Empirical Studies of ECG Multiple Fiducial-points Based Binary Sequence Generation (MFBSG) algorithm in E-Health Sensor Platform

Kashif Saleem, Haider Abbas, Jalal Al-Muhtadi
Center of Excellence in Information Assurance (CoEIA)
King Saud University
Riyadh-12372, Saudi Arabia
{ksaleem; hsiddiqui; jalal}@ksu.edu.sa

Mehmet A. Orgun, Rajan Shankaran, Guanglou Zheng
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
{mehmet.orgun; rajan.shankaran}@mq.edu.au
guanglou.zheng@students.mq.edu.au

***Abstract*—In this paper, the Arduino Uno based e-Health Sensor Platform V2.0 by Libelium is enhanced with the ECG Multiple Fiducial-points based Binary Sequence Generation (MFBSG) algorithm to secure wireless sensors within Wireless Body Area Networks (WBANs). The eHealth kit includes biometric and other medical related functionalities to monitor the human body conditions by utilizing 10 different sensors that includes electrocardiogram (ECG). Therefore, MF-BSG algorithm generates secret keys for encryption, decryption and authentication purposes. Furthermore, we have analyzed the performance of the enhanced version of the toolkit and compared it with the Enhanced Very Fast Decision Tree (EVFDT) mechanism based health care systems in terms attack detection accuracy. The results confirm that the monitored data is transferred to the required destination in a more accurate and secure manner as compared to previous algorithms.**

Keywords— applications; biometric; communication; eHealth; electrocardiogram; encryption; medical; security; sensor; wireless body area network (WBAN)

I. INTRODUCTION

eHealthcare provides a multitude of electronic healthcare services that facilitate the medical world. One of the most important of these services is to provide remote assistance, where sensors measure the patient's condition, feed the data over wireless body area network (WBAN) to handheld devices or special portable medical device from where monitored data is transmitted to heath provider's for assistance [1-3].

Addressing integrity, authentication, non-repudiation, availability, and confidentiality implies security issues like data verification, accountability etc. because end to end security cannot be ensured without these [4, 5]. Security requirements are further compounded when a WBAN in integrated into the IoT infrastructure presenting a huge security risk [6-10]. When data being handled in this enterprise is of extreme personal and private nature, its mismanagement, either intentionally or unintentionally, could seriously hurt a patient along with future prospects of e-Healthcare enterprise [11].

Research carried out in order to address security concerns is not truly holistic in nature. It focuses on certain parts of the e-Healthcare enterprise successfully but at the same time fails to fully address all aspects of security [12]. Diverse and critical security threats emerge due to the vulnerable nature of the underlying wireless channels being utilized in data communication [11]. Some of the major vulnerabilities in this setting are eavesdropping, data modification, impersonation attack, replaying, and denial of service [13-15].

Recently, the e-Health Sensor Shield V2.0 as shown in Figure 1 is developed by Libelium [16] that allows Arduino users to read and collect biometric information by using 10 different sensors that includes electrocardiogram (ECG). The generated data helps to monitor a patient in real time or to be subsequently analyzed for medical diagnosis by storing or ring it for remote monitoring. Since the eHealth kit is specifically built for research purposes, it has an option to transfer biometric data over different wireless radio channels: 3G, GPRS, Wi-Fi, ZigBee, and Bluetooth [16].

Fig. 1. e-Health Sensor Shield V2.0 with Arduino Uno

In terms of security, the eHealth kit provides AES 128 for ZigBee and WPA2 for Wifi in the communication link layer and HTTPS (secure) protocol in the application layer as shown in [16]. The biometric data generated by the kit can be sent to the cloud in order to store it permanently [6, 17] or visualized in real time by sending the data directly to a laptop or Smartphone. iPhone and Android applications have been designed in order to easily see the patient's

This work was supported by the Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia.

DOI 10.1109/LCNW.2016.39

information. Despite the tremendous benefits offered by the eHealth kit, secure data communication between the eHealth kit and the cloud is still an open issue [6, 17]. The availability of patients' critical data anytime and anywhere in a secure manner is the main goal [6, 17]. Existing security approaches are not directly applicable on the eHealth kit and the WBAN network due to their resource constrained nature [1, 12, 18]. Analyzing the flow of network traffic shows that the patterns of network traffic have irregular structure, and therefore, statistical pattern identification approaches are required [19]. Therefore, the eHealth kit requires an approach that is light weight and efficient in handling real-time streaming data.

