Securing e-healthcare applications with PPS and PDS

Archana Tayal and Prachi
CSE and IT Department
ITM University
Gurgaon, India
tayal.archi@gmail.com, prachi@itmindia.edu

***Abstract*—Instead of being measured face to face, e-healthcare is a new promising technology that facilitates monitoring patients health related parameter continuously and in real time, with the help of wireless sensor network. Wireless Body Sensor Network (WBSN) reduces heavy dependence on specialized healthcare staff and thus a desirable technique for countries that lack sufficient medical infrastructure and trained staff. However, layout and design of wireless body sensor network without security can influence the system. In this paper we review existing WBSNs and introducing a new approach for Proxy Patient Server (PPS) and a Proxy doctor Server (PDS) to improve e-healthcare services.**

Keywords- WBSN, PPS, PDS, healthcare, security, hospital.

I. INTRODUCTION

The Hospitals are health care institution providing medical, surgical treatment with nursing care in a hygienic aseptic environment and in the invigilation of a specialist. They facilitate easy diagnose in a short period of time, are equipped with specialist team as well as trained staff, who take care of patients, and accelerate the treatment. Dietician, physiotherapist and pharmacist are altogether available and one can consult them indolently.

But, in spite of latest medical infrastructure available, people are deprived of health care services because of several reasons like unwillingness, aging, lack of awareness, hospital environment and many other reasons. A person visits hospital only when there are clear symptoms. Regular health checkups are inconvenient for elder people.

Long term patients feel isolated in hospital due to the fix visiting hours with maximum 2 persons and thus have a bounded communication which in return results in depression. WBSN a hospital from home is bless for people which will save them from the hazards of visiting hospital frequently. It combines the services of hospitals with the comfort of home. A WBSN is a good alternative for the patients not willing to stay in hospitals.

From a survey it has been found that every year because of human error approximately 98,000 people die [9]. So with WBSN a log of previous errors can be maintained. We all know that hospitals are not a desirable place for elderly patients [1]. According to [2], 14 % patient died within 90 days and 39 % died within 2 years.

According to the World Health Organization (WHO) elderly patients are becoming troublesome and their bed-bound (torpid) lifestyle is further adding to the problems of gastrointestinal, muscular atrophy and imbalance of nutrition [10], [11]. This in turn will further create complications that will lead to deterioration in service quality. Lots of staff is required in the hospitals, which adds to expenses, but with WBSN less staff can be employed for monitoring more patients at a time which ultimately helps in reduction of costs and assure quality services.

A wireless body sensor network is composed of economical, feathery mini motes that are capable to feel, think and talk. These sensor nodes are densely deployed for measuring a specific environment. With the growth in technologies different kind of sensors (motes) have been developed and are widely accepted as well as implemented. WBSN kit incorporates different kind of sensors, processors, transceivers, battery. Motes are worn by patients, they feel vital signs, think and process them and communicate it to hospitals database. WBSN beforehand detects the anomalous signals in order to initiate preventive measures in real time. Rapid growth in the use of WSN has made the developers to design light-weight, inexpensive sensors that can be implemented in the diverse applications of WSN. Various types of commercial sensors including dust, temperature, pulse, light, humidity sensors are available in market for a variety of applications. Sensors best suited to the healthcare kind of application are motion detector sensors like SpO2, ECG, EEG, EMG, and pulse-oximeter because in this type of application, we require to detect movements of patient which varies with the mobility involved in routine activities. SpO2 sensor measures relative amount of oxygen to the hemoglobin present in the blood. ECG sensor measures the rate and regularity of heartbeats. EMG sensor records the electrical activity of skeletal muscles. EEG sensor is used to measure the voltage fluctuations resulting from ionic current flows within the neurons of the brain [8]. These motion detector motes are used to sense patient's body parameters like oxygen saturation, blood pressure, electrocardiography (ECG), electromyography (EMG), and electroencephalography (EEG) in real time.

This paper presents a survey of existing WBSN projects in Section II. In Section III we review the threats and challenges faced by WBSN. Section IV discusses the existing WBSN architectures. We propose our new architecture with Proxy Patient Server and Proxy Doctor Server in section V. We conclude in section VI with the future work to be done.

II. PROJECTS

In the past few years many projects on wireless body sensor networks have been proposed and developed. We briefly discuss some popular WBSN projects of e-healthcare.

