An efficient method for Secure ECG Feature Based Cryptographic Key Generation

S.Premkumar, J.Mohana

Abstract- A novel method to generate ECG feature oriented cryptographic keys is proposed. Due to the advantage of the uniqueness and randomness properties of ECG's main feature, this feature is achieved. As the production of key depends on four reference- free ECG main features, Low-latency property is obtained. These features are obtained in short time. This process is referred as (SEF)-based cryptographic key production. The SEF has the following features like: 1) identifying the appearance time of ECG's fiducial values by means of Daubechies wavelet transform to calculate ECG's main features conversely; 2) A dynamic method is used to denote the best quantity of bits that can be obtained from the main ECG feature, which consists of PR, RR, PP, QT, and ST time periods; 3) Generating cryptographic keys by the ECG features extracted in the method mentioned above and 4) Making the SEF method as strong with cryptographically secure pseudo-random number generators. Fibonacci linear feedback shift register and recent encryption traditional algorithms are executed as the pseudo-random number generator to improve the safety stage of the produced cryptographic keys. This method is executed to 239 subjects' ECG signals consisting of normal sinus rhythm, arrhythmia, atrial brillation, and myocardial infraction. Normal ECG rhythms have slightly better randomness when compare with the abnormal.The output results proves that the SEF method is faster than the present existing key production methods. It produces higher security level when compared to existing methods.

Key word: Cryptographic key generation, electrocardiogram, bio-electrical signal, body area network.

I. INTRODUCTION

Body Area Network (BAN) is a key technology for healthcare systems [1]. It monitors the patient efficiently eventhough the patient is in remote location. BAN has medical sensors which contains patients health related data. As medical sensor nodes share out with patients' vital health data, their communication safety is mandatory [2]. Lack of strong safety features may affect the privacy of the patients and opponents can potentially control actual health data resulting in incorrect analysis and medicine [3].

Medical sensors depends on cryptography to safe their interactions [4]. Proper application of cryptography necessitates the usage of secure keys and key production methods. Key generation approaches that are proposed for generic wireless sensors are not directly applicable to tiny sensors used in BANs as they are highly resource-constrained and demand a higher security level [5]. Key generation in sensor networks generally requires few standards pre-deployment.

Revised Manuscript Received on October 10, 2019

Correspondence Author

S.Premkumar, Assistant Professor, ECE, Saveetha School of Engineering, SIMATS, Chennai, India. premkumar@saveetha.com

J.Mohana, Associate Professor,ECE, Saveetha School of Engineering, SIMATS, Chennai, India. mohana@saveetha.com

Traditional key production methods may potentially engage reasonable calculations as well as latency throughout network or any following adjustments, as their necessity for pre-deployment. Biometrics are normally considered as the only resolution that is lightweight, demands less resources, and certainly can recognized authenticated topic in BANs [4], [6] [8]. Through the creation of strong key production methods, the safety of medical sensors can be provided in a plug-n-play way in which neither a net-work is set nor a key pre-distribution method is wanted. Cryptographic keys can be produced within the network on the y by means of biometric, the information obtained through medical sensors. Moreover, key call back and renewal are carried on routinely when required. The range of a biometric to be used to generate cryptographic keys relies on the strength of medical sensors on getting a biometric data. The chosen key points should follow the constraints [4]: (i) it should be varying for the subjects. (ii) that it should change for the same person at different time periods. (iii) it should be cryptographically not a constant. A low degree of randomness provides an attacker to get a patient's cryptographic key and predict their medical data. (iv) It should be measurable from all the subjects.

The ECG is a noninvasive tool used to record the electrical manifestation of the contractile and relaxation activity of the heart. Nobel laureate, Willem Einthoven, was the first who had recorded the ECG in 1903. It can be recorded with the surface electrodes placed on the limbs and chest. ECG devices use varying number of electrodes ranging from 3 to 12 for signal acquisition while the system using more electrodes exceeding 12 and up to 120 is also available. Each normal cycle of an ECG signal contains P, QRS, and T waves (for instance see Figure 1). The P wave is a representation of contraction of the atrial muscle and has duration of 60–100 millisecond (ms). It has low-amplitude morphology of 0.1–0.25 millivolt (mV) and usually found in the beginning of the heartbeat. The QRS complex is the result of depolarization of the messy ventricles. It is a sharp biphasic or triphasic wave of 80–120 ms duration and shows a significant amplitude deflection that varies from person to person. The time taken for ionic potential to spread from sinus node through the atrial muscle and enter the ventricles is 120–200 ms and known as PR interval. The ventricles have a relatively long ionic potential duration of 300–420 ms known as the QT interval. The plateau part of ionic potential is of 80–120 ms after the QRS and known as the ST segment. The return of the ventricular muscle to its resting ionic state causes the T wave that has an amplitude of 0.1–0.5 mV and duration of 120–180 ms. The duration from resting of ventricles to the beginning of the next cycle of atrial contraction is known as TP segment which is a long plateau part of negligible elevation.

