Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 34 (2014) 511 – 517

Procedia Computer Science

The 2nd International Workshop on Communications and Sensor Networks (ComSense-2014)

A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks

Farrukh Aslam Khan[a,b,*], Aftab Ali[a,b], Haider Abbas[b,c], Nur Al Hasan Haldar[c]

[a]National University of Computer and Emerging Sciences, Islamabad, Pakistan.
[b]Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia
[c]National Unviesity of Sciences and Technology, Islamabad, Pakistan

Abstract

The recent developments in remote healthcare systems have witnessed significant interests from IT industry (Microsoft, Google, VMware etc) that provide ubiquitous and easily deployable healthcare systems. These systems provide a platform to share medical information, applications, and infrastructure in a ubiquitous and fully automated manner. Communication security and patients' data privacy are the aspects that would increase the confidence of users in such remote healthcare systems. This paper presents a secure cloud-based mobile healthcare framework using wireless body area networks (WBANs). The research work presented here is twofold: first, it attempts to secure the inter-sensor communication by multi-biometric based key generation scheme in WBANs; and secondly, the electronic medical records (EMRs) are securely stored in the hospital community cloud and privacy of the patients' data is preserved. The evaluation and analysis shows that the proposed multi-biometric based mechanism provides significant security measures due to its highly efficient key generation mechanism.

Keywords: Mobile Healthcare; Wireless Body Area Network (WBAN); Data Security; Cloud Computing.

1. Introduction

Wireless Body Area Networks (WBANs) consist of small and tiny sensor nodes attached or implanted on a human body in order to measure the physiological values of the body. WBANs have been successfully used in the area of healthcare, which includes e-health, remote patient monitoring, and health monitoring of soldiers in a battlefield etc. By connecting WBANs to the cloud will increase efficiency, scalability, and overall performance of the system by sharing resources with a large number of devices in the cloud. In this way, the computational power and storage of WBANs can be increased to a large extent. Cloud computing trend reveals the next generation application architecture [1].

The goal of this work is to develop a generic, reliable, easily deployable, and secure ubiquitous architecture for a cloud-based mobile healthcare system. There are two main phases of the proposed work. In the first phase, the communication of sensors in WBANs is made secure, while in the second phase, Electronic Medical Records (EMRs) are securely stored in the hospital community cloud along with preserving the privacy of patients' personal

*Corresponding author. Tel.: +966-11-4697341; fax: +966-11-4695237
E-mail address: fakhan@ksu.edu.sa

Selection and peer-review under responsibility of Conference Program Chairs
doi:10.1016/j.procs.2014.07.058

data. The proposed framework uses sensors attached to the human body that measure physiological values (PVs) and send these values securely to different servers located at the hospital community cloud. Physicians and other medical personnel connected to the cloud will then carry out patients' treatment according to the measured values. The overall architecture of our proposed system shown in Figure 1, which consists of sensors attached to the patient's body and a gateway for each patient (e.g., a PDA or a laptop computer). The indoor and outdoor users i.e. patients, physicians, and medical staff are connected to the cloud and are able to access information and resources with proper privileges in order to ensure security and privacy. All the resources and information are made available in the hospital community cloud for all the registered users. The proposed framework is evaluated in terms of security of inter-sensor communication and privacy of patients' data. The results are very encouraging and show the validity of the proposed architecture for next generation mobile healthcare systems.

The rest of the paper is organized as follows: Section 2 presents the related work. In section 3, the proposed cloud-based mobile healthcare framework is presented. Section 4 shows the results and analysis, whereas, section 5 concludes the paper.

