338-343.
86. O. Chabbouh, S. B. Rejeb, N. Agoulmine and Z. Choukair, "Cloud RAN Architecture Model Based upon Flexible RAN Functionalities Split for 5G Networks," 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, 2017, pp. 184-188.
87. Y. -J. Ku, D. -Y. Lin and H. -Y. Wei, "Fog RAN over General Purpose Processor Platform," 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 2016, pp. 1-2.

88. A. Sattari, R. Ehsani, T. Leppänen, S. Pirttikangas and J. Riekki, "Edge-supported Microservice-based Resource Discovery for Mist Computing," 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 2020, pp. 462-468.
89. A. Rindos and Y. Wang, "Dew Computing: The Complementary Piece of Cloud Computing," 2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom) (BDCloud-SocialCom-SustainCom), Atlanta, GA, USA, 2016, pp. 15-20.
90. Z. Sojaat and K. Skalaa, "The dawn of Dew: Dew Computing for advanced living environment," 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2017, pp. 347-352.
91. M. Maksimović, "The role of Osmotic computing in Internet of Things," 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2018, pp. 1-4.
92. M. Villari, M. Fazio, S. Dustdar, O. Rana and R. Ranjan, "Osmotic Computing: A New Paradigm for Edge/Cloud Integration," in IEEE Cloud Computing, vol. 3, no. 6, pp. 76-83, November-December 2016.
93. M. L. F. Sindjoung, M. Velempini and A. B. Bomgni, "A MEC architecture for a better quality of service in an Autonomous Vehicular Network," Computer Networks, vol. 219, December 2022.
94. J. Nakazato, M. Nakamura, Y. Tao, G. K. Tran and K. Sakaguchi, "Benefits of MEC in 5G Cellular Networks from Telecom Operator's View Points," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-7.
95. ETSI. Network Functions Virtualisation (NFV). [Online]. Available: https://www.etsi.org/technologies/nfv?highlight=ytoxontpoja7czozoijuznyio30=. Accessed: February 2023.
96. C. B. Canto, P. J. Roig, S. Filiposka, S. A. Carrasco and K. Gilly, "Challenges of Implementing NFV-based Multi-Access Edge Computing Environments," 2021 29th Telecommunications Forum (TELFOR), Belgrade, Serbia, 2021, pp. 1-4.
97. ETSI. ETSI Multi-access Edge Computing group publishes white paper on role for 5G. June 2018. [Online]. Available: https://www.etsi.org/newsroom/press-releases/1314-2018-06-press-etsi-multi-access-edge-computing-group-publishes-white-paper-on-role-for-5g. Accessed: February 2023.
98. ETSI. ETSI GS MEC 003 V2.1.1 (2019-01). 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/mec/001_099/003/02.01.01_60/gs_mec003v020101p.pdf. Accessed: February 2023.
99. P. Cruz, N. Achir and A. C. Viana, "On the Edge of the Deployment: A Survey on Multi-access Edge Computing," ACM Computing Surveys, vol. 55, no. 5, pp. 1–34, December 2022.
100. S. Seng, X. Li, C. Luo, H. Ji and H. Zhang, "A D2D-Assisted MEC Computation Offloading in the Blockchain-Based Framework for UDNs," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6.
101. F. Giust, X. Costa-Perez and A. Reznik, "Multi-Access Edge Computing: An Overview of ETSI MEC ISG," IEEE Future Networks. IEEE 5G Tech Focus: vol. 1, no. 4, December 2017.
102. M. C. Filippou et al., "Multi-Access Edge Computing: A Comparative Analysis of 5G System Deployments and Service Consumption Locality Variants," in IEEE Communications Standards Magazine, vol. 4, no. 2, pp. 32-39, June 2020.
103. C. Parada, F. Fontes, C. Marques, V. Cunha and C. Leitão, "Multi-Access Edge Computing: A 5G Technology," 2018 European Conference on Networks and Communications (EuCNC), Ljubljana, Slovenia, 2018.
104. H. Rahimi, Y. Picaud, K. D. Singh, G. Madhusudan, S. Costanzo and O. Boissier, "Design and Simulation of a Hybrid Architecture for Edge Computing in 5G and Beyond," in IEEE Transactions on Computers, vol. 70, no. 8, pp. 1213-1224, August 2021.
105. V. Passas, N. Makris, C. Nanis and T. Korakis, "V2MEC: Low-Latency MEC for Vehicular Networks in 5G Disaggregated Architectures," 2021 IEEE Wireless Communications and Networking Conference (WCNC), Nanjing, China, 2021, pp. 1-6.
106. 5G Coral. ETSI MEC meeting in UC3M. November 2018. [Online]. Available: https://euprojects.netcom.it.uc3m.es/5g-coral/etsi-mec-meeting-in-uc3m/. Accessed: February 2023.
107. 3GPP. 3GPP TS 23.501. 2017. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/. Accessed: February 2023.
108. J. Lu, L. Xiao, Z. Tian, M. Zhao and W. Wang, "5G Enhanced Service-based Core Design," 2019 28th Wireless and Optical Communications Conference (WOCC), Beijing, China, 2019, pp. 1-5.
109. L. Xia, M. Zhao and Z. Tian, "5G Service Based Core Network Design," 2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW), Marrakech, Morocco, 2019, pp. 1-6.
110. X. Wang et al., "Holistic service-based architecture for space-air-ground integrated network for 5G-advanced and beyond," in China Communications, vol. 19, no. 1, pp. 14-28, January 2022.
111. T. Li, L. Zhao, R. Duan and H. Tian, "SBA-Based Mobile Edge Computing," 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 2019, pp. 1-6.
112. Y. Wang, L. Zhao, H. Tu, G. Zhou and Q. Yin, "Design and Implementation of Endogenous Intelligence-based Multi-Access Edge Computing," 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Kyoto, Japan, 2022, pp. 515-521.
113. W. Li and X. Wan, "An Analysis and Comparison for Public Cloud Technology and Market Development Trend in China," 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Shanghai, China, 2018, pp. 200-205.
114. X. Wang, M. Lu and Y. Wang, "Workload Optimization and Energy Consumption Reduction Strategy of Private Cloud in Manufacturing Industry," 2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2020, pp. 440-444.
115. P. Xu, J. Su and Z. Zhang, "Distributed Hybrid Cloud Management Platform Based on Rule Engine," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2018, pp. 836-839.

116. R. Baig et al., "Community Clouds at the Edge Deployed in Guifi.net," 2015 IEEE 4th International Conference on Cloud Networking (CloudNet), Niagara Falls, ON, Canada, 2015, pp. 213-215.
117. Chengtong Lv, Qing Li, Zhou Lei, Junjie Peng, Wu Zhang and Tingting Wang, "PaaS: A revolution for information technology platforms," 2010 International Conference on Educational and Network Technology, Qinhuangdao, 2010, pp. 346-349.
118. S. Kahvazadeh, H. Khalili, R. N. Silab, B. Bakhshi and J. Mangues-Bafalluy, "Vertical-oriented 5G platform-as-a-service: user-generated content case study," 2022 IEEE Future Networks World Forum (FNWF), Montreal, QC, Canada, 2022, pp. 706-711.
119. H. Castro, M. Villamizar, O. Garcés, J. Pérez, R. Caliz and P. F. P. Arteaga, "Facilitating the Execution of HPC Workloads in Colombia through the Integration of a Private IaaS and a Scientific PaaS/SaaS Marketplace," 2016 16th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), Cartagena, Colombia, 2016, pp. 693-700.
120. Z. Liumei, W. Yichuan, Z. Lei and J. Wenjiang, "Towards Energy Efficient Cloud: An Optimized Ant Colony Model for Virtual Machine Placement," in Journal of Communications and Information Networks, vol. 1, no. 4, pp. 116-132, December 2016.
121. W. Li, Q. Fan, W. Cui, F. Dang, X. Zhang and C. Dai, "Dynamic Virtual Machine Consolidation Algorithm Based on Balancing Energy Consumption and Quality of Service," in IEEE Access, vol. 10, pp. 80958-80975, 2022.
122. C. Pahl, A. Brogi, J. Soldani and P. Jamshidi, "Cloud Container Technologies: A State-of-the-Art Review," in IEEE Transactions on Cloud Computing, vol. 7, no. 3, pp. 677-692, July-September 2019.
123. T. Jin, W. Zheng, X. Wen, X. Chen and L. Wang, "Optimization of Computation Resource for Container-Based Multi-MEC Collaboration System," 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Istanbul, Turkey, 2019, pp. 1-7.
124. F. Barbarulo, C. Puliafito, A. Virdis and E. Mingozzi, "Enabling Application Relocation in ETSI MEC: A Container-Migration Approach," 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Kyoto, Japan, 2022, pp. 1-6.
125. D. Reis, B. Piedade, F. F. Correia, J. P. Dias and A. Aguiar, "Developing Docker and Docker-Compose Specifications: A Developers' Survey," in IEEE Access, vol. 10, pp. 2318-2329, 2022.
126. N. Xue, H. Haugerud and A. Yazidi, "On automated cloud bursting and hybrid cloud setups using Apache Mesos," 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), Rabat, Morocco, 2017, pp. 1-8.
127. R. Botez, C. -M. Iurian, I. -A. Ivanciu and V. Dobrota, "Deploying a Dockerized Application With Kubernetes on Google Cloud Platform," 2020 13th International Conference on Communications (COMM), Bucharest, Romania, 2020, pp. 471-476.
128. A. Lingayat, R. R. Badre and A. Kumar Gupta, "Performance Evaluation for Deploying Docker Containers On Baremetal and Virtual Machine," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2018, pp. 1019-1023.
129. A. Pereira Ferreira and R. Sinnott, "A Performance Evaluation of Containers Running on Managed Kubernetes Services," 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Sydney, NSW, Australia, 2019, pp. 199-208.
130. T. Goethals, F. De Turck and B. Volckaert, "Extending Kubernetes Clusters to Low-Resource Edge Devices Using Virtual Kubelets," in IEEE Transactions on Cloud Computing, vol. 10, no. 4, pp. 2623-2636, October-December 2022.
131. L. Phan and K. Liu, "OpenStack Network Acceleration Scheme for Datacenter Intelligent Applications," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2018, pp. 962-965.
132. A. J. Gonzalez, G. Nencioni, A. Kamisiński, B. E. Helvik and P. E. Heegaard, "Dependability of the NFV Orchestrator: State of the Art and Research Challenges," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3307-3329, Fourthquarter 2018.
133. W. -L. Chin, H. -A. Ko, N. -W. Chen, P. -W. Chen and T. Jiang, "Securing NFV/SDN IoT Using Vnfs Over a Compute-Intensive Hardware Resource in NFVI," in IEEE Network.
134. D. Breitgand, V. Eisenberg, N. Naaman, N. Rozenbaum and A. Weit, "Toward True Cloud Native NFV MANO," 2021 12th International Conference on Network of the Future (NoF), Coimbra, Portugal, 2021, pp. 1-5.
135. H. -M. Chen, Y. -F. Lu, S. -Y. Chen, C. -J. Chang and Z. -X. Zheng, "Design of an NFV MANO Architecture for 5G Private Network with 5G CN Cloud-Edge Collaborative Mechanism," 2022 8th International Conference on Applied System Innovation (ICASI), Nantou, Taiwan, 2022, pp. 92-95.
136. H. D. Chantre and N. L. Saldanha da Fonseca, "The Location Problem for the Provisioning of Protected Slices in NFV-Based MEC Infrastructure," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 7, pp. 1505-1514, July 2020.
137. I. Sarrigiannis, E. Kartsakli, K. Ramantas, A. Antonopoulos and C. Verikoukis, "Application and Network VNF migration in a MEC-enabled 5G Architecture," 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, Spain, 2018, pp. 1-6.
138. I. Sarrigiannis, K. Ramantas, E. Kartsakli, P. -V. Mekikis, A. Antonopoulos and C. Verikoukis, "Online VNF Lifecycle Management in an MEC-Enabled 5G IoT Architecture," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4183-4194, May 2020.
139. Z. Lv and W. Xiu, "Interaction of Edge-Cloud Computing Based on SDN and NFV for Next Generation IoT," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 5706-5712, July 2020.
140. N. Kiran, X. Liu, S. Wang and C. Yin, "VNF Placement and Resource Allocation in SDN/NFV-Enabled MEC Networks," 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Seoul, Korea (South), 2020, pp. 1-6.
141. S. D. A. Shah, M. A. Gregory, S. Li and R. D. R. Fontes, "SDN Enhanced Multi-Access Edge Computing (MEC) for E2E Mobility and QoS Management," in IEEE Access, vol. 8, pp. 77459-77469, 2020.
142. Y. Wu, H. -N. Dai, H. Wang, Z. Xiong and S. Guo, "A Survey of Intelligent Network Slicing Management for Industrial IoT: Integrated Approaches for Smart Transportation, Smart Energy, and Smart Factory," in IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 1175-1211, Secondquarter 2022.
143. Ramneek et al., "Multi-access Edge Computing in 5G Network Slicing: Opportunities and Challenges," 2019 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2019, pp. 30-32.

144. A. Cárdenas and D. Fernández, "Network Slice Lifecycle Management Model for NFV-based 5G Virtual Mobile Network Operators," 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Leganes, Spain, 2020, pp. 120-125.
145. S. Wijethilaka and M. Liyanage, "Survey on Network Slicing for Internet of Things Realization in 5G Networks," in IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 957-994, Secondquarter 2021.
146. J. Mei, X. Wang and K. Zheng, "Intelligent Network Slicing for V2X Services Toward 5G," in IEEE Network, vol. 33, no. 6, pp. 196-204, November-December 2019.
147. G. Gür, P. Porambage and M. Liyanage, "Convergence of ICN and MEC for 5G: Opportunities and Challenges," in IEEE Communications Standards Magazine, vol. 4, no. 4, pp. 64-71, December 2020.
148. M. Rayani, R. H. Glitho and H. Elbiaze, "ETSI Multi-Access Edge Computing for Dynamic Adaptive Streaming in Information Centric Networks," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan, 2020, pp. 1-6.
149. Alcardo Barakabitze; Andrew Hines, "Management of Multimedia Services in Emerging Architectures Using Big Data Analytics: MEC, ICN, and Fog/Cloud computing," in Multimedia Streaming in SDN/NFV and 5G Networks: Machine Learning for Managing Big Data Streaming, IEEE, 2023, pp.119-132.
150. J. Li, W. Liang and Y. Ma, "Robust Service Provisioning With Service Function Chain Requirements in Mobile Edge Computing," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 2138-2153, June 2021.
151. M. M. Erbati and G. Schiele, "Application- and reliability-aware service function chaining to support low-latency applications in an NFV-enabled network," 2021 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Heraklion, Greece, 2021, pp. 120-123.
152. R. Behravesh, D. Harutyunyan, E. Coronado and R. Riggio, "Time-Sensitive Mobile User Association and SFC Placement in MEC-Enabled 5G Networks," in IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3006-3020, September 2021.
153. M. Wang, B. Cheng, W. Feng and J. Chen, "An Efficient Service Function Chain Placement Algorithm in a MEC-NFV Environment," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6.
154. Y. -T. Chen and W. Liao, "Mobility-Aware Service Function Chaining in 5G Wireless Networks with Mobile Edge Computing," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6.
155. S. Forti et al., “Probabilistic QoS-aware Placement of VNF Chains at the Edge,” Theory and Practice of Logic Programming (Cambridge University Press), vol. 22, no. 1, February 2021.
156. B. Feng, H. Zhou, G. Li, Y. Zhang, K. Sood and S. Yu, "Enabling Machine Learning with Service Function Chaining for Security Enhancement at 5G Edges," in IEEE Network, vol. 35, no. 5, pp. 196-201, September/October 2021.
157. G. Li et al., “Fuzzy Theory Based Security Service Chaining for Sustainable Mobile-Edge Computing,” Mobile Information Systems, vol. 2017, Feb 2017.
158. M. Masoumi et al., "Dynamic Online VNF Placement with Different Protection Schemes in a MEC Environment," 2022 32nd International Telecommunication Networks and Applications Conference (ITNAC), Wellington, New Zealand, 2022, pp. 1-6.
159. J. Bai, X. Chang, F. Machida, L. Jiang, Z. Han and K. S. Trivedi, "Impact of Service Function Aging on the Dependability for MEC Service Function Chain," in IEEE Transactions on Dependable and Secure Computing.
160. C. -L. I, J. Huang, R. Duan, C. Cui, J. Jiang and L. Li, "Recent Progress on C-RAN Centralization and Cloudification," in IEEE Access, vol. 2, pp. 1030-1039, 2014.
161. Y. Zeng, A. Al-Quzweeni, T. E. H. El-Gorashi and J. M. H. Elmirghani, "Energy Efficient Virtualization Framework for 5G F-RAN," 2019 21st International Conference on Transparent Optical Networks (ICTON), Angers, France, 2019, pp. 1-4.
162. Y. Xu, G. Gui, H. Gacanin and F. Adachi, "A Survey on Resource Allocation for 5G Heterogeneous Networks: Current Research, Future Trends, and Challenges," in IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 668-695, Secondquarter 2021.
163. R. S. Alhumaima, M. Khan and H. S. Al-Raweshidy, "Modelling the energy efficiency of Heterogeneous Cloud Radio Access Networks," 2015 International Conference on Emerging Technologies (ICET), Peshawar, Pakistan, 2015, pp. 1-6.
164. T. Kim and J. M. Chang, "Profitable and Energy-Efficient Resource Optimization for Heterogeneous Cloud-Based Radio Access Networks," in IEEE Access, vol. 7, pp. 34719-34737, 2019.
165. N. Makris, V. Passas, C. Nanis and T. Korakis, "On Minimizing Service Access Latency: Employing MEC on the Fronthaul of Heterogeneous 5G Architectures," 2019 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), Paris, France, 2019, pp. 1-6.
166. M. M. Abdelhakam and M. M. Elmesalawy, "Joint Beamforming Design and BBU Computational Resources Allocation in Heterogeneous C-RAN with QoS Guarantee," 2018 International Symposium on Networks, Computers and Communications (ISNCC), Rome, Italy, 2018, pp. 1-6.
167. M. Elhattab, M. Kamel and W. Hamouda, "Edge-Aware Remote Radio Heads Cooperation for Interference Mitigation in Heterogeneous C-RAN," in IEEE Transactions on Vehicular Technology, vol. 70, no. 11, pp. 12142-12157, November 2021.
168. L. Wang, K. -K. Wong, M. Elkashlan, A. Nallanathan and S. Lambotharan, "Secrecy and Energy Efficiency in Massive MIMO Aided Heterogeneous C-RAN: A New Look at Interference," in IEEE Journal of Selected Topics in Signal Processing, vol. 10, no. 8, pp. 1375-1389, December 2016.
169. M. Mehrabi et al., “Mobility- and Energy-Aware Cooperative Edge Offloading for Dependent Computation Tasks,” Network, vol. 1, no. 2, September 2021.
170. J. Feng, L. Zhao, J. Du, X. Chu and F. R. Yu, "Computation Offloading and Resource Allocation in D2D-Enabled Mobile Edge Computing," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 1-6.
171. H. B. Mahmoodi, J. Kaleva, S. P. Shariatpanahi and A. Tölli, "D2D Assisted Multi-Antenna Coded Caching," in IEEE Access, vol. 11, pp. 16271-16287, 2023.
172. E. Baccour et al., “Collaborative hierarchical caching and transcoding in edge network with CE-D2D communication,” Journal of Network and Computer Applications, vol. 172, December 2020.

