Realizing contact-less applications with Multi-Access Edge Computing

Pasika Ranaweera[a,*], Chamitha de Alwis[b], Anca D. Jurcut[a], Madhusanka Liyanage[a,c]

[a] School of Computer Science, University College Dublin (UCD), Ireland
[b] Department of Electrical and Electronic Engineering, University of Sri Jayewardeneprua, Sri Lanka
[c] Centre for Wireless Communications, University of Oulu, Finland

Abstract

The entire world progression has ceased with the unexpected outbreak of the COVID-19 pandemic, and urges the requirement for contact-less and autonomous services and applications. Realizing these predominantly Internet of Things (IoT) based applications demands a holistic pervasive computing infrastructure. In this paper, we conduct a survey to determine the possible pervasive approaches for utilizing the Multi-Access Edge Computing (MEC) infrastructure in realizing the requirements of emerging IoT applications. We have formalized specific architectural layouts for the considered IoT applications, while specifying network-level requirements to realize such approaches; and conducted a simulation to test the feasibility of proposed MEC approaches.
© 2022 The Author(s). Published by Elsevier B.V. on behalf of The Korean Institute of Communications and Information Sciences. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Keywords: Contact-less; COVID-19; MEC; IoT; IoMT; Low-latency; AR; VR

Contents

* Corresponding author.
E-mail addresses: pasika.ranaweera@ucdconnect.ie (P. Ranaweera), chamitha@sjp.ac.lk (C. de Alwis), anca.jurcut@ucd.ie (A.D. Jurcut), madhusanka@ucd.ie, madhusanka.liyanage@oulu.fi (M. Liyanage).

1. Introduction

The COVID-19 pandemic has led us to realize that prevailing knowledge, methodologies, technologies, or facilities are not adequate to mitigate the impact it caused. Though there are few promising vaccines been introduced by reputable pharmaceutical institutions, their effectiveness is still in a questionable state in light of the new mutated strains of the pathogen. The level of contagiousness characterized by the stealthy transmission of COVID-19 has led to develop novel means of human interaction methods to mitigate its spread. For this, Internet of Things (IoT) concept plays a key role in accomplishing such strategies. Already established IoT devices, protocols, and frameworks along with the standardization institutions are paving the most feasible digital infrastructure to find solutions for the current dilemma. In addition, the 'Smart City' concept aligned with IoT guarantees the coverage of all essential aspects of urban development for such digital solutions. Though, a digital infrastructure alone is not sufficient to meet the current demands. A pervasive or ubiquitous computing capability is an intrinsic aspect; where edge computing paradigms are capable of facilitating. In the pandemics' context, Internet of Medical Things (IoMT) directives are the most essential to deploy medical services featured with contact-less patient inspection, sample extraction, treatment, and monitoring methods. Infact, the digital IoMT infrastructure that interconnects all the medical appliances within a medical vicinity are improving the integration capability of novel requirements for contact-less practices [1].

It is obvious that accustoming into a contact-less and confined daily routine that circumvents the tensity and anxiety require the usage of technology from the consumer perspective. Such adaptability is not only limited to healthcare, but for entertainment, occupation, trading, fashion, and education. Eventhough the current technology offer remote access to resources, online video conferencing facilities, online collaborative platforms, support for smart sensory and actuator devices are sufficient for the time being, would not scale with the demand for the digital services in the future. As IoT based services are employing devices that are limited on resources, their advancement is depended on the offloading capability, where resource consuming processing phase of their operation is performed in an outsourced manner at a third-party infrastructure. Further, most emerging services are not designed to operate stand-alone; require real-time and all-time connectivity to their respective servers or control stations to maintain their pervasive features along with monitoring capability. Thus, the most lacking aspect for contact-less and

pervasive digital solutions is the existing networking infrastructure, where every emerging application or service demands enormous bandwidths with extremely low latency to maintain their operation online without interruption. Conversely, industries and critical infrastructure are heavily relying on the emerging fifth generation (5G) related technological advancements for enabling the contact-less operating services for improving the current networking infrastructure.

Emerging directives of Augmented Reality (AR), Virtual Reality (VR), Ultra Reliable Low Latency Communication (URLLC), enhanced Mobile BroadBand (eMBB), and massive Machine Type Communication (mMTC) are essential to contrive the digital infrastructure intrinsic to enable envisaged use cases [2]. Though, service requisites demanded by these novel concepts, specially the ubiquitous computing capability; are inconceivable with the prevailing networking infrastructure that complemented through cloud computing based services. The emergent edge computing paradigm Multi-Access Edge Computing (MEC) attributes the capability to overcome the stated pitfalls of cloud computing. MEC platforms established at mobile base stations are capable of provisioning dynamic services at a proximate locality. With these decentralized server placements, location and context awareness are possible while ultra-low-latency, higher bandwidth, security, and privacy aspects are enhanced to cater novel service specifications.

The edge infrastructure of the MEC is structured with virtualized entities of Mobile Edge Hosts (MEHs) that operate as Virtual Machines (VMs), while Mobile Edge Platform Manager (MEPM) and Virtualization Infrastructure Manager (VIM) are acting as the orchestrator and the hypervisor for the MEC platform as explicated in [3]. Further, cloud deployments are enduring unintended latency due to its centralized nature with globally dispersed server placements. This service model is not optimal for Internet of Things (IoT) based services that attribute higher heterogeneity. Thus, an alternative service model is intrinsic to improve the pragmatic feasibility of the nascent technologies.

In this article, we investigate the possibility for launching various IoT technologies, utilizing the edge computing capabilities of the MEC paradigm through a state-of-the-art review of the existing work; that serves as a position paper for contactless pervasive strategies. In fact, findings of this research aids to realize the use cases specified in Section 2. Section 3 states various driving technologies enabled by MEC, while Section 4 discusses the realization of the stated use cases in the context of MEC standardization. Validating the MEC capability in contrast to cloud computing deployments is presented in Section 5. Section 6 concludes the article.

2. Emerging IoT contact-less use cases

Smart City paradigm and IoT play a vital role in enabling new services of contact-less nature. Though, the coverage of Smart City is wider, and the context of this paper narrows to contact-less possibilities to mitigate the concerns with the pandemic. This section explains some of such important IoT based cases that falls under the umbrella of Smart City. The selected use cases are direct contributors for overcoming the issues of COVID-19, through aiding to develop effective and efficient contact-less practices.

2.1. Smart hospitals

The hospitals and other health care facilities are the most lacking and unprepared vicinity's to face this pandemic. Means of implementing contact-less practices in general can be achieved with social distancing and circumspect handling of materials or items. Though, transforming patient inspection, consulting, laboratory sample collection, conducting experiments, surgeries, and patient caring activities to be contact-less is proving to be arduous with existing technologies, and require IoMT directives to succeed. Robotics are engaged to revitalize these requirements by means of clinical care, logistics, and reconnaissance. Utilization of AR has been envisaged for Robot Assisted Surgeries (RASs). Further, remote patient caring can be accomplished with robotic engagement while patients can be monitored remotely via visual and audible means with embedding IoT devices in to their medical beds. The vital medical data aggregated during monitoring, performing clinical tests, and laboratory experiments are managed by information systems catered for big data requirements in state-of-the-art hospitals. Reaching the stated advancements within a hospital premises however, is infeasible at present in a technological perspective [4].

