Microservices – A Catalyzer for Better Managing Healthcare Data Empowerment

Marilena IANCULESCU[1,2]*, Adriana ALEXANDRU[1]

[1] National Institute for Research and Development in Informatics, 8-10 Averescu Avenue,
Bucharest, 011455, Romania
marilena.ianculescu@ici.ro (*Corresponding author*), adriana.alexandru@ici.ro

[2] Politehnica University of Bucharest, 313 Splaiul Independenței, Bucharest, 060042, Romania

Abstract: The digital transformation process of the healthcare sector has improved the citizens' access to care and the efficiency and sustainability of the healthcare sector. The sensitive nature of healthcare data requires additional protection against the risks of unauthorized access. Data privacy is an essential concern. This paper presents the patient empowerment and underlines the importance of data empowerment in healthcare domain. In order to address the deployment of a suitable and efficient architecture for a remote healthcare monitoring system, several aspects of the monolithic architecture and Service-Oriented Architecture versus microservices architecture are discussed. A case study related to the RO-SmartAgeing software system used for an improved health data management is presented.

Keywords: Microservices, Remote healthcare monitoring system, Data empowerment, Scalability.

1. Introduction

The global rise in life expectancy and in the number of chronic disease cases has as a result an *increased* number of patients with long term / permanent conditions that burden the health system. Digital transformation of healthcare provides a better retrieval of health information and health services of an enhanced quality. At the same time, this approach saves time and reduces the health spending.

The further development of eHealth is based on:

- Greater and secured access and sharing of citizens' healthcare data;
- Improved quality of data to support medical research, disease prevention and personalized medicine;
- Increased citizens' empowerment and awareness regarding personal health based on patient-centric care approaches facilitated through digital tools. The patients are actively involved in the treatment decisions and health information sharing with a view to preventing diseases rather than seeking preventing diseases rather than seeking treatment;
- Increasing number of available and accessible services that are provided anywhere and at any time and are based on the progress of technology;
- Improved access to health due to the development of mobile-based high-speed medical devices for improving the access to health, knowledge and patient behavior;
- The reduction in the health-related costs based on an easy access to online health services and to a more efficient health service delivery;
- The possibility to customize the contents of telecare for patients at home.

The *patients' empowerment* is related to their capacity to access and understand health information, to participate actively in helping medical staff in the decision making process, to have control over their health status and to communicate with healthcare professionals, providing details about their symptoms and asking information for a better understanding of the disease evolution (Russo, Moretta & Cavacece, 2019).

This paper presents the deployment of a healthcare remote monitoring system that uses healthcare data management with microservices. In order to create a broad perspective to the reader, Section 2 underlines the sensitive nature of healthcare data that are related to the physical or mental health of the patients. This data has to be protected from unauthorized access. The data privacy is one of the major concerns in the health domain. *Data empowerment* grants patients with rights of production and control over their own data and, in conjunction with patient empowerment through digital solutions, acts as a trigger in improving access to healthcare. In Section 3, microservices architecture is compared with monolithic and Service-Oriented Architecture (SOA) and the advantages and disadvantages of this approach

https://doi.org/10.24846/v29i2y202008

are underlined. Some considerations about data management in this context are also discussed. The main contribution of the paper is presented in Section 4, where, in the context of remote health monitoring, Ro-SmartAgeing system is discussed as a possibility of enhancing healthcare data management by using microservices. The Conclusions of this paper are presented in Section 5.

2. Healthcare Data Empowerment

2.1 Healthcare Data and its Sensitive Nature

Healthcare systems are continuously monitoring and collecting healthcare data, that is data related to patients' health conditions and wellness. The gathering of such data by using health information technology has led to a huge amount of healthcare data.

Healthcare data is related to the physical or mental health of persons and includes information related to patients' conditions, treatment details, etc. The GDPR (General Data Protection Regulation) states that "data concerning health" is personal data, also referred to as "sensitive data", and requires additional protection as its processing or unauthorized disclosure could raise significant risks for the persons' fundamental rights and freedoms. (EU, 2016). Therefore, a particular attention is required in order to cope with cybersecurity aspects, and privacy and ethical concerns.

2.2 Authorized Users of Healthcare Data

The primary users of patient healthcare data are (Yuan & Li, 2019):

- *Patient* that provide their current healthcare data and historical information to primary care physician;

- *Primary care or consulting physician* that analyses patient's healthcare data in order to assess the patient's medical problems and needs and to develop an appropriate treatment plan; prescribes diagnostic tests, orders treatment, etc. and analyses their results and the patient evolution; documents patient's medical needs and maintains ongoing record of services provided to patients in order to ensure the continuity of care; collaborates with other physicians for providing proper treatment;

- *Clinical laboratory* that processes and analyzes patient samples and reports the results of analysis to patient's primary care physician; maintains record of results of medical investigations in order to be able to provide it if requested;

- *Local hospital* that provides care to patient as directed by a patient's primary care physician; maintains the ongoing record of services (diagnostic tests, treatment) provided to patient in order to be able to explain the patient's evolution.

