ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

A Cloud Based Privacy Preserving Healthcare Framework using Fuzzy Extractor for Wireless Body Area Networks

[1]Nivetha Shri, M. and [2]Aasha, M.

[1]PG Scholar Dept. of CSE, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India.
[2]Assistant professor Dept. of CSE, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India

ARTICLE INFO

Article history:
Received 28 January 2015
Accepted 25 February 2015
Available online 6 March 2015

Keywords:
Wireless Body Area Network (WBAN), Data Security, Cloud Computing, Electronic Medical Records, Hashing, Fuzzy Extractor

ABSTRACT

Privacy issue is an important security problem in body sensor networks, and key negotiation method is the foundation to address the problem. In the paper, we first present a new fuzzy-extractor-based key negotiation method that not only enlarges the option of physiological signals to produce shared keys, but also can resist a new attack based on ultra wide band technology. Analyses show the new key negotiation method is suitable to body sensor networks. A fuzzy extractor addresses both error tolerance and non-uniformity. Multi biometric based key generation scheme is used to secure the inter-sensor communication. Patient's original data will be preserved and medical records are stored securely in the hospital community cloud. The evaluation and analysis shows that the proposed multi-biometric based mechanism provides significant security measures due to its highly efficient key generation mechanism.

To Cite This Article: Nivetha Shri, M. and Aasha, M., A Cloud Based Privacy Preserving Healthcare Framework using Fuzzy Extractor for Wireless Body Area Networks. ***Aust. J. Basic & Appl. Sci.,*** *9(10): 93-98, 2015*

INTRODUCTION

Wireless body area networks (WBANs) are becoming more popular due to the advancement in several current technologies. In health care services, the large number of monitor data in WBANs is a major issue. One of the major issues in WBANs is energy, low memory and communication. For real time processing large storage structure and high performance computing should be accessible and also information analysis in online and offline (Farukh Salaam, 2014). Cloud is the latest paradigm which is used as a distributed storage via the internet. It is step by step turning into a promising technology, which software services and data storage in a virtualized manner at less cost (Wang, X., 2013). The confidentiality of the patient's medical records is major issue when patients use business cloud servers to store their medical records because it can be access the patient's data by unauthorized person. To assure the patients management over access to their own electronic medical records, this technique to encrypt the files before outsourcing. The goal of the proposed work is given as follows:

a) The health monitoring systems have to be either no fixed infrastructure systems or no lacking of ubiquitous nature of communication with plug-n-play capabilities.

b) The physiological value-based key agreement schemes should be based on a multiple biometric value and hence can improve sufficient randomness and key length.

Our work presented can be provided based on a cloud platform, where the health of patients can be monitored securely by using sensors implanted on the human body, as well as the privacy of patients' sensitive data can be kept securely. The main objective is to develop intelligent decision support systems within the medical domain for improving clinical activities. The main aim of this work is to develop an effective secure ubiquitous architecture for a cloud-based mobile healthcare system with high reliability and easily deployable cloud based health monitoring system.

In order to achieve this goal in this work, a secure key management method in cryptography is proposed for cloud enabled WBAN. In cloud based WBANs, we use ECG, EEG, EMG and Blood Pressure signal to generate pair wise keys. The highly dynamic nature can produces time-variant PV (i.e., ECG and EEG). The generated pair wise keys in EKG using Keyed-hashing message authentication code (HMAC-MD5) and it ensures the authenticity, confidentiality and integrity of the EEG and ECG Feature vectors (FV). Using Hybrid Discrete wavelet transform (DWT) and Discrete Cosine Transform

Corresponding Author: Nivetha Shri, M., PG Scholar Dept. of CSE, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India
E-mail: nivesrib2@gmail.com

(DCT)extract the features to form FV from ECG and EEG signals. 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 mobile based communication. The remainder of the research work is represented as follows: The related work is presented in section 2 and section 3 the enhanced multi biometric based scheme is explained. In section 4 the results are described and the conclusion and future work is described in Section5.

Related Work:

J. Liu, Q. Wang, and B. Zeng (2013) discussed the WBANs have restricted energy resources and limited network capacity, memory, and computation, but the real-time processing and data storage in WBANs need more powerful computing capability, system reliability, and reasonable storage infrastructure for online and offline data analysis. Beyond that, it is too expensive that the medical systems rely only on their data centres to store or process data.

M. Chen, T. T. Kwon, L. Yang (2014) presented the cloud computing is poised to become an emerging and promising technology. It is a model for conveniently accessing a shared pool of computing resources, which plays a significant role in limitless functionality and services for resilient Internet computing, broad network access, secure storage, and information sharing in a scalable at low cost.