2. Related work

The related work section is divided into three parts on the basis of modules that constitute the cloud-based secure healthcare system i.e., healthcare monitoring systems, cloud computing based architectures, and physiological value based key agreement and security. A PDA-Based Patient-Monitoring System [2] is a mobile patient monitoring system that uses a personal digital assistant (PDA) and a wireless local area network (WLAN). CodeBlue is an Ad-hoc sensor network infrastructure for emergency medical care comprising low-power physiological sensors and PDAs [3]. CodeBlue was proposed to improve the ability of first responders to evaluate patients while performing their normal duties. The MobiHealth System [4] is an end-to-end healthcare platform for ambulant patient monitoring deployed on UMTS and GPRS networks. The mobile healthcare systems discussed above are not cloud-based and hence face the problems of accessibility, storage, and computational capabilities. In [12], the authors proposed the idea of connecting a mobile device to a cloud in order to get valuable information through queries, such as "what is the average temperature of nodes within a mile of my location?". The VMware hospital secure private cloud provides services via an infrastructure-as-a service (IaaS) or software-as-a-service (SaaS) model [13]. Microsoft in [14] aims to manage the health of the user or subject by monitoring and tracking the health condition or body activity via body sensor network leveraging cloud computing. Dossia is a Personal health record service offered by some of the largest employers in the United States [15]. In case of physiological value based security, the authors in [6] used electrocardiogram (ECG) data to generate cryptographic keys using discrete wavelet transform (DWT) for feature extraction. In [7] and [8], the authors proposed a pair-wise key management protocol that used accelerometer data (from a handheld device) as a PV for generating keys. The scheme functions by physically shaking the communicating devices. In [9-10], a cluster-based secure key-agreement protocol for WBANs is presented, considering the network as a heterogeneous sensor network consisting of a powerful high-end sensor (H-sensor) node and several low-end sensor (L-sensor) nodes. In [11], PVs are used as a means for security in WBANs.

The above-mentioned health monitoring systems are either fixed infrastructure systems or lack the ubiquitous nature of communication with no plug-n-play capabilities. The physiological value-based key agreement schemes discussed above are based on a single biometric value and hence lack sufficient randomness and key length. The work presented in this paper provides a cloud-based platform, where the health of patients is monitored securely by using sensors implanted on the human body, as well as keeping the privacy of patients' sensitive data.

3. Proposed framework

The proposed framework consists of sensors attached to a patient, a personal server (PS), a client interface/data reader, remote base station (RBS), and a hospital community cloud as depicted in Figure 1. The computational servers would be deployed using the hospital community cloud. The proposed hierarchical framework has two modes: the indoor-patient mode and the outdoor-patient mode. In indoor–patient mode, the hospital provides connectivity to the hospital community cloud through their local servers, while in outdoor-patient mode the patient is connected to the hospital community cloud via RBS.

In the indoor-patient mode, the patients are admitted to the hospital and are kept under observation in a room or a ward. The sensors capable of measuring human physiological values are attached to their bodies to sense the PVs

i.e. electrocardiogram (ECG) and electroencephalogram (EEG) values. Each patient has a personal server (a PDA or a laptop) and is responsible for gathering data from sensors on the patient's body, and a client interface/data reader to transfer data from personal servers to the hospital community cloud. Each department (comprising several rooms) in the hospital has a department server. The department servers connect to the hospital's main server.

In outdoor-patient mode, the patient is considered to be outside the hospital and not located in the server's range. Thus, the patient (WBAN) must connect to a remote base station (RBS), which transfers the patient's data to the hospital community cloud. If the patient is not within the range of the RBS, inter-body communication is initiated that routes the patient's data to the RBS through the PSs of other patients (WBANs) within the range of the first patient. Once the data is directed to the cloud, it will be stored in the EMR system of the hospital. This system consists of the hospital servers like main server, application server, and database server etc. UBUNTU Enterprise Cloud (UEC) Eucalyptus database would be used to store data in buckets and objects. The received data (PVs) are securely stored in the Eucalyptus database using database schema redesign and cryptographic technique [19].