The Secondary users of healthcare data employ such information for a variety of societal, business, and government purposes other than providing care. They include:

- *Payer organizations* (insurance companies, or government programs) that analyze the results obtained during the treatment of patient's medical problems and his associated costs.

- *Researchers in medical and social areas, rehabilitation programs, marketing firms, pharmaceutical companies, media, etc.* that use health information for researching the benefits of alternative treatments, understanding health needs, providing news, and finding new markets for health-related products.

2.3 Privacy and Security Requirements for Healthcare Data

Healthcare data security refers directly to *protection against unauthorized access*, and namely to the methods employed in order to protect the privacy, integrity and availability of health information and to help medical personnel in providing reliable information. The security was applied initially to health records in paper form, but, due to the evolution of electronic health records, regulatory guidelines specific to electronic health information became a necessity. Data security is related to the means used for storing the data so that it could be accessed only by authorized people.

Health data protection refers to keeping patient's personal data safe. This is done by using a combination of policies, measures and guidelines related to storing and accessing health information and to the security of health data.

Health data privacy is defined as the *right of the patient* to make decisions about the sharing of his own personal information (Brodnik, Rinehart-Thompson & Reynolds, 2012). Privacy is depending on the information flow, the actors involved, the ways of accessing information and the purpose of the access to information.

Security and privacy aspects related cu e-Health domain are discussed in (Abouelmehdi, Beni-Hessane, & Khaloufi, 2018) and (Essén et al., 2018).

The differentiation between security and privacy of healthcare data is presented in Table 1.

In accordance with General Data Protection Regulation (GDPR) in Europe and Health Insurance Portability and Accountability Act (HIPAA) in USA guidelines, a set of useful security and privacy requirements for e-Health domain has been proposed (Table 2).

2.4 Emerging Empowerment of Healthcare Data

The access to healthcare has become one of the citizens' major concerns. This fact is leading healthcare organizations to the necessity of finding new ways to adapt to population's needs and to work with patients for building sustainable value. The patient must be empowered by digital solutions and acts as an active participant in the management of the status of his health, while the providers have to respond in a timely and actionable manner to his / her needs.

Data empowerment is the process through which people are granted the right of control and promotion of their own data for their wellbeing and the society wellbeing (Cañares, 2019).

People have the right to create and are involved in the production of their data. They need to know how this data is used: where data goes, who is using it and how. In order to ensure data accessibility, digital solutions are used for health data interpretation and for enhancing connection

Table 1. Differences between security and privacy of healthcare data

Security	**Privacy**
Is defined as the privacy, integrity and availability of health information	Is defined as the proper use of patient's health information, decided by himself
The medical organization has to prevent health data compromise due to technology or network vulnerabilities by using different techniques such as encryption, firewall, etc.	The medical organization can't sell the patient healthcare data without his / her prior consent
Is concerned with protecting a medical organization or ensuring confidentiality	Is concerned with protecting patient information and rights
Security provides the ability to be confident that decisions are respected	Privacy is the ability to decide what information about an individual can be accessed and where it goes

Table 2. Security and privacy requirements as recommended by GDPR & HIPAA

Requirement	***Description***
Patients' understanding	Patients have a complete right to understand how their sensitive and private health information are stored and utilized by any healthcare stakeholder.
Patients' control	Patients have the permission to decide who can access his / her healthcare data.
Confidentiality	Health information should be hidden from people who have no permission to access it.
Data integrity	Manipulation and amendment or modification of original health information is totally prohibited.
Consent exception	This stipulates that patient's information could be accessed without his / her consent only in emergency cases.
Non-repudiation	The healthcare practitioner should deny the fact that he / she has performed a certain activity on the sensitive data of patient. Such activity should be supported with evidence to avoid dispute or suspicion.

with healthcare providers. Patient-centered healthcare is the future of healthcare domain and implies the use of explicit digital solutions to be used to create patients' awareness. People also have the right to privacy and the right to be protected from online risks. In healthcare sector, cybersecurity has to provide the protection of information as well as to enhance trust in the framework of doctor-patient relationship.

In the context of prioritizing digital tools that incorporate cybersecurity to protect the information patients share and uphold, the sacred trust they have in the doctor-patient relationship will also be important. Using a blockchain-based system to secure and track patient data may be a good option for establishing an additional layer of trust and allowing the provision of discounted services to be provided to patients who participate as partners (Mathew, 2019).

Data empowerment provides to people three main dimensions (Cañares, 2019):

1. *Ability to access data* – need to access relevant government data by prioritizing the degree of relevance based on people's needs;
2. *Capacity to produce and use relevant data* – involvement of citizens in the use and, in some cases, even in the early collection of data;
3. *Power to control personal data* – understanding and determining the way of using their data and the benefits obtained from it.

