Accepted Manuscript

A joint resource-aware and medical data security framework for wearable healthcare systems

Sandeep Pirbhulal, Oluwarotimi Williams Samuel, Wanqing Wu, Arun Kumar Sangaiah, Guanglin Li

PII: S0167-739X(18)31547-4
DOI: https://doi.org/10.1016/j.future.2019.01.008
Reference: FUTURE 4701

To appear in: *Future Generation Computer Systems*

Received date : 30 June 2018
Revised date : 6 December 2018
Accepted date : 6 January 2019

Please cite this article as: S. Pirbhulal, O.W. Samuel, W. Wu et al., A joint resource-aware and medical data security framework for wearable healthcare systems, *Future Generation Computer Systems* (2019), https://doi.org/10.1016/j.future.2019.01.008

A Joint Resource-Aware and Medical Data Security Framework for Wearable Healthcare Systems

Sandeep Pirbhulal[a,b,c], Oluwarotimi Williams Samuel[a,b,c], Wanqing Wu[a,b]*, Arun Kumar Sangaiah[d], and Guanglin Li[a,b]

[a]CAS Key Laboratory of Human-Machine Intelligence-Synergy Systems, Shenzhen Institutes of Advanced Technology (SIAT), Shenzhen 518055, China
[b]Institute of Biomedical and Health Engineering, SIAT, Chinese Academy of Sciences (CAS), Shenzhen 518055, China
[c]Shenza hen College of Advanced Technology, University of Chinese Academy of Sciences, Shenzhen 518055, China
[d]School of Computing Science and Engineering, VIT University, Vellore-632014, Tamil Nadu, India

---

Abstract

Internet of Medical Things (IoMTs) is a building block for modern healthcare having enormously stringent resource constraints thus lightweight health data security and privacy are crucial requirements. A critical issue in implementing security for the streaming health information is to offer data privacy and validation of a patient's information over networking environment in a resource efficient manner. Therefore, we developed a biometric-based security framework for resource-constrained wearable health monitoring systems by extracting heartbeats from ECG signals. It is analyzed that time-domain based biometric features play a significant role in optimizing security in IoMT based medical applications. Moreover, resource optimization model based on utility function is proposed for clinical information transmission in IoMT. In this study, ECG signals from 40 healthy subjects were employed comprising lab environment and publicly available database i-e-physionet. The experimental results validate that proposed framework requires less processing time and energy consumption (0.0068ms and 0.19[illegible] microJoule/Byte) then Alarm-net (0.0128ms and 0.351 microJoule/Byte) and BSN-care (0.0175ms and 0.53 microJoule/Byte). Moreover, from the results, it is also observed that biometric key generation mechanism not only provide random and unique keys but it also offer a trade-off between security and resource optimization. Thus, it can be concluded that the proposed framework has got both social and economic significance for real-time healthcare applications.

Keywords: Healthcare, Data Security, Patient's Privacy, Resource-Efficient, Internet of Medical Things

---

* Corresponding author. Tel.: +86-000-000-0000; fax: +0-000-000-0000 .
E-mail address: wq.wu@siat.ac.cn

1. Introduction

The Internet of Things (IoT) is a transformative and evolving paradigm which has gained attention in several application domains including smart homes, smart environment, personal, and remote healthcare among others [1-5]. In IoT, there are various intelligent nodes which can be interconnected and cooperated with each other for information visualization and acquisition, without the requirement for human involvement [6]. The IoT has been expressed as a technology development that would transform life, trade, and the economy of the world at large [7]. One of the essential domains that will be intensely influenced by the IoT is health monitoring applications [8]. The primary usage of the IoT in the medical area is known as the Internet of Medical Things (IoMT) [9][10]. The IoMT is a system of associated medical nodes and applications whose aim is to offer better and more healthcare services. The IoMT is receiving attention owing to the occurrence of state-of-the-art products including magnetic resonance imaging (MRI), handy ultrasound devices, and wearable devices which will facilitate the streamlining of health procedures including tele-tracking of patients and disease diagnosis among others. In IoMT, wireless medium is used to transfer medical information between entities, so there is a possibility that unauthorized person can eavesdrop on the communication using several attacks. Therefore, security is paramount for IoMT based healthcare systems [11-13]. It is stated by Health Insurance Portability and Accountability Act (HIPAA) that secure communication must be brought into the network so valuable information should not be acquired by illegal users[14]. Moreover, IoMT is a collection of several resource-constrained devices hence it is highly significant to deliver a balance between secure communication and resource utilization.

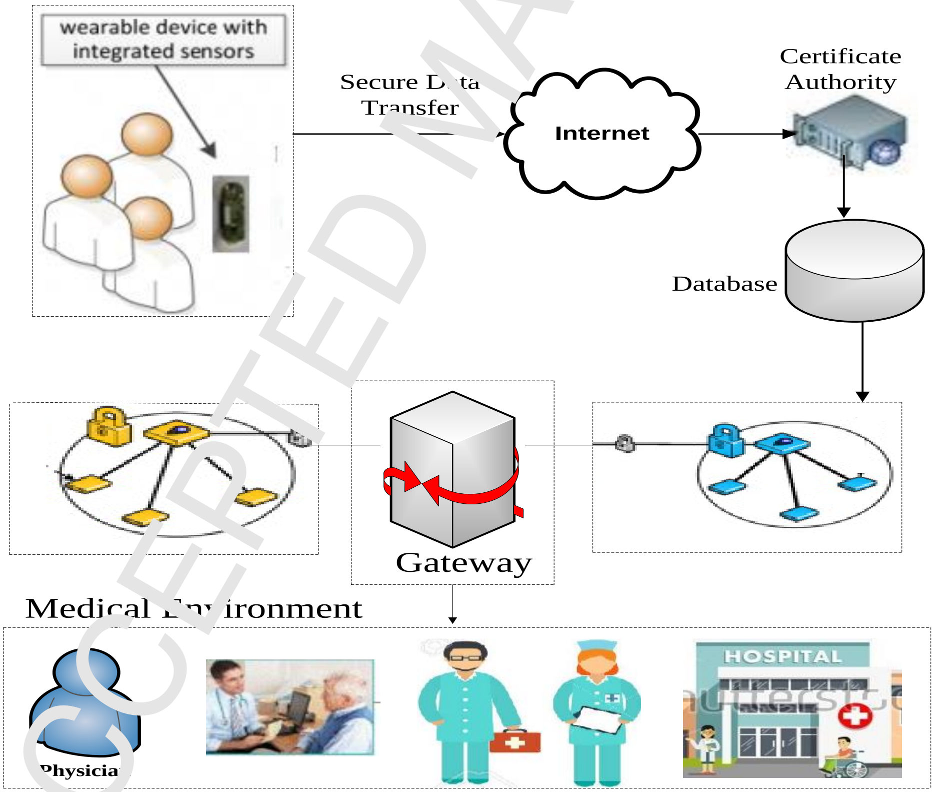


Fig .1. Architecture of Internet of Medical Things based Remote Healthcare Systems

In general, the IoMT structure is constituted of three layers (perception, network, and application) [9]. The main responsibility of the perception layer is to accumulate medical information with several devices. The network layer is comprised of wired/wireless system and middleware, which processes and communicates the input acquired by the perception layer provisioned by technical stages. Well-designed transportation rules not only increase transmission proficiency and decrease energy intake but also guarantee data confidentiality and security. The application layer incorporates the health data resources to offer medical facilities and fulfill the final individual's needs, due to the real circumstances of the target residents and the service requirement. The data privacy and security of patient associated data are two essential conceptions of IoMT. In the context of patient's information safety and privacy, it needs to be acquired, accumulated and sent securely to the authorized person [15]. More reasonable protection strategies could be developed according to different purposes and requirements. The widespread use of IoMT devices provides a better guarantee for people's health [16]; however, it also puts much pressure on information security and privacy protection. How to ensure the security of such data has always been the focus of academic research.

The development of remote healthcare framework based on IoMT has many challenges, such as power management, secure node-node communication, timely delivery of data and device's movement sustenance among others. Moreover, by the real-time implementation of IoMT without bearing in mind patient's data confidentiality and security will allow unauthorized people to eavesdrop medical information during its transmission between wireless devices. As a result, the privacy of subjects is comprised, and hackers may put critical data on public websites for illegal usage. Once the data is available on the social network, it can be utilized in several wicked ways such as:

a) Some treatments may be costly, in case fraudsters get information on physician services, can damage a victim's financial well-being.

b) Attackers, who are not ill and don't require treatment, can obtain a reasonable income ordering some expensive drugs by using medical cardholder so that they can get resale medicines.

c) If criminals manage to get in touch with a devious clinic, an insurance company may be billed for services that have never been rendered, and the money will be distributed among clinic and fraudsters.

