An Internet of Things Framework for Remote Monitoring of the HealthCare Parameters

Ioan UNGUREAN[1,2], Adrian BREZULIANU[3]
[1]*Stefan cel Mare University of Suceava, 720229, Romania*
[2]*Integrated Center for Research, Development and Innovation in Advanced Materials, Nanotechnologies, and Distributed Systems for Fabrication and Control (MANSiD), Stefan cel Mare University, Suceava, Romania*
[3]*Gheorghe Asachi Technical University of Iaşi, 700050, Romania*
ioanu@eed.usv.ro

***Abstract*—Due to its very high potential, the Internet of Things (IoT) concept has been integrated in modern telemedicine systems. These systems enable real-time monitoring of patients at home, by using devices for acquiring various medical parameters or wearable devices that allow real-time monitoring of the medical signals. The data are transmitted to a medical specialist's office via the Internet and can be stored in cloud for further analysis. This article proposes an IoT architecture that can be used in healthcare for monitoring ECG signals independently acquired by the patient, using a mobile tele-electrocardiograph, without the help of a specialist. The main features of the mobile device are described, as well as how these features are integrated into the proposed IoT architecture. The article also tackles the security issues that may occur during the using of this system: integrity, confidentiality and authenticity.**

***Index Terms*—internet of things, telemedicine, electrocardiography, software architecture, distributed information systems.**

I. INTRODUCTION

The term Internet of Things (IoT) was originally defining the connection of RFID devices and of wireless sensor networks to the Internet [1]. The IoT paradigm has evolved and currently, it comprises technologies necessary for connecting physical devices to the Internet in order to interact with each other in the virtual environment. This is part of the Future Internet paradigm, making the shift from people-to-people communication to things-to-things and people-to-things communication [2].

The IoT paradigm comprises new techniques available for data acquisition in the ubiquitous environments (sensors), communication technologies (sensor networks, device-to-device communication, machine-to-machine communication), fog computing (IoT Gateways) and cloud computing. Currently, there are several available definitions of IoT, but none is generally agreed on. For example, ITU (International Telecommunication Union) defines IoT as "a global infrastructure for the information society, enabling advanced services by Interconnecting (physical and virtual) Evolving things based on existing and inter-operable information and communication technologies"[3]. Basically, this paradigm refers to transferring real-world objects in the virtual world and interacting with each other in the virtual environment.

In the last decade, the IoT concept developed strongly, being currently used in domains like industrial environments [4] (Industrial Internet of Things), intelligent homes, telemedicine, etc. Therefore, IoT encounters new challenges, such as latency constrains, network bandwidth constrains, resource-constrains devices, uninterrupted service without Internet access, and new security challenges. Furthermore, IoT has high potential on the commercial market. General Electric estimates that by 2020, IoT will generate 514 billion worth business [5]. The raw information that must be processed will also grow. Currently, IoT contains billions of connected devices that each day generates two Exabyte of data. The consulting McKinsey & Company estimates that the development of the IoT technology will result in increased productivity, and by 2025 it will reach an added value of 2.7 to 6.2 trillion dollars per year [6]. Cisco also analysed the market potential of the IoT technology and estimated that in the next decade, IoT will interconnect 50 billion devices and, because of the increased productivity, will generate an additional profit of 14 trillion dollars [7].

Thanks to the rapid development of the concept, IoT solutions have also been developed in the field of healthcare [8]. These solutions enable the remote monitoring of medical parameters acquired from the home patient and sending the data to specialists for analysis. Furthermore, after the analysis of data, certain decisions can be made, such as the automatic notification of emergency medical services. In this article, the authors propose an IoT system used for acquiring ECG signals from the home patient and transmitting them to specialists for analysis. The core component of this system is a mobile tele-electrocardiograph that may acquire the ECG signals from the patient. This tele-ECG is not as competitive as an electrocardiograph from the specialist's offices, but it provides basic monitoring by which the patient's evolution over time can be analyzed. In this paper, we focused on presenting the IoT architecture proposed for patient monitoring and on describing the way in which the mobile device is integrated in the proposed IoT architecture.