173. M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma and J. Ott, "Security and Privacy in Device-to-Device (D2D) Communication: A Review," in IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 1054-1079, Secondquarter 2017.
174. L. F. Del Carpio, A. A. Dowhuszko, O. Tirkkonen and G. Wu, "Simple Clustering Methods for Multi-Hop Cooperative Device-to-Device Communication," 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, UK, 2015, pp. 1-6.
175. L. P. Bopape, B. Nleya and P. Khumalo, "A Privacy and Security Preservation Framework for D2D Communication Based Smart Grid Services," 2020 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 2020, pp. 1-6.
176. K. W. Choi and Z. Han, "Device-to-Device Discovery for Proximity-Based Service in LTE-Advanced System," in IEEE Journal on Selected Areas in Communications, vol. 33, no. 1, pp. 55-66, January 2015.
177. D. Griffith, A. Ben Mosbah and R. Rouil, "Group discovery time in device-to-device (D2D) proximity services (ProSe) networks," IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, Atlanta, GA, USA, 2017, pp. 1-9.
178. L. Liang, G. Y. Li and W. Xu, "Resource Allocation for D2D-Enabled Vehicular Communications," in IEEE Transactions on Communications, vol. 65, no. 7, pp. 3186-3197, July 2017.
179. Z. Liu, Y. Xie, K. Y. Chan, K. Ma and X. Guan, "Chance-Constrained Optimization in D2D-Based Vehicular Communication Network," in IEEE Transactions on Vehicular Technology, vol. 68, no. 5, pp. 5045-5058, May 2019.
180. Y. He, J. Ren, G. Yu and Y. Cai, "D2D Communications Meet Mobile Edge Computing for Enhanced Computation Capacity in Cellular Networks," in IEEE Transactions on Wireless Communications, vol. 18, no. 3, pp. 1750-1763, March 2019.
181. M. Wang, W. Fu, X. He, S. Hao and X. Wu, "A Survey on Large-Scale Machine Learning," in IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 6, pp. 2574-2594, June 2022.
182. ITU-T. FG-NET2030 – Focus Group on Technologies for Network 2030. Network 2030 Architecture Framework. June 2020. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Network_2030_Architecture-framework.pdf. Accessed: February 2023.
183. L. von Rueden et al., "Informed Machine Learning – A Taxonomy and Survey of Integrating Prior Knowledge into Learning Systems," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 1, pp. 614-633, January 2023.
184. F. Tang, B. Mao, Y. Kawamoto and N. Kato, "Survey on Machine Learning for Intelligent End-to-End Communication Toward 6G: From Network Access, Routing to Traffic Control and Streaming Adaption," in IEEE Communications Surveys & Tutorials, vol. 23, no. 3, pp. 1578-1598, thirdquarter 2021.
185. M. Vaezi et al., "Cellular, Wide-Area, and Non-Terrestrial IoT: A Survey on 5G Advances and the Road Toward 6G," in IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 1117-1174, Secondquarter 2022.
186. M. M. Adam, L. Zhao, K. Wang and Z. Han, "Beyond 5G networks: Integration of communication, computing, caching, and control," in China Communications.
187. Z. M. Fadlullah, B. Mao and N. Kato, "Balancing QoS and Security in the Edge: Existing Practices, Challenges, and 6G Opportunities With Machine Learning," in IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2419-2448, Fourthquarter 2022.
188. H. Xue, B. Huang, M. Qin, H. Zhou and H. Yang, "Edge Computing for Internet of Things: A Survey," 2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Rhodes, Greece, 2020, pp. 755-760.
189. Q. Zhou et al., "On-Device Learning Systems for Edge Intelligence: A Software and Hardware Synergy Perspective," in IEEE Internet of Things Journal, vol. 8, no. 15, pp. 11916-11934, August 2021.
190. A. Ndikumana et al., "Joint Communication, Computation, Caching, and Control in Big Data Multi-Access Edge Computing," in IEEE Transactions on Mobile Computing, vol. 19, no. 6, pp. 1359-1374, June 2020.
191. Z. Chen, Q. He, L. Liu, D. Lan, H. -M. Chung and Z. Mao, "An Artificial Intelligence Perspective on Mobile Edge Computing," 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), Tianjin, China, 2019, pp. 100-106.
192. Y. Sun, H. Ochiai and H. Esaki, "Decentralized Deep Learning for Multi-Access Edge Computing: A Survey on Communication Efficiency and Trustworthiness," in IEEE Transactions on Artificial Intelligence, vol. 3, no. 6, pp. 963-972, December 2022.
193. K. Jiang, C. Sun, H. Zhou, X. Li, M. Dong and V. C. M. Leung, "Intelligence-Empowered Mobile Edge Computing: Framework, Issues, Implementation, and Outlook," in IEEE Network, vol. 35, no. 5, pp. 74-82, September/October 2021.
194. H. Tang, H. Wu, G. Qu and R. Li, "Double Deep Q-Network based Dynamic Framing Offloading in Vehicular Edge Computing," in IEEE Transactions on Network Science and Engineering.
195. A. Islam et al., “A Survey on Task Offloading in Multi-access Edge Computing,” Journal of Systems Architecture, vol. 118, September 2021.
196. B. Li and R. Wu, “Joint Perception Data Caching and Computation Offloading in MEC-Enabled Vehicular Networks,” Computer Communications, vol. 199, pp. 139-152, February 2023.
197. H. Ke, J. Wang, L. Deng, Y. Ge and H. Wang, "Deep Reinforcement Learning-Based Adaptive Computation Offloading for MEC in Heterogeneous Vehicular Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 7, pp. 7916-7929, July 2020.
198. F. Tusa and S. Clayman, “The Impact of Encoding and Transport for Massive Real-time IoT Data on Edge Resource Consumption,” Journal of Grid Computing, vol. 19, July 2021.
199. S. Abdelwahab, B. Hamdaoui, M. Guizani and T. Znati, "Replisom: Disciplined Tiny Memory Replication for Massive IoT Devices in LTE Edge Cloud," in IEEE Internet of Things Journal, vol. 3, no. 3, pp. 327-338, June 2016.
200. Z. Ning, P. Dong, X. Kong and F. Xia, "A Cooperative Partial Computation Offloading Scheme for Mobile Edge Computing Enabled Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4804-4814, June 2019.
201. H. –C. Hu and P. –C. Wang, “Computation Offloading Game for Multi-Channel Wireless Sensor Networks,” Sensors, vol. 22, no. 22, November 2022.
202. A. Qin, C. Cai, Q. Wang, Y. Ni and H. Zhu, "Game Theoretical Multi-user Computation Offloading for Mobile-Edge Cloud Computing," 2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), San Jose, CA, USA, 2019, pp. 328-332.

203. C. M. S. Magurawalage et al., “Energy-efficient and network-aware offloading algorithm for mobile cloud computing,” Computer Networks, vol. 74, Part B, pp. 22-33, December 2014.
204. Y. Wu, "Cloud-Edge Orchestration for the Internet of Things: Architecture and AI-Powered Data Processing," in IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12792-12805, August 2021.
205. H. Wu, K. Wolter, P. Jiao, Y. Deng, Y. Zhao and M. Xu, "EEDTO: An Energy-Efficient Dynamic Task Offloading Algorithm for Blockchain-Enabled IoT-Edge-Cloud Orchestrated Computing," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2163-2176, February 2021.
206. M. Xue, H. Wu, R. Li, M. Xu and P. Jiao, "EosDNN: An Efficient Offloading Scheme for DNN Inference Acceleration in Local-Edge-Cloud Collaborative Environments," in IEEE Transactions on Green Communications and Networking, vol. 6, no. 1, pp. 248-264, March 2022.
207. M. Xue, H. Wu, G. Peng and K. Wolter, "DDPQN: An Efficient DNN Offloading Strategy in Local-Edge-Cloud Collaborative Environments," in IEEE Transactions on Services Computing, vol. 15, no. 2, pp. 640-655, March-April 2022.
208. Z. Hu et al., "An Efficient Online Computation Offloading Approach for Large-Scale Mobile Edge Computing via Deep Reinforcement Learning," in IEEE Transactions on Services Computing, vol. 15, no. 2, pp. 669-683, March-April 2022.
209. Y. Xu, B. Gu, R. Q. Hu, D. Li and H. Zhang, "Joint Computation Offloading and Radio Resource Allocation in MEC-Based Wireless-Powered Backscatter Communication Networks," in IEEE Transactions on Vehicular Technology, vol. 70, no. 6, pp. 6200-6205, June 2021.
210. F. Guo, H. Zhang, H. Ji, X. Li and V. C. M. Leung, "Joint Trajectory and Computation Offloading Optimization for UAV-assisted MEC with NOMA," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 2019, pp. 1-6.
211. Y. He, J. Ren, G. Yu and Y. Cai, "Joint Computation Offloading and Resource Allocation in D2D Enabled MEC Networks," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6.
212. J. Wang et al., “Joint Computation Offloading and Resource Allocation for MEC-Enabled IoT Systems With Imperfect CSI,” IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3462 – 3475, March 2021.
213. F. Guo, H. Zhang, H. Ji, X. Li and V. C. M. Leung, "Energy Efficient Computation Offloading for Multi-Access MEC Enabled Small Cell Networks," 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 2018, pp. 1-6.
214. P. -D. Nguyen, V. N. Ha and L. B. Le, "Computation Offloading and Resource Allocation for Backhaul Limited Cooperative MEC Systems," 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 2019, pp. 1-6.
215. W. Shu and Y. Li, “Joint Offloading Strategy Based on Quantum Particle Swarm Optimization for MEC-Enabled Vehicular Networks,” Digital Communications and Networks, vol. 9, no. 1, pp. 56-66, February 2023.
216. H. Kang, M. Li, S. Fan and W. Cai, "Combinatorial Auction-enabled Dependency-Aware Offloading Strategy in Mobile Edge Computing," 2023 IEEE Wireless Communications and Networking Conference (WCNC), Glasgow, United Kingdom, 2023, pp. 1-6.
217. C. Su, F. Ye, T. Liu, Y. Tian and Z. Han, "Computation Offloading in Hierarchical Multi-Access Edge Computing Based on Contract Theory and Bayesian Matching Game," in IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 13686-13701, November 2020.
218. X. Yang, H. Luo, Y. Sun, J. Zou and M. Guizani, "Coalitional Game-Based Cooperative Computation Offloading in MEC for Reusable Tasks," in IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12968-12982, August 2021.
219. J. Chen, Q. Ding and X. Yang, “Non-Cooperative Game Algorithms for Computation Offloading in Mobile Edge Computing Environments,” Journal of Parallel and Distributed Computing, vol. 172, pp. 18-31, February 2023.
220. J. Li, H. Gao, T. Lv and Y. Lu, "Deep reinforcement learning based computation offloading and resource allocation for MEC," 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 2018, pp. 1-6.
221. N. Waqar, S. A. Hassan, A. Mahmood, K. Dev, D. -T. Do and M. Gidlund, "Computation Offloading and Resource Allocation in MEC-Enabled Integrated Aerial-Terrestrial Vehicular Networks: A Reinforcement Learning Approach," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 11, pp. 21478-21491, November 2022.
222. Q. Yang et al., “Computation Offloading for Fast CNN Inference in Edge Computing,” RACS '19: Proceedings of the Conference on Research in Adaptive and Convergent Systems, September 2019, pp. 101–106.
223. X. Zhang et al., “BiLSTM-based Federated Learning Computation Offloading and Resource Allocation Algorithm in MEC,” ACM Transactions on Sensor Networks, vol. 19, no. 3, pp. 1–20, March 2023.
224. L. Huang, L. Zhang, S. Yang, L. P. Qian and Y. Wu, "Meta-Learning Based Dynamic Computation Task Offloading for Mobile Edge Computing Networks," in IEEE Communications Letters, vol. 25, no. 5, pp. 1568-1572, May 2021.
225. M. D. Hossain, T. Sultana, M. A. Hossain and E. -N. Huh, "Edge Orchestration Based Computation Peer Offloading in MEC-Enabled Networks: A Fuzzy Logic Approach," 2021 15th International Conference on Ubiquitous Information Management and Communication (IMCOM), Seoul, Korea (South), 2021, pp. 1-7.
226. L. Nadeem et al., "Integration of D2D, Network Slicing, and MEC in 5G Cellular Networks: Survey and Challenges," in IEEE Access, vol. 9, pp. 37590-37612, 2021.
227. Q. Hu, C. Wu, X. Zhao, X. Chen, Y. Ji and T. Yoshinaga, "Vehicular Multi-Access Edge Computing With Licensed Sub-6 GHz, IEEE 802.11p and mmWave," in IEEE Access, vol. 6, pp. 1995-2004, 2018.
228. J. Liu, G. Shou, Y. Liu, Y. Hu and Z. Guo, "Performance Evaluation of Integrated Multi-Access Edge Computing and Fiber-Wireless Access Networks," in IEEE Access, vol. 6, pp. 30269-30279, 2018.
229. H. Peng, Q. Ye and X. Shen, "Spectrum Management for Multi-Access Edge Computing in Autonomous Vehicular Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 7, pp. 3001-3012, July 2020.
230. Z. Song, Y. Hao, Y. Liu and X. Sun, "Energy-Efficient Multiaccess Edge Computing for Terrestrial-Satellite Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 18, pp. 14202-14218, September 2021.
231. M. Li, X. Zhou, T. Qiu, Q. Zhao and K. Li, "Multi-Relay Assisted Computation Offloading for Multi-Access Edge Computing Systems With Energy Harvesting," in IEEE Transactions on Vehicular Technology, vol. 70, no. 10, pp. 10941-10956, October 2021.

232. M. Liu, Y. Teng, K. Cheng, Y. Man and B. Zhang, "Joint Content Caching and Delivery Policy for Heterogeneous Cellular Networks," 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Bologna, Italy, 2018, pp. 1-5.
233. C. Fang et al., "Cache-Assisted Content Delivery in Wireless Networks: A New Game Theoretic Model," in IEEE Systems Journal, vol. 15, no. 2, pp. 2653-2664, June 2021.
234. S. Yang, L. Jiao, R. Yahyapour and J. Cao, "Online Orchestration of Collaborative Caching for Multi-Bitrate Videos in Edge Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 33, no. 12, pp. 4207-4220, December 2022.
235. E. E. Ugwuanyi, S. Ghosh, M. Iqbal, T. Dagiuklas, S. Mumtaz and A. Al-Dulaimi, "Co-Operative and Hybrid Replacement Caching for Multi-Access Mobile Edge Computing," 2019 European Conference on Networks and Communications (EuCNC), Valencia, Spain, 2019, pp. 394-399.
236. S. Woo et al., “Comparison of caching strategies in modern cellular backhaul networks,” 11th annual international conference on Mobile systems, applications, and services, June 2013, pp. 319–332.
237. A. C. B. L. Monção, S. L. Correa, A. C. Viana and K. V. Cardoso, "Combining Resource-Aware Recommendation and Caching in the Era of MEC for Improving the Experience of Video Streaming Users," in IEEE Transactions on Services Computing, 2022.
238. X. Wei et al., “Wireless Edge Caching Based on Content Similarity in Dynamic Environments,” Journal of Systems Architecture, vol. 115, May 2021.
239. S. Zhong, S. Guo, H. Yu and Q. Wang, “Cooperative Service Caching and Computation Offloading in Multi-Access Edge Computing,” Computer Networks, vol. 189, April 2021.
240. E. E. Ugwuanyi, M. Iqbal and T. Dagiuklas, "A Novel Predictive-Collaborative-Replacement (PCR) Intelligent Caching Scheme for Multi-Access Edge Computing," in IEEE Access, vol. 9, pp. 37103-37115, 2021.
241. G. Tefera, K. She, M. Shelke and A. Ahmed, “Decentralized Adaptive Resource-Aware Computation Offloading & Caching for Multi-Access Edge Computing Networks,” Sustainable Computing: Informatics and Systems, vol. 30, June 2021.
242. S. Kumar, S. V. Doddala, A. A. Franklin and J. Jin, “RAN-Aware Adaptive Video Caching in Multi-Access Edge Computing Networks,” Journal of Network and Computer Applications, vol. 168, October 2020.
243. C. Ding, A. Zhou, Y. Liu and S. Wang, “ECDU: An Edge Content Delivery And Update Framework In Mobile Edge Computing,” EURASIP Journal on Wireless Communications and Networking, vol. 268, December 2019.
244. F. M. Caceres, K. Sithamparanathan and S. Sun, "Theoretical Analysis of Hybrid SIC Success Probability Under Rayleigh Channel for Uplink CR-NOMA," in IEEE Transactions on Vehicular Technology, vol. 71, no. 10, pp. 10584-10599, October 2022.
245. K. Chung, "Correlated Superposition Coding: Lossless Two-User NOMA Implementation Without SIC Under User-Fairness," in IEEE Wireless Communications Letters, vol. 10, no. 9, pp. 1999-2003, September 2021.
246. L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen and L. Hanzo, "A Survey of Non-Orthogonal Multiple Access for 5G," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2294-2323, thirdquarter 2018.
247. I. Budhiraja et al., "A Systematic Review on NOMA Variants for 5G and Beyond," in IEEE Access, vol. 9, pp. 85573-85644, 2021.
248. D. -T. Do, M. -S. V. Nguyen, F. Jameel, R. Jäntti and I. S. Ansari, "Performance Evaluation of Relay-Aided CR-NOMA for Beyond 5G Communications," in IEEE Access, vol. 8, pp. 134838-134855, 2020.
249. M. Rebhi, K. Hassan, K. Raoof and P. Chargé, "Sparse Code Multiple Access: Potentials and Challenges," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1205-1238, 2021.
250. X. Qi, M. Peng and H. Zhang, "Joint mmWave Beamforming and Resource Allocation in NOMA-MEC Network for Internet of Things," in IEEE Transactions on Vehicular Technology.
251. S. S. Yılmaz and B. Özbek, "Massive MIMO-NOMA Based MEC in Task Offloading for Delay Minimization," in IEEE Access, vol. 11, pp. 162-170, 2023.
252. L. P. Qian, B. Shi, Y. Wu, B. Sun and D. H. K. Tsang, "NOMA-Enabled Mobile Edge Computing for Internet of Things via Joint Communication and Computation Resource Allocations," in IEEE Internet of Things Journal, vol. 7, no. 1, pp. 718-733, January 2020.
253. G. Zheng, C. Xu, H. Long and X. Zhao, "MEC in NOMA-HetNets: A Joint Task Offloading and Resource Allocation Approach," 2021 IEEE Wireless Communications and Networking Conference (WCNC), Nanjing, China, 2021, pp. 1-6.
254. Q. Cheng et al., "Efficient Resource Allocation for NOMA-MEC System in Ultra-Dense Network: A Mean Field Game Approach," 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 2020, pp. 1-6.
255. Z. Yang, Y. Liu, Y. Chen and N. Al-Dhahir, "Cache-Aided NOMA Mobile Edge Computing: A Reinforcement Learning Approach," in IEEE Transactions on Wireless Communications, vol. 19, no. 10, pp. 6899-6915, October 2020.
256. J. Du, N. Xue, D. Zhai, H. Cao, J. Feng and G. Lu, "Energy-efficient User Clustering and Resource Management for NOMA Based MEC Systems," 2020 IEEE Globecom Workshops (GC Wkshps, Taipei, Taiwan, 2020, pp. 1-6.
257. M. Nduwayezu and J. Yun, “Latency and energy aware rate maximization in MC-NOMA-based multi-access edge computing: A two-stage deep reinforcement learning approach,” Computer Networks, vol. 207, April 2022.
258. Z. Ding, D. Xu, R. Schober and H. V. Poor, "Hybrid NOMA Offloading in Multi-User MEC Networks," in IEEE Transactions on Wireless Communications, vol. 21, no. 7, pp. 5377-5391, July 2022.
259. Y. Mao, B. Clerckx and V. O. K. Li, “Rate-splitting multiple access for downlink communication systems: bridging, generalizing, and outperforming SDMA and NOMA,” EURASIP Journal on Wireless Communications and Networking, vol. 133, May 2018.
260. A. Bansal, K. Singh, B. Clerckx, C. -P. Li and M. -S. Alouini, "Rate-Splitting Multiple Access for Intelligent Reflecting Surface Aided Multi-User Communications," in IEEE Transactions on Vehicular Technology, vol. 70, no. 9, pp. 9217-9229, September 2021.
261. A. Mishra, Y. Mao, L. Sanguinetti and B. Clerckx, "Rate-Splitting Assisted Massive Machine-Type Communications in Cell-Free Massive MIMO," in IEEE Communications Letters, vol. 26, no. 6, pp. 1358-1362, June 2022.
262. A. Kumar, F. Y. Li and J. Martinez-Bauset, "Revealing the Benefits of Rate-Splitting Multiple Access for Uplink IoT Traffic," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 111-116.