Since, there are many ways that attackers can compromise the source data and use it for not legal purposes. Therefore, this study aims to develop a joint resource-aware security model for IoMT based remote healthcare. In the proposed model, medical information will be encrypted before transmitting to its destination node in order to guarantee privacy and security. Moreover, bio-key generation mechanism developed in this study will make it difficult for hackers to use the previous session information to decrypt current session message. The proposed framework offers a tradeoff between security and resource consumption for the medical data transmission in the hospitals. This research will not only reduce the economic cost in the medical market across the globe with economical healthcare facilities but also guarantee the security of real-time health data transmission between patients and doctors. Thus, this study has got both social and economic significance.

The rest of the paper is organized as follows. In Section 2, a literature review is discussed. The Section 3 and Section 4 include methods and materials, experimental results and discussion, respectively. Finally, the paper is concluded in Section 5.

2. Literature Review

In the modern era, IoMT is widely utilized for tele-healthcare [17][18]. In, IoMT, the medical cloud can distribute data to several nodes via wireless medium [19]. Though IoMTs, are the best method of healthcare, but medical IoT devices carry highly critical patient's data, so it is mandatory to offer secure communication in IoMT [20][21]. Authors in [22], developed lightweight identity-based cryptography (IBE-Lite) method, it claims to offer security and confidentiality with accessibility. However, their method recognizes numerous safety and privacy concerns as well as efficiency problems. Wood et al. [23] have developed Alarm-net for smart home automation based on query protocol. This approach was not only susceptible to the adversarial privacy attacks, which may reveal the locality of the inhabitant. On the other hand, it also consumes a lot of resources, hence requires more execution time for applying security. The BSN-care method [24], provides modern healthcare technique for health monitoring. Due to the utilization of external keys, it requires more cycles to generate random keys. In the above discussed methods for IoMT, external keys for securing medical data are used. It is well-known fact that different humans have distinct biological activities and features, so they may be applied for securing IoMT. Hence, it will not be easy for an assailant to attack the medical information. Consequently, physiological based security is a more reliable way to ensure communication in healthcare systems since it offers fast action and resources efficient safety solutions than conventional methods. In this research, we are focusing on developing ECG based security framework for IoMT which could provide not only stability between resource-efficiency and security but it also increases secret key strength so an attacker should not compromise either key or medical information.

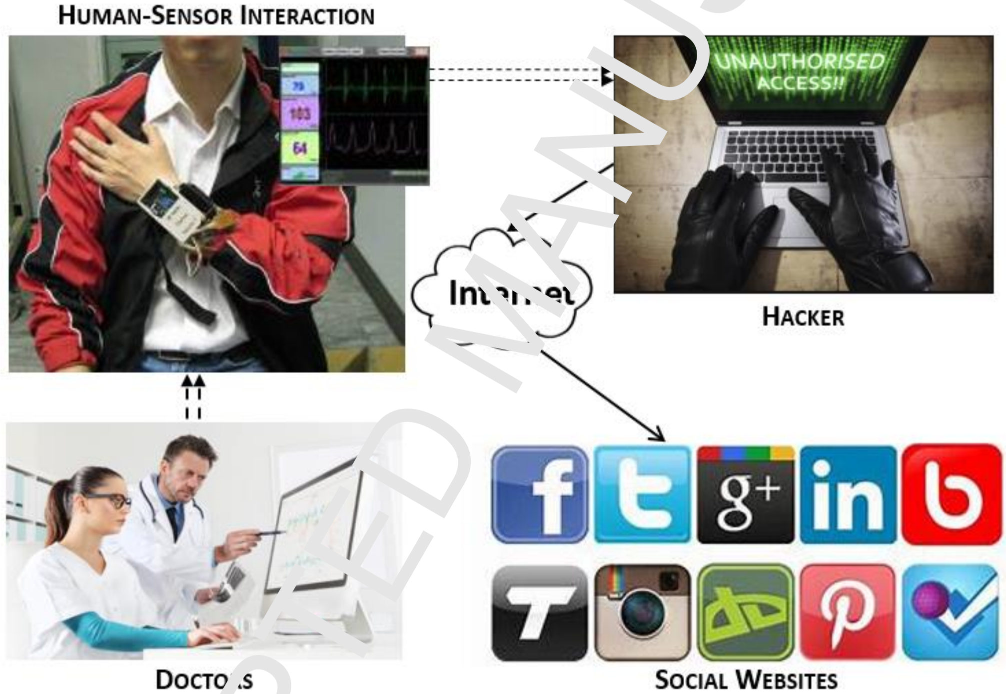


Fig. 2. Security and Privacy Risks for Tele-Healthcare Systems

In recent studies, several researchers have revealed that ECG based secret keys are vital for securing medical applications [24-30]. Though, the chief concern of resource-constrained IoMT devices is that it ought to be functioning under severe constraints. Time-domain features of ECG i-e inter-pulse intervals (IPIs) are recently used to offer a trade-off between resource efficient and secure communication in healthcare systems. One of the critical factors to start data transmission between IoMT devices is time synchronization. Owing to the construction of the circulation system of individuals, QRS-complex necessities recognition of a beat. Firstly, device that collects ECG sends the synchronization indicator, which specifies that biometric trait is generated, it is essential to assure that the IPIs collected by other devices. If synchronization pointer generated by means of any device that does not include adequate data then the communication between nodes will not be started [31-35]. Hence, the Hamming distance can be useful to quantity distinctiveness between IPI based secret keys; this factor would be useful to clarify that these keys can be used for security aspects in IoMT.

In modern health monitoring systems, it is noteworthy for providing a trade-off between protected communication and energy-efficiency due to several restrictions of IoMT systems. The main motivation of this study is related to provide stability in IoMT by presenting effective bio-key based security mechanism for secure data transmission. Consequently, this study developed patient-centered information security framework using IPIs for IoMT based healthcare applications which can acquire a more bits from each heartbeat of individuals. The main goal of our study is to present secure and low power IoMT system for the medical data transmission in the hospitals, due to the emerging big data notion, reliable and safe healthcare is very vital.

3. Applications of Wearable Healthcare Systems

There are various applications of the remote healthcare, but few of them are discussed below:

3.1. Adaptive-care Provisioning

Machine learning and artificial intelligence based healthcare applications are playing the key role to revolutionize the healthcare domain with more focus on the automatic and adaptive care provisioning. Generally, numerous statistical and intelligent systems are developed to present linear/ non-linear models for neural networks [36]. The medical data obtained from these systems is vital and its secure transmission for remote healthcare in also mandatory.

3.2. Remote Health Monitoring

The mobile-based patient's health monitoring has the good connection and features sharing capability with the state of the art wireless technologies for the discrete and continuous event management [37]. There are various platforms in the medical domain such as operation theatres, military operations, fields, and farms, where this application is suitable.

3.3. Stroke Restoration

Several patients can use the feature of video conferencing for sending the medical information to the remote physicians; it will increase the viability, effectiveness, and level of recognition of telerehabilitation for stroke individuals [38].

3.4. Wireless Capsule Endoscopy

This is a subset of the Tele-monitoring and Tele-healthcare for the patient monitoring in the medical market. For the healthcare system, it is imperative to transfer all the information such as physiological signals, video and image signals. Wireless capsule endoscopy is one of the paradigm shift in the medical market to facilitate the physicians and patients by providing the state of the art facilities. The major point of this application is the high and clear visibility with a bright and big picture of the critical scene. High-quality camera sensors are the significant parts to be enhanced and amended for these technologies [39].

3.5. Emergency Healthcare

The fundamental purpose of this section is to facilitate the patients and medical doctors by providing the efficient treatment of the cardiovascular diseases especially, the heart attack of the emergency patients [40]. For this reason, there is a need for intelligent sensor-based devices to manage the overall process and mechanism of the personal medical healthcare. For example, several physicians monitor the old age patients remotely at their respective homes via the emerging technology.

3.6. Healthcare Management

Tele-presence is the key factor in the neuro-computing healthcare system management in the medical market. Besides, there are several components for facilitating the physicians and patients in the hospital theatres and medical centers to give the medications and precautions to the emergency patients [41].

