Advances in Science, Technology and Engineering Systems Journal Vol. 6, No. 4, 44-51 (2021)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ
ISSN: 2415-6698

Remote Patient Monitoring Systems with 5G Networks

Antonio Casquero Jiménez*, Jorge Pérez Martínez

Signal System and Radiocommunication Department, Polytechnic University of Madrid, Madrid, 28040, Spain

ARTICLE INFO

Article history:
Received: 03 May, 2021
Accepted: 15 June, 2021
Online: 10 July, 2021

Keywords:
5G
IoT
Remote patient monitoring
eHealth

ABSTRACT

The new generation of mobile communications and the recent advances in data management are going to enable a fast transformation in the health sector of many countries. 5G networks, with superior technical characteristics, would allow the development of a new set of application and services gathered under the concept of eHealth. In this article we propose a remote monitoring system based on 5G networks that would allow to provide a varied set of medical services from long distance. However, for achieving an optimal performance, the network must guarantee high bandwidths and low latencies, at the time that a massive number of devices and its corresponding generated data are handle efficiently. Consequently, an appropriated system architecture and data model structure are proposed, taking into consideration the high security requirements that any health-related application or service inherently implies.

1. Introduction

Today, health systems in many countries are facing some important sanitary challenges regarding an increasingly aging population, the rise of chronic diseases and the Covid-19 pandemic. In this context, the digital transformation of the health sector with the development of new services supported by the latest technological advances is considered as an indispensable way of saving expenses, optimizing the resources of the sector, and obviously improving the populations welfare. As a result, concepts such eHealth and technologies as 5G or IoT have become essential elements in this digitalization process.

Most of the new and innovative applications and services that are expected to appear in the following years would arise from the combination of 5G and IoT and would be generally supported on Big Data and Artificial Intelligence techniques. Among them, remote patient monitoring systems would be one of the most popular and deployed applications.

This paper is an extension of the paper "5G networks in eHealth services in Spain: remote patient monitoring system", originally presented by the authors in the 2020 IEEE Engineering International Research Conference (EIRCON) [1]. In addition to the results and achievements presented in [1], in this current article we deepen in the theorical concepts behind the solution proposed, emphasising the role of 5G networks. Although the general system architecture is the same as the one presented in [1], this paper extends its study providing a more detailed description of the involved elements and their function within the system. Finally, and in addition to the initial results gathered in [1], the security and data privacy of the remote patient monitoring system proposed is analysed.

1.1. The remote patient monitoring service: definition and communication requirements

Remote patient monitoring (RPM) is an eHealth application that consists in the monitorization of a patient's health state with sensors, wearables or medical devices that measures vital and contextual parameters such as temperature, pulse, sugar or oxygen in the blood, among others [2]. Moreover, the term RPM also includes the applications and platforms that allows the analysis of medical data by means of BigData and artificial intelligence (AI) techniques to provide self-consultation and evaluation by doctors. In general, these applications are especially designed for the monitoring and follow-up in real time of patients with different illnesses, although the uses of RPM systems can be directed to other use cases such as the follow-up of post-operative processes.

According to the predictions done by STL Partners [3] remote patient monitoring applications would be one of the main eHealth services in the next decade, experimenting a tremendous growth, following the trends of a more personalized and continuous home centric health care. In addition, and thanks to the use of 5G networks, the forecasts determine that the adoption of these kind

*Corresponding Author: Antonio Casquero, Polytechnic university of Madrid, Madrid, 28040, Spain, +34649034991, acasquerojimenez@gmail.com

https://dx.doi.org/10.25046/aj060406

of applications could lead to more than 50 Billion USD of global annual cost savings for the health sector by the year 2030 [3].

However, these kinds of applications impose important communications requirements being the availability of a wide coverage area the most important one, as it is mandatory for a remote patient monitoring system to connect all the agents that might be involved such as patients, doctors, caregivers, or even patients´ family members [4]. Nevertheless, it is also crucial to consider the network's capacity to efficiently manage a large number of connected devices, as the network that supports the system must be able to handle an increasing deployment of devices without impacting the service performance. In this line, the security and reliability of the data transmitted must be guaranteed, as well as the continuity of the service so that patients are monitored at all times. Special attention must also be paid to coverage in indoor environments, as most of the sensors and devices deployed will be located in these environments [4]. On the other hand, both energy consumption and battery life of the devices are critical aspects to consider in order to have self-sustaining connected devices, whose batteries are adapted to the duration of the medical processes. Likewise, remote monitoring aplications imposes requirements related to high-speed mobility, especially in the case of emergency situations.

In the following table the main communication requirements can be summarized. However, it is worth mentioning that these would considerably depend on the medical service derived from the system.

