Data Collection via Wearable Medical Devices for Mobile Health

Vincenza Carchiolo[1][a], Alessandro Longheu[1][b], Simone Tinella[1], Salvo Ferrara[2]
and Nicolò Savalli[2]
[1]*University of Catania, Italy*
[2]*Wisnam S.R.L., Acireale (CT), Italy*

Keywords: Mobile Health, IoT, Werable Medical Device, Big Data.

Abstract: The prevention and early detection of illness symptoms is becoming more and more essentials in a world where the improvements in healthcare extends life expectancy. New technologies led to new paradigma as e-health, m-health, smart-health and pervasive health. Wearable networked devices for real-time and self-health monitoring represent an effective approach that fulfil prevention goal at the same time keeping costs under control. In this work, we present a Wearable Health Monitoring Systems (WHMS) capable of collecting, digitizing, connecting to a wearable medical device via Bluetooth, and measuring various physiological parameters of patients in particular suffering from heart disease. System's architecture, requirements, adopted technologies and implementation issues are presented and discussed, showing its effectiveness in healthcare support.

1 INTRODUCTION

Advances in medical researches and the related improvement of both life quality and expectancy (GHO, 2019) is shifting the main reason for humans death from infectious diseases to chronic illnesses; in such a scenario, the prevention and early detection of illness symptoms plays a key role to preserve people's life.

The strengthening of medical care, either at home or in the hospital, required the adoption of new technologies and led to new paradigma as e-health (Eysenbach, 2001), m-health (Istepanian et al., 2006), smart-health (Solanas et al., 2014) and pervasive-health (Postolache et al., 2013). Among the set of new frameworks and innovative architectures as IoT and Smart cities, wearable devices (Haghi et al., 2017) also significantly endorse the self-health monitoring approach, that allows to detect and prevent illness also reducing overall costs in healthcare management.

The concept of wearable equipment devoted to wellness and healthcare actually goes back to the XIII century, when corrective lenses were firstly used and evolved across decades through ears trumpets and contact lenses, arriving to the XX century with electric/electronic devices as pacemakers, insulin pumps and hearing digital aids. Recent trends for this market are highly promising (TMR, 2019), although significant drawbacks still deserve a major attention, as regulatory hurdles that somehow prevents an intensive adoption of such devices by healthcare professionals and final users, and security issues that hold a critical position due to the nature of personal information.

A further question to consider is the data management, from gathering to the storage and processing steps, being health data sometimes collected in a real-time fashion and/or requiring additional information as the (possibly full) patient's medical history extracted from central databases of healthcare providers (Ferebee et al., 2016). Problems related to data management also includes irregularity, high-dimensionality and sparsity (Ismail et al., 2019), that naturally leads to the world of Big data algorithms and analytics (Chen et al., 2014).

The work presented in this paper falls into this scenario, in particular here we present a case study concerning an architecture where health data are collected and stored, and can be later retrieved and visualized through a Web application. We focus on collection and manipulation of data gathered via wearable technology in cardiology. The use of wearable devices in cardiology is well established but recently wearable devices allowing passive hearth rate moni-

[a] https://orcid.org/0000-0002-1671-840X
[b] https://orcid.org/0000-0002-9898-8808

Carchiolo, V., Longheu, A., Tinella, S., Ferrara, S. and Savalli, N.
Data Collection via Wearable Medical Devices for Mobile Health.
DOI: 10.5220/0009100705860592
In *Proceedings of the 13th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2020) - Volume 5: HEALTHINF*, pages 586-592
ISBN: 978-989-758-398-8; ISSN: 2184-4305

toring become largely available. On the other side, wide range for applications in the active monitoring sector and in the emergency management is a current area of concern. The new frontiers of application of wearable devices in cardiology also highlight open problems in the field of data security and their validation. Another aspect of great interest lies in the requirements for real-time data collection management and how they can be effectively used to train future intelligent systems; the case study presented in this paper concerns issues related to real time and data security.

The paper is organized as follows: in section 2 a brief overview of related works concerning health systems is discussed, while in section 3 the case study is presented and in section 4 some specific use cases are illustrated. Finally, section 5 shows our concluding remarks and future works.