The empowerment of patients through digital solutions has as a result the redesigning of the provision and access to healthcare (Synergus, 2019). The key elements that influence this shift of dynamics are:

- *Empowering change* – interest in behavioral change directed to disease prevention in case of persons at risk; adherence to digital solutions used both for diagnostic solutions and lifestyle modification;
- *Smart healthcare interaction* – patients' engagement in submitting health-related results leading to cost reduction and improved collection of evidence;
- *Access to data* – obtaining a huge amount of valuable data from wearables and provision of ready access to diagnostic laboratory results for opening the way to the adoption of a preventive lifestyle; use of new integrated digital healthcare solutions for data delivery in concise usable formats for physicians and in easily understandable updated formats for patients.

3. Microservices

3.1 Monolithic and SOA vs Microservices

Building an application based on ***monolithic architecture*** implies encompassing all the components in a single indivisible unit and logical executable (Saransig & Tapia, 2019). It is the traditional approach in developing software applications in which a unique technology is used and the focus is on the aggregated application seen as a whole.

The *advantages of monolithic architecture* are:

- The initial development and error tracing of the application are easy and fast;
- All the capabilities are managed in a single place;
- A small number of transformations can be done in the same context, therefore it is cost-efficient;
- Only one code base is used, so the current development team doesn't need any additional programming skills;
- Communication among components is uncomplicated and much easier to control;
- It's quite easy to deploy;
- It is appropriate for small teams with minimum cross-cutting concerns.

The *disadvantages of monolithic architecture* are:

- Any changes, fault isolation or debugging cause the functional interruption of the entire application, as the components are tightly coupled;
- It is more difficult to maintain;
- As the code base grows, the development of the application becomes slower and more difficult to manage;
- A single server is used. In order to scale the application, it is compulsory to use several updated instances / server-side of it;

- Developers depend on each other as the components themselves depend on each other, therefore entering the market takes longer;

- As digital technologies are evolving continuously and quite fast, it is very complicated to shift the existing monolithic-based application towards a new version or emerging technology, as the whole application has to be written again.

Service-Oriented Architecture (SOA) consists in a collection of services communicating with each other while performing associated functions. The components of the application are grouped around loosely-coupled services. The communication through the public interfaces implies data exchange or an activity managed by several services. SOA is based on distinct multiple layers. The services can vary from small (for a simple application) to large (for an enterprise-targeted application).

The *advantages of SOA* are:

- The components can be developed in different code bases and platforms;

- The services can be developed and upgraded easily and independently, without affecting the whole application;

- Pre-built services can be used many times for multiple components and in heterogeneous environments like Java or C++;

- As the services are smaller compared with the whole application, they can be more easily tested. Furthermore, testing can be divided according to some specific areas like security or it can be performed independently for a certain service;

- The independent nature of the services makes them appropriate to be used by other systems at the same time;

- It provides a remarkable degree of flexibility as this extensible architecture can be configured according to the users' specific needs;

- The implementation of the services can be made on a single server or on multiple servers, which provides location transparency;

- Maintaining the technology and custom development are cost-efficient.

The *disadvantages of SOA* are:

- As it requires more skills on the part of the development team, more technologies and a more complex management, SOA is more expensive than monolith architecture;

- The performance of the application may decrease due to the response time that is imposed through the validation of the inputs before any interaction among provided services;

- Enterprise Service Bus, the middleware tool used in SOA, has a core role in the service orchestration that reflects in slow communication speed, reduced performance or it may become a single point of failure;

- The coarse-grained feature is still present together with a high level of dependency among services which may drive, like in the case of monolithic architecture, to large-scale re-developments;

- It is more expensive as it requires bigger investments in larger teams and different technologies.

Microservices, also called microservices-based architecture, represent a relatively new approach for a service-oriented architecture in which a single application is developed as a group of diverse small independent components (i.e. services) with a unique business-capability. Every service is loosely-coupled, it can have a distinct database, a well-defined interface, it can be written in different languages and deployed independently (Dragoni et al., 2017). These aspects lead to a decentralized control and management of the services.

Services are built so as to include every necessary resource in order to deliver a distinct function or task. They are fine-grained, function-oriented, independent, with their own databases and adapted so as to communicate through language-agnostic APIs. The services can be developed, tested and upgraded by small distinct teams that can decide independently on every aspect related to their design and functionality in a bounded context.

As it was mentioned above, though monolithic architecture is the traditional approach that is still appropriate for some business models, it also has several weaknesses, like tightly-coupled components or shared data, which bring about serious impediments in terms of scaling up, better control over development, restricted reuse or operational agility. The requirements of the business environment have evolved thereby imposing an increased need for faster development, innovation, flexibility, and scalability while decreasing complexity and costs of monolithic architecture-based applications.

SOA was the response to many of these issues by setting apart the components of the application into services of different sizes oriented towards the desired functionality. Among the services it uses messaging protocols like Simple Object Access Protocol / XML-based services over HTTP or Java Message Service to ensure the communication. Nevertheless, there are still some features that make SOA act like a monolith when the business expands and the new requirements lead to a rather complex architecture with a number of interdependencies that are not insignificant.

