IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 August 2022, accepted 12 September 2022, date of publication 27 September 2022, date of current version 6 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3210262

RESEARCH ARTICLE

Managing Physical Distancing Through 5G and Accelerated Edge Cloud

LUCA VALCARENGHI[1], (Senior Member, IEEE), ALESSANDRO PACINI[1], JUSTINE CRIS BORROMEO[1], SILVIA FICHERA[1,2], MARIA GAGLIARDI[1], DENISE AMRAM[1], AND VINCENZO LIONETTI[3]

[1]Scuola Superiore Sant'Anna, 56124 Pisa, Italy
[2]Vodafone, 20147 Milano, Italy
[3]Fondazione Toscana Gabriele Monasterio, 56124 Pisa, Italy

Corresponding author: Luca Valcarenghi (luca.valcarenghi@santannapisa.it)

This work was supported in part by the 5G-Enabled SOS Intelligent Assistant (5G-SOSIA) Project through Regione Toscana under the Bando Salute 2018 Program.

ABSTRACT Specific 5G Release 17 work items are dealing with critical medical applications. Moreover, the adoption of mobile health (m-health) and e-health has been accelerated by the COVID-19 pandemic. This paper first examines the requirements of critical medical applications that 5G is expected to support. Then it illustrates possible data protection, management, and privacy issues. Finally, it shows a first implementation of an m-health framework supporting physical distance management. Experimental results show that, by exploiting 5G connectivity and the computing capacity provided by an accelerated edge cloud, the proposed framework can detect physical distance violations faster than a user equipment (UE)-based implementation, while saving UE energy.

INDEX TERMS m-health, e-health, 5G, accelerated edge cloud, social/physical distancing.

I. INTRODUCTION

Besides connectivity, provided already by previous mobile technologies, the fifth generation of mobile communications (5G) provides processing via accelerated edge data centres or edge clouds [1] and artificial intelligence/machine learning (AI/ML) [2]. The combination of such technologies opens the road towards innovative applications in various fields, such as medicine. 5G is expected to have a strong impact on the way patients are cared for in various aspects. Thanks to its ultra-low latency, it is expected that 5G and, most likely, beyond 5G technologies enable remote surgery with doctors and operating rooms connected wirelessly via a mobile network. Thanks to its enhanced mobile broadband 5G will also enable telemedicine, remote assistance, real-time patient monitoring, and the transfer of diagnostic images and large data sets [3].

The request for mobile health (m-health) and e-health services has increased dramatically, also because of the recent COVID-19 pandemic. New services have emerged, such as the ones dedicated to preventing the spread of the virus (e.g., social/physical distancing) and contact tracing. As shown in [4] one of the most effective ways to limit the spread of the SARS-CoV-2 virus is the so-called 'social/physical distancing', which requires the distance between two people to be greater than the approximate distance of the drops (i.e., a few metres). To calculate the distance between two or more people, some approaches, based on Bluetooth, have been proposed. They measure the strength of the received signal between portable or wearable devices to calculate the distance between two or more people [5]. Other applications are emerging that apply AI/ML techniques to perform real-time analysis of social/physical distance in scenes captured by different types of cameras [6]. They might run on the handheld devices of personnel devoted to check physical/social distancing, such as smart handheld cameras or mobile phones. However, if such applications run continuously, they can quickly drain the battery or slow down the devices due to the large amount of required computing power. By shifting processing capabilities to an

The associate editor coordinating the review of this manuscript and approving it for publication was Olutayo O. Oyerinde.

accelerated edge cloud, enabled by 5G connectivity, capable of transferring captured images and other data with extremely low latency, mobile device battery savings can be achieved without sacrificing application response time.

This paper first outlines the performance requirements of m-health applications critical to the 5G network. Furthermore, it highlights the main legal issues related to possible risks for fundamental rights of people, privacy, data protection and management, and processing of m-health applications and services. These issues are sometimes underestimated but represent a key factor for the sustainable deployment of e-health and m-health. Then, the paper proposes the implementation of a framework exploiting AI/ML and accelerated edge cloud to process real-time images for physical distancing management. Finally, the related data processing risk analysis is presented. The proposed framework makes it possible to process transferred images with extremely low latency and, at the same time, to save the battery of the mobile device. Moreover, it is so general that it can be applied to any future medical application requiring low latency response and computationally intensive image processing.

The conducted experimental performance evaluation shows that the proposed implementation outperforms the same service implementation in a mobile device in terms of processed frames per second: the number of processed frames per second is about three times. Indeed, the GPU-based acceleration is capable of more than compensating for the delay for transferring the data to the edge, where they are elaborated. In addition, the energy consumption of the considered GPU is less than the energy consumption of a general-purpose CPU.

II. MEDICAL APPLICATION REQUIREMENTS FOR 5G

Specific work items of 5G Release 17 are dedicated to medical applications: "Communication Service Requirements for Critical Medical Applications" (CMED) [7] and Study on CMED [8]. Such study items originated several 3GPP Technical Specifications (TS) and Technical Reports (TR). In particular, the outcome of the studies performed in the aforementioned work items are reported in [9], and references therein (i.e., 3GPP TS 22.104 and 3GPP TS 22.263), and in [10].

This section provides a brief overview of the requirements and proof of concepts available in current Standard Developing Organisations (SDOs) and in the literature. The main content is extracted from [10] which provides a single specific reference point for medical application scenarios. In addition, some examples of trials conducted by the 5G-HEART project are provided [11].