3.7. Smart Homes

An efficient and smart home automation system for controlling medical equipment's or wearable/ implantable devices distantly using smartphone plays a vital role in modern healthcare. [42].This is the critical role player application because most of the human bodies symptoms are covered with a clear understanding of the disease, then precautions are suggested with specified dosages to get refrain from it. These days human body feature based sensor deployment methods are getting too much attention due to the coverage of the overall body characteristics and health monitoring.

3.8. Clinical Decision Support Systems

The gap between superlative indication from organized trials and actual world proof in healthcare research has encouraged the global organizations to contemplate the use of original medical information to enhance the understanding securely as well as efficiently [43]. Therefore, telemonitoring will renovate wound care research and increase the standards of healthcare while assisting doctors to provide a better life to patients.

3.9. Telemedicine Systems

Telemedicine is one of the critical parameters for the healthcare monitoring in the various departments of the medical market. There are significant benefits of the system advancement for the healthcare. To efficiently and effectively manage the entire healthcare environment it is vital to maintain the Telemedicine and make it more autonomous and intellectual. In this application, Bluetooth Low Energy (BLE) is the key component to handle and maintain the health issues. Since, BLE has the flexible and tight integration with the 5G technologies and has changed the size of the medical sensor nodes entirely, due to these advantages it has caught the attention of both medical world and the health departments [44].

3.10. Monitoring of Old-age Patients

This application focuses on the caregiving facilities of the old age and elderly patients in the near and remote location. This is the most emerging healthcare domain in every corner of the world, and most of the developing countries are focusing at the key points to entertain the critical aspects of the medical health corner [45].

4. Security and Privacy Requirements for IoMT based Healthcare

In IoMT, destroying the security of the medical system or network could cause disastrous consequences [46]. Meanwhile, the patient's private information exists at all stages of data collection, data transmission, cloud storage, and data republication. In developing secure healthcare system, the following requirements should be considered.

4.1. Data Confidentiality

In IoMTs, it is entailed to defend the original medical data from any disclosure. In modern health monitoring system, the wearable devices accumulate and forwards specific medical data to the sever. An attacker can eavesdrop medical information and can overhear during data transmission. This eavesdropping process can result in severe challenges to the patients since the hacker can utilize the collected medical data for numerous illegal purposes.

4.2. Data Integrity

Alongside confidentiality, the integrity of medical data is also a significant factor for its transmission in WBSNs. Attackers could modify the data by introducing some fake fragments within the original data to change the original meaning. Then, duplicate data will be delivered to the destination node. Thus, ensuring data integrity is the very prominent solution for protecting original data from external attacks.

4.3. Data Availability

This property verifies that accurate data must be available to the legitimate users so that reliable access of the network resources is given to appropriate nodes promptly. In the context of IoMT, it is very crucial that network resources and medical data be available to the authenticated nodes/users.

4.4. Data Freshness

An attacker can passively perceive the medical data during its transmission from patients to the concerned doctor, and can subsequently replay it by applying old keys to perplex the coordinator. Data freshness assures that the data is fresh and nobody can replay old data.

4.5. Scalability

As the network increase and the number of managers and customers turn out to be more, so it is significant to reduce latency, so the computational and storing overheads need to be controlled.

4.6 Secure key distribution

It is crucial to allow encryption and decryption operation for accomplishing the estimated security and confidentiality. The controller must have the capability to accomplish stable implication and detachment of devices.

5. Method and Material

This section comprises details of physiologically based key generation mechanism and details about the proposed joint resource aware and security model for wearable healthcare systems.

5.1. Wearable System for ECG Measurement

In this study, a wearable system for ECG measurement is designed as shown in Fig.3. The flexible electrodes and wearable platform are integrated to simplify the ECG signal acquisition task and as well ensuring guarantee the quality of ECG the recorded signals with low power consumption of the system, and higher reliability and precision.

The medical devices collect bio-signals from individuals, these signals are associated with some undesirable noise. It could affect the feature extraction procedure from the collected signals to generate EI for securing WBSNs. For that reason, unwanted noise from bio-signals needs to be removed so that neat signals can be acquired and applied in the e-health monitoring applications. There are numerous kinds of noises that can be mixed with the obtained physiological signals from the subjects because hardware system may not entirely filter all noises. In this context, it is essential to utilize appropriate filters for eradicating undesirable information from initially captured signals from wearable devices. As hardware filters are contingent on capacitors which are deliberated as the major restraint for completely removing unwanted noise, their association cannot be explained well both in the manufacturing and in demonstrative deployment. Meanwhile, software filtering depends typically on cut-off frequencies which may be controlled explicitly by operation of state-of-the-art filtering approaches. The signal levels are immensely low such as 1mV for physiological signals including ECG recordings. Given that, it is vital to put on filtering for eradicating extensive undesirable noises [50-54]. The noise in ECG waveform is mostly owing to not steady direct current offset between the human body and electrode interface, power line noise, construction of the medical device, muscle noise, and electrical instrumental noise in the environment [52].

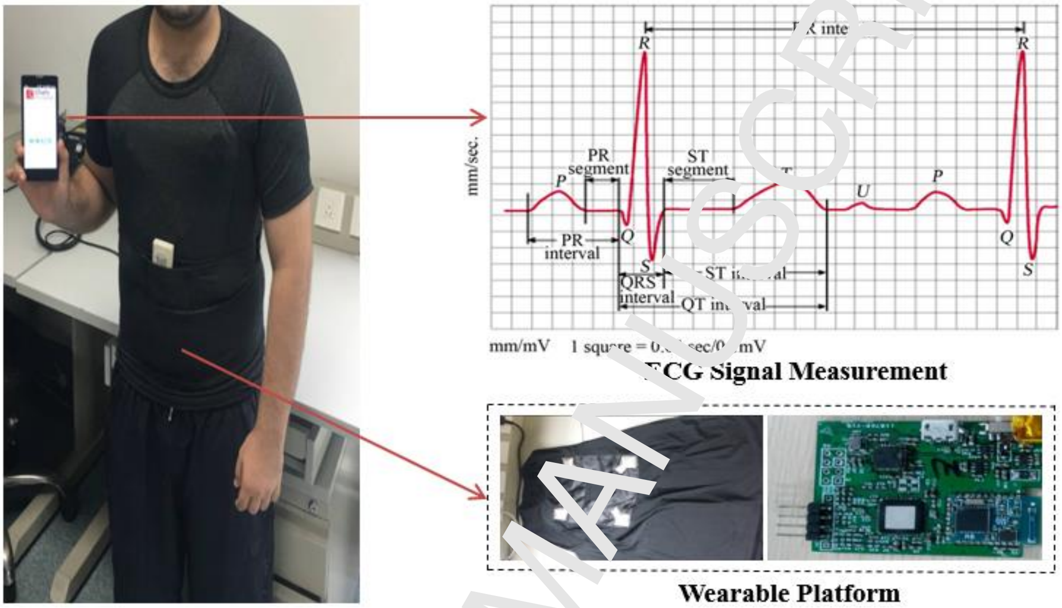


Fig .3. Wearable System for ECG Measurement

5.2. Proposed Security Framework for Healthcare

This research aims to provide resource efficient security framework, so physiological based keys are generated for securing IoMT. Once the ECG signals are filtered, next step is to calculate time domain features for creating random secret keys for healthcare systems as shown in Fig.4.

We have used IPIs obtained from ECG to produce bio-keys for implementing security in IoMT because this process can preserve memory usage as well as require less computation since they can be acquired from several cardiac signals. If the 128-bit bio-key (Kb) based on IPIs are satisfactorily arbitrary, then they may be applied as security keys for securing communication between medical devices in IoMT systems.