Present ECG- oriented cryptographic keys are normally produced by means of (IPI) keypoints of an ECG signal [5], [7], [2] [6]. It is calculated from two consecutive R peak points .

In this article, we propose a new approach, called Several ECG Feature (SEF) based cryptographic key generation. The SEF approach improves the key production implementation execution over-head of the present and the previous methods, while conserve the obtained high safety stages. The proposed method is executed to both normal and abnormal ECG signals. Three important points are discussed in this article.

The SEF approach uses 4 main reference-free1 features of the ECG signal (being extracted from every ECG heartbeat cycle) along with consecutive IPI sequences to generate ECG-based cryptographic keys.

To reinforce and improve the safety stage of the method, we combine the SEF key production method with two separate cryptographically secured pseudo random number generators: (i) SEF-PRNG: we strengthened the security level of the SEF method by making use of the Fibonacci-LFSR pseudo random number generator (ii) SEF-AES: The SEF approach is also strengthened by using the AES algorithm in counter style. This method make use of the SEF key generation method as the seed generator for the AES algorithm.

We calculate the efficiency of the SEF, SEF-PRNG, and SEF-AES methods by simulations in various terms and implementation time on real ECG data from 239 subjects with various heart health conditions.

The remainder of the paper is scheduled as below: in Section II, the associated work are described. In Section III, bio-electrical signals and ECG properties are described. Section IV describes the suggested cryptographic key production methods using the ECG bio-electrical signal. Key production implementation time are presented and examined in Section V. Atlast, Section VI concludes the article.

II. BIO-ELECTRICAL SIGNALS AND ELECTROCARDIOGRAM (ECG) PROPERTIES

Bioelectrical signals are very low amplitude and low frequency electrical signals that can be measured from biological beings, for example, humans. Bioelectrical signals are generated from the complex self-regulatory system and can be measured through changes in electrical potential across a cell or an organ. The bioelectrical signals of our interest are in particular, the electrocardiogram (ECG) and the electroencephalogram (EEG). An ECG measures the electrical manifestation of the ionic potential of the heart while an EEG measures the electrical activity evoked along the scalp of the brain. The ECG and the EEG are recorded using standard equipments in the noninvasive fashion. The researchers of multiple disciplines have shown their greater interest in analyzing the ECG and the EEG to understand the high level features an individual is producing. However, the interdisciplinary analysis of bioelectrical signals not only helps in assessing the individuals state of health but also it suggests that the bioelectrical signals can be used as the candidate of biometrics for identity verification.

ECG is a rhythmically repeating and quasi-periodical signal which is synchronized by the function of the heart, and the heart execute the production of bio-electrical activities. It is the electrical demonstration of the contractile process of the heart that is measured at the chest level by recording signal stages from numerous electrical leads appended to the patient's skin. ECG has been mainly used in different medical applications. For example, it has been used to find cardiac diseases [2],[8]. Nowadays, ECG has been broadly used for biometric identification [5].

ECG signals has a set of positive and negative waves. Each signals recorded from each leads gives various datas. A heartbeat cycle has waves called P, QRS and T that can be identified by means of various leads for recording. The first peak, the P wave, is a small upward wave, which mentions atrial depolarization. Approximately 165 ms subsequent to the onset of the P wave, the QRS wave is generated by ventricle depolarization. The ventricular T wave in the ECG denotes the levels of re-polarization of the ventricles. An important changes about the ECG anatomy happens from birth to adult stage. The amplitude of the P wave does not varies to a large extent considerably meanwhile the amplitudes of the S and R waves minimized from childhood to adolescence. A progressive changes of the T wave from childhood to adolescence has also been presented by Dickinson [7]. Apart from that, the QT interval will reduce when compare to the remaining intervals when the heart rate rises. This change can be corrected by normalizing the QT interval according to the heart rate. The dependence of the QT interval to heart rate can be modified using Bazett's QT interval changes for which the modified QT interval is considered as to be somewhat static for many years [8]. QT interval normalization is not used in this article. Aging does not disturb any gender-based variances in cardiac electrophysiological factors in adults. Conversely, stress, anxiety, and physical exercise can modify the Heart Rate Variability (HRV) and morphology [6].