In [10] several use cases are considered, which are classified according to the following scenarios for what concerns mobility and location:

- Static, fixed environment with a stable connectivity.
- Moving, dynamically changing context with unstable connectivity.
- Local, inside the hospital facility.
- Remote, far from the hospital facility.

The technical report [10] considers all the possible mobility-location combinations. In particular, the *static-local* and the *moving-local* scenarios deal with the delivery of critical care in the context of a hospital or a medical facility. In these cases, both the medical team and the patients are co-located. In these use cases indoor communications services are delivered by a non-public network, similarly to what happens in many Industry 4.0 use cases.

The *static-remote* and the *moving-remote* scenarios include the use cases considering the delivery of critical care where medical specialists and patients are located at different places. In this case, the communications services are delivered by Public Land and Mobile Network (PLMN).

Here below a summary of the different use cases described in [10] is presented for providing the reader with a glimpse on the considered requirements. For further details the reader is referred to the original documents.

For static-local scenarios, one of the considered use cases are hybrid operating rooms. The idea is to have operating rooms which are fully interconnected with many medical devices, fully exploiting the 5G wireless technology. They could be equipped with many imaging systems, such as fixed C-arms, Computed Tomography (CT) scans and Magnetic Resonance Imaging (MRI) scans, that send high resolution images to a medical application for further processing. Thanks to that, a medical staff can see the real time patient data on one or more monitors, enabling a minimally invasive surgery.

A second use case for static-local scenarios is Augmented Reality Assisted Surgery. In this case real time data from the patient (e.g., endoscopy, overhead) are merged with the live reference medical imaging over wireless connectivity.

Robotic Aided Surgery (RAS) is considered as a further static-local scenario. RAS can be beneficial for invasive surgical procedures requiring delicate tissue manipulation and access to areas with difficult exposure. This is achieved by using a system that takes a surgeon's hand movements and translates them to movements of small instruments. Haptic feedback is required to render the applied forces generated by the surgical procedure.

For the aforementioned use cases, the following 5G technical requirements are considered:

- Support for confidentiality methods and data integrity protection that serve Ultra Reliable Low Latency Communications (URLLC) and energy constrained devices.
- Support for the network operator to define priorities among different networks if there is competition for resources on the same physical network.
- Requirements related to the 5G LAN type service management and transport of Ethernet frames.
- Flexible Broadcast/Multicast service requirements.

In uses case where timely feedback shall be provided to the surgeon, such as augmented reality assisted surgery and robotic aided surgery, the 5G system should provide strict synchronization by:

- Offering mechanisms for processing and transmitting IEEE1588v2 / Precision Time Protocol messages to support 3rd-party applications utilizing this protocol.
- Support for mechanism to synchronize the user-specific time clock of UEs with a working clock. Time synchronization shall be provided with a precision of $\leq 1\ \mu s$.
- The 5G system shall provide an interface to the 5G sync domain, that applications can use to derive their working clock domain or global time domain (i.e., Reference Clock Model).

As stated in [10], the latency of the imaging system compromises the achievable accuracy at a given hand speed. Surgeons often are comfortable with a latency that provides an accuracy of 0.5 cm at 30 cm/s hand speed. In general, the median reaction time of humans to visual events is in the order of 200ms. Thus, the imaging system latency from image generation to display on a monitor shall be of about 16 ms for procedures on a static organ where the only moving object is the surgeon's hand.

For what concerns static-remote scenario, the Remote Specialist Practice is one of the use cases considered in [10]. In this case, a truck equipped with medical devices is sent into rural areas to provide examinations, screenings, or medical check-ups. This is done by a mobile expert with the support of remote ones, which allows people to receive specific and tempestive treatments without moving to distant hospitals. The truck provides one or more examination rooms with high end video/audio equipment, whose results will be sent then, through a dedicated non-public 5G network or a private slice, to remote experts.

The Remote Robotic Telesurgery is another static-remote use case, that requires strict synchronization and the lowest latency possible because the surgery is performed remotely. Thus, the 5G system shall support very challenging requirements, such as the one reported in [10]. For example, a jitter of less than 2 ms is required for force and vibration in haptic feedback. In addition, a data rate of 137 Mb/s-1.6 Gb/s (and up to 6 Gb/s for good imaging) for real-time multimedia.

Emergency care is another static-remote use case where medical staff can perform ultrasound examination in a non-moving ambulance. This operation, together with teleguidance by a remote expert allows to drastically improve the management of prehospital care.

The former use cases, since they are performed on a remote site, imply additional requirements to the ones listed earlier for the static-local scenarios, such as enabling the network operator to define a priority order between different network slices.

In moving-local scenarios instead, a considered use case is the continuous monitoring of the patient cardiac activity (i.e., cardiac telemetry) within the hospital facility wirelessly. The aim is to drastically decrease the usage of monitoring cables, which could represent an obstacle in emergency situations. A proposed approach is to use 5G non-public network along with multiple radio access technologies (e.g., Wi-Fi) allowing the reuse of already existing architectures that would be extended with next generation functionalities.

The monitoring of the patient cardiac activity can also be implemented in the moving-remote scenario when the patient is outside the hospital. Patients receive a 5G wearable telemetry device that includes body sensors (e.g., ECG). This device streams heartbeat data 24/7 to the hospital and automatically issues an emergency call in case a critical episode occurs. The patient's position is automatically sent along with its medical identity within the call.