The first WBSN application developed for pre-hospital care, in hospital care and emergency response was

978-0-7695-4941-5/13 $26.00 © 2013 IEEE
DOI 10.1109/ACCT.2013.20

Codeblue [6]. Codeblue was designed to monitor patient's blood oxygen saturation, heart rate, ECG [5]. It relies on tiny wearable sensors that monitor patient vital activities in real time and transmit the gathered data either to local medical database having medical records or direct to doctor's mobile device or PDA's. Codeblue provides protocols for device discovery and publish/subscribe multi hop routing, as well as a simple query interface that is tailored for medical monitoring with the help of Mote Track location system [7], [15].

SMART a Scalable Medical Alert and Response Technology system was introduced by Dorothy Curtis et. Al. for the overloaded emergency ward of hospitals. Because of the rush in emergency ward a patient with more dreadful condition may have to wait which would further worsen the situation. To forestall such situation and rank the patients in order of necessity, SMART measured the SpO2 and ECG of the emergency ward's patients [18]. This is done by keeping a track of locations of patients, doctors and belongings [19].

A. Wood et. Al. comes up with idea of ALARM-NET, another WBSN contrived for assisted-living and residential monitoring. In ALARM-NET physiological and environmental sensors are blended in a scalable divergent architecture to monitor patient's data at their residence. Circadian Activity Rhythm (CAR) is integrated in ALARM-NET for analysis of patients' paradigm of their day to day activity [12].Star gateway is the major component of ALARM-NET for handling the security affairs of password protocols, authentication, and communication [5].

Aid-N is furtherance in WBSN with the use of electronic tags used for prioritizing the patients who needs attention first. Aid-N has special ultralow power enclosed hardware. These electronic triage tags use non-invasive, biomedical sensors (pulse oximeter, electrocardiogram, and blood pressure cuff) to continuously monitor the vital signs of a patient [17]. Like previously developed projects, Aid-N not only automatically monitor patient's health related parameters continuously and in real time but also fulfill the requirement of triage system. It uses wireless ad-hoc network and web portals for the transfer of data [20].

Carenet is a wireless sensor network developed for remote healthcare service. As proposed by Shanshan Jiang et. Al. in [21] Carenet is constructed on a heterogeneous network, multilayered software infrastructure. Heterogeneous network inculpate data collection, transmission, and access phases. TinyOS operating system and NesC was used as a programming language in the multilayered software of Carenet. Its architecture is two-tired and uses TCP sockets to implement routing protocol. Carenet is highly reliable, scalable and extendable. It supports privacy, data confidentiality, data protection.

A Mobile is comfortable to carry wherever you go. The LiveNet system combines the service of wireless sensor network with mobile technology. The system was based on the Zaurus SL-5500, a Linux-based PDA mobile device [3]. It supports real-time data analysis with peer-to-peer wireless networking. Full-duplex audio channels were used for communication.

A mobile is the chief constituent of The Mobile U Health Service System (The MUSS). All the functions of data capture or transfer is done via mobile [13]. The-MUSS supports reusability as the current data gathered by mobile is continuously send to the database saving from unnecessary wastage of memory. Web Vine BPMS is used to build THE-MUSS. Communications between a cellular phone and server is done using common techniques like CDMA or wireless LAN.

III. CHALLENGES

The patient's data accumulated by sensor nodes of WBSN is most important for diagnosis and treatment as any mishandling or malicious modification of data may deprive a patient from correct treatment or even lead to an ill-advised treatment, there by endangering his life. Intruder may amend the data; replay the previous data or any other attack that threats to data security will directly affect the patient's health resulting into unacceptable results. Security is the big issue a WBSN needs to focus. WBSN without security will become curse instead of becoming a boom to healthcare. WBSN is to promote patient's health and in the absence of appropriate security mechanism it cannot survive.

So in order to secure data against various internal and external attacks from eavesdropper we need to address the following challenges.

A. Confidentiality

The communication between the patient and doctor is a privileged communication and legally no third party is allowed to interfere. The data stored must be kept confidential from the attacks of attacker to save data from amendments. A third party may made amendments in the treatment that is given to the patient, and due to these amendments, a patient's health may start deteriorating. So it is highly inevitable to keep patient's body parameters and given confidential treatment.