In this paper, we investigate the incorporation of the ECG Multiple Fiducial-points based Binary Sequence Generation (MFBSG) algorithm in the eHealth kit. MF-BSG is a recently proposed light-weight algorithm specifically designed to generate random binary sequences (BSes) which can then be used in secure communication. The algorithm is proved to be the most efficient of its kind in terms of handling stream data and hence is considered to be very appropriate to be embedded in e-Health Sensor Shield V2.0. The algorithm exploits multiple ECG feature values, including RR, RQ, RS, RP and RT intervals, to generate random BSes with low latency. These random BSes can be used as security keys for encryption or authentication, or be used to facilitate key distribution. Previous proposed algorithms solely rely on Inter-pulse Interval (IPI) features in binary sequence (BS) generation. Since the last 4-bits of each binary IPI can be regarded as random bits and are extracted to form BSes, generating a 128-bit BS normally takes around half a minute, which is very time consuming and is not feasible in real-time. Therefore, MFBSG is able to improve the performance of the generation of BSes in terms of time efficiency and avoids the protection of random seeds, a general requirement in many security systems.

In this paper, the eHealth sensor platform is enriched with the enhanced version of MFBSG algorithm to perform efficient data encryption and authentication. The contributions of this paper include the following:

1. We propose an improved MFBSG algorithm specifically for the eHeath sensor platform. We also program the eHealth sensor kit with the improved MFBSG.
2. We enable a cloud platform to acquire and store encrypted data for further analysis.
3. Deployment of real time WBAN test bed to monitor the resilience of the system in the presence of legitimate attacks.
4. We perform an analysis on the streaming data and its impact on the accuracy rate while detecting malicious behavior in the network.
5. We compare the performance of the MFBSG algorithm with that of the EVFDT algorithm [19, 20] in the E-Health Sensor Platform.

The remainder of this paper is structured as follows: Section 2 summarizes the MFBSG and EVFDT algorithms. Section 3 presents the method by which the MFBSG algorithm is improved and applied on a real-time WBAN test bed to enhance the overall efficiency of the system. Section 4 provides the details regarding performance analysis and comparison of the enhanced MFBSG algorithm with the EVFDT algorithm. Section 5 concludes the paper and addresses future research directions.

II. A Review of the EVFDT and MFBSG Algorithms

In this section, the MFBSG and EVFDT algorithms in eHealth sensor platform and are comprehensively reviewed and theoretically compared in every aspect.

A. The *EVFDT Algorithm*

An improvement of the Very Fast Decision Tree (VFDT) algorithm namely the enhanced VFDT (EVFDT) algorithm that differs from former by reasonable extension via regulating the tree size growth and providing a sustainable classification accuracy while consuming less time resources and memory [20]. VFDT was considered to be an appropriate algorithm for low-power sensors utilized in WBAN, because of its efficiency in handling the stream data. The VFDT algorithm is preferred by Abbas et al in [6], because first of all it is based on the data mining algorithm that is light weight. Secondly, from scratch it can build a decision tree. Furthermore, the algorithm keeps the stored data up to date, by performing the test and train process at the arrival of every new data segment. The fourth aspect of the VFDT is it consumes very less memory space as it does not require to read the complete data. Hence, the algorithm is also applicable to handle the huge amount of streaming and non-stationary traffic generated by wireless sensors motes. Therefore, Abbas et al in [20] have taken the original VFDT-τ and enhance it to make it more efficient to classify distributed denial-of-service (DDoS) attack [21] in cloud-assisted WBAN environment [17, 22] and named it as Enhanced Very Fast Decision Tree (EVFDT).

The main issue is the noise percentage in real-time data acquisition is high and because of this noise the accuracy of detection suffers, which eventually increase the size of the classification tree. To overcome this issue Abbas et al in [20] have incorporated accuracy enhancement and tree pruning approaches. These two approaches help in controlling the tree size and as well improves the detection rate. In EVFDT the procedure of tree initialization is same as VFDT-τ, but onwards while building the tree, it is updated with tree pruning and accuracy.