III. CREATING CRYPTOGRAPHIC KEYS USING ECG BIO-ELECTRICAL SIGNAL

Medical sensors depends on cryptographic keys to safe end-to-end communications or encrypt/decrypt messages that are required to be communicated among the sensors and health caregivers [7], [9]. Solutions based on cryptographic keys produced from single ECG signals are best matching for small medical sensors as these solutions are lightweight and wants reduced resources [8]. By creating strong and effective cryptographic key production methods, the safety of medical sensors can be provided in a plug-and-play style in which where neither a system formation nor a key pre-distribution mechanism is required. Cryptographic keys are produced in the network on the y via the usage of ECG data received by medical sensors when and as required. The created keys can be used, for example, in end-to-end interactions to safely encrypt/decrypt patients' medical data being exchanged among sensors and health caregivers [7], [9]. The keys can also be utilized to authenticate peers and reliability of the transmitted messages in BSNs [10] [2]. A strong cryptographic key produced within a BAN can also block probable attack conditions counting passive datas and message damages, replay attacks and Denial of Service attacks (DoS).

Fig. 1 shows first step to create ECG-based cryptographic keys and is referred as raw ECG data acquisition from subjects. The obtained ECG data comprises of information about the heart rate, morphology, and rhythm being measured by keeping a group of electrodes on body regions such as neck, chest, legs, and arms. Once collected, raw ECG data required to be created for additional analysis. Study of the ECG signal can be divided into two main steps by functionality: ECG signal pre-processing and keypoints extraction.

A. ECG SIGNAL PRE-PROCESSING

The purpose of pre-processing is to remove all these noise and makes ECG for proper functioning. The shape and pattern of waves in ECG signals are differing from each other. The main category of waves includes P-waves, QRS complex and T-waves. The QRS complex is the most characteristic waveform of the ECG signals. The QRS duration indicates how fast the ventricles depolarize. The normal QRS is < 0.10 seconds.

B. ECG SIGNAL FEATURE EXTRACTION

ECG keypoints extraction is a technique where the main features of a sample are obtained. The main purpose of the ECG feature extraction process is to choose and preserve relevant data of an original signal. Present ECG feature extraction tecniques are categorized into two major classes, fiducial techniques and nonfiducial techniques. In fiducial approaches, points of interest together with P, Q, R, S, and T inside a single heart-beat waveform (i.e., local minimum or maximum or amplitude diversity among successive fiducial points) are used. Algorithms on non- fiducial points do not use peculiar values to produce the feature set. Non- fiducial methods get discriminative data from an ECG signal. They spreads the calculational overhead and wants more information for learning that are commonly limitless [4]. High dimensional datas can corrupt the classifier's performance.

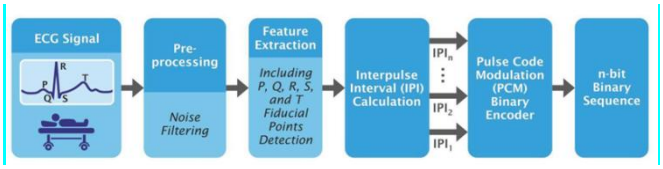

Fig 1. Block diagram of ECG signal analysis and n-bit binary sequence generation using consecutive IPI sequences

article, a fiducial-based algorithm is used to execute the ECG feature extraction task. Discrete Wavelet Transform (DWT) is utilized to get the necessary features of each ECG signal.