The article is structured as follows: in section 2, some IoT solutions from the medical field, described in the literature,

This paper was supported by the project “Development and integration of a mobile tele-electrocardiograph in the GreenCARDIO© system for patients monitoring and diagnosis - m-GreenCARDIO”, Contract no. BG58/30.09.2016, PNCDI III, Bridge Grant 2016, 2016, using the infrastructure from the project “Integrated Center for research, development and innovation in Advanced Materials, Nanotechnologies, and Distributed Systems for fabrication and control”, Contract No. 671/09.04.2015.

Digital Object Identifier 10.4316/AECE.2017.02002

are presented; section 3 describes the architecture of the proposed system; section 4 depicts the methods of integrating a mobile ECG device in the system are described; section 5 tackles the main security problems of the proposed architecture, as well as methods to avoid them; section 6 consists of the final conclusions.

II. Related Works

In this section, there are presented the most important projects in the field of Internet of Things with applicability in healthcare that are presented in the specialty literature. There are more healthcare services that can be activated by the IoT [8]: ambient assisted living (AAL), Internet of m-heath (m-IoT), monitoring the adverse drug reaction, community healthcare, children healthcare information, access the wearable device, indirect emergency healthcare. The principal application that can be activated by the IoT [8] are monitoring the EGC signals, monitoring the body temperature, monitoring the glucose level, monitoring the blood pressure, monitoring the oxygen saturation. For all these applications, there are used non-invasive methods to acquire medical information from the patients. These systems use advanced algorithms [9] in order to analyse the medical information acquired from the patients.

A first service that is activated by IoT is Ambient Assisted Living (AAL). Usually, these systems are specialized for elderly individuals. These systems are found in smart homes or IoT healthcare systems and there are aimed to ensure primarily independent life for older people. AAL provides greater autonomy elderly and incapacitated individuals by assisting them with any problems. A reference architecture for systems IoT-AAL is presented in [10], referred to as a NEMO-HWSN. This architecture can provides healthcare services for elderly and disability individuals. NEMO-HWSN is modular and is based on 6LoWPAN protocol for communication and RFID and NFC technology for identification. In the context of the IoT, in a F7 project there defined an open architecture and reference specifications for AAL [11]. This architecture, refereed as universAAL, provide the runtime support for AAL service and support for developers and community.

Another service that can be activated by the IoT Internet of m-health things (m-IoT). The m-health concept refers to the use of mobile devices (especially smartphones) for data collection in real-time from the patients. These solutions are used by physicians in order to remotely monitor the patients and use wearable and medical sensors together with communication technologies for data acquisition. An example of an m-IoT system for non-invasive measuring of the glucose level is presented in [12].

Among the applications that can be activated by IoT one of the most important is the monitoring of the electrocardiogram (ECG). An ECG monitoring system based on the IoT is presented in [13]. The proposed architecture uses a device with three electrodes that connects to the Internet through three interfaces: Wi-Fi, Bluetooth and ZigBee (for the last two a smartphone is used as gateway). In order to transmit data to the Internet it is used the MQTT middleware protocol. The data are stored in the cloud and can be viewed by the patient, family members and the doctor via a GUI interface (via HTTP requests or MQTT subscriptions). Others IoT architectures for monitoring of the ECG are presented in [14],[15],[16].

Other healthcare application that can be implemented throughout the IoT is the monitoring of the blood pressure. IoT solutions for this type of application are presented in [17] and [18]. In these systems, emphasis is placed on the use of wearable sensors and the use of non-invasive sensors for the acquisition of the medical data.

An m-IoT solution for the monitoring of the body temperature is presented in [19]. An IoT solution for the monitoring of the oxygen saturation based on wearable sensor is presented in [20].

In [21] is presented a review for the IoT-based prognostics and systems health management (PHM). The authors introduce the PHM terms and there are identified the IoT opportunities for the design of the PHM using the IoT. PHM are used to detect the diagnosing failures. The PHM system consists of four modules: sensing, diagnosis, prognosis, and management. Furthermore, the authors identifies the main challengers for adoption oh the IoT in de development of the PHM systems.

