Patient HealthManagement System using e-Health Monitoring Architecture

Srijani Mukherjee, Koustabh Dolui
Electronics and Communications Engineering
St. Thomas' College of Engineering and Technology
Kolkata, India
{doluikoustabh, mukherjeesrijani}@gmail.com

Soumya Kanti Datta
Mobile Communication Department,
EURECOM
Biot, France
Soumya-Kanti.Datta@eurecom.fr

***Abstract*— This paper illustrates the design and implementation of an e-health monitoring networked system. The architecture for this system is based on smart devices and wireless sensor networks for real time analysis of various parameters of patients. This system is aimed at developing a set of modules which can facilitate the diagnosis for the doctors through tele-monitoring of patients. It also facilitates continuous investigation of the patient for emergencies looked over by attendees and caregivers. A set of medical and environmental sensors are used to monitor the health as well as the surrounding of the patient. This sensor data is then relayed to the server using a smart device or a base station in close proximity. The doctors and caregivers monitor the patient in real time through the data received through the server. The medical history of each patient including medications and medical reports are stored on cloud for easy access and processing for logistics and prognosis of future complications. The architecture is so designed for monitoring a unitary patient privately at home as well as multiple patients in hospitals and public health care units. Use of smartphones to relay data over internet reduces the total cost of the system. We have also considered the privacy and security aspects of the system keeping the provision for selective authority for patients and their relatives to access the cloud storage as well as the possible threats to the system. We have also introduced a novel set of value added services through this paper which include Real Time Health Advice and Action (ReTiHA) and Parent monitoring for people with their family living abroad.**

Keywords—e-health monitoring; wireless sensor networks; smart devices; remote health advice.

I. INTRODUCTION

Wireless Sensor Network (WSN) has paved the way for advancements in various aspects of sensing. These advancements have been possible with arrival of smart sensing techniques, smaller transceiver and sensing modules as well as stronger processing units. Applications of WSNs range from military applications [1] to global climate monitoring applications [2] and from applications in underwater networks [3] to applications in structural health monitoring [4] and beyond. An important aspect of WSN has been the design of health monitoring systems centering on wearable sensor modules for patients. With the ageing population around the world, research into health monitoring application has gained prominence over the recent years. Authors of [5] mention use of microprocessor based applications to compute the data from sensors to analyze a patient. This data was transmitted over telephonic networks like the facsimile systems. Since the computational power of the devices was weak, the applications were limited to measuring simple parameters. With further research and stronger processors and communications systems multiple parameters could be monitored at once and data could be relayed over the internet [6]. It has also provided an increased sense of security to patients suffering from certain diseases.

Our paper is aimed at developing an architecture based on smart devices and wireless sensor networks to monitor health of patients in various scenarios. The patients are monitored using a portable and mobile device which accumulates and processes data from an array of wearable sensors. This data is furthermore correlated to data from sensors embedded in the surrounding environment. The accuracy of the data received and responsiveness to an impending emergency increases with the use of higher quantity of sensors or with sensors possessing stronger sensing and processing capabilities. Hence the total number of parameters to be monitored has to be designed keeping mind the balance with cost, complexity and the reliability of the system.

The proposed e-health monitoring is highly suitable for the following four scenarios. Firstly patients with unstable physiologic regulatory systems for e.g. a patient suffering from respiratory congestion as a result of drug overdose or anesthesia. The second situation for patients is those with a suspected life threatening situation, e.g. diagnosis predicting possibility of a heart attack. Thirdly are patients with a high risk of developing a life threatening condition (e.g. a baby born with an abnormality in the heart or lungs). The fourth type of patients requiring monitoring is those with a critical physiological state, for e.g. patients with a major trauma or recovering post accident. Our system is also designed for the elderly people who require regular monitoring [7] for multiple instances of the above mentioned cases. This system is aimed at facilitating accelerated diagnosis of diseases and also increased efficiency and accuracy in the process. It is also designed to instill a sense of security in the patient at all times by providing instantaneous attention for emergencies. In our architecture for the system, the smart device plays a major role in processing as well as relaying of data acting as a gateway hence reducing costs in the process. We have developed this architecture keeping in mind the prospect of this being used in rural parts of India, where health care units and hospitals are not as well equipped as their urban counterparts. In these regions, this system with mobile sensors and smart devices can be implemented for prognosis of patients.