Existing Challenges: The medical apparatus market is a well-established, and exorbitant trade that involve plethora of manufacturers with a highly scaled design range. Thus, following challenges should be answered to pragmatically launching this concept.

- Minimizing latency of the existing network infrastructure to cater services as RASs.
- Compatibility and inter-operability issues associated with the employed sensory, haptic, laboratory-measuring, audio-visual, and robotic appliances.
- Robotic entanglements introduce the 'Robot Ethics' consensus to medical applications; where ethical legislation's should be clearly specified due to human subjects.
- Securing personal health information while preserving privacy of patients.
- Restriction of the envisioned advancements due to excessive regulations and standardization.

2.2. Smart factories

With the COVID-19 outbreak, factories have faced significant operational challenges, resulting in temporarily shutting down their operation due to strict social distancing measures. Thus, contact-less and autonomous approaches are quite essential to industries for seamless operation, and for minimizing human involvement that offers a solution for both social distancing and for work force minimization. Such pervasive approaches are quite adoptable for Industrial IoT (IIoT) through robotic intervention [5]. This can facilitate full or partial operations of factories, especially the IoMT supply chains to facilitate the continuous manufacturing and dispersion of COVID-19 vaccines and devices. Sensors can be used to monitor different conditions and the operation in the Factory environment, report events, and trigger alarms in an Industry 4.0 smart manufacturing environment. The Digital Twin (DT) concept can be used to create a digital factory environment to operate, monitor and optimize the production chain while continuously collecting and processing data. AR based collaborative tools can be used for remote maintenance and operation of industrial equipment. The smart factory environment can also be extended to have interactive interfaces that facilitates business management, human resource and infrastructure management, and security control.

Existing Challenges: Several challenges need to be addressed in order to facilitate smart factories to combat the COVID-19 pandemic.

- Connect all the machinery, sensors, and actuators to be cyber–physical systems to an IoT network.
- Facilitate an extremely dense network of IoT devices.
- Minimize End-to-End (E2E) delays to about 1 ms to support autonomous control, remote control and actuation.
- Provide extremely reliable wireless communication between IoT devices (over 99.999%).
- Support ultra low-delay and high-bandwidth access to powerful cloud computing services analyze *Small Data* and *Big Data* gathered through large number of IoT sensors and devices.
- Ensure the security of sensitive data and business secrets while maintaining the privacy of online connected workforce.

2.3. Consumer trading

Digitization of economic trading is identified as a pivotal aspect for overcoming the restrictions imposed by COVID-19 on consumer trading. For instance, grocery based e-commerce has incremented up to 74% during the pandemic, while platforms such as Amazon have increased their sales in new product ranges including habitual commodities [6]. To facilitate this trend, existing trading platforms should realize a transformation towards digital product presentation, marketing, sales, supply chain management, and delivery. For instance, virtual shopping malls should provide facilitated with a simulated experience resembling the actual visualization, tangibility, and mechanics of the product through VR/AR with haptic feedback. This requires data collected through numerous sensors to harness powerful edge computing capabilities to provide a realistic shopping experience. Furthermore, intelligent payment solutions, smart vending machines,

and smart shelves can also be implemented as possible solutions. Unmanned Aerial Vehicles (UAVs) are quite popular with emerging delivery systems as they are contact-less and reduces the human workforce requirement. Similarly, other consumer trading sectors such as fashion industry, architecture, real estate, and restaurants can also benefit from using numerous IoT devices and MEC to provide digitized consumer trading experiences during the pandemic.

Existing Challenges:

Realizing a fully functional IoT based digitized consumer trading platform requires addressing a number of challenges, as listed below.

- Efficiently communicate multiple data streams obtained through numerous IoT sensors in real-time.
- Store and process multiple data streams in real-time to provide a comprehensive and realistic VR/AR based shopping experience.
- Process large amounts of *Small Data* as well as *Big Data* to obtain meaningful insights for user profiling, marketing and providing a customized user experience.
- Offload computationally intensive tasks of resource constrained user devices.
- Ensure the security and privacy of consumer data and information.

2.4. Contact tracing

Apart from vaccination, the most effective ways of preventing the spread of the SARS-CoV-2 virus and a rise in disease are non-pharmaceutical methods such as social distancing and isolation. The virus has an average incubation period from infection to symptoms of approximately 5.2 days and it is estimated that approximately 50% of infections are asymptomatic [7,8]. To contain this infection, it is vital to be able to effectively and rapidly identify all social interactions during the infectious period and enable proper contact tracing. This is especially relevant to healthcare workers, who are hypothesized to be at an increased risk of severe disease due to higher viral load exposure and their potentially close contact with infected individuals. Gadgets (i.e. IoT wearable, mobile devices and dedicated IoT devices) based Contact tracing enables authorities to identify individuals that have a high risk of spreading the virus and to subsequently encourage them to self isolate to limit the spread of the virus. In addition, UAVs can be employed to conduct city-wide surveillance for detecting any lockdown violations.

Existing Challenges:

The efficient deployment of IoT based contact tracing requires to address few challenges as listed below.

- People want to keep their location and movement information private without over seen by authorities
- The use cloud based system to store collected IoT location data could raise privacy concerns
- Storing row contact tracing information and processing of information at the cloud will increase the probability of cyber attacks and operational cost.

2.5. Working from home and online education

COVID-19 has imposed restrictions across over 185 countries. Businesses are asking employees to work from home, while the schools and university are resorted to online learning. The IoT plays a crucial role in connecting businesses and employees and respectively, e-learning and students in recent years. Most of the remote work and education requires internet connected devices such as laptops, mobile phones, webcams and microphones. According to UNESCO, over 1.57 billion learners which represent about 89.4% of total registered learners are affected [9]. The pandemic opened a new opportunity for institutions — most of the universes and institutions over the world replaced the classroom teaching with e-learning [10]. All these sectors are seeking new methods and technologies to seamlessly continue their usual operations as normal, while working remotely and practicing e-learning. All these sudden changes are over-stressing the network since the functionally of these sectors are now depend mainly on both wired and wireless communication networks to remain in operation [11].

Existing Challenges: Working from home and e-learning are bringing new challenges that impact their feasibility and quality including:

- A great increase in the use of online learning platforms, social media platforms and XR applications (virtual laboratories), causing a surge in traffic demand on the existing networks.
- Due to the stay-at-home policy, there is also a sudden shift in the traffic demand pattern from city centers to the residential areas.
- Working from home policy has increased the risk exposure of insider threats, since the individuals are a potential weak factor in preserving security and privacy.
- Employees could boost incident rates through eagerness to prove their effectiveness working from home by bypassing policy or operating under less restricted parameters.
- New intelligent service to identify the speaker, live transcription, better virtual whiteboards, background noise and visual distractions need to be addressed for work and education from home. New algorithms to improve these capabilities will be important.

3. MEC based services for IoT/IoMT

MEC can realize new services which can be integrated with IoT/IoMT applications to mitigate their challenges and improve the performance, specially in the pervasive context. This section explains some of such important services related to IoT/IoMT applications.

The requirements for each application discussed in this section are specified in Table 1.

3.1. Efficient augmented reality

AR is one of the prominent wearable based service used in many IoT applications. For AR based processing, MEC

Table 1
Requirements on the networking perspective for realization of the proposed use cases [12–14].