Currently, there are many IoT solutions that enable different healthcare applications. These applications focuses on the use of sensors that can acquire medical data without interfering too much in daily life of the patients. They use wearable sensor or mobile sensors that can directly transmit data to Internet or through a gateway (smartphone or a computer). These systems monitor the patient evolution but they does not perform a diagnosis of the patient, the physicians perform the diagnosis based on data received from sensors. In the best-case scenario, these systems can activate different alarms that are transmitted to the doctor when medical parameters are not in the normal range.

With the exponential development of the concept of IoT and smart home, IoT increasingly advanced solutions for healthcare applications will be developed and launched on the market. Remote monitoring of the medical parameters can reduce the healthcare costs and the doctors will always have medical data about patients without their presentation in the doctor's office.

III. The Proposes m-IoT Framework

This paper proposes an IoT framework for the monitoring of ECG signals. It is an m-IoT architecture because it uses the mobile devices to acquire data from the medical sensors. The architecture consists of four levels: sensing, middleware gateway, storage and application (according with Figure 1).

At the bottom is the sensing level consists of devices that acquires ECG signals. In this architecture, it is desired to use a mobile device that can be purchased by the patient. For this reason, it was designed and developed a mobile embedded device in order to meet the requirements of the current architecture and to be as inexpensive as possible. The device provides multiple communication interfaces in order to have multiple alternatives for Internet connection. It has been designed around of the STM32F107 microcontroller (ARM® 32-bit Cortex® -M3 CPU with 256 Kbytes and 64 Kbytes of general-purpose SRAM) to which ADAS1000 device from Analog Device (a peripheral designed for acquiring ECG signals) has been connected. The main features of the mobile device are the following:

socket for mini-SD flash card (used for storing the acquired ECG signals), Bluetooth, GSM and USB communications, powered by a rechargeable battery that can be charged via the USB port, three signalling LEDs and a button for initiating / stopping the acquiring operations.