Chowdhury *et al* (2011) analysed and examined the applications that cloud computing gains access to data sharing and collaboration and provided optimum healthcare with the help of cloud computing.

Xiao Yun Peng (2008) discussed the web engine and distributed website blocks management infrastructure based on cloud computing, and processing the power of cloud to parser HTML page.

C. Zou, S. Ulla, M. Zhou, and X. Wang (2013) designed the cloud-enabled WBANs architecture to improve the ambulatory monitoring of healthcare services on three types of scenarios (home, hospital, or outdoor environment) using different mobile cloud computing. QoS improvement in cloud-enabled WBAN platforms includes the development of temperature, cross-layer routing protocols, resource allocation on cloud, and data privacy and security mechanisms to support effective data transmission to the clouds.

A. Bahga and K. Marinetti (2013) discussed the electronic health record (EHR) based on cloud systems, cloud health information system technology architecture (CHISTAR), was presented to achieve the semantic interoperability; two key functions about the data storage and integration engine architecture were designed. And the data integration engine architecture of CHISTAR makes the system get more effective and efficient patient care from disparate data sources.

Enhanced Multi-Biometric Based Scheme Methodology:

Multi-biometric scheme uses the combination or fusion of two biometrics that involve two physiological values such as 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 detail of the scheme is illustrated in Fig.3.1.

a. Pre-processing and Feature Extraction:

First, R points and then RR intervals are detected for each ECG and EEG recording. The RR signal correction takes place to eliminate errors in ECG and EEG, which might still be present in the RR interval series, such as ectopic beats, artifacts, and outliers. If any RR interval is shifted from a previous RR interval by more than 0.3 ms, it is assumed to be erratic and is then replaced by the average of its previous and the next RR intervals. The unwanted noise of the heart bio signal should be removing. Band pass filter is used in ECG between 0.06HZ-100Hz to remove the artifact, and to eliminate line noise. Feature extraction is completed by Hybrid DWT-DCT.

Discrete Wavelet Transform (DWT):

Analyses the signal in DWT at various resolution through the decomposition of the signal into several frequency bands and it utilizes the functions are $\Phi(t)$and$\Psi(t)$, with the low and high pass filters (Wen-Chung Kao, 2012). The two functions are performed because the weighted sum of the scaled and shifted version of the scaling function itself:

$$\Phi(t) = \sum_n h[n]\Phi(2t-n) \quad (3.1)$$

$$\Psi(t) = \sum_n g[n]\Phi(2t-n) \quad (3.2)$$

Here, $h[n]$ and $g[n]$is the two half band low and high pass filter. Decomposing the signal and image into approximation of hierarchical set is contained in wavelet analysis. Daubechies D4 wavelet is chosen and it resembles a heartbeat waveform. The 23 coefficients are selected on the morphology preservation criterion, and then the another task is to form Feature vectors.

Discrete Cosine Transform (DCT):

In this discrete cosine transform applied for feature extraction has the advantage of reducing the machine. The transform is applied to the individual ECG beats and the coefficients of the frequency in DCT are evaluated as follows:

$$Y[u] = G[u]\sum_{i=0}^{N-1} y[u]\frac{\pi\cos(2i+1)u}{2N} \quad (3.3)$$

Where N is the length of the signal $y[i]\ for\ i = 0, 1\ldots(N-|m|-1)$. AC/DCT technique $y[i]$ is the correlated Electrocardiogram. $G[k]$Is given from:

$$G[k] = \begin{cases} \sqrt{\frac{1}{N}} & k = 0 \\ \sqrt{\frac{2}{N}} & k \neq 0 \end{cases} \quad (3.4)$$

In representation permits the lower dimensions in DCT and the way, close to zero elements of the frequency representation can be discarded. The important coefficients are reduced eventually. This transform offers a powerful feature extraction mechanism. The individual heartbeats are measured to 1- dimensional DCT. The 30 DCT coefficients were selected again based on the morphology preservation with a metric of PRD and also the energy content.

$$PRD = \frac{\sqrt{\sum_N (\hat{x}_i - x_i)^2}}{\sqrt{\sum_N (x_i)^2}} \quad (3.5)$$

$\hat{x}$ Is reconstructed ECG and x is original ECG signals. Thefeature vectors are generated from two signals in quantization phase and it divided into 20 blocks every containing 16 coefficients for ECG and same for EEG, then the blocks quantized into a binary stream. These blocks are exchanged by applying keyed hashing (HMAC-MD5).

b. Fuzzy Extractor based key negotiation scheme:

In this, a fuzzy negotiation structure designed as follows: The structure consists of a pair of procedures:" Trans" and "Rec". In the initialization of the structure, each sensor node is preloaded a secret K that is divided into two keys,K_0 andk_1 with$|k_0| = |k_1| = l$. In addition, each sensor node is assigned with a keyed one-way pseudo-random function $F_k(\cdot): \{0,1\}' \rightarrow \{0,1\}'$ with$|k| = l$, an error-correcting function $Dec(\cdot)$ belonging to a selected error-correcting code *C* and a function $f(\cdot): \{0,1\}' \times \{0,1\}' \rightarrow \{0,1\}'$and that satisfies $z = f(x,y) \Rightarrow y = f(x,y) \Rightarrow x = f(z,y)$.

Procedure "Trans":

Collecting a biometric value from a pointed physiological signal, and encoding it into a binary value $\|w\| = l$; Selecting a code word c from the error-correcting code *C*, and computing the relationship between c and $w: v = f(w,c)$; Generating an open random value r with $|r| = l$, and then using $F(\cdot)$ to hide $v: u = v \oplus F_{k_0}(r)$; Finally, deriving the shared key: $k_{shared} = F_{k_0}\left(F_k_1(w \oplus r)\right)$where $\oplus$ is bitwise XOR operation), and outputting the commitment corresponding $w: P = < u, r, F\_k_0(u\|r\|c)$("||" denotes concatenation operation)

Procedure "Rec":

Collecting the same kind of biometric value, and encoding it into a binary value $w'$with $w' = l$; Using the pre-deployed key $k_0$to recover the relationship Encoding $v: v = u \oplus F_{k_0}(r)$; Encoding $w'$and v into $c^*: c' = Dec(c^*)$. If $F_{k_0}(u\|r\|c) = F_{k_0}(u\|r\|c')$, the correction is successful, and wcan be recovered as:$w = f(v,c)$. And then, the shared key can be reproduced as: $k_{shared} = F_{k_0}\left(E_{k_1}(w \oplus r\right.$.

Otherwise, If $F\_k_0(u\|r\|c) \neq F_{k_0}(u\|r\|c')$, it means the failure of shared keys' negotiation [10].

c. 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. Every node compares the received blocks. Then the received blocks are extract the common blocks. The extraction is performed by constructing a matrix, wherever every element of the matrix represents Hamming distance between the i th block and jth block of Sensor. 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.

The two values of ECG and EEG signals are used. The signals used for the generation of keys. When sensor node 'a' (SN_a) wishes to communicate with sensor node 'b'(SN_b), SN_a sends hello message with its ID and$m1$. Nonce is an integer value included to check the transaction freshness. $m1: \forall SN_a \in \{SN\} : SN_a \rightarrow SN_b :$
$(ID_{SN_a}, Hello, nonce)$

After receiving *m1*, theSN_b calculates pair-wise keys ECG, EEG and ID of SN_aandSN_b,

$$K1_{SN_a,SN_b} = HMAC\ \ Calculated\ ECG\ values \left\| ID_{SN_a} \right\| ID_{SN_b}$$
$$K2_{SN_a,SN_b} = HMAC\ \ Calculated\ EEG\ values \left\| ID_{SN_a} \right\| ID_{SN_b} \quad (3.6)$$

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

$$m2: \forall SN_b \rightarrow SN_a : ID_{SN_b}, EK_{SN_a,SN_b}\{ID_{SN_b}, Data\},\ MAC_{K_{SN_a,SN_b}}(ID_{SN_b}, data, nonce) \quad (3.7)$$

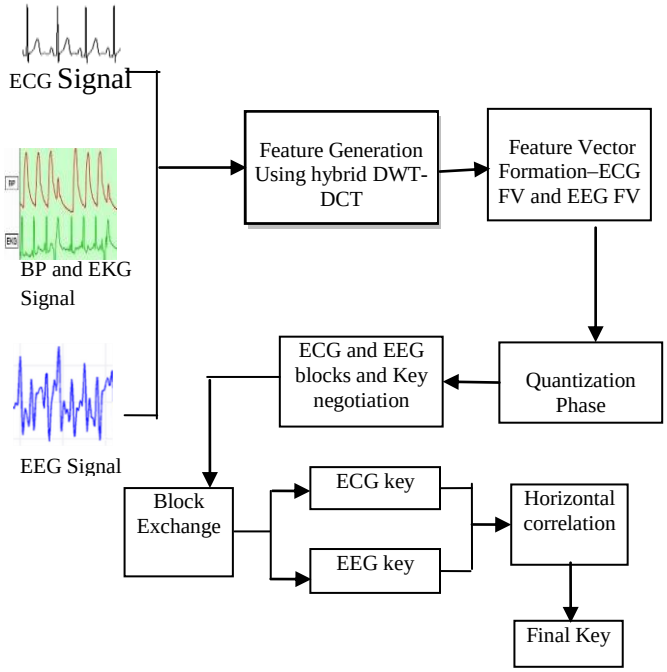

Fig. 3.1: Enhanced Multi-Biometric based key generation process.