The DWT is a widespread method for frequency and time analysis. Wavelet transformation is a linear function which decays a signal into elements at various scales. Let $\psi(t)$ be the real $\in L^2(R)$. The $\psi(t)$ function is expressed as a wavelet, if and only if, its Fourier transform meets the below equation [3]:

$$\int_{-\infty}^{\infty}\left(\frac{|\hat{\psi}(\omega)|^2}{|\omega|}\right) = F_{\psi} < \infty \qquad (1)$$

This tolerability segment measures that:

$$\int_{-\infty}^{\infty}\psi(t)dt = 0 \qquad (2)$$

This means that zero. Let x (t):

$$\psi_x(t) = \frac{1}{\sqrt{x}}\psi\left(\frac{t}{x}\right) \qquad (3)$$

be the expansion of $\psi(t)$ through a scale factor of x > 0. In the expression, $\frac{1}{\sqrt{x}}$ is used for energy standardization. px Wavelet transform uses a set of wavelets with limited time limit in order to crumble a signal. Hence, the wavelet transform of a function $f(t) \in L^2(R)$at scale x and position l can be modified as:

$$W_f(x, l) = \frac{1}{\sqrt{x}}\int_{-\infty}^{\infty} f(t)\psi^*\left(\frac{t-l}{x}\right)dt \qquad (4)$$

where x denotes the scale factor, l is the translation of $\psi(t)$ and * indicates the composite conjugate of $\psi(t)$.

The nature of ECG signals permits one to widen the principal functions formed by shifting and scaling of a single prototype function indicated as the mother wavelet. Different wavelet families including Haar and Daubechies present in the literature and are used to extract the key values present in the ECG signal. Haar wavelet is the normal type of wavelets. Its easy to understand and easy to calculate, meanwhile few data cannot be stored through it. Daubechies wavelet is complex when compare to Haar and has more calculational complexity. The advantage of it when compare to haar wavelet [8] is its reliability.

This article discusses the usage of Daubechies wavelet transform for the keypoint extraction from ECG signal. Daubechies DB4 wavelet is selected because of the resemblance of its scaling property to the ECG signals shape[4]. R peak detection is the keypoint of feature extraction and the other fiducial values are obtained considering the location of the R peak values. DB4 possess four wavelet and scaling function coefficients. wavelet function is used in all the stages of the wavelet transform. If the dataset has MN values, the wavelet function are executed in order to find MN =2 differences which informs about the modifications in the data. The wavelet values are stored in the upper half of the MN element input vector. The scaling and wavelet functions are calculated by considering the inner output of the coefficients and four data points. The scaling function coefficients (h) and the wavelet function coefficient (g) points can be denoted as:

$$h_0 = \frac{1+\sqrt{3}}{4\sqrt{2}} = -g_3 \qquad h_1 = \frac{3+\sqrt{3}}{4\sqrt{2}} = g2$$
$$h_2 = \frac{3-\sqrt{3}}{4\sqrt{2}} = -g_1 \qquad h_3 = \frac{1-\sqrt{3}}{4\sqrt{2}} = g_0 \qquad (5)$$

Daubechies DB4 scaling (a) and wavelet (c) functions can be mentioned as:

$$a_i = h_0S_{2i} + h_1S_{2i+1} + h_2S_{2i+2} + h_3S_{2i+3}$$
$$c_i = g_0S_{2i} + g_1S_{2i+1} + g_2S_{2i+2} + g_3S_{2i+3} \qquad (6)$$

Each level in DB4 stage calculates a scaling function point and a wavelet function point. The index i is increased by two for each stage, and new scaling and wavelet function points are calculated.

It should be denoted that a normal ECG signal has observable P waves, QRS complex and T waves (See Fig. 2). The heart rate for a normal adult varies among 60-100 beats per minute. The time period for the recording are also within normal ranges. However, cardiac abnormalities are considered in many databases. These abnormalities normally happens when patients are suffering from particular cardiovascular diseases, such as myocardial infraction, super vascular arrhythmia. Even normal subjects' ECG signals may have some variations due to anxiety, stress, and physical exercises. In these scenarios, the peak values of some waves may not be detectable within one heartbeat using the most common order of the Daubechies wavelet, that is DB4. Hence, the intended main ECG features cannot be extracted and computed. In such scenarios, it is found that DB6 and DB9 are the best candidates among different Daubechies scales to extract features from abnormal types of ECG signals [8], [5]. This happens because of these Daubechies scales maintain few details and squaring of the balance signal approximation which leads to the flexible identification of the R peak points. After the R peak points of an abnormal ECG signal are identified, other key peak points are also identified with respect to the location of R. Based on the above points, the optimum selection of the DB scales depends on the usage and the category of ECG signals required to be used. When the Daubechies wavelet transform cannot able to extract the keypoints from main features of an ECG signal, another scale may offer more detail and good results. Thus, there will be reduced probability that the effectiveness of the ECG-based crypto-graphic key production methods is disturbed. Accuracy and flexibility is more effective with the higher Daubechies scales. Meanwhile, the higher Daubechies scales demands more coefficients and processing time.