The rest of the paper is organized as follows. The underlying framework and architecture of the system for monitoring of patients is mentioned in Section II. Section III illustrates in detail the design of this system. The privacy and security issues regarding this system are taken into consideration in Section IV along with countermeasures to these issues. Section V and VI illustrates a use case and state-of-the-art respectively. We have discussed the prospects of this system and its applications in the concluding section.

II. E-HEALTH MONITORING ARCHITECTURE

The architecture consists of three major layers which act as the backbone for our system. We have broadly categorized the architecture of our system into three layers based on the functionality of the components being used. Fig. 1 illustrates the three layers used in our architecture.

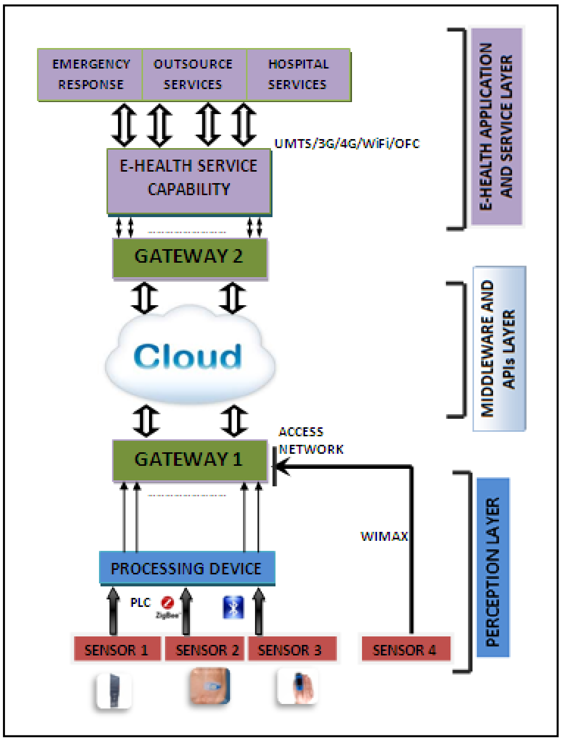

Fig. 1. Illustration of the e-Health Monitoring Architecture

A. Perception Layer

The first layer at the bottom of the hierarchy consists of various types of sensors which collect real time data. These wearable sensors are embedded in and around the environment surrounding the patient and in his/her body as well. They can be broadly classified into two types, viz. medical sensors and environmental sensors. The medical sensors monitor vital parameters of the patient whereas the environmental sensors monitor parameters of the room including room temperature, oxygen levels and beyond. The data accumulated by the sensors are relayed to a processing device which attaches several data like unit, timestamp etc. and thereby creating metadata. With that, one unique id is attached to each unit data in order to distinguish which report is for which patient. The data is sent to the next layer in the hierarchy through Gateway 1. The data is transmitted in the form of Sensor Markup Language (SenML) [8]. A sample representation of a value recorded by the sensor in SenML is given by,

{"e":[{"n":"body","v":101.3,"u":"Far", "t": 1753.36084}]};

where 101.3 denotes value of the sensor, "u" denotes the unit in Fahrenheit and "t" denotes time elapsed in seconds i.e. the timestamp and "n" denotes the type which in this case is a body temperature from the patient. The communication between the sensors and the gateway are conducted through short range communication systems including Local Area Network (LAN), ZigBee, Bluetooth or Power Line Communicator (PLC).

B. Middleware and APIs layer

This layer is the pivotal layer of the system consisting of various APIs (Application Programming Interfaces). The cloud storage stores the medical history of the patient as well as current records of the monitored parameters. This storage plays a central role in the emergency response and hospital monitoring system to correlate the data collected from the sensors to the stored thresholds for the parametric values. The cloud storage is instrumental in analyzing an emergency and declaring a state of emergency for the patient. Whenever a patient is registered in the system one API creates the profile for that patient. Another API can also be developed which would fetch the patient history for a patient who is already using the system and analyze the report. These APIs support the profile creation, storage, queries regarding patient history and other reports synchronizing with the whole system. The data from the cloud is relayed to the Gateway 2 over UMTS, optical fibers or over Wi-Fi. The data is then relayed to this layer for outsourcing applications and services from the Gateway 2 or E-Health Service Capability module.