B. A uthenticity

To ensure that only authorized person is allowed to access the data and preventing it from revealing it to malicious person. A person who is not associated in the treatment of patient is unauthorized. Doctor, nurses, hospital staff are the authorized persons those are allowed to retrieve or access patient's data where as only concerned doctor is allowed to make modification in the treatment. Also the sender of the patient related data must be authenticated so that redundant data is not sent. Redundant data may be harmful or may put patient's health in danger.

C. Masquerading

Masquerader may wear a mask of an authority and misguide the network, thus preventing the information to be sent to actual authority and himself start sending falsie response threatening patient's life.

D. Integrity

Integrity refers to the truthfulness of data. In WBSN integrity must be secured to avoid hypocrisy. Patient's hypocrite data may make hospital authorities to give inappropriate treatment to patient therefore creating encumbrance to patient's health.

E. Denial of service

Adversary couldn't affect the encrypted data but determining the location and identity of host, traffic might

be created to slowdown the network resulting in a kind of Denial of service that is not able to transfer or receive the patient's update. Both sender and receiver are not aware of traffic willingly created by adversary.

F. Freshness

Sensors embedded on patient's body gather vital signs of patient in real time and continuously. Data received by hospitals authorities may not be as fresh as presumed. Eavesdropper may replay the former data creating hindrances in case of emergency. Hospital authorities will continue receiving former data and necessary action will not be taken at the time of need that may take the patient to death-bed.

IV. ARCHITECTURES

Many authors have proposed different architectures for WBSN. Usually it is comprised of infrared sensors, database server, doctor's PDA, transmission channel. For monitoring the patient's body parameters these sensors are embedded into patient's clothes [14]. With the help of routing protocols, data is transferred over the internet and delivered to the hospital authorities. We have briefly discussed the design of WBSN architectures proposed.

As described by Ming Li et. al. in [4] the general architecture of WBSN consists of 3 tiers. Tier 1 composed of patient, his bed, home surrounding environment. Sensor nodes implied on patient monitors patient health parameters like SpO2, ECG, blood pressure etc. and environment sensors measures the temperature, humidity of surroundings. It has raw data generated by wearable sensor nodes. Energy efficient Medium Access Protocols (MAC) is proposed in tier 2 to provide communication over multihop base stations. To support scalability, adaptability, and avoid collision, carrier sense multiple access/collision avoidance (CSMA/CA) technique is adopted. Hospital's central database, doctor's PDA or mobile devices comprises tier 3. Centralized healthcare database is maintained for permanent records. Doctor has continuous update of patients on his device as shown in Fig. 1. Architecture proposed here didn't have any security mechanism, and thus lacked to secure the patient data. Data was vulnerable to various types of attacks as discussed in previous section.

To develop bridge among WBSN and the transmission channel, gateway was interpolated by Hairong Yan et. al. Gateway receives the data from base station and treasures them in database and forwards data to the internet [15]. The proposed gateway was acting as an intermediate only. So it was not capable of detecting of emergency situations. To resolve this issue a smart gateway was proposed in [16] by Yaoming Chen et al. for tracking patient's status of past as well as present. The purpose of this smart gateway was to generate emergency alert and informing the database server and doctor in case of hardship. It provided fast responses at low cost and consuming less power but lacked to offer tips, first aid and advices.

To meet this requirement Deena M. Barakah et Al in [9] came up with a new idea of virtual doctor server (VDS). VDS was capable of managing patient's history, medicines, and remind patient to have medicine on time. It presented advices to caretaker, what first aid steps to be taken if patient is unconscious.

All the aforementioned architectures maintain a single database about patient's records. However, to retrieve record of a single patient activities from huge database become cumbersome task. To rectify this issue, in next section we propose a new architecture which is able to retrieve patient records efficiently.

V. PROPOSED ARCHITECTURE

We extend the idea of general architecture presented by Ming Li et. al. in [4] by introducing Proxy Patient Server (PPS) in tier1 and Proxy Doctor Server (PDS) in tier 3 as shown in Fig. 2 in order to provide security which general architecture lacked. The purpose of PPS and PDS is to make the system more secure and keep a track of communication made by patients and hospital separately. With the help of PPS and PDS separate log of data will be maintained to reduce errors on both sides.