In addition, Abbas et al in [20] found that the Hoeffding bound (HB) fluctuation in VFDT-τ generate enormous noise that increses the tree size and thus effects the accuracy. In EVFDT, Abbas et al restricts the decision node in splitting the attribute by utilizing an adaptive tie-breaking threshold τ.

The main reason while reviewing VFDT-τ and EVFDT is the value of τ is pre-configured in VFDT-τ and throughout the entire tree building process the value of τ remains is static. The way to acquire the optimal value of τ can be by running brute force on all possibilities, which is totally unrealistic. In front of VFDT-τ, the value of τ in EVFDT is

dynamic and is calculated as a mean of the difference between HB values. This provides adaptive tie-breaking threshold τ value that totally depends on every and is calculated at every instance.

Furthermore, the second approach incorporated by Abbas et al in [20] is the pruning to eliminate the node from the tree that are not active in classification of instances and results in reduces the tree size. Abbas et al evaluated the performance of the EVFDT algorithm by deploying it in a real WBAN experimental testbed [19].

B. The *MFBSG Algorithm*

Zheng et al. [23], proposed a Multiple Fiducial-point based Binary Sequence Generation (MFBSG) algorithm for securing wireless implantable devices in a WBAN. Besides considering the features of IPI, the MFBSG algorithm utilizes other ECG signal's characteristic within one cycle heartbeat, that are RS intervals, RQ intervals, RT and RP intervals. This is based on the fact that P wave, QRS complex and T wave are also observable within a normal sinus rhythm, and their intervals possess characteristics of randomness.

In the MFBSG algorithm, more components of an ECG signal are taken under consideration and based on that the actual time required to generate random BSes is significantly reduced. In this manner the design goal of low-latency is achieved, which is the most important requirement of a WBAN system. The Zheng et al. use discrete wavelet transforms in the MFBSG algorithm to detect ECG fiducial points and can obtain time intervals between them in a more precise manner.

The authors have analyzed the complexity of the wavelet transforms, and found that it is comparable to that of fast Fourier transforms. In [23], Zheng et al. have conducted analysis on several methods that are meant to generate BSes, all of these methods totally depends on IPIs. While performing experimentation Zheng et al. found that MFBSG algorithm eliminates sampling noise at the very beginning and further execute two major processes, that are ECG Wavelet Process and BS Generation Process.

The purpose of ECG wavelet process is to use the technique of wavelet transforms to process sampled ECG signals, involving the following steps: "QRS detection, P wave detection and T wave detection. Wavelet transforms are based on a set of analyzing wavelets with a limited duration, and allow the representation of temporal features of a signal at different resolutions.

Since the ECG signal is characterized by a cyclic occurrence of patterns with a different frequency content (QRS complexes, T waves, and P waves), it is suitable to use the wavelet transform to analyze the ECG signal. After the wavelet transform, timing information of the ECG fiducial points (peak values of P, Q, R, S & T) are detected. Then five feature values from one heartbeat cycle (RR, RQ, RS, RP & RT intervals) are calculated and are then used as inputs to the next stage".

The second is BS generation process that is to generate random BSes by processing five feature values from one heartbeat cycle. "After receiving the ECG feature values, binary digits are extracted from each feature, named binary features (BFs). These BFs are then concatenated to obtain an x-bit long BS. Randomness is a vital requirement if BSes are used for WBAN security purposes.

Meanwhile, generating BSes with a high timing efficiency is another important requirement for a communication system. In order to balance the requirements of randomness and timing efficiency, this process is broken down into 3 steps: mean value removal, adaptive BF extraction and BF concatenation".

In order to ensure that generated BSes satisfy the requirement of randomness, the Zheng et al. in [23] runs number of tests that includes entropy calculation. These tests are based on the NIST randomness test suite on the MIT PhysioBank database. Experiments were carried out on the ECG data from 97 subjects: 18 from the MIT-BIH Normal Sinus Rhythm database and 79 from the European ST-T database. In [23], Zheng et al. have compared the MFBSG algorithm with the schemes that are based on IPI. The analysis shows that the required time by MFBSG algorithm to generating a BS is reduced significantly.

III. METHODOLOGY

The eHealth sensor kit has been studied extensively to update and enhance it with the MFBSG algorithm. The functions in MFBSG algorithm to delineate ECG signals and detect ECG fiducial points by using discrete wavelet transforms are as below [23].