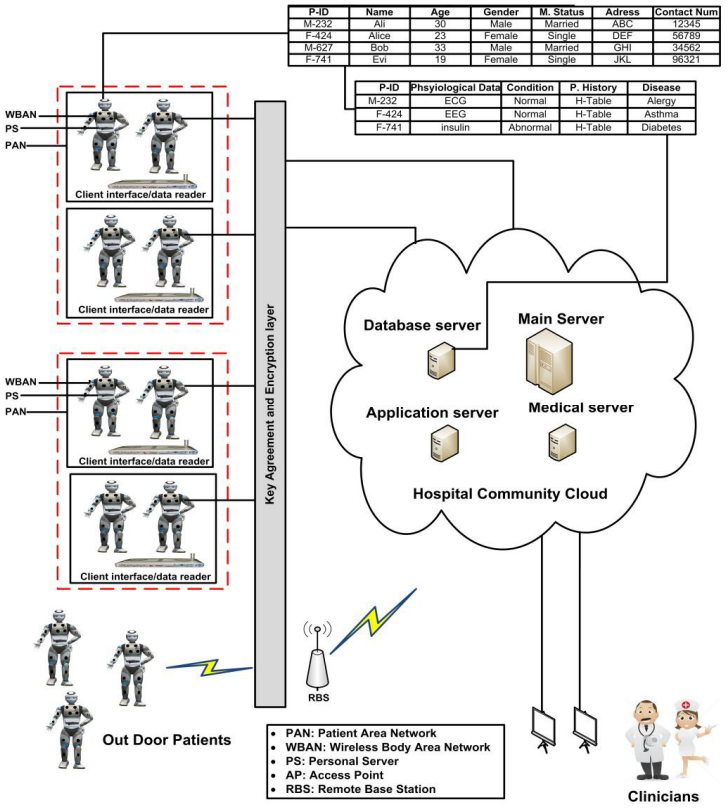

Fig. 1. Cloud based mobile healthcare system architecture

3.1 Multi-biometric based scheme

Multi-biometric scheme uses the combination or fusion of two biometrics that involve two physiological values namely ECG and EEG. The motivation behind the usage of multiple biometrics is to increase the length, and get a more random and secure key. The details of the scheme are as follows:

3.1.1 Feature selection

The features are extracted and quantized for secure inter-sensor communication from ECG and EEG signals using discrete wavelet transform (DWT). The input to the system is two signals ECG and EEG, while a long and more random combined key of ECG and EEG is generated. For communication between SNs and PS, sensors sample the ECG and EEG signals at the sampling rate of 125Hz in the time duration of 5 seconds. The process is

carried out in parallel to generate a long and more random key. The selected features from ECG and EEG are then collected in two feature vectors i.e., ECG FV and EEG FV. In quantization phase, the generated feature vectors from both ECG and EEG signals are divided into 20 blocks each containing 16 coefficients for ECG and same for EEG, and are quantized into a binary stream. These blocks are exchanged by applying keyed hashing (HMAC-MD5).

3.1.2 Key Generation

On the receiving ends, both the sensors collect ECG and EEG blocks, and apply the KeyGen algorithm. The KeyGen generates two keys of length 160 bits. The generated keys are then horizontally concatenated to get a 320 bit long key. The key generation process and key exchange is shown in Figure 2. Each sensor node compares the received blocks to extract common blocks. The extraction is performed by constructing a matrix, where each element of the matrix represents Hamming distance between the i^{th} block of Sensor 1 and the j^{th} block of Sensor 2. The generated keys are used by the sensors to verify the received message authentication code (MAC). Upon the successful MAC verification , the sensor nodes use these keys for further communication.

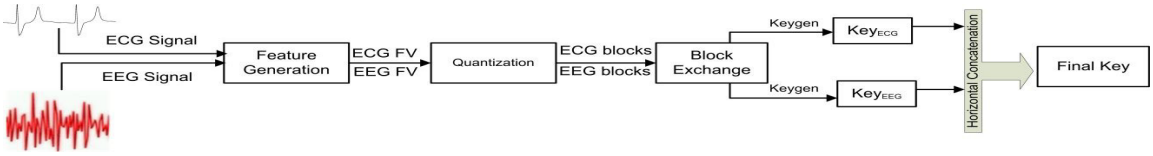

Fig. 2. Multi-Biometric based key generation process

ECG and EEG values are used for the generation of keys. When sensor node 'a' (SN_a) wishes to communicate with sensor node 'b' (SN_b), SNa sends hello message with its ID and nonce in *m1*. Nonce is an integer value included to check the transaction freshness.

$$\text{m1: } \forall SN_a \in \{SN\}: SN_a \rightarrow SN_b : (ID_{SN_a}, \text{Hello}, \text{nonce})$$

After receiving *m1*, SN_b calculates pair-wise keys ECG, EEG and ID of SN_a and SN_b

$$K1_{SN_a,SN_b} = \text{HMAC}\left(\text{CalculatedECG values}||ID_{SN_a}||ID_{SN_b}\right) \quad (1)$$

$$K2_{SN_a,SN_b} = \text{HMAC}\left(\text{Calculated EEGvalues}||ID_{SN_a}||ID_{SN_b}\right) \quad (2)$$

As ECG and EEG values are same on both sides, $K1_{SN_a,SN_b}$ and $K2_{SN_a,SN_b}$ generated by SN_a is same as that of SN_b. These two keys are then horizontally concatenated to form one large key K_{SN_a,SN_b} called the final key. SN_b encrypts the data with K_{SN_a,SN_b} and computes MAC on ID of SN_a, nonce from SN_a and data using same key K_{SN_a,SN_b}. In *m2*, SN_b sends its ID, encrypted data and MAC to SN_a.

$$m2: \forall\, SN_b \rightarrow SN_a : ID_{SN_b}, EK_{SN_a,SN_b}\{ID_{SN_b}, Data\}, MAC_{K_{SN_a,SN_b}}(ID_{SN_b}, Data, nonce)$$

SN_a upon receiving *m2,* decrypts it with K_{SN_a,SN_b} and compares ID_{SN_b} and received ECG and EEG values with decrypted message ID_{SN_b} and ECG and EEG values on SN_a to ensure that both parties have generated the same key. The message authenticity is checked by SN_a through *MAC* verification with K_{SN_a,SN_b}.