Microservices have been evolved from SOA in order to solve its weaknesses. Thus, significant improvements have been obtained:

- While SOA aims to share as much as possible, microservices aim to obtain independence to the greatest extent possible in a bounded context;
- A faster and more sustained deployment;
- The choice to share a database or not;
- As all the services are independent, a common server for applications is useless;
- An increased degree of scalability due to the use of containers;
- A higher communication overhead;
- No common standards are taken into consideration;
- The speed of development and deployment is increased, together with the agility and quick-time-to-market;
- A shortcoming of a service is highly unlikely to set off a failure elsewhere in the application;
- Because services are smaller than those used in SOA, they can be caught up by a different team which no longer need to be aware of the rest of services and application.

3.2 Reasons for Using Microservices

Microservices have emerged with a range of attractive characteristics that has made it possible to use them on large scale. The most representative ones are:

- *Agility and speed of deployment*: different stages of the services can be developed and inter-connected simultaneously by different teams in a shorter time to market;
- *Flexibility*: different programming languages and technologies can be used at the same time;
- *Scalability*: a service can be upgraded, used for another task or in another context and application;
- *Decentralized data management*: it allows services to be loosely-coupled and the most appropriate type of database to be chosen, which leads to increased business performance and task speed;
- *Fault isolation and detection*: a failure of a service can be detected faster. The service can be replaced by another one or stopped without affecting the rest of the application;
- *Autonomous, cross-functional teams:* small teams with various skills can independently develop and re-use specific business capabilities associated with the respective services;
- *Increased quality of data:* as each service can have its own database and the data management is decentralized, it is easier to better control the data and its flow (Nadareishvili et al., 2016), (Filip et al., 2018).

3.3 Drawbacks of Microservices

Despite the benefits of microservices, certain limitations and drawbacks cannot be neglected. Among the most challenging ones are the following:

- *Increased complexity:* the higher the number of services, the higher the complexity of required management and monitoring that is required;

- *Higher costs*: ensuring both an increased level of communication due to remote calls among services and expenditures associated with the organizational change are higher than in case of traditional architectural approach;

- *Augmented security issues*: as the volume of data exchange increases because of the communication among services, possible security breaches are also augmented (Ianculescu et al., 2019).

3.4 Data Management Considerations in the Context of Microservices

Each service manages its own database directly, which implies a strict control of it, also in terms of privacy and security. Other services can access this data through a query using its API; while more services are added to the application, the communication becomes more complex, so the challenge is to aggregate data from several databases associated to distinct services through an API Gateway pattern. As a service is loosely-coupled, independently built and re-used, the allowed changes in data schema might affect the other services that use / rely on that specific database, with direct consequences on their deployment and scalability.

Data consistency is a sensible issue due to multiple services with different data storage patterns, such as Database-per-Service (in which every service has its own database) or Database-is-the-Service (where the database is embedded into the business logic implementing the targeted service) patterns (Messina et al., 2016).

4. Managing Healthcare Data with Microservices within Remote Healthcare Monitoring Systems

4.1 Remote Healthcare Monitoring Systems (RHMS)

Globally, the growing number of patients with chronic diseases, with mobility issues as well as of elderly patients poses a significant challenge due to the limited capacity of health services to provide sufficient healthcare (Malasinghe, Ramzan, & Dahal, 2019). At the same time, chronic conditions increase the demand for intense medical management. Proactive self-management and early recognition of changes in one's health condition might reduce hospital admissions and treatment costs, while also enhancing health-related quality of life.

RHMS involve a tele-monitoring device in the patients' home that can collect real-time patient's vital signs and data together with environmental parameters and transmit them electronically to a clinical site for interpretation and diagnosis (Walker et al., 2019). RHMS can support home or community-based care and remote settings, thereby enabling the patients to improve their ability to self-manage their health status and the quality of their lives.

The basic elements of RHMS are (Malasinghe, Ramzan, & Dahal, 2017):

- *Data acquisition system*: consists in different sensors / wearable small and non-invasive sensors for collecting patient's vital parameters or ambiental parameters. These sensors work wirelessly. Sensors incorporated in mobile devices (smartphones) can be also considered. (McDuff et al. 2015);

- *Data processing system*: aims at the processing of received / transmitted data;

- *End-terminal at the hospital*: a computer / database / smartphone of the doctor;

- *The communication network*: connects the data acquisition system to data processing system and transmits data / alarms to a healthcare professional connected to RHMS, who decides on the necessary actions to be taken: pill administration, caution steps, admission in the hospital.

Mobile technology devices such as smartphones and tablets combined with telehealth video conferencing and healthcare wearables are used in the deployment of RHMS. Despite the potential benefits, patients show resistance to adopting RHMS due to their distrust in new technologies.

