Future Generation Computer Systems 98 (2019) 109–119

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Biometric-based authentication scheme for Implantable Medical Devices during emergency situations

Taha Belkhouja [a,*], Xiaojiang Du [b], Amr Mohamed [c], Abdulla K. Al-Ali [c], Mohsen Guizani [a]

[a] University of Idaho, United States
[b] Temple University, United States
[c] Qatar University, Qatar

HIGHLIGHTS

- ECG signals can provide a random source for securing any Implantable Medical Device communication.
- The combination between ECG and fingerprints creates a light but efficient secure authentication.
- Biometrics perform well in the security and privacy of any Implantable Medical Device.
- Emergency situations are no longer ignored in the security protocols of Implantable Medical Devices.

ARTICLE INFO

Article history:
Received 22 October 2018
Received in revised form 22 January 2019
Accepted 2 February 2019
Available online 8 February 2019

Keywords:
Implantable Medical Devices
Emergency access
Biometric readings
Wireless authentication

ABSTRACT

Biometric recognition and analysis are among the most trusted features to be used by Implantable Medical Devices (IMDs). We aim to secure these devices by using these features in emergency scenarios. As patients can witness unpredictable lethal accidents, any implantable medical device should allow access to urgent medical interventions from legitimate parties. Any delay in providing immediate medical support can endanger the patient's life. Hence, we propose in this work an authentication scheme that allows access to the implanted devices in emergency situations for only legitimate users. We have designed in the first place a scheme for authentication using Electrocardiogram instantaneous readings. Then, we joined the latter to a fixed biometric reading, which is fingerprint reading, to enable access to emergency medical teams. We have designed a scheme in a way to prevent attackers from accessing/hijacking the device even during emergency situations. This scheme has been assisted with elliptic curve cryptography to protect the wireless exchange of requested keys. The scheme relies on the instantaneous reading of the patient's heartbeat and his/her fingerprint reading to create a secure key. This key will validate the authentication request of the new medical team. We have analyzed this scheme deeply to verify that they offer the necessary security for the patient's life. We have tested if the wireless exchange of the key will expose the device's privacy. We have also tested the accuracy of the authentication process to ensure a safe and a valid performance of the authentication process. The scheme has been designed with consideration to any hardware/software limitation that characterize any implantable medical device.

1. Introduction

Wearable or Implantable Medical Devices (IMD/WMD) are becoming essential to improve patients quality of life. Their remote use to all different health issues provides a better and more efficient way to treat chronic and normal diseases. Meanwhile, an IMD should guarantee the privacy of the patient. The use of electronic devices exposes the patient's life and his/her information to different threats. Researchers are aware of the severe limitations of IMDs regarding energy consumption and low resources. For this reason, their goal is to find the best trade-off between efficiency and security. This solution needs to guarantee that access is provided for the patient and any other authorized party, while protecting the user at the same time from any other malicious agent.

Focusing on the unique goal of the protection of the IMD's access from malicious threats, designers might endanger the patient's life during some scenarios. One of these critical scenarios is that health complications may occur suddenly in unpredictable times. This usually leads to an emergency medical team to take immediate action to save the patient's life. If the IMD's access scheme does not consider such events, the IMD will prevent the medical team to interact with the patient's health and will endanger his/her life more. In another case, the IMD will open its access for any emergency team. This will expose the privacy of the user

* Corresponding author.
E-mail address: belk7517@vandals.uidaho.edu (T. Belkhouja).

https://doi.org/10.1016/j.future.2019.02.002
0167-739X/

to any attacker in the surroundings. Therefore, an authentication scheme that provides a solution for this problem must be included in the IMDs' access schemes. However, these schemes must be well-studied. If not, it will present an open door for hackers to attack the system.

To defend this threat, biometrics are among the solutions that have been studied. One of these biometrics is fingerprints. The patterns they provide are proven to relate uniquely to one person. This makes fingerprint a key feature to be used for authentication. Scanning the literature, several schemes have been proposed to secure general IMD access. To alleviate security vulnerabilities of IMDs, Ankarli et al. [1] presented a technique for physical layer authentication. This technique allows IMDs to avoid using any existing methods of cryptology. They provided also in their work some techniques to provide additional advantages for IMD implementations. They improved the processing complexity of IMDs algorithms and enhanced the overall communications performance. As for Kim et al. [2], they introduced a new vibration-based secure side channel to be used for IMD security. They provided the necessary analysis to prove the robustness of their scheme. The vibration signal was used as a wake-up signal and their analysis was established in a human body realistic model. Additionally, Long et al. [3] presented a study where an authentication protocol is based on the recognized standards of AES and SHA. They also demonstrated an encryption protocol for the same purpose and a model that protects against multiple network threats. Also, Chi et al. [4] presented in their work an encryption algorithm to encrypt and compress the IMD data simultaneously. This compression will reduce the data transmission overhead and also ensures a high data confidentiality and usability. Their scheme was based on smartphones as a proxy to undertake most of the security-related tasks. The smartphone had the task to establish a connection between the IMD and the doctor, responsible for all operations on patients using IMDs, a secure channel. Their work is based on secret key sharing that were extracted from a physically inaccessible seed by outsiders. Other researchers focused on key management [5–8] as an essential tool for security and several other papers (e.g., [9–14]) have studied related security issues. The main common point between these previous schemes is that they rely on the knowledge of both ends to each other, or that they both request to establish a link. These schemes may under emergency situations, e.g., loss of consciousness, medical situation in a foreign city, prevent an emergency medical team to interfere with the IMD. Without the user's or the IMD's doctor acknowledgment, the security schemes are intended to prevent any additional access to the IMD's functions.

In our previous work [15], we have exploited ElectroCardioGraphic (ECG) signals to authenticate the emergency staff. The scheme allows a non-previously-authenticated party to obtain access to the IMD for emergency interventions. This scheme creates a backdoor in IMDs that does not block access under emergency situations to unknown parties. Emergency scenarios are usually critical for the user, he/she may not have enough time to wait for his/her doctor or medical team to interfere with the IMD to help with his/her sudden medical condition. In the same time, the user's consciousness is not guaranteed to allow an emergency medical team to interfere with the device. However, the IMD has to make sure that the new device that will be given access is a legitimate one through a signature. This signature can be verified and validated by the IMD using the established key. This secret key is to be computed within both devices. The wireless communication that takes place will not enable any malicious eavesdropper to estimate the resulting key. This can be placed using elliptic curve cryptographic properties. This scheme is to be used only in emergency situations. If the mechanisms were triggered in normal situations, the user would be notified and he/she has the possibility to interrupt it and takes the needed precautions. To enhance this idea, we have extended in this work the previous scheme to use two biometric readings to authenticate any new user. Based on our previous analysis on the ECG readings, we have designed a two-factor scheme to create a publicly-shared key to permit the new team to access the IMD. We designed this scheme in a way that one biometric is an instantaneous reading, and the second is an unchanging reading that is unique to each individual. Fingerprint authentication has always attracted the engineers' attention to secure electronic devices. Several research has exploited fingerprints' readings to maximize their trustworthiness in any access schemes like in [16–20].

We have designed this scheme in which the IMD access is based on these two biometrics while focusing on minimizing the analysis cost on both features and avoid sharing them publicly during all authentication requests from any legitimate device.This authentication can be triggered through an emergency flag during the access request. Upon approval, this scheme will be as a backdoor to access the IMD without the need for the user's knowledge. The scheme can be also in use for regular authentication, but its main goal is to guarantee legitimate access to the IMD when the user is unconscious.