Table 1: Technical requirements of RPM systems [5]-[7]

Use case attribute	Value
Throughput	< 1Mbps
Latency	<50ms
Reliability	99,99%
Number of devices	10-10^4/km^2
Battery duration (use case dependant)	10 years
Security	Critical
Mobility	0-500 km/h
Coverage	Important, including indoor
Indoor coverage	No critical 1-10 m horizontal, < 3m vertical

1.2. Organisation of this paper

This paper is structured as follows. In section 44 we have provided the definition of remote patient monitoring as well as an analysis of the requirements imposed by these types of systems. In section 2 we study the main technologies involved in the provision of the connectivity required in RPM systems whereas in section 3 we present a RPM system architecture based on 5G networks. Afterwards, in section 4, a data model for the adequate treatment and management of the data in the system is proposed. In the next section, two crucial aspects such as the security and data privacy of the system are reviewed playing special attention to the advantages of 5G in this context and the possible additional measures that could be taken. Finally, in section 6, the conclusions of the paper are presented.

1.3. Related projects and papers

The development of 5G networks as well as the possible services derived from them are still in an early stage, moving from the commercial verification period to the small-scale deployment of certain solutions. Consequently, to the best of our knowledge, there are no commercial systems or solutions such as those proposed in this paper, although it is true that in the specialized literature, we do find truly interesting proposals.

In [8], the authors present a continuous monitoring system based on 5G networks using wearables and sensors. The devices measure certain vital parameters and via Bluetooth, they send the captured data to the smartphone, which then forwards the data to external servers through 5G networks. In this project, they also propose an intelligent algorithm for decision making and alert generation based on the evaluation of the measured parameters. On the other hand, in [9] they propose a remote monitoring system for smart environments based on IoT and on the existing 4G network infrastructures. In this article, they analyse the communication requirements of the system, especially those referred to the bandwidth, and perform a detailed study of the communication protocols. In this context [10] designs a home monitoring system based on 5G networks and Edge computing with the scope of treating remotely chronic diseases and to promote active aging, in line with the developments and advances reported in [11]. From another perspective, in [12] they also propose the joint use of short-range networks and mobile networks, as an optimal way to develop a remote monitoring system, putting in this case special emphasis on the security of the system and its vulnerabilities. Finally, and with a more general approach, in [13], in addition to a complete review of 5G technology and its applicability to the healthcare sector, they propose a 5G network architecture capable of supporting multiple medical services, including patient monitoring. The system is characterized by the joint use of small cells and macro cells and the deployment of computing and processing servers in the edge. The requirements that eHealth applications impose on telecommunication networks and, in particular, the suitability of 5G networks to meet them are also presented in [13].

2. Connectivity Technologies

The development of eHealth services and applications, like the one we are analysing in this paper, would appear from the combination of 5G and IoT. However, it is worth mentioning the important role that Big Data and Artificial Intelligence techniques and algorithms would play regarding the intelligent analysis of the data generated by these systems. Indeed, the role of data treatment and management platforms is considered indispensable, as they provide a secure and ubiquitous source of information for the consultation of the generated data among all the agents involved in a particular service [2].

However, in this section we focus on the main connectivity technologies involved in the provision of remote patient monitoring systems. These technologies must take into consideration the requirements defined in section 1.1 and must satisfied them properly.

2.1. 5G

5G is the new paradigm of wireless communications designed to support a wide variety of services. 5G networks improve considerably the performance of the previous generations of mobile communications thanks to the introduction of a new radio interface known as "the New Radio" (NR) and the redefinition of the core of the network resulting in the 5GCN (5G Core Network) [14].

In addition, the 5G system is defined as a service-based architecture (SBA) that through the recent advances in network function virtualisation (NFV) and software-defined networking (SDN) allows a flexible usage and configuration of network functions. As a consequence, different use cases with very diverse requirements can be defined by means of network slices and consequently multiple verticals can develop their services within a single physical infrastructure [15].

The new frequency bands, which include the ultra-high capacity mmWaves, the new waveform used, the utilization of massive MIMO techniques, or the use of heterogeneous access networks, which supports non 3GPP standardised access networks, jointly with the improvements in the network architecture, allows 5G networks to offer the following characteristics [1]:

- Guaranteed user data rate of 100Mbps in DL and 50 Mbps in UL with peak rates of 20Gbps.
- 1/10 X in end-to-end latency, reaching delays of 1 ms.
- Service transmission reliability of >99.999%
- 1000 X in number of IoT devices reaching a density of 1 million terminals/km^2
- 1/10 X in energy consumption

Finally, it is worth mentioning the recent advances in Multi-access edge computing (MEC) technology regarding 5G networks. This concept enables to bring cloud computing processes and storage (typically performed in the core of the network) closer to the final users. Running these processes in close proximity to end users, for example in the 5G base stations, reduces network congestion and improves applications performance by providing faster and more reliable connections with lower latencies [16].