In this research, the initial stage of physiological based key generation mechanism is the detection of R peaks from heartbeats. Moreover, prior to obtaining more bits from IPIs, bounded increasing sequences are generated from IPIs which could extract multiple bits. There are numerous approaches to encode decimal IPIs into binary values; we used block encoding for generating binary bits. It has advantages of reducing measurement errors, also increasing the tolerance of the produced binary sequences. Furthermore, binary features (BF) are extracted from encoded bits from the ith heartbeat, which are further concatenated to generate bio-keys as demonstrated in eq.(1).

$$Kb(i) = BF_1 \,||\, BF_2 \,||\, BF_3 ....BF_n \qquad (1)$$

whereas $Kb(i)$ is secret key produced from the ith heartbeat and $||$ characterizes concatenation procedure. For generating y-bit Kb, Kb_i constructed from k succeeding heartbeats are concatenated as shown in eq.(2).

$$Kb(y) = BS_1 \parallel BS_2 \parallel BS_3 .... BS_k \tag{2}$$

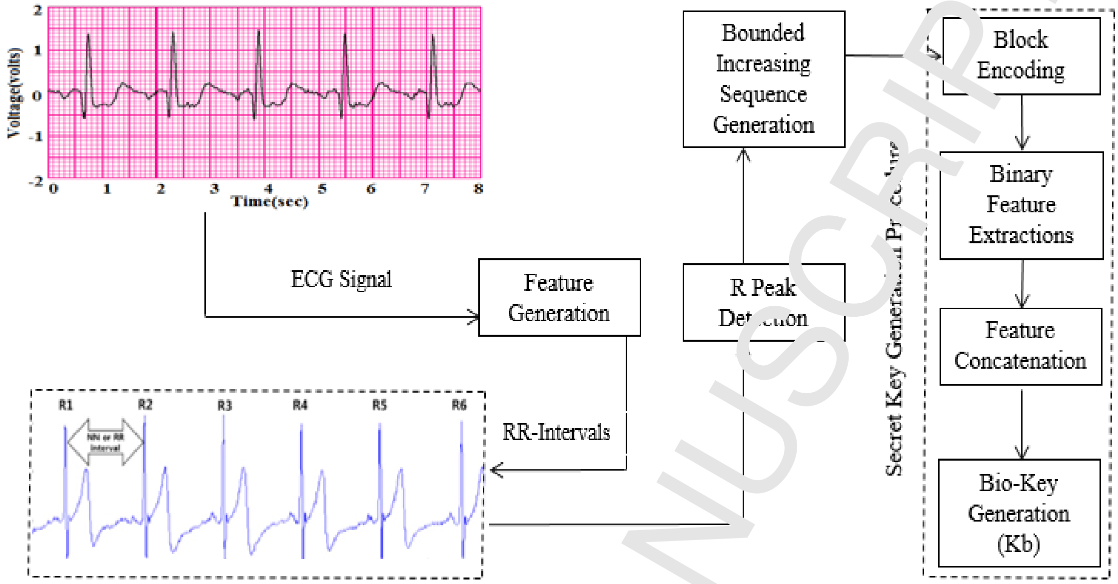


Fig.4. Physiological based key generation mechanism for security aspects in medical applications

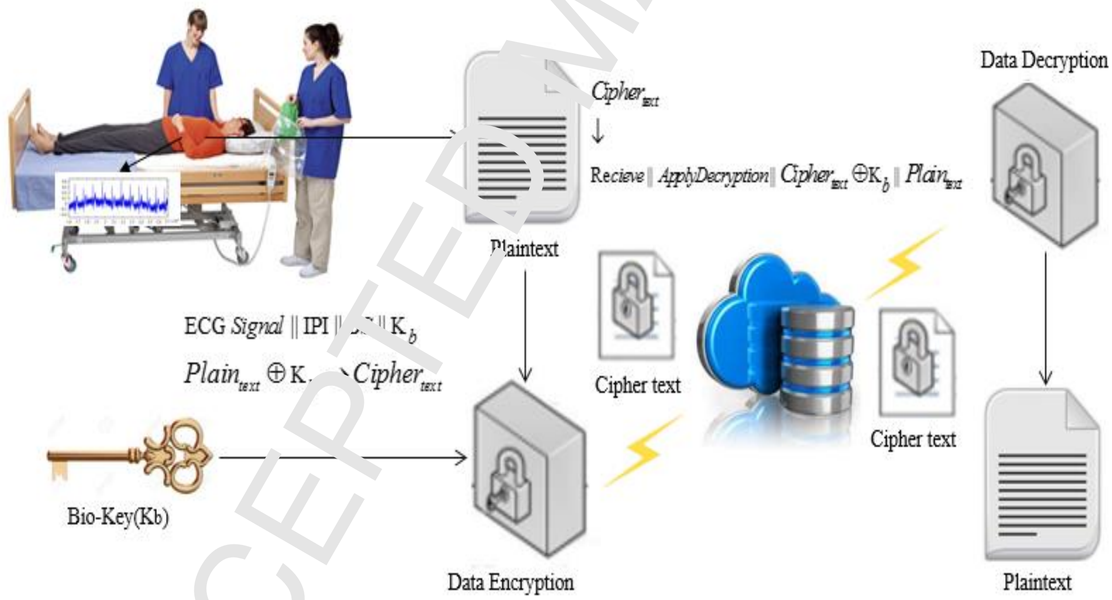


Fig.5. Proposed Security Framework for healthcare applications

It is necessary to check that bio-keys generated from ECG signals must possess properties of randomness and uniqueness. Firstly the 128-bit Kb should be sufficiently random to apply for security aspects of healthcare applications. Secondly, it also needs to be validated that different persons will produce distinctive

Kb. In the section, we have presented a complete mode for providing secure communication between the source and destination nodes as shown in Fig.5. Once the source node collects the medical information using wearable devices, ciphertext will be generated by means of applying logical operations between 128-bit Kb and plain text. In case any user wants to get medical data, the main step will be to check either secret key (Kb) matches or not. If the Kb matches then data can be transmitted between the source and destination devices. Generally, communication between medical devices in IoMT via wireless medium has two security phases. At the initial phase, secret keys are exchanged between nodes for that purpose Trusted Third Party (TTP) is widely used. At the second stage, utilization of generated secret keys for securing IoMT is done. The proposed framework has high significance at the second phase for implementing security in remote health monitoring, and the block diagram for patient's data confidentiality and security by utilizing the proposed framework is demonstrated in Fig.5. Initially, every medical device will produce bio keys, further, these keys will be used to generate ciphertext and then accumulated at the medical database server using TTP protocol. When a receiver request for patients information from the remote server, the secret key will be checked so that to main data privacy and security. If the Kb is matched, then cipher will be sent to the receiver. At last, the receiver will decrypt the ciphertext to acquire the original information. The chief benefits of the proposed framework are that it provides end-end health information security and also require less energy for securing IoMT.

5.3 Resource Optimization Model

The crucial issue of constructing joint energy and security model for medical data transmission over the internet of medical things (IoMT) networks is resource optimization. In this central model, the relationship is established between the length of the security key and the energy depletion. The energy-security coordination is a utility function f_{ut} that defines a relationship between energy consumption EC and security (Sect) as an aggregate objective function as depicted in eq.(3)

$$f_{ut} = \alpha EC + (1-\alpha)Sect \tag{3}$$

Whereas, α is the priority factor to prioritize the security or energy according to the need of the user and system.

It is observed and examined that as the length of the security key and energy drain increases than battery charge consumption will be increased and hence the shorter lifetime of the IoMT system, that is why the relationship as shown in eq.(4)

$$Charge = a \times m \times k^{b} + \zeta \tag{4}$$

Whereas, a and b are the coefficients, and m, k, ζ are the message size, key size and difference error between energy and security, respectively.

Suppose, that difference error ζ is minimal and can be neglected, then eq.(2) will be re-written as

$$\frac{Charge}{m \times k^{b}} = K \tag{5}$$

Whereby, K in eq.(5) is the constant

At given values of different security keys, further energy drain and the security level are calculated then coefficients are computed for overall performance optimization in IoMT system.

$$a = \frac{Ch\arg e}{m \times k^b} \tag{6}$$

$$b = \min_k \left[\sigma\left(\frac{Ch\arg e}{m \times k^b}\right) \right] \tag{7}$$

Whereas, σ shows the standard deviation between battery charge, security key and energy dissipation.

$$EC = e^{b \times k} \times a^m \tag{8}$$

Whereas, e is exponential, k is the length of the key, m is the message length with energy drain EC as represented in Eq. (6). Similarly, security analysis in association with energy dissipation is shown in eq.(9).

$$Sect = \left\lfloor \log_2 \left(\frac{EC}{a^m} \right)^{1/b} \right\rfloor_{k=2} \tag{9}$$

Eq.(9) depicts the logarithmic relationship between energy drain and the security for the IoMT system at the given value of the security key.

6. Experimental Results and Discussion

This section describes the performance results of the proposed joint resource-efficient and security approach for securing health information in IoMT. The foremost step is to estimate the quality of created bio-keys by using two crucial parameters including randomness and uniqueness. It is an essential requirement that physiologically based keys must not merely be sufficiently random but also retain anticipated individuality to ensure that the distinct human will yield totally different keys. Therefore, it is not easy for attackers to attain any valuable information regarding keying material or patient's data by capturing the ECG of any subject. In this study, ECG signals from 40 healthy subjects were employed for performing experimental analysis including lab environment and publicly available database physionet. Furthermore, IPIs are calculated from ECG to generate 128-bit bio-keys. The protocol for this research was approved by the Clinical Ethics Committee of the Xili People Hospital of Shenzhen, China. Written informed consent was obtained from subjects before the experiment.