The motivation behind this scheme is to guarantee foreign interventions with the IMD under emergency scenarios. The main purpose of the IMD is offering spatial freedom and remote health supervision. Also, the IMD should be well-protected against exterior threats, hence the fact that only the IMD technician and the patient's doctor should have direct access to the IMD, in addition to the user itself. However, for certain common medical conditions like diabetes and seizures, the patient may suddenly lose his conscious and needs immediate attention from the closest qualified medical team. Lacking the means to authenticate and obtain access to the IMD, the patient's life is threatened if the IMD does not hold backdoor access for before-mentioned scenarios. Consequently, we have elaborated the work presented in this paper to alleviate this problem while guaranteeing the patient's privacy and security. Under unsecure conditions, such scenarios represent an opportunity for attackers to hijack the IMD for present or future attacks.

Therefore, the main contributions in this paper can be summarized as follows:

- Propose a new model to secure IMDs to authenticate their data.
- Design an efficient scheme that provides a secure access for non-previously identified entities during emergency scenarios.
- Investigate the use of ECG signals and fingerprints as biometrics readings for entity authentication.

The remainder of this paper is organized as follows: Section 1 introduces this work, its contributions and the similar works in the field. Section 2 presents the design of the one-factor scheme used for authenticating new devices to the IMD. Section 3 presents how a second factor is added for the authentication scheme to reinforces the previous one. Section 4 analyzes how the security issues are defended throughout this work. Section 5 shows the analysis results achieved while studying both schemes. Finally, Section 6 concludes the paper.

2. One factor authentication

2.1. Goal

As a first step in this work, we want to use ElectroCardioGraphic (ECG) signals as a biometric to authenticate emergency medical staff. The scheme we designed plays the role of a backdoor in IMDs for emergency situations. This scheme grants access for legitimate non-previously authenticated parties that need control over the

Fig. 1. Normal ECG waveform.

IMD to monitor the patients' life. At the same time, the IMD should ensure that the new authenticated device is a legitimate node. To achieve this purpose, our design will allow an external device to synchronize with the IMD to obtain a shared secret key. The shared key is used to create a signature related to the message sent to the IMD. On the IMD level, the signature can be validated or rejected by applying the secret key. In our design, we intend to prohibit any malicious eavesdropper on the wireless communication to estimate the resulting key. For this reason, we adopted the elliptic curve cryptographic properties. This scheme is to be used only in emergency situations. If the mechanisms are triggered under normal circumstances, the user would be notified and he/she has the possibility to interrupt it and take the needed precautions.

2.2. ECG signal acquisition

ElectroCardioGraph (ECG) [21] records depict the electrical activity of the heart. It is the time series of the electrical oscillations of the heart cyclic rhythm. ECG is very useful to inform that:

- The heart cycle is being normal, too slow, too fast or irregular by the duration of the electrical activity.
- The performance of the heart muscle and its chambers is normal or abnormal. This is described by the different magnitude of the electrical activities.

The frequency range of an ECG signal is generally within [0.05,100] Hz and its dynamic range is about 1 mV to 10 mV. The performance of ECG acquisition system depends mainly on the accuracy and reliability of the detection of the QRS complex, as well as T- and P-waves. Fig. 1 illustrates the electrical signal variation describing the rhythm of a typical healthy person's heart. This periodic variation consists mainly of a PR interval representing the time that takes the electrical activity to move between the atria and ventricles and a QRS interval describing the depolarization of the ventricles. A third interval is also to be considered important which is the ST segment. The latter describes the time between depolarization and repolarization of the ventricles. The duration of the heartbeat can be identified by measuring the time interval between two consecutive R peaks. This can be achieved by an external sensor on the wrist of the patient, for example. This sensor will communicate with the IMD using emergency flags, in order to synchronize with the device and acquire a synchronized ECG signal. Afterwards, the sensor will send the data to the medical team device for further analysis.

2.3. Elliptic curve cryptography

In 1985, Elliptic Curve Cryptography (ECC) was presented by Miller [22] of IBM and Koblitz [23] of the University of Washington as an adequate alternative in cryptographic schemes for the traditional cryptosystems, e.g., DSA and RSA. ECC systems perform

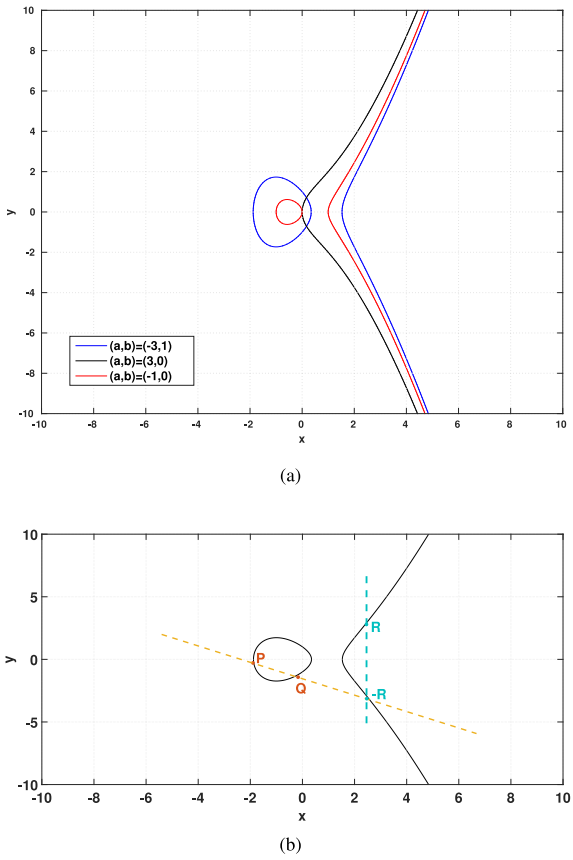

Fig. 2. (a) Elliptic curves for different (a, b) pairs and (b) the graphical resolution of an elliptic curve system.

robustly even with short keys and have lower computational overhead compared to the traditional methods. This becomes important when the devices in question suffer from serious limitations in processing power, memory, and battery life [24].

We intend to exploit the hard-to-solve discrete log problem with ECC to secure the authentication between the two new devices. This problem is as follows:

$$\begin{cases} \text{Given } g \text{ and } PK \\ \text{For } PK = f(g, SK) \\ \quad f : (a, b) \rightarrow a^b \end{cases} \Rightarrow \text{Find } SK.$$

For this purpose, each end, separately, would generate randomly its secret key SK_i. Then, each will compute its public key $PK_i = f(g, SK_i)$ and share it with the other end wirelessly. The function f is most likely to be the modular exponentiation [25]. After sharing the public key, both parties would achieve a final key $FK_i = f(SK_i, PK_j)$. Due to the properties of ECC, both are sharing the same secret $FK_i = FK_j$. This can be achieved publicly if a group G and a fixed group element g are previously agreed upon.