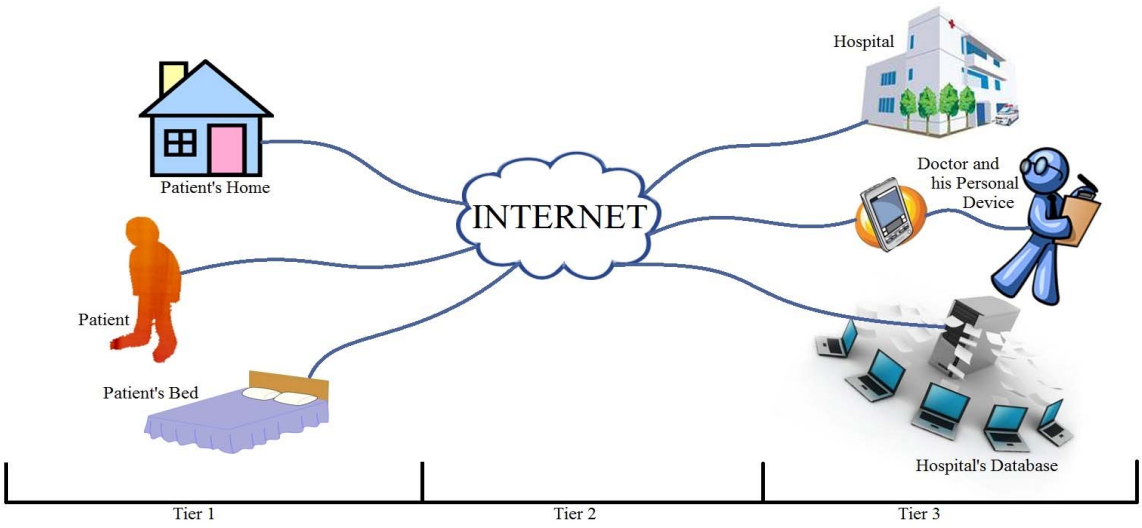

Figure1. General Architecture of WBSN

PPS act as local representative of patient's side to keep track of patient's data and its communication with hospital authorities including concerned doctor, hospital and ambulance. With separate data server of individual patient, it will be tranquil to look after patient's activities. Hospital's database has records of all the patients, looking for an individual patient's record is too time consuming.

With PPS it will be helpful to know what kind of treatment is given earlier and if some changes are required then the amendment can be done quickly, hence saving time to look into hospital's database. Also it can be inferred from previous log, about the salts (tablets) patients is allergic to. A separate server will be capable of identifying any unauthorized access and thus preventing eavesdropping of data.

PPS will also serve the purpose of creating a communication with hospital as sensor nodes embedded on the patient will invoke the PPS and PPS will then transfer the data to PDS over internet. Hence PPS will be responsible for the data transmission.

PDS will be local representative of doctor's side. Like PPS, PDS will maintain the log of hospital's activity; it's communication with all its patients, treatment given to patients etc. The log will maintain the information about what kind of reactions were there for a particular diagnose. Also it will keep a track of treatments that accelerated the patient's health. This log of information will be helpful to choose the treatment to be given to new patients.

PDS will be responsible for transferring doctor's response to PPS and it will ensure that transfer is done to the required PPS. Sending data to wrong patient may endanger the life of two patients, the one who didn't get the response in time and the one who got maleficent response because treatment was not meant for him. So it is necessary to ensure that doctor's response is sent to right patient and PDS will serve this. Benefits of PPS and PDS are listed in Table 1.

Table 1. Benefit of PPS & PDS

Patient activity monitor	PPS manages track of each and every activity performed by patient.
Marshalling	Securing patient's private data by means of encryption before its transfer.
Demarshalling	In order to get patients original data from the encrypted text, receiver demarshalls the data.
Secure data transfer	Marshalling and demarshalling provides secure data transfer over the internet.
Consistency	PPS and PDS must have consistent data in their database to detect anomaly attack.
Error reduction	Log maintained by the PPS and PDS helps in minimizing future errors.

Having data at both sides will keep a check that correct data resides in data server. In case an intruder attempts to modify data then he requires modifying patient as well as doctor's data, mismatch data at two can be detected easily. Besides all the above functions, PPS and PDS also provide secure data communication by means of marshalling (Marshalling is the method of converting unsecured data to secure data which is egress to anomaly) and demarshalling (demarshalling is to get original data from the secured data). PPS/PDS marshalls/demarshalls the data by applying encryption/decryption techniques before/after the transmission.