C. QRS COMPLEX AND R PEAK DETECTION

The QRS identification are measured by using Pan Tompkins algorithm. It has low pass filter, high pass filter trailed by derivative, squaring and integration part. Slope of the wave details are obtained by derivative stage. The squaring function is carried on to increase the derivative output. This creates all data values as non negative. The data about both the width and slope of the wave is got from the output of the moving integration stage.

D. P AND T PEAKS DETECTION

To determine P and T-waves from collapsing samples we use Partially Collapsed Gibbs Sampler (PCGS). The output of PCGS is then applied to Wave Indicator Estimation, amplitude estimation and amplitude estimation block. The wave indicator is done by using Local Map A Posteriori (MAP) method. The amplitude estimation is done by using fuzzy theory. The waveform estimation is done by using neural network. Estimated onset and end points are obtained from the P and T-wave delineation division. The calculation of noise variance of the wave is carried on by applying MMSE method.

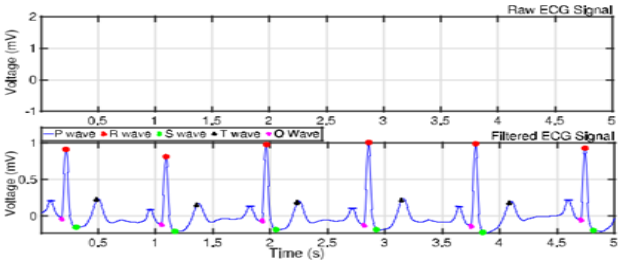

Fig 2. ECG signal and the filtered ECG signal with the key fiducial points marked.

E. PR, RR, PP, QT, AND ST INTERVALS

The PR interval is indicated as the time interval between the onset of the P wave and the onset of the R wave. The RR time period is also expressed as the time elapsed among the nearby R peaks. Heart rate can be found as the reciprocal of the RR interval, that is, the time variations among the two R peak points. The PP interval is denoted as the interval among the adjacent P waves due to atrial depolarization. The PP interval is used to compute the atrial rate. The ST interval is indicated as the interval among the offset of the S-wave and offset of the T-wave. The QT interval is calculated by finding the dissimilarity among the onset of the Q wave and the offset of the T wave. These intervals are used as the key ECG keypoints in this article.

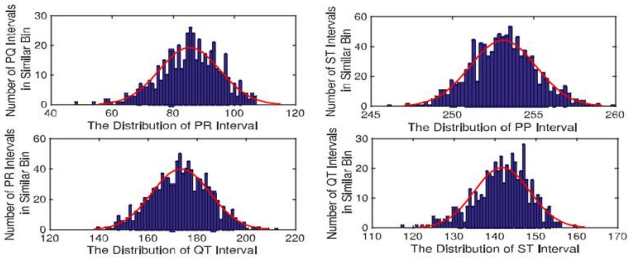

FIG 3. The normal distribution of PR, PP, QT, and ST intervals

In [1], two methods about ECG-based crypto-graphic key production techniques are discussed. It uses singular ECG feature. The first method, IPI-PRNG, depends on a pseudo-random number generator and successive IPI sequences. The second approach, IPI-AES, depends on the AES block cipher in counter mode, using IPI as the seed generator for the AES algorithm. The subsequent presents the suggested cryptographic key generation using many ECG keypoints. The suggested method expands the earlier work by minimizing the key production implementation times and offer high level of safety features. This article follows the fact that to improve the key production implementation times, meanwhile preserving high safety stages, other important keypoints of an ECG signal can be used.

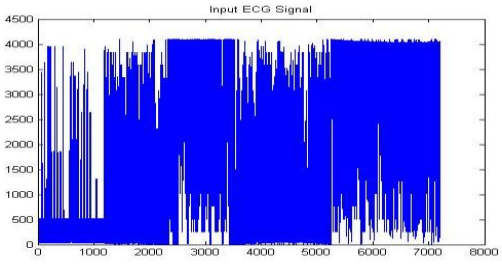

Fig 4. ECG Input Signal

The ECG input signal is shown in figure 5. Golay filter is applied for filtering purpose and its shown in figure.6. QRS waves are extracted as shown in figure.7. Key generation is the next process and is shown in figure 8. Atlast, the signal is encrypted and shown in figure 9.