MEC based application or service	Requirements						
	End-to-End Latency	Jitter	Packet Loss Rate	Bandwidth/ Bit rate	Availability	Max. # of UEs	Security Level
Augmented Reality							
Stereoscopic 4K (3840x2160 pixels) 120 fps real-time video stream	< 1 ms	< 10μs	10^{-3}	> 24 Gbps	>99.99999%	1	MEDIUM
4K 120 fps real-time video stream with lossless compression	< 50 ms	< 2 ms	10^{-3}	> 12 Gbps	>99.99999%	10	MEDIUM
Robot Telemetry / Motion control data stream	< 2 ms	< 2 ms	10^{-4}	> 16 Mbps	>99.999999%	10	HIGH
Haptic Feedback data stream	< 2 ms	< 2 ms	10^{-4}	> 16 Mbps	>99.999999%	1	MEDIUM
Low-Latency Communication							
URLLC channel	< 0.5 ms	< 100μs	10^{-4}	> 2 Mbps	>99.99%	1	LOW
Offloading							
Less critical offloading channel	< 20 ms	< 2 ms	10^{-4}	> 2 Mbps	>99.99%	1	MEDIUM
Command and control data stream	< 2 ms	< 2 ms	10^{-4}	> 16 Mbps	>99.999999%	1	HIGH
Sensor fusion channel data stream	< 2 ms	< 2 ms	10^{-4}	> 16 Mbps	>99.999999%	10	MEDIUM
Caching							
High quality audio stream	< 100 ms	< 30 ms	10^{-2}	> 128 Kbps	>99.99%	20	MEDIUM
Stereoscopic 4K 60 fps color coded real time video monitoring	< 250 ms	< 30 ms	10^{-3}	> 2 Gbps	>99.99%	20	MEDIUM
Edge AI							
Sensor fusion/ telemetry edge-ingress channel	< 2 ms	< 2 ms	10^{-4}	> 16 Mbps	>99.999999%	10	MEDIUM
edge-egress decisive URLLC channel	< 0.5 ms	< 100μs	10^{-4}	> 1 Mbps	>99.99%	1	HIGH
Micro Data Centres							
Data feeding/ extraction channels	< 1 s	< 30 ms	10^{-3}	> 1 Gbps	>99.99%	20	MEDIUM
Channel for priority services	< 250 ms	< 10 ms	10^{-4}	> 2 Gbps	>99.99999%	5	MEDIUM

Capabilities of Pre-5G   Capabilities of General 5G   Capabilities of MEC enabled 5G

infrastructure can be leveraged to perform required heavy-duty tasks that cannot be launched at typical IoT devices. A MEH can be utilized to perform the AR function. It is possible to implement main functions of computing, caching, and visualization of the AR process as Mobile Edge Applications (ME Apps) within a MEH [13]. Such ME Apps can be deployed as light-weight virtualized entities. AR content within the MEH process configured for AR cache can be classified as object and data caching. The computing platform ME App should conduct computing and graphical processing. Further, visualization function is composed of feature classification, video analysis, and tracking sub functions to formalize the AR perception. Mobile Edge Platform (MEP) of this AR based MEH should be pre-configured to orchestrate these entities within the MEH.

3.2. Low latency communication

Cloud computing is capable of providing efficient data processing capabilities by offloading computationally intensive tasks from devices to powerful cloud servers. However, cloud services can result in long communication delays and high packet errors as cloud servers are not located in close proximity to IoT devices. MEC brings cloud functionalities such as providing efficient data processing capabilities by offloading computationally intensive tasks from devices to the edge of the network to execute computationally intensive tasks of IoT devices. This is done through harnessing the computational capabilities in multiple edge nodes located within close proximity. For instance, MEC can cooperatively use the computational resources of network nodes such as, nearby access points, aggregation points of the core network, micro data centers, cloudlets, and gateways. Furthermore, by harnessing the high capacity mmWave access and a dense deployment of MEHs, MEC is also able to connect IoT devices with low latency access to facilitate delay sensitive applications and services. Such services will be exposed to the features of efficient and secure network level protocols in addition to the enhancements attributed with mmWave access channels. This will significantly shorten the delays and jitters, minimize packet errors, speed up application response, improve user experience and reduce potential network congestion [15]. In addition, Terahertz (THz) communication links can utilize the mostly unused 0.3–10 THz range to strengthen the existing back-haul networks [16]; which can reduce the latency drastically among the MEC servers, and eventually for offloading and migration processes. Further, the virtualization infrastructure in the MEC platform enables dynamic automated responses that alleviate any processing or computing delays that might encounter apart from the network-level latency. Such softwarized strategies incorporating the optimization processes would further converge to diminutive delays from the edge infrastructure and networking [17,18] point of views; that benefit the services immensely to deploy their autonomous constructs. Applications of robotics, and UAVs could benefit from this feature of 5G enabled MEC for the use cases specified in Section 2.

3.3. Micro data center and wireless big data analysis

MEC can offer new ways of deploying data centers to collect IoT data. It can provide greater flexibility by embedding MEC resources in giant data centers or clustering it with

multiple small and medium scale servers, which leads towards the micro data center concept. Using MEC resources, micro data centers can be easily deployed within the base stations and other telecom nodes. With the development of 5G and beyond, MEC devices will be available ubiquitously to collect IoT data with enhanced optimization of networking capabilities [19]. Then, multiple MEC servers in closed proximity can even form a cluster to scale up resources for these micro data centers in heavy IoT environments. With IoT and IoMT, a wide range of massive data is generated, collected, and stored in a wireless mobile network. This data is called as wireless big data. When more and more wireless IoT devices are connected, the amount of wireless big data getting increase. It is necessary to process such huge amount of IoT data efficiently and with a minimum delay to enable novel 5G services. Since centralized cloud approaches have the drawbacks of limited backhual, high latency, lack of localization, and lack of privacy, MEC can be used to efficiently process such wireless big data. Moreover, this can be optimized by coupling with micro data center deployments.

3.4. Edge-AI and cognitive assistance

Since modern IoT networks are highly dynamic and diverse, the edge networks should support Self-organizing networks (SON) and Self-sustaining Networks (SSN) abilities. Further, to improve the performance of the network and computing at the edge, various techniques are used to manage, orchestrate and sustain the network infrastructure ranging from topology management (edge site orchestration), to data and service provisioning. Among such techniques, AI and Machine Learning (ML) are considered as a key solution for many challenges. The marriage of edge computing and AI established a new research area known as "edge AI" or "Edge Intelligence (EI)", that is providing AI insight to most of the widespread edge resources. EI is generating lot of attention from both the industry and academia including Google, Amazon, Microsoft, Intel, and IBM. Edge AI used for wide range of IoT applications including live video analytics, cognitive assistance, healthcare and Industrial Internet; and they clearly demonstrate the advantages of edge computing in paving the last mile of AI. In the current context, the effectiveness of the vaccines can be tracked via Edge AI means with patient records collected at MEC based micro-data centers. Furthermore, EI as a service (EIaaS) started to become a new promising paradigm which is encouraging the development of new EI platforms with powerful edge AI functionalities. While ML as a service (MLaaS) focuses on selecting the proper server configuration and ML framework to train the model in clouds in a cost-efficient manner; the EIaaS is focusing on how to perform model training and inference in resource-constrained and privacy-sensitive edge computing environments [20].