263. Z. Yang, M. Chen, W. Saad, W. Xu and M. Shikh-Bahaei, "Sum-Rate Maximization of Uplink Rate Splitting Multiple Access (RSMA) Communication," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6.
264. L. Li, K. Chai, J. Li and X. Li, "Resource Allocation for Multicarrier Rate-Splitting Multiple Access System," in IEEE Access, vol. 8, pp. 174222-174232, 2020.
265. O. Abbasi and H. Yanikomeroglu, "Rate-Splitting and NOMA-Enabled Uplink User Cooperation," 2021 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Nanjing, China, 2021.
266. G. Arora and A. Jaiswal, "Zero SIC Based Rate Splitting Multiple Access Technique," in IEEE Communications Letters, vol. 26, no. 10, pp. 2430-2434, October 2022.
267. Z. Yang, M. Chen, W. Saad and M. Shikh-Bahaei, "Optimization of Rate Allocation and Power Control for Rate Splitting Multiple Access (RSMA)," in IEEE Transactions on Communications, vol. 69, no. 9, pp. 5988-6002, September 2021.
268. H. Liu, Z. Bai, H. Lei, G. Pan, K. J. Kim and T. A. Tsiftsis, "A New Rate Splitting Strategy for Uplink CR-NOMA Systems," in IEEE Transactions on Vehicular Technology, vol. 71, no. 7, pp. 7947-7951, July 2022.
269. H. Liu, T. A. Tsiftsis, K. J. Kim, K. S. Kwak and H. V. Poor, "Rate Splitting for Uplink NOMA With Enhanced Fairness and Outage Performance," in IEEE Transactions on Wireless Communications, vol. 19, no. 7, pp. 4657-4670, July 2020.
270. Z. Yang, M. Chen, W. Saad, W. Xu and M. Shikh-Bahaei, "Sum-Rate Maximization of Uplink Rate Splitting Multiple Access (RSMA) Communication," in IEEE Transactions on Mobile Computing, vol. 21, no. 7, pp. 2596-2609, July 2022.
271. J. Zeng, T. Lv, W. Ni, R. P. Liu, N. C. Beaulieu and Y. J. Guo, "Ensuring Max–Min Fairness of UL SIMO-NOMA: A Rate Splitting Approach," in IEEE Transactions on Vehicular Technology, vol. 68, no. 11, pp. 11080-11093, November 2019.
272. E. J. D. Santos, R. D. Souza and J. L. Rebelatto, "Rate-Splitting Multiple Access for URLLC Uplink in Physical Layer Network Slicing With eMBB," in IEEE Access, vol. 9, pp. 163178-163187, 2021.
273. H. Kong et al., “Ergodic sum rate for uplink NOMA transmission in satellite-aerial-ground integrated networks,” Chinese Journal of Aeronautics, vol. 35, no. 9, pp.58-70, September 2022.
274. W. Jaafar, S. Naser, S. Muhaidat, P. C. Sofotasios and H. Yanikomeroglu, "Multiple Access in Aerial Networks: From Orthogonal and Non-Orthogonal to Rate-Splitting," in IEEE Open Journal of Vehicular Technology, vol. 1, pp. 372-392, 2020.
275. H. Kong, M. Lin, Z. Wang, J. -Y. Wang, W. -P. Zhu and J. Wang, "Combined Robust Beamforming With Uplink RSMA for Multibeam Satellite Systems," in IEEE Transactions on Vehicular Technology, vol. 71, no. 9, pp. 10167-10172, September 2022.
276. S. Khisa, M. Almekhlafi, M. Elhattab and C. Assi, "Full Duplex Cooperative Rate Splitting Multiple Access for a MISO Broadcast Channel With Two Users," in IEEE Communications Letters, vol. 26, no. 8, pp. 1913-1917, August 2022.
277. S. A. Tegos, P. D. Diamantoulakis and G. K. Karagiannidis, "On the Performance of Uplink Rate-Splitting Multiple Access," in IEEE Communications Letters, vol. 26, no. 3, pp. 523-527, March 2022.
278. X. Ou, X. Xie, H. Lu and H. Yang, "Resource Allocation in MU-MISO Rate-Splitting Multiple Access With SIC Errors for URLLC Services," in IEEE Transactions on Communications, vol. 71, no. 1, pp. 229-243, January 2023.
279. O. Abbasi and H. Yanikomeroglu, "Transmission Scheme, Detection and Power Allocation for Uplink User Cooperation With NOMA and RSMA," in IEEE Transactions on Wireless Communications, vol. 22, no. 1, pp. 471-485, January 2023.
280. Y. Xiao, S. A. Tegos, P. D. Diamantoulakis, Z. Ma and G. K. Karagiannidis, "On the Ergodic Rate of Cognitive Radio Inspired Uplink Multiple Access," in IEEE Communications Letters, vol. 27, no. 1, pp. 95-99, January 2023.
281. H. Liu, Y. Ye, Z. Bai, K. J. Kim and T. A. Tsiftsis, "Rate Splitting Multiple Access Aided Mobile Edge Computing in Cognitive Radio Networks," 2022 IEEE International Conference on Communications Workshops (ICC Workshops), Seoul, Korea, Republic of, 2022, pp. 598-603.
282. B. Li, Z. Fei and Y. Zhang, "UAV Communications for 5G and Beyond: Recent Advances and Future Trends," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2241-2263, April 2019.
283. Q. Li, L. Shi, Z. Zhang and G. Zheng, "Resource Allocation in UAV-Enabled Wireless-Powered MEC Networks With Hybrid Passive and Active Communications," in IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2574-2588, February 2023.
284. A. Sharma et al., “Communication and Networking Technologies for UAVs: A Survey,” Journal of Network and Computer Applications, vol. 168, October 2020.
285. Z. Song et al., “A Comprehensive Survey on Aerial Mobile Edge Computing: Challenges, State-of-the-Art, and Future Directions,” Computer Communications, vol. 191, pp. 233-256. July 2022.
286. N. Gao, S. Jin, X. Li and M. Matthaiou, "Aerial RIS-Assisted High Altitude Platform Communications," in IEEE Wireless Communications Letters, vol. 10, no. 10, pp. 2096-2100, October 2021.
287. W. You, C. Dong, Q. Wu, Y. Qu, Y. Wu and R. He, "Joint task scheduling, resource allocation, and UAV trajectory under clustering for FANETs," in China Communications, vol. 19, no. 1, pp. 104-118, Jan. 2022.
288. M. N. Bashir and K. Mohamad Yusof, "Green Mesh Network of UAVs: A Survey of Energy Efficient Protocols across Physical, Data Link and Network Layers," 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 2019, pp. 1-6.
289. Z. Jiang, R. Cao and S. Zhang, “Joint Optimization Strategy of Offloading in Multi-UAVs-Assisted Edge Computing Networks,” Journal of Ambient Intelligence and Humanized Computing, February 2023.
290. X. Diao, W. Yang, L. Yang and Y. Cai, "UAV-Relaying-Assisted Multi-Access Edge Computing With Multi-Antenna Base Station: Offloading and Scheduling Optimization," in IEEE Transactions on Vehicular Technology, vol. 70, no. 9, pp. 9495-9509, September 2021.
291. P. A. Apostolopoulos, G. Fragkos, E. E. Tsiropoulou and S. Papavassiliou, "Data Offloading in UAV-Assisted Multi-Access Edge Computing Systems Under Resource Uncertainty," in IEEE Transactions on Mobile Computing, vol. 22, no. 1, pp. 175-190, January 2023.
292. K. Zhang, X. Gui, D. Ren and D. Li, "Energy–Latency Tradeoff for Computation Offloading in UAV-Assisted Multiaccess Edge Computing System," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6709-6719, April 2021.

293. A. J. Williams, M. F. Torquato, I. M. Cameron, A. A. Fahmy and J. Sienz, "Survey of Energy Harvesting Technologies for Wireless Sensor Networks," in IEEE Access, vol. 9, pp. 77493-77510, 2021
294. Q. Wu, G. Y. Li, W. Chen, D. W. K. Ng and R. Schober, "An Overview of Sustainable Green 5G Networks," in IEEE Wireless Communications, vol. 24, no. 4, pp. 72-80, August 2017
295. M. Liu et al., "Biomechanical Energy Harvesting for Wearable And Mobile Devices: State-of-the-Art and Future Directions," Applied Energy, vol. 321, September 2022.
296. S. Gupta et al., "Development of a novel footwear based power harvesting system," Advances in Electrical Engineering, Electronics and Energy, vol. 3, March 2023.
297. S. Y. R. Hui, "Past, present and future trends of non-radiative wireless power transfer," in CPSS Transactions on Power Electronics and Applications, vol. 1, no. 1, pp. 83-91, December 2016.
298. Y. Li, X. Li and X. Dai, "A Simultaneous Wireless Power and Data Transmission Method for Multi-Output WPT Systems: Analysis, Design, and Experimental Verification," in IEEE Access, vol. 8, pp. 206353-206359, 2020.
299. EPC. Taiwan Technology Standards Agency Introduces AirFuel Alliance's Resonant Wireless Charging Standard. December 2016. [Online]. Available: https://epc-co.com/epc/events-and-news/news/artmid/1627/articleid/1756/taiwan-technology-standards-agency-introduces-airfuel-alliances-resonant-wireless-charging-standard--. Accessed: February 2023.
300. AirFuel. 2nd Annual Developers Forum. 2019. [Online]. Available: https://airfuel.org/developers-forum-2019-recap/. Accessed: February 2023.
301. A. Mahesh, B. Chokkalingam and L. Mihet-Popa, "Inductive Wireless Power Transfer Charging for Electric Vehicles–A Review," in IEEE Access, vol. 9, pp. 137667-137713, 2021.
302. A. Khalifeh et al., "Radio Frequency Based Wireless Charging for Unsupervised Clustered WSN: System Implementation and Experimental Evaluation," Energies, vol. 14, no. 7, March 2021.
303. Z. Hu, C. Yuan and F. Gao, "Maximizing Harvested Energy for Full-Duplex SWIPT System With Power Splitting," in IEEE Access, vol. 5, pp. 24975-24987, 2017.
304. S. Kang, H. Lee, S. Hwang and I. Lee, "Time Switching Protocol for Multi-Antenna SWIPT Systems," 2020 IEEE Wireless Communications and Networking Conference (WCNC), Seoul, Korea (South), 2020, pp. 1-6.
305. J. Jalali, A. Khalili, A. Rezaei, J. Famaey and W. Saad, "Power-efficient Antenna Switching and Beamforming Design for Multi-User SWIPT with Non-Linear Energy Harvesting," 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2023, pp. 746-751.
306. S. Mondal and J. Paramesh, "Power-Efficient Design Techniques for mm-Wave Hybrid/Digital FDD/Full-Duplex MIMO Transceivers," in IEEE Journal of Solid-State Circuits, vol. 55, no. 8, pp. 2011-2026, August 2020.
307. T. D. Ponnimbaduge Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas and J. Li, "Simultaneous Wireless Information and Power Transfer (SWIPT): Recent Advances and Future Challenges," in IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 264-302, Firstquarter 2018.
308. Y. Zhang, S. Chen, X. Li and Y. Tang, "Design of high-power static wireless power transfer via magnetic induction: An overview," in CPSS Transactions on Power Electronics and Applications, vol. 6, no. 4, pp. 281-297, December 2021.
309. Y. Liang, Y. He, J. Qiao and A. P. Hu, "Simultaneous Wireless Information and Power Transfer in 5G Mobile Networks: A Survey," 2019 Computing, Communications and IoT Applications (ComComAp), Shenzhen, China, 2019, pp. 460-465.
310. S. Ghosh, S. D. Roy and S. Kundu, "UAV Assisted SWIPT Enabled NOMA Based D2D Network for Disaster Management," Wireless Personal Communications, vol. 128, pp. 2341–2362, September 2022.
311. D. -W. Lim, C. -J. Chun and J. -M. Kang, "Transmit Power Adaptation for D2D Communications Underlaying SWIPT-Based IoT Cellular Networks," in IEEE Internet of Things Journal, vol. 10, no. 2, pp. 987-1000, January 2023.
312. I. Budhiraja, N. Kumar, S. Tyagi, S. Tanwar and M. Guizani, "SWIPT-Enabled D2D Communication Underlaying NOMA-Based Cellular Networks in Imperfect CSI," in IEEE Transactions on Vehicular Technology, vol. 70, no. 1, pp. 692-699, January 2021.
313. W. Liu, X. Zhou, S. Durrani and P. Popovski, "SWIPT with practical modulation and RF energy harvesting sensitivity," 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 2016, pp. 1-7.
314. J. -M. Kang, I. -M. Kim and D. I. Kim, "Wireless Information and Power Transfer: Rate-Energy Tradeoff for Nonlinear Energy Harvesting," in IEEE Transactions on Wireless Communications, vol. 17, no. 3, pp. 1966-1981, March 2018.
315. D. -T. Do, C. -B. Le and F. Afghah, "Enabling Full-Duplex and Energy Harvesting in Uplink and Downlink of Small-Cell Network Relying on Power Domain Based Multiple Access," in IEEE Access, vol. 8, pp. 142772-142784, 2020.
316. Y. Meng, Z. Zhang and Y. Huang, "Cache- and Energy Harvesting-Enabled D2D Cellular Network: Modeling, Analysis and Optimization," in IEEE Transactions on Green Communications and Networking, vol. 5, no. 2, pp. 703-713, June 2021.
317. Ammar et al., "Requirements for Energy-Harvesting-Driven Edge Devices Using Task-Offloading Approaches," Electronics, vol. 11, no. 3, January 2022.
318. M. Min, L. Xiao, Y. Chen, P. Cheng, D. Wu and W. Zhuang, "Learning-Based Computation Offloading for IoT Devices With Energy Harvesting," in IEEE Transactions on Vehicular Technology, vol. 68, no. 2, pp. 1930-1941, February 2019.
319. A. M. Seid, J. Lu, H. N. Abishu and T. A. Ayall, "Blockchain-Enabled Task Offloading With Energy Harvesting in Multi-UAV-Assisted IoT Networks: A Multi-Agent DRL Approach," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3517-3532, December 2022.
320. Z. Wang, T. Lv and Z. Chang, "Computation Offloading and Resource Allocation Based on Distributed Deep Learning and Software Defined Mobile Edge Computing," Computer Networks, vol. 205, March 2022.
321. A. Shakarami, A. Shahidinejad and M. Ghobaei-Arani, "An Autonomous Computation Offloading Strategy In Mobile Edge Computing: A Deep Learning-Based Hybrid Approach," Journal of Network and Computer Applications, vol. 178, March 2021.