In more details, the elliptic curve is given by Eq. (1):

$$y^2 = x^3 + ax + b \tag{1}$$

where x, y, a and b are elements in a Galois Field [24]. The pair (a,b) defines the elliptic curve. An example of these curves with different (a,b) pairs is described in Fig. 2. The group of the elliptic curve is closed under the addition operation given by:

$R(x_R, y_R) = P(x_P, y_P) + Q(x_Q, y_Q)$, such that

$$\text{if } x_P \neq x_Q : \begin{cases} \alpha = \dfrac{y_Q - y_P}{x_Q - x_P} \\ x_R = \alpha^2 - x_P - x_Q \\ y_R = \alpha \times (x_P - x_R) - y_P \end{cases} \quad (2)$$

$$\text{if } x_P = x_Q : \begin{cases} \alpha = \dfrac{3 \times x_P^2 + a}{2 \times y_P} \\ x_R = \alpha^2 - 2 \times x_P \\ y_R = \alpha \times (x_P - x_R) - y_P \end{cases} \quad (3)$$

For the computation of $R = k \times P$, all what we need to do is compute

$$R = \underbrace{P + P + \cdots + P}_{\text{k times}} \quad (4)$$

For our design, the point R represents the final shared secret key, k represents the individual secret key and P represents the shared key. The Elliptic Curve Discrete Logarithm Problem given here, is that, with a prior knowledge of P and R, it is practically unfeasible to obtain k such that $R = k \times P$.

2.4. Security scheme

The average inter-beat time of any human heart is between 665 ms and 1.5 s. In order to guarantee the achievement of synchronized keys, we had to verify if both acquisitions (the IMD and the sensor) will include the same readings. In the literature, the average latency time for an IMD to detect electric signals on a body-level wireless communication is defined to be 200 ms [26] in the worst case. Therefore, both devices will synchronize their acquisition while taking into accounts these delays. A threshold is computed accordingly to the R-peak frequency in order to discard any out-of-sync heart beat. This will ensure that both devices will record similar ECG acquisitions.

Fig. 3 demonstrates the procedure of establishing a secret key. This key will be used for request validation. The shared secret key will finally be $Seret\_Key = k_a \times R_b = k_b \times R_a$. Both devices have the necessary variables to compute it. k_a and k_b could be:

- Random numbers generated independently in the IMD and the medical team system, respectively.
- Numbers specific to the devices themselves, like hidden PIN or ID numbers. This can be the case when a decreased computational work is desired.

In order to generate the pair (x_P, k) of the Elliptic-Curve algorithm, the measured values of R–R intervals in *ms* will be converted into a binary format. Table 1 explains an example of this conversion when a 4-bit value is assigned to each measure. The range of the values recorded is to be divided into 2^{bits} intervals limited by th_i.

Fig. 4 explains the extraction process. Each part computes the secret key from the initial keys acquired from the ECG signal.

3. Two factor authentication

3.1. Goal

The second factor we intend to add to our authentication scheme in this work is fingerprint readings. The shared key at this level is a result of a two-way function that has the ECG reading and the fingerprint data as inputs. We intend to use the fingerprint scan as a second proof for the IMD that the party requesting authentication is a legitimate party and is with the IMD user. This scheme allows the medical team to gain access to the IMD without the need of the user permission, even if they were never

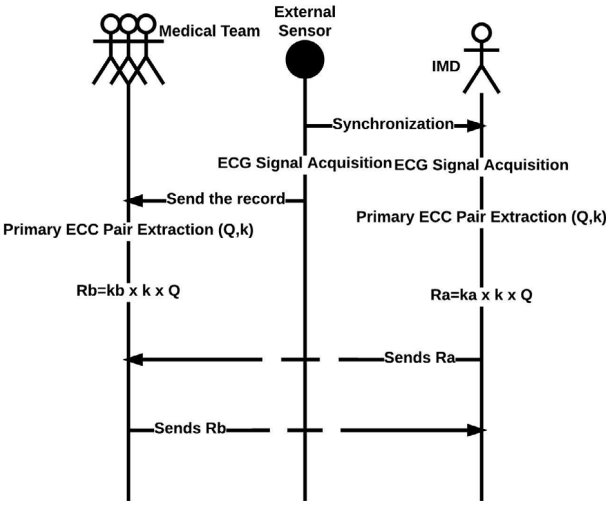

Fig. 3. Secret key establishment protocol.

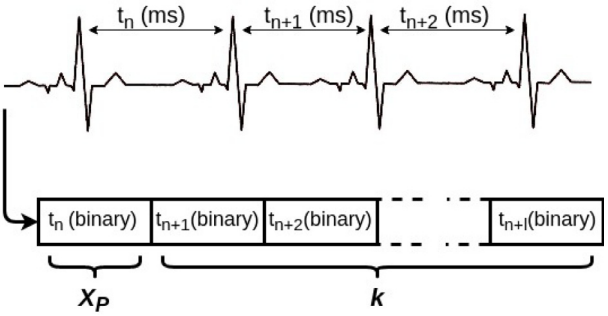

Fig. 4. Keys extraction from inter-beat values.

authenticated before. The team will acquire the fingerprint of the user in the moment of the emergency and will use to form the authentication key. As for the IMD, it will use the stored fingerprint data in its system to verify the integrity of the received key. If the received key is in conform with the generated key, the IMD will accept any request from the medical team's end.

3.2. Fingerprint recognition

Human fingerprints have been widely used to identify the person's identity as they have been proven to be unique to each individual. Human fingerprints show particular permanent patterns that are associated with the identity of that person. They are considered as one of the most reliable human features that can be easily acquired [27]. The fingerprints are constituted of ridges, called minutiae. The most notable types of minutiae are ridge ending and ridge bifurcation. These two allow an automatic matching between different fingerprints when detected. A minutia is characterized by a list of attributes that includes its type (as shown in Fig. 5), its position within the fingerprint scanned and its orientation. These three attributes help match the different minutiae along the fingerprints, the more similar they are, the more likely the fingerprints are associated to one individual.

Several approaches have been proposed to achieve a strong fingerprint matching technique. This is due to the fact that several assumptions had to be taken for fingerprint matching:

- When scanned, the fingers may be placed in different locations during acquisition, resulting therefore in a translation or in a rotation of the fingerprint.

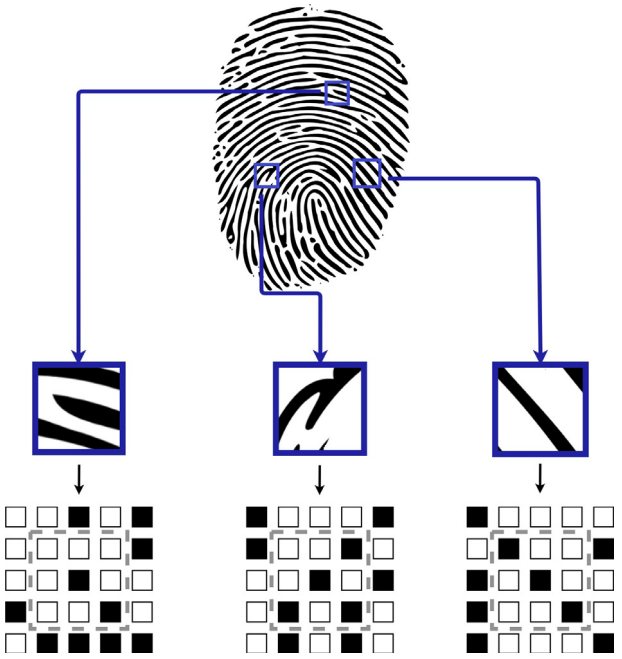

Fig. 5. Left to right: Continuous ridge, ending ridge and bifurcation examples for minutiae detection and identification.

Table 1
Look-up table for conversion measures.