C. E-Health Application and Service Layer

The third layer of the system is a terminal layer offering outsourcing services for the monitored data. This layer offers E-health Advice services to the patient. This process involves prescribing medicines or providing suggestions to the patient correlating to the values of parameters that are being received from the sensors. Based on the pattern of data from the previous medical records of the patient, the e-health services offer advice comparing the previous trends with the current trend of sensor data. The emergency response system plays the role of informing the doctors and the caregivers in accordance with the level of emergency. Depending on the level of emergency the response team takes required action. The hospital module monitors the patient remotely from the location of the patient, if the monitored patient is at home or a remote location. This module also allows analysis of all patients under monitoring centrally in the hospital or health care centre.

The mode of communication between layer 2 and layer 3 is duplex in nature since the data for this service is received from the cloud storage and the targeted response for the patient is relayed back to the layer 2 for storage and dissemination.

III. Functional Components of the Architecture

In this section we have discussed about the functionality of the system with emphasis on the operation of sensors, the types of parameters monitored, process of accumulation and dissemination of data. We have also taken into consideration the various services that are offered through this monitoring system in this section.

A. Sensors and Processing Units

The monitoring system is based on primarily two kinds of sensors. These sensors are medical sensors which are attached with the patient to measure vital parameters and the environmental sensors embedded in and around the various parts of the room where the patient is present. These values considered together present the real time situation of the patient at all times.

1) Medical Sensors:

These sensors are used to analyze the health of the patient by measuring various bodily parameters. The sensors in the environment as well as on the patient should be small in size and as unobtrusive to the patient as possible for acquiring natural values of the parameters. The sensors include heart rate monitor, oximeter, blood pressure sensor, ECG module, and thermometer.

These sensors produce raw values of data which are wirelessly relayed to a central transceiver unit worn by the patient. This transceiver unit processes the raw data and converts it into meaningful metadata [9]. Raw sensor data contains only values of the parameters measured hence has little value. Sensor Metadata when added to these values, viz. type of parameter being monitored, feature of interest, timestamp and unit of measurement makes these values meaningful.

2) Environmental Sensors:

These sensors monitor the surrounding of the patient and ensure that the patient is in healthy living conditions. These sensors can be embedded in particular rooms for private health care or in Intensive Care Units in health care centers and hospitals. Following describe this category of sensors.

- Gas detection sensors are used to maintain proper oxygen level.
- Temperature sensors are used to report room temperature. This can be used in a feedback mechanism to control the temperature of the room.
- The bed is equipped with a set of piezoelectric sensor to detect whether the person is in the bed. The room can also be embedded with such piezoelectric sensors to detect motion. These sensors can also be programmed with a microcontroller to detect a fall or collapse of the patient.

3) Central Transceiver Unit and Central Base Station

The Central Transceiver Unit is a wearable module and can be attached to the patient. This is designed to receive the raw data from the wearable medical sensors through multiple channels tuned to multiple frequencies. Serialized transmission of data through one channel may cause delays or collisions, thus loss in data. Hence multiple channels are used to ensure that different sensors send their values at different frequencies separated by an offset value to prevent interference. This transceiver unit then transfers the processed metadata values to a central base station in the room using wireless communication like Zigbee or Bluetooth.

The central base station gathers the values from the environmental sensors as well and then relays the data to the layer 2 as mentioned in the architecture in Section II. Hence, the Central Base Station acts as a gateway for the system between layer 1 and layer 2 of the architecture. The use of the central base station can be made cost effective and mobile if a smart device is used as the gateway being carried at all times by the patient. The metadata of sensors sent from the base station to the cloud storage is in the form of eXtensible Markup Language (XML) which facilitates sharing of SenML data. The smart device can be also used for local processing of data to analyze the health condition of the patient. The communications in this system is depicted in Fig. 2.