322. M. Min et al., "Learning-Based Privacy-Aware Offloading for Healthcare IoT With Energy Harvesting," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4307-4316, June 2019.
323. S. Xia, Z. Yao, Y. Li and S. Mao, "Online Distributed Offloading and Computing Resource Management With Energy Harvesting for Heterogeneous MEC-Enabled IoT," in IEEE Transactions on Wireless Communications, vol. 20, no. 10, pp. 6743-6757, October 2021.
324. F. Zhao, Y. Chen, Y. Zhang, Z. Liu and X. Chen, "Dynamic Offloading and Resource Scheduling for Mobile-Edge Computing With Energy Harvesting Devices," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 2154-2165, June 2021.
325. H. Hu, Q. Wang, R. Q. Hu and H. Zhu, "Mobility-Aware Offloading and Resource Allocation in a MEC-Enabled IoT Network With Energy Harvesting," in IEEE Internet of Things Journal, vol. 8, no. 24, pp. 17541-17556, December 2021.
326. E. Mustafa et al., "Joint Wireless Power Transfer and Task Offloading in Mobile Edge Computing: A Survey," Cluster Computing, vol. 25, pp. 2429–2448, August 2021.
327. NTT DoCoMo and Metawave announce successful demonstration of 28GHz-band 5G using world's first meta-structure technology. [Online]. Available: https://www.bloomberg.com/press-releases/2018-12-04/ntt-docomo-and-metawave-announce-successful-demonstration-of-28ghz-band-5g-using-world-s-first-meta-structure-technology. Accessed: March, 2023.
328. D. Pérez-Adán et al., "Intelligent Reflective Surfaces for Wireless Networks: An Overview of Applications, Approached Issues, and Open Problems," Electronics, vol. 10, no. 19, September 2021.
329. W. Long, R. Chen, M. Moretti, W. Zhang and J. Li, "A Promising Technology for 6G Wireless Networks: Intelligent Reflecting Surface," in Journal of Communications and Information Networks, vol. 6, no. 1, pp. 1-16, March 2021.
330. Z. Wang, D. Shi and H. Wu, "The Role of Massive MIMO and Intelligent Reflecting Surface in 5G/6G Networks," 2021 International Conference on Wireless Communications and Smart Grid (ICWCSG), Hangzhou, China, 2021.
331. E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M. -S. Alouini and R. Zhang, "Wireless Communications Through Reconfigurable Intelligent Surfaces," in IEEE Access, vol. 7, pp. 116753-116773, 2019.
332. S. Hu, F. Rusek and O. Edfors, "Beyond Massive MIMO: The Potential of Data Transmission With Large Intelligent Surfaces," in IEEE Transactions on Signal Processing, vol. 66, no. 10, pp. 2746-2758, May 2018.
333. A. -A. A. Boulogeorgos and A. Alexiou, "Performance Analysis of Reconfigurable Intelligent Surface-Assisted Wireless Systems and Comparison With Relaying," in IEEE Access, vol. 8, pp. 94463-94483, 2020.
334. E. Björnson, Ö. Özdogan and E. G. Larsson, "Intelligent Reflecting Surface Versus Decode-and-Forward: How Large Surfaces are Needed to Beat Relaying?," in IEEE Wireless Communications Letters, vol. 9, no. 2, pp. 244-248, February 2020.
335. S. Gong et al., "Toward Smart Wireless Communications via Intelligent Reflecting Surfaces: A Contemporary Survey," in IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2283-2314, Fourthquarter 2020.
336. Q. Wu, S. Zhang, B. Zheng, C. You and R. Zhang, "Intelligent Reflecting Surface-Aided Wireless Communications: A Tutorial," in IEEE Transactions on Communications, vol. 69, no. 5, pp. 3313-3351, May 2021.
337. S. Abeywickrama, R. Zhang and C. Yuen, "Intelligent Reflecting Surface: Practical Phase Shift Model and Beamforming Optimization," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6.
338. J. Wang, Y. -C. Liang, S. Han and Y. Pei, "Robust Beamforming and Phase Shift Design for IRS-Enhanced Multi-User MISO Downlink Communication," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6.
339. G. Pan, J. Ye, J. An and M. -S. Alouini, "Full-Duplex Enabled Intelligent Reflecting Surface Systems: Opportunities and Challenges," in IEEE Wireless Communications, vol. 28, no. 3, pp. 122-129, June 2021.
340. Y. Zhu, B. Mao and N. Kato, "A Dynamic Task Scheduling Strategy for Multi-Access Edge Computing in IRS-Aided Vehicular Networks," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 4, pp. 1761-1771, December 2022.
341. J. Lu et al., "Performance Analysis for IRS-Assisted MEC Networks with Unit Selection," Physical Communication, vol. 55, December 2022.
342. M. Sheng, Y. Wang, X. Wang and J. Li, "Energy-Efficient Multiuser Partial Computation Offloading With Collaboration of Terminals, Radio Access Network, and Edge Server," in IEEE Transactions on Communications, vol. 68, no. 3, pp. 1524-1537, March 2020.
343. T. Bai, C. Pan, C. Han and L. Hanzo, "Reconfigurable Intelligent Surface Aided Mobile Edge Computing," in IEEE Wireless Communications, vol. 28, no. 6, pp. 80-86, December 2021.
344. W. Zheng and L. Yan, "Latency minimization for IRS-assisted mobile edge computing networks," Physical Communication, vol. 53, August 2022.
345. G. Chen, Q. Wu, R. Liu, J. Wu and C. Fang, "IRS Aided MEC Systems With Binary Offloading: A Unified Framework for Dynamic IRS Beamforming," in IEEE Journal on Selected Areas in Communications, vol. 41, no. 2, pp. 349-365, February 2023.
346. Y. Zhou et al., "Joint Optimization for Cooperative Computing Framework in Double-IRS-Aided MEC Systems," in IEEE Wireless Communications Letters.
347. G. Chen, Q. Wu, W. Chen, D. W. K. Ng and L. Hanzo, "IRS-Aided Wireless Powered MEC Systems: TDMA or NOMA for Computation Offloading?," in IEEE Transactions on Wireless Communications, vol. 22, no. 2, pp. 1201-1218, February 2023.
348. DB. Ha, VT. Truong, V. N. Vo, "Performance Analysis of Intelligent Reflecting Surface-Aided Mobile Edge Computing Network with Uplink NOMA Scheme." In: NS. Vo, QT. Vien, DB. Ha (eds) Industrial Networks and Intelligent Systems. INISCOM 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 444. Springer, Cham. June 2022.
349. W. Tushar et al., "A Survey of Cyber-Physical Systems From a Game-Theoretic Perspective," in IEEE Access, vol. 11, pp. 9799-9834, 2023.
350. C. Chi, Y. Wang, X. Tong, M. Siddula and Z. Cai, "Game Theory in Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 12125-12146, July 2022.
351. L. Cheng and T. Yu, "Game-Theoretic Approaches Applied to Transactions in the Open and Ever-Growing Electricity Markets From the Perspective of Power Demand Response: An Overview," in IEEE Access, vol. 7, pp. 25727-25762, 2019.
352. U. Singh et al., "Coalition Games for Performance Evaluation in 5G and Beyond Networks: A Survey," in IEEE Access, vol. 10, pp. 15393-15420, 2022.

353. W. Liang, S. X. Ng and L. Hanzo, "Cooperative Overlay Spectrum Access in Cognitive Radio Networks," in IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1924-1944, thirdquarter 2017.
354. M. E. Mkiramweni, C. Yang, J. Li and W. Zhang, "A Survey of Game Theory in Unmanned Aerial Vehicles Communications," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3386-3416, Fourthquarter 2019.
355. Z. Sun et al., "Applications of Game Theory in Vehicular Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2660-2710, Fourthquarter 2021.
356. X. Song, W. Jiang, X. Liu, H. Lu, Z. Tian and X. Du, "A survey of game theory as applied to social networks," in Tsinghua Science and Technology, vol. 25, no. 6, pp. 734-742, December 2020.
357. Z. A. E. Houda, B. Brik, A. Ksentini, L. Khoukhi and M. Guizani, "When Federated Learning Meets Game Theory: A Cooperative Framework to Secure IIoT Applications on Edge Computing," in IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 7988-7997, November 2022.
358. J. Moura and D. Hutchison, "Game Theory for Multi-Access Edge Computing: Survey, Use Cases, and Future Trends," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 260-288, Firstquarter 2019.
359. N. Li, J. -F. Martinez-Ortega and V. H. Diaz, "Distributed Power Control for Interference-Aware Multi-User Mobile Edge Computing: A Game Theory Approach," in IEEE Access, vol. 6, pp. 36105-36114, 2018.
360. R. Chen et al., "Joint Computation Offloading, Channel Access and Scheduling Optimization in UAV Swarms: A Game-Theoretic Learning Approach," in IEEE Open Journal of the Computer Society, vol. 2, pp. 308-320, 2021.
361. H. Wang, Z. Lin, K. Guo and T. Lv, "Energy and Delay Minimization Based on Game Theory in MEC-Assisted Vehicular Networks," 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 2021, pp. 1-6.
362. N. Li, J. Yan, Z. Zhang, J. F. Martinez and X. Yuan, "Game Theory based Joint Task Offloading and Resource Allocation Algorithm for Mobile Edge Computing," 2020 16th International Conference on Mobility, Sensing and Networking (MSN), Tokyo, Japan, 2020, pp. 791-796.
363. S. Li, X. Hu and Y. Du, "Deep Reinforcement Learning and Game Theory for Computation Offloading in Dynamic Edge Computing Markets," in IEEE Access, vol. 9, pp. 121456-121466, 2021.
364. C. Xia, Z. Jin, J. Su and B. Li, "Mobility-Aware Offloading and Resource Allocation Strategies in MEC Network Based on Game Theory," Wireless Communications & Mobile Computing, vol. 2023, February 2023.
365. X. Chen, Y. Cai, L. Li, M. Zhao, B. Champagne and L. Hanzo, "Energy-Efficient Resource Allocation for Latency-Sensitive Mobile Edge Computing," in IEEE Transactions on Vehicular Technology, vol. 69, no. 2, pp. 2246-2262, February 2020.
366. J. Jiang, J.D. Li and X.Y. Liu, "Network selection policy based on auction theory in heterogeneous wireless communication systems," Science China Information Sciences, vol. 58, pp. 1-10, December 2014.
367. B. Wu, X. Chen, L. Jiao, "Collaborative Computing Based on Truthful Online Auction Mechanism in Internet of Things". In: H. Gao, X. Wang, (eds) Collaborative Computing: Networking, Applications and Worksharing. CollaborateCom 2021. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 407, Springer, Cham. January 2022.
368. H. Qiu, K. Zhu, N. C. Luong, C. Yi, D. Niyato and D. I. Kim, "Applications of Auction and Mechanism Design in Edge Computing: A Survey," in IEEE Transactions on Cognitive Communications and Networking, vol. 8, no. 2, pp. 1034-1058, June 2022.
369. N. Sharghivand, F. Derakhshan and N. Siasi, "A Comprehensive Survey on Auction Mechanism Design for Cloud/Edge Resource Management and Pricing," in IEEE Access, vol. 9, pp. 126502-126529, 2021.
370. Y. Shoham and K. Leyton-Brown, Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations. Cambridge, U.K.: Cambridge Univ. Press, 2008.
371. J. He, D. Zhang, Y. Zhou, X. Lan and Y. Zhang, "Towards a Truthful Online Auction for Cooperative Mobile Task Execution," 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, 2018, pp. 546-553.
372. D. Kumar, G. Baranwal and D. P. Vidyarthi, "A Survey on Auction based Approaches for Resource Allocation and Pricing in Emerging Edge Technologies," Journal of Grid Computing, vol. 20, December 2021.
373. M. Diamanti and S. Papavassiliou, "Trading in Collaborative Mobile Edge Computing Networks: A Contract Theory-based Auction Model," 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS), Marina del Rey, Los Angeles, CA, USA, 2022.
374. H. Zhang, F. Guo, H. Ji and C. Zhu, "Combinational Auction-Based Service Provider Selection in Mobile Edge Computing Networks," in IEEE Access, vol. 5, pp. 13455-13464, 2017.
375. Y. Xu, K. Zhu and S. Li, "Hierarchical Combinatorial Auction in Computing Resource Allocation for Mobile Blockchain," Wireless Communications and Mobile Computing, vol. 2020, Aug 2020.
376. Xiao et al., "Multi-Round Auction-Based Resource Allocation for Edge Computing: Maximizing Social Welfare," Future Generation Computer Systems, vol. 140, pp. 365-375, March 2023.
377. R. Zeng, S. Zhang, J. Wang and X. Chu, "FMore: An Incentive Scheme of Multi-dimensional Auction for Federated Learning in MEC," 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, Singapore, 2020, pp. 278-288.
378. F. Wei, S. Chen and W. Zou, "A Greedy Algorithm for Task Offloading in Mobile Edge Computing System," in China Communications, vol. 15, no. 11, pp. 149-157, November 2018.
379. Y. Zhang and J. Fu, "Efficient Computation Offloading in Mobile Edge Computing Based on Dynamic Programming," 2020 Chinese Automation Congress (CAC), Shanghai, China, 2020, pp. 1381-1385.
380. T. Wu, W. Jing, X. Wen, Z. Lu and S. Zhao, "A Scalable Computation Offloading Scheme for MEC Based on Graph Neural Networks," 2021 IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 2021, pp. 1-6.

381. C. Pop, M. Prata, M. Antal, T. Cioara, I. Anghel and I. Salomie, "An Ethereum-based implementation of English, Dutch and First-price sealed-bid auctions," 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, 2020, pp. 491-497.
382. Y. Wang and C. Xiang, "Which is more suitable for rare flowers, first-price sealed-bid auction or second-price sealed-bid auction?," 2014 IEEE International Conference on Mechatronics and Automation, Tianjin, China, 2014, pp. 2111-2111.
383. C. Semeraro, M. Lezoche, H. Panetto and M. Dassisti, “Digital twin paradigm: A systematic literature review,” Computers in Industry, vol. 130, September 2021.
384. G. Caiza and R. Sanz, "Digital Twin for Monitoring an Industrial Process Using Augmented Reality," 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), Madrid, Spain, 2022, pp. 1-5.
385. M. Schluse, M. Priggemeyer, L. Atorf and J. Rossmann, "Experimentable Digital Twins—Streamlining Simulation-Based Systems Engineering for Industry 4.0," in IEEE Transactions on Industrial Informatics, vol. 14, no. 4, pp. 1722-1731, April 2018.
386. E. Örs, R. Schmidt, M. Mighani and M. Shalaby, "A Conceptual Framework for AI-based Operational Digital Twin in Chemical Process Engineering," 2020 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Cardiff, UK, 2020, pp. 1-8.
387. Y. Wu, K. Zhang and Y. Zhang, "Digital Twin Networks: A Survey," in IEEE Internet of Things Journal, vol. 8, no. 18, pp. 13789-13804, September 2021.
388. A. P. Plageras and K. E. Psannis, “Digital Twins and Multi-Access Edge Computing for IIoT,” Virtual Reality & Intelligent Hardware, vol. 4, no. 6, pp. 521-534, December 2022.
389. W. Sun, H. Zhang, R. Wang and Y. Zhang, "Reducing Offloading Latency for Digital Twin Edge Networks in 6G," in IEEE Transactions on Vehicular Technology, vol. 69, no. 10, pp. 12240-12251, October 2020.
390. D. Van Huynh, S. R. Khosravirad, A. Masaracchia, O. A. Dobre and T. Q. Duong, "Edge Intelligence-Based Ultra-Reliable and Low-Latency Communications for Digital Twin-Enabled Metaverse," in IEEE Wireless Communications Letters, vol. 11, no. 8, pp. 1733-1737, August 2022.
391. J. Guo et al., “Survey on digital twins for Internet of Vehicles: Fundamentals, challenges, and opportunities,” Digital Communications and Networks, June 2022.
392. L. Zhao, G. Han, Z. Li and L. Shu, "Intelligent Digital Twin-Based Software-Defined Vehicular Networks," in IEEE Network, vol. 34, no. 5, pp. 178-184, September/October 2020.
393. L. U. Khan, Z. Han, W. Saad, E. Hossain, M. Guizani and C. S. Hong, "Digital Twin of Wireless Systems: Overview, Taxonomy, Challenges, and Opportunities," in IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2230-2254, Fourthquarter 2022.
394. T. Liu, L. Tang, W. Wang, Q. Chen and X. Zeng, "Digital-Twin-Assisted Task Offloading Based on Edge Collaboration in the Digital Twin Edge Network," in IEEE Internet of Things Journal, vol. 9, no. 2, pp. 1427-1444, January 2022.
395. Y. Lu, X. Huang, K. Zhang, S. Maharjan and Y. Zhang, "Communication-Efficient Federated Learning for Digital Twin Edge Networks in Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5709-5718, August 2021.
396. Y. Lu, X. Huang, K. Zhang, S. Maharjan and Y. Zhang, "Communication-Efficient Federated Learning and Permissioned Blockchain for Digital Twin Edge Networks," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2276-2288, February 2021.
397. B. Fan, Y. Wu, Z. He, Y. Chen, T. Q. S. Quek and C. -Z. Xu, "Digital Twin Empowered Mobile Edge Computing for Intelligent Vehicular Lane-Changing," in IEEE Network, vol. 35, no. 6, pp. 194-201, November/December 2021.
398. X. Yuan, J. Chen, N. Zhang, J. Ni, F. R. Yu and V. C. M. Leung, "Digital Twin-Driven Vehicular Task Offloading and IRS Configuration in the Internet of Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 12, pp. 24290-24304, December 2022.
399. H. Cui et al., "Space-air-ground integrated network (SAGIN) for 6G: Requirements, architecture and challenges," in China Communications, vol. 19, no. 2, pp. 90-108, February 2022.
400. C. Zhou, J. Gao, M. Li, X. Sherman Shen and W. Zhuang, "Digital Twin-Empowered Network Planning for Multi-Tier Computing," in Journal of Communications and Information Networks, vol. 7, no. 3, pp. 221-238, September 2022.
401. W. Sun, S. Lian, H. Zhang and Y. Zhang, "Lightweight Digital Twin and Federated Learning with Distributed Incentive in Air-Ground 6G Networks," in IEEE Transactions on Network Science and Engineering, 2022.
402. S. D. Okegbile, J. Cai, C. Yi and D. Niyato, "Human Digital Twin for Personalized Healthcare: Vision, Architecture and Future Directions," in IEEE Network.
403. D. Van Huynh et al., "URLLC Edge Networks With Joint Optimal User Association, Task Offloading and Resource Allocation: A Digital Twin Approach," in IEEE Transactions on Communications, vol. 70, no. 11, pp. 7669-7682, November 2022.
404. F. Tang, X. Chen, T. K. Rodrigues, M. Zhao and N. Kato, "Survey on Digital Twin Edge Networks (DITEN) Toward 6G," in IEEE Open Journal of the Communications Society, vol. 3, pp. 1360-1381, 2022.
405. G. Cai, B. Fan, Y. Dong, T. Li, Y. Wu and Y. Zhang, "Task-Efficiency Oriented V2X Communications: Digital Twin Meets Mobile Edge Computing," in IEEE Wireless Communications.
406. M. Groshev, C. Guimarães, J. Martín-Pérez and A. de la Oliva, "Toward Intelligent Cyber-Physical Systems: Digital Twin Meets Artificial Intelligence," in IEEE Communications Magazine, vol. 59, no. 8, pp. 14-20, August 2021.
407. J. Yang et al., "A Parallel Intelligence-driven Resource Scheduling Scheme for Digital Twins-based Intelligent Vehicular Systems," in IEEE Transactions on Intelligent Vehicles.
408. M. O. Ozdogan, L. Carkacioglu and B. Canberk, "Digital Twin Driven Blockchain Based Reliable and Efficient 6G Edge Network," 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS), Marina del Rey, Los Angeles, CA, USA, 2022, pp. 342-348.
409. M. Garrich, F. -J. Moreno-Muro, M. -V. Bueno Delgado and P. Pavón Mariño, "Open-Source Network Optimization Software in the Open SDN/NFV Transport Ecosystem," in Journal of Lightwave Technology, vol. 37, no. 1, pp. 75-88, January 2019.
410. S. Massari, N. Mirizzi, G. Piro and G. Boggia, "An Open-Source Tool Modeling the ETSI-MEC Architecture in the Industry 4.0 Context," 2021 29th Mediterranean Conference on Control and Automation (MED), PUGLIA, Italy, 2021, pp. 226-231.