Measured value	Binary value
$\geq th_i$	0100
$\geq th_{i+1}$	0101
...	...
$\geq th_{i+n}$	1110

- Non-linear deformation may take place during the acquisition process due to the finger pressure on the sensor.
- Two different scans of the same fingerprint can lead to two results with some different minutiae.

3.3. Fingerprint reading

3.3.1. Image processing

As a common procedure, a pre-process of the acquired fingerprint image takes place before the extraction of its feature [28]. To improve the image, an histogram equalization is applied on the image to increase the contrast of the image lines. This enhances the detection of the features. After this, a normalization [29] takes place. This gives the fingerprint image a balanced data magnitudes, matching a pre-defined mean and variance elaborated by the algorithm. Following this step, the direction and frequency of ridges are estimated following local ridges orientation and their local frequencies. After these steps, the image is converted to a black-and-white image. This step is intended to help in the segmentation of the fingerprint. Finally, an image thinning takes place to define the lines of the fingerprint features on a single-pixel level. Therefore, minutiae can be extracted at each pixel level with a 3×3 filter. The filter detects, according to the black pixels representing the fingerprint's ridges, the type of that ridge. Fig. 5 shows some examples of minutiae detection within a 3×3 pixels filter (discontinuous line). A continuous line along the filter means there is a continuous ridge, so no minutiae are located on those coordinates. If the pixel shows a ridge end (white pixels) or a bifurcation, then a minutia is detected and its characteristics are extracted.

This process is not implemented in the IMD. The stored fingerprint will be received after the processing of the scans. As for any future acquisition, it will be processed by auxiliary devices. Therefore, we have not accommodated this step for the IMD, as it is independent. It is better that the IMD is not burdened by this processing scheme in its configuration.

3.4. Minutiae matching

To match the fingerprint scanned with another one, the minutiae matching rate is the metric used to identify similarities between both. The first step before computing the matching rate is to align the fingerprints according to local minutiae structures. This improves the miscalculation due to the translation or the rotation of the fingers while acquiring the print. After the alignment, every two minutiae (each belongs to a different fingerprint) in a close location and orientation are paired together and are considered as a corresponding pair. The more corresponding pairs are between two fingerprints, the higher the matching score is. After a full analysis of the database and the scan quality, a threshold is set for the score to define the minimum score that needs to be obtained to consider both fingerprints as similar. Several algorithms exist in the literature that provide this step [30–32].

3.5. Scheme

Starting from the first use of the IMD implementing the security scheme presented in this work, the user will have his/her fingerprint stored in the device. This information will be used later for any authentication attempt to verify the identity of the person asking for the IMD access. This will be the first factor to enable the success of the authentication, the fingerprint of the requester must match the stored one. When the medical team arrives at the emergency location, it would know how to operate. A standardization of the scheme will be present. Identifying that the patient is equipped with an IMD, they will scan his/her finger to activate the authentication scheme. This will whether deactivate the IMD or give an authentication key for the medical team to operate the IMD. For each IMD, a specific case of study will be achieved to decide.

The second factor of this scheme is the instantaneous ECG signal, as shown in Section 2. The user will start by recording the ECG signal information to generate the first needed sequence. This sequence is established as explained in Section 2.4. Once it is computed, it will be encoded according to a Hadamard encoder [33]. The use of this encoder is for the purpose of extending the size of the previous input to match relatively the data format of the fingerprint reading. For the fingerprint reading, the minutiae characteristics will undergo a second encoding scheme to form a binary matrix detailing the features of the scanned fingerprint. Fig. 6 represents the transformation process that a fingerprint scan undergoes through our protocol. Once achieved, the scheme will possess two sequences generated from the two different biometric readings, as shown in Fig. 7. Both outputs will contain the singularities of each biometric. They join afterwards in a summation function (XOR function as an example to lower the complexity) to form the authentication key. The use of this simple function is to guarantee the non-waste of the hardware resources of the IMD. More sophisticated IMDs can rely on two-way deterministic functions. This key is to be sent to the IMD to request access. A public share of this key is permitted as it is considered as a token of the medical team. Replay attacks are prevented using this procedure. As it will be proven in Section 5, ECG readings are equivalent to a random process. Hence, the fingerprint cannot be identified nor the key cannot be replayed in a future time. The ECG reading result would expire by the next attempt.

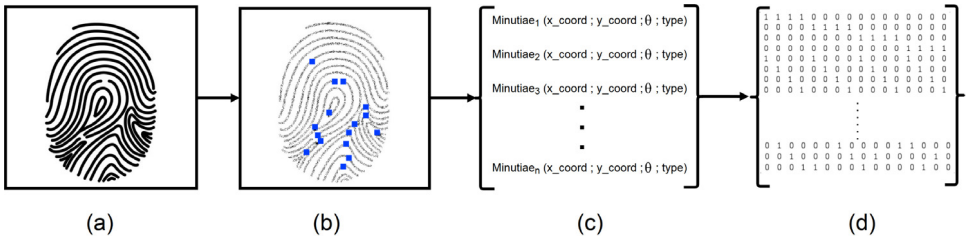

Fig. 6. Fingerprint scan transformation process. (a) Scan acquisition. (b) Minutiae identification. (c) Minutiae characteristics matrix. (d) Binary form of the minutiae characteristics matrix encoded with Hadamard.

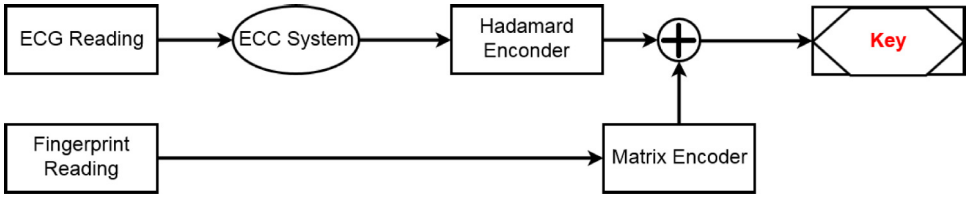

Fig. 7. Sender's key generation scheme using ECG and fingerprint readings.

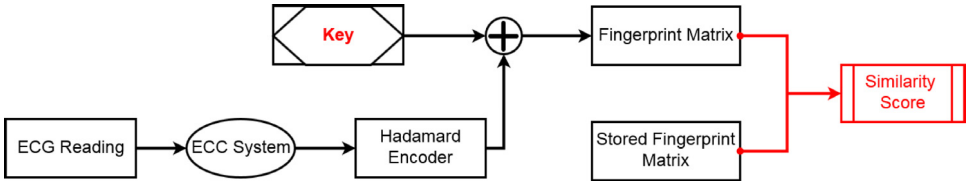

Fig. 8. Receiver's key decoding scheme using ECG and fingerprint readings.

The IMD will receive a request to operate the emergency authentication scheme. It will be informed that the patient is in a critical situation and will accept to process the authentication request. In case of any malicious manipulation of this backdoor, it can alert the user to verify his surroundings. After processing the key, as explained in Fig. 8, the fingerprint matrix can be extracted. The result will be in a form of a binary matrix containing the minutiae features of the scanned fingerprint. This matrix will be compared to the one stored within the IMD to verify if the sender is an authorized user that has just scanned the patient's finger. If the matching score is higher than a given threshold, the sender is granted the IMD access.