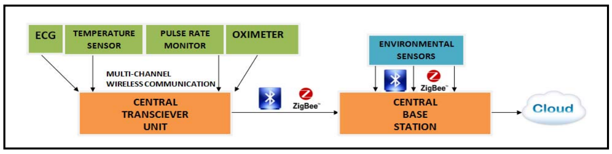

Fig. 2. Communications in Layer 1 of the Architecture

B. Services for the monitoring system

The data acquired from the sensors are stored in a central database on the cloud. This data is processed in two ways, viz. on-board processing and on device processing [10].

- On-board processing can be carried out on the central base station preferably a smart device. This allows immediate detection anomalies and care could be taken before the patient reaches healthcare institutes.
- On-server processing uses the real time metadata received from the sensors to process them with respect to data stored in the cloud itself. This type of processing requires better resources in the form of memory, throughput and processing time and hence is more suitable for on server processing than On-device processing.

Based on the processing and storage of data our system offers a set of services as follows.

1) Hospital Services

Each patient is monitored using the vital parameters from the sensors embedded on the patient as well as in the surroundings. The values are further monitored by attendees present in the health care centre premises. For any anomalies in the values both visual alarm and audible alarm are deployed. The caregivers monitor these alarms for each of the patients and attend the patient with required medication to address the situation. These services are also available to patients opting for private monitoring at their residences. In this case, a caregiver is present on the premises however the monitoring is done remotely at a hospital. If an alarm is triggered it alerts both the staff present in the hospital and the caregiver on premises as well.

2) Cloud Storage Services

In this set of services we offer a unique set of services in the form of cloud storage. The cloud storage is used to store medical histories of the patients with a particular database pertaining to each patient. These records can be used to correlate the current data received from the sensors for diagnosis. This pattern recognition process plays a pivotal role in the services mentioned subsequently.

Cloud Storage can be used to securely store (i) medical reports, (ii) medical prescriptions along with particular medicines for which the patient has showed best recovery patterns and (iii) medicines to which the patient is allergic. The preferable method of storage for these prescriptions would be in the form of XML files rather than plain text. This would allow easier parsing of data and would hence facilitate the processing on the cloud.

3) Emergency Response Services

Unlike the response from caregivers mentioned in the Hospitality Services, there are cases in which immediate attention is required from the caregivers for situations which may prove to be life threatening. There may be cases in which the threat may be beyond the scope of the caregivers and require intervention from the doctors. Fig. 3 illustrates the block diagram for the emergency response module.

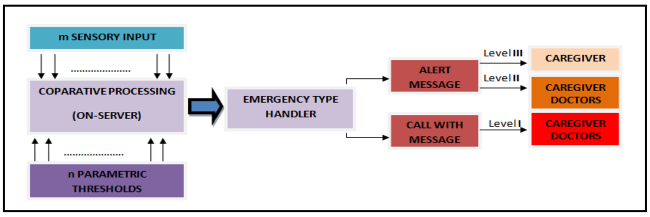

Fig. 3. Block Diagram for Emergency Response Service

The values received in real time from the sensors are sent to the cloud for storage as well as processing. The database for each patient stores abnormal values for each parameter considered. On-server processing is used to compare all these values to the thresholds in real time. The breaches in threshold values acquired from the initial stage of processing are then sent to the Emergency Type Handler. The Emergency Type Handler then applies predefined logic to determine whether the breaches are inter-related and pose a greater threat combined. Based on the kind of threat the Emergency Type Handler assigns the threat to one of three levels.

- For Level III emergency, a message/alarm is sent with vital parameters and threshold breaches only to the caregivers.
- For a Level II emergency, a message/alarm is sent in a similar manner but to both the patient's doctors and caregivers.
- For a Level I Emergency or emergency with the maximum threat, the system sends a call with a recorded message of the threat and breached parameters to both doctors and caregivers.

Based on these alerts the patient is immediately attended by the doctors or the caregivers in an attempt to bring the patient back to a normal state with required treatment and medications.

4) Real Time Health Advice and Action (ReTiHA)

This service is designed to operate when the Emergency Response System fails to arrive or the patient is unattended even though a level I emergency is disseminated. If the monitoring system in the On-Server processing determines further deterioration of the patient as a result of further breaches in thresholds, this service is triggered.