2.1.1. *Why 5G?*

The characteristics and advantages of 5G networks in the provision of medical services can be summarized in the following points:

- Reliability and security. The ultra-reliable connections of 5G networks are the main driver for the utilization of this technology for the development of eHealth applications as patient´s data privacy and service continuity can be guaranteed. Network slices isolation, advanced data encryption techniques and the new and improved authentication mechanisms contribute to this objective.
- High performance. As we have stated in the previous section, 5G networks provide high average data rates and ultra-low latencies, fulfilling the requirement of a wide majority of medical services, including the one we are analysing. Massive MIMO with 3D beamforming and Edge computing and MEC (Multi-access Edge Computing) platforms are some of the innovations included in this field of action.
- Ultra-high Capacity. With up to one million of devices per Km^2,5G networks can efficiently manage the simultaneous connections of multiple medical devices from multiple users. Beside this, these networks provide 90% reduction in energy consumption with 10 years of battery life for low power IoT devices.

2.2. IoT

IoT ("Internet of things") consists in the grouping and interconnection of devices and objects through a network. As we can infer from this definition, RPM systems can be classified as an IoT application, in which the technology chosen for the provision of such connectivity would be 5G [1]. In 5G networks, we can define different categories of IoT according to their requirements [17]: Massive IoT, Broadband IoT, Critical IoT and Industrial Automation IoT. The characteristics of RPM system can be included within the framework of the massive IoT and Broadband IoT.

2.2.1. *Massive IoT*

Massive IoT intends to provide connectivity to a very large number of devices that transmit and/or receive small volumes of data. These devices, that frequently rely on battery power supply, are usually low-cost and can be located in remote places with little coverage [18].

In this context, LTE-M (LTE-MTC) and NB-IoT (Narrowband-IoT), both standardized by the 3GPP [19], fulfil all 5G requirements from both ITU and 3GPP for massive machine type communications. Although they are both LTE technologies, they are designed to coexist within the new 5G NR, thanks to techniques such as Dynamic spectrum sharing (DSS), defined in Release 15, and the numerology used by the sub-carriers, compatible with the NR.

Table 2: Technical comparison of NB-IoT and LTE-M [18].

Characteristics	NB-IoT	LTE-M
Bandwidth	180 KHz	1.4 MHz
Subcarrier bandwidth	15 KHz	15 KHz
Peak data rate	250 Kbps	1 Mbps
Latency	1.5-10 s	50-100 ms
Battery duration (use case dependant)	+10 years	10 years
Operation mode	FDD	FDD/TDD
Voice support	No	Yes
Coverage DL (MCL)	164 dB	164 dB

Coverage UL	Gain: 20dB	Gain: 15 dB
Indoor coverage	Excellent	Good

2.2.2. *Broadband IoT*

Broadband IoT is a category of IoT developed from mobile broadband communications (MBB). The introduction of 5G with the NR and the new frequency bands, allows offering IoT services with higher data rates and lower latencies than those offered by mIoT technologies, reaching peak values of tens of Gbps in transmission and latency values of 5ms [17]. Currently, many broadband IoT applications are being developed due to the already mentioned combination of MBB features (high bandwidth, high transmission speed, low latencies) with the characteristics of IoT services (wide coverage range, energy efficiency).

In this context, it is worth mentioning that the 3GPP as part of Release 17 [20], has introduced a new concept defined as the 5G NR-Light. It consists in a set of modifications of the 5G NR in order to reduce its capabilities to efficiently develop a set of IoT applications that will require devices more complex than those used in mIoT (massive IoT) communications but less complex than those used in 5G NR. These devices are usually going to be wireless industrial sensors (with low latencies and moderate transmission rates), video systems, high-capacity wearables, and patient monitoring systems.

3. RPM system architecture

Remote patient monitoring systems (RPM), as previously discussed, allows the monitoring of an individual's health status using sensors and/or wearables thanks to the control and measure of certain relevant medical indicators and parameters. Currently, we can find some remote monitoring systems models and proposals (section 1.3) in which these devices use personal area networks (PAN) such as Bluetooth and local area networks as Wi-Fi to connect to a hub (e.g. a smartphone) or a gateway. The data are collected and processed in mobile applications for smartphones that allow the patient to monitor and manage relevant medical information.

However, these applications are generally not standardized and therefore the monitoring processes performed does not have the required medical rigor. The systems should be able to send, periodically, or in real time, this medical data to authorized third parties, in order to obtain a more exhaustive analysis involving healthcare professionals and the use of Big Data techniques. This will facilitate diagnosis and follow-up tasks without the patient having to travel to the hospital or primary care center. In addition, it would be possible to detect anomalous patterns in the data and activate alarms in emergency situations.