2 MOBILE HEALTH AND WEARABLE DEVICES

First E-health systems were developed in the early 2000s with personal medical data recording also known as Electronic Health Record or EHR (Baird et al., 2011), thus providing easy access to patients information. More recently, the exploitation of mobile devices endorsed the diffusion of M-Health paradigma (Istepanian et al., 2006), where medical data, related treatments and two-way communication with physicians is granted via apps avoiding physical meetings at the hospital whenever possible.

IoT universe (Miraz et al., 2015) improved M-Health with new services thanks to the massive use of medical sensors, seamlessly integrated into mobile/wearable devices as smartphones and fitness bands, therefore making it possible even real-time vital signs detection. One step further was achieved with Smart Cities integration, determining the so-called Smart-Health or S-Health (Solanas et al., 2014); the harnessing of city related information results in the healthcare improvement, for instance pollution data can be used to suggest allergic individuals to avoid specific areas to prevent allergy attacks, or an emergency can be better managed by optimizing ambulance path exploting both patient’s position and traffic information.

In general, smart-health allows to seize several opportunities as:

- Chronic illness prevention and management, indeed thanks to data gathering a situation requiring immediate intervention can be detected and proper action will be carried out timely
- Data analysis can allow to discover incorrect or inefficient medical cases management, so these can be dealt with better in the future. Data can also be matched with state, position and current patient activities to tailor actions and treatment to personal needs, for instance identifying and excluding false positives for specific scenarios.
- Emergency detection and control by leveraging citizen vital signs and activities, and major risk areas; such information can be used to effectively and safely address situation as for instance outbreaks, unexpected pollution increase, chemical/nuclear accidents etc.
- Healthcare cost reduction, thanks to the increase in overall efficiency and effectiveness, avoiding unnecessary hospitalization, therapies and/or treatments; this reduction is expected to increase more and more also thanks to a better monitoring of elder people

All these fascinating advances collide with privacy issues coming from the massive personal health data gathering. Some projects have been developed to define boundaries for health related data exploitation and protect from data breaching, as the Trustworthy Health and Wellness (THaW) (THaW, 2019), an NSF-founded project aiming to provide trustworthy information systems for health and wellness, or the Strategic Healthcare IT Advanced Research Project on Security (SHARPS) (SHARPS, 2019) whose goal is to develop ”technologies and policy insights concerning the requirements, foundations, design, development, and deployment of security and privacy tools and methods as they apply to health information technology.”

Systems for monitoring healthcare data can be classified as follows:

- Remote Health Monitoring Systems or RHMS, that include those systems capable to send and/or receive remotely their data
- Mobile Health Monitoring Systems (MHMS), an RHMS enhancement that leverages smartphones or other mobile devices for local data processing whenever needed
- Wearable Health Monitoring Systems (WHMS), where mobility is further enriched with wearable devices/sensors
- Smart Health Monitoring Systems (SHMS), where ’smart’ characterizes the approach and related devices

According to this classification, in (Ren et al., 2010) an MHMS is proposed, specifically focused on energy management, whereas in (Shih et al., 2010) authors introduce a system for ECG monitoring via RF id (WHMS) based on a client-server architecture that collect and store patient's data, sent to the server via mobile network on a regular basis. Some MHMS solutions can exploit local processing capabilities of mobile devices to analyze gathered data and establish whether critical conditions arise; in such cases, immediate alert is generated and transmitted to medical staff, whereas a not-real-time data upload is usually adopted to mitigate power consuption. The work (S. et al., 2017) provide a comparison of several health and activity monitoring systems, including textile-based sensors intended for wearable systems, whereas in (Hong et al., 2010) daily activities are detected using wireless accelerometers, permitting the detection of falls, incorrect postures and sleeping disorders. Authors proposed accellerometers as wearable devices communicating with mobile devices via low power protocols as Bluetooth or ZigBee; the mobile device collects and eventually processes and sends data to physicians. An advanced proposal is described in (Pandian et al., 2008), where authors present a washable shirt embedding a set of sensors working as an array for continuously monitoring physiological signals.

3 WHMS FOR HEART DISEASE PATIENTS: A CASE STUDY

In this section we introduce a case study of a WHMS capable of collecting, digitizing, connecting to a wearable medical device via Bluetooth, and measuring various physiological parameters of patients in particular suffering from heart disease. The developed system has an user friendly interface based on a web portal that allows to monitor in real time both health conditions as well as the status of devices, thus providing an effective tool to reduce the time of intervention when complications rise, as well as allowing continuous long-term monitoring and data collection.