3.5. Offloading

MEC infrastructure at the edge is accomplishing a year-old lacking aspect in the IoT market for performing computationally intensive or high resource consuming (i.e. storage, or memory) tasks within resource constrained minimalist devices through offloading. This fact is severe in IoMT apparatus, as most of such data should be aggregated and stored securely within a trusted platform. Presumably, data extracted by end devices are conveyed to the MEC edge platform for either storage or processing purpose that utilizes the energy consumption of such apparatus optimally. Processing based offloading approaches are diverse as they can be varied from simple sensory aggregated processing (healthcare wearable devices, contact monitoring, or digital PCR) to actuating via a control matrix (robots, or drones). Thus, the softwarized architecture for offloading should be dynamic and configurable in accordance to the processing and data ingress/ egress model requisites. Therefore, it is evident that MEC or any other edge computing paradigm is intrinsic for achieving offloading functions. Each offloading task can be instigated as a User Equipment (UE) App from the end device perspective, where a MEH configured for provisioning the specialized offloading service is launching the corresponding Mobile Edge (ME) App within its virtual domain [3]. These ME Apps should be task intensive, and resources should be allocated dynamically to leverage the process with minimal spending. Since different MEHs are configured to provision different offloading services, the internal structure of the MEH can be designed and configured to the service specifications. Transferring the content from the UE to the MEC edge is another challenge; that should minimize the energy spending in terms of processing and transmitting, and the bandwidth. Apart from the latency that reflects the service quality, energy becomes the dominant factor for offloading decision making, as most IoT devices are scarce on resources. The amount of content, content wise encapsulation, security and reliability measures embedded into the content that are to be offloaded will determine the energy spending; in fact, specify the energy constrains. Thus, it is important to model such offloading schemes in accordance to the well-known models such as Markov or Lyapunov approaches to alleviate the discrepancies while in transit [21,22]. Further, privacy is a major concern with the offloaded content, specially in the medical or healthcare context. Privacy preserving techniques such as Blockchain, improved privacy-awareness through machine learning, anonymity management, or physical layer approaches are ideal for mitigating such issues associated with offloading [23,24].

3.6. Caching, dynamic content delivery, video streaming and analysis

The issue of caching in nascent applications of dynamic nature is a profound predicament solved by the edge computing paradigms. MEC infrastructure offers a proximate caching placement to IoT based services that lack resources at the device end. In addition, caching in Device-to-Device (D2D) connections in IoT networks can be performed efficiently using a clustered architecture coordinated via the MEC edge. In this case, the popularity of the content can be considered for maximizing the hit probability [25]. Furthermore, caching

policies based on content appearing frequency, user preference, Q-learning, and cooperative or non-cooperative aspects can be augmented to optimize the caching of dynamic audio/ visual content. Also, depending on the IoT application, caches can be established as MEHs, or caches inside a MEH where policy management can be conducted by MEP. However, streaming protocols should attribute dynamic accessibility in the networking infrastructure within the MEC edge platform to provide a smooth user experience.

3.7. MEC based security and privacy

Ensuring security and privacy requirements is critical for pragmatic IoT based services. Though, resource scarcity exhibited in IoT devices are restricting the application of tamper-proof security measures. Thus, most state-of-the-art security directives are envisaging to employ light-weight security means (elliptic curve, lattice-based, attribute-based, or physical unclonable function based) for such end devices and their protocols. Though, such approaches have their limits with the considered spectrum of possible threats. In addition, cyber-threat landscape has been expanded to the attack vectors of injecting or instilling malicious content/ agents to the preceding IoT networks, where mitigation is improbable in a stand-alone or isolated context. Thus, MEC edge environment offers a unique opportunity to perceive the holistic security awareness in the considered domain. Security as a Service (SECaaS) is an innovative concept that caters to the MEC based service model as presented in [26].

4. Realizing IoT use cases with MEC

It is important to study about, how the MEC architecture is going to accommodate the diversity required by the use cases specified in Section 2. As shown in Fig. 1, despite the overall architectural components of the MEC infrastructure being solid, internal construct of the MEHs and their function should be amended in accordance to the specifications of the use case. As most novel services are inclusive of interfaces that enable rapid online access, localization would further improve the serving and processing times, that can reach the level of real-time. Though the novel applications are specifying more functions or processes for pre-processing, tagging, and security, localization offered by the MEC proximate infrastructure is capable of achieving real-time responsiveness for the specified use cases with 5G radio access technologies. This section explicates how each use case would be realized from the technical perspective.

4.1. MEC for smart hospitals

As Fig. 1-Ⓐ depicts, deploying a MEC based In-building Base Station (IBS) within the vicinity of the hospital improves the odds in launching the envisioned applications in sub-Section 2.1 [14]. MEHs can be configured to cater diverse medical applications leveraging their dynamic softwarized infrastructure. For IoMT-data aggregation scenarios, MEH storage resources can be utilized for data storing; can be formed

as a cluster of MEHs for scalability extending to external MEC domains; can be configured with rapid data retrieval mechanisms leveraging the autonomous operation. The external connectivity towards the backhaul that interface the cloud systems is pertinent for such MEHs. This is required to retrieve intrinsic medical history, or latest medical guidelines for treating patients efficiently. MEHs for RASs can be formulated with AR based processing platform (explicated in Section 3.1) that embed a telemetry system for robotic sensor fusion. In addition, feedback (haptic or otherwise), Simultaneous Localization and Mapping (SLAM), and trajectory tracking of robots should be performed under this MEH. A resembled approach can be employed for controlling medical robots launched for automating daily routines of medical personnel with AR.

Though MEC offers a IBS solution to launch envisaged services within the hospital vicinity, it creates a single point of failure with an edge infrastructure disruption, unless a redundancy scenario is implemented leveraging a cloud platform. Since the backhaul network engagement is minimal compared to cloud scenarios, reliability and availability aspects are reliant on the local access networks' capability or the IBS. Further, privacy of medical data and ethical practices are key aspect that should be standardized with federated approaches.

4.2. MEC for smart factories

MEC brings cloud computational capabilities, connectivity and storage to the edge of the network to facilitate flexible and real-time processing for IoT and IIoT based smart factories, as illustrated in Fig. 1-Ⓑ. MEC facilitates low latency and location aware IoT applications due to the close proximity to devices. This helps achieving low end-to-end delay, low jitter, high reliability and high bandwidth that is required for IIoT in smart factories. Furthermore, MEC can support rapid configuration needed for on-demand and customized manufacturing in IoT based smart factories by facilitating dynamic changes in the production conditions. Also, MEC aids to extend the capabilities of IIoT devices by providing powerful computing, abundant storage and caching. These capabilities can be harnessed in a smart factory environment for autonomous and cloud manufacturing processes. MEC can also provide the high computational power required for analyzing large amounts of data collected from heterogeneous machines and IoT sensors. Video footage on the processes followed in industries can also be sent to the MEC where learning algorithms can detect anomalies and make appropriate decisions to implement proper countermeasures. [27].

