Fusion of Electrocardiogram and Arterial Blood Pressure Signals for Authentication in Wearable Medical Systems

Hang Cai, Krishna K. Venkatasubramanian
Department of Computer Science
Worcester Polytechnic Institute
Worcester, MA 01609
Email: {hcai, kven}@wpi.edu

***Abstract*—Wearable medical systems allow their users to be monitored continuously without being tethered. They are very useful for tracking patient health deterioration in hospital ER and in patient general wards. It is therefore essential to identify who the data is being collected from. In this paper we present an authentication approach that fuses characteristics of electrocardiogram (ECG) with arterial blood pressure (ABP) to authenticate users. The idea behind the use of multiple physiological signals is that it allows us to ensure that the authentication approach works effectively irrespective of the current state of the user's health. This is an important requirement given that wearable medical systems might be worn by user who have ailments that causes their physiological signals used in authentication to be "non-standard". An evaluation of our approach showed that it was over 97% *accurate* with a false positive rate (e.g., accepting illegitimate users) of 1.2% in identifying the user on whom the system is deployed. Further, it enabled authentication after just 3 seconds of signal measurement.**

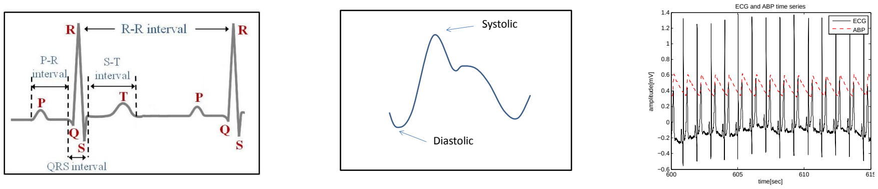
I. Introduction

Recent years have seen a dramatic increase in the number of *wearable medical systems* that move beyond the current paradigm of movement monitoring [1] to medical monitoring and even actuation e.g., [2], [3]. These medical systems allow caregivers to manage the user's health conditions through timely treatment and therapies (though actuation) based on continuous monitoring of the patient's health state.

Wearable medical systems help in monitoring patients in an ambulatory fashion. They can be very helpful in hospital emergency rooms (and even in inpatient general care), where patients can often go hours without being monitored. In such medical scenarios, if the patient's health is deteriorating, it is often not caught in time leading to longer hospital stays and even increased mortality [4]. Wearable medical systems that can monitor vital signs continuously can aid in the ameliorating this process. In fact several such vital signs monitors are available that can measure a variety of signs including electrocardiogram (ECG), continuous blood pressure, heart-rate, body temperature, SPO2 in a non-invasive fashion [5], [4]. Given the cost of these wearable medical systems, the devices are often shared between multiple patients over time. It is therefore crucial that the data from the "wrong" user is not used to determine treatment and therapies for a particular user. *Protecting against these situations requires that we verify the deployment of wearable system on a particular user.* Given the hospital emergency rooms are already very busy, the authentication process cannot be manual.

Physiological signals such as electrocardiogram (ECG) are often used to authenticate users in a wearable context as they are (1) difficult to spoof, (2) use vital signs that are already being continuously collected, and (3) do not require traditional input modalities unlike authentication solutions based behavioral cues (e.g., voice, touch or gestures), input entry (e.g., passwords), or biometrics (e.g., fingerprinting, iris scan). However, traditionally, authentications solutions (physiological signal-based and others) were largely designed for and validated on a generally healthy user population. It is not clear how well these solutions perform when the user population has ailments that cause their physiological signals used in authentication to be "non-standard". However, in a wearable medical system context this assumption of user healthiness may not be always true and we need solutions that work for normal patients and those patients with ailment. This is a non-trivial problem because ailments can drastically affect the temporal and morphological characteristics of physiological signals being used for authentication.