The implemented system provide several functionalities to:

- Collect the health data from measurements on the patient;
- Transmit them to Cloud services;
- Memorize measurements in a long-term storage;
- Assess statistics from such data;
- Retrieve data for authorized users, i.e. patients and/or medicians.

Figure 1 depicts the overall system architecture.

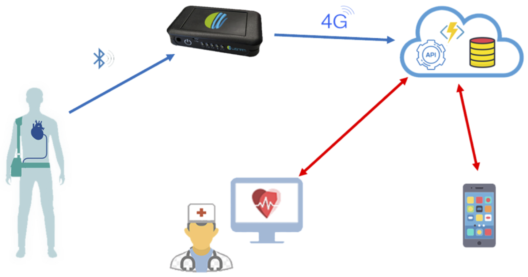


Figure 1: System Architecture.

From a software point of view, main components to implement the service are:

- A Backend Server for the communication and data processing functions.
- A Database to store data collected by the monitoring subsystem (and used by the Backend)
- Web Portal available for computers and mobile devices, to provide access to the system.

3.1 Functional Requirements

An intelligent monitoring system that allows to manage the patients should provide different functionalities for users as patients themselves, but also doctors, control staff, each according to his/her own profile.

In particular, the system must be able to display the various data collected over time in the right format for the different types of analysis that can be performed by users; a simple interface is therefore essential to display the most relevant measurements in real time. Furthermore, time charts are useful to show the dynamic data behaviour; it should be also possible to graph and export data within a given period of time to allow historical medical analysis with other specific tools. All this data can be used for training an intelligent system to detect and prevent alarm situation.

Finally, the system comes with the following features:

- Management of user accounts
- Management of devices
- Associate devices to users
- Access to the measurements collected by the devices
- Provide data graphical representation.
- Notification and management of alarm situation
- Export the data within a given time interval

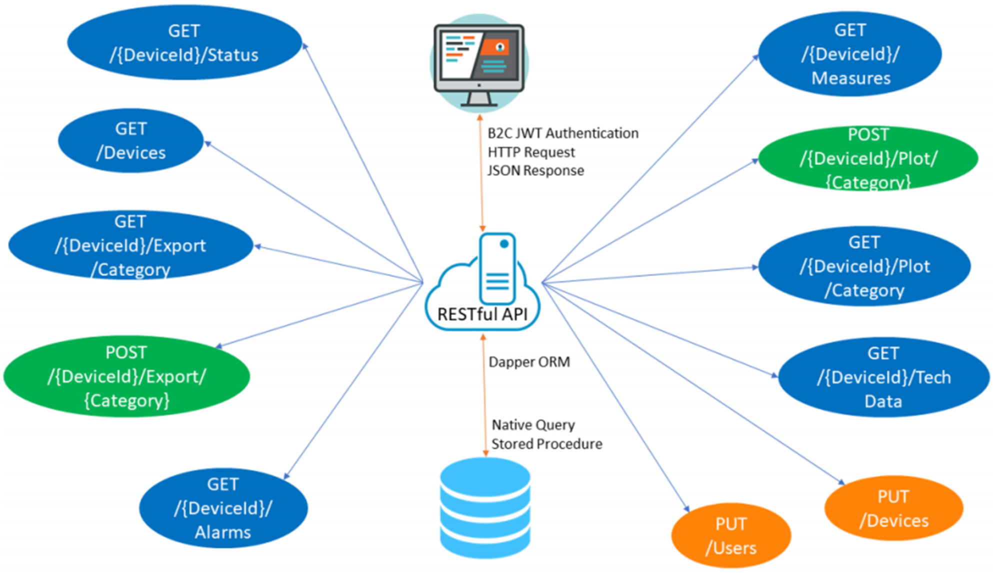

GET /{DeviceId}/Status
GET /Devices
GET /{DeviceId}/Export /Category
POST /{DeviceId}/Export/ {Category}
GET /{DeviceId}/ Alarms
B2C JWT Authentication
HTTP Request
JSON Response
RESTful API
Dapper ORM
Native Query
Stored Procedure
GET /{DeviceId}/ Measures
POST /{DeviceId}/Plot/ {Category}
GET /{DeviceId}/Plot /Category
GET /{DeviceId}/Tech Data
PUT /Devices
PUT /Users

Figure 2: System Components.