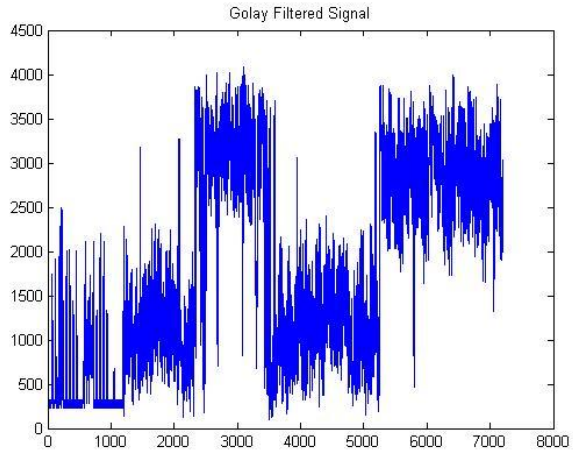

Fig 5. Golay Filtered Signal

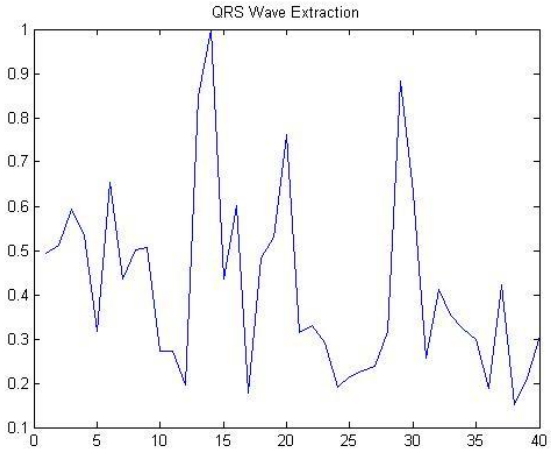

Fig. 6. QRS wave Extraction

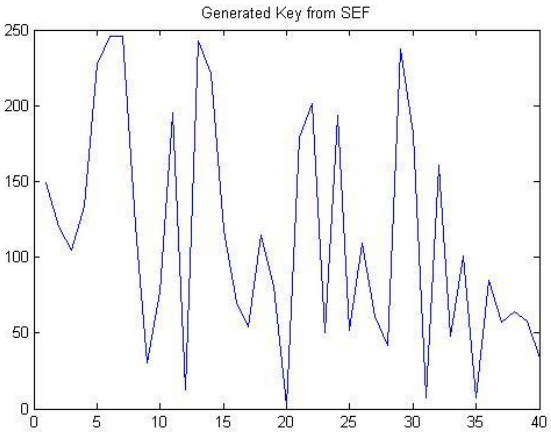

Fig.7. Key Generation

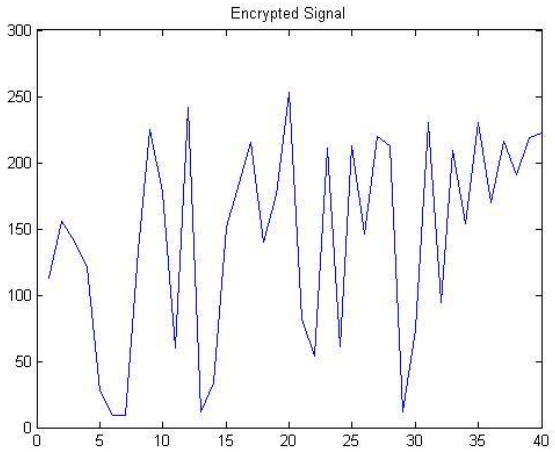

Fig 8. Encrypted Signal

IV. CONCLUSIONS

An efficient method to generate safe ECG feature oriented cryptographic keys is presented. The present key production methods are not directly applicable to BANs. The sensors present in BANs are tremendously resource- controlled and expects a low-latency key production time as well as a high safety stage. To overcome these limitations, a robust key generation method using many ECG values, called SEF is proposed. Our SEF method uses 4 main reference-free ECG values consisting of PR, RR, PP, QT, and ST. A dynamic method is used to indicate the best quantity of bits that can be taken from the ECG values. SEF method is further strengthened by means of cryptographically safe pseudo-random number generator methods. The Fibonacci linear feedback shift register and the AES algorithm are implemented as pseudo-random generators to enhance the safety features of the method. The safety metrics of the produced keys was made in terms of individuality. This method is executed on both the normal and abnormal ECG signals. The output results show that the production method of key provides more safety level when compare to present methods which depends only on singleton ECG values. The result also describes that the normal ECG signals have slightly better randomness compared to the abnormal ones. Cryptographic keys that are produced using the strengthened SEF method provides the entropy of 1. In addition, the reinforced key generation approach has also better P-value NIST pass rates compared to state-of-the-art approaches which rely only on singleton ECG features. The proposed method is more faster than the present IPI-based key production methods.