Consequently, in this work, our approach fuses characteristics of two vital signs often measured in tandem, namely electrocardiogram (ECG) and arterial blood pressure (ABP), to authenticate users in a user health-context independent manner. The reason that traditional ECG based authentication solutions does not work well for ailing users is because the solutions depend on the ECG having defined shapes and timing properties. This assumption does not always hold for users ailing with specific health conditions. By considering multiple physiological signals, we aim to capture the nuances of the cardiac process of a user from diverse perspectives despite the non standard nature of one of the signal. Our main idea is to build a machine learning model of the physiological relationship between synchronously measured ECG and ABP from a user and use it as a template. Any time we need to authenticate the fact that the claimed wearer of the wearable system is a particular user, we take a sample of the ECG and ABP from the user and compare its characteristics with that of our model to see if they match. We have evaluated our approach based on a dataset of 36 (healthy and ailing) users from the MIT PhysioBank Fantasia and MGH databases [6] to determine its feasibility. We found our approach to be



(a) P, Q, R, S, T waves in a typical ECG

(b) Systolic Peak & Diastolic Trough in ABP

(c) ECG and ABP superimposed

Fig. 1: ECG and ABP signal and their Relationship

over 97% *accurate* with a false positive rate (e.g., accepting illegitimate users) of 1.2% in identifying the user on whom the system is deployed. Further, it enabled authentication after just 3 seconds of signal measurement. The **contributions** of this work are two-fold: (1) the uses combined ECG and ABP signals for authenticating users of wearable medical systems, (2) the demonstration of the feasibility of the approach in a user health-context independent manner for both healthy and ailing users.

Related Work: Over the past few years several efforts have been directed toward user authentication in wearable contexts using physiological signals such as electrocardiogram (ECG) [7], [8], [9], [10], [11], PPG [12], vocal resonance [13], bioimpedence [14], heart-rate [15], and EEG [16]. Most of these efforts have focused on creating a template for a user based on characteristics points in the signal waveforms followed by statistical or machine learning approaches for authenticating the user. Some work has also been done on using fusion of several physiological signals as a way to authenticate users. These have been done to improve the accuracy of authentication process as [17] where ECG with electroencephalogram (EEG) signals were combined or for improving the ECG based authentication particularly in the presence of artifacts such as movements [18], [19]. None of these solutions have been shown to work for both normal as well as users with ailments affecting the physiological signal being used for authentication. In recent years, there have been some efforts to consider a diversity of user population when using physiological signal authentication [20], [21]. However, these approach produce relatively low accuracy and high false negative rates (i.e., rejects legitimate users).

II. System Model and Problem Statement

System Model: A wearable medical system consists of set of sensor devices (and actuator devices). Sensors monitor the patient's physiological state and send their measured data to a cloud (a sink for data storage and processing), via a base station like a smartphone. The cloud provides an interface for the patient/caregiver to analyze and visualize the data. Caregivers can then determine appropriate treatment for the user and inform the user, who may then use their actuators to enable the specific therapies. Every time a sensor sends its measurement to the cloud, it identifies the user on whom it is deployed.

The *problem* we are addressing in this work is to use the fusion of ECG and ABP signal features for authentication in a user-health context independent manner. In this regard, we like to satisfy two primary **design goals**: (1) it should be *accurate* with low false positive and false negatives, (2) it should be *responsive* and quick to identify the user on whom the system is deployed.

III. Background

In this section, we provide some background information on the principal signals that we consider for this work, i.e., electrocardiogram (ECG), arterial blood pressure (ABP) signals. ECG is the measurement of the electrical representation of the cardiac process of a person. As shown in Figure 1a, and ECG signal is made up of peaks and trough combinations which is made up of five elements named P, Q, R, S and T waves. The P wave is observed during atrial depolarization (which causes the blood to be pushed to the ventricles), the QRS complex is observed during the rapid depolarization of the right and left ventricles (which causes the blood to be pushed out of the ventricles and into the lungs and the rest of the body), and the T wave is the depolarization of the ventricles. The time difference between two R peaks is known as an RR-interval. The RR-interval refers to the beat-to-beat variations in heart rate and is a measure of heart rate. Atrial blood pressure (ABP), on the other hand, is the continuous measurement of blood pressure and can be measured non-invasively [22] much like ECG. As shown in Figure 1b, a typical atrial blood pressure contains the trough which is diastolic blood pressure and the peak which is systolic blood pressure. Diastolic troughs occur near the beginning of the cardiac cycle and systolic peaks occur when the ventricles contract. As ECG and ABP signals are both measures of the cardiac process and both controlled by our autonomic nervous system and they track each other. For example, an R peak in the ECG signal will typically be followed by a systolic peak in the ABP signal as both represent the compression of the ventricles that results in the blood being circulated through the entire body via the Aorta (see Figure 1). Similarly, the pathologies in the cardiac process that results in abnormal ECG waveform is also reflected in the ABP signal [23].