Taking into consideration these aspects, an once we have described what is a RPM system and the main technologies involved, we present a possible system architecture based on 5G networks [1].

3.1. Functional high-level architecture

The system we propose is an open multiplatform system, based on European standards, which will allow the continuous monitoring of the health state of patients, as well as the possible detection of new pathologies and new therapeutic approaches.

The design of the network, responsible of providing the required connectivity, must be in line with the requirements of the proposed system where we highlight the massive creation of data by the end users (directly or indirectly) from multiple sources. In this context, the system and the network must guarantee the availability and security of the data so that the agents involved in the provision of health services can make use of the multiple applications and services that can be offered from the exploitation of these.

In order to obtain an open and scalable solution, both the data model and structure and the IoT architecture are based on the ETSI reference architecture, particularly on the ITU-T Recommendation Y.2060 [21], which offers the description of a reference model for IoT applications.

In the Figure 1 and taking the multilayer ETSI reference model as a reference, the functional high-level architecture of the system proposed is presented.

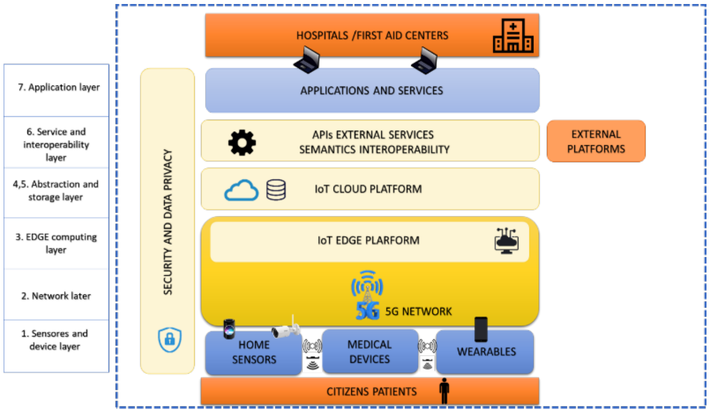
7. Application layer
6. Service and interoperability layer
4,5. Abstraction and storage layer
3. EDGE computing layer
2. Network later
1. Sensores and device layer
SECURITY AND DATA PRIVACY
HOSPITALS /FIRST AID CENTERS
APPLICATIONS AND SERVICES
APIs EXTERNAL SERVICES
SEMANTICS INTEROPERABILITY
EXTERNAL PLATFORMS
IoT CLOUD PLATFORM
IoT EDGE PLARFORM
5G
5G NETWORK
HOME SENSORS
MEDICAL DEVICES
WEARABLES
CITIZENS PATIENTS

Figure 1. Architecture of the proposed RPM system together with the ETSI reference layer model [1]

3.2. Architecture description

In this subsection we provide a detailed description of the different layers that define the system. The security and data privacy module, which covers all the layers of the system, will be studied in detail in section 5.

3.2.1. *Sensors and device layer*

This is the physical layer of the system that encompass a set of devices and sensors responsible of collecting information about the health status of the patient and of its environment [10]. In this layer we can find contextual sensors, medical devices and wearables that transmit and/or receive information directly over the mobile network without the need of using local networks (LAN OR WLAN) or gateways (routers or smartphones). However, we must also highlight the role that smartphones or virtual assistants can play in the system, due to the considerable number of sensors that they have integrated.

3.2.2. *Network layer*

5G networks will be the telecommunications network in charge of providing the connectivity in the system.

In our solution, we would mainly use low-cost devices and sensors that will perform periodic measurements of certain vital and contextual parameters, using narrow bandwidths. These would deal with very small amounts of data and will not require low latency values. Therefore, the best solution, as this scenario matches the characteristics of mIoT, is to use LTE-M or NB-IoT networks [1].

On the other hand, and in order to provide high performance monitoring applications, we can find another group of devices (advanced medical devices or high capacity wearables) that will perform measurements and monitoring processes of higher capacity. Consequently, they will require higher transmission rates and generally lower latencies. These devices would work with higher data volumes, and their requirements would be similar to those associated with Broadband IoT applications. As a result, we will use the 5G NR or 5G NR-Light [20].

Finally, we must highlight the possibility of using other wireless technologies, such as Wi-Fi 6, for connectivity at indoor environments. The new Wi-Fi standard, officially named as 802.11ax, is capable of providing theorical peak rates of 9.6 Gbps and can quadruplicate the number of simultaneous connected devices [22]. This new Wi-Fi standard, thanks to new security mechanisms and to the definition of network energy efficiency techniques, can effectively provide mIoT communications. The main advantage of this technology is the greater variety of sensors and devices that can be used, since the Wi-Fi 6 access points (AP) allows the integration of other communication modules (by means of external cards) associated to IoT communications such as RFID, ZigBee, and Bluetooth [22]. In this particular case, Wi-Fi 6 could provide indoor connectivity and 5G networks would act as backhaul technology.