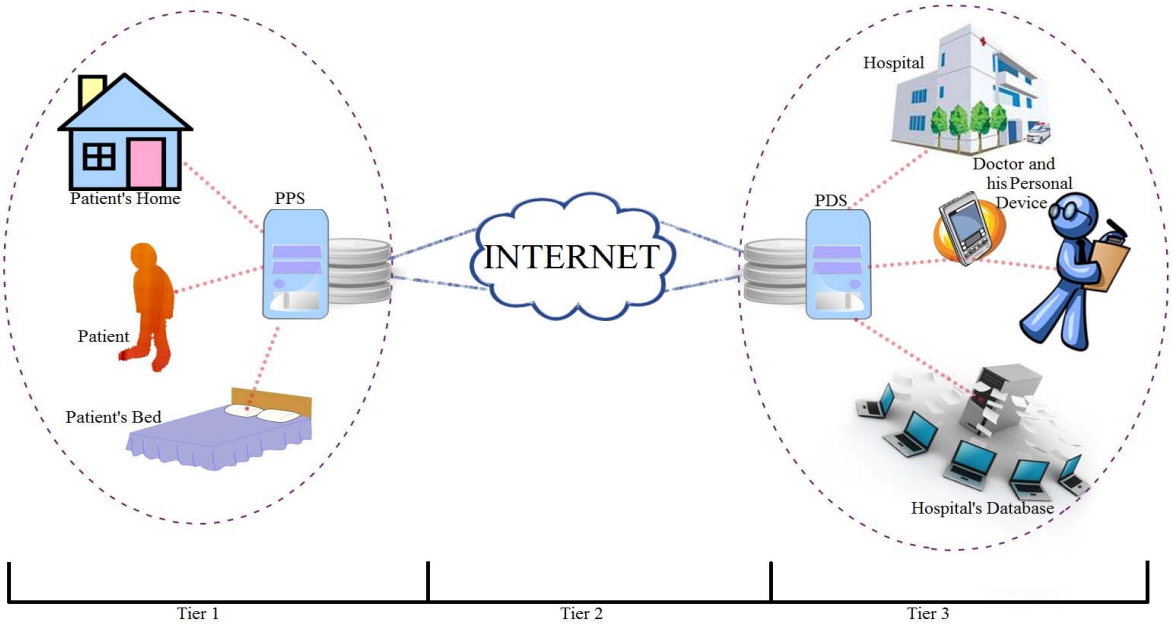

Figure2. Proposed Architecture with PPS & PDS

Communication model between patient and hospital comprises of following 3steps:

- Sensor nodes embedded on patient's body will collect patient's data and call PPS.
- PPS will marshall the patient's body parameters with some effective encryption approach of sensitive information and thus establish a secure communication channel for data transfer to PDS.
- PDS will unmarshall the information received from authenticated PPS and deliver it to Doctor.

VI. Conclusion And Future Work

In this paper we reviewed different WBSN architectures implemented and introduced the concept of PPS & PDS for the safe transmission of data as well as keeping a backup of both patient's and doctor's side to maintain the log so that learning can be done from previous errors.

With the proposed approach, WBSN will be more secure. The amendments introduced by anomaly could be detected easily as both data server must have same data and data security can be recovered. Also secure data will be transmitted, if anomaly somehow gains access to data he will not be able to interpret it as it will be encrypted by effective cryptosystem. The proposed approach will be beneficial to minimize previous errors. In the existing architectures, there's no log mechanism on patient side, to infer any information about patient. It is time consuming to search into hospital's database of multiple patients. With PPS information could be retrieved in no time.

We also presented the projects so far developed for WBSN and the threats they are facing with data security and authenticity. Next we will be focusing how we can make WBSN more secure and safe from intruder

References

[1] Cassel, C.K. 2004. Geriatrics: A Vital Core of Hospital Medicine. In Caring for the Hospitalized Elderly: Current Best Practice and New Horizons. A special supplement to The Hospitalist, 2-3.

[2] Inouye, S.K., Peduzzi, P.N., Robison, J.T., Hughes, J.S., Horwitz, R.I. and Concato, J. 1998. Importance of functional measures in predicting mortality among older hospitalized patients. In JAMA 279(15), 1187-1193.

[3] Sung, M. and Pentland, A. 2004. LiveNet: Health and Lifestyle Networking Through Distributed Mobile Devices. Technical Report. MIT Media Laboratory.

[4] Li, M., Lou, W., and Ren, K. 2010. Data Security and Privacy in wireless Body Area Networks. In Wireless Communications, IEEE, 17(1), 51-58.