Industrial factories are vicinity's that embed massive amount of IoT based devices, and the scalability is a key factor in terms of the networking perspective. With enormous amount of interfaces (wireless or otherwise) that had to be maintained between the devices and the MEC platform, congestion within the local area networks is quite eminent. Thus, dynamic and priority based channel allocation schemes are required to improve the reliability of such networks.
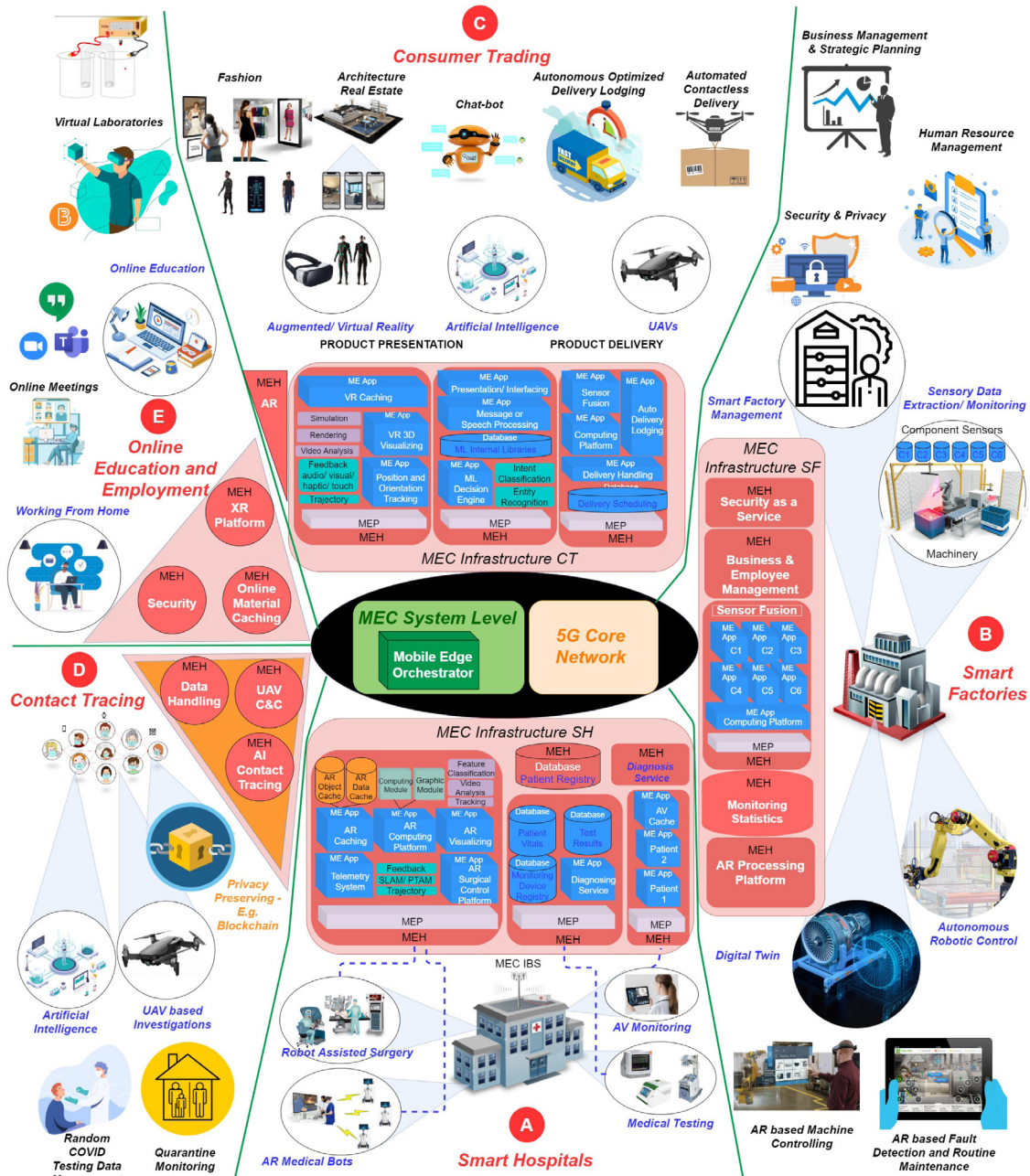
Fig. 1. MEC based IoT use cases for forming contact-less strategies.

4.3. MEC for consumer trading

As more individuals turn to IoT as a resource, its use in consumer and commodity trading will significantly increase, which will positively impact the business' growth based on innovation and new uses of technology. Businesses will exploit the advantages of using IoT to meet client expectations and improve the company's goals for the future.

The MEC based trading infrastructure can be categorized into product presentation and delivery initiatives as illustrated in Fig. 1-C. The VR based product presentation initiatives will be most preferable in the future. The MEHs configured for VR processing will be linked to the cooperate clouds that include the VR specification model of the product. Unlike

AR, VR do not require a computing platform to process the detection and tracking of realistic perception; though, requires caching and 3D visualization rendering features in addition to position and orientation tracking. Each ME App is subscribed by a distinct product range under different vendors. Launching AI based chat-bots are less resource intensive in contrast to VR deployments. The ML based decision engine that perform intent classification and entity recognition can be placed inside a MEH linked to external libraries. The message or speech processing components are acting as the response agents, operating in line with global databases. ME Apps are configured by each vendor based on their requirements and themes to interface the consumers. Product delivery services are acting separately, as they are typically outsourced to delivery agents

by the prosumers or vendors. Non human engaged delivery can be implemented as a generic logistic system, where all the operations are autonomous; including the deliveries managed through UAVs. UAV based delivery services can deploy and control their drones via the MEC platform formed as an offloading model as in [28]. It is obvious that MEC offers an efficient interface for UAV applications in contrast to cloud-native scenarios due to its proximate server environment and rapid response capability.

Online trading is not a priority service in its nature, but the security level of the transactions along with reliability and availability should be high due to the monetary content that are conveyed through the channels. With the UAV based delivery however, rapid delivery of the content through the network should be prioritized. Unless, the UAV should attribute the self-navigation capability within itself.

4.4. MEC for contact tracing

MEC can be efficiently utilized for gadget/IoT based COVID-19 contact tracing, as depicted in Fig. 1-D. To prevent the privacy issues in contact tracing, MEC can be used to implement a distributed data management approach. With the possibility to deploy localized micro data center, collected IoT data can stored locally. Moreover, wireless big data processing at the edge and edge AI techniques can be used to process such data in a localized manner. In such a way, MEC can prevent the transmission and storage raw user and IoT data in the cloud and also sharing them with authorities. Only the processed information (i.e privacy sensitive markers has been removed) at the edge will be shared with the authorities. This will also improve the overall scalability of the contact tracing mechanism. Moreover, MEC and edge AI can be used for efficient Command and Control (C&C) for UAVs which play a vital role in monitoring quarantine violations.

The details and status of contact tracing should be accessible for relevant authorities at all times. Thus, availability of these servers or storage instances within the MEC platform should be ensured with proper security levels to prevent any undue service denying threats. Reliable and hierarchical data access through dynamic rapid querying that fits this model should be proposed to maintain the data flow with appropriate privacy and anonymity measures. Further, data access should be deployed either with federated data engines running on MEC or replication to the cloud native data clusters to make the querying efficient globally and locally.