This hybrid solution, which offers an optimized performance, is technically feasible thanks to the fact 5G network support multiple access technologies, even if they are not 3GPP standardized.

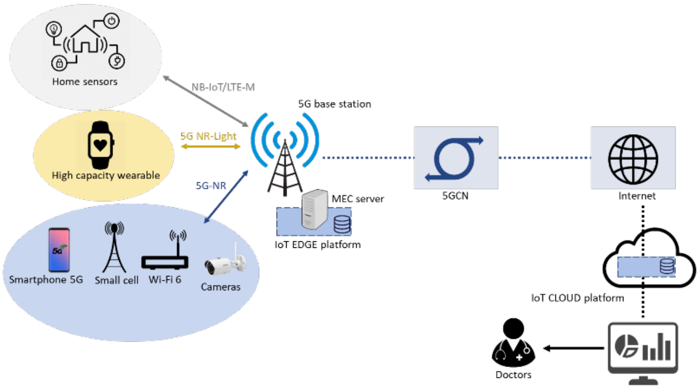

Figure 2: Representation of the global system architecture

3.2.3. *Edge computing layer*

The main function of IoT Edge platform is the integration and aggregation of the data collected in the previous layers and the transmission of the data to the cloud. The platform also carries out filtering and processing tasks in order to reduce the volume of data to be transmitted to the upper layers and consequently the bandwidth required. In this layer, a first analysis of the data can be made as analysing it in the proximity of the users makes it possible to improve the reaction or intervention in real time in cases of risk or emergencies and allows the execution of AI processes based on the collected data with very low latencies.

3.2.4. *Abstraction and storage level*

The abstraction and storage layer is encompassed by the IoT cloud platform, which is in charge of collecting the information processed by the previous levels, gathering the information from all the IoT Edge platforms deployed in a health region (south-bound) and integrating the semantic interoperability layer (north-bound).

Moreover, this platform is responsible of performing cloud computing tasks from the pre-processed data in the previous layers. At this level of the system is where the management of identities is performed as well as storage and administration tasks. The proposed platform is also where we carried out the intelligent analysis of the data [1]. In addition, thanks to the use of data models and information collection standards, the IoT cloud platform can manage information from various different sources such as IoT Edge platforms (user-generated data) or health systems (clinical history databases).

3.2.5. *Semantic interoperability layer*

The concept of semantic interoperability layer was introduced and developed in the ACTIVAGE project [11], a European project which develops IoT solutions for Smart Living Environments. However, the role of this layer is crucial for the proper development of the system and therefore it must also be included in our design.

The semantic interoperability layer allows the described IoT platforms to share data and exchange information with other external platforms thanks to the definition of interfaces and to the conversion of the data to a common model. Data from different sources are harmonized in using HL7 and the SNOMED vocabulary[10]. This layer also includes security and access control functions to the upper layers.

3.2.6. *Application and intelligent services layer*

The application layer enables the provision of a wide range of intelligent services from the captured and processed data. They are categorized as intelligent because in all of them there may be data processes that use artificial intelligence and/or big data techniques. The offered services are intended for patients but also for healthcare personnel or even informal caregivers of the patients. The final services can be adapted to the socioeconomic context of the region in which the system is deployed.

The most relevant medical services that can be derived from the proposed system are now presented. These services can address the main sanitary challenges considered in section 1:

- Chronic care services. Chronic diseases are progressively increasing every year over the population of many countries [23]. The RPM system proposed is expected to allow a personalized management and administration of patients with these conditions thanks to a rigorous and continuous follow up of the medical and contextual parameters that reflect their condition. In addition, the system could favor the capacity for early detection of diseases thanks to the predictive analysis of data running both in the Edge and in the cloud.

- Elderly care services. In this category we can include any service aimed at maintaining and improving the quality of life of the elderly. In this line monitoring services can facilitate the independence of the elderly allowing them to maintain an autonomous life away from health institutions for a longer period.
- Personal health self-management services. These are services aimed at people whose objective is the prevention of possible chronic diseases based on the detection of one or more conditions but in which there is still no organ damage.

4. System data model

The proposed RPM system, as can be inferred from the functional description of it, can be considered as data centric. The massive amount of data that the system has to handle jointly with the demanding security requirements that any health-related application imposes, demands a reorganization of the traditional data management procedures. The changes required in this respect, side with those introduced in 5G networks.