4.2 Advantages of Microservices for RHMS

Beside the previously emphasized opportunities brought about by microservices, there are some specific advantages that make them suitable for RHMS:

- As the smaller teams work independently, they have the capacity to faster support better decision-making with the view to scaling up the application in the very complex and heterogenous domain of RHMS;

- Since the Internet of Things (IoT), broadly used for remote monitoring, comes in a great diversity of devices and technologies for collecting an even greater variety of healthcare data, the use of microservices enables an enhanced capacity to adapt the single business capability of a service to versatile contexts and environments (Rogojanu et al., 2018);

- Because the remote monitoring implies a stringent requirement for constant and secure gathering and processing of accurate healthcare data, the loosely-coupled and fault tolerance features of microservices are very useful for isolating and replacing a malfunctioning service without affecting the overall application.

Here are some constraints of two RHMS applications based on other types of architectures that can be mitigated with microservices:

- The *SafeNeighborhood model* (SN) (Bicharra et al., 2017) aggregates data from a variety of sources with mobile, Ambient Assisted Living and Artificial Intelligence technologies to monitor the elderly outdoor. SN is based on a client-server architecture and a cloud-based server. Each of the three-layers of the architecture (data acquisition, communication and application) can be assimilated with a monolithic architecture which is inappropriate for frequent changes usually leading to the deployment of the whole SN, with tight coupling, unchangeable common technology.

- The *Framework for sensor- based monitoring patients for a pervasive care* (Triantafyllidis et al., 2016) is based on SOA in order to be scalable and flexible, but it demands interoperability for the heterogeneous modules to be integrated.

4.3 Improved Healthcare Data Management. Case Study- RO-SmartAgeing System

Bringing the microservices power for healthcare data management

Emerging comprehensive computer capabilities and smart wearable technology facilitate the gathering, processing and storage of increasing amounts of sensitive healthcare data. Microservices come with the power to provide *flexibility* in carrying out the management of the healthcare data (because the database associated to a service does not have a direct connection with the data associated to another service), *agility* and *polyglot persistence* (i.e. different data storage technologies and data models are used according to the context) and *increased security and privacy* (healthcare data can be multiplied based on an event-driven model for all the services asking for it).

RO-SmartAgeing

”*Non-invasive monitoring and health assessment of the elderly in a smart environment (*RO-SmartAgeing)” is a research project that is currently in the third phase, i.e. the general architecture design. One of the main objectives of the project is the development of a RHMS that has an elderly-centered approach which is able to provide customized support for healthcare services in a personalized smart environment.

As elderly are usually persons with multiple chronic conditions and age-related frailties, the support for the personalized assistance delivered by RO-SmartAgeing system takes into account *prevention* as a key role for better healthcare outcomes (Alexandru & Ianculescu, 2017), *better engagement of the elderly person in the management of his / her health statu*s as an aware and responsible partner with his / her healthcare providers, *improved quality of life* through the monitoring of his / her lifestyle and daily activities (Balog et al. 2019), and *enhanced support for diagnosis, therapeutic protocols and healthcare decision-making*. By building an adaptable controlled framework for embedding important prerequisites necessary for the healthy, qualitative, independent and active life of a particular elderly, RO-SmartAgeing system sustains a safe, long-term monitoring while avoiding unnecessary readmissions or institutionalizations in hospitals or residential homes.

RO-SmartAgeing system integrates IoT technologies (physiological, motion and environmental (smart) sensors), data analytics and cloud computing technologies, in order to provide supportive healthcare services.

Healthcare data, the keystone of RO-SmartAgeing

RO-SmartAgeing system is designed to provide a reliable alternative for the complete management of the healthcare data flow that is generated in a non-clinical environment. The architecture of RO-SmartAgeing is structured according to the particular characteristics of healthcare data that is heterogeneous, (un)structured, complex, often in big amounts, generated from different sources in various locations.

The system described above takes into consideration that healthcare data of the monitored elderly is collected as raw data from a wide range of different (smart) devices, it is cleaned, aggregated, analyzed, processed and used in targeted applications, while specific system functionalities ensure its accuracy, security, privacy, confidentiality, accessibility, and interoperability.

The management of the elderly`s healthcare data is strictly controlled through the mechanisms of the n-layer architecture and microservices in order to get insights into the respective data and store data that is complete, reliable, recognizable by healthcare providers, relevant, actual, and empowered for supporting medical decision-making.

The ***data flow*** within RO-SmartAgeing system (Figure 1) highlights how the healthcare data empowerment is reflected in the main functionalities of the system.