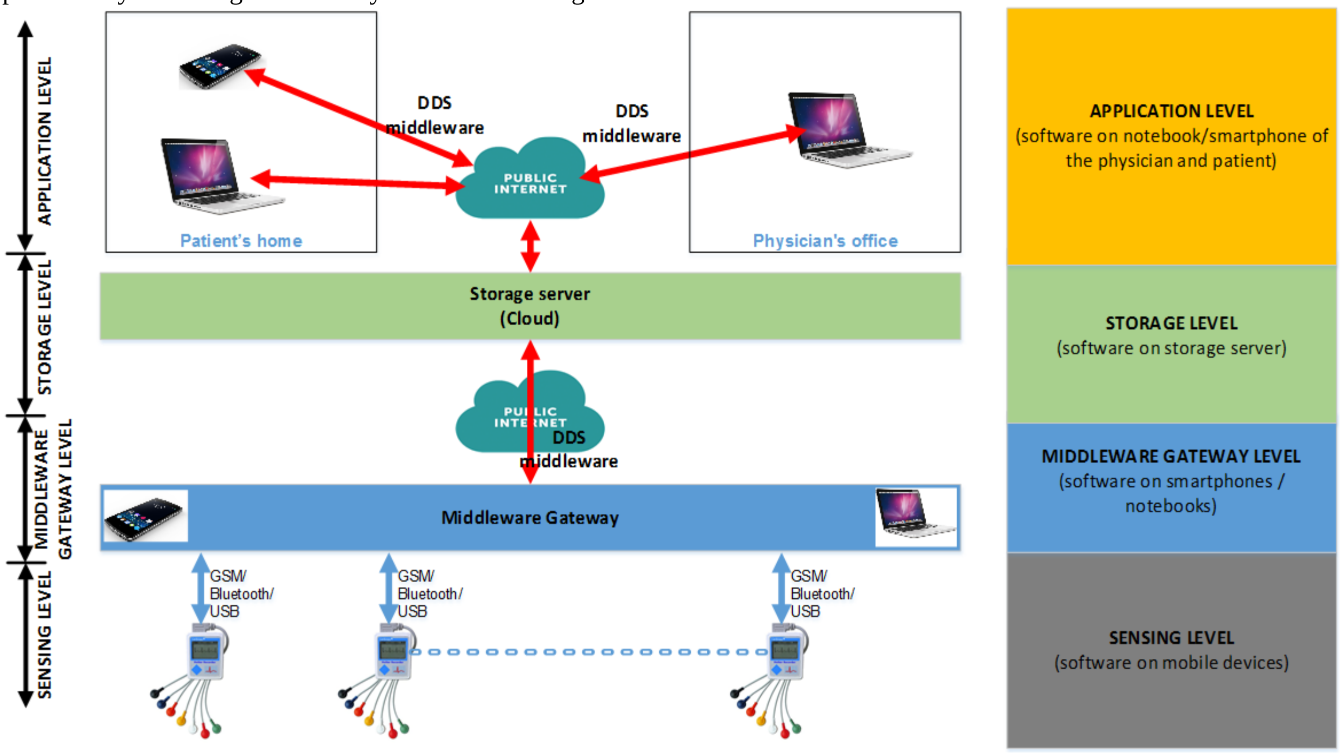

Figure 1. The proposed IoT framework

The device has three electrodes for ECG signal acquisition (according to the speciality literature is sufficient the acquisition of the three ECG signals to obtain an electrocardiography that can be analysed by the physician [13]). The hardware and software architecture of the mobile device will be presented in another article, because the present article is focused on the IoT architecture and the integration of the mobile device.

The gateway middleware level allows the transmission of data acquired from the mobile device to a central server where the data are stored. This level contains the entire software infrastructure for mobile devices (smartphones, notebooks) necessary to retrieve data from the mobile ECG device and to transmit data to the central server. For data acquisition is used the MODBUS protocol on the command Bluetooth (Virtual COM), USB and GSM (SMS messages) interfaces. These data are packaged and sent to the central server using the Data Distribution Service for real-time systems (DDS) middleware protocol [4]. It was chosen this protocol because it allows a high security level.

At the third level, there are stored patient's ECG data in order to be viewed and analysed later by the physician. In this case, it is used a virtual computer system on the cloud that is focused on data storage. The system executes a server that allows the transfer of data from patients in order to be stored and it answers at the requests from the physician and patient (applications used to visualization the ECG signals from the server).

On the last level is the application for the m-IoT architecture. In this case, there are two software application: one in the physician's office and one in the patient's mobile device (notebook or smartphone). On each application, physicians and the patients must use authentication data in order to access the information form the storage server. The application from the physician's office allows the visualization and analysing of the ECG signals acquired by the patients. Based on this information, he may decide to call the patient in the physician's office to make an electrocardiogram using a professional ECG signal or to require to the patient to perform other ECG acquisitions in order to eliminate any suspicion of erroneous data acquisition. The application from the patient's mobile device is used to view the ECG acquisition made and to receive messages from any doctor. The application in the doctor's office is designed and developed for Windows based devices and patient related application is developed an designed in two versions: for Windows and Android devices.

IV. Integration of the Mobile ECG Device in the M-IoT Architecture

This section presents several methods of integrating the mobile ECG device in an Internet of Things type architecture (m-IoT). The integration refers to how the mobile ECG device connects and sends the acquired information to the central storage server. The mobile ECG device is used at home by the patient in order to acquire and transmit the ECG data to the central server via an Internet connection. If there is no Internet connection, the data is stored in an internal flash memory and transmitted to the storage server, when there is an active Internet connection. Figure 2 shows the software architecture of the system in which the mobile device is integrated. It can be seen that the mobile device has multiple data transmission options (direct connection via a smartphone or a notebook / PC).

In order to integrate the mobile ECG device in the m-IoT architecture, it's communication interfaces must be taken into consideration (according to section 3, it will be able to communicate via the Bluetooth, GSM, and USB interfaces, the latter used for charging the rechargeable battery).