The aforementioned shift of paradigm implies that beyond the management of the devices involved in the monitoring processes, the system must establish mechanisms and tools for the efficient management of the data itself. In this context, and following the indications reflected in [24], the system should consider the following aspects:

- Data ownership. Patients should have control over the data generated by their monitoring devices. To this end, we must establish an ownership structure for the data and the devices, that allows to establish a relationship and association among them. This structure must allow the patient to manage, locally or remotely, the generated data.
- Data provenance. It is essential to create an immutable record of the source of the data, thus establishing a unique version of it. The system must be able to identify the device that generated the data and at what time it was generated. This information makes possible to guarantee the authenticity and veracity of the information collected.
- Data governance. Patients should be able to manage the access to their data, being able to grant permissions to third parties for external consultation.

Therefore, we can conclude that for data management in 5G networks, and by extension in our system, we must manage the data generated and the users with access to them. One possible solution consists in the utilization of two separate platforms, one in charge of property management and the other of data storage [24].

These concepts are particularly relevant in certain processes and management tasks that the system must perform. In the Figure 3, we show an example which reflects the registration of a device in the system and the access of an authorized third party to the data generated by it. In this scenario we have three entities: the patient, owner of the medical device, the medical device itself, which generates the data, and the healthcare personnel, who wishes to consult the generated medical data.

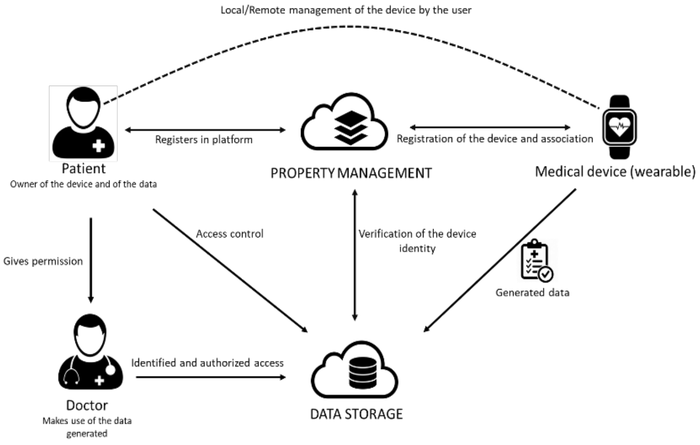
Local/Remote management of the device by the user
Patient
Owner of the device and of the data
Registers in platform
PROPERTY MANAGEMENT
Registration of the device and association
Medical device (wearable)
Gives permission
Access control
Verification of the device identity
Generated data
Doctor
Makes use of the data generated
Identified and authorized access
DATA STORAGE

Figure 3: System´s data management model. Based on [24]

As part of this registration process, the patient must register in the system in order to be able to add and associate to his/her identity different medical devices. This process will allow the user to manage the device and control the data generated by the it. Once the registration is completed, and as part of the monitoring process, the data generated will be stored in a data storage platform. This platform will verify the identity of the device and the authenticity of the stored data, which can be consulted by the patient or by authorized third parties.

5. Security and data privacy in the system

The proposed system is responsible of the creation, maintenance and exploitation of the data generated by the patients. In this context, as we are dealing with an application framed within the health sector, there is a series of legal obligations related to data security and privacy that must be considered and therefore, the system must be designed in line with the General Data Protection Regulation (GDPR) established by the European Union. Consequently, the Security and Privacy (S&P) module defined in our system architecture must cover all the layers, from the sensors and devices to the final applications, ensuring three main security principles: confidentiality, availability, and integrity.

In this context, 5G networks introduce a series of improvements in the security domain compared to previous generations of mobile networks. Moreover, we would define a set of specific security measures to enhance the system overall security.

5.1. 5G security improvements

5G networks offers better capabilities than other mobile technologies not only in terms of bandwidth, latency or density of devices that can be supported, but also in terms of security and data privacy. In this context, the main improvements are related to authentication procedures and to the encryption of the data in the network.

Authentication and identity management are fundamental aspects in cellular networks. In 4G networks, authentication tasks are performed establishing a mutual authentication process in which, by means of the authentication and key agreement (AKA) protocol, both the user's terminals and the network core validate their identities [25]. However, these processes do not include the encryption of the data in the access network in certain signalling processes, for example, when sending the user's identity. To this end, 5G networks encrypt the international mobile subscriber identity (IMSI) and extends the length of the session keys from 128 to 256 bits, thereby improving the protection of communication between the device and the network core [25]. In addition, fifth generation networks introduce a number of specific network functions designed to improve the security of authentication processes, such as the AUSF (Authentication Server Function) or the SEAF (Security Anchor Function) and defines a unified framework with new authentication methods: 5G-AKA, EAP-AKA and EAP-TLS [26]. This framework enables the authentication of a user's equipment independently of the access technology used, whether it is standardized by the 3GPP or not. This fact responds to the heterogenous access capabilities of 5G networks and is a concept extremely important in our system as we propose different access technologies as part of the solution, some of them non 3GPP standardized. Consequently, and in all situations, the user's data privacy would be guaranteed.