- ECGDetect():the main function.
- ECGsignalLoad():load ECG signals from file but in our case ECG signals in realtime.
- RefineECGsignal():remove noise from the ECG signals.
- detectECGFeatures(): the main process function to detect fiducial points on ECG. It uses discrete wavelet transforms to decompose the ECG at 4 levels and detect maxima pairs and their zero-crossing points to locate these fiducial points.

Wavelet transforms is to process the ECG and obtain fiducial points is a complex process, therefore it programmed and is reduced according to the requirements and the updated one is then implemented in the platform. In the initialization phase the ECG feature detection requires additional processing.

In addition to above, the generated random BS is then utilized as secret key to encrypt and transfer to the server or to the authenticated mobile device as described in [23] section four. The MFBSG algorithm code as shown in Figure 2 is programed specifically for the kit based on the above mentioned functions and is flashed in it to perform the experiments. Figure 3 shows the flow of processes performed by improved MFBSG algorithm in e-Health kit.

```
include <eHealth>
include <discrete wavelet transforms>
include <ECG-MFBSG>

// routine runs once when press reset
void setup() { Serial.begin(115200); }

// The routine runs in loop forever

eHealth.getECG();

load ECG signal();

Refine ECG signal();

detect ECG fiducial points by using discrete wavelet
transforms();

Generate BS value;

loop() {
        eHealth.getECG();
        if (BS value available)
        Encrypt based on ECG BS();
        Else generate BS;

        print/transfer(encrypted "ECG value");

delay (1); // millisecond wait
}
```

Fig. 2. Pseudo Code of Improved MFBSG algorithm in e-Health Sensor Shield V2.0 with Arduino Uno

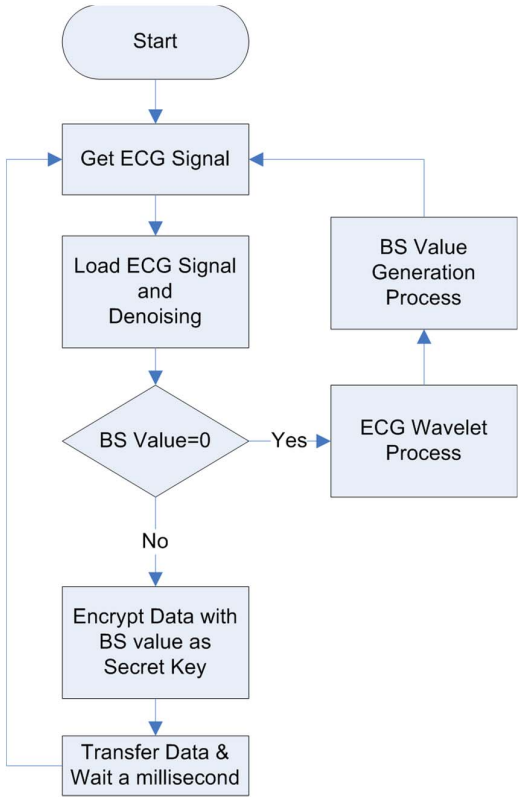

Fig. 3. Improved MFBSG algorithm process flowchart

IV. Experimental Analysis

A real WBAN experimental testbed has been deployed using the eHealth sensor kit with the improved MFBSG algorithm. The results from these experiments are analyzed for which the details are given below.

A. Experimental test bed

To evaluate the performance of the improved MFBSG algorithm in a real-time test bed using eHealth Sensor Shield V2.0 with Arduino Uno platform. The experiments were run on a Ubuntu 64-bit workstation with Dell XPS 27inch Touch All-in-One that includes 4GHz 4th Generation Intel® Core™ i7 processor, 16GB RAM with all background processes switched off. The system is installed with Wireshark 2.0.5. to analyze the real-time traffic generated by the eHealth kit.