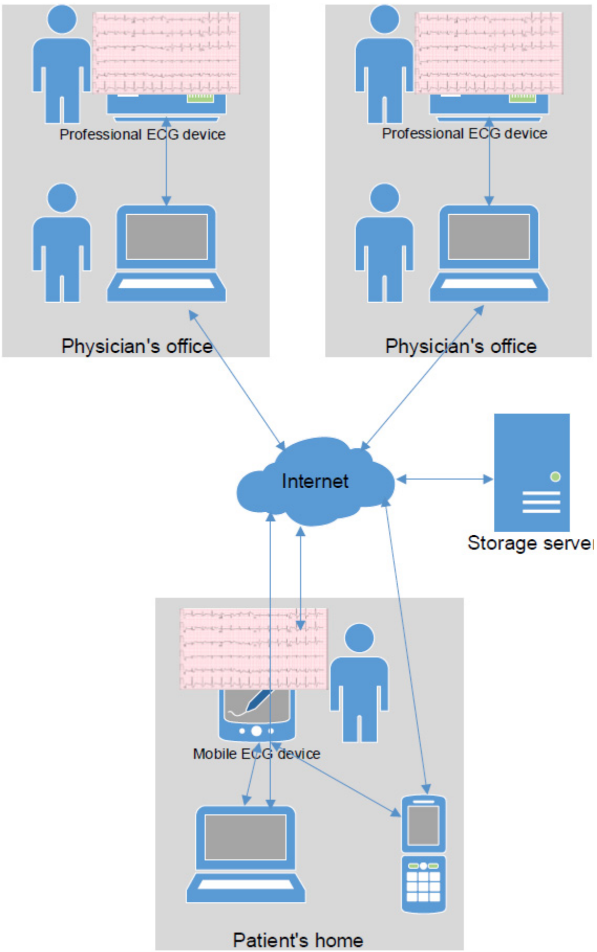

Figure 2. Integrating the mobile ECG device in the proposed m-IoT architecture

In conclusion, the following methods for transmitting data to the central storage server are possible:

- Bluetooth – smartphone mobile device (with an Internet Connection) - storage server.
- Bluetooth – PC/notebook mobile device (with Internet Connection) - storage server.
- GSM data mobile device – storage server.
- GSM data mobile device –PC/ notebook (with Internet connection) with GSM modem from the storage server.
- USB mobile device – PC/notebook (with Internet connection) - storage server.

Besides the two connections, a possible communication via the USB port has been added. The USB port on the mobile device is used for charging, but it can also be used for downloading data from the mobile device and for transmitting them to the storage server.

A. Communication via the Bluetooth interface

Figure 3 shows how to integrate the mobile ECG device in the m-IoT system, when it transmits data via the Bluetooth communication interface. Since the device cannot be directly connected to the Internet via the Bluetooth interface, we need an intermediary device with an Internet connection and a communication interface. In this case, a smartphone (with Android operating system) or a notebook /PC can be used. These intermediary systems take the raw data from the mobile device and can perform a basic processing (filtering, presenting the data, adding identification information for the patient for whom the ECG signal has been acquired etc.) and transmit the data to the core server for monitoring and further evaluation by specialists. For an complete ECG acquisition the amount of raw data that must be transferred is 30Kbytes (500 samples per second * 3 signals * 2bytes for each value * 10 seconds).

If already connected to a smartphone or a notebook, the mobile device can initiate the transmission of data; after connecting to a device, the intermediary system can also initiate data transmission. The application running on the intermediary device (smartphone/ notebook) also enables the setting of the device with patient identification parameters.

Figure 3. Transmitting data through the Bluetooth interface

B. Communicating via the GSM interface

Figure 4 presents the integration of the mobile ECG device in the m-IoT architecture when it is transmitting data through the GSM communication interface. In this case, the device is equipped with a GSM modem in which a SIM card from a data GSM service provider is inserted. In this case, the microcontroller of the mobile device communicates with the GSM modem via a serial port and AT commands (Hayes command set for GSM modems). This method of data transmission differs from the transmission through the Bluetooth network. In the first version, the mobile device can initiate a data connection and send data directly to the central monitoring server. In this case, the device uses a GPRS/2G/3G connection and must implement the communication stack for the communication protocol with the central storage server.