IV. Approach

In this section, we introduce our combined Electrocardiogram (ECG) and arterial blood pressure (ABP) based authentication approach. The approach leverages the fact that the inter-relationship between the synchronously measured ECG and ABP signals from different users has different characteristics. Fig 2 shows our system setup. It works in two stages: enrollment stage and authentication stage. In the *enrollment stage*, we collect ECG and ABP data from a user we are trying to authenticate, extract specific features from it and build a user-specific model. This model forms a "template" that describes the user's unique physiological behavior. During the *authentication stage*, we collect a short snippets of current ECG and ABP signals from a unknown user who is trying to authenticate themselves, extract the same features from the snippets and feed them to the user-specific model, which then labels this new features as belonging to the user or not (see Figure 2). We describe the two steps in details below.

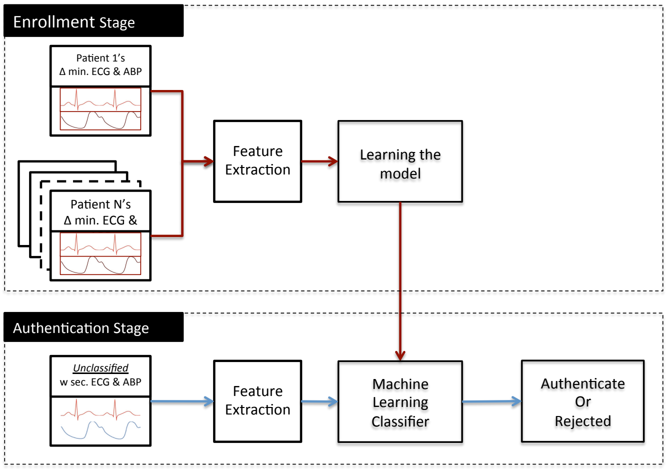


Fig. 2: The ECG and ABP based Authentication Approach

A. Enrollment Stage

The goal of enrollment phase is to build a model for a particular user that captures the characteristics of the ECG and ABP signals measured from them in tandem. We use a supervised-learning-based approach to construct (train) the user-specific model. We use a *extremely randomized trees* [24] as the machine learning classifier in our model. Extremely randomized trees is an ensemble classifier method that extends conventional decision trees by introducing randomness during the construction process [24].

The feature vectors we used during our enrollment stage were 11-dimensional values extracted from Δ time-units of synchronously measured ECG and ABP signals. Before the feature extraction step, we preprocess both ECG and ABP signals by applying a 3rd order Butterworth bandpass filter with a cutoff frequency at 1-50 Hz thus eliminating the low- (baseline wandering) and high- (muscle contractions) interferences. We then segment both signals into several w-sized windows (where $w < \Delta$) such that at least one RR-interval are presented within our moving window. Our extremely randomized trees-based training required as input two classes of feature vectors referred to as positive and negative class points. Each w window therefore generates a positive or negative class feature point for the model. The positive class points capture the situations where the ECG and ABP measurements originate from the user whose model is being trained, while the negative class points capture the situations where the ECG and ABP measurements originate from other users.

For each w-sized window of ECG and ABP segments we extracted the following 11 features. (1) The ratio between average RR-intervals and SS-intervals;.(2) The difference between average RR-intervals and SS-intervals. (3) The difference between the standard deviation of RR-intervals and SS-intervals. (4) The ratio between average R peak amplitude and Systolic peak amplitude. (5) The ratio between average R peak amplitude and Diastolic peak amplitude; (6) Average *Pulse Transmit Time (PTT)*. We define PTT as the distance between R peak and the systolic peak that follows it. (7) Standard deviation of PTT. (8) Root Mean Square (RMS) of PTT. (9) Average backward PTT. We define *backward PTT* as the distance between R peak and the systolic peak occurs ahead of that R peak. (10) Standard deviation of backward PTT. (11) RMS of backward PTT.