6.1 Performance Evaluation of Bio-key

The randomness of the generated keys is one of the primary constraints for remote healthcare security. Entropy (E) is usually utilized for measuring the randomness by demonstrating the degree of uncertainty of the produced bio-keys as elaborated in equation (10).

$$E(x) = \sum_{i=1}^{n} P(x_i) \log P(x_i) \tag{10}$$

Fig.6 presents that the entropy of the generated keys is approximately 1, with the mean value of 0.9704. As a result, the yielded keys from different subjects elaborates the features of randomness.

To analyze the uniqueness of the produced keys, Hamming distance (HD) is widely used. HD between two bio-keys of identical sizes were applied to measure the uniqueness between them. Larger value of HD specifies that the generated 128-bit keys are efficient for securing real-time IoMT systems. The average HD of z-bit of biometric keys is estimated to be nearly z/2. Fig.7 demonstrates that the average HD value of yielded keys is 47.25%, which is approximately equal to 50%, so different subject's ECG are distinctive and have potential to be applied for IoMT based healthcare applications.

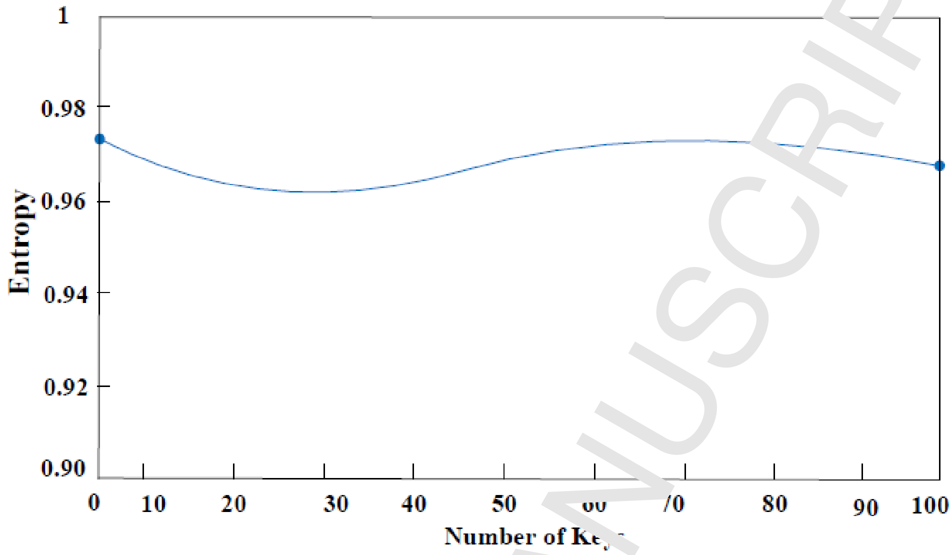


Fig.6. Entropy analysis of biometric-based 128-bit bio-keys

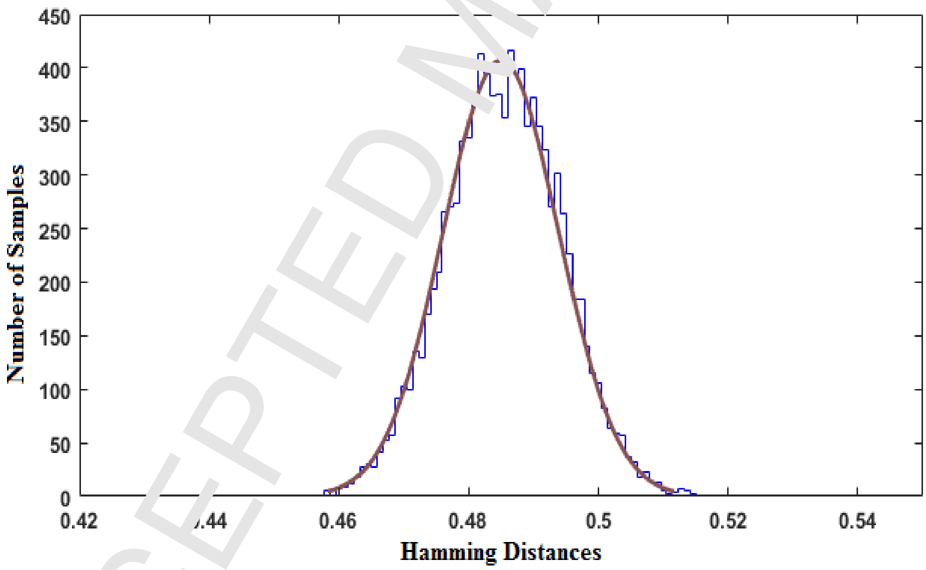


Fig. 7. Distinctiveness analysis of biometric-based 128-bit bio-keys

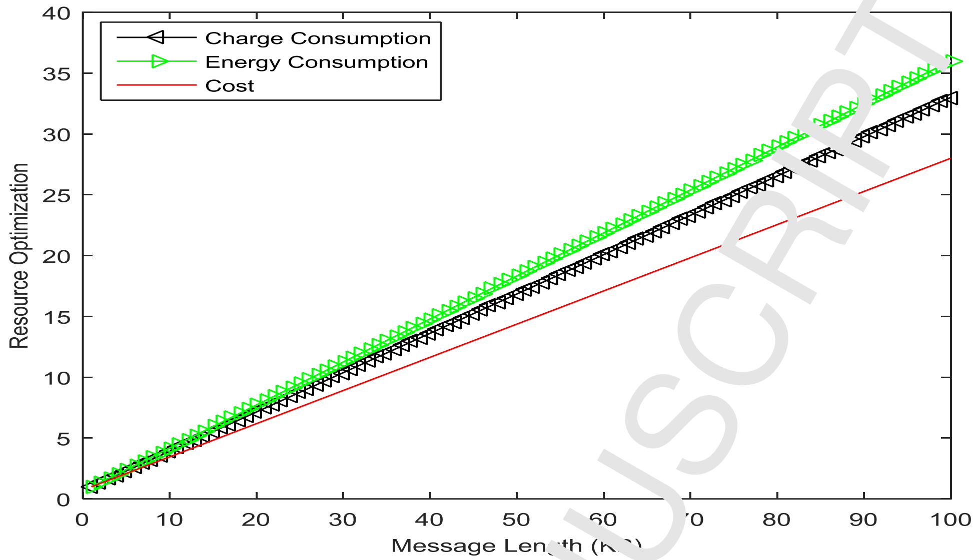


Fig.8 Relationship between number of security keys and Resource optimization

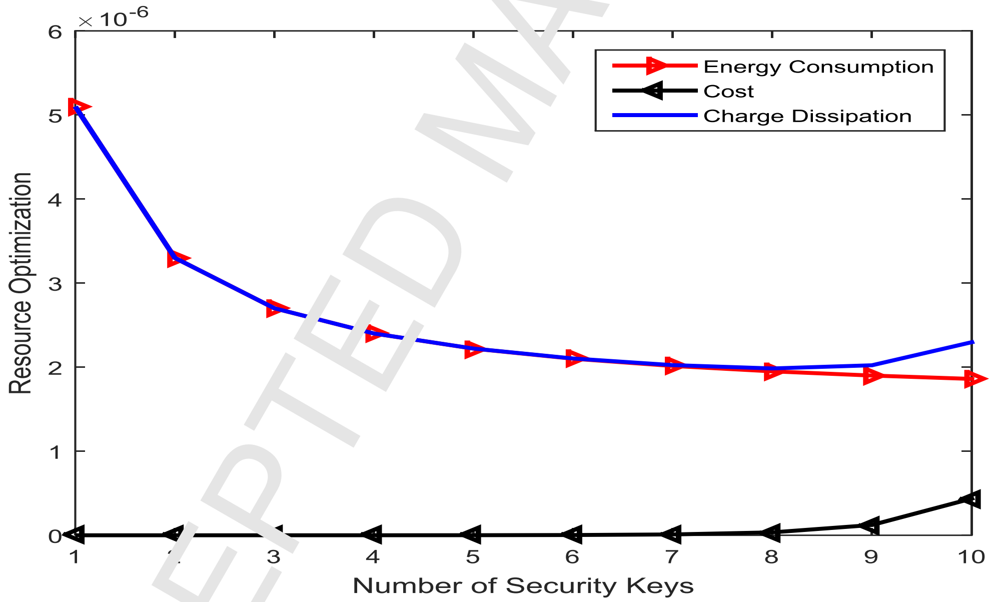


Fig.9 Trade-of between Message Length and Resource optimization

6.2 Resource Optimization Analysis

In Fig.8 we present the trade-off between a number of keys and resource (i.e., energy consumption, charge dissipation and cost). It is examined that cost is minimized significantly while energy and charge drains are exponentially decreasing with the increasing number of keys.