3.6. Similarity score computation

The similarity score of the fingerprints is based on the ratio of the matching minutiae between both fingerprints and the total number of identified minutiae. After the alignment of the fingerprint, two minutiae from the same type are considered similar if they have the same spatial coordinates and the same orientation. If we consider that a given minutiae is represented by (x, y) spatial coordinates and an angle θ, two minutiae are similar if:

- They both belong to the same type of minutiae τ.
- $$\begin{cases} \sqrt{\Delta x^2 + \Delta y^2} \leq D_{th} \\ \min(|\Delta\theta|, 2\pi - |\Delta\theta|) \leq \theta_{th} \end{cases} \quad (5)$$

with Δx, Δy and $\Delta\theta$ being the difference between the x-coordinate, y-coordinate and the orientation of the minutiae, respectively.

In order to compare two fingerprint scans F_α and F_β, the scan will be locally aligned. We define a minutiae point i by the vector

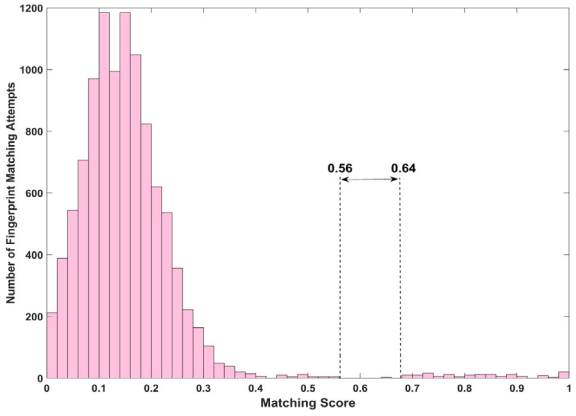

Fig. 9. Histogram of the matching scores of different fingerprint matching attempts.

$M_i = (x_i, y_i, \theta_i, \tau_i)^T$. A fingerprint scan contains N minutiae points. A set of random $\Upsilon = \{i \,/\, i \in$ Minutiae points set$\}$ is defined with cardinality $0.25 \times N$. The factor $N_f = 0.25$ was chosen after statistical test for giving the best score close to the score of the fingerprint matching if all minutiae points were considered. Fig. 10 shows the average effect of N_f variation on the accuracy of the matching score of fingerprints belonging to the same person. We define $Ng(i)$ the minutiae points in the same spatial circle of radius r and center (x_i, y_i). Now for each $(i, j) \in \{\Upsilon_\alpha \times \Upsilon_\beta \,/\, i \in Ng(j)$ and M_i similar to $M_j\}$:

$$\begin{cases} dx = x_j - x_i \\ dy = y_j - y_i \\ d\theta = min(|\theta_j - \theta_i|, 360 - |\theta_j - \theta_i|) \end{cases} \quad (6)$$

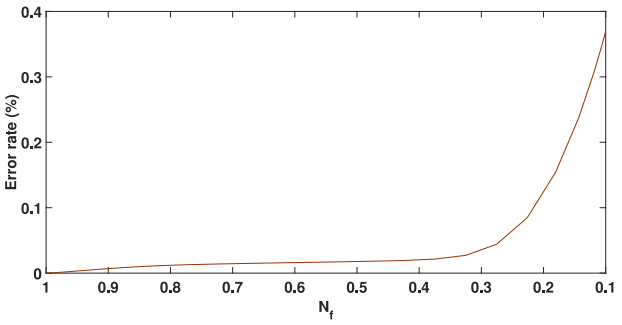

Fig. 10. N_f Factor average effect on the accuracy of the matching algorithm on the same person's fingerprints.

Then according to (dx, dy), F_β will translated so that $(dx, dy) = (0, 0)$; and according to $d\theta$, F_β will rotated so that $d\theta = 0$. We call the result of the latter F'_β.

The algorithm will compute the number η_i of similar minutiae between F_α and F'_β according to the thresholds $(\Delta x, \Delta y, \Delta\theta)$. The final local score is:

$$S = \frac{\eta_i^2}{|\Upsilon_\alpha| \times |\Upsilon_\beta|} \tag{7}$$

The final score will be the highest S.

Fig. 9 shows the resulting score of matching different fingerprints. These fingerprints were collected through different databases [34] that offer fingerprint scans for different individuals and different scans for the same individual, to allow a better analysis of the fingerprint algorithms. To enhance the data, the scans originating from the same individual were multiplied by inducing several modification to the original sample, e.g., cropping, rotation, blurring. This histogram shows clearly a gap between the scores resulted from comparing different individuals' fingerprints and from comparing different scans of the same individual's fingerprint. This can easily clear the choice of the threshold to be defined for the protocol to conclude from the computed score if the fingerprints belong to the same person or not.

4. Security analysis

The IMD is threatened from two different types of attackers: passive and active. Emergency situations represent an advantage for attackers to launch their attacks. Most of IMDs, with their simple resources, will simply stop working or open its access to the environment under such circumstances. This is due to the fact that an abnormality in the user's health had happened and the IMD may behave as an obstacle for urgent interventions. This can easily be the opportunity for attackers to hijack the disregarded IMD. Our scheme focuses well on this scenario and offers access to any foreign medical team to control the IMD while the user is unconscious. At the same time, this same scheme can be used in general situations for authentication needs to avoid any waste of resources. The wireless exchange of the generated key prevents any kind of Man-In-The-Middle attacks. The ECG reading plays the role of an expirable token that makes the key expirable for Replay attacks. The combination of both biometric prevents any spoofing, phishing and jamming attacks. Packet sniffing is shown through the results presented in the following section to be uninformative to eavesdroppers. This was mainly enhanced by introducing the properties of ECC systems. This scheme helps any new medical staff to access the IMD to take the needed actions while ensuring that no other malicious party can take place in the communication. If the emergency access was triggered under a regular scenario, the IMD can inform the user and he/she will take the necessary precautions.

Table 2
Results of randomness tests applied on multiple sequence generations.

Randomness test	Success rate
Monobit test	89%
Frequency test	100%
Runs test	96%
DFT	100%

Also, an abnormality detection scheme [35] can be used to detect emergency situations and when the authentication can take place. In a more general context, the user can trigger this mechanism to authenticate a new doctor too.

Among the problems an IMD can face, are the regulatory authorities [36], e.g., the US Food and Drug Administration (FDA). Such authorities must ensure the safety and security of medical devices designed for commercial use. For this reason, the FDA has placed the responsibility for the devices security issues with the medical product manufacturer. They published for this matter premarket [37] and postmarket guidelines [38]. These guidelines englobe the management procedure of medical device cybersecurity risks throughout the product life cycle. As the scheme provided through this work has no reason to be constantly updated, regulations should not be a major issue. Basically, FDA has concerns for security patches and update plans for security reason. This work has shown that once it is designed within the IMDs scheme, it is functional against most of the possible malicious attacks. Additionally, the security scheme is shown effective from the design scheme.

5. Results

5.1. One-factor scheme

5.1.1. Randomness tests

To guarantee that the generated binary sequences from the ECG instantaneous readings are truly random, we have used the National Institute of Standards and Technology (NIST) [39] statistical test suite. The results are shown in Table 2.

- *Monobit test*: verifies the randomness of the given sequence by checking if the appearance proportions of 0's and 1's are approximately the same.
- *Frequency Test within a Block*: checks that the proportion of 1's and 0's within an M-bit block is random.
- *Runs test*: verifies if the oscillation between the bits 0 and 1 are at a random pace.
- *Discrete Fourier Transform (Spectral) Test*: checks if there are no periodic features that may contradict the randomness of the bit sequence.