REFERENCES

1. Qi Lin ; Weitao Xu ; Jun Liu ; Abdelwahed Khamis ; Wen HU ; Mahbub Hassan ; Aruna Seneviratne, "H2B: Heartbeat-based Secret Key Generation Using Piezo Vibration Sensors",18th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN),2019.
2. Guanglou Zheng ; Rajan Shankaran ; Wencheng Yang ; Craig Valli ; Li Qiao ; Mehmet A. Orgun ; Subhas Chandra Mukhopadhyay,"A Critical Analysis of ECG-Based Key Distribution for Securing Wearable and Implantable Medical Devices",IEEE Sensors Journal,2019.

3. Sanaz Rahimi Moosavi ; Ethiopia Nigussie ; Marco Levorato ; Seppo Virtanen ; Jouni Isoaho,"Low-Latency Approach for Secure ECG Feature Based Cryptographic Key Generation",IEEE Access, 2018.
4. Polash Kumar Das ; Fenghua Zhu ; Shichao Chen ; Can Luo ; Prabhat Ranjan ; Gang Xiong ,"Smart Medical Healthcare of Internet of Medical Things (IOMT): Application of Non-Contact Sensing", 14th IEEE Conference on Industrial Electronics and Applications (ICIEA), 2019.
5. Yong Huang ; Mengnian Xu ; Wei Wang ; Hao Wang ; Tao Jiang ; Qian Zhang,"Towards Motion Invariant Authentication for On-Body IoT Devices",ICC, 2019.
6. William J. Tomlinson ; Stella Banou ; Christopher Yu ; Michele Nogueira ; Kaushik R. Chowdhury,"Secure On-skin Biometric Signal Transmission using Galvanic Coupling",IEEE INFOCOM ,2019.
7. Mana Al Reshan ; Hang Liu ; Chunqiang Hu ; Jiguo Yu,"MBPSKA: Multi-Biometric and Physiological Signal-Based Key Agreement for Body Area Networks",IEEE Access, 2019.
8. Zisang Xu ; Cheng Xu ; Wei Liang ; Jianbo Xu ; Haixian Chen,"A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things",IEEE Access,2019.
9. Zhouzhou Li ; Hua Fang ; Honggang Wang," Integrated Node Authentication and Key Distribution Method for Body Area Network",International Conference on Computing, Networking and Communications (ICNC),2019.
10. Saru Kumari ; Pradeep Chaudhary ; Chien-Ming Chen ; Muhammad Khurram Khan,"Questioning Key Compromise Attack on Ostad-Sharif et al.'s Authentication and Session key Generation Scheme for Healthcare Applications",IEEE Access,2019.

AUTHORS PROFILE

S.Premkumar is Assistant Professor of Electronics and Communication in the Engineering Department, Saveetha School of Engineering, SIMATS, Chennai, India. Received Bachelor's degree in Electronics and Communication Engineering from Anna University in the year 2007 and Master's in Applied Electronics from Anna University in 2012 and Pursuing Doctoral degree in SIMATS, Chennai. Member of many professional societies such as IET, IAENG.

Dr.J.Mohana is Associate Professor of Electronics and Communication in the Engineering Department, Saveetha School of Engineering, SIMATS, Chennai, India. Received Bachelor's degree in Electrical and Electronics Engineering from Madras University in the year 2001 and Master's in Applied Electronics from Dr.M.G.R. Educational and Research Institute in 2007 and Doctorate from SIMATS, Chennai in 2016.

In the field of teaching and research for the past 16 Years. Authored well over 50 papers in reputed journals/conference proceedings. Guiding about 6 members towards their PhD. Her professional interests include Wireless Body Area Network, Telemedicine, broadband networks and mobile communication. Member of many professional societies such as IET, IAENG and IEEE Submitted proposal for funding to DRDO.