Fig.9, reveals the trade-off between message length and the resource optimization. It is observed that energy, charge drain, and cost linearly increases with the message length. Cost is optimized at a remarkable level, while energy and charge are drained at more level. Fig.10 shows the relationship between a number of rounds and the resource optimization, it is interpreted that energy consumption is less while charge drain is high with the increase of the number of rounds. Moreover, it is observed that resources are optimized efficiently.

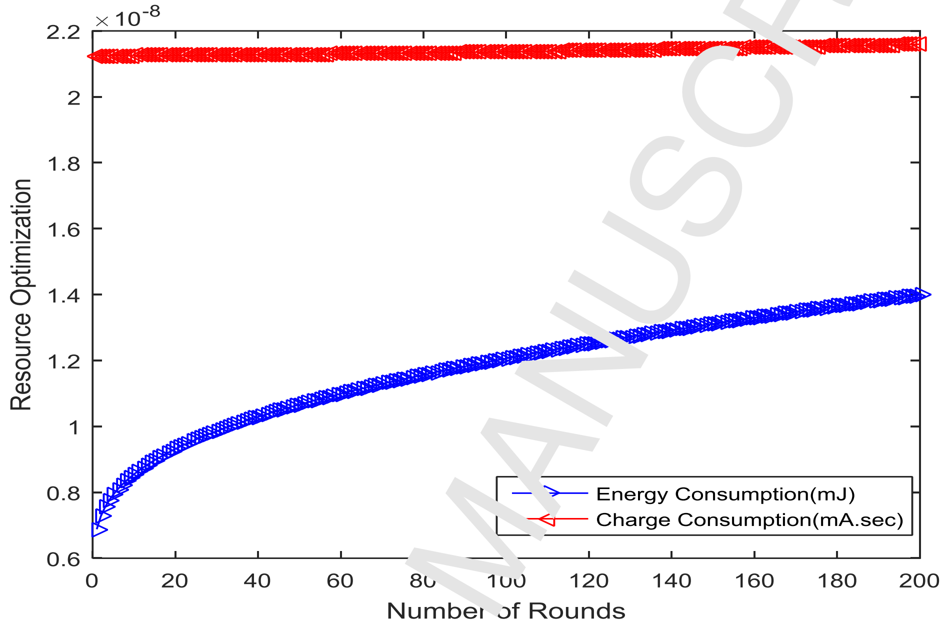
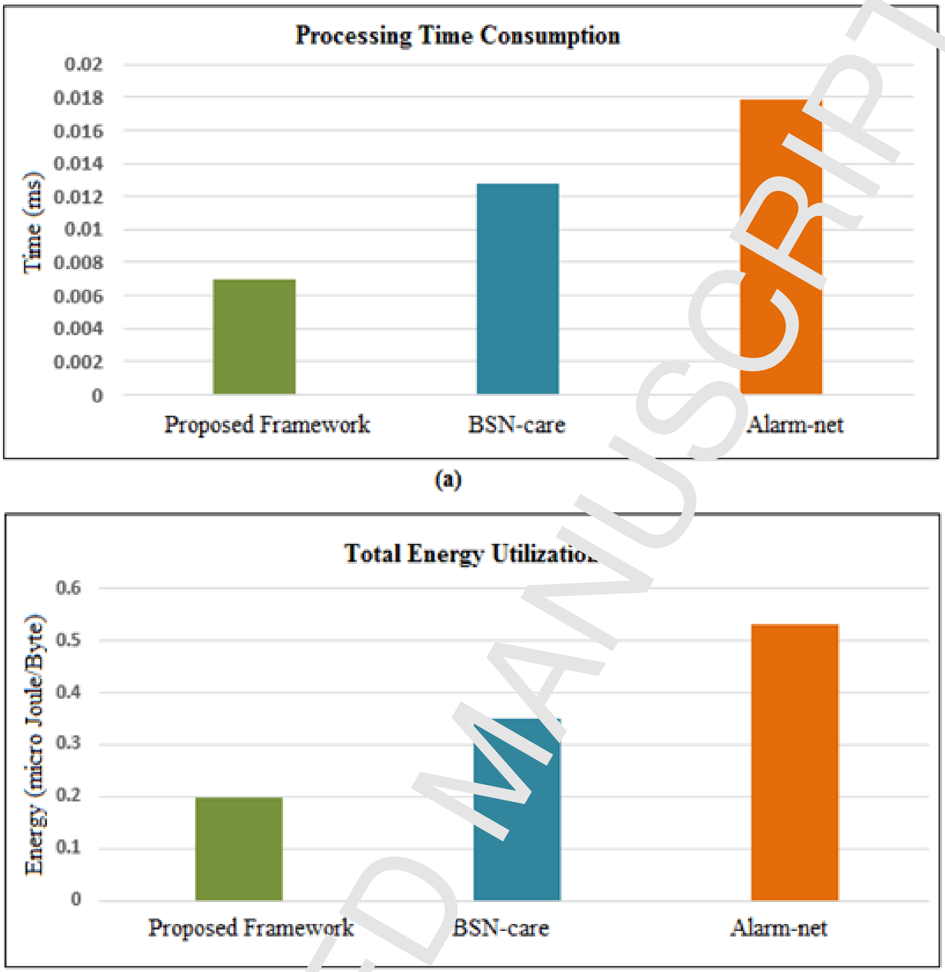


Fig.10 The relationship between number of rounds and resource optimization

6.3 Resource Consumption Comparison

Fig.11 (a) illustrates that the total processing time consumption for the proposed framework, Alarm-net, BSN-care, are 0.0068ms, 0.0128 ms and 0.01785 ms, respectively. It can be illustrated from the experimental analysis, that the detailed analysis of the proposed approach requires more processing time in comparison with existing techniques, therefore existing techniques are not cost-effective solution for securing IoMT based healthcare. In Alarm-Net, more processing cycles are needed to produce secret keys, so time is expended for the medical data encryption than the compared approaches. BSN-care uses simple practices, so it needs less encryption time for data encryption than alarm-net, but due to the utilization of external keys, BSN-care requires more cycles to generate random keys than the proposed approach. Therefore, in this study biometric keys are generated for providing a balance between processing time and security for IoMT systems.

It can be observed from Fig.11 (b) that the proposed framework consumes less energy than the conventional, traditional security methods for healthcare. Since biometric key generation procedure is applied in the proposed framework. Hence less energy is utilized. Therefore, the proposed IoMT based healthcare framework provides a resource-efficient and secure model for medical information transmission between patient and remote available doctors.



(b)

Fig.11 Resource consumption comparison of different method

7. Conclusion and Future Research

This research aims to develop joint resource aware and security framework for IoMT based remote healthcare systems. To offer stability in IoMT, we applied bio-keys generation mechanism for medical data encryption which is beneficial for reducing resource requirement of system. The experimental results reveal that generated biometric keys from different subjects are sufficiently random and unique thus can be used for securing IoMT. Moreover, proposed IoMT based healthcare framework requires less processing time and energy consumption than the compared approaches. The proposed framework also offers a trade-off between security and resource consumption in real-time hospital scenarios. This research not only decrease the economical healthcare solution but also guarantee the secure transmission of medical data between patients and physicians

It is our future, we hope to further conduct more experiments that would involve more number of medical devices with capability to acquire different signals including EMG, EEG, PPG and body temperature in IoMT systems. Moreover, we also hope to develop an adaptive bio-key generation mechanism so that it can provide different keys based on multiple heart rate bands for real-time healthcare.

