Middle-East Journal of Scientific Research 23 (12): 2961-2967, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.12.101171

Structural Design of Secure Transmission Module for Protecting Patient Data in Cloud-Based Healthcare Environment

Mohamed Doheir, Burairah Hussin, Abd Samad Hasan Basari and Malik B. Alazzam

Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka, Melaka 76100, Malaysia

Abstract: Nowadays, the tradition healthcare system becomes inefficient as there are a lot of people who have long-lasting diseases that require continuous medical care and treatment. Cloud computing brings substantial benefits to the healthcare domain including hospitals, medical centers and health clinics that necessitate fast access to some facilities for computing and storage which are not usually available in the traditional sites. Furthermore, healthcare data should to be shared across several locations that may burden the healthcare organization and the patient causing major delay in treatment and time wastage. Cloud satisfy such requirements by furnishing the healthcare providers an unbelievable opportunity to enhance the services provided to their customers, patients and also for sharing information effectively and improving operational efficiency as well. However, cloud computing is associated with security concerns. The present cloud-based healthcare systems lack of efficient management of medical data and unreliability of end-system communication to the cloud databases. Therefore, with the growth of the demand on healthcare and the availability of new technologies, a secure and reliable communication unit along with an efficient cloud service-based healthcare system is highly required. This paper presents the design structure and operation of an innovative secure and reliable communication module that would ensure the privacy of the patient biological data.

Key words: Healthcare · Cloud satisfy Secure Transmission Module

INTRODUCTION

Cloud computing is an interesting methodology enabled by delivering software, infrastructure and the entire computation platform as a service. Four basic cloud deployment models by National Institute for Standards and Technology (NIST) are presented: the public cloud, private cloud, hybrid cloud and community cloud. Services in cloud computing are characterized into three main categories [1]: Software as a Service (SaaS), Platform as a Service (PaaS) and Cloud Software Infrastructure that is composed of three layers namely; computational resources (or Infrastructure as a Service (IaaS)), Data-Storage as a Service (DaaS) and Communication as a Service (CaaS). Moreover, there are other types of service models are provided: Storage as a service (STaaS), Security as a Service (SECaaS) and Test Environment as a Service (TEaaS). Examples of these service models include Google Compute Engine, Google App Engine, Windows Azure Virtual Machines, Amazon Elastic Beanstalk and Microsoft Office 365, to name a few. As commercial cloud services are increasing more and more, cloud system architecture that can process large-scale data for portable wireless devices is emerging rapidly due to the high speed of wireless broadband and the availability of virtual machines for portable (mobile) devices to form what is called "wireless cloud" or "mobile cloud". Numerous wireless cloud-based applications have been developed such as education (distance learning) [2], healthcare (medical diagnoses and surgical operations) [3] and multimedia (seminars and conferences) [4]. These applications seek services provided by cloud for data processing, data mining, data storage and data analysis.

Cloud-Based Healthcare Environment: There are several factors that determine the evolution of the home healthcare market universally, for example aging population and growing number of people who diagnosed with chronic diseases like diabetes, cardiac disorders and respiratory diseases. As patients have different disease

Corresponding Author: Mohamed Doheir, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka 76100, Malaysia.