The list of potential service performance requirements for both the moving-local and the moving-remote cardiac telemetry are summarized in *Table 1* reported from [10]. Most of the requirements are similar but, for example, in the moving-remote scenario higher speeds shall be supported considering that the use could be in cars or trains. In addition, in the moving-remote scenario the additional following requirements shall be supported:

- All requirements related to positioning services (capillary deployment).
- All performance requirements related to high accuracy positioning.
- Service requirements related to emergency calls.

Another moving-remote use case is monitoring patients inside ambulances. Ambulances act as a connection hub for medical equipment and wearables and stream patient's data to the awaiting destination hospital through its 5G connection. This allows a better preparation for the emergency crew. Clearly all the devices' data streams must be synchronized to correlate events and images, and the 5G connection must be stable and reliable.

The following technical requirements must be met:

- The 5G system must support data integrity and confidentiality protection methods that serve URLLC and low-power devices.
- All requirements related to slice management, access, capacity and QoS. Also, the prioritisation of some slices over others (in case of competition for resources on the same network).
- All requirements related to private slice management, access, restriction to a specific geographical area, isolation, fault tolerance.
- All requirements related to security management in private slices.
- The 5G system must minimise packet loss during (inter/intra) UE handovers.
- The 5G system shall minimise the outage time during handovers (inter/intra) of UEs.
- Clock synchronization service level requirements related to the management of a global clock domain, clock synchronization service performance requirements (accuracy level 1).

In addition to the use cases presented in [10] the 5G-HEART project reports in [11] some additional use cases.

TABLE 1. Moving-local and moving-remote cardiac telemetry requirements.

	Within the hospital	Outside the hospital
Communications service availability target value	99.99999%	99.9999%
Communications service reliability: mean time between failures	>1 year	Below 1 year but >> 1 month
End-to-end latency: maximum	<100ms	<100 ms
Service bitrate: user experienced data rate	0.5 Mb/s	0.5 Mb/s
Message size: [byte]	≤1000	≤1000
Survival time	100 ms	< 1s
UE speed	≤ 5 km/h	≤ 500 km/h
#of UEs	≤ 1000 per km^2	-In area with hospital up to 1000 per km^2 -In suburb an area up to 10 per km^2
Service area	Hospital (incl. elevator)	Countrywide including rural areas and deep indoor
Remarks	-Use case entails body-worn IoT device. -Use case involves possible deployment using non-public network and/or multi-RAT technologies (incl. handover to PLMN)	-Use case entails body-worn IoT device -User could be moving by car or train

The use case 'Educational Surgery' concerns 5G support for remote learning and remote participation in clinical operations. The use case "Remote Ultrasound Examination" is related to an expert in a central hospital helping a doctor in a local/remote hospital to perform a high-quality ultrasound examination. The two explored approaches are: the remote expert supporting the local doctor in performing an ultrasound examination (e.g., via a Skype-like platform or a mixed reality platform) and the remote expert remotely controlling a robot in the local hospital. The use case 'Support to paramedics' aims to enable pre-hospital triage on board ambulances by transmitting ECG data and other vital parameters. The use case 'Critical Health Event' deals with four clinical cases that wearable cameras worn by paramedics can be beneficial for: mass casualty supervision support, chronically ill child (e.g., chronic illness with a child known to the hospital), cancer drug follow-up at home, paramedic-to-paramedic drug administration support. The use case "Automatic pill camera failure" considers a Wireless Endoscopic Capsule (WCE) pill for the early detection of colon cancer. The capsule, ingested by the patient, sends high-quality images to an external receiver. The 'Vital-Sign Patch Prototype' focuses on the development of a prototype disposable, direct-to-cloud, vital sign detection patch. This is a smart patch that measures a patient's vital signs 24/7 and communicates them directly to the cellular network. The 'Locatable Tag' use case uses a tag to trigger an emergency alarm when patients with critical conditions require immediate help.

III. DATA PROTECTION, PRIVACY, AND DATA MANAGEMENT IN MEDICAL APPLICATIONS SUPPORTED BY 5G

In addition to the technical requirements, this paper addresses some of the most common ethical-legal issues to provide a legal attentive pre-assessment of the given technologies. In fact, despite of the fact that different legal constrains and requirements may be applicable in different legal systems, a risk-based approach finds out possible grounds of assessment in the development of the illustrated solutions as an innovative methodology for R&D in healthcare. These technical-legal remarks are, indeed, functional to provide an interdisciplinary multi-level classification of 5G-based emergency medical devices.

Different scenarios require a specific ethical-legal analysis to ensure that tools, solutions, and technologies are used in compliance with all requirements. Data protection and IT security challenges are posed by both devices and IT infrastructures. Therefore, attention must also be paid to several issues when selecting and implementing appropriate technical and organisational measures [12].

Since in medical applications supported by 5G sensitive and personal data are stored, collected, and shared, particular attention must be dedicated to the compliance with the General Data Protection Regulation (EU Reg. nr. 679/2016, GDPR) and with the respective national safeguards implemented in the EU Member States to process health-related data.