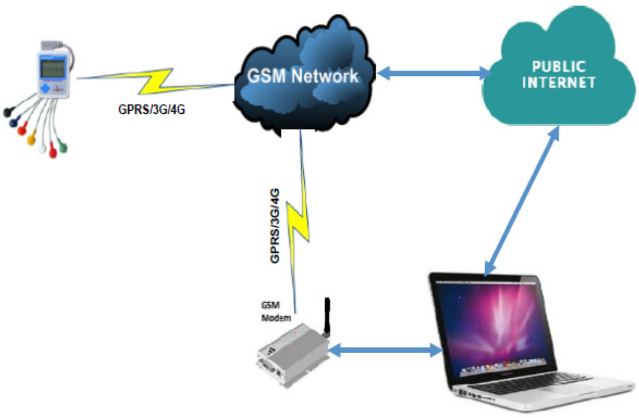

Figure 4. Transmitting data through the GSM interface

Since the implementation of this stack would consume many computing and energy resources, the second option can be chosen; for this option, there is an intermediary system (notebook/PC) with a GSM modem that supports data connections and that can be called by the mobile device for the transmission of data. After receiving the data from the mobile device, the intermediate system may perform basic processing (filtering, data representation mode, adding acquired identification data of the patient for whom the ECG signal has been acquired, etc.), after which it will transmit the received information to the central monitoring server. The intermediary system with the GSM modem can be placed in the office of the physician or in the same location as the central storage server. Moreover, this last option enables the transmission of data also from locations where there is no Internet connection and it is not necessary that the intermediary system is in the close vicinity of the mobile device, as in the case of using the Bluetooth interface. The downside is that a SIM card with a valid number and an activated data transmission option must be allocated for the mobile device, and this may entail additional costs.

C. Communicating via the USB interface

The mobile ECG device can be integrated in the m-IoT architecture through the USB communication interface. The USB interface is included in the mobile device to charge the battery, but it can be used for transmitting data to the central monitoring server. The same software module can be used as in the case of transmitting data via the Bluetooth network.

Furthermore, the USB interface can be used for setting the device with the identification parameters of the patient using the mobile device. The USB interface is an alternative to the other methods of transmitting data and can be used in the stage of debugging and testing the mobile device (it is much easier for the user to configure a connection through the USB network than to configure a connection through the Bluetooth network).

D. Conclusions regarding the integration of the mobile ECG device in the m-IoT system

Based on the integration methods mentioned above, the following conclusions can be drawn regarding the design of the mobile device: an Android application (for the smartphone) communicating with the mobile device had to be designed and developed for the Bluetooth interface, and a PC application has been developed for the Windows operating systems (notebook / PC with Bluetooth interface).

If the mobile device uses the GSM interface to connect directly to the central monitoring server, the implementation of the communication stack requires a microcontroller with a higher computing power, thus generating higher energy consumption and a higher final cost. Therefore, this method is not reliable and it is not integrated in the design and development of the mobile device.

If GSM communication is used with an intermediary (a PC with GSM modem), then an application for Windows operating systems must be developed, that communicates with the mobile device via the GSM modem. The application may be the same as with the Bluetooth interface, allowing multiple types of connections with the mobile device. This solution generates additional costs for SIM data cards used for the mobile device and the intermediary system. The intermediary system can be located any place with GSM signal and Internet connection (family physician's office, the same data center as the central storage server etc.).

The USB interface is used for charging the battery of the mobile device and enables communication with the device for making the basic settings; it ca also be used in the phase of debugging and testing the mobile device. During the design stage, a communication protocol between the mobile device and the intermediary systems has been defined. This protocol is as simple as possible, in order not to complicate the communication stack (as few computing requirements as possible and, consequently, as low energy consumption as possible).

The applications on the intermediate devices will implement the communication protocol based on the DDS specifications with the central monitoring server. Here, more complex operations on the acquired data can be made, because the available computing resources are much higher compared to the mobile device.