4.5. MEC for WFH and online education

It is paramount to carefully address (1) the security of the IoT devices and of the networks used, and (2) the security and privacy aspects of users who access various online collaborative working/learning platforms and apps. Virtual machine introspection services can run using the MEC infrastructure and monitor the behavior of WFH and online education based apps to detect any attack that intends to compromise the virtualized entities. AI based intrusion detection systems can

harness the MEC capabilities to monitor the network behavior and data transmitted in the network. MEC based trusted platform manager techniques can handle secure authentication and also verify the integrity of software and executable programs through validation of operational statistics such as firmware, operating system kernel, etc. MEHs are also capable of deploying context aware security mechanisms to detect anomalous behavior of apps [3]. In addition, XR based working/learning platforms can harness the MEC capabilities to process high volumes of data in real-time to facilitate virtual meetings, virtual classrooms, virtual laboratories, etc. Most WFH connections are established through Virtual Private Networks (VPNs). MEC networking infrastructure can be leveraged to launch Virtual Private LAN Service (VPLS) based off site remote connections that can be more secure and faster than individual VPN connections. Usage of MEC for WFH and online educational activities are illustrated in Fig. 1-E.

Usage of VPN or VPLS level access encapsulation can overburden the network drastically with the increasing demand for WFH apps. Managing traffic is becoming a pragmatic dilemma for the MEC access network with such a demand for online access. With MEC deployments, the links between MEC platforms are becoming more prone for traffic. Thus, managing traffic in these links becomes an issue for reliable delivery. Feeding online meetings or online lectures with HD level audio and video streams is going to further burden the network infrastructure. Therefore, methods and techniques should be developed for managing this accumulated traffic introduced with novel demand for online delivery. Table 2 summarizes the significance of each MEC based service for IoT use cases.

5. Feasibility evaluation

Proposed use cases in this paper have two different deployment options. Its either through cloud computing or edge computing. In order to determine the feasibility of the proposed use cases to be deployed with MEC, an evaluation was conducted via simulating the performance to the following criteria. Each criteria was selected based on the essential services required by the stated use cases that rely on MEC for their pragmatic deployment. In fact, this section validates the pervasiveness of the MEC paradigm for the stated use cases. The intention of this evaluation was to study the limits of each use case from the deployment perspective, and to determine the better performing scenario. The simulations for the stated criteria targeting the proposed MEC based edge computing deployments are running in contrast to the prevailing cloud computing capabilities. We assume that the same access network model is applied for both MEC and cloud scenarios, where the dynamics on mobility is similar for both instances.

- **Criterion 1:** General AR applications — for less resource intensive AR uses such as virtual education and trading initiatives. Assuming 30 ms, 10^7, 5 Gbps of processing delay, CPU cycles, and data rate for achieving a single task.
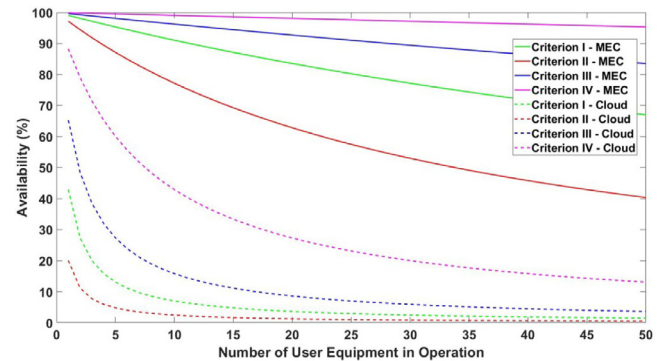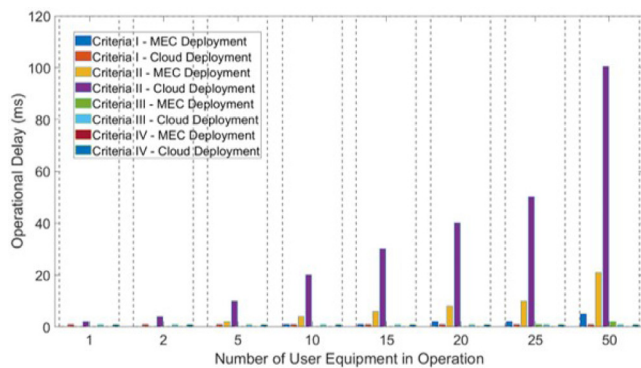
Table 2

Significance/Importance of MEC services for potential IoT Applications and their implementation challenges.

Potential IoT Applications	MEC based Applications and Services							Implementation challenges					
	Augmented Reality	Low Latency Communication	Micro Data Centres and Wireless Big Data Analysis	Edge-AI and Cognitive Assistance	Offloading	Caching, Dynamic content delivery, Video Streaming and Analysis	MEC based Security and Privacy	Security & Privacy	Scalability	Edge Resources	Network Resources	Mobility	Compatibility
Smart Hospitals													
Robot assisted surgery	H	H	M	H	H	H	M	M	L	H	H	L	L
Remote robotic monitoring and patient care	M	M	M	H	H	H	M	M	M	H	H	L	M
Patient vital data aggregation and management	L	M	H	M	M	M	H	H	H	M	M	M	H
Smart Factories													
Production via autonomous robotic operations	L	H	H	H	M	M	L	L	H	M	H	M	H
Digital twin	H	M	H	H	M	H	M	M	M	H	H	L	M
Smart sensory data aggregation and management	L	H	H	M	H	L	M	M	H	M	M	M	M
Efficient logistic and delivery management	L	M	H	H	M	L	L	L	H	M	M	M	M
Consumer Trading													
Contact-less/remote product presentation strategies	H	M	H	L	M	H	L	L	M	H	H	H	H
Autonomous intelligent interactive agents - Chatbots	L	M	L	H	M	M	L	L	H	M	M	M	M
Autonomous optimized contact-less delivery lodging	L	H	H	H	M	M	M	M	H	M	H	H	H
Contact Tracing													
Distributed data management	L	L	H	H	M	L	H	H	H	M	M	H	M
Efficient contact tracing and infectious forecasting	L	M	H	H	M	M	H	H	H	M	M	H	M
Contact-less quarantine monitoring	L	H	H	H	H	M	H	H	H	H	H	H	H
Working From Home													
WFH with virtual environment/ laboratory	H	H	H	H	M	H	M	M	H	H	H	M	H
Advanced online caching and presenting	H	M	H	H	M	H	M	M	H	H	H	M	H

Low Importance	Medium Importance	High Importance
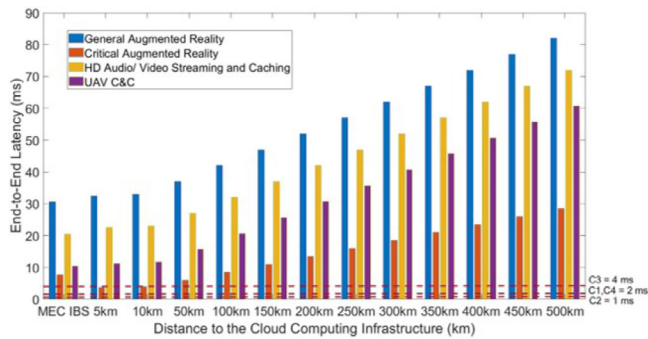
Fig. 2. Impact of distance to the core network for E2E latency.

Fig. 3. Impact of scalability for operational delay.

Fig. 4. Impact of scalability for availability.

- **Criterion 2:** Critical AR applications — formed for RAS or AR controlled IIoT deployments. The corresponding assumed parameters are 5 ms, 10^9, 20 Gbps, and the controlling station located 50 km from the operating premises.
- **Criterion 3:** Audio/ Video (AV) streaming and caching applications — suited for video caching or eMBB type services with parameters 20 ms, 5×10^6, and 2 Gbps.
- **Criterion 4:** UAV autonomous C&C applications — assuming the UAV is operating 2.5 km away from the MEC locality where the parameters are 10 ms, 10^6, and 0.5 Gbps.