Two main steps are at the basis of the applicable ethical-legal framework: the first one refers to the identification of relevant threats and risks for data protection and data subjects' fundamental rights (including security and data protection requirements); the second one is a clear understanding of the corresponding responsibilities. In other words, it is often required or recommended to go through a data protection impact assessment evaluation under article 35 GDPR to identify technical and organizational measures that shall be implemented to make any possible attempt to the integrity, availability, and confidentiality of data flows ethically and legally acceptable. As a standard criterion, all data processing activities and endpoints shall embed privacy-preserving techniques in accordance with the identified level of risk emerged during the impact assessment. In this regard, the European Union Agency for Cybersecurity (ENISA) identified a tool to guide the assessment activities, including a library of measures to be applied to mitigate for any level of perceived risks for the data flow [13].

The developer shall deal with the following issues to undertake the impact assessment: security and integrity of systems (either in terms of cybersecurity or governance), aims and purposes of data processing activities (also considering the data subjects' perspective), duration and data retention policies (to comply with the principle of minimization), nature and types of processed data (to comply with the lawful principle), information to data subjects and their rights (to comply with the principle of transparency), flows of data and different controllers or processors to set the governance and maintain the control upon the data flows. In the healthcare sector, many agents are potentially involved: hospitals, telco operators, cloud providers, clinicians, and patients as end-users. Thus, it is crucial to recognise and support operators with different roles and responsibilities that shall be assigned by design. In particular, Data Controllers, under article 25 GDPR, are responsible for handling the whole data life cycle, by determining means and purposes of the processing, and they are in charge of establishing or amending technical and organizational measures to ensure that personal data processing fully complies with regulatory requirements. A series of consultants may intervene in the assessment to tailor the technology to the specific scenario (e.g., the Data Protection Officer, the IT services, the stakeholders' representatives, etc.).

Considering that the GDPR structure of rights and obligations has affected also other legislative initiatives on data protection laws (e.g., in Brazil, Israel, and in part also in China and USA), since the extra-EU flows are facilitated whereas the non-EU legislation is aligned (*rectius* it received an adequacy decision) with the GDPR, the proposed risk-based approach seems particularly useful also beyond the EU borders and it could contribute to an interdisciplinary and international standardization debate on the topic [14].

IV. THE 5G-SOSIA SYSTEM FOR EMERGENCY CARE AND PUBLIC HEALTH

The 5G-enabled SOS Intelligent Assistant (5G-SOSIA) project [15] proposes a system to jointly improve the response to emergencies and the personalized healthcare. The flexibility of the proposed system is such that it can be used for preserving public health in general. The 5G-SOSIA system main elements are: an RFID patch that a person can carry (e.g., attached to a necklace, an earring, a bracelet or embedded into a smartwatch); a remote device that an informal caregiver can use to read the information stored in the RFID patch and connect to the 5G network, an AI-assisted dispatching engine deployed in the edge-cloud of the emergency system [16], [17]. Because of the current COVID-19 pandemic situation, it should be emphasized that the proposed system is able to read the necessary data in a contactless way, thus preserving the informal caregiver's and the patient's health.

As shown in Figure 1, an informal caregiver assists a patient during an emergency. The informal caregiver uses the closest 5G-SOSIA remote device to automatically read the information stored in the 5G-SOSIA RFID patch. This behavior is based on the same working principle of the Automated External Defibrillator (AED) that can be used by anybody. Different information can be stored in the patch, depending also on the privacy policies to be implemented (a more detailed explanation of this issue is provided in the following sections). For example, the patch stores the patient's medical history or data identifying the patient's record in an electronic health record stored elsewhere. The only action performed by the informal caregiver is to bring the 5G-SOSIA remote device close to the patient's patch. The 5G-SOSIA remote device performs all other actions, described below, automatically. In such a way the first aid provided by the informal caregiver is facilitated.

As soon as the 5G-SOSIA remote device is in the proximity of the 5G-SOSIA patch a data and voice call is initiated. Necessary data are transmitted to the emergency center. The simultaneous voice call is used by the emergency center staff to interact with the informal caregiver for guidance in the patient's first aid procedure. The 5G-SOSIA AI-assisted dispatch engine processes the patient data to support the emergency dispatch center personnel to select the most suitable emergency center and optimize the patient care. Processing is based on information collected through the data available in the patient patch from different databases (e.g., patient's historical data) and on information related to available emergency means of transport and to hospital capacities (e.g., type of care provided, availability of beds).

In this study, the 5G-SOSIA system is applied to a recent emergency: the COVID-19 pandemic. Specifically, as illustrated in Figure 2, it is utilized to monitor social/physical distancing. However, such scenario is only one of the many scenarios where the 5G system can be employed. The 5G-SOSIA system has been devised for the interaction between two end users: the informal caregiver and the emergency dispatch center. However, the 5G-SOSIA

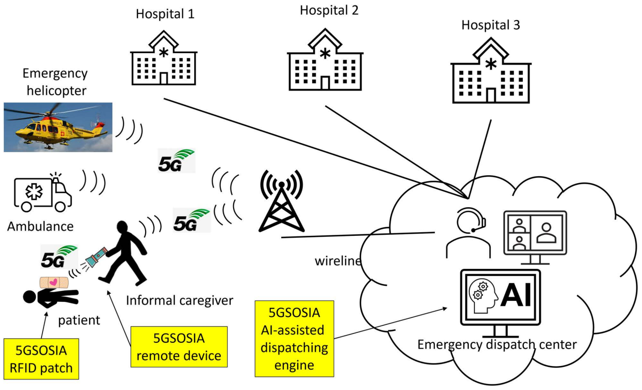

FIGURE 1. 5G-SOSIA system architecture.