In this service the On-Server program executes a pattern recognition program to determine whether such an emergency has been reported earlier in the records. If such a pattern is found matching the current pattern of parameters, the on-Server program checks with the prescribed history as to which medicine was applied to cure the patient in such a situation. If such a suitable medication is found, the On-server program suggests the medication to the patient through the central reporting system. The medication can then be applied by a relative present in the bedside or by the care giver. This is particularly useful and applicable to patients with a chronic disease requiring similar yet vital medications on emergency and for patients on private monitoring where emergency response might be delayed.

5) Parent Monitoring Services:

With the ageing population worldwide and opportunities to work abroad, it is a common situation in which the parents stay away from their working off-springs. In cases of sudden health disorders and medical emergencies the off-springs are often deprived of the information regarding the emergency due to a delay in communication. To bridge this gap between working professionals and their parents we have designed this service.

This is designed as a value-added service in which the off-springs receive continuous updates of the vital parameters of their parents and are updated on the emergencies through alerts similar to that of a caregiver. To implement this service we can send these updates through a smart phone application. This smart device application will be equipped with an API which can received updates from Layer 2 of the architecture. For e.g. the date and time for the next appointment with the doctor or change in prescribed medicines can be relayed through this application. The location of the parent can be also monitored by using a wearable GPS device or by localizing the parent using beacon nodes [11].

IV. SECURITY AND PRIVACY

In this section we have discussed about the various security threats to this e-health monitoring system. As the system is concerned with the condition of human health and prescriptions are made online by the doctor, we need to consider rigid security measures.

This is required in order to secure the patient's health and to assure whether the patient is receiving proper medical guidance. If the patient's profile is compromised or a prescription is uploaded by any unauthorized person other than the doctor, this can have a deleterious effect on the patient. Hence the following aspects of end-to-end security are to be considered to ensure that there are no loopholes in the security of the system.

A. Confidentiality

It is a necessity to keep the health record of the patient confidential such that the privacy of the patient is ensured. While the health record is sent and received between the doctor and the patient, no other person can be allowed to eavesdrop on this exchange in an unauthorized manner. In our architecture, we have kept a provision for some trusted people (family members) to access the patient profile. The system allows these trusted people to access the database with a private key shared and approved by the patient. The data can be processed using 8-bit or 16-bit microprocessor, after which RSA-256 is used to secure all data. The timestamp ensure the freshness of the data. These data are sent to the cloud from devices through HTTPS connection to obviate any kind of security threats regarding confidentiality.

B. Integrity

Integrity assures accuracy of data throughout the process. The data should never be made available to an unauthorized person as he/she may tamper the data, leaving the patient vulnerable to wrong diagnosis. Secure hash algorithm (SHA-1 or the latest version of it) is used in this system to ensure message integrity. The timestamp is also checked to know the freshness of the data. If the data is not fresh it has to be discarded as the condition of health of a patient may change within a second.

C. Authenticity

The identity of both the doctor and patient requires validation in order to ensure authenticity of the system. In this case digital signatures can be used as a symbol of validation through which we can assure that the person is real and is truly who he/she is claiming to be. Digital Signature is one of the most trusted processes of ensuring authenticity in this case.

D. Non Repudiation

Often we come across some incidents of medical negligence in hospitals and clinics. Non Repudiation is one of those principles of the security system which ensures integrity and authenticity of data. If a message is sent, the sender cannot deny that he/she has sent the data. Similarly the receiver cannot deny the fact that the data has been received. In our system non repudiation is necessary to ensure that the doctor himself/herself is receiving the medical data and not getting it done by someone else. If non repudiation is assured the doctor should always be responsible for each of his responses through the system. The digital signature will ensure the doctor receives the data and takes action accordingly as the permission of writing prescription will be for the doctor only.

V. USE CASES

In this section, we have discussed a few of the real life applications of our system. There are many real life scenarios, where the system can prove to be efficient and useful. We have mentioned two of such cases and the system's function in the same.