The parameters for above 4 criteria were selected in accordance to the limits specified under Table 1. Each criteria

Table 3
Implementation challenges of MEC based IoT applications.

Technical aspect	Issue/Challenge/Threat	Description	Possible solutions
Security	Social engineering threats on IoT users	COVID-19 pandemic has forced the users with lesser awareness/literacy on online practices to engage in remote work via IoT devices. This fact has been leveraged by cyber-criminals to launch phishing type attacks to attain confidential information.	Awareness is the key for avoidance. The institutions should educate consumers regarding possible threats, while preventive mechanisms such as spam filters, anti-phishing add-ons, or firewalls should be pre-installed.
	Malware intrusions	Circumstances with the pandemic are used to tempt online users into download and execute spyware, adware, or ransomware type agents for unauthorized access. These malware can compromise the MEC edge components.	Advance and adaptive intrusion detection and prevention systems are required while enhancing the security at Internet access points within organizations.
	Untrusted service outsourcing	WFH initiatives have forced the employees to use third-party web-based streaming, collaborative, educational, and file sharing tools exclusive to the company network domains. Their unverified security and limited functionalities are compromising the trade secrets.	Strengthen the remote access procedures of the institutions and employ secure tunneling approaches for cooperate communications and collaborations.
	Denial of Service (DoS) and Jamming type threats	The excessive use of online services are inviting adversaries to launch DoS attacks at channels connecting the IoT device layer and the edge. These will impede the services while jamming on UAV type devices will change its trajectory.	Detecting the illegitimate traffic via a trusted platform manager would allow mitigation at routing level. Further, anti-jamming techniques to secure UAVs.
Privacy	Contact tracing	The unavoidable tracing of the contacts of the infected is exposing the private information including their whereabouts. This is a complete violation of EU GDPR legislation's, and the process is neglecting the personal dissent in some countries.	Information of the contacts can be restricted to localized domain while AI, and blockchain like technology can be integrated to secure the private data of individuals from the authorities, where only a social security number of the contact will be sent to them.
	News, printed, digital, and social media	Governments used fear cultivated from media as a mean of restricting the movements of citizens in the early days of the pandemic. Such practices have violated the privacy rights of exposed personnel and institutions.	Concrete legislation's should be formed by the authorities, specific to pandemic situations for media usage.
	Health data extracted from IoMT wearables	The vitals of the patients are extremely private information that are extracted from wearables by medical services. With MEC, IoMT services are provisioned with a localized processing infrastructure, though privacy violations are imminent.	Blockchain can be employed to contrive an anonymous data network where only a representative value is conveyed to the IoMT servers, not the actual value.

(*continued on next page*)

was assumed to be operating following an offloading scenario, where UE content is offloaded either to the cloud or MEC platforms for processing, and the corresponding outcome is delivered to the UE at the end. The simulation environment was formulated in accordance to [14]; where the parameters are specified below.

- ☐ Computing capacity of the MEC — 5×10^{10} CPU cycles
- ☐ Computing capacity of the cloud — 10^{11} CPU cycles
- ☐ Bandwidth of the MEC access connectivity 50 Gbps

- ☐ Bandwidth of the backhaul network — 10 Gbps
- ☐ Displacement of the eNB from the MEC — 1 km
- ☐ Delays in MEC and cloud access are 0.25 ms and 1 ms
- ☐ Distance dependent core network delay — 0.05 ms/km

E2E latency impacted by the distance to the cloud infrastructure, Operation Delay impacted by the scalability of the UEs, and Availability of the each criterion on the scalability aspects were simulated and the results are illustrated in Figs. 2–4 respectively. The availability was computed in

Table 3 (*continued*).

Technical aspect	Issue/Challenge/Threat	Description	Possible solutions
Edge and Network Resources with Scalability	Wireless access channels	Increasing IoT and IoMT devices are exceeding the existing spectrum allocations (or bandwidth).	Utilizing more frequency bands as in mmWave technology and advance spectrum re-using strategies.
	Traffic bottlenecks	Rapid accumulation of all sorts of online traffic is creating bottlenecks in certain access points of the network. Such points are affecting the entire network performance towards the edge.	Delegating traffic to various mediums optimally, so that the network performance is not reliant on a single medium such as RF.
	MEC resource depletion	Increasing number of UEs will eventually deplete the resources of the edge infrastructure. This will terminate in-proximity un-prioritized IoT services and reject the new requests.	Establishing a migrating strategy that utilizes the closest resourceful MEC.
Mobility	Switching MEC edges	Highly mobile device will keep sifting from one MEC BS to another rapidly.	An efficient and fast migration strategy is required.
	Coverage of IoMT wearables	Wearables embedded to the human body do not possess a direct transmission capability to a network hub, and relies on short range technologies such as Bluetooth. With a highly mobile device, these technologies become obsolete for communication.	Developing a re-transmission protocol for mobility detected situations.
	Energy Depletion	It is obvious that mobility is degrading the energy of IoT devices, specially for location based services.	Attaching energy harvesting systems to the IoT devices.
Compatibility	IoMT hardware integration compatibility	Due to heterogeneity exhibited with various IoT manufacturers, integrating IoT devices to the medical premises systems become quite questionable.	Policies, and protocols should be established for integration for IoMT devices while universal connection options should exist on each IoT device.
	Integration issues with the edge	At software level, with different IoT based operating systems are attempting to connect to the edge, there will be obvious compatibility issues.	Integration policies and protocols should be standardized by the authorities such as ETSI.

accordance to [29], where the respective mean down times were estimated referring [30], and implying traffic congestion instances to failures rates. It is observable that MEC deployments have a lesser E2E delay in contrast to cloud scenarios; while operational delay is accumulating with the increasing number of UEs. This is mainly due to the proximate locality of the MEC deployment. The processing of HD video in criterion 3 for 1080p with 60 fps requires up to 5 Mbps bit rate, and a significant processing delay is endured even for cloud-native scenario in contrast to criterion 4, where the processing is limited to telemetry data. Thus, E2E delay in criterion 3 is higher than criterion 4. Fig. 4 indicates that availability in MEC scenario is significantly higher and within the limits of the 5G network specifications. However, the high resource requirement of the specified criteria are limiting the number of UEs that can operate simultaneously. This proves that MEC is capable of enabling the IoT applications to realize the identified key COVID-19 related IoT use cases. In addition, implementation challenges for various technical aspects are tabulated in Table 3.

6. Conclusion

This paper presents how MEC can be used to realize key IoMT based use-cases as a pervasive approach that enhances the computing infrastructure. e-Health use cases ranging from smart hospitals, smart factories, consumer trading, contact tracing, working from home, and online education have been discussed, highlighting the challenges and requirements of each use case. Then, MEC based IoT contact-less services such as AR, low latency communication, micro data center and wireless big data analysis, edge-AI and cognitive assistance, offloading, caching, dynamic content delivery, video streaming and analysis, and MEC based Security and Privacy are presented elaborating how MEC can realize the identified IoT use-cases. Simulation results clearly indicate that MEC based solutions are more suitable for realizing the stated use cases compared to cloud computing in terms of end-to-end latency, scalability, and availability. Insights drawn from this article are expected to encourage both telecommunication and internet service providers to launch MEC in a global context to extend the computing infrastructure to the mobile edge, and overcome the limitations of current technologies that lacks the pervasiveness.