On the other hand, and considering the wide variety of medical devices and sensors that can that take part in the monitoring processes, the aforementioned authentication framework includes alternative authentication methods, such as the EAP-TLS, formed by an extensible authentication protocol (EAP) with transport level security (TLS). This method is expected to be considerably used in IoT applications as it does not require the use of (U)SIM cards for identity management and authentication processes. This could facilitate the use of low cost devices with different sizes and shapes [26].

Nevertheless, there are some other important aspects regarding 5G networks security, such as the isolation between the access network and the 5GCN. In this context, in the 5G system there is a clear separation between these two parts, in which the access network performs radio management tasks, and the core manages and controls network resources and security[26]. This separation makes it possible to easily identify and isolate network elements in case they are under attack. As a result, the core is the responsible of ensuring the user authentication and the encryption of the data and signalling traffic, with the advanced encryption standard (AES), whereas the access network sends the encrypted traffic between the user's equipment and the core, thus protecting traffic at the radio interface. In addition, the definition of a service-based architecture in the network core allows protection mechanisms to be applied at higher layers, e.g. transport and application [27].

Finally, we must mention the advantages of defining network slices to provide these kinds of services, not only in terms of network resources allocation, but also in terms of security, as possible failures or attacks in one slice will not affect the services being provided in others. To this end, mechanisms and tools must be developed to allow isolation between slices and to prevent unauthorized users from accessing both the assigned network resources and the information they carry.

5.2. Specific measures

However, and despite of the improvements in terms of security and data privacy that 5G networks include, the highly regulated healthcare sector also imposes the need of the definition of an appropriated data model structure. This model, which has been studied in the previous section, responds to the Edge computing paradigm, so that part of the data, before being send to the cloud, is processed, and managed in a secure space. Therefore, part of the management, processing and storage tasks of the data will be carried out on the IoT Edge platform. This platform will be able to manage, independently and autonomously, the users and the devices associated to them [16].

On the other hand, and as the system will rely on the cloud, the communications between the different platforms and cloud services must be performed securely. In this context, a research group of the Polytechnic University of Madrid called the Life Supporting Technologies group, recently proposed the use of distributed identity systems for this kind of purposes, with the scope of integrating different healthcare services [10]. The proposed distributed system will be the one we will use in our system and will be in charge of managing user identities anonymously. In addition, it will also incorporate smart semantic contracts (SSCs) to control data access, its usage and conditions. The SSCs will be able to unlock encrypted data only when the conditions of the contract are met, so it will be possible to transmit encrypted data between different systems without affecting data privacy.

6. Conclusions

In the following decade, and accelerated by the current situation, the health sector of many countries would experience a deep digitalization process. As part of it, 5G networks would play an important role as they would allow the development of new applications and services. Among them, we highlight remote patient monitoring systems that would permit to offer a more personalized and continuous healthcare from long distance.

In this article, we have presented a possible RPM system architecture based on 5G networks. In this context, the new mobile communication generation offers not only a far more superior performance but also a more secure and reliable environment for the management and treatment of the generated data. In order to improve the general system performance, we also make use of other important technological advances in other fields such as IoT or MEC computing. The development of IoT systems, based on 5G networks, with more accurate and enhanced characteristics and the improvement of MEC computing would allow to considerably upgrade the final performance of the system. As a result, a wide flexible variety of medical devices can be offered, as the system is inherently flexible and adaptable.

Finally, the new enhancement in 5G networks security and data management together with additional security and data privacy measures would allow to give the system the required security. This aspect is crucial as 5G networks can help to achieve the severe regulations and security measures that health systems and applications suffer.

References

[1] A. Casquero, J. Perez, "5G networks in eHealth services in Spain: Remote patient monitoring system," In IEEE Engineering International Research Conference, EIRCON 2020, 1–4, 2020, doi:10.1109/EIRCON51178.2020.9254013.

[2] IDATE, "Ehealth Market trends, players & outlook," DigiWorld Interactive Platform, 1–38, 2018.

[3] D. Singh, "5G'S HEALTHCARE IMPACT: 1 BILLION PATIENTS WITH IMPROVED ACCESS IN 2030," STL Partners, 1–39, 2019.

[4] IDATE, "5G IoT in the healthcare sector," DigiWorld Interactive Platform, 56–67, 2019.