3.2 Performance and Security Requirements

Dealing with sensitive data the system must be equipped with appropriate security mechanisms. It must be designed to protect information access from unauthorized users, also providing appropriate clearances for different types of users according to their profiles. Moreover, the system must cope with various performance issue, i.e. it must be able to manage peaks of information transmission (up to thousand of active users on the web portal and a lot of devices that continuously produce data). To address this, it is necessary to design a robust and scalable architecture able to manage variable workloads while maintaining constant performance and high fault tolerance.

The features described above can be summarized in the following points:

- The access to the system must be allowed only to registered users according to proper ACL (Access Control List)
- Each user must have access only to his/her own devices.
- The web interface must be compatible with common browsers.
- The system must be scalable to cope high-volume of active users simultaneously.
- The system must have low fault recovery times and high availability.

3.3 Technologies and Services

To implement all requirements described so far, we chose the following technologies.

- ASP.NET Core as framework for Back-end development, as it natively supports various security-related features also in cloud services scenario
- Microsoft Azure as a cloud service provider, as it provides integration with the projects developed in ASP.NET Core thanks to the App Service hosting services. It also provides the Azure Active Directory B2C service for managing user authentication as an Identity Provider
- Angular as a complete framework for developing client-side applications
- Microsoft SQL Server to support transactions and backup features (high reliability); it also provides adequate security management mechanisms; Based on the type of data (mainly structured), we did not choose a NoSQL database.

4 IMPLEMENTATION ISSUES

The WHMS architecture proposed in the previous section is actually implemented following the Model-View-Controller (MVC) pattern arranged into two components: Controller-Model and View. The back-end server (i.e. the Controller-Model) is hosted on a cloud service that implements different REST APIs for data extraction and that are accessed through the

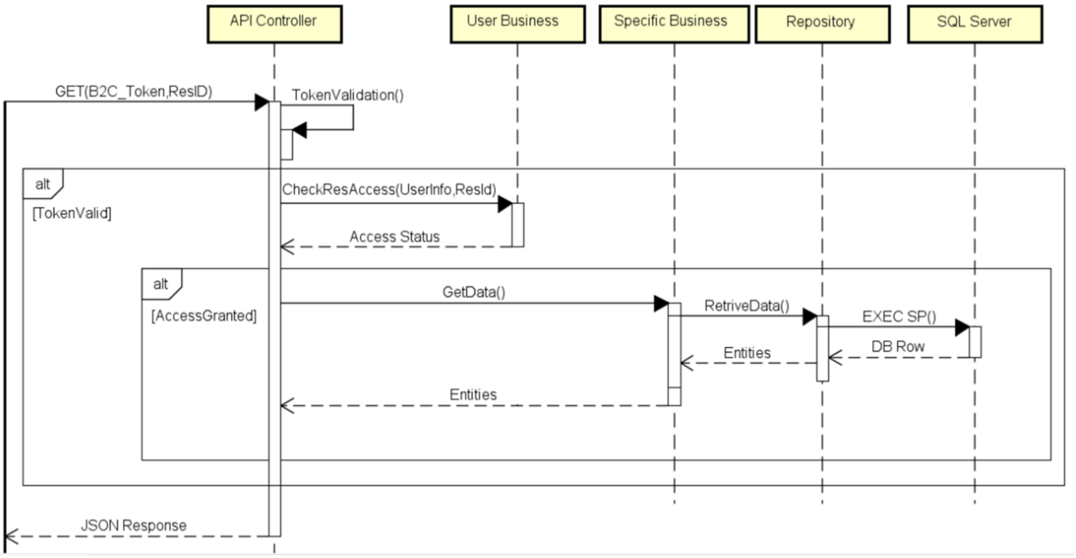


Figure 4: General Sequence diagram of an API.

frontend interface (the View). Between the backend server and the database there is often an intermediate level to decouple the two actors using a set of Stored Procedures. Figure 2 shows the MVC architecture with the main APIs offered by the backend server to fulfil the requirements.