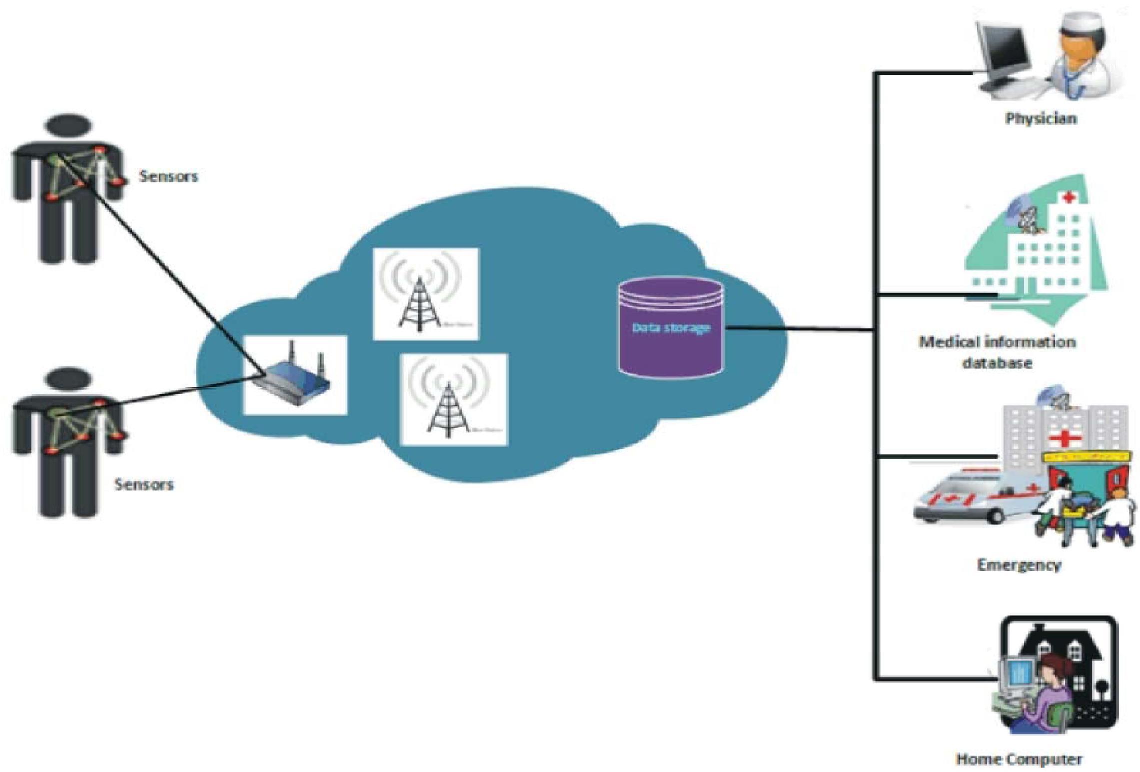

Fig. 1: Wireless Body Area Networks (WBANs) for healthcare

conditions and management requirements patients and commonly spend most of their time at home with self-management and care away from hospital environments, especially those who have a long-lasting disease, it is essential to offer integrated and personalized healthcare services for the patients [5]. Furthermore, the World Health Organization (WHO) has stated that the number of people aged 65 years and above is expected to increase from 605 million to 2 billion by 2050. All this would increase the demand for home healthcare during the study period and therefore increase market for healthcare. Healthcare integration into the cloud open a lot of opportunities to offer options for supporting healthcare industry and organizations in order to lay the path towards providing improved clinical relevant services to meet the patient's requirements.

Healthcare Architecture: The common architecture used for healthcare is Wireless Body Area Networks (WBANs) illustrated in Figure 1 where a patient is equipped with sensors (positioned on his body) that are clustered to save energy consumption [6]. Sensors send the sensed data to their Cluster Head (CH) which in turn transfers the data to a gateway and then the gateway relays data to a database through the Internet where hospital staff, system administrators and the patient (and his family) are able to access them. WBAN is standardized within the IEEE 802.15.6 where its components are equipped with wireless communication radio that supports human body communications.

WBAN is still attracting attention in this research field which is increasing rapidly [7]. However, privacy is one of the major challenging issues in WBAN that is related closely to users' concerns. This is because of the unique characteristics of WBAN, like flexible infrastructure, mobile terminals, open medium channel and signal noise, leading to many novel security vulnerabilities and threats. For instance, in remote healthcare applications, authorized patients should anonymously access and share medical services and doctors have to know the patient bio-information only, whereas all the rest private information (name and ID number) must be kept unknown. Thus, further development and practical application of such networks are highly needed.

Furthermore, any research on the healthcare architecture should first consider the rules of Health Insurance Portability and Accountability Act (HIPAA) in regards to security and privacy. Health Information Technology for Economic and Clinical Health (HITECH) legislation of the United States of America (USA) summaries plans for essential privacy and security controls on digital healthcare system [8].