Highlights of the Manuscripts

- We developed a joint resource aware and security model for healthcare applications
- A wearable platform is developed for bio-signal collection
- Physiological based Key Generation Mechanism is also developed
- The performance comparisons of proposed security model with existing methods

Acknowledgments

We appreciatively acknowledge the volunteers who contributed to this study. This work was supported in part by the Shenzhen Governmental Basic Research Grant (JCYJ20160331185848286, JCYJ20150529164154046), the National Natural Science Foundation of China under grants (U1613222, U16132228, 61873349), the Guangdong Province Natural Science Fund (2016A030310129), the Guangzhou Science and Technology Planning Project (201704020079, 201[illegible]0301009[illegible]), CAS President's International Fellowship for Visiting Scientists (2017VTA0011)

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] Lin, W. H., Wang, H., Samuel, O. W., Liu, G., Huang, Z., & Li, G. (2018). New photoplethysmogram indicators for improving cuffless and continuous blood pressure estimation accuracy. Physiological measurement, 39(2), 025005.

[2] A. H. Sodhro, A. K. Sangaiah, S. Pirphulal, A. Sekhari, and Y. Ouzrout, "Green media-aware medical IoT system," *Multimedia Tools and Applications*, pp. 1-20, 2018.

[3] S. Pirbhulal, H. Zhang, M. E. E Alahi, H. Ghayvat, S. C. Mukhopadhyay, Y.-T. Zhang, *et al.*, "A novel secure IoT-based smart home automation system using a wireless sensor network," *Sensors*, vol. 17, p. 69, 2016.

[4] Z. Ali, M. Imran, M. Alsulaiman, M. Shoaib, S. Ullah, Chaos-based robust method of zero-watermarking for medical signals, Future Generation Computer Systems, Vol. 88 (11), pp. 400-412, Nov, 2018.

[5] D. Lin, Y. Tang, F. Labeau, Y. Yao, M. Imran, A. V. Vasilakos, "Internet of Vehicles for E-health Applications: A Potential Game for Optimal Network Capacity", IEEE Systems Journal, Vol. 11 (3), pp. 1888-1896, sept, 2017.

[6] Pirbhulal, S., Shang, P., Wu, W., Sangaiah, A.K., Samuel, O.W. and Li, G., 2018. Fuzzy vault-based biometric security method for tele-health monitoring systems. Computers & Electrical Engineering, 71, pp.546-557.

[7] M. M. Rodgers, V. M. Pai, and R. S. Conroy, "Recent advances in wearable sensors for health monitoring," *IEEE Sensors Journal*, vol. 15, pp. 3119-3126, 2015.

[8] A. H. Sodhro, S. Pirbhulal, A. K. Sangaiah, S. Lohano, G. H. Sodhro, and Z. Luo, "5G-Based Transmission Power Control Mechanism in Fog Computing for Internet of Things Devices," *Sustainability*, vol. 10, p. 1258, 2018.

[9] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and Privacy in the Medical Internet of Things: A Review," *Security and Communication Networks*, vol. 2018.

[10] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework," *IEEE Consumer Electronics Magazine*, vol. 7, pp. 18-21, 2018.

[11] S. Pirbhulal, H. Zhang, S. C. Mukhopadhyay et al., "An efficient biometric-based algorithm using heart rate variability for securing body sensor networks," Sensors, vol. 15, no. 7, pp. 15067-15089, 2015.

[12] Z. Ali, M. Imran, M. Alsulaiman, T. Zia, M. Shoaib, A zero-watermarking algorithm for privacy protection in biomedical signals, Future Generation Computer Systems, Vol. 82, pp. 290-303, May, 2018.

[13] S. Pirbhulal, H. Zhang, W. Wu et al., "A comparative study of fuzzy vault based security methods for wireless body sensor networks." IEEE, 10th International Conference on Sensing Technology, 11-13 Nov, Nanjing, China, pp.57-62, 2016.

[14] W.-B. Lee, and C.-D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 1, pp. 34-41, 2008.

[15] T. Hayajneh, B. Mohd, M. Imran, G. Almashaqbeh, A. Vasilakos, Secure Authentication for Remote Patient Monitoring with Wireless Medical Sensor Networks, Sensors 2016, 16(4), 424; doi:10.3390/s16040424.

[16] W. Sun, Z. Cai, F. Liu et al., "A survey of data mining technology on electronic medical records," in Proceedings of the International Conference on E-Health Networking, Application and Services, pp. 1–6, 2017

[17] J.H. Abawajy and M.M. Hassan, "Federated internet of things and cloud computing pervasive patient health monitoring system", IEEE Communications Magazine, vol.55, no.1, pp.48-53, 2017.

[18] A.M. Rahmani, et al. "Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach", Future Generation Computer Systems, vol.78, no.1, pp.641-658, 2018.

[19] J. Kim, "Energy-efficient dynamic packet downloading for medical IoT platforms. IEEE Transactions on Industrial Informatics", vol.11, no.6, pp.1653-1659, 2015.

[20] A. A. Fadele, et al. "Internet of Things security: A survey." Journal of Network and Computer Applications, vol.88, pp.10-28, 2017.

[21] R. M. Sanaz et al. "End-to-end security scheme for mobility enabled healthcare Internet of Things." Future Generation Computer Systems, vol.64, no.2, pp.108-124, 2016.

[22] C. Tan, H. Wang, S. Zhong, Q. Li, "IBE-Lite: A lightweight identity-based cryptography for body sensor networks", IEEE Transactions on Information Technology in Biomedicine, vol.13, no.6, pp.926–932, 2016.

[23] A. Wood., et.al, "Wireless sensor networks for assisted-living and residential monitoring. University of Virginia Computer Science Department Technical Report" vol.2, pp.1-15, 2006.

[24] P. Gope., T. Hwang, "BSN-care: A secure iot-based modern healthcare system using body sensor network", IEEE Sensors Journal, vol.16, pp.1368-1376, 2016.

[25] G.-H. Zhang, C. Poon, and Y.-T. Zhang, "Analysis of using interpulse intervals to generate 128-bit biometric random binary sequences for securing wireless body sensor networks," IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 1, pp. 176–182, 2012.

[26] G. Zheng, G. Fang, R. Shankaran 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. 21, no. 3, pp. 655-663, 2017.

[27] S. N. Ramli, R. Ahmad, and M. F. Abdollah, "Electrocardiogram (ECG) signals as biometrics in securing Wireless Body Area Network." 8th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 536-541, 2013.

[28] S. Peter, B. Pratap Reddy, F. Momtaz et al., "Design of secure ECG-based biometric authentication in body area sensor networks," Sensors, vol. 16, no. 4, pp. 570, 2016.

[29] K. Saleem, H. Abbas, J. Al-Muhtadi et al., "Empirical Studies of ECG Multiple Fiducial-Points Based Binary Sequence Generation (MFBSG) Algorithm in E-Health Sensor Platform." IEEE 41st Conference on Local Computer Networks Workshops (LCN Workshops), pp. 236-240, 2016.

[30] H.-S. Choi, B. Lee, and S. Yoon, "Biometric authentication using noisy electrocardiograms acquired by mobile sensors," IEEE Access, vol. 4, pp. 1266-1273, 2016.

[31] C. C. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," IEEE Communications Magazine, vol. 44, no. 4, pp. 73-81, 2006.

[32] S.-D. Bao, C. C. Poon, Y.-T. Zhang, and L.-F. Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," IEEE Trans. Inf. Technol. Biomed., vol. 12, no. 6, pp. 772–779, 2008

[33] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in Proc. IEEE Conf. Comput. Commun., pp. 1862–1870, 2011.

[34] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker."A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-Allen and Hamilton Inc Mclean Va, vol. 1, no. 1, pp.1-164, 2001

[35] K. Venkatasubramanian, A. Banerjee, and S. Gupta, "EKG-based key agreement in body sensor networks," in IEEE INFOCOM Workshops April, pp. 1–6, 2008.

[36] O.W. Samuel, G.M. Asogbon, A.K. Sangaiah, P. Fang, and G. Li, "An integrated decision support system based on ANN and Fuzzy_AHP for heart failure risk prediction," Expert Systems with Applications, 68, pp. 163-172, 2017

[37] Pawar, P., Jones, V., Van Beijnum, B. J. F., & Hermens, H. A framework for the comparison of mobile patient monitoring systems. Journal of biomedical informatics, 45(3), pp.544-556, 2012.

[38] Samuel, O. W., Li, X., Geng, Y., Asogbon, M. G., Fang, P., Huang, Z., & Li, G. (2017). Resolving the adverse impact of mobility on myoelectric pattern recognition in upper-limb multifunctional prostheses. Computers in biology and medicine, 90, 76-87.

[39] Sodhro, Ali Hassan, Sandeep Pirbhulal, and Arun Kumar Sangaiah. "Convergence of IoT and product lifecycle management in medical health care." Future Generation Computer Systems , 2018.