SN_a Upon receiving *m2*, decrypts it with K_{SN_a,SN_b} and compares ID_{SN_b}, received ECG and EEG values on SN_a. Ensure the two parties have generated the same key. Also the message authenticity is verified by SN_a through *MAC* verification with K_{SN_a,SN_b}.

d. Cloud based EMR:

EMR provide quality healthcare and it is important that medical personnel. The concerned physicians should access the EMRs. The ubiquitous access are provided by storing the EMR over the cloud. The first work of the proposed framework focus on the security of sensor communication on WBANs and the second work is to focus on the privacy of cloud-based patient's medical data storage.

The privacy of patient's medical records may be endangered if securely communicated medical information is not stored in a very secure manner. To make sure to secure the patient's medical data, we have used an adaptation of the cloud user data privacy preservation mechanism based on reconstruction of metadata as presented.

e. Categories of Patient's Data:

The following categories were described of patient's medical data that mobile healthcare system commonly uses:

1. Patient personal data.

i) Patient's ID ii) patient name and gender iii) patient address.

2. Patients' Medical History

i) Unique Medical condition id ii) Medical condition name, iii) Date of diagnosis d) Recommended treatment.

3. Preservation of patients' medical data stored in the database server

Here, the data items identified in single process. It categories into sensitivity parameterization classes of exclusively and partially degree, and non-private as depicted in Fig 3.2.

For reference purposes, the NHS data model and dictionary is used. Using SQL Server 2008 R2, we created a generic database consisting of the data items mentioned above. Using this method, the data classification on the database information followed by the horizontal/vertical table splitting.

Experimental Results:

Most of the security techniques have expressed their cryptographic strength. In terms of number of key bits that an attacker needs to guess in order to break the system. For example, it is partially predictable, if the attacker starts with key material and it indicates the weakness of the security system regardless of the algorithm and protocols used.

If the key of 128 bit contains 16 predictable bits and does not ensure 128-bit protection using AES 128. Then, 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. Example one of the most famous randomness-testing suites is DIEHARD, which is made up of twelve tests.

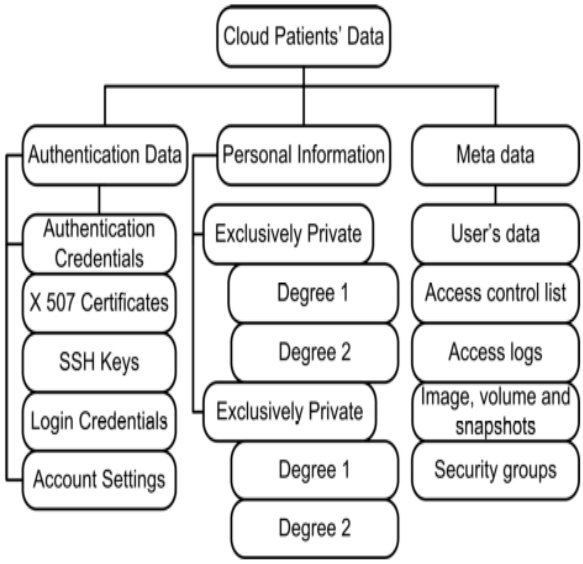

Fig. 3.2: Patients' data sensitivity parameterization of exclusively private and partially private data.

a. Randomness:

To check the randomness, a number of P-value is produced for each statistical test. A P-value is a probability measure to test the statistic larger than the one observed, if the sequence is random. Similarly, tiny numbers indicate a sequence is to be random and the decision rules in the case states that "for a fixed significance value a, a sequence fails the statistical test if it's P-value < a." The sequence sending a statistical test, whenever the P-value = a or fail otherwise and it assumes that a test taken into account failing if it outcomes a P-value less than or equal to 0.0001 or greater than (>) or equal to 0.999(=0). It results in a 95% confidence interval of P-values. During this work the keys are calculated for 25 subjects. The EEG and ECG data are taken from MIT physiobank and UBUNTU Enterprise Cloud (UEC) Eucalyptus database. The die harder testing is applied on the keys generated from the BP, EKG, EEG and ECG patient's data of the 25 subjects. Table 1 shows the average 25 subject keys of P-value and their many assessments. It's evident from Table 1 that P-values is violating the condition.