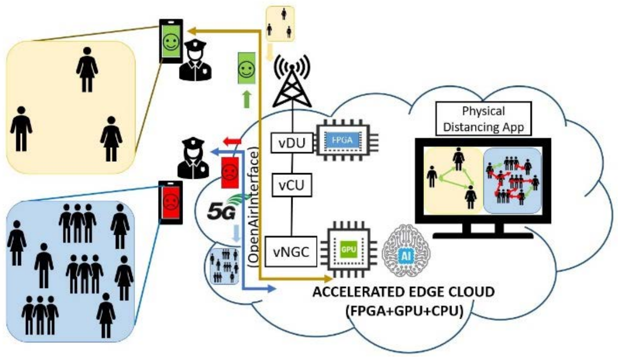

FIGURE 2. Social/physical distancing scenario.

architecture has been designed with flexibility in mind so that the two end-users can be played by different actors. In specific cases the two actors can be replaced by an intelligent autonomous machine. Moreover, the 5G-SOSIA system could be used in situations where any close contact between patient and informal caregiver shall be avoided. Furthermore, any scenario in which crowd management shall be implemented can leverage the 5G-SOSIA system, such as directing people in emergency situations.

In the case of social/physical distancing management, one end user is represented by the personnel (e.g., a policeman) that oversees physical distancing while the other one is represented by an intelligent autonomous social distancing verification program based on AI/ML. The policeman smartphone (i.e., UE) captures images of a crowded area. The smartphone sends the raw images to an edge cloud by means of the 5G network. The edge cloud is equipped with general and specialised programmable hardware (e.g., CPU, GPU, and FPGA) and it hosts several functional elements. It hosts virtualised 5G Radio Access Network (vRAN) and Next Generation Core (vNGC) functions. It also hosts an AI/ML-based physical distance calculation application.

The physical distancing application processes, anonymises, and does not store, for privacy reasons, the images received through the 5G fronthaul and backhaul network. The output of the elaboration is then sent back to the UE. The response consists of either a green (i.e., physical distancing satisfied) or red (i.e., physical distancing not satisfied) symbol.

The proposed system exploits accelerated computation in the edge cloud. Thus, thanks to the exploitation of more powerful and specialized hardware than the one available in the smartphones, smartphone battery is preserved, and image processing is faster. Moreover, the 5G enhanced mobile broadband capacity sensibly reduces the time needed to send the images to the edge cloud and receive the response.

V. 5G-SOSIA SYSTEM FOR SOCIAL DISTANCING EVALUATION

In the following a 5G-SOSIA system implementation is detailed together with its performance evaluation in a laboratory testbed. In addition, a preliminary data protection risk analysis is provided.

A. SYSTEM IMPLEMENTATION AND PERFORMANCE EVALUATION SCENARIO

The physical distancing implementation setup, shown in Figure 3, consists of the following devices: a commercial smartphone, that is used as a User Equipment (UE); a Universal Software Radio Peripherals (USRPs) Ettus X310, that is employed as gNB Radio Unit (RU) performing Radio Frequency (RF) functions; two Dell PowerEdge R740 servers each one with 2 processors (8 cores per processor) at a 3.6GHz clock frequency, that host the Distributed Unit (DU) and Central Unit (CU) in bare metal and the Next Generation Core (NGC) functions in a Docker Container; an NVIDIA Tesla T4 GPU featuring 320 NVIDIA Turing tensor cores. Because of the low profile PCIe, the NVIDIA T4 supports all AI frameworks with 50x higher energy efficiency compared to the CPUs [19].

The utilized mobile software is OpenAirInterface [18]. The radio access network (RAN) utilizes a 10MHz wireless channel bandwidth. Functional split option 2 is utilized. The DU implements PHY, Media Access Control (MAC), and Radio Link Control (RLC) functions of the mobile protocol stack. The CU implements the Packet Data Convergence Protocol (PDCP) functions. The NGC is implemented by means of the OAI Core Network (CN).

The accelerated edge cloud equipped with the NVIDIA Tesla T4 hosts, beyond the NGC, the physical distancing app. The physical distancing app is based on an open-source physical distancing app exploiting You Only Look Once version 3 (YOLOv3) [20]. The app contains the COCO dataset for object detection [21]. The physical distancing app detects physical distancing violations by performing the following steps. First the application performs person detection. The person is detected by simultaneously computing the bounding box coordinates and class label probabilities of the received input image. The images are streamed by the smartphone utilizing the IPwebcam application. The person prediction probability and the bounding box coordinates with the centroid are provided. Non-maxima suppression (NMS) is also

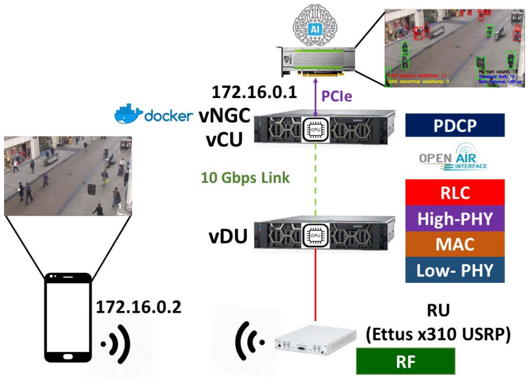

FIGURE 3. Physical distancing application setup.

used in person detection to reduce overlapping boxes to only a single bounding box to ideally count the number of persons in each frame. Then, the application computes the distance between detected individuals. Euclidean distances between all pairs of the centroids are computed based on the number of pixels (N). Three different distance violations are defined based on Maximum (N_{MAX}) and minimum (N_{MIN}) violation limits based, also, on the distance of the person from the camera: *no violation (green)* if $N > N_{MAX}$; *abnormal violation (yellow)* if $N_{MAX} > N > N_{MIN}$; *serious violation (red)* if $N < N_{MIN}$.