CRediT authorship contribution statement

Pasika Ranaweera: Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Chamitha**

de Alwis: Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Anca D. Jurcut:** Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Madhusanka Liyanage:** Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing.

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.

Acknowledgment

References

[1] K.K. Karmakar, V. Varadharajan, U. Tupakula, S. Nepal, C. Thapa, Towards a security enhanced virtualised network infrastructure for internet of medical things (iomt), in: 2020 6th IEEE Conference on Network Softwarization, NetSoft, IEEE, 2020, pp. 257–261.

[2] P. Ranaweera, A.D. Jurcut, M. Liyanage, Survey on multi-access edge computing security and privacy, IEEE Commun. Surv. Tutor. 23 (2) (2021) 1078–1124.

[3] P. Ranaweera, A.D. Jurcut, M. Liyanage, Realizing multi-access edge computing feasibility: Security perspective, in: 2019 IEEE Conference on Standards for Communications and Networking, CSCN, IEEE, 2019, pp. 1–7.

[4] G.-Z. Yang, B.J. Nelson, R.R. Murphy, H. Choset, H. Christensen, S.H. Collins, P. Dario, K. Goldberg, K. Ikuta, N. Jacobstein, et al., Combating covid-19—the role of robotics in managing public health and infectious diseases, 2020.

[5] Y. Siriwardhana, C. De Alwis, G. Gür, M. Ylianttila, M. Liyanage, The fight against the covid-19 pandemic with 5 g technologies, IEEE Eng. Manag. Rev. 48 (3) (2020) 72–84.

[6] A. Bhatti, H. Akram, H.M. Basit, A.U. Khan, S.M. Raza, M.B. Naqvi, E-commerce trends during covid-19 pandemic, Int. J. Future Gener. Commun. Netw. 13 (2) (2020) 1449–1452.

[7] Q. Ye, B. Wang, J. Mao, J. Fu, S. Shang, Q. Shu, T. Zhang, Epidemiological analysis of covid-19 and practical experience from china, J. Med. Virol. 92 (7) (2020) 755–769.

[8] M. Yanes-Lane, N. Winters, F. Fregonese, M. Bastos, S. Perlman-Arrow, J.R. Campbell, D. Menzies, Proportion of asymptomatic infection among covid-19 positive persons and their transmission potential: A systematic review and meta-analysis, PLoS One 15 (11) (2020) e0241536.

[9] K. Markelova, Mapping the world: Education: An unprecedented crisis, UNESCO Courier 2020 (3) (2020) 54–57.

[10] M.S. Elsayed, N.A. Le-Khac, A.D. Jurcut, Dealing with COVID-19 network traffic spikes, IEEE Secur. Priv. 19 (1) (2020).

[11] A.I. Abubakar, K.G. Omeke, M. Öztürk, S. Hussain, M.A. Imran, The role of artificial intelligence driven 5G networks in COVID-19 outbreak: opportunities, challenges, and future outlook, Front. Commun. Netw. 1 (2020).

[12] 3GPP, Study on Communication Services for Critical Medical Applications, 3GPP Technical Report 22.826, 2019, [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3546. (Last Accessed 13 July 2020).

[13] J. Ren, Y. He, G. Huang, G. Yu, Y. Cai, Z. Zhang, An Edge-computing based Architecture for Mobile Augmented reality, IEEE Netw. 33 (4) (2019) 162–169.

[14] P.S. Ranaweera, M. Liyanage, A.D. Jurcut, Novel MEC based approaches for smart hospitals to combat COVID-19 pandemic, IEEE Consum. Electron. Mag. (2020).

[15] M. Merluzzi, P. Di Lorenzo, S. Barbarossa, V. Frascolla, Dynamic computation offloading in multi-access edge computing via ultra-reliable and low-latency communications, IEEE Trans. Signal Inf. Process. Netw. 6 (2020) 342–356.

[16] L.A. Grieco, G. Boggia, G. Piro, Y. Jararweh, C. Campolo, Ad-hoc, mobile, and wireless networks.

[17] A.M. Somarin, Y. Alaei, M.R. Tahernezhad, A. Mohajer, M. Barari, An efficient routing protocol for discovering the optimum path in mobile ad hoc networks, Indian J. Sci. Technol. 8 (S8) (2015) 450–455.

[18] A. Mohajer, M. Bavaghar, H. Farrokhi, Reliability and mobility load balancing in next generation self-organized networks: Using stochastic learning automata, Wirel. Pers. Commun. 114 (3) (2020) 2389–2415.

[19] A. Mohajer, M. Barari, H. Zarrabi, Big data-based self optimization networking in multi carrier mobile networks, Bull. Soc. Roy. Sci. Liège 85 (2016) 392–408.

[20] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, J. Zhang, Edge intelligence: Paving the last mile of artificial intelligence with edge computing, Proc. IEEE 107 (8) (2019) 1738–1762.

[21] G. Yang, L. Hou, X. He, D. He, S. Chan, M. Guizani, Offloading time optimization via markov decision process in mobile-edge computing, IEEE Internet Things J. 8 (4) (2020) 2483–2493.

[22] Y. Hu, T. Cui, X. Huang, Q. Chen, Task offloading based on lyapunov optimization for mec-assisted platooning, in: 2019 11th International Conference on Wireless Communications and Signal Processing, WCSP, IEEE, 2019, pp. 1–5.

[23] D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning, IEEE Trans. Netw. Serv. Manag. 17 (4) (2020) 2536–2549.

[24] X. He, R. Jin, H. Dai, Physical-layer assisted privacy-preserving offloading in mobile-edge computing, in: ICC 2019-2019 IEEE International Conference on Communications, ICC, IEEE, 2019, pp. 1–6.

[25] S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, W. Wang, A survey on mobile edge networks: Convergence of computing, caching and communications, IEEE Access 5 (2017) 6757–6779.

[26] P. Ranaweera, V.N. Imrith, M. Liyanag, A.D. Jurcut, Security as a service platform leveraging multi-access edge computing infrastructure provisions, in: ICC 2020-2020 IEEE International Conference on Communications, ICC, IEEE, 2020, pp. 1–6.

[27] B. Chen, J. Wan, A. Celesti, D. Li, H. Abbas, Q. Zhang, Edge computing in iot-based manufacturing, IEEE Commun. Mag. 56 (9) (2018) 103–109.

[28] P.A. Apostolopoulos, G. Fragkos, E.E. Tsiropoulou, S. Papavassiliou, Data offloading in uav-assisted multi-access edge computing systems under resource uncertainty, IEEE Trans. Mob. Comput. (2021).

[29] L. Jereb, Network reliability: models, measures and analysis, in: Proceedings of the 6th IFIP Workshop on Performance Modelling and Evaluation of ATM Networks, Tutorial Papers, Ilkley, UK, 1998, p. T02.

[30] Ponemon, Data center downtime at the core and the edge: A survey of frequency, duration and attitudes, 2021, [Online]. Available: https://www.vertiv.com/490a6d/globalassets/documents/reports/ponemon/vertiv-ponemon-datacenterdowntimesurveyreport_321796_0.pdf.