Table 1: Die harder testing result.

Test Name	Ntup	t-samples	p-sample	Average P-value of 25 keys	Assessment
diehard_birthdays	0	100	100	0.653760029	OK
diehard_operm 5	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_dna	0	2097152	100	0.49437631	OK
diehard_count_1s_byt	0	256000	100	0.570959702	OK
diehard_parking_lot	0	12000	100	0.611109984	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

b. Entropy:

Entropy is the quantitative measure of disorder or randomness in a system. High entropy means higher security. Fig.3 shows the entropy comparison of the proposed method with ECG and EEG based scheme. The proposed multi-biometric based scheme has high entropy as compared to both ECG and EEG based schemes and multi-biometric based scheme, which shows more randomness on average. Moreover, the length of the generated keys is 128 bits, while the proposed enhanced multi-biometric based scheme produces 320 bits. 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 million people each make a different guess. With the same effort, the probability of success to decreases for each additional key bit.

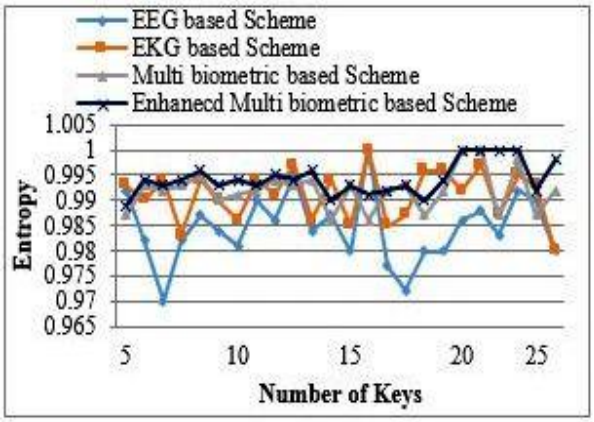

Fig. 4.1: Entropy comparison of keys generated.

Conclusion and Future Work:

The paper presented a cloud-based secure framework for mobile healthcare system in WBANs to improve the security in sensor communication and preserving the patient's data. The enhanced work is to generate the common key for sensor communication using Hybrid DWT-DCT feature extraction. The enhanced framework is to evaluate the security and the results indicate that the enhanced system is a viable solution for the next generation mobile healthcare systems. The work is to unique and it provides a complete cloud-based framework and security solution for a mobile healthcare. Future Enhancement will be on various algorithms for speed optimization and further optimization of the feature extraction and an effective cryptography method.

REFERENCES

Bahga, A. and K. Marinetti, 2013. "A cloud-based approach for interoperable electronic health records (EHRs)," National journal of Biomedical, 17(5).

Chowdhury, S., A. Yadav and N. Garg, 2011. "Cloud computing: future prospect for e-health," in International Conference on Computer Technology.

Farukh salaam, Khana, Aftab, B., 2014. **"**A cloud-based healthcare framework for security and patients data privacy using body area networks", International Workshop on Communications and Networks, Science Direct.

Kwak, K.S., 2012. "An efficient certificate less remote anonymous authentication scheme for wireless body area networks, "International Conference on Communications.

Liu, J. and S. Kwan, 2010. "Hybrid security mechanisms for wireless body area networks," Conference on Ubiquitous and Future Network.

Liu, J., Q. Wang, 2013. "Towards key issues of disaster based on wireless body area networks," KSII, 7(5).

Marinetti, V.K., 2013. "A cloud-based approach for interoperable electronic health records (EHRs)," published in Biomedical and Health Informatics.

Rajesh, A. Ghol, 2007. "Performance Evaluation of ECG Feature Extraction Techniques for Artificial Neural Network Based Classification", IEEE.

Ulla, S., X. Wang, 2013. "Cloud-Enabled body area networks for pervasive healthcare, "National conference on Computer Technology, 7.

Wang, X., 2013. "A Framework of Mobile Video Streaming and Efficient Social Video Sharing in the Clouds," IEEE.

Wen-Chung Kao, 2012. "Detection of cardiac disease in ECG using adaptive feature extraction and modified support vector machines", Workshop on computational intelligence.

Xiao, Y., T. Yang, Q. Li, 2008. "A new wireless web access mode based on cloud computing," IEEE.

Yang, L., 2013. "Cloud based framework of adaptive video streaming and efficient social video sharing in the clouds," IEEE.