B. Authentication Stage

In the ***authentication stage***, the trained user-specific model will decide whether to authenticate a user or not based on newly received snippet of the ECG and ABP measurements. In this regard, we collect w time-unit of newly measured ECG and ABP signals from the user, and then extract the 11-dimensional feature from it. Then we feed this feature point into the user-specific model. The model will then output a positive or negative label for this feature point. If the feature point is labeled as positive, then the user is considered as a legitimate user and will be authenticated.

V. Parameter Selection

In this section, we illustrate how we select the two most important parameters of our authentication system: (1) Δ, the amount of the data needed to train the model (i.e., *training time*), and (2) w, the amount of data needed to be able to make an authentication decision. We begin with an introduction of the dataset we used, followed by performance metrics used to choose the two parameters. Finally, we discuss the parameter selection process itself.

Dataset: In this work, we collected data belonging to 36 subjects (i.e., users) from the MIT PhysioBank Fantasia and MGH/MF databases [6]. We chose these particular subjects from these databases because the availability of both ECG and ABP signals for them. Furthermore, the Fantasia database is made up of healthy subjects, while the MGH/MF database mainly contains data from subjects with specific cardiac conditions (such as sinus tachycardia, atrial fibrillation and etc.). Table I shows the statistics on the patient population we used to train and test our ECG plus ABP authentication system. We categorized the patients in the dataset into two types based on their ECG signals: (1) *Normal subject type*, which only includes subjects who did not suffer from any ailments and had a normal sinus rhythm ECG; (2) *Ailing subject type*, which only includes subjects who are suffering from the cardiac diseases. For each of the 36 subjects we had on average about 40 minutes of usable ECG and ABP data for our experiments.

TABLE I: Subject Data Summary

Type	**Total #**	**Male**	**Female**	**Avg. Age (years)**	**Std. Age (years)**
Normal	12	5	7	46.5	24.4
Ailing	24	8	6	64.4	18.7

Metrics: In this work, we have formulated the problem of authentication as an instance of a binary classification task. To evaluate the classification performance, the performance metrics are based on the notion of the false positive rate (FPR), false negative rate (FNR), true positive rate (TPR) and true negative rate (TNR). In our case, *true positive rate* (*true negative rate*) refers to the fraction of the cases in which a legitimate (illegitimate) user is correctly accepted (rejected), respectively. Similarly, *false positive rate* (*false negative rate*) refers to the fraction of the cases in which an illegitimate (legitimate) user is incorrectly accepted (rejected) as a legitimate (illegitimate) user. Furthermore, we also calculate the *equal error rate* (EER) to evaluate the performance of the classification by varying a discrimination threshold. EER is the rate at which both FPR and FNR are equal.

Selecting Δ and w: To select w, we tried several window sizes w for a fixed Δ of 10 minutes and evaluated our authentication approach (i.e., cross-validated the machine learning model). Figure 3 shows the average accuracy rate, FPR, FNR and EER for different window size w. We can see that the average accuracy rates of the user-specific models for 4 different window size w are all considerably high. In terms of the EER, we can see that 3 seconds window size outperforms the other cases with the lowest average EER at 3.00%. We therefore chose window size $w = 3$ seconds, as it provided us with the best performance and responsiveness for our authentication system. Once the value of w was set to 3 seconds, we tried several Δ sizes and evaluated our authentication approach. Figure 4 shows the average accuracy rate, FPR, FNR and EER for different values of Δ. Similarly, we can see that the accuracy rate for 4 different training time Δ are all considerably high with only a small deviation. Further, the more data we have the better models we were able to create overall. Therefore, we set $\Delta = 20$ minutes as the training time for our model. Even though our training time is quite large, it needs to be noted that it is a one-time cost. The fact that we have a window size of just 3 seconds means that once the authentication system is deployed, we can quickly authenticate users. Further, if time is of essence, we can reduce the size of Δ without losing much in accuracy (up to a point). Reducing the overall training time to a much smaller value is an important future work for us.