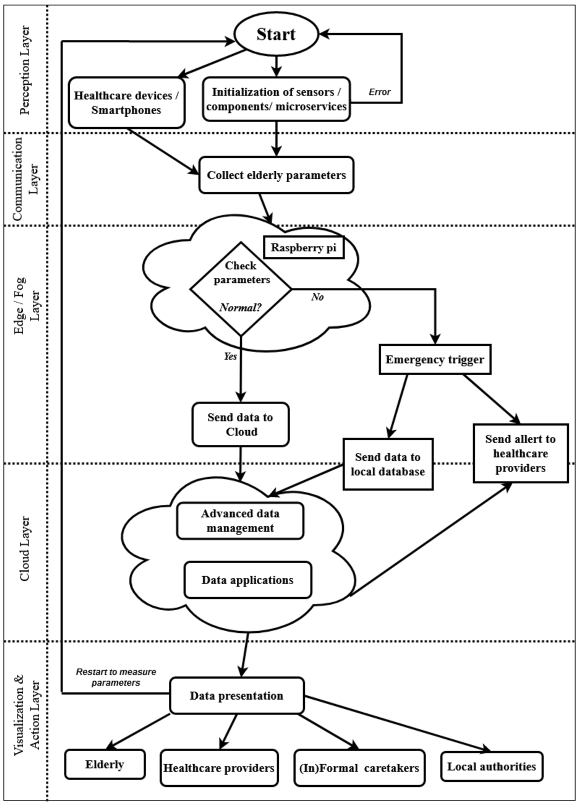

Figure 1. RO-SmartAgeing healthcare data flow diagram

Data is collected continuously at flexible time periods; then it is pre-processed at the Edge / Fog layer according to a personalized set of rules, in order to faster identify (closer to the sources of data) an abnormal value of a monitored parameter. If that happens, an emergency trigger is activated and an alert is sent instantly to the current healthcare provider, which can initialize a medical action in real time and before a worse deterioration of the elderly's health occurs.

The data, sent afterwards to the Cloud, is processed and analyzed so that the health-related information can be transformed into insights and applications that will allow the healthcare providers to respond in a pro-active and preventative manner to the particular needs of the elderly. Furthermore, the whole healthcare data flow highlights the potential of healthcare data-driven decisions to comprise the elderly as active and empowered stakeholders in the monitoring and management of their health.

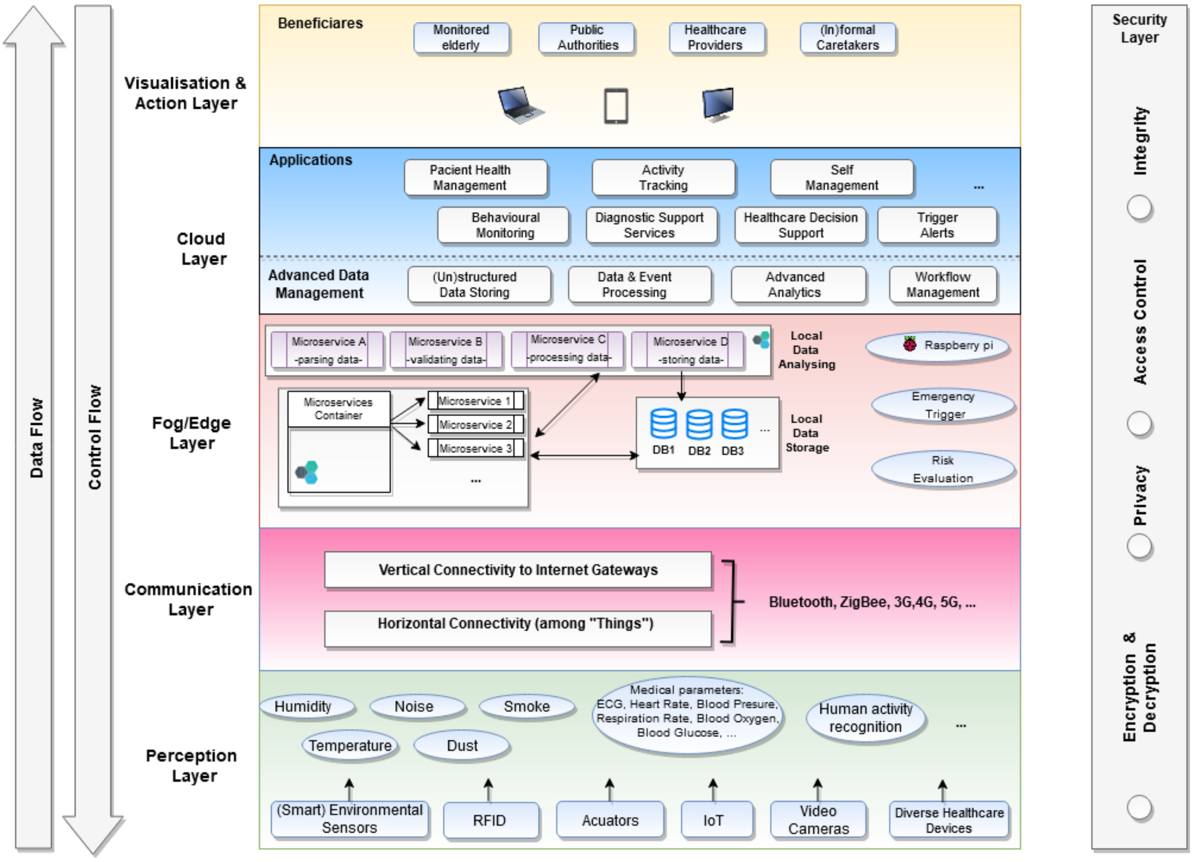

Figure 2. RO-SmartAgeing general architecture

RO-SmartAgeing general architecture

The architecture chosen for RO-SmartAgeing system (Figure 2) combines the n-layered IoT architecture with microservices in order to benefit from both types of architectures:

Perception Layer: The raw data is collected from a large diversity of IoT, smart wearables, or other devices that are disposed in a personalized configuration, aiming to obtain the most suitable health and ambiental parameters, chosen according to the current needs and requirements of a specific elderly.