Related Works: We review some of the well-known and most cited healthcare systems. A Mobile Cloud for Assistive Healthcare (MoCAsH) proposed by Hoang and Chen [9] as a framework for assistive healthcare, which tackle security and privacy issues via utilizing a selective Peer-to-Peer Cloud to protect data integrity and reinforce security aspects. Chen [10] proposed a NDNC-BAN framework to distribute healthcare contents by using the Named Data Networking (NDN) for reliable delivery of rich media content without service disruption and accomplishing low cost and bandwidth saving simultaneously. Liu *et al.* [11] proposed an interconnection architecture for e-Healthcare Cloud Computing and Networking solutions, considering the cloud-enabling characteristics of the e-Healthcare application. Their architecture helps in adapting an important health information technology into the cloud and allowing continuing evolution of interconnected cloud services and solutions for e-Healthcare. Pandeya *et al.* [12] presented a scalable and economical cloud-based system for hosting collection of electrocardiogram (ECG) data analysis services. The design purpose is to collect ECG data through mobile nodes and transmit the collected data to distant processing unit for further analysis. Xia *et al.* [13] proposed a cloud-based system for clients who have smart mobile phones or web browsers. The proposed system was validated by uploading ECG data to a web server from a mobile device at a definite frequency and the data analysis was done in real time. Tartarisco *et al.* [14] proposed an architecture for personal health system that helps in monitoring patients and supporting clinical decisions.. Pang *et al.* [15] formulated a cooperative Health-IoT ecosystem, through which they developed a business-technology framework for integrated devices and services for in-home healthcare. It has three key integrated and aligned elements: business model, integrated device and service architecture.Hu *et al.* [16] designed a robust cluster-based Medical Ad Hoc Sensor Network (MASN) architecture based on wavelet theories for ECG data mining that help in tracking cardiac patients and extracting ECG features. A lightweight mechanism for medical security is used to reach a confidential transmission of ECG data over a wireless connection. Khalaf *et al.* [17] proposed an alert cloud-based system that sends immediate notification to doctors upon detection of a serious condition according to the analysis of the patient collected data. Moreover, classification process is performed by an efficient machine-learning technique. Android and MQTT-based system was proposed by António *et al.* [18] for gaining, transmitting, storing and visualizing of pulse oximeter and ECG data. Data is acquired and transmitted by Bluetooth to android mobile devices which in turn send the data to distant server. After processing, the data is kept in the database and it is available for visualization. The system offers efficient data delivery (one second) with no loss as data transmission is done over MQTT. Abderrahim *et al.* [19] proposed a ubiquitous health monitoring system where patients' conditions are determined by using cloud computing, data location and a neural network through an architecture that consists of WBASN, smart phone and cloud medical server. In order to validate the system, measurements processing and user Input/output were done by a pulse oximeter (as WBASN) and Samsung galaxy S. Once the condition of a patient changes, a notification is triggered to alert the medical authority timely. Xu *et al.* [20] proposed cloud-based m-Health monitoring system, called Cloud-MHMS, for ubiquitous health monitoring. The system has several layers: Cloud Storage and Multiple Tenants Access Control Layer, Healthcare Data Annotation Layer and Healthcare Data Analysis Layer. Felisberto *et al.* [21] presented a multi-agent, open and distributed architecture for monitoring and identifying human postures and movements as well as detecting potential harmful activities. Multiple sensors are used to recognize unhampered falls accidents and analyze the movement of human.

The well-known cloud-based healthcare systems mentioned above are lack of efficient, reliable and secure data transmission and communication. Moreover, new requirements on reporting breaches are enforced by HITECH. This indicates that health information related to patients must be encrypted and health specialists must destroy unencrypted data after use [8]. However, there is scarce attention on securing the communication in the first place, which is as important as the integrity of the patient data. Therefore, we present in this paper a secure and reliable communication module to protect the sensed patient's biological data during transmission.