Furthermore, we have analyzed the generated sequences from the ECG readings for patterns consisting of multiple bits. This ensures that eavesdropped sequences are not threatened by statistical attacks. We have tested for every different bit configuration its occurrence probability in the sequence. Fig. 11 shows the average probability of a bit sequence with a given length to appear in a generated bit chain from ECG readings. The figure features also the probability deviation of the most probable sequence and the least probable sequence. We can observe well the deviation is very small. This ensures that there can be no pattern to be detected in any generated sequence to help the attacker to predict any future generated sequence.

5.1.2. FAR-FRR

The False Acceptance Rate (FAR) [40], exhibits the possibility that the security system will mistakenly accept an authentication attempt from an unauthorized user. It is defined as follow:

$$FAR = \frac{Number\ of\ false\ acceptance\ trials}{Total\ number\ of\ authentication\ attempts} \tag{8}$$

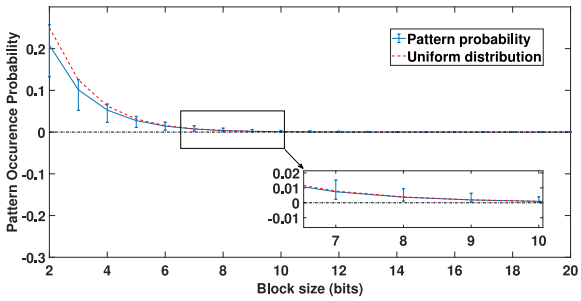

Fig. 11. Occurrence probability of bit sequences with a pre-defined length.

Table 3
FAR & FRR rates.

Metric	Rate
FAR	0.9%
FRR	6.3%

The False Recognition Rate (FRR) [40], displays the possibility that the security system will falsely reject an authentication attempt by an authorized user. It is defined as follow:

$$FRR = \frac{Number\ of\ false\ recognition\ trials}{Total\ number\ of\ authentication\ attempts} \quad (9)$$

The results are shown in Table 3. The analysis have been run through different data segments extracted the ECG recordings offered by PhysioNet [41] database. This database offers several physiologic signals for academic use by the biomedical research community. For ECG signals, they offer python and MatLab libraries to thoroughly investigate the recordings they have. The recording we have investigated are from different subjects. These subjects contain healthy persons along with few of them showing some dysfunctional heart activities. The subjects are from different age intervals too. Each data is linked to its origin through the analysis to keep track of right and false authentications.

5.2. Two-factor scheme

5.2.1. Formal security analysis

To present this protocol in a formal verification, we opted to use the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The AVISPA tool serves to verify the efficiency of a programmed cryptographic protocol [42] using High-Level Protocols Specification Language (HLPSL) [43]. This language assists the role of each participant in the given protocol; while defining all the significant scenarios of these participants in a role architecture. The role system contains a number of sessions, principals and roles. An intruder (I) in HLPSL is modeled according to the Dolev–Yao model [44] where I plays as an authentic role. Using different back-ends to analyze the protocol, the output of this tool generally contains:

- Summary section: It notifies whether the programmed protocol is safe, unsafe or unpredictable.
- Details section: It defines the conditions that have been considered during the analysis.
- Goal section: It designates the considered goals of the test.
- Back-end section: It declares the back-end name that has been used.
- Comments and Statistics section: It describes the trace of any present attack.

For our work, we have implemented three basic roles:

Fig. 12. Result of the AtSe analysis.

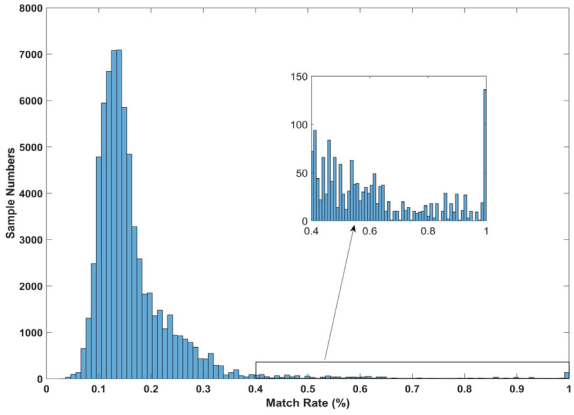

Fig. 13. Histogram of the matching scores.

- Sensor: Defines the communication role of the sensor acquiring the ECG signal.
- Medical Team: Defines the intervening medical system.
- IMD: Defines the IMD from the patient's side.

The implementation covers the phase of sending the ECG signal from the sensor to the medical team and the parameters exchange between the IMD and the medical team to obtain the final secret key. The proposed protocol is simulated under the Constraint-Logic-based Attack Searcher (AtSe) back-end using the AVISPA web tool [42]. This back-end translates the protocol into a set of constraints to pinpoint the possible attacks on protocols [45]. The executability check has been well attained for this protocol. The execution of any protocol sometimes is incomplete. This is mainly due to some modeling errors. This gives erroneous simulation results and might give a false positive on the security of the protocol. That is why most consider the executability test as indispensable in AVISPA. This back-end checks if the legitimate agents in the protocol — which are in our case the medical team, the sensor and the IMD — can execute the specified protocol safely during the existence of an intruder. During this check, the AtSe verifies additionally the possibility of any Man-in-The-Middle attack by an intruder. The test result shown in Fig. 12, which ensures that the proposed protocol can defend replay attack.

5.2.2. Identification rate

The histogram in Fig. 13 shows the matching score resulted by the authentication algorithm presented in this work. Different

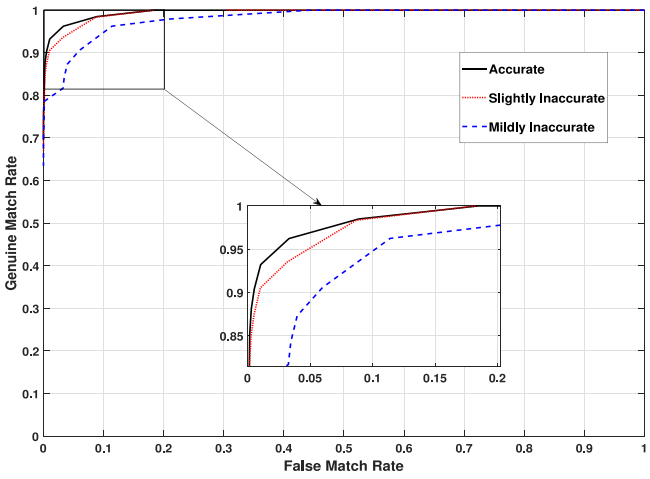

Fig. 14. ROC curves evaluation of the proposed algorithm.

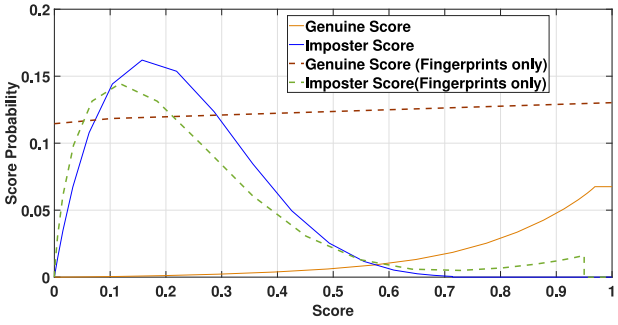

Fig. 15. Distribution of the possible achieved scores by an imposter or a legitimate user authentication.

sample of fingerprints and ECG recording have been used, belonging to the same or different subjects. According to the data, any score higher than the value of 0.57 corresponds to a legitimate authentication request. Any score lower than the value of 0.5 corresponds to an illegitimate authentication request. The interval between these two values is where there is an overlap between legitimate and illegitimate requests. Therefore, the threshold upon which it is decided to grant access to the user will be within this interval. The decision of the exact value can be achieved statically while reviewing the FAR–FRR metrics that correspond to each threshold.