411. A. Ghosh, A. Maeder, M. Baker and D. Chandramouli, "5G Evolution: A View on 5G Cellular Technology Beyond 3GPP Release 15," in IEEE Access, vol. 7, pp. 127639-127651, 2019.
412. T. Li, L. Zhao, R. Duan and H. Tian, "SBA-Based Mobile Edge Computing," 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 2019, pp. 1-6.
413. E. A. Papatheofanous, D. Reisis and K. Nikitopoulos, "LDPC Hardware Acceleration in 5G Open Radio Access Network Platforms," in IEEE Access, vol. 9, pp. 152960-152971, 2021.
414. T. Hoeschele, F. Kaltenberger, A. I. Grohmann, E. Tasdemir, M. Reisslein and F. H. P. Fitzek, "5G InterOPERAbility of Open RAN Components in Large Testbed Ecosystem: Towards 6G Flexibility," European Wireless 2022; 27th European Wireless Conference, Dresden, Germany, 2022, pp. 1-6.
415. H. Lee, Y. Jang, J. Song and H. Yeon, "O-RAN AI/ML Workflow Implementation of Personalized Network Optimization via Reinforcement Learning," 2021 IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 2021, pp. 1-6.
416. S. Kukliński, L. Tomaszewski, R. Kołakowski and P. Chemouil, "6G-LEGO: A framework for 6G network slices," in Journal of Communications and Networks, vol. 23, no. 6, pp. 442-453, December 2021.
417. H. Liu, J. Zong, Q. Wang, Y. Liu and F. Yang, "Cloud Native Based Intelligent RAN Architecture Towards 6G Programmable Networking," 2022 7th International Conference on Computer and Communication Systems (ICCCS), Wuhan, China, 2022, pp. 623-627.
418. B. Angui, R. Corbel, V. Q. Rodriguez and E. Stephan, "Towards 6G zero touch networks: The case of automated Cloud-RAN deployments," 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2022, pp. 1-6.
419. H. Kumar, V. Sapru and S. K. Jaisawal, "O-RAN based proactive ANR optimization," 2020 IEEE Globecom Workshops (GC Wkshps, Taipei, Taiwan, 2020, pp. 1-4.
420. L. Yan, X. Fang, G. Min and Y. Fang, "A Low-Latency Collaborative HARQ Scheme for Control/User-Plane Decoupled Railway Wireless Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 8, pp. 2282-2295, August 2016.
421. O. Onireti, A. Imran, M. A. Imran and R. Tafazolli, "Cell Outage Detection in Heterogeneous Networks with Separated Control and Data Plane," European Wireless 2014; 20th European Wireless Conference, Barcelona, Spain, 2014, pp. 1-6.
422. H. Gupta, M. Sharma, A. Franklin A. and B. R. Tamma, "Apt-RAN: A Flexible Split-Based 5G RAN to Minimize Energy Consumption and Handovers," in IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 473-487, March 2020.
423. S. Matoussi, I. Fajjari, S. Costanzo, N. Aitsaadi and R. Langar, "5G RAN: Functional Split Orchestration Optimization," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 7, pp. 1448-1463, July 2020.
424. C. Dai, K. Zhu, R. Wang and Y. Xu, "Decoupled Uplink-Downlink User Association in Ultra-Dense Networks: A Contract-Theoretic Approach," 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 2019, pp. 1-6.
425. Y. Xu, B. Qian, K. Yu, T. Ma, L. Zhao and H. Zhou, "Federated Learning Over Fully-Decoupled RAN Architecture for Two-Tier Computing Acceleration," in IEEE Journal on Selected Areas in Communications, vol. 41, no. 3, pp. 789-801, March 2023.
426. M. Y. -K. Chua, F. R. Yu and S. Bu, "Dynamic Operations of Cloud Radio Access Networks (C-RAN) for Mobile Cloud Computing Systems," in IEEE Transactions on Vehicular Technology, vol. 65, no. 3, pp. 1536-1548, March 2016.
427. M. A. Hasabelnaby and A. Chaaban, "Multi-Pair Computation for C-RAN With Intra-Cloud and Inter-Cloud Communications," in IEEE Wireless Communications Letters, vol. 11, no. 12, pp. 2537-2541, December 2022.
428. A. S. Mubarak, H. Esmaiel and E. M. Mohamed, "LTE/Wi-Fi/mmWave RAN-Level Interworking Using 2C/U Plane Splitting for Future 5G Networks," in IEEE Access, vol. 6, pp. 53473-53488, 2018.
429. W. Guan, H. Zhang and V. C. M. Leung, "Customized Slicing for 6G: Enforcing Artificial Intelligence on Resource Management," in IEEE Network, vol. 35, no. 5, pp. 264-271, September/October 2021.
430. J. J. Rico-Palomo, J. Galeano-Brajones, D. Cortes-Polo, J. F. Valenzuela-Valdes and J. Carmona-Murillo, "Chained Orchestrator Algorithm for RAN-Slicing Resource Management: A Contribution to Ultra-Reliable 6G Communications," in IEEE Access, vol. 10, pp. 113662-113677, 2022.
431. J. Mei, X. Wang and K. Zheng, "An intelligent self-sustained RAN slicing framework for diverse service provisioning in 5G-beyond and 6G networks," in Intelligent and Converged Networks, vol. 1, no. 3, pp. 281-294, December 2020.
432. M. A. Habibi, F. Z. Yousaf and H. D. Schotten, "Mapping the VNFs and VLs of a RAN Slice Onto Intelligent PoPs in Beyond 5G Mobile Networks," in IEEE Open Journal of the Communications Society, vol. 3, pp. 670-704, 2022.
433. Y. Azimi, S. Yousefi, H. Kalbkhani and T. Kunz, "Applications of Machine Learning in Resource Management for RAN-Slicing in 5G and Beyond Networks: A Survey," in IEEE Access, vol. 10, pp. 106581-106612, 2022.
434. D. Giannopoulos, P. Papaioannou, C. Tranoris and S. Denazis, "Monitoring as a Service over a 5G Network Slice," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 2021, pp. 329-334.
435. V. -Q. Pham, H. -T. Thieu, A. Kak, and N. Choi., “HexRIC: Building a Better near-Real Time Network Controller for the Open RAN Ecosystem,” In Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications (HotMobile '23), Association for Computing Machinery, pp. 15–21, New York, NY, USA, February 2023.
436. P. S. Khodashenas et al., "Service Mapping and Orchestration Over Multi-Tenant Cloud-Enabled RAN," in IEEE Transactions on Network and Service Management, vol. 14, no. 4, pp. 904-919, December 2017.
437. R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," in IEEE Access, vol. 8, pp. 99999-100009, 2020, doi: 10.1109/ACCESS.2020.2997702.
438. M. Liyanage, A. Braeken, S. Shahabuddin and P. Ranaweera, “Open RAN Security: Challenges and Opportunities,” Journal of Network and Computer Applications, March 2023.
439. M. Gramaglia et al., "Network Intelligence for Virtualized RAN Orchestration: The DAEMON Approach," 2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Grenoble, France, 2022, pp. 482-487.

440. B. Agarwal, M. A. Togou, M. Ruffini and G. -M. Muntean, "QoE-Driven Optimization in 5G O-RAN-Enabled HetNets for Enhanced Video Service Quality," in IEEE Communications Magazine, vol. 61, no. 1, pp. 56-62, January 2023.
441. I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat and H. Dai, "A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3098-3130, Fourthquarter 2018.
442. M. A. Hasabelnaby and A. Chaaban, "End-to-End Rate Enhancement in C-RAN Using Multi-Pair Two-Way Computation," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 2021, pp. 49-54.
443. A. -I. -E. Ciobanu, E. Borcoci and M. -C. Vochin, "A Quality-of-Service Scenario Awareness for Use-Cases of Open-Source Management and Control System Hub in Edge Computing," 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Bucharest, Romania, 2021, pp. 1-5.
444. N. Slamnik-Kriještorac and J. M. Marquez-Barja, "Demo Abstract: Assessing MANO Performance based on VIM Platforms within MEC Context," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 2020, pp. 1338-1339.
445. L. Song, X. Hu, G. Zhang, P. Spachos, K. N. Plataniotis and H. Wu, "Networking Systems of AI: On the Convergence of Computing and Communications," in IEEE Internet of Things Journal, vol. 9, no. 20, pp. 20352-20381, October 2022.
446. A. Giannopoulos et al., "Supporting Intelligence in Disaggregated Open Radio Access Networks: Architectural Principles, AI/ML Workflow, and Use Cases," in IEEE Access, vol. 10, pp. 39580-39595, 2022.
447. N. Li et al., "Transforming the 5G RAN With Innovation: The Confluence of Cloud Native and Intelligence," in IEEE Access, vol. 11, pp. 4443-4454, 2023.
448. A. Arnaz, J. Lipman, M. Abolhasan and M. Hiltunen, "Toward Integrating Intelligence and Programmability in Open Radio Access Networks: A Comprehensive Survey," in IEEE Access, vol. 10, pp. 67747-67770, 2022.
449. J. Haavisto, M. Arif, L. Lovén, T. Leppänen and J. Riekki, "Open-source RANs in Practice: an Over-The-Air Deployment for 5G MEC," 2019 European Conference on Networks and Communications (EuCNC), Valencia, Spain, 2019, pp. 495-500.
450. R. Ullah, M. A. U. Rehman and B. -S. Kim, "Design and Implementation of an Open Source Framework and Prototype For Named Data Networking-Based Edge Cloud Computing System," in IEEE Access, vol. 7, pp. 57741-57759, 2019.
451. L. Zhao, G. Zhou, G. Zheng, C. -L. I, X. You and L. Hanzo, "Open-Source Multi-Access Edge Computing for 6G: Opportunities and Challenges," in IEEE Access, vol. 9, pp. 158426-158439, 2021.
452. C. -L. I, S. Kuklinskí and T. Chen, "A Perspective of O-RAN Integration with MEC, SON, and Network Slicing in the 5G Era," in IEEE Network, vol. 34, no. 6, pp. 3-4, November/December 2020
453. B. Brik, P. A. Frangoudis and A. Ksentini, "Service-Oriented MEC Applications Placement in a Federated Edge Cloud Architecture," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6.
454. A. Huang, N. Nikaein, T. Stenbock, A. Ksentini and C. Bonnet, "Low latency MEC framework for SDN-based LTE/LTE-A networks," 2017 IEEE International Conference on Communications (ICC), Paris, France, 2017, pp. 1-6.
455. P. -H. Huang, F. -C. Hsieh, W. -J. Hsieh, C. -Y. Li and Y. -D. Lin, "Prioritized Traffic Shaping for Low-latency MEC Flows in MEC-enabled Cellular Networks," 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2022, pp. 120-125.
456. H. Lv, D. Chen and Y. Wang, "Deployment of Edge-Computing in 5G NFV Environment and Future Service-Based Architecture," 2018 IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 2018, pp. 811-816.
457. R. Alvizu et al., "Comprehensive Survey on T-SDN: Software-Defined Networking for Transport Networks," in IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2232-2283, Fourthquarter 2017.
458. S.M. H. Krishna and R. Sharma, “Survey on Application Programming Interfaces in Software Defined Networks and Network Function Virtualization,” Global Transitions Proceedings, vol. 2, no. 2, pp. 199-204, November 2021.
459. E. Pencheva and I. Atanasov, "Mobile Edge Computing Services for Dynamic Quality of Service Control," 2017 20th Conference of Open Innovations Association (FRUCT), St. Petersburg, Russia, 2017, pp. 365-370.
460. L. Fan and Z. Han, "Hybrid Quantum-Classical Computing for Future Network Optimization," in IEEE Network, vol. 36, no. 5, pp. 72-76, September/October 2022.
461. K. Bertels et al., "Quantum Computer Architecture Toward Full-Stack Quantum Accelerators," in IEEE Transactions on Quantum Engineering, vol. 1, pp. 1-17, 2020.
462. I. K. Sohn and J. Heo, "An Introduction to Fault-Tolerant Quantum Computation and its Overhead Reduction Schemes," 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, 2018, pp. 44-46.
463. G. De Micheli, J. -H. R. Jiang, R. Rand, K. Smith and M. Soeken, "Advances in Quantum Computation and Quantum Technologies: A Design Automation Perspective," in IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 12, no. 3, pp. 584-601, September 2022.
464. S. Wang, Z. Pei, C. Wang and J. Wu, "Shaping the Future of the Application of Quantum Computing in Intelligent Transportation System," in Intelligent and Converged Networks, vol. 2, no. 4, pp. 259-276, December 2021.
465. L. P. Santos, T. Bashford-Rogers, J. Barbosa, and P. Navratil, “Towards quantum ray tracing,” arXiv preprint. arXiv: 2204.12797, 2022.
466. M. Xu et al., “Learning-based Sustainable Multi-User Computation Offloading for Mobile Edge-Quantum Computing,” arXiv preprint. arXiv: 2211.06681. 2022.
467. A. Passian et al., “The Concept of a Quantum Edge Simulator: Edge Computing and Sensing in the Quantum Era,” Sensors, vol. 23, no. 1, December 2022.
468. C. Li, Y. Zhang and Y. Luo, “Quantum ant colony-based mobile-aware service deployment in SDN-based multi- access edge computing environments,” Research Square preprint. https://doi.org/10.21203/rs.3.rs-821834/v1.

469. M. Masdari, K. Majidzadeh, E. Doustsadigh, A. Babazadeh and R. Asemi, “Energy-Aware Computation Offloading in Mobile Edge Computing Using Quantum-Based Arithmetic Optimization Algorithm,” Research Square preprint. https://doi.org/10.21203/rs.3.rs-2221212/v1.
470. X. Liu, "Enabling Optical Network Technologies for 5G and Beyond," in Journal of Lightwave Technology, vol. 40, no. 2, pp. 358-367, January 2022.
471. B. Kantarci and H. T. Mouftah, "Bandwidth Distribution Solutions for Performance Enhancement in Long-Reach Passive Optical Networks," in IEEE Communications Surveys & Tutorials, vol. 14, no. 3, pp. 714-733, Third Quarter 2012.
472. I. Dias, L. Ruan, C. Ranaweera and E. Wong, “From 5G to beyond: Passive optical network and multi-access edge computing integration for latency-sensitive applications,” Optical Fiber Technology, vol. 75, January 2023.
473. X. Wang, Y. Ji, J. Zhang, L. Bai and M. Zhang, "Low-Latency Oriented Network Planning for MEC-Enabled WDM-PON Based Fiber-Wireless Access Networks," in IEEE Access, vol. 7, pp. 183383-183395, 2019.
474. S. Das and M. Ruffini, "Optimal virtual PON slicing to support ultra-low latency mesh traffic pattern in MEC-based Cloud-RAN," 2021 International Conference on Optical Network Design and Modeling (ONDM), Gothenburg, Sweden, 2021, pp. 1-5.
475. X. Wang, Y. Ji, J. Zhang, L. Bai and M. Zhang, "Joint Optimization of Latency and Deployment Cost Over TDM-PON Based MEC-Enabled Cloud Radio Access Networks," in IEEE Access, vol. 8, pp. 681-696, 2020.
476. S. Das, F. Slyne, A. Kaszubowska and M. Ruffini, "Virtualized EAST–WEST PON Architecture Supporting Low-Latency Communication for Mobile Functional Split Based on Multiaccess Edge Computing," in Journal of Optical Communications and Networking, vol. 12, no. 10, pp. 109-119, October 2020.
477. L. Hu, W. Wang, S. Zhong, H. Guo, J. Li and Y. Pan, "APP-aware MAC Scheduling for MEC-backed TDM-PON Mobile Fronthaul," in IEEE Communications Letters.
478. S. -R. Yang, Y. -J. Tseng, C. -C. Huang and W. -C. Lin, "Multi-Access Edge Computing Enhanced Video Streaming: Proof-of-Concept Implementation and Prediction/QoE Models," in IEEE Transactions on Vehicular Technology, vol. 68, no. 2, pp. 1888-1902, February 2019.
479. R. Singh, R. Sukapuram and S. Chakraborty, "Mobility-aware Multi-Access Edge Computing for Multiplayer Augmented and Virtual Reality Gaming," 2022 IEEE 21st International Symposium on Network Computing and Applications (NCA), Boston, MA, USA, 2022, pp. 191-200.
480. C. -M. Huang and C. -F. Lai, "The Delay-Constrained and Network-Situation-Aware V2V2I VANET Data Offloading Based on the Multi-Access Edge Computing (MEC) Architecture," in IEEE Open Journal of Vehicular Technology, vol. 1, pp. 331-347, 2020.
481. M. Li, F. R. Yu, P. Si and Y. Zhang, "Energy-Efficient Machine-to-Machine (M2M) Communications in Virtualized Cellular Networks with Mobile Edge Computing (MEC)," in IEEE Transactions on Mobile Computing, vol. 18, no. 7, pp. 1541-1555, July 2019.
482. M. Li, L. Yang, F. R. Yu, W. Wu, Z. Wang and Y. Zhang, "Joint Optimization of Networking and Computing Resources for Green M2M Communications Based on DRL," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6.
483. M. Qin, L. Chen, N. Zhao, Y. Chen, F. R. Yu and G. Wei, "Computing and Relaying: Utilizing Mobile Edge Computing for P2P Communications," in IEEE Transactions on Vehicular Technology, vol. 69, no. 2, pp. 1582-1594, February 2020.
484. A. V. Rivera, A. Refaey and E. Hossain, "A Blockchain Framework for Secure Task Sharing in Multi-Access Edge Computing," in IEEE Network, vol. 35, no. 3, pp. 176-183, May/June 2021.
485. Z. Ma and S. Sun, "Research on Vehicle-to-Road Collaboration and End-to-End Collaboration for Multimedia Services in the Internet of Vehicles," in IEEE Access, vol. 10, pp. 18146-18155, 2022.
486. D. Wu, J. Liu and Z. Yang, "Bilateral Satisfaction Aware Participant Selection With MEC for Mobile Crowd Sensing," in IEEE Access, vol. 8, pp. 48110-48122, 2020.
487. M. R. Anwar, S. Wang, M. F. Akram, S. Raza and S. Mahmood, "5G-Enabled MEC: A Distributed Traffic Steering for Seamless Service Migration of Internet of Vehicles," in IEEE Internet of Things Journal, vol. 9, no. 1, pp. 648-661, January 2022.
488. P. Bellavista, D. Belli, S. Chessa and L. Foschini, "A Social-Driven Edge Computing Architecture for Mobile Crowd Sensing Management," in IEEE Communications Magazine, vol. 57, no. 4, pp. 68-73, April 2019.
489. A. Cenedese, A. Zanella, L. Vangelista and M. Zorzi, "Padova Smart City: An urban Internet of Things experimentation," Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, Sydney, NSW, Australia, 2014, pp. 1-6.
490. T. Alam et al., “Big Data for Smart Cities: A Case Study of NEOM City, Saudi Arabia.” In: M. A. Khan, F. Algarni, M. T. Quasim, (eds) Smart Cities: A Data Analytics Perspective. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham. December 2020.
491. Y. Zhao, K. Xu, H. Wang, B. Li, M. Qiao and H. Shi, "MEC-Enabled Hierarchical Emotion Recognition and Perturbation-Aware Defense in Smart Cities," in IEEE Internet of Things Journal, vol. 8, no. 23, pp. 16933-16945, December 2021.
492. H. Wang, X. Wang, X. Lan, T. Su and L. Wan, "BSBL-Based Auxiliary Vehicle Position Analysis in Smart City Using Distributed MEC and UAV-Deployed IoT," in IEEE Internet of Things Journal, vol. 10, no. 2, pp. 975-986, January 2023.
493. K. Peng, H. Huang, P. Liu, X. Xu and V. C. M. Leung, "Joint Optimization of Energy Conservation and Privacy Preservation for Intelligent Task Offloading in MEC-Enabled Smart Cities," in IEEE Transactions on Green Communications and Networking, vol. 6, no. 3, pp. 1671-1682, September 2022.
494. P. K. Reddy Maddikunta et al., "Unmanned Aerial Vehicles in Smart Agriculture: Applications, Requirements, and Challenges," in IEEE Sensors Journal, vol. 21, no. 16, pp. 17608-17619, August 2021.
495. J. Chen and A. Yang, "Intelligent Agriculture and Its Key Technologies Based on Internet of Things Architecture," in IEEE Access, vol. 7, pp. 77134-77141, 2019.
496. C. Qu et al., “DroneCOCoNet: Learning-Based Edge Computation Offloading and Control Networking for Drone Video Analytics,” Future Generation Computer Systems, vol. 125, pp. 247-262, December 2021.
497. D. Nallaperuma et al., "Online Incremental Machine Learning Platform for Big Data-Driven Smart Traffic Management," in IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 12, pp. 4679-4690, December 2019.
498. D. -J. Lin, M. -Y. Chen, H. -S. Chiang and P. K. Sharma, "Intelligent Traffic Accident Prediction Model for Internet of Vehicles With Deep Learning Approach," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 3, pp. 2340-2349, March 2022.