Communication Layer: It enables the vertical communication among the other layers and the horizontal one among the "Things" by using gateways and the network.

Edge / Fog Layer: A number of microservices associated with the data sources (devices) are located here for a fast management. Each service has a unique functionality such as parsing, validating, processing and local storing. As a result of the preliminary local analytics and risk evaluation, a time-sensitive decision-support function is provided if an abnormal value of a parameter is detected.

Cloud Layer: The data generated by the previous layers is analyzed in-depth and processed and it is stored in databases that allow Create, Read, Update and Delete (CRUD) procedures. Data can also be filtered so as to provide only the most appropriate information that is needed in applications with a well-defined target like "Patient Health Management" or "Diagnostic Support Services". The Cloud Layer is accessed periodically in a controllable way with a view to a prompt exploitation of the resources.

Visualization & Action Layer: The end beneficiaries, starting with the elderly, are given a personalized access to the applications developed inside RO-SmartAgeing.

Security Layer: Taking into consideration the sensitive feature of healthcare data, it is compulsory to enforce security actions along and across all layers such as authentication, secure gathering and transmission, encryption & decryption, customized security measures that take into consideration the particularities of IoT and smart wearable devices, message integrity check, etc.

4.4 Discussion

Microservices improve the current and future development of RO-SmartAgeing system in terms of scalability and flexibility (as they can be reused across different healthcare domains) or reliability (the fault tolerance feature allows the system to keep on performing the other functionalities if one service stops working). These are essential characteristics of a RHMS, because the trigger alerts or the continuous monitoring of an elderly are crucial. Moreover, the system can be reconfigured according not only to the specific health conditions of an older person, but also to the evolution of age-related conditions.

Scheduling, storing, and managing the data acquired from the IoT, wearables and devices at the Edge / Fog level are the main capabilities of this layer and thus an additional computational burden for the Cloud Layer is eliminated.

The most efficient place for the functionalities of RO-SmartAgeing that are related to in-depth analytics is considered to be the Cloud Layer, since they need comprehensive computation and storage capabilities. Moreover, data storing at this level provides continuous data accessibility and agility.

The 6-layer architecture of RO-SmartAgeing system allows different adjustable technologies to be assimilated for developing both the smart environment and the microservices providing single functionalities. The considerable agility of this system is ensured by fault isolation, the fine-grained access control for enhanced healthcare data security, and the loosely-coupled units.

5. Conclusion

Patient and healthcare data empowerment have made their presence felt more and more strongly in a worldwide ageing society. Personalized RHMS are a reliable solution for improved medical services, and their fast extensibility, maintainability and flexibility can be supported by a microservices-based architecture.

By presenting the underdevelopment of the RO-SmartAgeing system, this paper aimed to highlight the benefits of the microservices for a RHMS that has to be scalable, with a high degree of personalized complexity, and agile for coping with the devices and technologies that are continuously evolving. Also, the potential of the microservices-based architecture to be customized for other types of monitoring like the one needed in the context of COVID-19 pandemic will be further taken into consideration.

Acknowledgements

The authors gratefully acknowledge the contribution of the Romanian Ministry of Research and Innovation with regard to the funding of the projects “*RO-SmartAgeing - Non-Invasive Monitoring System and Health Assessment of the Elderly in a Smart Environment*” for the period 2019-2022 and “*vINCI: Clinically-validated INtegrated Support for Assistive Care and Lifestyle Improvement: the Human Link*” for the period 2018-2021.

REFERENCES

Abouelmehdi, K., Beni-Hessane, A. & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy, *Journal of Big Data*, *5*(1), p.1. DOI: 10.1186/s40537-017-0110-7

Alexandru, A. & Ianculescu, M. (2017). Enabling Assistive Technologies to Shape the Future of the Intensive Senior-Centred Care: A Case Study Approach, *Studies in Informatics and Control*, *26*(3), 343-352. DOI: 10.24846/v26i3y201710

Balog, A., Băjenaru, L. & Cristescu, I. (2019). Analyzing the Factors Affecting the Quality of IoT-based Smart Wearable Devices Using the DANP Method, *Studies in Informatics and Control*, *28*(4), 431-442. DOI: 10.24846/v28i4y201907

Bicharra, G. A. C., Vivacqua, A. S., Sanchez-Pi, N., Marti, L. & Molina, J. M. (2017). Crowd-Based Ambient Assisted Living to Monitor the Elderly's Health Outdoors, *IEEE Software*, *34*(6), 53-57.