[40] Sodhro, A.H., Sangaiah, A.K., Pirphulal, S., Sekhari, A. and Ouzrout, Y. Green media-aware medical IoT system. Multimedia Tools and Applications, pp.1-20, 2018.

[41] Pellionisz, Andras J., David L. Tomko, and Charles C. Jorgensen. "Artificial cerebellum ACE: tensor network transformer enabling virtual movement in virtual environment: facilitating teleoperation in telepresence." In Neural Networks, IEEE International Conference on, pp. 648-654. IEEE, 1993.

[42] Chandramohan, J., Nagarajan, R., Satheeshkumar, K., Ajithkumar, N., Gopinath, P.A. and Ranjithkumar, S., 2017. Intelligent smart home automation and security system using Arduino and Wi-fi. International Journal Of Engineering And Computer Science, pp.1-5, 2015.

[43] Serena, Thomas E., Caroline E. Fife, Kristen A. Eckert, Raphael A. Yaakov, and Marissa J. Carter. "A new approach to clinical research: Integrating clinical care, quality reporting, and research using a wound care network‐based learning healthcare system." Wound Repair and Regeneration 25, no. 3 (2017): 354-365.

[44] Larburu, N., Bults, R.G., Van Sinderen, M.J. and Hermens, H.J. An ontology for telemedicine systems resiliency to technological context variations in pervasive healthcare. IEEE journal of translational engineering in health and medicine, 3, pp.1-10, 2015.

[45] He, D. and Zeadally, S.,. Authentication protocol for an ambient assisted living system. IEEE Communications Magazine, 53(1), pp.71-77, 2015.

[46] M. Huang, A. Liu, T. Wang, and C. Huang, "Green data gathering under delay diferentiated services constraint for internet of things," Wireless Communications and Mobile Computing, vol. 2018, Article ID 9715428, 2018.

[47] Wu W.; Pirbhulal S.; Sangaiah AK.; Mukhopadhyay SC.; Li G. Optimization of signal quality over comfortability of textile electrodes for ECG monitoring in fog computing based medical applications. Future Generation Computer Systems. pp.1-19,2018.

[48] Pirbhulal, S.; Zhang, H.; Mukhopadhyay.; Wu, W.; Zhang, Y.-T. Heart-Beats Based Biometric Random Binary Sequences Generation to Secure Wireless Body Sensor Networks. IEEE Transactions on Biomedical Engineering, vol.18, no.1, http://ieeexplore.ieee.org/document/8314739, pp.1-9, 2018.

[49] Wu, W., Pirbhulal, S. and Li, G., 2018. Adaptive computing-based biometric security for intelligent medical applications. Neural Computing and Applications, pp.1-10, 2018.

[50] Bernard, T.; Nakib, A. Adaptive ecg signal filtering using bayesian based evolutionary algorithm. Metaheuristics for medicine and biology, Springer, 2017, 17, 187-211.

[51] Gong, Y.; Gao, P.; Wei, L.; Dai, C.; Zhang, L.; Li, Y. An enhanced adaptive filtering method for suppressing cardiopulmonary resuscitation artifact. IEEE Transactions on Biomedical Engineering 2017, 64, 471-478.

[52] Belchandan, A.K.; Deshmukh, K.; Kumar, J. Removal of noises in ECG signal by using a digital fir-iir filter in vhdl. Digital Signal Processing 2016, 8, 135-139.

Dr. Sandeep Pirbhulal received his Ph.D. degree in Pattern Recognition and Intelligent Systems with the University of Chinese Academy of Sciences in 2017. He is currently working as Postdoc Fellow at CAS Key Laboratory of Human-Machine Intelligence-Synergy Systems, Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences (SIAT-CAS). Dr. Pirbhulal has a vast experience of 6 years in Academia & Research. His current research focus on wireless body sensor networks (WSNs), privacy and security for WSNs, and Internet of Medical Things. He has published more than 30 international journal articles including IEEE TBME, IEEE Sensor Journal, and IEEE JBHI among others, over 5 international conference proceeding papers, and 4 book chapters. He is also an assistant professor at College of Computing and Information Sciences (CoCIS, 2013-2014), Karachi, Sindh, Pakistan. He is Guest Editor of peer-reviewed international journals i-e IEEE Access, Journal of Medical Imaging and Health Informatics (JMIHI) etc. He served as reviewer for exceed 10 international journals such as IEEE Sensor Journal, IEEE Access. He received an award of "Visiting Scientist" form Massey University, New Zealand in 2016.

Dr. Samuel Oluwarotimi Williams, a research fellow with the Center for Neural Engineering, Shenzhen Institutes of Advanced Technology, China, received his Ph.D. degree from the University of Chinese Academy of Sciences in Pattern Recognition and Intelligent Systems. His outstanding research contributions has earned him a number of awards including the outstanding youth innovation research fund, best Ph.D. Thesis award, and best paper award at the International Conference on Biomedical Engineering and Health Informatics (ICBHI 2015) among others. In addition, Dr. Samuel has published more than 60 peered-reviewed articles in reputable international journals/conferences. Dr. Samuel currently serves as a reviewer for a number of reputable international peer-reviewed journals including IEEE Communications Magazine (IEEE Comm. Mag.), IEEE Transactions on Neural Systems & Rehabilitation Engineering (IEEE TNSRE), among others. His research focus is on Rehabilitation robotics, Biomedical signal processing and control, Clinical decision support systems, and Computational intelligence.

Dr. Wanqing Wu received his BS degree in computer science and technology from Hunan Normal University, Hunan, China, in 2004, an ME in computer science from Chongqing University, Chongqing, China, in 2007, and a PhD from the Pusan National University of Computer Engineering, Korea, in 2013. He is currently an Associate Professor at the Institute of Biomedical and Health Engineering, Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China. He also works within the Key Laboratory for Health Informatics of the Chinese Academy of Sciences, China. His research interests include wearable sensing technology, biomedical signal sensing and processing, body sensor networks, biofeedback, biometric security, internet of things and multimodal medical data fusion. Dr Wu has published over 40 papers in renowned journals and conferences, mostly in the area of wearable sensor technology, wireless body sensor network and Internet of Medical Things, and has also contributed to the peer review of 10 journals. He has secured over 15 major competitive research grants.

Dr. Arun Kumar Sangaiah has received his Master of Engineering (ME) degree in Computer Science and Engineering from the Government College of Engineering, Tirunelveli, Anna University, India. He had received his Doctor of Philosophy (PhD) degree in Computer Science and Engineering from the VIT University, Vellore, India. He is presently working as an Associate Professor in School of Computer Science and Engineering, VIT University, India. His area of interest includes software engineering, computational intelligence, wireless networks, bio-informatics, and embedded systems. He has authored more than 100 publications in different journals and conference of national and international repute. His current research work includes global software development, wireless ad hoc and sensor networks, machine learning, cognitive networks and advances in mobile computing and communications. Also, he was registered a one Indian patent in the area of Computational Intelligence. Besides, Prof. Sangaiah is responsible for Editorial Board Member/Associate Editor of various international journals.

Dr. Guanglin Li received the Ph.D. degree in biomedical engineering from Zhejiang University, China, in 1997. During 1999-2002, he worked as a Postdoctoral Research Associate in the Department of bioengineering, the University of Illinois at Chicago, on the studies of electrocardiography and electroencephalography inverse problems and cardiac electrophysiology. From 2002 to 2006, he was a senior Research Scientist at BioTechPlex Corporation, where he worked on the research and development of biomedical and biological products. From 2006 to 2009, he was with the Rehabilitation Institute of Chicago (the best rehabilitation hospital in America for 19 consecutive years), where he was a Senior Research Scientist in the Neural Engineering Center for Artificial Limbs and with Northwestern University, where he was an Assistant Professor of Physical Medicine and Rehabilitation, Chicago. Since 2009, he has been with Shenzhen Institute of Advanced Technology (SIAT), Chinese Academy of Sciences, where he is currently a Professor in the Research Center for Neural Engineering at Institute of Biomedical and Health Engineering.


Dr. Sandeep Pirbhulal


Dr. Samuel Oluwarotimi Williams


Dr. Wanqing Wu


Dr. Arun Kumar Sangaiah


Dr. Guanglin Li

Highlights of the Manuscripts

- We developed a joint resource aware and security model for healthcare applications
- A wearable platform is developed for bio-signal collection
- Physiological based Key Generation Mechanism is also developed
- The performance comparisons of proposed security model with existing methods