Access to each API is protected by the Azure B2C authentication mechanism (namely Active directory B2C or AD–B2C). In each request it is necessary to send the JWT Token obtained through the log-in procedure. In addition to the mechanism offered by AD–B2C, in each API there is an additional level of security that verifies whether the user who made the request has access to the resources he is also requesting for; some specific APIs such as those related to device or user management are protected by a user type filter as only administrators are authorized to use it.

Using these two security levels, access to data is guaranteed only to users authenticated via AD B2C and authorized through a proper internal policy of access management.

In Figure 3 is represented the two levels MVC architecture, in particular the Controller is represented by the API Controller that intercepts calls coming from the frontend (View), retrieving the necessary information from the Model. The Model is represented by the DataAccess Layer, but to make the Model flexible a Business level has been added to the DataAccessLayer to decouple the implementation of the business rules from the implementation of each individual variant of the Model itself.

Taking into account this software structure where the Business Layer represents an extension and interface to the DAL, we included a caching mechanism for data with low rates of change and high request rates. In particular the data concerning the users are continuously requested for security purposes as it is necessary to verify the access authorizations to the resources. Since the UserBusiness module in the Business Layer is the only that manipulate such data, it is easy to keep this cache coherent, invalidating it when a modification method is called.

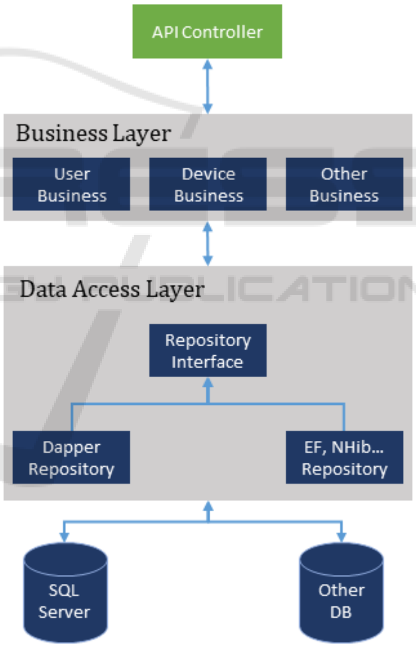
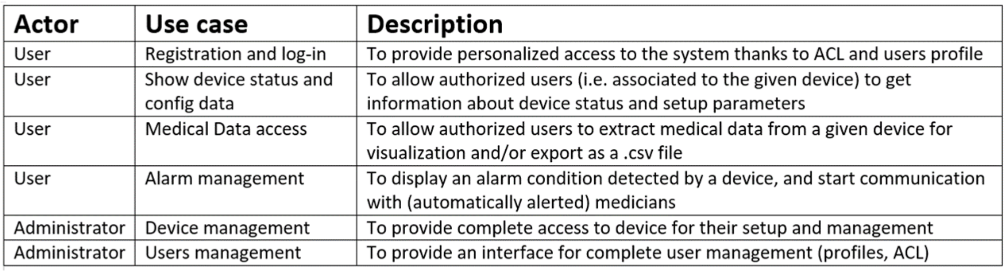


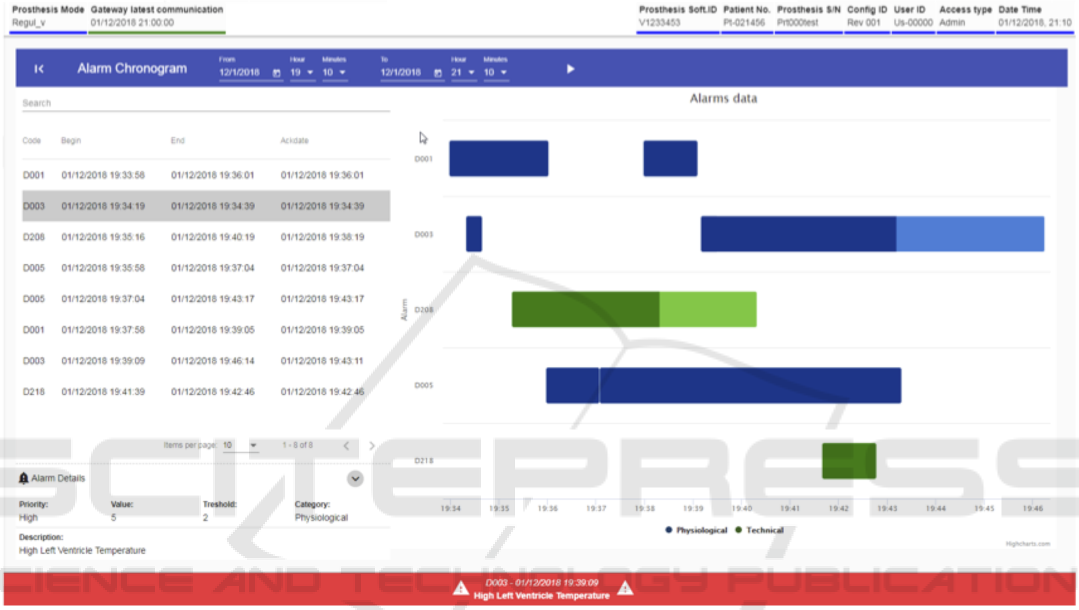
Figure 3: Back-end structure.