A. Doctor Finder

This architecture can support storage of regional databases from which the information about a patient can be fetched based on his/her location. The details about the availability of doctors in that area will be stored in the database. It will contain all details like doctor's name, field of specialization, address of the clinic, timings of appointments, fee of the doctor and availability of appointment. The database has to be updated regularly, so that, whenever the patient feels unwell, he/she can have an appointment through the system, choosing preferred doctor from the suggested list of doctors by the system. This will help a patient to go to nearby doctors for emergency and minor check up instead of going to the hospital.

A patient can use a smart phone application which connects to the database with location information and category of doctor needed by a patient. The system can give the patients the details about the available doctors in that particular locality.

B. Location information for Emergency Response Team

A smart phone can also report the location of the patient to the Emergency Response Team (ERT). This is helpful for people having trouble with their health while not being at home. Even when there is no one to help the patient, the mobile application will send every necessary piece of information as well as the current location of the patient to the ERT which is nearby to the patient according to the information from the database. This will trigger the ERT to come and take action as soon as possible.

VI. RELATED WORK

Health Care Systems have vastly improved over the recent past with the introduction of devices compatible with digital signal processing; better image processing techniques, introduction of MEMS based sensors facilitating diagnosis of various diseases. With the advent of better health care technologies research on monitoring systems have been extensive in the past few years. Various publications on this research area are based on different aspects of health monitoring including data collection from sensors, data dissemination methods and protocols, processing of sensor data as well as security and privacy of these systems. The research can also be classified according to the nature of application whether in a private scenario, for elderly patients or for monitoring in a health care centre. These proposed methods and their implementations have facilitated health care systems in multiple aspects in more ways than one.

Existing literature [12] has mentioned monitoring systems based on Wireless Sensor Networks with unobtrusive sensors embedded on the patient who does not restrict his activities and body movements. The architecture used is multi-tiered with ad-hoc self managing sensors to reduce operational costs. A.Triantafyllidis et al [13] mentions use of reconfigurable and decentralized sensors for monitoring which will henceforth allow easy addition and deletion of sensors for new patients to the system. The authors of [14] have proposed a whole architecture for collection and dissemination of medical sensor data based on SNMP and Code Blue Agents. Hairong Yan et al [15] takes into consideration the localization of the patient using Received Signal Strength Indicator (RSSI) with respect to beacon nodes whose positions are fixed and predefined. The use of video to monitor the patient in addition to the existing architecture is mentioned in literature [16]. The video is triggered when values of sensors breach a certain given threshold. Wan-Young Chung et al. [17] puts forward the idea of using a mobile device in the communication layer to receive data from the sensor networks when the threshold is reached. The mobile device is used to perform minor computations and relay the data to the management layer. An Android device used to analyze ECG signals from a mobile monitoring terminal is also mentioned in existing literature [18].

Marıa de los Angeles Cosio Leon, in her paper [19] studies the privacy and security issues of privacy and security in a WSN based monitoring system. The paper considers the privacy aspect of when recording from the microphone or capturing video is to be considered inappropriate and when it is necessary by defining a filter for the same. This paper also considers active and passive attacks to the system along with key management schemes to ensure safe end to end communications.

VII. CONCLUSION

Even though a lot of research has been conducted on e-health monitoring systems, we have proposed a set of novel services based on the monitoring system. ReTiHA will require immense research and testing before implementation, however it paves a new path for remote health monitoring systems. We have also proposed other novel services in the form of Parent Monitoring system and the Emergency Response Services. The use of SenML in our system ensures organized transmission of sensor metadata. The medical data and history acquired for the patients are personal in nature. Hence our system ensures security of the highest order for the medical data on cloud storage. With further research in this aspect, our system can change the way we currently look at remote health monitoring services.

REFERENCES

[1] Michael Winkler, Michael Street, Klaus-Dieter Tuchs, Konrad Wrona, “Wireless Sensor Networks for Military Purposes” in Autonomous Sensor Networks Springer Series on Chemical Sensors and Biosensors Volume 13, 2013, pp 365-394

[2] Pahuja Roop, Verma H.K. ,Uddin Moin, "A Wireless Sensor Network for Greenhouse Climate Control", Pervasive Computing, IEEE (Volume:12 , Issue: 2), April-June 2013, pp: 49 - 58