499. J. Sun, C. Yang, T. Tanjo, K. Sage, K. Aida, “Implementation of Self-adaptive Middleware for Mobile Vehicle Tracking Applications on Edge Computing.” In: Y. Xiang, J. Sun, G. Fortino, A. Guerrieri, J. Jung (eds) Internet and Distributed Computing Systems. IDCS 2018. Lecture Notes in Computer Science, vol. 11226. Springer, Cham.
500. F. Liu, J. Chen, Q. Zhang and B. Li, "Online MEC Offloading for V2V Networks," in IEEE Transactions on Mobile Computing, 2022.
501. L. Zhang, J. Hao, G. Zhao, M. Wen, T. Hai and K. Cao, "Research and Application of AI Services Based on 5G MEC in Smart Grid," 2020 IEEE Computing, Communications and IoT Applications (ComComAp), Beijing, China, 2020, pp. 1-6.
502. C. Ma et al., "5G Enabling Streaming Media Architecture with Edge Intelligence Gateway in Smart Grids," 2022 IEEE 5th International Conference on Computer and Communication Engineering Technology (CCET), Beijing, China, 2022, pp. 233-237.
503. J. Jiang, Y. Wang and P. Xin, "Blockchain Technology Enabled Communication Network for 5G MEC Architecture of Smart Grids," 2022 IEEE 8th International Conference on Computer and Communications (ICCC), Chengdu, China, 2022, pp. 253-257.
504. S. Bebortta, D. Senapati, C. R. Panigrahi and B. Pati, "Adaptive Performance Modeling Framework for QoS-Aware Offloading in MEC-Based IIoT Systems," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 10162-10171, June 2022.
505. C. Deng, X. Fang, X. Wang and K. Law, "Software Orchestrated and Hardware Accelerated Artificial Intelligence: Toward Low Latency Edge Computing," in IEEE Wireless Communications, vol. 29, no. 4, pp. 110-117, August 2022.
506. Q. Qu, C. Liu and X. Bao, “E-Commerce Enterprise Supply Chain Financing Risk Assessment Based on Linked Data Mining and Edge Computing,” Mobile Information Systems, May 2021.
507. P. K. Bishoyi and S. Misra, "Towards Energy-And Cost-Efficient Sustainable MEC-Assisted Healthcare Systems," in IEEE Transactions on Sustainable Computing, vol. 7, no. 4, pp. 958-969, October-December 2022.
508. CDC. Preventing Stroke Deaths. [Online]. Available: https://www.cdc.gov/vitalsigns/stroke/index.html. Accessed: February 2023.
509. R. Jain and V. B. Semwal, "A Novel Feature Extraction Method for Preimpact Fall Detection System Using Deep Learning and Wearable Sensors," in IEEE Sensors Journal, vol. 22, no. 23, pp. 22943-22951, December 2022.
510. S. S. Fakhrulddin, S. Kamel Gharghan and S. L. Zubaidi, "Accurate Fall Localization for Patient based on GPS and Accelerometer Sensor in Outside the House," 2020 13th International Conference on Developments in eSystems Engineering (DeSE), Liverpool, United Kingdom, 2020, pp. 432-436.
511. M. S. Al-Rakham et al., “FallDeF5: A Fall Detection Framework Using 5G-Based Deep Gated Recurrent Unit Networks,” IEEE Access, vol. 9, pp. 94299- 94308, June 2021.
512. Y. Liu, M. Peng, G. Shou, Y. Chen and S. Chen, "Toward Edge Intelligence: Multiaccess Edge Computing for 5G and Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6722-6747, August 2020.
513. A. Sharma and C. Diwakar, "Future aspects on MEC (Mobile Edge Computing): Offloading Mechanism," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 2021, pp. 34-39.
514. M. S. Mahmud, H. Wang, A. M. Esfar-E-Alam and H. Fang, "A Wireless Health Monitoring System Using Mobile Phone Accessories," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 2009-2018, December 2017.
515. E. E. Ugwuanyi, S. Ghosh, M. Iqbal and T. Dagiuklas, "Reliable Resource Provisioning Using Bankers’ Deadlock Avoidance Algorithm in MEC for Industrial IoT," in IEEE Access, vol. 6, pp. 43327-43335, 2018.
516. A. Al-lawati and A. H. Al-Badi, "The impact of cloud computing IT departments: A case study of Oman's financial institutions," 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 2016, pp. 1-10.
517. J. Chakareski, "Joint Source-Channel Rate Allocation and Client Clustering for Scalable Multistream IPTV," in IEEE Transactions on Image Processing, vol. 24, no. 8, pp. 2429-2439, August 2015.
518. Y. Gao, X. Wei, X. Zhang and W. Zhuang, "A Combinational LDA-Based Topic Model for User Interest Inference of Energy Efficient IPTV Service in Smart Building," in IEEE Access, vol. 6, pp. 48921-48933, 2018.
519. T. Guo, C. H. Foh, J. Cai, D. Niyato and E. W. M. Wong, "Performance Evaluation of IPTV Over Wireless Home Networks," in IEEE Transactions on Multimedia, vol. 13, no. 5, pp. 1116-1126, October 2011.
520. M. Li, "Queueing Analysis of Unicast IPTV With Adaptive Modulation and Coding in Wireless Cellular Networks," in IEEE Transactions on Vehicular Technology, vol. 66, no. 10, pp. 9241-9253, October 2017.
521. M. A. Barry, J. K. Tamgno and C. Lishou, "Influence of quality service in IP/MPLS network load with IPTV and VoD services," 2020 22nd International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Korea (South), 2020, pp. 378-385.
522. T. -H. Chao, J. -H. Wu, Y. Chiang and H. -Y. Wei, "5G Edge Computing Experiments with Intelligent Resource Allocation for Multi-Application Video Analytics," 2021 30th Wireless and Optical Communications Conference (WOCC), Taipei, Taiwan, 2021, pp. 80-84
523. X. Jiang, F. R. Yu, T. Song and V. C. M. Leung, "Intelligent Resource Allocation for Video Analytics in Blockchain-Enabled Internet of Autonomous Vehicles With Edge Computing," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14260-14272, August 2022.
524. W. Ma and L. Mashayekhy, "Poster: Adaptive Video Offloading in Mobile Edge Computing," 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS), DC, USA, 2021, pp. 1130-1131.
525. R. Viola, A. Martin, M. Zorrilla and J. Montalbán, "MEC Proxy for Efficient Cache and Reliable Multi-CDN Video Distribution," 2018 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Valencia, Spain, 2018, pp. 1-7.
526. Y. Zhang, J. -H. Liu, C. -Y. Wang and H. -Y. Wei, "Decomposable Intelligence on Cloud-Edge IoT Framework for Live Video Analytics," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8860-8873, September 2020.
527. S. Wang, S. Bi and Y. -J. A. Zhang, "Edge Video Analytics with Adaptive Information Gathering: A Deep Reinforcement Learning Approach," in IEEE Transactions on Wireless Communications.
528. C. -W. Wu et al., "Enhancing Fan Engagement in a 5G Stadium With AI-Based Technologies and Live Streaming," in IEEE Systems Journal, vol. 16, no. 4, pp. 6590-6601, December 2022.
529. M. S. Elbamby, C. Perfecto, M. Bennis and K. Doppler, "Toward Low-Latency and Ultra-Reliable Virtual Reality," in IEEE Network, vol. 32, no. 2, pp. 78-84, March-April 2018.

530. E. S. Goh, M. S. Sunar and A. W. Ismail, "3D Object Manipulation Techniques in Handheld Mobile Augmented Reality Interface: A Review," in IEEE Access, vol. 7, pp. 40581-40601, 2019.
531. Y. K. Dwivedi et al., “Metaverse Beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy,” International Journal of Information Management, vol. 66, October 2022.
532. Y. Li et al., "Collaborative Content Caching and Task Offloading in Multi-access Edge Computing," in IEEE Transactions on Vehicular Technology, 2022.
533. M. E. C. Santos, A. Chen, T. Taketomi, G. Yamamoto, J. Miyazaki and H. Kato, "Augmented Reality Learning Experiences: Survey of Prototype Design and Evaluation," in IEEE Transactions on Learning Technologies, vol. 7, no. 1, pp. 38-56, January-March 2014.
534. S. Qiu, Z. Li, W. He, L. Zhang, C. Yang and C. -Y. Su, "Brain–Machine Interface and Visual Compressive Sensing-Based Teleoperation Control of an Exoskeleton Robot," in IEEE Transactions on Fuzzy Systems, vol. 25, no. 1, pp. 58-69, February 2017.
535. X. Qiao, Y. Huang, S. Dustdar and J. Chen, "6G Vision: An AI-Driven Decentralized Network and Service Architecture," in IEEE Internet Computing, vol. 24, no. 4, pp. 33-40, July-August 2020.
536. X. Qiao, P. Ren, S. Dustdar, L. Liu, H. Ma and J. Chen, "Web AR: A Promising Future for Mobile Augmented Reality—State of the Art, Challenges, and Insights," in Proceedings of the IEEE, vol. 107, no. 4, pp. 651-666, April 2019.
537. K. Cao, Y. Liu, G. Meng and Q. Sun, "An Overview on Edge Computing Research," in IEEE Access, vol. 8, pp. 85714-85728, 2020.
538. S. Bolettieri, D. Thai Bui and R. Bruno, “Towards end-to-end application slicing in Multi-access Edge Computing systems: Architecture discussion and proof-of-concept,” Future Generation Computer Systems, vol. 136, pp. 110-127, November 2022.
539. P. Ranaweera, A. Jurcut and M. Liyanage, “MEC-enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures,” ACM Computing Surveys, vol. 54, no. 9, October 2021.
540. T. W. Nowak et al., "Verticals in 5G MEC-Use Cases and Security Challenges," in IEEE Access, vol. 9, pp. 87251-87298, 2021.
541. P. Ranaweera, A. D. Jurcut and M. Liyanage, "Survey on Multi-Access Edge Computing Security and Privacy," in IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1078-1124, Secondquarter 2021.
542. Y. Hou, S. Garg, L. Hui, D. N. K. Jayakody, R. Jin and M. S. Hossain, "A Data Security Enhanced Access Control Mechanism in Mobile Edge Computing," in IEEE Access, vol. 8, pp. 136119-136130, 2020
543. Y. Kim, J. G. Park and J. -H. Lee, "Security Threats in 5G Edge Computing Environments," 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2020, pp. 905-907.
544. I. H. Abdulqadder and S. Zhou, "SliceBlock: Context-Aware Authentication Handover and Secure Network Slicing Using DAG-Blockchain in Edge-Assisted SDN/NFV-6G Environment," in IEEE Internet of Things Journal, vol. 9, no. 18, pp. 18079-18097, September 2022.
545. S. Liu, C. Zheng, Y. Huang and T. Q. S. Quek, "Distributed Reinforcement Learning for Privacy-Preserving Dynamic Edge Caching," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 3, pp. 749-760, March 2022.
546. M. Maniatakos, "Privilege escalation attack through address space identifier corruption in untrusted modern processors," 2013 8th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS), Abu Dhabi, United Arab Emirates, 2013, pp. 161-166.
547. N. G. Tsoutsos and M. Maniatakos, "Fabrication Attacks: Zero-Overhead Malicious Modifications Enabling Modern Microprocessor Privilege Escalation," in IEEE Transactions on Emerging Topics in Computing, vol. 2, no. 1, pp. 81-93, March 2014.
548. F. Jaafar, G. Nicolescu and C. Richard, "A Systematic Approach for Privilege Escalation Prevention," 2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Vienna, Austria, 2016, pp. 101-108.
549. W. Qiang, J. Yang, H. Jin and X. Shi, "PrivGuard: Protecting Sensitive Kernel Data From Privilege Escalation Attacks," in IEEE Access, vol. 6, pp. 46584-46594, 2018.
550. Z. Zhang, S. Yoon and M. Shin, "The design of graph-based privacy protection mechanisms for mobile systems," 2019 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea (South), 2019, pp. 1-6.
551. Y. Zhang, J. Xiao, S. Hao, H. Wang, S. Zhu and S. Jajodia, "Understanding the Manipulation on Recommender Systems through Web Injection," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3807-3818, 2020.
552. I. Bang, V. A. S. Manya, J. Kim and T. Kim, "On the Effect of Malicious User on D2D Cluster: CSI Forgery and Countermeasures," in IEEE Access, vol. 11, pp. 5517-5527, 2023.
553. H. -B. Ye, H. -Y. Weng and H. C. Jiau, "Exploiting Third-party SDK Sensitive Data Leakage," 2020 International Computer Symposium (ICS), Tainan, Taiwan, 2020, pp. 485-490.
554. X. Yang, W. Luo, L. Zhang, Z. Chen and J. Wang, "Data Leakage Attack via Backdoor Misclassification Triggers of Deep Learning Models," 2022 4th International Conference on Data Intelligence and Security (ICDIS), Shenzhen, China, 2022, pp. 61-66.
555. A. Sivanathan, H. H. Gharakheili and V. Sivaraman, "Detecting Behavioral Change of IoT Devices Using Clustering-Based Network Traffic Modeling," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 7295-7309, August 2020.
556. M. V. K, I. Johnraja Jebadurai, G. J. Leelipushpam Paulraj and J. Jebadurai, "Mitigating Sinkhole attack in RPL based Internet of Things Environment using Optimized K means Clustering technique," 2022 6th International Conference on Electronics, Communication and Aerospace Technology, Coimbatore, India, 2022, pp. 502-507.
557. A. Verma and V. Verma, “Comparative Study of Cloud Computing and Edge Computing: Three Level Architecture Models and Security Challenges,” International Journal of Distributed and Cloud Computing, vol. 9, no. 1, pp. 13-17, September 2021.
558. M. Dulik, "Deploying Fake Network Devices to Obtain Sensitive User Data," 2021 Communication and Information Technologies (KIT), Vysoke Tatry, Slovakia, 2021, pp. 1-5.
559. Y. Lin, Y. Huang, S. -Y. Hsieh, L. Lin and F. Xia, "Layered Malicious Nodes Detection with Graph Attention Network in Human-Cyber-Physical Networks," 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS), Denver, CO, USA, 2022, pp. 523-529.
560. R. K. Varshney and A. K. Sagar, "An Improved AODV Protocol to Detect Malicious Node in Ad hoc Network," 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 2018, pp. 222-227.