[5] Next Generation Mobile Networks Ltd, Perspectives on Vertical Industries and Implications for 5G, NGMN P1 Requirements & Architecture - Verticals Requirements, 1–41, 2016.

[6] Next Generation Mobile Networks Ltd, Recommendations for NGMN KPIs and Requirements for 5G, NGMN P1 WS#3 Key Performance Indicators to 3GPP TSG RAN, (2016), 1–19, 2016.

[7] 3GPP ETSI 3rd Generation Partnership Project, "5G; Service requirements for next generation new services and markets (Release 15)," 3GPP TS 22.261 Version 15.5.0 Release 15, 1–52, 2018.

[8] R. Singh, R. Garhewal, "Smart M-Health Continuous Monitoring System Using 5G Technology," Research Project University of Ottawa, 1–7, 2018, doi:10.13140/RG.2.2.15946.21440.

[9] Ngo Manh Khoi, S. Saguna, K. Mitra, C. Ahlund, "IReHMo: An efficient IoT-based remote health monitoring system for smart regions," 2015 17th International Conference on E-Health Networking, Application and Services, HealthCom 2015, 563–568, 2015, doi:10.1109/HealthCom.2015.7454565.

[10] MYSPHERA, Life SupportingTechnologies Group, Universidad Politécncia de Madrid, "Public consultation for the remote monitoring of chronic patients," Red.Es, 1–35, 2019.

[11] P. Barralon, B. Charrat, I. Chartier, V. Chirié, G. Fico, S. Guillen, N. Homehr, O. Horbowy, R. Kamenova, F. Lamotte, A. Peine, "IoT for Smart Living Environments Recommendations for healthy ageing solutions," WG5 - Smart Living Environment for Ageing Well – Recommendation Paper Alliance for Internet of Things Innovation, (April), 37–67, 2019.

[12] P.K.D. Pramanik, G. Pareek, A. Nayyar, "Security and privacy in remote healthcare: Issues, solutions, and standards," Telemedicine Technologies: Big Data, Deep Learning, Robotics, Mobile and Remote Applications for Global Healthcare, 201–225, 2019, doi:10.1016/B978-0-12-816948-3.00014-3.

[13] A. Ahad, M. Tahir, K.-L.A. Yau, "5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions," IEEE Access, **7**, 100747–100762, 2019, doi:10.1109/ACCESS.2019.2930628.

[14] S. Redana, O. Bulakci, "View on 5G ArchitectureView on 5G Architecture - 5G PPP Architecture Working Group," 5G Public Private Partnership (5G PPP), 1–182, 2020, doi:10.5281/zenodo.3265031.

[15] G. Brown, "Cloud RAN & the Next-Generation Mobile Network Architecture," Heavy Reading White Paper Huawei Technologies Co. Ltd., 1–9, 2017.

[16] Y.C. Hu, M. Patel, D. Sabella, N. Sprecher, V. Young, "ETSI White Paper #11 Mobile Edge Computing - A key technology towards 5G," ETSI White Paper No. 11 Mobile, 1–16, 2015.

[17] A. Zaidi, A. Bränneby, A. Nazari, M. Hogan, C. Kuhlins, "Cellular IoT in the 5G era," Ericsson White Paper, 1–17, 2019.

[18] C. Kuhlins, B. Rathony, A. Zaidi, M. Hogan, "Cellular networks for Massive IoT," Ericsson White Paper, 1–16, 2019.

[19] 3GPP Technical Specification Services Group, "Release 15 Description-TR 21.915," 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects, 1–118, 2019.

[20] 3GPP, "New SID on Support of Reduced Capability NR Devices," 3GPP Work Item Description, 1–4, 2019.

[21] UIT-T, "UIT-T Rec. Y.2060 General description of Internet of things," ITU Telecommunication Standardization Sector, 1–20, 2012.

[22] H. Fangming, "Wi-Fi 6 and 5G and Their Application Scenarios," Huawei Campus Network Marketing Support Module, 1–47, 2019.

[23] R. Hanno, R. George, K. Taylor, "Vital Signs: How to deliver better healthcare across Europe," Deloitte Centre for Health Solutions, 1–56, 2016.

[24] G. Horn, "5G End-to-End Data Management," Qualcomm Technologies, 2020.

[25] Huawei Technologies Co LTD, "5G Security: Forward Thinking," Huawei White Paper, 1–12, 2016.

[26] D. Basin, S. Radomirovic, J. Dreier, R. Sasse, L. Hirschi, V. Stettler, "A formal analysis of 5g authentication," Proceedings of the ACM Conference on Computer and Communications Security, 1383–1396, 2018, doi:10.1145/3243734.3243846.

[27] P. Teppo, K. Norrman, "Security in 5G RAN and core deployments," Ericsson White Paper, 6–13, 2020.