We have analyzed the FAR and the FRR metrics of this work's scheme to identify how reliable it is. Commonly, biometrics are very reliable to identify any identity. However, when using low resources to analyze the data, the accuracy of the identification is not always ensured. Figs. 14 and 15 show the results of our analysis on the database we have collected. The database includes fingerprints and ECG readings of the same and different subjects. The data has been shuffled and processed through our protocol. Then we have compared the results of our algorithm with the actual identification result. We have introduced a sensitivity parameter to this algorithm. The lower this parameter is, the less accurate are the biometric readings. This sensitivity factor reflects the sophistication of the IMD in use. This helped to give more realistic results as inputs to our algorithm. The sensitivity parameter can affect the accuracy of the fingerprint scan or the precision of the ECG signal acquisition. We can see through the figures that the results are acceptable and promising for the success of the authentication request. Fig. 14 shows the Receiver Operating Characteristic (ROC) curves for different sensitivity levels. We can conclude from this how close the curve is to the upper-left corner that our work offers a good trade-off between the sensitivity and the specificity of the authentication algorithm. Fig. 15 demonstrates how statistically efficient can our algorithm be. It represents the statistical probability of the possible score of the authentication attempt of an imposter or a legitimate node. The figure shows two cases: The first one where the ECG corresponding input is discarded (Fingerprints only) and the second one featuring the complete algorithm. This figure shows the important contribution of the ECG corresponding input to the functionality of the algorithm.

6. Conclusion

In this work, we have investigated the security of Implantable Medical Devices (IMDs) from malicious attacks by providing a new backdoor scheme for any medical team to get involved in any emergency scenario. Authentication usually takes place between two previously identified parties. In emergency scenarios, this can be a problem as the IMD will refuse any sudden intervention. We have designed a backdoor to the IMD access while taking into consideration that an attacker may take advantage of the scheme. We introduced first a one-factor authentication scheme. This scheme relies on instantaneous ECG readings to grant access to the new medical team. The ECG readings were enhanced with elliptic curve cryptography to provide more security for the patient. For more sophisticated IMDs, we have designed a two-factor authentication scheme. The latter relies on two different types of biometrics: The first is instantaneous and the second is fixed. We have evaluated the security this scheme can provide the IMD while ensuring it is hardware-friendly towards the limitations of any IMD. We concluded that the proposed system can be used by different kinds of implantable medical devices, and can ensure users' secure wireless communication even in emergency situations.

Acknowledgment

This publication was made possible by NPRP grant #8-408-2-172 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

[1] Z.E. Ankarali, A.F. Demir, M. Qaraqe, Q.H. Abbasi, E. Serpedin, H. Arslan, R.D. Gitlin, Physical layer security for wireless implantable medical devices, in: Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), 2015 IEEE 20th International Workshop on, IEEE, 2015, pp. 144–147.

[2] Y. Kim, W.S. Lee, V. Raghunathan, N.K. Jha, A. Raghunathan, Vibration-based secure side channel for medical devices, in: Proceedings of the 52nd Annual Design Automation Conference, ACM, 2015, p. 32.

[3] W.J. Long, W. Lin, An authentication protocol for wearable medical devices, in: Emerging Technologies for a Smarter World (CEWIT), 2017 13th International Conference and Expo on, IEEE, 2017, pp. 1–5.

[4] H. Chi, L. Wu, X. Du, Q. Zeng, P. Ratazzi, e-SAFE: Secure, Efficient and Forensics-Enabled Access to Implantable Medical Devices. arXiv preprint arXiv:1804.02447, 2018 Apr 6.

[5] X. Du, M. Guizani, Y. Xiao, H.H. Chen, A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks, IEEE Trans. Wirel. Commun. 8 (3) (2009) 1223–1229.

[6] T. Belkhouja, X. Du, A. Mohamed, A.K. Al-Ali, M. Guizani, Symmetric encryption relying on chaotic henon system for secure hardware-friendly wireless communication of implantable medical systems, J. Sensor Actuator Netw. 7 (2) (2018) 21.

[7] S.C. Nelson, J.D. Rose, Location and energy based hierarchical dynamic key management protocol for wireless sensor networks, in: International Conference on Next Generation Computing Technologies, Springer Singapore, 2017, pp. 198–211.

[8] F. Zhan, N. Yao, Z. Gao, G. Tan, A novel key generation method for wireless sensor networks based on system of equations, J. Netw. Comput. Appl. 82 (2017) 114–127.