B. EXPERIMENTAL RESULTS

The experimental results evaluate an important performance parameter for image processing: the *response time*. The response time is defined as the time needed for a single image elaboration (i.e., in this case the person detection and distance calculation in each frame). The response time is the inverse of the Frames per Seconds (FPS) (i.e., *1/response time)*, that is the number of frames that can be elaborated in a second.

The implemented system, shown in Section V-A, is compared with the standalone implementation where the web camera is connected to a desktop PC with Intel Core i7-7700K CPU @ 4.2 GHz, and the CPU performs the person detection and distance calculation.

After running the physical distancing implementation in GPU and CPU, results show that the former can process images at *6.90 FPS* while the latter can process them at *3.64 FPS*. Thus, response time is of about 145 *ms* and 275 *ms*, respectively. It must be noted that if the frames are sent faster (e.g., 20 FPS) than the frame processing rate, the frames arriving within the elaboration of the previous frame are discarded by the physical distance app. However, such evaluation does not consider the frame propagation delay within the 5G network.

The round-trip time (RTT), measured through *ping,* between the UE and the server hosting the Tesla T4 in the setup shown in Figure 3, is around *25ms*. By summing the half of the RTT experienced by the UE-Tesla T4 communication a response time of about 170 *ms* is obtained, resulting in an equivalent *FPS* of around *5.8 FPS* for the accelerated edge-based implementation.

Thus, the experiment shows that the accelerated edge core implementation of the physical distancing application can achieve a higher FPS and a shorter processing time compared to its implementation in a CPU, even if some time is needed to send the images to the GPU through the 5G network for elaboration.

Another parameter used to evaluate the performance of the CPU- and GPU-based implementation is the energy usage per frame. This is quantified as the amount of power consumed by the hardware (GPU or CPU) during the physical distancing application elaboration of a single frame. Results show that performing the social distancing application in the GPU requires *2.58J* of energy per frame while *12.21J* of energy is used in the CPU. Thus, the CPU-based implementation needs *4.73* times more energy than the GPU-based implementation making GPU more energy-efficient than the CPU.

C. DATA PROTECTION AND FUNDAMENTAL RIGHTS RISK ANALYSIS

Considering the legal frameworks outlined in the previous sections, the implementation of physical distancing raises several issues whose impact assessment needs to be addressed.

Personal data flows must be identified and recorded, not only when the GDPR, or similar obligations, applies but also as an organizational measure. This would allow to identify and manage possible risks in processing activities.

The first consideration concerns the *type of personal data* collected by the system. In the considered scenario, personal images, their geolocation, and their distance represent personal data and the purpose of the technology is to prevent and manage the flow of people, in aggregate, in case of emergency situations. Thus, based on the principle of minimization, images could be pseudonymized at least and any facial recognition should be avoided.

Another important aspect is the *access to the collected information* that shall be limited to instructed and authorized persons/organizations. Required security measures shall be implemented that can always trace any access or alteration. A tailor-made data breach policy shall be agreed between the parties involved and a data protection impact assessment shall be carried out and kept up to date.

As for the data used to train the algorithm, it is important to remark that the algorithm training is a different purpose respect to the physical distancing one. Furthermore, the same data shall be collected by different controllers (e.g., the developer) respect to the ones that are involved in the operational scenario. Under these premises, a physical separation of the two flows might ensure for instance that non-pseudonymized data could be processed only by the developer and for a limited period. At the same time, it could increase the risk of external threats and breaches. In the specific context, it could be evaluated a proper balance, depending on the techniques applied to encrypt and decrypt data flows.

Another crucial profile is that of *data retention*: according to the principles of purpose and minimization, it appears that images are collected and immediately pseudonymized with a face blurring technique, then transferred to the external server and processed together with the geolocation signal. The profiling provided by the AI solution is then linked to the prediction of the distance between each pseudonymized image associated with a given location. The distance signal can be overwritten in the physiology of the activity and only be recorded and stored if an emergency signal needs to be shared with the user of the physical distancing App via the App. After this signal, perhaps, the user of the physical distancing App could decide to destroy the data associated with the signal and keep it for further investigation/signaling.

Therefore, a more general risk analysis shall be combined with the algorithm training activity and performed during its development. This means that, as the algorithm is considered as ethical-legal compliant for the given purposes, in the peculiar application, it is necessary to consider also a re-assessment of its impact on fundamental rights protection under the three pillars of ethics, law, and technical robustness, where the step of training in the chosen scenarios is included.Another aspect to be analysed is the one related to the *rights of data* subjects. To guarantee the exercise of one's rights, a certain procedure must be indicated and described in the privacy policy. In such cases, the balance between legitimate and unlawful access requests must be predetermined, considering data retention policy and public policy purposes.