Figure 4 shows a general sequence diagram rep-



Actor	Use case	Description
User	Registration and log-in	To provide personalized access to the system thanks to ACL and users profile
User	Show device status and config data	To allow authorized users (i.e. associated to the given device) to get information about device status and setup parameters
User	Medical Data access	To allow authorized users to extract medical data from a given device for visualization and/or export as a .csv file
User	Alarm management	To display an alarm condition detected by a device, and start communication with (automatically alerted) medicians
Administrator	Device management	To provide complete access to device for their setup and management
Administrator	Users management	To provide an interface for complete user management (profiles, ACL)

Figure 5: Use cases.



Prosthesis Mode	Gateway latest communication
Regul_v	01/12/2018 21:00:00

Prosthesis Soft.ID	Patient No.	Prosthesis S/N	Config ID	User ID	Access type	Date Time
V1233453	Pt-021456	Prt000test	Rev 001	Us-00000	Admin	01/12/2018, 21:10

Alarm Chronogram

From 12/1/2018 Hour 19 Minutes 10

To 12/1/2018 Hour 21 Minutes 10

Search

Code	Begin	End	Ackdate
D001	01/12/2018 19:33:58	01/12/2018 19:36:01	01/12/2018 19:36:01
D003	01/12/2018 19:34:19	01/12/2018 19:34:39	01/12/2018 19:34:39
D208	01/12/2018 19:35:16	01/12/2018 19:40:19	01/12/2018 19:38:19
D005	01/12/2018 19:35:58	01/12/2018 19:37:04	01/12/2018 19:37:04
D005	01/12/2018 19:37:04	01/12/2018 19:43:17	01/12/2018 19:43:17
D001	01/12/2018 19:37:58	01/12/2018 19:39:05	01/12/2018 19:39:05
D003	01/12/2018 19:39:09	01/12/2018 19:46:14	01/12/2018 19:43:11
D218	01/12/2018 19:41:39	01/12/2018 19:42:46	01/12/2018 19:42:46

Items per page: 10 1 - 8 of 8

Alarm Details

Priority:	Value:	Treshold:	Category:
High	5	2	Physiological

Description:
High Left Ventricle Temperature

D003 - 01/12/2018 19:39:09
High Left Ventricle Temperature

Figure 6: The application interface showing an alarm.

resenting the typical operations that are performed at each invocation of an API. Note the lack of communication between UserBusiness and Repository as the caching mechanism is often used.

On the front-end architecture we briefly discuss the implementation of the communication logic with the APIs. In particular with AD–B2C policies web pages where users can register or log in are available. Once these operations are completed, the web pages automatically redirect the browser to the web application page by sending the generated access token to the URL. The application caches the token during the session using the API as Bearer Token at every request. Most APIs implement a simple communication flow that ends with a single call. For instance, the API that return the points for the graphs implements a paging mechanism where the whole data flow is received through several calls; this is performed since data to download are huge and we want to avoid communication timeout problems.

Figure 5 illustrate a set of use cases the proposed application actually address; here we focus on users and administrators as two main actors that can access the system.

Finally, figure 6 shows the GUI of the proposed WHMS, in particular displaying an example of an alarm detected (high left ventricle temperature warning).