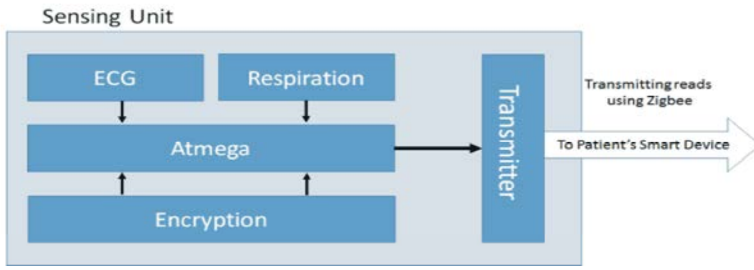

Fig. 2: Sensing unit of the proposed communication module

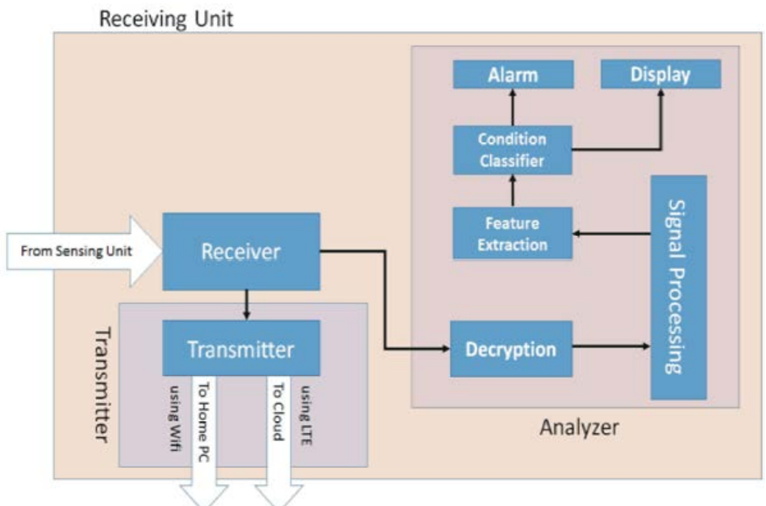

Fig. 3: Receiving unit of the proposed communication module

Proposed Communication Module: The principle goal of the work presented in this paper is to develop a cloud-based secure healthcare communication module for monitoring patient condition by utilizing cloud wireless and sensor networks. The proposed secure communication module is consists of two units: Sensing Unit and Receiving Unit, as illustrated in Figure 2 and Figure 3, respectively. Receiving unit has two components: Transmitter and Analyzer.

Sensing unit is implemented in the cluster head while receiving unit is implemented in home smart device (whole unit) and healthcare system at hospital (analyzer part only). The patient's biological data is encrypted while it resides in the cloud. Transmitter would send the encrypted bio data as is to the cloud and home PC using LTE or WiFi (through access point).

As shown in Figure 2, sensing unit includes two types of sensors; Electro-cardiogram (ECG) sensor which is a health indicator that is appropriate for long-term body monitoring and Respiration sensor that detects body expansion/contraction and shows the respiration waveform and amplitude. These sensors are connected to Atmega microprocessor and transmitter components. The bio data is encrypted by the encryption component before it is sent to the transmitter component. Elliptic curve cryptography (ECC) mechanism is used in encrypting the patient's biological data during the communication as it requires smaller key size reducing storage and transmission requirements compared to non-ECC mechanisms. Then, the encrypted biological data are transmitted to the patient's smart device where received data is analyzed for further characterization, decision-making and choices.