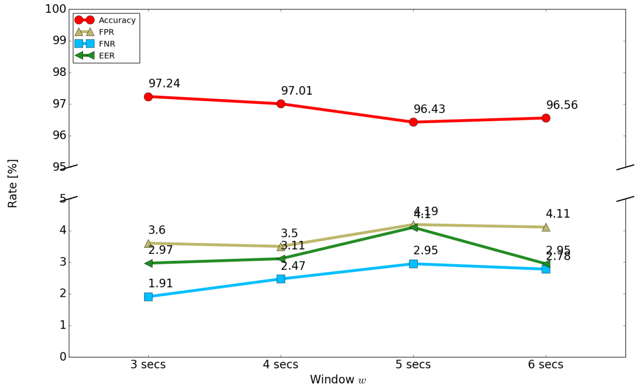


Fig. 3: Average Accuracy Rate, FPR, FNR and EER for Different w

VI. Security Analysis

In previous section, we selected the parameter for the authentication system and build the user-specific model at the enrollment phase. In this section, we address the viability of our authentication system with respect to two cases: (1) accepting a legitimate user, and (2) rejecting an illegitimate user. Before we delve into the details, we introduce two key notations used in this section. We define T_{learn} as a time interval for which we collected ECG and ABP data from a user to build their user-specific models. The duration of T_{learn} is same as the training time Δ, i.e., 20 minutes. T_{curr} is the current time interval when we are testing our authentication model. *It is to be noted, that the signals in the T_{curr} time-interval are new and have never been seen by the patient specific-model in enrollment phase.*

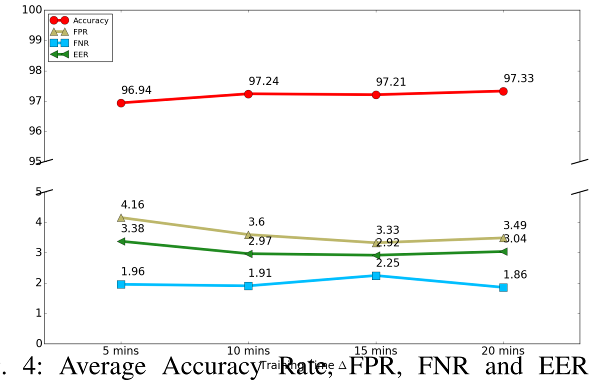


Fig. 4: Average Accuracy Rate, FPR, FNR and EER for Different Δ

We first tested our authentication model to see if it can correctly authenticate a legitimate user after his user-specific model is trained. For each trained model, we have exactly one legitimate user. Therefore, we divided his $T_{curr} = 15$ minutes of synchronously measured ECG and ABP signals into 300, 3-second intervals (windows), each of which produced an 11-dimensional feature point. These 300 feature points were then input into the user-specific model, which then labeled them as positive or negative. Ideally, we should get all positive labels for the points and authenticate them all, as they are all from the legitimate user.

Then, we tested our authentication model to see if it can correctly reject the illegitimate user who tries to access into the system. Therefore, for each trained model, we obtained $T_{curr} = 15$ minutes of synchronously measured ECG and ABP signals from every other user in our dataset. The two resulting signal time series were then divided into 300×35 (since for each user-specific model, we have 35 illegitimate users), 3-second intervals (windows), each of which produced an 11-dimensional feature point. These 10500 feature points were then input into the user-specific model, which then labeled as positive or negative. Ideally, we should get all negative labels for the points and reject them all, as they are all from illegitimate users.

Overall with a Δ set to 20 minutes and w of 3 seconds, our approach produced an accuracy of 97.43%, with an EER of 2.39%, with FPR of 1.2% and FNR of 3.94%. The Table II shows how our approach fares in comparison to other approaches that utilize ECG signals from healthy and ailing patients for authentication. It can be seen that overall we perform much better in terms of accuracy and false positives. Our authentication speed, once the model is deployed, is fastest (only 3 seconds). However, we pay the penalty in terms

TABLE II: Performance Comparison

Approach	Accuracy	False Positives	Enrollment Time	Authentication Time
Singh et. al [21]	82%	7%	1/2 record	1/2 record
Arteaga-Falconi et al. [20]	84.93%	1.29%	30 seconds	4 seconds
Our approach	97.43%	1.2%	20 minutes	3 seconds

of enrollment time, which plan to improve in the future.