The eHealth kit with the help of sensors get the biometric data from the human body and is transferred to the server for storage or in real-time to the mobile device of the authorized physician for analysis. Figure 1 shows the eHealth sensor shield and the Arduino Uno 2.0 board. The eHealth kit can sense upto ten different kind biometrics, as glucometer, body temperature, electrocardiogram (ECG), patient position (accelerometer), oxygen in blood (SPO2), galvanic skin response (GSR-sweating), blood pressure (sphygmomanometer), air flow (breathing), and muscle/electromyography (EMG) sensor. In this experimentation the SPO2, ECG, and accelerometer is enabled. The XBee radio module fits in the communication socket. The data is transferred securely from this eHealth kit to the gateway or the base station. Onward, from the gateway to the database server / cloud for permanent storage.

B. Results

Scenario is configured and traffic is generated as same as in [19], to evaluate the performance of the proposed algorithm on the real-time cloud-assisted WBAN test bed. The attack detection rate is considered as the performance metric as elaborated in [19], to perform comparison between EVFDT and MFBSG as shown in Table 1.

TABLE I. Empirical Results

No. of Instances	Attack Detection Accuracy in %	
	EVFDT	MFBSG
10,000	95.7	96.4
20,000	96.8	97
30,000	97.6	98.5
40,000	98.1	98.7
50,000	98.8	99.1

V. Conclusion and Future Work

In this paper, the eHealth sensor platform is enhanced with the improved MFBSG algorithm to perform efficient data encryption and authentication. An improved MFBSG algorithm has been proposed specifically for the eHealth sensor platform considering its inherent characteristics. A cloud platform is enabled to acquire and store encrypted data for further analysis. The enhanced eHealth Sensor Platform is evaluated over a real-time WBAN experimental test bed that is deployed to monitor the efficiency in the presence of both kind of legitimate and illegitimate traffic. An analysis on the streaming data is performed and its impact on the accuracy rate while detecting malicious behavior in the network. The results clearly demonstrate that the MFBSG algorithm in the E-Health Sensor Platform is more efficient in comparison with the EVFDT algorithm.

In future, MFBSG algorithm based eHealth Sensor Platform is evaluated with different radio modules and as well as by involving more of attacks.

References

[1] B. M. C. Silva, J. J. P. C. Rodrigues, I. de la Torre Díez, M. López-Coronado, and K. Saleem, "Mobile-health: A review of current state in 2015," *Journal of Biomedical Informatics,* vol. 56, pp. 265-272, 8// 2015.

[2] K. Saleem, A. Derhab, J. Al-Muhtadi, and B. Shahzad, "Human-oriented design of secure Machine-to-Machine communication system for e-Healthcare society," *Computers in Human Behavior,* vol. 2015, pp. 977–985, 2015.

[3] K. Saleem, A. Derhab, and J. Al-Muhtadi, "Low delay and secure M2M communication mechanism for eHealthcare," in *e-Health Networking, Applications and Services (Healthcom), 2014 IEEE 16th International Conference on*, 2014, pp. 105-110.

[4] M. S. KHALIL, F. KURNIAWAN, and K. SALEEM, "AUTHENTICATION OF FINGERPRINT BIOMETRICS ACQUIRED USING A CELLPHONE CAMERA: A REVIEW," *International Journal of Wavelets, Multiresolution and Information Processing,* vol. 11, p. 1350033, 2013.

[5] K. Saleem, A. Derhab, J. Al-Muhtadi, B. Shahzad, and M. A. Orgun, "Secure transfer of environmental data to enhance human decision accuracy," *Computers in Human Behavior,* 2015.

[6] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," *IEEE Access,* vol. 4, pp. 1375-1384, 2016.

[7] J. Santos, J. J. P. C. Rodrigues, B. M. C. Silva, J. Casal, K. Saleem, and V. Denisov, "An IoT-based mobile gateway for intelligent personal assistants on mobile health environments," *Journal of Network and Computer Applications,* 2016.

[8] J. Santos, J. J. P. C. Rodrigues, J. Casal, K. Saleem, and V. Denisov, "Intelligent Personal Assistants Based on Internet of Things Approaches," *IEEE Systems Journal,* vol. PP, pp. 1-10, 2016.

[9] J. V. V. Sobral, J. J. P. C. Rodrigues, K. Saleem, J. F. d. Paz, and J. M. Corchado, "A composite routing metric for wireless sensor networks in AAL-IoT," in *2016 9th IFIP Wireless and Mobile Networking Conference (WMNC)*, 2016, pp. 168-173.