In the Receiving Unit, upon the receipt of encrypted biological data, it would be retransmitted and analyzed by different modules as shown in Figure 3. The patient's smart device retransmits the received encrypted biological data to the cloud using LTE (Long Term Evolution) technology, or to home Personal Computer (PC) using WiFi (Wireless Fidelity) technology, using the Transmitter module. Whereas, the Analyzer module decrypts and filters the data to extract the expressive features that would enable the classifier to designate the condition of the patient. Then, the patient would be able

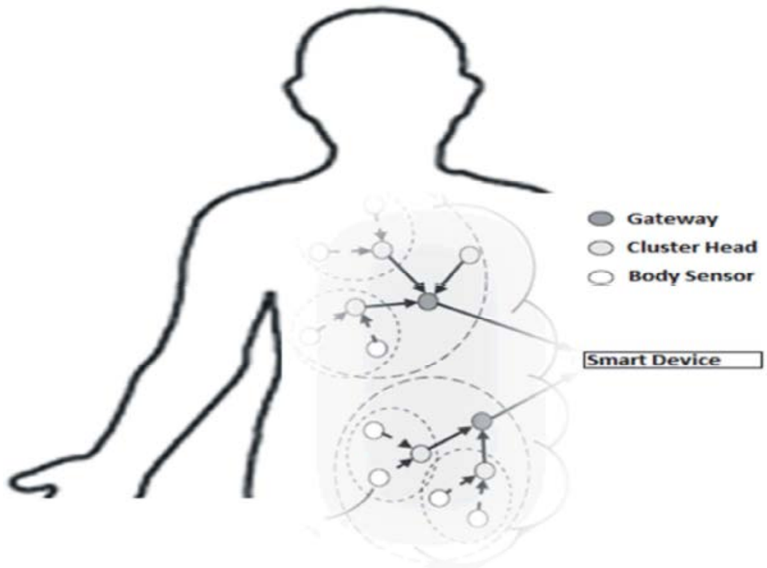

Fig. 4: Hierarchical clustering of body sensors

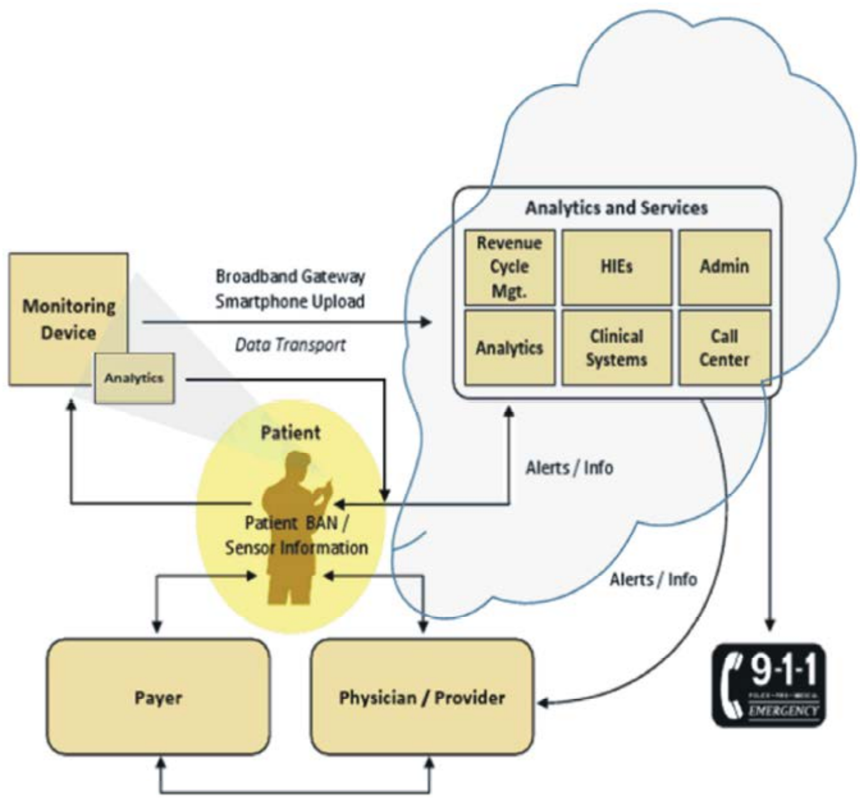

Fig. 5: Cloud-based remote patient monitoring and healthcare service

to see the results via the display. If the condition is critical, the module in the smart device will activate an alarm to immediately warn the patient, family, caregivers and doctors in hospital or medical centers through the cloud service.