[9] Y. Cheng, X. Fu, X. Du, B. Luo, M. Guizani, A Lightweight Live Memory Forensic Approach Based on Hardware Virtualization, Vol. 379, Elsevier Information Sciences, 2017, pp. 23–41.
[10] X. Hei, et al., PIPAC: Patient infusion pattern based access control scheme for wireless insulin pump system, in: Proc. of IEEE INFOCOM 2013, Turin, Italy, 2013.
[11] T. Belkhouja, X. Du, A. Mohamed, A.K. Al-Ali, M. Guizani, New plain-text authentication secure scheme for implantable medical devices with remote control, in: GLOBECOM 2017 2017 IEEE Global Communications Conference, 2017, 1–5.
[12] G.Z. Yang, Implantable Sensors and Systems: From Theory to Practice, Springer, 2018.
[13] L. Pycroft, T.Z. Aziz, Security of Implantable Medical Devices with Wireless Connections: The Dangers of Cyber-Attacks, 2018.
[14] K. Katzis, R.W. Jones, G. Despotou, The challenges of balancing safety and security in implantable medical devices, in: ICIMTH, 2016, pp. 25–28.
[15] T. Belkhouja, X. Du, A. Mohamed, A.K. Al-Ali, M. Guizani, Salt generation for hashing schemes based on ECG readings for emergency access to implantable medical devices, in: 2018 International Symposium on Networks, Computers and Communications (ISNCC), IEEE, 2018, pp. 1–6.
[16] B. Tams, P. Mihilescu, A. Munk, Security considerations in minutiae-based fuzzy vaults, IEEE Trans. Inf. Forensics Secur. 10 (5) (2015) 985–998.
[17] C. Li, J. Hu, A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures, IEEE Trans. Inf. Forensics Secur. 11 (3) (2016) 543–555.
[18] S. Chavan, P. Mundada, D. Pal, Fingerprint authentication using Gabor filter based matching algorithm, in: Technologies for Sustainable Development (ICTSD), 2015 International Conference on, IEEE, 2015, pp. 1–6.
[19] C. Yuan, X. Sun, R. Lv, Fingerprint liveness detection based on multi-scale LPQ and PCA, China Commun. 13 (7) (2016) 60–65.
[20] Z. Jin, M.H. Lim, A.B. Teoh, B.M. Goi, Y.H. Tay, Generating fixed-length representation from minutiae using kernel methods for fingerprint authentication, IEEE Trans. Syst. Man Cybern.: Syst. 46 (10) (2016) 1415–1428.
[21] R. Gupta, M. Mitra, J. Bera, ECG Acquisition and Automated Remote Processing, Springer India, 2014.
[22] V. Miller, Uses of elliptic curves in cryptography, in: Advances in Cryptology, Crypto 85, in: LNCS, vol. 218, Springer Verlag, 1986, pp. 417–426.
[23] N. Koblitz, Elliptic curve cryptosystems, Math. Comp. 48 (1987) 203–209.
[24] K. Lauter, The advantages of elliptic curve cryptography for wireless security, IEEE Wirel. Commun. 11 (1) (2004).
[25] V. Kapoor, V.S. Abraham, R. Singh, Elliptic curve cryptography, Ubiquity 2008 (May) (2008) 7.
[26] D.B. Smith, D. Miniutti, T.A. Lamahewa, L.W. Hanlen, Propagation models for body-area networks: A survey and new outlook, IEEE Antennas Propag. Mag. 55 (5) (2013).
[27] M. Martin, K. Štefan, F. L'ubor, Biometrics authentication of fingerprint with using fingerprint reader and microcontroller arduino, TELKOMNIKA 16 (2) (2018) 755–765.
[28] D. Chek Ling Ngo, A. Beng Jin Teoh, J. Hu, Biometric Security, Cambridge Scholars Publishing, 2015, ISBN (10):1-4438-7183-4.
[29] T.M. Khan, D.G. Bailey, M.A.U. Khan, Y. Kong, Efficient hardware implementation strategy for local normalization of fingerprint images, J. Real-Time Image Process. 1 (2016) 1–13.
[30] W. Lee, S. Cho, H. Choi, J. Kim, Partial fingerprint matching using minutiae and ridge shape features for small fingerprint scanners, Expert Syst. Appl. 87 (2017) 183–198.
[31] M.H. Tran, T.N. Duong, D.M. Nguyen, Q.H. Dang, A local feature vector for an adaptive hybrid fingerprint matcher, in: Information and Communications (ICIC), 2017 International Conference on, IEEE, 2017, pp. 249–253.
[32] M.M. Ali, V.H. Mahale, P. Yannawar, A.T. Gaikwad, Fingerprint recognition for person identification and verification based on minutiae matching, in: Advanced Computing (IACC), 2016 IEEE 6th International Conference on, IEEE, 2016, pp. 332–339.
[33] A. Hadi, E. Alsusa, On the application of the fast hadamard transform in polar codes, in: Signal Processing Advances in Wireless Communications (SPAWC), 2016 IEEE 17th International Workshop on, IEEE, 2016, pp. 1–5.
[34] J. Fierrez, J. Ortega-Garcia, D. Torre-Toledano, J. Gonzalez-Rodriguez, Biosec baseline corpus: A multimodal biometric database, Pattern Recognit. 40 (4) (2007) 1389–1392.
[35] H. Rathore, A. Al-Ali, A. Mohamed, X. Du, M. Guizani, DLRT: Deep learning approach for reliable diabetic treatment, in: InGLOBECOM 2017-2017 IEEE Global Communications Conference, IEEE, 2017, pp. 1–6.
[36] P.A. Williams, A.J. Woodward, Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem, Medical Devices (Auckland, NZ). 8 (2015) 305.
[37] US Food and Drug Administration, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff. 2014.
[38] US Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff Additional Copies. 2016.
[39] National Institute of Standards and Technology, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April, 2010.
[40] M.E. Schuckers, Computational Methods in Biometric Authentication, Information Science and Statistics, Springer-Verlag London Limited, 2010.
[41] PhysioBank Databse, https://physionet.org/physiobank/, 2016.
[42] L. Vigano, Automated security protocol analysis with the AVISPA tool, Electron. Notes Theor. Comput. Sci. 155 (2006) 61–86.
[43] D. von Oheimb, The high-level protocol specification language HLPSL developed in the EU project AVISPA, in: Proceedings of APPSEM 2005 workshop, 2005, pp. 1–17.
[44] M. Backes, B. Pfitzmann, Symmetric encryption in a simulatable Dolev-Yao style cryptographic library, in: Null 2004, IEEE, 2004, p. 204.
[45] AVISPA Team. AVISPA v1. 1 user manual: http://avispa-project.org/package/usermanual.pdf 2006 Jun..

Taha Belkhouja received his Engineering Degree in Telecommunications from the Higher School of Communication (Sup'Com) Tunisia, in 2016. He enrolled during his last year of engineering studies in a Master Exchange Program with the University of Padova, Italy. He is currently pursuing a Ph.D. program in Electrical Engineering at the University of Idaho, USA. His research interests focus on the security of wireless communications in medical devices.

Xiaojiang Du is a professor in the Department of Computer and Information Sciences at Temple University, USA. Dr. Du received his B.S. Tsinghua University, Beijing, China in 1996, and his Ph.D. degree from the University of Maryland College Park in 2003. His research interests are wireless networks, security, and systems. He has authored over 230 journal and conference papers in these areas. Dr. Du has been awarded more than $5 million US dollars research grants.

Amr Mohamed (S'00, M'06) received his M.S. and Ph.D. in electrical and computer engineering from the University of British Columbia, Vancouver, Canada, in 2001, and 2006 respectively. He has worked as an advisory IT specialist in IBM Innova- tion Center in Vancouver from 1998 to 2007, taking a leadership role in systems development for vertical industries. He is currently an associate professor in the college of engineering at Qatar University and the director of the Cisco Regional Academy. He has over 23 years of experience in wireless networking research and industrial systems development. He holds three awards from IBM Canada for his achievements and leadership, and three best paper awards. His research interests include networking and MAC layer techniques mainly in wireless networks. Dr. Mohamed has authored or co-authored over 50 refereed journal and conference papers and one textbook.

Abdulla Khalid Al-Ali, Ph.D. obtained his Master degree in Software Design Engineering and PhD degree in Computer Engineering from Northeastern University in Boston, MA, USA in 2008 and 2014, respectively. He is an active researcher in Cognitive Radios for smart cities and vehicular ad-hoc net- works (VANETs). He has published a number of peer-reviewed papers in journals and conferences. Dr. Abdulla is currently head of the Technology Innovation and Engineering Education (TIEE) at the College of Engineering in Qatar University.

Mohsen Guizani (S'85-M'89-SM'99-F'09) re- ceived the B.S. (with distinction) and M.S. degrees in electrical engineering, the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor and the ECE Department Chair at the University of Idaho, USA. Previously, he served as the Associate Vice President of Graduate Studies, Qatar University, Chair of the Computer Science Department, Western Michigan University, and Chair of the Computer Science Department, University of West Florida. He also served in

academic positions at the University of Missouri-Kansas City, University of Colorado-Boulder, Syracuse University, and Kuwait University. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He currently serves on the editorial boards of several international technical journals and the Founder and the Editor-in-Chief of Wireless Communications and Mobile Computing journal (Wiley). He is the author of nine books and more than 500 publications in refereed journals and conferences. He guest edited a number of special issues in IEEE journals and magazines. He also served as a member, Chair, and General Chair of a number of international conferences. He received the teaching award multiple times from different institutions as well as the best Research Award from three institutions. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He served as the IEEE Computer Society Distinguished Speaker from 2003 to 2005. He is a Fellow of IEEE and a Senior Member of ACM.