In conclusion, for integrating the mobile device in the IoT system, two software applications have been designed and developed:

- An application on the mobile devices with Android operating system. This application communicates with the phone via the Bluetooth interface and implements the protocol for communicating with the central monitoring server. The application can be run on the smartphone or tablet with an Internet connection.
- An application on computers with Windows operating systems. This application communicates with the mobile device via the Bluetooth, USB and GSM (via a modem connected to the PC) interfaces and implements the protocol for communicating with the central monitoring server. The application needs to run on a system with an Internet connection. The application also allows the configuration of the mobile device with the data of the patient using the device for acquiring the ECG signals.

V. SECURITY

Security is very important in medical systems. Data must be confidential and can only be accessed by the patient and the medical specialist. Therefore, all data on the central server can be accessed only after a prior authentication. When transmitting data to the central server, security issues appear in two points. The first point regards the transmission of data by the mobile device. The transmission via USB or GSM does not raise security issues, because the transmission is done point to point. In regard to communication via Bluetooth, a code must be entered for establishing the connection. Without this code, the smartphone or the PC cannot establish a connection with the mobile device. This code can be changed in the setup process, via the USB port. The second point regarding security is during the transmission of data to the central server. For this transmission to take place, an authentication on the central server (based on username and password) is performed, and then the transmission is performed using DDS specifications. In this case, the security specifications published in December 2016 are also implemented [22].

These specifications provide solutions for data confidentiality, non-repudiation of data, message integrity, authentication and authorization of entities that write and read data. The main threats removed by these specifications are the following: unauthorized subscription, unauthorized publication, unauthorized access to data, tampering and replay.

VI. CONCLUSION

The present article proposed an IoT architecture that enables the remote monitoring of ECG signals. The software architecture of the system has been detailed. A mobile device for ECG signal acquisition has been designed and developed; the device can transfer data to a central storage server through various communication interfaces. Once reaching these servers, the data are further available for medical specialists. PC and smartphone applications have been designed for integrating the mobile device in the IoT architecture, and for increased security; these application mediate the connection between the mobile device and a central server from the IoT architecture. The advantage of the proposed architecture is that it can monitor patients remotely, without the need to be present at the doctor's office. The system also includes security mechanisms that can guarantee the confidentiality and integrity of data transmitted over the Internet.

As was seen in Section 2, there are already software solutions for remote monitoring of the patients. The novelty of the presented solution is the implementation of the concept of remote monitoring of patients in the context of the IoT paradigm. In addition, for data transmission in the Internet, it was used a middleware system that implements the DDS protocol. The middleware systems allow a standardization of the communication interfaces between the software modules. Another new contribution is the data on security, integrity and security that are implemented using the DDS security specifications.

As a disadvantage, it can be said that the measurements of the ECG signals are not as precise as when performed in the doctor's office, because the aim was to design a mobile device as cost effective as possible. Based on data acquired by the mobile device, the medical specialist can decide if more accurate measurements need to be performed in the doctor's office. Therefore, the system enables a screening of patients who must visit the doctor's office for further investigations. In the future, the system can be developed by introducing other devices for acquiring medical data that can be used by patients at home, without the help of medical specialists. In this case, patient's health can be monitored over time.

REFERENCES

[1] A. Kevin, "That ‘internet of things’ thing," RFiD Journal, 22 June, 2009.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015. doi:0.1109/COMST.2015.2444095

[3] International Telecommunication Union - ITU-T Y.2060 - (06/2012) - Global information infrastructure, "Internet protocol aspects and next-generation networks - Overview of the Internet of things," www.itu.int/rec/T-REC-Y.2060/en, Accessed Feb. 2017.

[4] I. Ungurean, N. C. Gaitan, V. G. Gaitan, "A Middleware Based Architecture for the Industrial Internet of Things," KSII Transactions on Internet and Information Systems, vol. 10, no. 7, pp. 2874-2891, 2016. DOI: 10.3837/tiis.2016.07.001

[5] General Electric (GE) Breaks Out on New "Industrial Internet" Project, http://www.t3live.com/articles/market-analysis/4217-general-electric-ge-breaks-out-on-new-qindustrial-internetq-project.html

[6] J. Manyika, C. Michael, J. Bughin, R. Dobbs, P. Bisson, A. Marrs, “Disruptive technologies: Advances that will transform life, business, and the global economy” McKinsey Global Institute, May 2013

[7] J. Chambers, “Internet of Everything”, Cisco, February 21, 2013, http://www.cisco.com/assets/sol/dc/internet_of_everything.pdf

[8] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, K. S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," in IEEE Access, vol. 3, no. , pp. 678-708, 2015. doi: 10.1109/ACCESS.2015.2437951.