A further important aspect is the *general assessment of technology* with respect to human police/security support through an App. The technology aims to support the decision-making process of educated operators who might show different attitudes towards the automated system (from experience of the digital divide to distrust of the technology). Before adopting a system such as the one currently analyzed, a specific training and awareness-raising campaign is therefore necessary. Indeed, new skills and competences may be needed even if the app interface is not expert. These profiles are part of an overall assessment of the technology and its sustainability in each context.

Finally, the development of a technology that introduces a surveillance system could be justified under certain conditions but, if possible, abuses and the related countermeasures are foreseen to *avoid discriminatory scenarios*. For instance, the detection of social distancing in public places could be useful in the context of COVID-19 containment measures, in the context of large events to manage unprecedented flows of people, but it constitutes a surveillance measure if the same data flows are cross-referenced with other datasets (such as those of mobile phones, for instance) that could be instrumental in undermining personal freedom and privacy, understood as the right to privacy, not just data protection.

At the end of this very preliminary risk assessment, it is worthwhile to note that any evaluation conducted for the social distancing purpose cannot be automatically extended to other purposes, any of which would require a new assessment and new suggestions.

VI. CONCLUSION

This paper reviewed both the technical and the privacy requirements that mobile health services are requesting to 5G. Then, it proposed a framework for physical distancing management. The framework is based on 5G connectivity and accelerated edge cloud. Experimental results showed that the proposed framework, exploiting GPU-based edge computation, is capable of elaborating images for physical distancing computation almost three times faster than a standalone implementation. In addition, it requires lower energy. Finally, the edge-based implementation can be easily extended to perform more complex and collaborative computations, such as merging different scenes.

REFERENCES

[1] K. Bilal, O. Khalid, A. Erbad, and S. U. Khan, "Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers," *Comput. Netw.*, vol. 130, pp. 94–120, Jan. 2018.

[2] E. Li, L. Zeng, Z. Zhou, and X. Chen, "Edge AI: On-demand accelerating deep neural network inference via edge computing," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 57–447, Jan. 2020.

[3] B. Anthony, Jr., "Use of telemedicine and virtual care for remote treatment in response to COVID-19 pandemic," *J. Med. Syst.*, vol. 44, no. 7, pp. 1–9, Jul. 2020, doi: 10.1007/s10916-020-01596-5.

[4] R. A. Stein, "COVID-19 and rationally layered social distancing," *Int. J. Clin. Pract.*, vol. 74, no. 7, Jul. 2020, Art. no. e13501, doi: 10.1111/ijcp.13501.

[5] B. Etzlinger, B. Nusbaummuller, P. Peterseil, and K. A. Hummel, "Distance estimation for BLE-based contact tracing—A measurement study," in *Proc. Wireless Days (WD)*, Jun. 2021, pp. 1–5, doi: 10.1109/WD52248.2021.9508280.

[6] S. Saponara, A. Elhanashi, and Q. Zheng, "Developing a real-time social distancing detection system based on YOLOv4-tiny and bird-eye view for COVID-19," *J. Real-Time Image Process.*, vol. 19, no. 3, pp. 551–563, Jun. 2022, doi: 10.1007/s11554-022-01203-5.

[7] *3GPP Work Item 840047 (CMED)*. Accessed: Sep. 25, 2022. [Online]. Available: https://www.3gpp.org/DynaReport/WiCr–840047.htm

[8] *3GPP Work Item 810016 (FS_CMED)*. Accessed: Sep. 25, 2022. [Online]. Available: https://www.3gpp.org/DynaReport/WiCr–810016.htm

[9] *Technical Specification Group Services and System Aspects; Service requirements for the 5G system; Stage 1 (Release 18)*, Standard 3GPP TS 22.261 V18.6.1, 3GPP, Jun. 2022.

[10] *Technical Specification Group Services and System Aspects; Study on Communication Services for Critical Medical Applications (Release 17)*, Standard 3GPP TR 22.826 V17.1.0, 3GPP, Dec. 2019.

[11] *D3.2: Initial Solution and Verification of Healthcare Use Case Trials, Revision: V.2.1*, document 5G-HEART project, May 2020.

[12] G. Comandè, "Regulating algorithms' regulation? First ethico-legal principles, problems, and opportunities of algorithms," in *Transparent Data Mining for Big and Small Data*, T. Cerquitelli, D. Quercia, and F. Pasquale, Eds. Cham, Switzerland: Springer, 2017, p. 169.

[13] ENISA. (2018). *Handbook on Security of Personal Data Processing*. [Online]. Available: https://www.enisa.europa.eu/risk-level-tool/risk

[14] D. Amram, "The role of the GDPR in designing the European strategy on artificial intelligence: Law-making potentialities of a recurrent synecdoche," in *Proc. Opinio Juris Comparatione*, 2020, p. 1.

[15] Accessed: Sep. 25, 2022. [Online]. Available: https://www.5gsosia.it/

[16] J. C. Borromeo, K. Kondepu, S. Fichera, P. Castoldi, and L. Valcarenghi, "Experimental demonstration of scalable and low latency crowd management enabled by 5G and AI in an accelerated edge cloud," in *Proc. Opt. Fiber Commun. Conf. (OFC)*, 2021, pp. 1–3.