3.2 Cloud based EMR

In order to provide quality healthcare, it is important that medical personnel and the concerned physicians should access the EMRs in a ubiquitous manner. The ubiquitous access can be provided by storing the EMR on the cloud. The first phase of our proposed framework focuses on the security of WBAN communication. The second part of focuses on the privacy of cloud-based patients' medical data storage. The security of patients' medical data, while it is in transit, and privacy of this data when it is at rest are concomitant; human life might be endangered if securely communicated medical data is not stored in a secure manner. To ensure the privacy of patients' medical data, we have used an adaptation of the cloud users' data privacy preservation mechanism based on dynamic reconstruction of metadata as presented in [19].

3.2.1 Categories of Patients' Medical Data

The following categories were identified of patients' medical data that mobile healthcare system commonly uses:

1. Patients' Personal Information
   a) patient's unique identification number, b) patient's name, c) patient's address.
2. Patients' Medical History
   a) Medical condition unique id, b) Medical condition name, c) Date of diagnosis, d) Recommended treatment.
3. Privacy preservation of patients' medical data stored in the database server

Here, we divide each of the data items identified in one of the above-mentioned categories into sensitivity parameterization classes of exclusively private (degree 1 and 2), partially private (degree 1 and 2), and non-private as depicted in Figure 3.

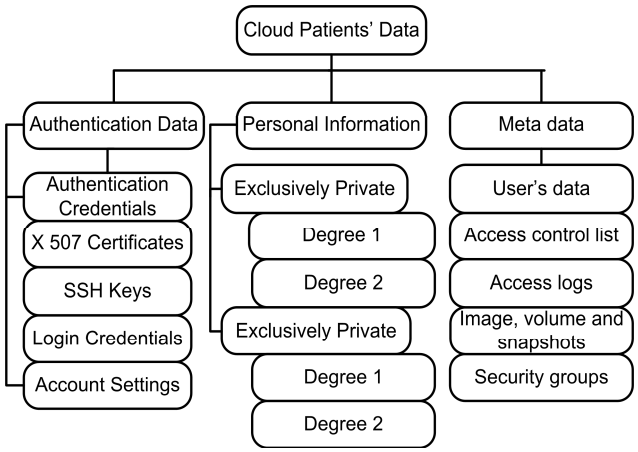

Fig. 3. Patients' data sensitivity parameterization of exclusively private and partially private data

For reference purposes, the NHS data model and dictionary is used [20]. Using SQL Server 2008 R2, we created a generic database consisting of the data items mentioned above. Using steps outlined in [19], we performed data classification on the sample database followed by the horizontal/vertical table splitting.

4. Experiments and Results

Most of the security techniques and protocols have expressed their cryptographic strength in terms of the number of (key) bits that an attacker needs to guess in order to break the system. For example, if the attacker starts with key material that is partly predictable, it indicates the weakness of the security system regardless of the algorithm or protocol used. If 128-bit key contains 16 predictable bits, using it in AES-128 does not ensure 128-bit protection, it only provides 112 bits of protection, making the security of the system compromised up to some level. To ensure the security of the system, the key used must be truly random. In our implementation, the generated keys are verified by Dieharder [18] testing suite on a UBUNTU machine. One of the most famous randomness-testing suite is DIEHARD [17], which is made up of twelve tests. DIEHARD has been expanded into the open source (GPL) set of tests called Dieharder, which includes the DIEHARD, NIST tests, as well as many new ones.

4.1 Randomness

To check the randomness, a set of P-values are produced for each statistical test. A P-value is a probability measure of obtaining a test statistic larger than the one observed, if the sequence is random. Similarly, small values indicate that a sequence is unlikely to be random. The decision rule in this case states that "for a fixed significance value α, a sequence fails the statistical test if it's P-value $< \alpha$." A sequence passes a statistical test whenever the P-value $\geq \alpha$ and fails otherwise. [16] assumes that a test is considered failed if it outcomes a P-value less than or equal to 0.0001 or greater than or equal to 0.9999. It results in a 95% confidence interval of P-values between 0.0001 and 0.9999. In this work the keys are generated for 25 different subjects. The EEG and ECG data are taken from MIT Physiobank database. The Dieharder testing suite is applied on the keys generated from the EEG and ECG data of the 25 subjects. Table 1 shows the average P-value of 25 keys and their respective assessments. It is evident from Table 1

that none of the P-values is violating the condition given in [16].