561. D. A. Varma and M. Narayanan, "Identifying malicious nodes in Mobile Ad-Hoc Networks using polynomial reduction algorithm," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 2016, pp. 1179-1184.
562. Y. Liu, Y. Peng, B. Wang, S. Yao and Z. Liu, "Review on cyber-physical systems," in IEEE/CAA Journal of Automatica Sinica, vol. 4, no. 1, pp. 27-40, January 2017.
563. A. Humayed, J. Lin, F. Li and B. Luo, "Cyber-Physical Systems Security—A Survey," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802-1831, December 2017.
564. H. Zhang and Z. Li, "Anomaly Detection Approach for Urban Sensing Based on Credibility and Time-Series Analysis Optimization Model," in IEEE Access, vol. 7, pp. 49102-49110, 2019.
565. C. Yang, Z. Shi, H. Zhang, J. Wu and X. Shi, "Multiple Attacks Detection in Cyber-Physical Systems Using Random Finite Set Theory," in IEEE Transactions on Cybernetics, vol. 50, no. 9, pp. 4066-4075, September 2020.
566. M. Barrère et al., "CPS-MT: A Real-Time Cyber-Physical System Monitoring Tool for Security Research," 2018 IEEE 24th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA), Hakodate, Japan, 2018, pp. 240-241.
567. C. K. Keerthi, M. A. Jabbar and B. Seetharamulu, "Cyber Physical Systems(CPS):Security Issues, Challenges and Solutions," 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, India, 2017, pp. 1-4.
568. F. Tang, B. Mao, N. Kato and G. Gui, "Comprehensive Survey on Machine Learning in Vehicular Network: Technology, Applications and Challenges," in IEEE Communications Surveys & Tutorials, vol. 23, no. 3, pp. 2027-2057, thirdquarter 2021.
569. V. Shende, G. Sudi and M. Kulkarni, "Fast cryptanalysis of RSA encrypted data using a combination of mathematical and brute force attack in distributed computing environment," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 2017, pp. 2446-2449.
570. Z. Lu, W. Wang and C. Wang, "On the Evolution and Impact of Mobile Botnets in Wireless Networks," in IEEE Transactions on Mobile Computing, vol. 15, no. 9, pp. 2304-2316, September 2016.
571. M. Idhom, H. E. Wahanani and A. Fauzi, "Network Security System on Multiple Servers Against Brute Force Attacks," 2020 6th Information Technology International Seminar (ITIS), Surabaya, Indonesia, 2020, pp. 258-262.
572. J. Carpenter, J. Layne, E. Serra and A. Cuzzocrea, "Detecting Botnet Nodes via Structural Node Representation Learning," 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 2021, pp. 5357-5364.
573. S. Oba, B. Hu, K. Kamiya and K. Takahashi, "Balanced Score Propagation for Botnet Detection," ICC 2022 - IEEE International Conference on Communications, Seoul, Korea, Republic of, 2022, pp. 2357-2362.
574. S. Lal, T. Taleb and A. Dutta, "NFV: Security Threats and Best Practices," in IEEE Communications Magazine, vol. 55, no. 8, pp. 211-217, August 2017.
575. A. Rehman, S. Alqahtani, A. Altameem and T. Saba, “Virtual Machine Security Challenges: Case Studies,” International Journal of Machine Learning and Cybernetics, vol. 5, pp. 729–742, April 2013.
576. P. Ranaweera, A. D. Jurcut and M. Liyanage, "Realizing Multi-Access Edge Computing Feasibility: Security Perspective," 2019 IEEE Conference on Standards for Communications and Networking (CSCN), Granada, Spain, 2019, pp. 1-7.
577. X. Jin, Q. Wang, X. Li, X. Chen and W. Wang, "Cloud Virtual Machine Lifecycle Security Framework Based On Trusted Computing," in Tsinghua Science and Technology, vol. 24, no. 5, pp. 520-534, October 2019.
578. C. Sharma and S. C. Jain, "Analysis and classification of SQL injection vulnerabilities and attacks on web applications," 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), Unnao, India, 2014, pp. 1-6.
579. M. Khari, Sonam, Vaishali and M. Kumar, "Comprehensive study of web application attacks and classification," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2016, pp. 2159-2164.
580. Mike Chapple; James Michael Stewart; Darril Gibson, "Malicious Code and Application Attacks," in (ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide , Wiley, 2021, pp.993-1040.
581. T. Barabosch and E. Gerhards-Padilla, "Host-based code injection attacks: A popular technique used by malware," 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE), Fajardo, PR, USA, 2014, pp. 8-17.
582. J. N. O.S. and S. M. S. Bhanu, "A Survey on Code Injection Attacks in Mobile Cloud Computing Environment," 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2018, pp. 1-6.
583. M. A. Al-Shareeda, S. Manickam and S. A. Sari, "A Survey of SQL Injection Attacks, Their Methods, and Prevention Techniques," 2022 International Conference on Data Science and Intelligent Computing (ICDSIC), Karbala, Iraq, 2022, pp. 31-35.
584. S. Chowdhury, A. Nandi, M. Ahmad, A. Jain and M. Pawar, "A Comprehensive Survey for Detection and Prevention of SQL Injection," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021, pp. 434-437.
585. B. Gogoi, T. Ahmed and A. Dutta, "Defending against SQL Injection Attacks in Web Applications using Machine Learning and Natural Language Processing," 2021 IEEE 18th India Council International Conference (INDICON), Guwahati, India, 2021, pp. 1-6.
586. J. Wu, K. Ota, M. Dong and C. Li, "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities," in IEEE Access, vol. 4, pp. 416-424, 2016.
587. S. M. Vidhani and A. V. Vidhate, "Security Challenges in 5G Network: A technical features survey and analysis," 2022 5th International Conference on Advances in Science and Technology (ICAST), Mumbai, India, 2022, pp. 592-597.
588. D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang and Z. Han, "Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City," in IEEE Access, vol. 7, pp. 54508-54521, 2019.
589. M. Hachimi, G. Kaddoum, G. Gagnon and P. Illy, "Multi-stage Jamming Attacks Detection using Deep Learning Combined with Kernelized Support Vector Machine in 5G Cloud Radio Access Networks," 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 2020, pp. 1-5.
590. G. Akman, P. Ginzboorg, V. Niemi, “Privacy-Preserving Access for Multi-Access Edge Computing (MEC) Applications,” In Computational Science and Its Applications – ICCSA 2021. ICCSA 2021. Lecture Notes in Computer Science, Springer, Cham.

591. Y. Deng et al., "Resource Provisioning for Mitigating Edge DDoS Attacks in MEC-Enabled SDVN," in IEEE Internet of Things Journal, vol. 9, no. 23, pp. 24264-24280, December 2022.
592. X. Tan, H. Li, L. Wang and Z. Xu, "Global Orchestration of Cooperative Defense against DDoS Attacks for MEC," 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 2019, pp. 1-6.
593. M. H. Khadr, H. B. Salameh, M. Ayyash, H. Elgala and S. Almajali, "Jamming resilient multi-channel transmission for cognitive radio IoT-based medical networks," in Journal of Communications and Networks, vol. 24, no. 6, pp. 666-678, December 2022.
594. J. Galloway, A. White, P. O'Boyle and S. Wyllie, "Poster Abstract: The Impact of DDoS Attack on Docker Containers Compared to Virtual Machines," 2019 IEEE Cloud Summit, Washington, DC, USA, 2019, pp. 122-123.
595. U. Bartwal, S. Mukhopadhyay, R. Negi and S. Shukla, "Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots," 2022 IEEE Conference on Dependable and Secure Computing (DSC), Edinburgh, United Kingdom, 2022, pp. 1-8.
596. Y. Li, R. Hou, K. -S. Lui and H. Li, "An MEC-Based DoS Attack Detection Mechanism for C-V2X Networks," 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6.
597. E. Gyamfi and A. Jurcut, "M-TADS: A Multi-Trust DoS Attack Detection System for MEC-enabled Industrial loT," 2022 IEEE 27th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Paris, France, 2022, pp. 166-172.
598. Y. Deng et al., "Resource Provisioning for Mitigating Edge DDoS Attacks in MEC-Enabled SDVN," in IEEE Internet of Things Journal, vol. 9, no. 23, pp. 24264-24280, December 2022.
599. J. Ali, B. -h. Roh, B. Lee, J. Oh and M. Adil, "A Machine Learning Framework for Prevention of Software-Defined Networking controller from DDoS Attacks and dimensionality reduction of big data," 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2020, pp. 515-519.
600. H. Li and L. Wang, "Online orchestration of cooperative defense against DDoS attacks for 5G MEC," 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 2018, pp. 1-6.
601. D. Dobrin and A. Dimiter, "DDoS attack identification based on SDN," 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA), Boston, MA, USA, 2021, pp. 1-8.
602. M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man In The Middle Attacks," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027-2051, thirdquarter 2016.
603. J. Singh, Y. Bello, A. R. Hussein, A. Erbad and A. Mohamed, "Hierarchical Security Paradigm for IoT Multiaccess Edge Computing," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5794-5805, 1 April1, 2021.
604. R. Du, W. He and J. Tian, "Virtual Machine Security Migration Strategy Based on the Edge Computing Environment," 2020 16th International Conference on Mobility, Sensing and Networking (MSN), Tokyo, Japan, 2020, pp. 803-808.
605. A. S. Khader and D. Lai, "Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol," 2015 22nd International Conference on Telecommunications (ICT), Sydney, NSW, Australia, 2015, pp. 204-208.
606. A. A. M. M. Amin and M. S. Mahamud, "An Alternative Approach of Mitigating ARP Based Man-in-the-Middle Attack Using Client Site Bash Script," 2019 6th International Conference on Electrical and Electronics Engineering (ICEEE), Istanbul, Turkey, 2019, pp. 112-115.
607. S. Chakaravarthi, P. Visu, B. Balu, V. Vineshwaran and M. Yakeshraj, "Web service registration and routing system and inter web proxy service model prevents the message alteration attacks, man-in-the middle attacks," 2017 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 2017, pp. 1-10.
608. Z. Zhang, H. Hasegawa, Y. Yamaguchi and H. Shimada, "Rogue AP Detection using Similarity of Backbone Delay Fluctuation Histogram," 2020 International Conference on Information Networking (ICOIN), Barcelona, Spain, 2020, pp. 239-244.
609. K. Igarashi, H. Kato and I. Sasase, "Rogue Access Point Detection by Using ARP Failure under the MAC Address Duplication," 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Helsinki, Finland, 2021, pp. 1469-1474.
610. G. Zhao, F. Zhang, L. Yu, H. Zhang, Q. Qiu and S. Xu, "Collaborative 5G Multiaccess Computing Security: Threats, Protection Requirements and Scenarios," 2021 ITU Kaleidoscope: Connecting Physical and Virtual Worlds (ITU K), Geneva, Switzerland, 2021, pp. 1-8.
611. M. Abbasi, M. Plaza-Hernández, J. Prieto and J. M. Corchado, "Security in the Internet of Things Application Layer: Requirements, Threats, and Solutions," in IEEE Access, vol. 10, pp. 97197-97216, 2022.
612. A. Samy, I. A. Elgendy, H. Yu, W. Zhang and H. Zhang, "Secure Task Offloading in Blockchain-Enabled Mobile Edge Computing With Deep Reinforcement Learning," in IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 4872-4887, December 2022.
613. P. A. Apostolopoulos, E. E. Tsiropoulou and S. Papavassiliou, "Risk-Aware Data Offloading in Multi-Server Multi-Access Edge Computing Environment," in IEEE/ACM Transactions on Networking, vol. 28, no. 3, pp. 1405-1418, June 2020.
614. W. Lu et al., "Secure NOMA-Based UAV-MEC Network Towards a Flying Eavesdropper," in IEEE Transactions on Communications, vol. 70, no. 5, pp. 3364-3376, May 2022.
615. Q. Xu and P. Ren, "Delay-aware Secure Transmission in MEC-enabled Multicast Network," 2020 IEEE/CIC International Conference on Communications in China (ICCC), Chongqing, China, 2020, pp. 1262-1267.
616. L. Wang, J. Wang, X. Jiang, J. Cui and B. Zheng, "Intelligent Reflective Surface-Assisted MEC Securely Calculates Offloading Policy," 2022 14th International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 2022, pp. 60-65.
617. S. Han et al., "Energy Efficient Secure Computation Offloading in NOMA-Based mMTC Networks for IoT," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5674-5690, June 2019.
618. L. Liu et al., "Blockchain-Enabled Secure Data Sharing Scheme in Mobile-Edge Computing: An Asynchronous Advantage Actor–Critic Learning Approach," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2342-2353, February 2021.
619. B. Liu, J. Song, J. Wang, H. Sun and Q. Wang, "Robust Secure Wireless Powered MISO Cognitive Mobile Edge Computing," in IEEE Access, vol. 8, pp. 62356-62366, 2020.

620. Z. Zhang, Y. Fu, G. Cheng, X. Lan and Q. Chen, "Secure Offloading Design in Multi-user Mobile-Edge Computing Systems," 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS), Chengdu, China, 2021, pp. 695-703.
621. R. Chen et al., "Overview of the Development of Secure Access Service Edge," International Conference On Signal And Information Processing, Networking And Computers, Lecture Notes in Electrical Engineering, vol. 996, pp. 138–145, February 2023.
622. C. Sun, X. Wu, X. Li, Q. Fan, J. Wen and V. C. M. Leung, "Cooperative Computation Offloading for Multi-Access Edge Computing in 6G Mobile Networks via Soft Actor Critic," in IEEE Transactions on Network Science and Engineering.
623. J. Suomalainen, J. Julku, M. Vehkaperä and H. Posti, "Securing Public Safety Communications on Commercial and Tactical 5G Networks: A Survey and Future Research Directions," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1590-1615, 2021.
624. M. A. Lopez, G. N. N. Barbosa and D. M. F. Mattos, "New Barriers on 6G Networking: An Exploratory Study on the Security, Privacy and Opportunities for Aerial Networks," 2022 1st International Conference on 6G Networking (6GNet), Paris, France, 2022, pp. 1-6.
625. S. J. Y. Go, R. Guinto, C. A. M. Feasting, I. Austria, R. Ocampo and W. M. Tan, "An SDN/NFV-Enabled Architecture for Detecting Personally Identifiable Information Leaks on Network Traffic," 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN), Zagreb, Croatia, 2019, pp. 306-311.
626. X. Deng, T. Lv and L. Song, "Novel Efficient Block Chain and Rule-based Intelligent Privacy Share System in Future Network," IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), New York, NY, USA, 2022, pp. 1-8.
627. J. Noh, Y. Kwon, J. Son and S. Cho, "Blockchain-Based One-Time Authentication for Secure V2X Communication Against Insiders and Authority Compromise Attacks," in IEEE Internet of Things Journal, vol. 10, no. 7, pp. 6235-6248, April 2023.
628. Y. Qiu and M. Ma, "A Privacy-Preserving Proximity Testing for Location-Based Services," 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6.
629. Y. Jiang, J. Huang and W. Jin, "The research progress of network intrusion tolerance," International Conference on Cyberspace Technology (CCT 2014), Beijing, 2014, pp. 1-4.
630. B. -Y. Zhang, C. -Z. Wei, X. -H. Yang and B. -B. Song, "Design and implementation of a network based intrusion detection systems," 2018 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), Jinan, China, 2018, pp. 451-454.
631. P. P. Singh and K. Borisagar, "Paging Vulnerabilities in 5G New Radio Networks and Mitigation to Enhance Security Performance," 2022 IEEE World Conference on Applied Intelligence and Computing (AIC), Sonbhadra, India, 2022, pp. 914-918.
632. Z. Wang, "Information Security Risk and Solution of Computer Network under Big Data Background," 2021 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS), Shenyang, China, 2021, pp. 312-314.
633. B. U. I. Khan, F. Anwar, R. F. Olanrewaju, M. L. B. M. Kiah and R. N. Mir, "Game Theory Analysis and Modeling of Sophisticated Multi-Collusion Attack in MANETs," in IEEE Access, vol. 9, pp. 61778-61792, 2021.
634. L. Anda, R. Roštecký and M. Galiński, "Identification of Malicious Behaviour in Content Delivery Network Environment," 2022 International Symposium ELMAR, Zadar, Croatia, 2022, pp. 115-118.
635. X. Li, H.-N. Dai, Y. Wang and H. Wang, "Eavesdropping activities in wireless networks: impact of channel randomness," TENCON 2015 - 2015 IEEE Region 10 Conference, Macao, 2015, pp. 1-4.
636. P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1094-1122, 2021.
637. M. Mulla and S. Sambare, "Efficient analysis of lightweight Sybil attack detection scheme in Mobile Ad hoc Networks," 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 2015, pp. 1-6.
638. S. R. Garzon, H. Yildiz and A. Küpper, "Towards Decentralized Identity Management in Multi-stakeholder 6G Networks," 2022 1st International Conference on 6G Networking (6GNet), Paris, France, 2022, pp. 1-8.
639. D. Xie, J. Yang, W. Bian, F. Chen and T. Wang, "An Improved Identity-Based Anonymous Authentication Scheme Resistant to Semi-Trusted Server Attacks," in IEEE Internet of Things Journal, vol. 10, no. 1, pp. 734-746, January 2023.
640. L. Deng, J. Luo, J. Zhou and J. Wang, "Identity-based Secret Sharing Access Control Framework for Information-Centric Networking," 2020 IEEE/CIC International Conference on Communications in China (ICCC), Chongqing, China, 2020, pp. 507-511.
641. J. -D. Kim, M. Ko and J. -M. Chung, "Novel Analytical Models for Sybil Attack Detection in IPv6-based RPL Wireless IoT Networks," 2022 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2022, pp. 1-3.
642. H. Wang, L. Ma and H. -y. Bai, "A Three-tier Scheme for Sybil Attack Detection in Wireless Sensor Networks," 2020 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, 2020, pp. 752-756.
643. C. -H. Liao, H. -H. Shuai and L. -C. Wang, "Eavesdropping prevention for heterogeneous Internet of Things systems," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2018, pp. 1-2.
644. D. N, S. J and S. P, "Intrusion Detection in Wireless Sensor Networks using Optics Algorithm," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 1265-1272.
645. J. -L. Luo, S. -Z. Yu and S. -J. Peng, "SDN/NFV-Based Security Service Function Tree for Cloud," in IEEE Access, vol. 8, pp. 38538-38545, 2020.
646. I. H. Abdulqadder and S. Zhou, "SliceBlock: Context-Aware Authentication Handover and Secure Network Slicing Using DAG-Blockchain in Edge-Assisted SDN/NFV-6G Environment," in IEEE Internet of Things Journal, vol. 9, no. 18, pp. 18079-18097, September 2022.
647. P. Jiang et al., "Building In-the-Cloud Network Functions: Security and Privacy Challenges," in Proceedings of the IEEE, vol. 109, no. 12, pp. 1888-1919, December 2021.
648. P. K. Thiruvasagam, A. Chakraborty, A. Mathew and C. S. R. Murthy, "Reliable Placement of Service Function Chains and Virtual Monitoring Functions With Minimal Cost in Softwarized 5G Networks," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1491-1507, June 2021.
649. L. Fawcett, S. Scott-Hayward, M. Broadbent, A. Wright and N. Race, "Tennison: A Distributed SDN Framework for Scalable Network Security," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 12, pp. 2805-2818, December 2018.