[5] Kanjee, M.R., Devi, K. and Liu, H. 2010. A Two-Tiered Authentication and Encryption Scheme in Secure Healthcare Sensor Networks. In Proceedings of the Sixth International Conference on Information Assurance and Security (Atlanta, GA, August 23 - 25, 2010), IEEE, 271-276.

[6] Welsh, M. 2005. CodeBlue: A Wireless Sensor Network for Medical Care and Disaster Response. Technical Report. Division of Engineering and Applied Science, Harvard University.

[7] Shnayder, V., Chen, B., Lorincz, K., Jones, T.R.F.F. and Welsh, M. 2005. Sensor Networks for Medical Care. Technical Report. Division of Engineering and Applied Science, Harvard University.

[8] Arafat, M.I. Brain–Computer Interface: Past, Present & Future. Technical Report. Department of Computer Science and Engineering, International Islamic University Chittagong (IIUC).

[9] Barakah, D. M. and Ammaduddin, M. 2012. A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of A Virtual Doctor Server in Existing Architecture. In Proceedings of the third International Conference on Intelligent Systems Modelling and Simulation (Kota Kinabalu, February 8-10, 2012), IEEE, 214-219.

[10] Patel, M., and Wang, J. 2010. Applications, challenges, and prospective in emerging body area networking technologies. In Wireless Communication, IEEE, 17(1), 80-88.

[11] Chen, M., Gonzalez, S., Vasilakos, A., Cao, H. and Leung, V. C. 2011. Body Area Networks: A Survey. In Journal Mobile Networks and Applications, 16(2), 171-193.

[12] Wood, A., Virone, G., Doan, T., Cao, Q., Selavo, L., Wu, Y., Fang, L., He, Z., Lin, S. and Stankovic, J. 2006. ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring. Technical Report. Department of Computer Science, University of Virginia.

[13] Han, D., Lee, M. and Park, S. 2010. THE-MUSS: Mobile u-health service system. In Journal Computer Methods and Programs in Biomedicine, 97(2), 178-188.

[14] Zhou, G., Wu, Y., Yan, T., He, T., Huang, C., Stankovic, J. A. and Abdelzaher, T. F. 2010. A Multifrequency MAC Specially Designed for Wireless Sensor Network Applications. In Journal ACM Transactions on Embedded Computing Systems, 9(4), 39.

[15] Yan, H., Xu, Y. and Gidlund, M. 2009. Experimental e-Health Applications in Wireless Sensor Networks. In P roceedings of the 2009 WRI International Conference on Communications and Mobile Computing - Volume 01(Yunnan, January 6-8, 2009), IEEE Computer Society Washington, DC, USA, 563-567.

[16] Chen, Y., Shen, W., Huo, H. and Xu, Y. 2010. A Smart Gateway for Health Care System Using Wireless Sensor Network. In Fourth International Conference on Sensor Technologies and Applications (Venice, July 18-25, 2010), IEEE Computer Society Washington, DC, USA, 545-550.

[17] Gao, T., Massey, T. , Selavo, L., Crawford, D., Chen , B., Lorincz, K., Shnayder, V., Hauenstein, L., Dabiri, F., Jeng, J., Chanmugam, A., White, D., Sarrafzadeh, M. and Welsh, M. 2007. The Advanced Health and Disaster Aid Network: A Light-Weight Wireless Medical System for Triage. In Biomedical Circuits and Systems, IEEE 1(3), 203-216.

[18] Curtis, D., Shih, E., Waterman, J., Guttag, J., Bailey, J., Stair, T., Greenes, R. A. and Machado, L. O. 2008. Physiological Signal Monitoring in the Waiting Areas of an Emergency Room. In Proceedings of the ICST 3rd international conference on Body area network, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) ICST, Brussels, Belgium, Belgium.

[19] Curtis, D., Stair, T., Guttag, J., Greenes, R. A. and Machado, L. O. Scalable Alert Medical Response Technology Summary Report. NLM Scalable Information Infrastructure Program.

[20] Welcome to the Advanced Health and Disaster Aid Network. DOI = http://www.jhuapl.edu/aid-n/ .

[21] Jiang, S., Cao, Y., Iyengar, S., Kuryloski, P., Jafari, R., Xue, Y., Bajcsy,R. and Wicker, S. 2008. CareNet: An Integrated Wireless Sensor Networking Environment for Remote Healthcare. In Proceedings of the ICST 3rd international conference on Body area network, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) ICST, Brussels, Belgium, Belgium.