[3] Ali Mansour, Isabelle Leblond, Denis Hamad, Felipe Artigas, "Sensor Networks for Underwater Ecosystem Monitoring & Port Surveillance Systems", Sensor Networks for Sustainable Development, M. Illias (Ed.) (2013) 1-25

[4] M. Reyer, S. Hurlebaus, John Mander, Osman E. Ozbulut, "Design of a Wireless Sensor Network for Structural Health Monitoring of Bridges", Wireless Sensor Networks and Ecological Monitoring, Smart Sensors, Measurement and Instrumentation Volume 3, 2013, pp 195-216

[5] S.J. Brown, "Modular Microprocessor Based Health Monitoring System", United States Patent, Patent Number 5,899,855, May 4, 1999

[6] Jovanov E, Raskovic D, Price J, Chapman J, Moore A, Krishnamurthy A, "Patient monitoring using personal area networks of wireless intelligent sensors", Biomed Sci Instrum. 2001;37:373-8.

[7] Hongwei Huo,Youzhi Xu, Hairong Yan, Mubeen S., "An Elderly Health Care System Using Wireless Sensor Networks at Home", Third International Conference on Sensor Technologies and Applications, 2009. SENSORCOMM '09, 18-23 June 2009, pp:158 – 163

[8] Jennings, Cullen, Jari Arkko, and Zach Shelby. "Media Types for Sensor Markup Language (SENML)." (2012).

[9] Jean-Paul Calbimonte, Zhixian Yan, Hoyoung Jeung, Oscar Corcho, Karl Aberer, "Deriving Semantic Sensor Metadata from Raw Measurements", 5th International Workshop on Semantic Sensor Networks. Boston

[10] Dolui, Koustabh, Srijani Mukherjee, and Soumya Kanti Datta. "Smart Device Sensing Architectures and Applications.", 17th IEEE International Computer Science and Engineering Conference, September 2013

[11] Sichitiu, Mihail L., and Vaidyanathan Ramadurai. "Localization of wireless sensor networks with a mobile beacon." In Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference on, pp. 174-183. IEEE, 2004.

[12] Virone, G., A. Wood, L. Selavo, Q. Cao, L. Fang, T. Doan, Z. He, and J. Stankovic. "An advanced wireless sensor network for health monitoring." In Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare (D2H2), pp. 2-4. 2006.

[13] Triantafyllidis, A., V. Koutkias, I. Chouvarda, and N. Maglaveras. "An open and reconfigurable wireless sensor network for pervasive health monitoring." In Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on, pp. 112-115. IEEE, 2008.

[14] Elaine Lawrence, Karla Felix Navarro, Doan Hoang, Yen Yang Lim, "Data Collection, Correlation and Dissemination of Medical Sensor Information in a WSN", Fifth International Conference on Networking and Services, 2009. ICNS '09, pp: 402 - 408

[15] Hairong Yan, Youzhi Xu, Gidlund, M. "Experimental e-Health Applications in Wireless Sensor Networks",WRI International Conference on Communications and Mobile Computing, 2009. CMC '09, (Volume:1), 6-8 Jan. 2009, pp: 563 – 567

[16] M. Fischer, Yen Yang Lim, E. Lawrence, L.K Ganguli, "ReMoteCare: Health Monitoring with Streaming Video", Mobile Business,7th International Conference on 2008. ICMB '08, 7-8 July 2008, pp: 280 - 286

[17] Wan-Young Chung, Seung-Chul Lee, Sing-Hui Toh, "WSN based mobile u-healthcare system with ECG, blood pressure measurement function",30th Annual International Conference of the IEEE, Engineering in Medicine and Biology Society, 2008. EMBS 2008, 20-25 Aug. 2008, pp: 1533 – 1536

[18] Pei-Cheng Hii, Wan-Young Chung, "A Comprehensive Ubiquitous Healthcare Solution on an Android™ Mobile Device", Sensors 2011, 11, 6799-6815; doi:10.3390/s110706799

[19] Marıa de los Angeles Cosio Leon, Juan Ivan Nieto Hipolito, Jesus Luna Garcıa, "A Security and Privacy Survey for WSN in e-Health Applications", Electronics, Robotics and Automotive Mechanics Conference CERMA '09, 22-25 Sept. 2009, pp: 125 – 130.