[9] I. Ungurean, N. C. Gaitan, "Speech analysis for medical predictions based on Cell Broadband Engine," 2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO), Bucharest, 2012, pp. 1733-1736.

[10] M. S. Shahamabadi, B. B. M. Ali, P. Varahram and A. J. Jara, "A Network Mobility Solution Based on 6LoWPAN Hospital Wireless Sensor Network (NEMO-HWSN)," 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Taichung, 2013, pp. 433-438. doi: 10.1109/IMIS.2013.157

[11] R. Ram, et al. "UniversAAL: provisioning platform for AAL services." Ambient Intelligence-Software and Applications. Springer International Publishing, 2013. 105-112.

[12] R. S. H. Istepanian, S. Hu, N. Y. Philip, and A. Sungoor, ``The potential of Internet of m-health Things `m-IoT' for non-invasive glucose level sensing,'' in Proc. IEEE Annu. Int. Conf. Eng. Med. Biol. Soc. (EMBC), Aug./Sep. 2011, pp. 5264-5266.

[13] Z. Yang, Q. Zhou, L. Lei, K. Zheng, W. Xiang, (2016). An IoT-cloud Based Wearable ECG Monitoring System for Smart Healthcare. Journal of medical systems, 40(12), 286.

[14] G. Yang et al., "A Health-IoT Platform Based on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor, and Intelligent Medicine Box," in IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2180-2191, Nov. 2014. doi: 10.1109/TII.2014.2307795

[15] E. Agu et al., "The smartphone as a medical device: Assessing enablers, benefits and challenges," 2013 IEEE International Conference on Sensing, Communications and Networking (SECON), New Orleans, LA, 2013, pp. 76-80. doi: 10.1109/SAHCN.2013.6644964

[16] M. F. A. Rasid et al., "Embedded gateway services for Internet of Things applications in ubiquitous healthcare," 2014 2nd International Conference on Information and Communication Technology (ICoICT), Bandung, 2014, pp. 145-148.doi: 10.1109/ICoICT.2014.6914055

[17] D. Metcalf, S. T. J. Milliard, M. Gomez, M. Schwartz, "Wearables and the Internet of Things for Health: Wearable, Interconnected Devices Promise More Efficient and Comprehensive Health Care," in IEEE Pulse, vol. 7, no. 5, pp. 35-39, Sept.-Oct. 2016. doi: 10.1109/MPUL.2016.2592260

[18] P. Appavoo, M. C. Chan, A. Bhojan, E. C. Chang, "Efficient and privacy-preserving access to sensor data for Internet of Things (IoT) based services," 2016 8th International Conference on Communication Systems and Networks (COMSNETS), Bangalore, 2016, pp. 1-8. doi: 10.1109/COMSNETS.2016.743994

[19] Z. J. Guan, ``Internet-of-Things human body data blood pressure collecting and transmitting device,'' Chinese Patent 202 821 362 U, Mar. 27, 2013

[20] A. J. Jara, M. A. Zamora-Izquierdo, A. F. Skarmeta, "Interconnection Framework for mHealth and Remote Monitoring Based on the Internet of Things," in IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 47-65, September 2013. doi: 10.1109/JSAC.2013.SUP.0513005

[21] D. Kwon, M. R. Hodkiewicz, J. Fan, T. Shibutani, M. G. Pecht, "IoT-Based Prognostics and Systems Health Management for Industrial Applications," in IEEE Access, vol. 4, no. , pp. 3659-3670, 2016. doi: 10.1109/ACCESS.2016.2587754

[22] OMG, DDS Security™ Specification (DDS-SECURITY™) http://www.omg.org/spec/DDS-SECURITY, (Accessed Match 2017)