5 CONCLUSIONS AND FUTURE WORK

In this paper, an implementation of a Wearable Health Monitoring Systems has been presented. The proposed system gathers physiological parameters of patients suffering from heart disease, sends data to Cloud services, and allow processing data for medical analysis, providing secure access to both patients and medicians within a proper architecture. The system has been implemented by Wisnam (https://www.wisnam.com/), and it is currently under intensive testing, also to exploit gathered data to train intelligent monitoring algorithms. In particular, machine learning techniques are under investigation to effectively support the prevention and early detection of relevant illness symptoms to activate timely needed medical treatments. Another line of research concerns the improvement of back-end services in order to process more and more data in a lesser time, for and also to support as many simultaneous users as possible. Finally, a next step is the migration of the system onto a serverless architecture, to not depend on a single point of failure at the same time achieving a high scalability.

REFERENCES

Baird, A., North, F., and Raghu, T. S. (2011). Personal health records (phr) and the future of the physician-patient relationship. In *Proceedings of the 2011 iConference*, iConference '11, pages 281–288, New York, NY, USA. ACM.

Chen, M., Mao, S., and Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, 19(2):171–209.

Eysenbach, G. (2001). What is e-health. *Journal of medical Internet research, vol. 3 no. 2*.

Ferebee, D., Shandilya, V., Wu, C., Ricks, J., Agular, D., Cole, K., Ray, B., Franklin, A., Titon, C., and Wang, Z. (2016). A secure framework for mhealth data analytics with visualization. In *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, pages 1–4.

GHO (2019). *Global Health Estimates - World Health Organization - https://www.who.int/ health-info/ global_burden_disease/en/*.

Haghi, M., Thurow, K., and Stoll, R. (2017). Wearable devices in medical internet of things: Scientific research and commercially available devices. *Healthcare Informatics Research*, 23:4–15.

Hong, Y.-J., Kim, I.-J., Ahn, S. C., and Kim, H.-G. (2010). Mobile health monitoring system based on activity recognition using accelerometer. *Simulation Modelling Practice and Theory*, 18(4):446 – 455. Modeling and Simulation Techniques for Future Generation Communication Networks.

Ismail, A., Shehab, A., and El-Henawy, I. M. (2019). *Healthcare Analysis in Smart Big Data Analytics: Reviews, Challenges and Recommendations*, pages 27–45. Springer International Publishing, Cham.

Istepanian, R. S. H., Laxminarayan, S., and Eds, C. S. P. (2006). *M-Health - Emerging Mobile Health Systems*. Springer US.

Miraz, D., Ali, M., Excell, P., and Picking, R. (2015). A review on internet of things (iot), internet of everything (ioe) and internet of nano things (iont). pages 219–224.

Pandian, P., Mohanavelu, K., Safeer, K., Kotresh, T., Shakunthala, D., Gopal, P., and Padaki, V. (2008). Smart vest: Wearable multi-parameter remote physiological monitoring system. *Medical engineering and physics*, 30:466–77.

Postolache, G., Girão, P. S., and Postolache, O. (2013). *Requirements and Barriers to Pervasive Health Adoption*, pages 315–359. Springer Berlin Heidelberg, Berlin, Heidelberg.

Ren, Y., Werner, R., Pazzi, N., and Boukerche, A. (2010). Monitoring patients via a secure and mobile healthcare system. *IEEE Wireless Communications*, 17(1):59–65.

S., M., T., M., and J., D. M. (2017). Wearable sensors for remote health monitoring. *Sensors (Basel, Switzerland)*, 17.

SHARPS (2019). *Strategic Healthcare IT Advanced Research Project on Security - https://sharps.org/*.

Shih, D., Chiang, H., Lin, B., and Lin, S. (2010). An embedded mobile ecg reasoning system for elderly patients. *IEEE Transactions on Information Technology in Biomedicine*, 14(3):854–865.

Solanas, A., Patsakis, C., Conti, M., Vlachos, I., Ramos, V., Falcone, F., Postolache, O., Pérez-Martínez, P., Pietro, R., Perrea, D., and Ballesté, A. (2014). Smart health: A context-aware health paradigm within smart cities. *IEEE Communications Magazine*, 52:74–81.

THaW (2019). *Trustworthy Health and Wellness - https://thaw.org/*.

TMR (2019). *Transparency Market Reasearch - Wearable Tech report - https://www.transparencymarketresearch.com/ pressrelease/ wearable-technology.htm*.