Table 1. Dieharder testing suite results

Test Name	ntup	t-samples	p-sample	Average P-value of 25 keys	Assessment
diehard_birthdays	0	100	100	0.653760029	OK
diehard_operm5	0	1000000	100	0.532907215	OK
diehard_rank_32x32	0	40000	100	0.510957518	OK
diehard_rank_6x8	0	100000	100	0.614881389	OK
diehard_bitstream	0	2097152	100	0.572861452	OK
diehard_opso	0	2097152	100	0.56342995	OK
diehard_oqso	0	2097152	100	0.564799784	OK
diehard_dna	0	2097152	100	0.49437631	OK
diehard_count_1s_str	0	256000	100	0.425854956	OK
diehard_count_1s_byt	0	256000	100	0.570959702	OK
diehard_parking_lot	0	12000	100	0.611109984	OK
diehard_2dsphere	2	8000	100	0.553310269	OK
diehard_3dsphere	3	4000	100	0.537745781	OK
diehard_squeeze	0	100000	100	0.589133353	OK
diehard_sums	0	100	100	0.13205638	OK
diehard_runs	0	100000	100	0.559359585	OK
diehard_craps	0	200000	100	0.563369301	OK
marsaglia_tsang_gcd	0	10000000	100	0.610666545	OK
sts_monobit	1	100000	100	0.606755002	OK
sts_runs	2	100000	100	0.501179924	OK
sts_serial	1-16	100000	100	0.504396057 -0.671142755	OK
rgb_bitdist	1-12	100000	100	0.481688763 - 0.702577895	OK
rgb_minimum_distance	2-5	10000	1000	0.445556424 - 0.652603025	OK
rgb_permutations	2	100000	100	0.601399862	OK
rgb_permutations	3	100000	100	0.630948728	OK
rgb_permutations	4	100000	100	0.534075445	OK
rgb_permutations	5	100000	100	0.461843218	OK
rgb_lagged_sum	0-32	1000000	100	0.388427623- 0.709601808	OK
rgb_kstest_test	0	10000	1000	0.45008513	OK
dab_bytedistrib	0	51200000	1	0.48189395	OK
dab_dct	256	50000	1	0.500848326	OK
dab_filltree	32	15000000	1	0.491787382	OK
dab_filltree	32	15000000	1	0.44187268	OK
dab_filltree2	0	5000000	1	0.532810523	OK
dab_filltree2	1	5000000	1	0.59660472	OK
dab_monobit2	12	65000000	1	0.603623061	OK

4.2 Entropy

Entropy is the quantitative measure of disorder or randomness in a system. High entropy means higher security. Figure 4 shows the entropy comparison of the proposed scheme with ECG based scheme [5] and EEG scheme. The proposed multi-biometric based scheme has high entropy as compared to both ECG and EEG based schemes, which shows more randomness on average. Moreover, the length of the generated keys in [5] is 128 bits, while the proposed multi-biometric based scheme produces 320 bits.

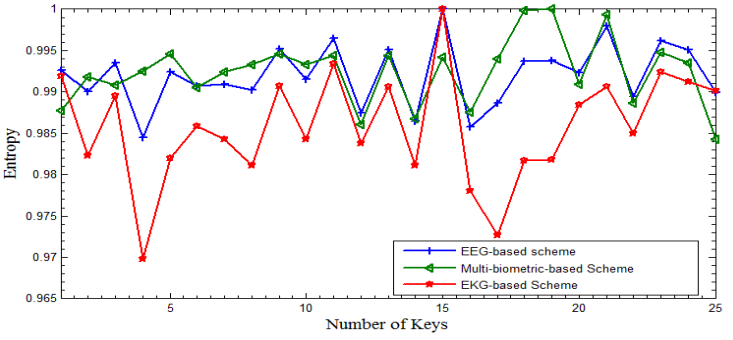

Fig. 4. Entropy comparison of keys generated from 25 subjects

The generated keys from proposed scheme generate the entropy of almost 265. For a 50-bit long key, the total probability is found to be one in a million if one billion people each make a different guess. With the same effort, the probability of success decreases for each additional key bit.