Sensors deployed on the patient's body are clustered hierarchically (as illustrated in Figure 4) and among each cluster a sensor is assigned as a cluster head (CH) while the rest sensors are ordinary sensors that only sense and signal to the CH which in turn sends the aggregated data to a gateway. The gateway then forwards the data to the patient's smart device. Clustering is formed statistically done during sensors placement and will not be changed in terms of number of member nodes and monitoring area covered. Clustering contributes to noticeable reduction in redundant data and interference.

Communication Module Operation within Healthcare System: Considering the remote patient monitoring and healthcare service depicted in Figure 5, which utilizes the facilities of the cloud environment. The cloud part system includes services such as Revenue Cycle Management, Health Information Exchange (HIE), Administration, Analytics, Clinical Systems and Call Centers.

Once a patient approaches doctors in hospital or medical/clinical centers, he/she would first undergo some medical in order to acquire the proper treatment. Then, the patient is registered in the hospital medical system and his/her bio-data and medical health record are stored in the hospital database. This information will be automatically transmitted to the hospital healthcare environment and to the cloud part system shown in the figure. When the patient condition requires deploying Body Area Nework (BAN) of portable sensors to monitor the health condition, it would be used even if the patient is discharged and move to home. Sensors that are deployed the patient body intelligently monitor the patient condition and send their sensed reads (data/signals) to the CH. The sensed data will be delivered to the patient mobile device (can be smart mobile phone, iPad, or tablet) and to the home healthcare environment using the sensors gateways. The administrator of hospital healthcare environment is responsible of uploading the patient's care services to the home healthcare environment. Thus, doctors would be able to interact with the home healthcare system remotely. Once an abnormality is detected in the patient's condition after analyzing the data, the module in the home healthcare environment would immediately report to the doctors. Then, based on the examination of the patient health data, a decision will be made on whether directly alert the involved caregivers and emergency response team that are connected to the cloud. All of these data that are transmitted between the home healthcare environment, hospital healthcare environment and the cloud part system over communication channels are encrypted to secure and protect the privacy of the sensed data in order to provide appropriate medical treatment decision on time. The services of the cloud part system would inform the doctors and healthcare providers if there is any update regarding the patient data, so that doctors/physicians can exchange the information with the patient family/payer.

CONCLUSION

In this paper, we propose a cloud-based secure healthcare communication module for monitoring patient condition by utilizing the services provided in the cloud environment, clustered and networked body sensors, mobile smart devices and the Internet communication protocols. The proposed communication module is consists of two units, Sensing Unit and Receiving Unit, for sensing, encrypting, transmitting and analyzing the patient biological data. The patient related biological data and diagnosis results are all encrypted before transmitted to ensure the privacy of the data order to provide accurate and immediate medical treatment decision that must be provided to patient according to his/her health condition.

For the future work, we are going to implement the design of the proposed healthcare communication module to verify and validate its efficiency and how well it satisfies the requirements of patient and healthcare providers.

ACKNOWLEDGEMENTS

This work was supported by Universiti Teknikal Malaysia Melaka (UTeM), Malaysia.

REFERENCES

1. Anderson, R.W., 2010. The cloud services stack and infrastructure, July 28, 2008.
2. Ye, Z., X. Chen and Z. Li, 2010. "Video based mobile location search with large set of SIFT points in cloud," in Proceedings of the 2010 ACM Multimedia Workshop on Mobile Cloud Media Computing (MCMC), pp: 25-30.
3. Hoang, D.B. and L. Chen, 2011. "Mobile Cloud for Assistive Healthcare (MoCAsH), " in Proceedings of the 2010 IEEE Asia-Pacific Services Computing Conference (APSCC), pp: 325, February.
4. Ferzli, R. and I. Khalife, 2011. "Mobile cloud computing educational tool for image/video processing algorithms, 2011." in Digital Signal Processing Workshop and IEEE Signal Processing Education Workshop (DSP/SPE), pp: 529.