Brodnik, M., Rinehart-Thompson, L. & Reynolds, R. (2012). *Fundamentals of Law for Health Informatics and Information Management Professionals*, *Chapter 1*. AHIMA Press, Chicago.

Cañares, M. (2019). What do we mean by data empowerment?, *Data Empowerment.* Available at: <https://medium.com/data-empowerment/what-do-we-mean-by-data-empowerment-f842ef9880b#:~:text=By%20data%20empowerment%2C%20we%20

mean,their%20and%20their%20society's%20wellbeing>.

Dragoni, N., Giallorenzo, S., Lafuente, A. L., Mazzara, M., Montesi, F. Mustafin, R. & Safina, L. (2017). Microservices: Yesterday, Today, and Tomorrow. In: Mazzara M. & Meyer B. (eds.), *Present and Ulterior Software Engineering*, 195-216. Springer, Cham. DOI: 10.1007/978-3-319-67425-4_12

Essén, A., Scandurra, I., Gerrits, R., Humphrey, G., Johansen, M. A., Kierkegaard, P., Koskinen, J., Liaw, S. T., Odeh, S., Ross, P. & Ancker, J. S. (2018). Corrigeum to "Patient Access to Electronic Health Records: Differences Across Ten Countries", *Health Policy and Technology*, *7*(1), 44-56.

EU. (2016). *General Data Protection Regulation* 2016/679 (GDPR).

Filip, I. D., Pop, F., Serbanescu, C. & Choi, C. (2018). Microservices Scheduling Model Over Heterogeneous Cloud-Edge Environments as Support for IoT Applications, *IEEE Internet of Things Journal*, *5*(4), 2672-2681. DOI: 10.1007/978-3-319-43949-5_18

Ianculescu, M., Alexandru, A., Neagu, G. & Pop, F. (2019). Microservice-Based Approach to Enforce an IoHT Oriented Architecture. In *Proceedings of the 7th edition of the IEEE International Conference on E-Health and Bioengineering (EHB 2019)*, Iasi, Romania (pp. 1-4). DOI: 10.1109/EHB47216.2019.8970059

Malasinghe, L. P., Ramzan, N. & Dahal, K. (2019). Remote patient monitoring: a comprehensive study, *Journal of Ambient Intelligence and Humanized Computing*, *10*(1), 57-76.

Mathew, G. (2019). *Patient Data: Empowering Consumers to Transform Health Care*, Forbes.

McDuff, D. J., Estepp, J. R., Piasecki, A. M. & Blackford, E. B. (2015). A survey of remote optical photoplethysmographic imaging methods. In *2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* (pp. 6398-6404).

Messina, A., Rizzo, R., Storniolo, P., Tripiciano, M. & Urso, A. (2016). The Database-is-the-Service Pattern for Microservice Architectures. In *7th International Conference in Information Technology in Bio- and Medical Informatics (ITBAM)*, (pp 223-233). Part of the *Lecture Notes in Computer Science* book series *(LNCS, volume 9832*), Springer, Cham.

Nadareishvili, I., Mitra, R., McLarty, M. & Amundsen, M. (2016). *Microservice Architecture - Aligning Principles, Practices, and Culture*. O'Reilly Media, Inc.

Rogojanu, T., Ghita, M., Stanciu, V., Ciobanu, R., Marin, R., Pop, F. & Dobre, C. (2018). NETIoT: A Versatile IoT Platform Integrating Sensors and Applications. In *2018 Global Internet of Things Summit (GIoTS)*, Bilbao (pp. 1-6).

Russo, G., Moretta Tartaglione, A. & Cavacece, Y. (2019). Empowering Patients to Co-Create a Sustainable Healthcare Value, *Sustainability*, *11*(5), p.1315. DOI: 10.3390/su11051315

Saransig, A. & Tapia, F. (2019). Performance Analysis of Monolithic and Micro Service Architectures – Containers Technology. In: Mejia J., Muñoz M., Rocha Á., Peña A. & Pérez-Cisneros M. (eds.), *Trends and Applications in Software Engineering (CIMPS 2018),* 270-279. Part of series*: Advances in Intelligent Systems and Computing*, *vol 865*, Springer, Cham.

Synergus, R W. E. (2019). *The Empowered Patient – Revamping healthcare through digital solutions.* Available at: <https://synergusrwe.com/blog/empowered-patient-revamping-healthcare-through-digital-solutions>.

Triantafyllidis, A. K., Koutkias, V., Chouvarda, I., Adami, I., Kouroubali, A. & Maglaveras, N. (2016). Framework of sensor-based monitoring for pervasive patient care, *Healthcare Technology Letters*, *3*(3), 153-158.

Walker, R.C., Tong, A., Howard, K. & Palmer, S. C. (2019). Patient expectations and experiences of remote monitoring for chronic diseases: Systematic review and thematic synthesis of qualitative studies, *International Journal of Medical Informatics*, *124*, 78-85.

Yuan, B. & Li, J. (2019). The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation, *International Journal of Environmental Research and Public Health*, *16*(6), p.1070. DOI: 10.3390/ijerph1606107