[17] L. Valcarenghi, A. Pacini, J. C. Borromeo, S. Fichera, M. Gagliardi, D. Amram, and V. Lionetti, ''A framework to support social distancing management based on 5G and accelerated edge cloud,'' in *Proc. IEEE Int. Medit. Conf. Commun. Netw. (MeditCom)*, Sep. 2021, pp. 94–99, doi: 10.1109/MeditCom49071.2021.9647551.

[18] *Openairinterface*. Accessed: Sep. 25, 2022. [Online]. Available: https://www.openairinterface.org/

[19] *Nvidia Tesla T4*. Accessed: Sep. 25, 2022. [Online]. Available: https://www.nvidia.com/content/dam/en-zz/Solutions/Data-Center/tesla-t4/t4-tensor-core-product-brief.pdf

[20] *Social Distancing Detection in Real Time*. Accessed: Sep. 25, 2022. [Online]. Available: https://github.com/saimj7/Social-Distancing-Detection-in-Real-Time

[21] J. Redmon and A. Farhadi, ''YOLOv3: An incremental improvement,'' 2018, *arXiv:1804.02767*.

LUCA VALCARENGHI (Senior Member, IEEE) has been an Associate Professor at Scuola Superiore Sant'Anna, Pisa, Italy, since 2014. He has published more than 100 papers in international journals and conference proceedings and actively participated in the TPC of several IEEE conferences, such as GLOBECOM and ICC. His research interests include optical networks design, analysis, optimization, artificial intelligence optimization techniques, communication networks reliability, fixed and mobile network integration, fixed network backhauling for mobile networks, and energy efficiency in communications networks. He received a Fulbright Research Scholar Fellowship, in 2009, and a JSPS ''Invitation Fellowship Program for Research in Japan (Long Term),'' in 2013.

ALESSANDRO PACINI received the bachelor's degree in computer science from the University of Camerino, in 2018, and the joint master's degree in computer science and networking from the University of Pisa and Scuola Superiore Sant'Anna, Pisa, Italy. He is currently pursuing the Ph.D. degree in emerging digital technologies with Scuola Superiore Sant'Anna. During this period, he won a one year research scholarship at SSSA, focused on building up a scalable and reliable monitoring architecture for optical networks. His research interest includes the field of the closed loop automation, with a specific focus on reusing existing network architectures to be shifted over a zero-touch paradigm.

JUSTINE CRIS BORROMEO received the B.S. degree in electronics engineering from the Iligan Institute of Technology—Mindanao State University, in 2015, and the M.S. degree in electronics engineering from the Ateneo de Manila University, in 2019. He is currently pursuing the Ph.D. degree in emerging digital technologies with Scuola Superiore Sant'Anna, Pisa. His research interests include radio access networks in 5G technologies, FPGA and GPU-based hardware acceleration, and 3D networks.

SILVIA FICHERA received the Ph.D. degree in emerging digital technologies, curriculum photonic technologies from Scuola Superiore Sant'Anna, Pisa, Italy, in 2019. She worked as a Research Assistant with Scuola Superiore Sant'Anna, until 2021, when she has joined Vodafone as a Senior Software Engineer, where she manages AIML projects for network virtual infrastructure. Her research interests include AIML application for future networks, business intelligence, network control and management, software defined networking, network security, and cloud computing.

MARIA GAGLIARDI received the Ph.D. degree in comparative law from the University of Florence. She is currently an Associate Professor in private law at Scuola Superiore Sant'Anna, Pisa. Since 2011, she has been teaching insurance law at the Department of Economics, University of Pisa. Her research and teaching interests include insurance law, privacy data protection and new technologies, tort law (mainly medical malpractice and personal injury damages), family law (mainly identity issues and protection of children), individual protection and risk society, and several interactions of related topics.

DENISE AMRAM received the Ph.D. degree in law, in 2012. She is currently an Assistant Professor in private comparative law at the LIDER Laboratory—DIRPOLIS Institute, Scuola Superiore Sant'Anna. In 2018 and 2021, she worked as a Data Protection Officer at Scuola Superiore Sant'Anna and Scuola Normale Superiore. She has coauthored around 110 publications in Italian, French, English, and Spanish, including a book and two co-editions. Her research interests include fundamental rights protection in the fields of data protection law, family law, tort and contractual liability in a national, EU, and comparative perspective.

VINCENZO LIONETTI received the Ph.D. and M.D. degrees. He has been an Associate Professor at Scuola Superiore Sant'Anna, Pisa, Italy, since 2014, and has been an Anesthesiologist at Fondazione Toscana G. Monasterio, Pisa, since 2009. He has published more than 110 papers in peer-reviewed international scientific journals, has authored two patents, and actively participated in several national and international working groups. He received the International Fellowship of American Heart Association: Council on Basic Cardiovascular Sciences (F. A. H. A.), in 2010. He was a Visiting Scholar at the University of Maryland, in 2011. His research interests include cardiovascular pathophysiology and epigenetics, strategies of perioperative cardioprotection and cardiac monitoring, and heart-brain axis in critical ill patients. He serves as an Editorial/a Reviewer Board Member of several Q1 scientific journals, such as the *American Journal of Physiology-Heart and Circulatory Physiology* and the *European Heart Journal*. He has been invited as an Expert with the European Research Executive Agency, since 2013.

• • •

Open Access funding provided by 'Scuola Superiore "S.Anna" di Studi Universitari e di Perfezionamento' within the CRUI CARE Agreement