5. Sangjin Jeong, 2013. “A Personalized Healthcare System for Chornic disease Care in Home-Hospital Cloud Environments,” International Conference on ICT Convergence, pp: 371-376.
6. Liu, J., Z. Zhang, X. Chen and K.S. Kwak, 2014. Certificateless remote anonymous authentication schemes for wirelessbody area networks Parallel and Distributed Systems, IEEE Transactions on, IEEE, 25: 332-342.
7. Chen, M., S. Gonzalez, A. Vasilakos, H. Cao and V.C. Leung, 2013. Body area networks: A survey Mobile networks and applications, Springer-Verlag New York, Inc., 2011, 16: 171-193.
8. US Government Information, Part II Department of Health and Human Services, Federal Register, January, 78(17).
9. Hoang, D.B. and L. Chen, 2010. Mobile cloud for assistive healthcare (MoCAsH) Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific, pp: 325-332.
10. Chen, M., 2014. NDNC-BAN: supporting rich media healthcare services via named data networking in cloud-assisted wireless body area networks Information Sciences, Elsevier, 284: 142-156.
11. Liu, W. and E.K. Park, 2013. E-healthcare cloud-enabling characteristics, challenges and adaptation solutions J. Commun, 8: 612-9.
12. Pandey, S., W. Voorsluys, S. Niu, A. Khandoker and R. Buyya, 2012. An autonomic cloud environment for hosting ECG data analysis services Future Generation Computer Systems, Elsevier, 28: 147-154.
13. Xia, H., I. Asif and X. Zhao, 2013. Cloud-ECG for real time ECG monitoring and analysis Computer methods and programs in biomedicine, Elsevier, 110: 253-259.
14. Tartarisco, G., G. Baldus, D. Corda, R. Raso and A. Arnao, 2012. “Personal Health System Architecture for Stress Monitoring and Support to Clinical Decisions “Journal of Computer Communications, 35: 1296-1305.
15. Pang, Z., L. Zheng, J. Tian, S. Kao-Walter, E. Dubrova and Q. Chen, 2015. Design of a Terminal Solution for Integration of In-home Health Care Devices and Services Towards the Internet-of-Things Enterp. Inf. Syst., Taylor & Francis, Inc., 9: 86-116.
16. Hu, F., M. Jiang, L. Celentano and Y. Xiao, 2008. Robust medical ad hoc sensor networks (MASN) with wavelet-based ECG data mining. Ad Hoc Networks, 7: 986-1012.
17. Khalaf, M., A. Hussain, D. Al-Jumeily, P. Fergus, R. Keenan and N. Radi, 2015. Huang, D.S., Jo, K.H. & Hussain, A. (Eds.) A Framework to Support Ubiquitous Healthcare Monitoring and Diagnostic for Sickle Cell Disease Intelligent Computing Theories and Methodologies, Springer International Publishing, 9226: 665-675.
18. António Damasceno, Andreia Carreiro, Andreia Carreiro and Gonçalo Louzada, 2013. ”System of acquisition, transmission, storage and visualization of Pulse Oximeter and ECG data using Android and MQTT”, CENTERIS 2013 - Conference on ENTERprise Information Systems, October.
19. Abderrahim Bourouis, Mohamed Feham and Abdelhamid Bouchachia, 2012. “A New Architecture of a Ubiquitous Health Monitoring System: A Prototype Of Cloud Mobile Health Monitoring System”, CoRR abs/1205.6910.
20. Xu, B., L. Xu, H. Cai, L. Jiang, Y. Luo and Y. Gu, 2015. The design of an m-Health monitoring system based on a cloud computing platform Enterprise Information Systems, Taylor & Francis, pp: 1-20.
21. Felisberto, F., R. Laza, F. Fdez-Riverola and A.A. Pereira, 2015. Distributed Multiagent System Architecture for Body Area Networks Applied to Healthcare Monitoring BioMed research international, Hindawi Publishing Corporation.