[10] J. Santos, J. J. P. C. Rodrigues, B. M. C. Silva, J. Casal, K. Saleem, and V. Denisov, "An IoT-based mobile gateway for intelligent personal assistants on mobile health environments," *Journal of Network and Computer Applications,* vol. 71, pp. 194-204, 8// 2016.

[11] K. Saleem, A. Derhab, M. Orgun, J. Al-Muhtadi, J. Rodrigues, M. Khalil*, et al.*, "Cost-Effective Encryption-Based Autonomous Routing Protocol for Efficient and Secure Wireless Sensor Networks," *Sensors,* vol. 16, p. 460, 2016.

[12] A. Gawanmeh, H. Al-Hamadi, M. Al-Qutayri, C. Shiu-Kai, and K. Saleem, "Reliability analysis of healthcare information systems: State of the art and future directions," in *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*, 2015, pp. 68-74.

[13] K. Saleem, M. S. Khalil, N. Fisal, A. A. Ahmed, and M. A. Orgun, "Efficient Random Key Based Encryption System for Data Packet Confidentiality in WSNs," in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom2013)*, Melbourne, Australia, 2013, pp. 1662-1668.

[14] K. Saleem, A. Derhab, J. Al-Muhtadi, and M. A. Orgun, "Analyzing ant colony optimization based routing protocol against the hole problem for enhancing user's connectivity experience," *Computers in Human Behavior,* vol. 51, Part B, pp. 1340-1350, 10// 2015.

[15] K. Saleem, N. Fisal, M. A. Baharudin, A. A. Ahmed, S. Hafizah, and S. Kamilah, "BIOSARP - Bio-Inspired Self-Optimized Routing Algorithm using Ant Colony Optimization for Wireless Sensor Network - Experimental Performance Evaluation," in *COMPUTERS and SIMULATION in MODERN SCIENCE, Included in ISI/SCI Web of Science and Web of Knowledge*. vol. IV, N. E. Mastorakis, M. Demiralp, and V. M. Mladenov, Eds., ed, 2011, pp. 165-175.

[16] C. Hacks, "e-Health Sensor Platform V2. 0 for Arduino and Raspberry Pi [Biometric/Medical Applications]," *Recuperado el,* vol. 24, 2014.

[17] H. A. Haider Ali Khan Khattak, Ayesha Naeem, Kashif Saleem, Waseem Iqbal, "Security Concerns of Cloud-Based Healthcare Systems: A Perspective of Moving from Single-Cloud to a Multi-cloud Infrastructure," in *17th International Conference on E-health Networking, Application & Services (Healthcom2015)*, 2015, pp. 50-56.

[18] P. J. Soh, G. A. E. Vandenbosch, M. Mercuri, and D. M. M. P. Schreurs, "Wearable Wireless Health Monitoring: Current Developments, Challenges, and Future Trends," *IEEE Microwave Magazine,* vol. 16, pp. 55-70, 2015.

[19] H. Abbas, R. Latif, S. Latif, and A. Masood, "Performance evaluation of Enhanced Very Fast Decision Tree (EVFDT) mechanism for distributed denial-of-service attack detection in health care systems," *Annals of Telecommunications,* pp. 1-11, 2016.

[20] R. Latif, H. Abbas, S. Latif, and A. Masood, "EVFDT: An Enhanced Very Fast Decision Tree Algorithm for Detecting Distributed Denial of Service Attack in Cloud-Assisted Wireless Body Area Network," *Mobile Information Systems,* vol. 2015, 2015.

[21] S. Alanazi, K. Saleem, J. Al-Muhtadi, and A. Derhab, "Analysis of Denial of Service Impact on Data Routing in Mobile eHealth Wireless Mesh Network," *Mobile Information Systems,* vol. 2016, p. 19, 2016.

[22] S. Alanazi, J. Al-Muhtadi, A. Derhab, K. Saleem, A. N. AlRomi, H. S. Alholaibah*, et al.*, "On resilience of Wireless Mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications," in *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*, 2015, pp. 205-210.

[23] G. Zheng, G. Fang, R. Shankaran, M. Orgun, J. Zhou, L. Qiao*, et al.*, "Multiple ECG Fiducial Points based Random Binary Sequence Generation for Securing Wireless Body Area Networks," *IEEE Journal of Biomedical and Health Informatics,* vol. PP, pp. 1-1, 2016.