5. Conclusion and Future work

The paper presented a cloud-based secure framework for mobile healthcare system that focuses on inter-sensor communication security as well as patients' data security and privacy. The proposed system uses multiple biometrics to generate a common key for inter-sensor communication. The proposed framework is evaluated in terms of security of inter-sensor communication and the results indicate that the proposed system is a viable solution for the next generation mobile healthcare systems. The proposed framework is unique as it provides a complete cloud-based framework and security solution for a ubiquitous mobile healthcare.

References

1. Hutchinson, C., Ward, J., Castilon, K. Navigating the next-generation application architecture. *IT Professional*, 1(2), pp. 18–22, 2009.
2. Lin, Y. H., Jan, I.C., Chow-In Ko, P. Chen, Y., Wong, J.M., Jan, G.J. A wireless PDA-based physiological monitoring system for patient transport. *IEEE Trans. Info. Tech. Biom.,* vol. 8, no. 4, pp. 439-447, December 2004.
3. Malan, D. Fulford Jones, T., Welsh, M., Moulton, S. CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care. *International Workshop on Wearable and Implantable Body Sensor Networks,* London, United Kingdom, April 6-7 2004.
4. Halteren, A.V., Bults, R., Wac, K., Konstantas, D., Widya, I., Dokovsky, N., Koprinkov, G., Jones,V., Herzog, R. Mobile patient monitoring: the MobiHealth system. *Journal on Information Technology in Healthcare,* vol. 2, no. 5, pp. 365–373,2004.
5. Venkatasubramanian, K. K, Banerjee, A., Gupta, S.K.S. EKG-based Key Agreement in Body Sensor Networks, *In Proc. of 2nd Mission Critical Networks Workshop, IEEE INFOCOM workshops,* Phoenix, AZ, April 2008.
6. Ali, A., Khan, F. A. An Improved EKG-Based Key Agreement Scheme for Body Area Networks. *In Proc. of International Conference on Information Security & Assurance*, Miyazaki, pp. 298-308, 2010.
7. Mayrhofer, R. The candidate key protocol for generating secret shared keys from similar sensor data streams. *In Proceedings of the 4th European conference on Security and privacy in ad-hoc and sensor networks (ESAS'07)*, Berlin, pp. 1-15, 2007.
8. Mayrhofer, R. Gellersen,H. Shake well before use: authentication based on accelerometer data. *In: Proceedings of the 5th international conference on Pervasive computing (Pervasive'07)*, Berlin, pp. 144-161, 2007.
9. Ali, A.,Irum, S.,Kausar, F., Khan, F.A. *A* cluster-based key agreement scheme using keyed hashing for Body Area Networks. *Multimedia Tools and Applications* vol. 66, pp.201–214, 2013.
10. Ali, A., Khan, F.A. Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications. *EURASIP Journal on Wireless Communications and Networking,* vol. 2013, no. 1, pp. 216,2013.
11. Venkatasubramanian, K.K., Gupta, S.K. S. Physiological value-based efficient usable security solutions for body sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, vol. 6, no. 4, pp.1-36, July 2010.
12. Marinelli, E.E. Hyrax: cloud computing on mobile devices using MapReduce. Masters Thesis, Carnegie Mellon University, 2009.
13. Vmware healthcare: http://www.vmware.com/solutions/industry/healthcare/virtualization-cloud.html (last accessed 11-12-2012).
14. Zhu, W., Li, S. Cloud-based Pervasive eHealth Online Services: http://www.msra.cn/eHealthworkshop/download/Wenwu_Zhu.pdf (last accessed 11-12-2012)
15. Dossia Consortium 2006: http://www.dossia.org/ (last accessed 11-12-2012)
16. Intel Platform Security Division. The Intel random number generator. *Intel technical brief*, 1999. Retrieved from http://citeseer.ist.psu.edu/435839.html (last accessed 11-12-2012)
17. Marsaglia, G. DIEHARD Statistical Tests. Florida State University.
18. Brown, R. G. DIEHARDER: A Random Number Test Suite: http://www.phy.duke.edu/~rgb/General/dieharder.php
19. Waqar, A., Raza, A., Abbas, H., Khan, M.K. A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata. *Journal of Network and Computer Applications*, Volume 36, Issue 1, Pages 235-248, January 2013.
20. NHS Connecting for Health: http://www.connectingforhealth.nhs.uk/systemsandservices/data/nhsdmds/dmd (last accessed 11-12-2012)