650. J. H. Cox et al., "Advancing Software-Defined Networks: A Survey," in IEEE Access, vol. 5, pp. 25487-25526, 2017.
651. G. S. Chawla et al., "VMGuard: State-Based Proactive Verification of Virtual Network Isolation With Application to NFV," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 4, pp. 1553-1567, July-August 2021.
652. X. Lu, X. Wan, L. Xiao, Y. Tang and W. Zhuang, "Learning-Based Rogue Edge Detection in VANETs with Ambient Radio Signals," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 1-6.
653. M. Shamseddine, W. Itani, A. Al-Dulaimy and J. Taheri, "Mitigating Rogue Node Attacks in Edge Computing," 2019 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Manama, Bahrain, 2019, pp. 1-6.
654. Z. M. Fadlullah, B. Mao and N. Kato, "Balancing QoS and Security in the Edge: Existing Practices, Challenges, and 6G Opportunities With Machine Learning," in IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2419-2448, Fourthquarter 2022.
655. T. Pourhabibi, K. -L. Ong, B. H. Kam and Y. L. Boo, “Fraud detection: A systematic literature review of graph-based anomaly detection approaches,” Decision Support Systems, vol. 133, June 2020.
656. R. V, S. K. R, M. V, S. M. M and M. B, "Fraudulent Information Prediction using Block Chain Technology and Machine Learning," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 1319-1325.
657. J. Zhang, B. Chen, X. Cheng, H. T. T. Binh and S. Yu, "PoisonGAN: Generative Poisoning Attacks Against Federated Learning in Edge Computing Systems," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3310-3322, March 2021.
658. B. Gopinath and B. Latha, "Restriction of Forgery Attacks using AntiForgery Token in Machine Learning," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2021, pp. 1-4.
659. C. -W. Tsou, Y. -W. Ma, Y. -H. Tu and J. -L. Chen, "Security Assist Mechanisms for Industrial Control Systems with Authentication," 2023 25th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, Republic of, 2023, pp. 186-188.
660. T. Kaur, A. Girdhar and G. Gupta, "A Robust Algorithm for the Detection of Cloning Forgery," 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, 2018, pp. 1-6.
661. H. Zhang and M. Li, "Multi-round Data Poisoning Attack and Defense against Truth Discovery in Crowdsensing Systems," 2022 23rd IEEE International Conference on Mobile Data Management (MDM), Paphos, Cyprus, 2022, pp. 109-118.
662. M. Xu, "FedDBG: Privacy-Preserving Dynamic Benchmark Gradient in Federated Learning Against Poisoning Attacks," 2022 International Conference on Networking and Network Applications (NaNA), Urumqi, China, 2022, pp. 483-488.
663. Y. Zou and J. Zhu, "Intercept Probability Analysis of Joint User-Jammer Selection against Eavesdropping," 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 2016, pp. 1-6.
664. H. Kim and J. Hur, "PCIe Side-channel Attack on I/O Device via RDMA-enabled Network Card," 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, 2022, pp. 1468-1470.
665. H. Gupta et al., "Impact of Side Channel Attack in Information Security," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2019, pp. 291-295.
666. A. Albalawi, V. Vassilakis and R. Calinescu, "Side-channel Attacks and Countermeasures in Cloud Services and Infrastructures," NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 2022, pp. 1-4.
667. H. Wang, H. Sayadi, G. Kolhe, A. Sasan, S. Rafatirad and H. Homayoun, "Phased-Guard: Multi-Phase Machine Learning Framework for Detection and Identification of Zero-Day Microarchitectural Side-Channel Attacks," 2020 IEEE 38th International Conference on Computer Design (ICCD), Hartford, CT, USA, 2020, pp. 648-655.
668. S. Bhasin, D. Jap and S. Picek, "On (in)Security of Edge-based Machine Learning Against Electromagnetic Side-channels," 2022 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI), Spokane, WA, USA, 2022, pp. 262-267.
669. H. Wang et al., "Evaluation of Machine Learning-based Detection against Side-Channel Attacks on Autonomous Vehicle," 2021 IEEE 3rd International Conference on Artificial Intelligence Circuits and Systems (AICAS), Washington DC, DC, USA, 2021, pp. 1-4.
670. D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain," in IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11743-11757, July 2021.
671. Z. Zhang, G. Huang, S. Hu, W. Zhang, Y. Wu and Z. Qin, "FDO-ABE: A Fully Decentralized Lightweight Access Control Architecture for Mobile Edge Computing," 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS), Chengdu, China, 2021, pp. 193-198.
672. P. Sun, L. Luo, S. Liu and W. Wu, "Adaptive Rule Engine for Anomaly Detection in 5G Mobile Edge Computing," 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C), Macau, China, 2020, pp. 690-691.
673. R. A. Mishra, A. Kalla, K. Shukla, A. Nag and M. Liyanage, "B-VNF: Blockchain-enhanced Architecture for VNF Orchestration in MEC-5G Networks," 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 2020, pp. 229-234.
674. Amith Raj MP, A. Kumar, S. J. Pai and A. Gopal, "Enhancing security of Docker using Linux hardening techniques," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, India, 2016, pp. 94-99.
675. M. J. Gul, R. Rabia, Y. Jararweh, M. M. Rathore and A. Paul, "Security Flaws of Operating System Against Live Device Attacks: A case study on live Linux distribution device," 2019 Sixth International Conference on Software Defined Systems (SDS), Rome, Italy, 2019, pp. 154-159.
676. C. B. Canto, P. J. Roig, S. Filiposka, S. A. Carrasco and K. Gilly, "Challenges of Implementing NFV-based Multi-Access Edge Computing Environments," 2021 29th Telecommunications Forum (TELFOR), Belgrade, Serbia, 2021, pp. 1-4.
677. M. Masoumi et al., "Dynamic Online VNF Placement with Different Protection Schemes in a MEC Environment," 2022 32nd International Telecommunication Networks and Applications Conference (ITNAC), Wellington, New Zealand, 2022, pp. 1-6.
678. M. Huang, W. Liang, X. Shen, Y. Ma and H. Kan, "Reliability-Aware Virtualized Network Function Services Provisioning in Mobile Edge Computing," in IEEE Transactions on Mobile Computing, vol. 19, no. 11, pp. 2699-2713, November 2020.
679. Z. Zhang, Z. Xu, G. Wu, J. Wang, H. Ren and G. Yuan, "Trust-Aware Service Chaining in Mobile Edge Clouds with VNF Sharing," 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Dalian, China, 2021, pp. 410-415.

680. L. F. Eliyan and R. D. Pietro, “DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges,” Future Generation Computer Systems, vol. 122, pp. 149-171, September 2021.
681. R. Vilalta et al., "TeraFlow: Secured Autonomic Traffic Management for a Tera of SDN flows," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 2021, pp. 377-382.
682. J. Szefer, P. Jamkhedkar, Yu-Yuan Chen and R. B. Lee, "Physical attack protection with human-secure virtualization in data centers," IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN 2012), Boston, MA, USA, 2012, pp. 1-6.
683. M. Tiwary, S. Sharma, P. Mishra, H. El-Sayed, M. Prasad and D. Puthal, "Building Scalable Mobile Edge Computing by Enhancing Quality of Services," 2018 International Conference on Innovations in Information Technology (IIT), Al Ain, United Arab Emirates, 2018, pp. 141-146.
684. S. Koteshwara, "Security Risk Assessment of Server Hardware Architectures Using Graph Analysis," 2021 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Shanghai, China, 2021, pp. 1-4.
685. P. Angin, B. Bhargava and R. Ranchal, "Tamper-resistant autonomous agents-based mobile-cloud computing," NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, 2016, pp. 843-847.
686. H. Chae, C. S. Lee and T. H. Kim, "The Anti-tampering Process and Case Study by the Operating Mode of Various Unmanned Ground Vehicles," 2018 IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM), Auckland, New Zealand, 2018, pp. 1432-1437.
687. S. N. Shirazi, A. Gouglidis, A. Farshad and D. Hutchison, "The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective," in IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2586-2595, November 2017.
688. R. Artych et al., "Security Constraints for Placement of Latency Sensitive 5G MEC Applications," 2022 9th International Conference on Future Internet of Things and Cloud (FiCloud), Rome, Italy, 2022, pp. 40-45.
689. Z. Riaz, F. Dürr and K. Rothermel, "Location Privacy and Utility in Geo-social Networks: Survey and Research Challenges," 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, Ireland, 2018, pp. 1-10.
690. M. AlShalaan, R. AlSubaie and R. Latif, "Location Privacy Issues in Location-Based Services," 2022 Fifth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU), Riyadh, Saudi Arabia, 2022, pp. 129-132
691. X. Zhang, Q. Jia and L. Guo, "Secure and optimized unauthorized secondary user detection in dynamic spectrum access," 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 2017, pp. 1-9.
692. N. Y. Yu, "Performance Analysis of Signature-Based Grant-Free Random Access Under Impersonation Attacks," in IEEE Access, vol. 10, pp. 72925-72935, 2022.
693. W. Wang, S. Ge and X. Zhou, "Location-Privacy-Aware Service Migration in Mobile Edge Computing," 2020 IEEE Wireless Communications and Networking Conference (WCNC), Seoul, Korea (South), 2020, pp. 1-6.
694. P. Guo, B. Ye, Y. Chen, T. Li, Y. Yang and X. Qian, "A location data protection protocol based on differential privacy," 2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), AB, Canada, 2021, pp. 306-311.
695. G. Cui, Q. He, F. Chen, H. Jin, Y. Xiang and Y. Yang, "Location Privacy Protection via Delocalization in 5G Mobile Edge Computing Environment," in IEEE Transactions on Services Computing, vol. 16, no. 1, pp. 412-423, January-February 2023.
696. T. He, E. N. Ciftcioglu, S. Wang and K. S. Chan, "Location Privacy in Mobile Edge Clouds: A Chaff-Based Approach," in IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2625-2636, November 2017.
697. J. Yu, "Design of Location Security Protection System Based on Internet of Things," 2022 4th International Conference on Applied Machine Learning (ICAML), Changsha, China, 2022, pp. 273-276.
698. S. -M. Cheng, B. -K. Hong and C. -F. Hung, "Attack Detection and Mitigation in MEC-Enabled 5G Networks for AIoT," in IEEE Internet of Things Magazine, vol. 5, no. 3, pp. 76-81, September 2022.
699. T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily and Y. Jararweh, "Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain Based Solutions," in IEEE Access, vol. 7, pp. 79694-79713, 2019.
700. G. Costantino, M. De Vincenzi, F. Martinelli and I. Matteucci, "A Privacy-Preserving Solution for Intelligent Transportation Systems: Private Driver DNA," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 1, pp. 258-273, January 2023.
701. X. Shu, D. Yao and E. Bertino, "Privacy-Preserving Detection of Sensitive Data Exposure," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 5, pp. 1092-1103, May 2015.
702. B. Hauer, "Data and Information Leakage Prevention Within the Scope of Information Security," in IEEE Access, vol. 3, pp. 2554-2565, 2015.
703. X. He, R. Jin and H. Dai, "Deep PDS-Learning for Privacy-Aware Offloading in MEC-Enabled IoT," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4547-4555, June 2019.
704. M. Sato, R. Nakamura, T. Yamauchi and H. Taniguchi, "Improving Transparency of Hardware Breakpoints with Virtual Machine Introspection," 2022 12th International Congress on Advanced Applied Informatics (IIAI-AAI), Kanazawa, Japan, 2022, pp. 113-117.
705. F. Rocha, T. Gross and A. V. Moorsel, "Defense-in-Depth Against Malicious Insiders in the Cloud," 2013 IEEE International Conference on Cloud Engineering (IC2E), San Francisco, CA, USA, 2013, pp. 88-97.
706. A. K. Chaturvedi, P. Kumar and K. Sharma, "Proposing Innovative Intruder Detection System for Host Machines in Cloud Computing," 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India, 2020, pp. 292-296.
707. P. Sheinidashtegol and M. Galloway, "Performance Impact of DDoS Attacks on Three Virtual Machine Hypervisors," 2017 IEEE International Conference on Cloud Engineering (IC2E), Vancouver, BC, Canada, 2017, pp. 204-214.
708. R. Aishwarya and S. Malliga, "Intrusion detection system- An efficient way to thwart against Dos/DDos attack in the cloud environment," 2014 International Conference on Recent Trends in Information Technology, Chennai, India, 2014, pp. 1-6.

709. A. K. Singh, R. K. Jaiswal, K. Abdukodir and A. Muthanna, "ARDefense: DDoS detection and prevention using NFV and SDN," 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Brno, Czech Republic, 2020, pp. 236-241.
710. A. Aljuhani and T. Alharbi, "Virtualized Network Functions security attacks and vulnerabilities," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2017, pp. 1-4.
711. H. w. Baek, A. Srivastava and J. V. d. Merwe, "CloudVMI: Virtual Machine Introspection as a Cloud Service," 2014 IEEE International Conference on Cloud Engineering, Boston, MA, USA, 2014, pp. 153-158.
712. D. Kim and S. An, "Efficient and scalable public key infrastructure for wireless sensor networks," The 2014 International Symposium on Networks, Computers and Communications, Hammamet, Tunisia, 2014, pp. 1-5.
713. J. Zhang, M. Wu, Q. Zhang and C. Peng, "A lightweight Data Sharing Scheme with Resisting Key Abuse in Mobile Edge Computing," IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 2021, pp. 1-6.
714. K. Kaur, S. Garg, G. Kaddoum, M. Guizani and D. N. K. Jayakody, "A Lightweight and Privacy-Preserving Authentication Protocol for Mobile Edge Computing," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6.
715. A. Alabdulatif, I. Khalil and X. Yi, “Towards Secure Big Data Analytic for Cloud-Enabled Applications with Fully Homomorphic Encryption,” Journal of Parallel and Distributed Computing, vol. 137, pp. 192-204, March 2020.
716. F. Tang, X. Chen, M. Zhao and N. Kato, "The Roadmap of Communication and Networking in 6G for the Metaverse," in IEEE Wireless Communications.
717. H. Li, S. Ci, C. Yang, X. Tan, S. Hou and Z. Wang, "Moving to Green Edges: A Cooperative MEC Framework to Reduce Energy Demand of Clouds," 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 2019, pp. 1-6.
718. D. Wang, X. Tian, H. Cui and Z. Liu, "Reinforcement learning-based joint task offloading and migration schemes optimization in mobility-aware MEC network," in China Communications, vol. 17, no. 8, pp. 31-44, August 2020.
719. T. M. Ho and K. -K. Nguyen, "Joint Server Selection, Cooperative Offloading and Handover in Multi-Access Edge Computing Wireless Network: A Deep Reinforcement Learning Approach," in IEEE Transactions on Mobile Computing, vol. 21, no. 7, pp. 2421-2435, July 2022.
720. J. Du et al., "Resource Pricing and Allocation in MEC Enabled Blockchain Systems: An A3C Deep Reinforcement Learning Approach," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 1, pp. 33-44, January-February 2022
721. T. X. Tran, A. Hajisami, P. Pandey and D. Pompili, "Collaborative Mobile Edge Computing in 5G Networks: New Paradigms, Scenarios, and Challenges," in IEEE Communications Magazine, vol. 55, no. 4, pp. 54-61, April 2017.
722. P. Shantharama, A. S. Thyagaturu, N. Karakoc, L. Ferrari, M. Reisslein and A. Scaglione, "LayBack: SDN Management of Multi-Access Edge Computing (MEC) for Network Access Services and Radio Resource Sharing," in IEEE Access, vol. 6, pp. 57545-57561, 2018.
723. J. Li et al., "Budget-Aware User Satisfaction Maximization on Service Provisioning in Mobile Edge Computing," in IEEE Transactions on Mobile Computing, 2022.
724. J. Singh, Y. Bello, A. R. Hussein, A. Erbad and A. Mohamed, "Hierarchical Security Paradigm for IoT Multiaccess Edge Computing," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5794-5805, April 2021.
725. F. D. Rango, G. Potrino, M. Tropea and P. Fazio, “Energy-Aware Dynamic Internet of Things Security System Based on Elliptic Curve Cryptography and Message Queue Telemetry Transport Protocol for Mitigating Replay Attacks,” Pervasive and Mobile Computing, vol. 61, January 2020.
726. Y. Li, Y. Yu, W. Susilo, Z. Hong and M. Guizani, "Security and Privacy for Edge Intelligence in 5G and Beyond Networks: Challenges and Solutions," in IEEE Wireless Communications, vol. 28, no. 2, pp. 63-69, April 2021.
727. F. Salahdine, T. Han and N. Zhang, “Security in 5G and Beyond Recent Advances and Future Challenges,” Security and Privacy, September 2022.
728. H. Peng, H. Wu and X. S. Shen, "Edge Intelligence for Multi-Dimensional Resource Management in Aerial-Assisted Vehicular Networks," in IEEE Wireless Communications, vol. 28, no. 5, pp. 59-65, October 2021.
729. J. Liu et al., “A Data-Driven Parallel Adaptive Large Neighborhood Search Algorithm for a Large-Scale Inter-Satellite Link Scheduling Problem,” Swarm and Evolutionary Computation, vol. 74, October 2022.
730. S. Bonafini, C. Sacchi, F. Granelli, R. Bassoli, F. H. P. Fitzek and K. Kondepu, "3D Cloud-RAN Functional Split to Provide 6G Connectivity on Mars," 2022 IEEE Aerospace Conference (AERO), Big Sky, MT, USA, 2022, pp. 1-13.
731. N. Cheng et al., “6G Service-Oriented Space-Air-Ground Integrated Network: A Survey,” Chinese Journal of Aeronautics, vol. 35, no. 9, pp. 1-18, September 2022.
732. F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji and V. C. M. Leung, "Enabling Massive IoT Toward 6G: A Comprehensive Survey," in IEEE Internet of Things Journal, vol. 8, no. 15, pp. 11891-11915, August 2021.
733. J. Mills, J. Hu and G. Min, "Multi-Task Federated Learning for Personalised Deep Neural Networks in Edge Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 33, no. 3, pp. 630-641, March 2022.
734. P. K. Mu, J. Zheng, T. H. Luan, L. Zhu, Z. Su and M. Dong, "AMIS-MU: Edge Computing Based Adaptive Video Streaming for Multiple Mobile Users," in IEEE Transactions on Mobile Computing.
735. Z. Ming et al., "Edge-Based Video Surveillance With Graph-Assisted Reinforcement Learning in Smart Construction," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9249-9265, June 2022.
736. X. Zhou, W. Liang, J. She, Z. Yan and K. I. -K. Wang, "Two-Layer Federated Learning With Heterogeneous Model Aggregation for 6G Supported Internet of Vehicles," in IEEE Transactions on Vehicular Technology, vol. 70, no. 6, pp. 5308-5317, June 2021.
737. S. Yu, X. Chen, Z. Zhou, X. Gong and D. Wu, "When Deep Reinforcement Learning Meets Federated Learning: Intelligent Multitimescale Resource Management for Multiaccess Edge Computing in 5G Ultradense Network," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2238-2251, February 2021.