So far, the authentication decision of our model is based on a single feature point (one-time authentication). As the physiological sensors like ECG and ABP sensors are monitoring the user continuously, our system has the instinct to be expanded to the continuous authentication system. The decision of our continuous authentication system is based on the number of w-sized windows n (each produces one feature point) and majority voting, i.e., if the majority labeled feature points are positive in n windows, then the user will be authenticated, otherwise the user will be rejected. Fig 5 shows the average FPR and FNR for the above two cases using different numbers of windows. The baseline is one window (i.e., one-time authentication), others are continuous authentication with different numbers of windows. We can see that comparing to the one time authentication, continuous authentication has the lower FPR and FNR.

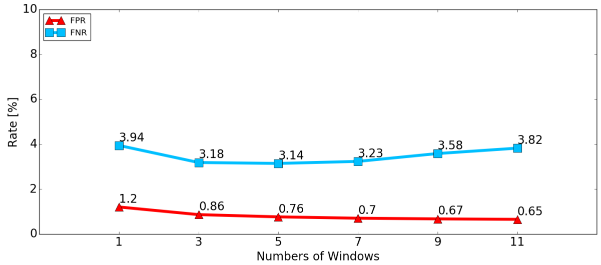


Fig. 5: Average FP and FN for Security Analysis using Different Numbers of Windows

VII. Conclusions

In this paper we presented an approach that combined electrocardiogram (ECG) with arterial blood pressure (ABP), to authenticate users. The use of multiple physiological signals allowed us to ensure that the authentication approach works effectively irrespective of the current state of the user's health. Our approach showed that it was over 97% *accurate* in identifying the user on whom the system is deployed with just 3 seconds of signal measurement. In the future we plan to work on several issues to improve this work. (1) we plan to reduce the amount of time it takes to train the model which is considerable, (2) we plan to evaluate our approach using data collected from actual ECG and ABP sensors, which might be considerably noisier that the data in our dataset, and (3) we plan to expand our data source to include a larger and even more diverse user population to provide extensive validation of the idea in this work.

References

[1] "fitbit," http://www.fitbit.com.

[2] *CardioMEMS*, http://www.sjm.com/cardiomems.

[3] "Pancreum: The Wearable Artificial Pancreas Company," http://pancreum.com/.

[4] "Sotera," http://www.soterawireless.com/.

[5] "Qardio," https://www.getqardio.com/.

[6] A. L. Goldberger, L. A. N. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C.-K. Peng, and H. E. Stanley, "Physiobank, physiotoolkit, and physionet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. e215–e220, 2000.

[7] 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.

[8] H. P. Da Silva, A. Fred, A. Lourenço, and A. K. Jain, "Finger ecg signal for user authentication: Usability and performance," in *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*. IEEE, 2013, pp. 1–8.

[9] M. Guennoun, N. Abbad, J. Talom, S. M. M. Rahman, and K. El-Khatib, "Continuous authentication by electrocardiogram data," in *Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto international conference*. IEEE, 2009, pp. 40–42.

[10] S. J. Kang, S. Y. Lee, H. I. Cho, and H. Park, "Ecg authentication system design based on signal analysis in mobile and wearable devices," *IEEE Signal Processing Letters*, vol. 23, no. 6, pp. 805–808, 2016.

[11] A. Page, A. Kulkarni, and T. Mohsenin, "Utilizing deep neural nets for an embedded ecg-based biometric authentication system," in *Biomedical Circuits and Systems Conference (BioCAS), 2015 IEEE*. IEEE, 2015, pp. 1–4.

[12] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," *Trans. Info. Tech. Biomed.*, vol. 14, no. 1, pp. 60–68, Jan. 2010.

[13] C. Cornelius, Z. Marois, J. Sorber, R. Peterson, S. Mare, and D. Kotz, "Vocal resonance as a passive biometric," 2014.

[14] C. Cornelius, R. Peterson, J. Skinner, R. Halter, and D. Kotz, "A wearable system that knows who wears it," in *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*. ACM, 2014, pp. 55–67.

[15] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (h2h): authentication for implanted medical devices," in *Proceedings of the 2013 ACM SIGSAC conference on Computer &#38; communications security*, ser. CCS '13, 2013, pp. 1099–1112.

[16] J. Sohankar, K. Sadeghi, A. Banerjee, and S. K. Gupta, "E-bias: A pervasive eeg-based identification and authentication system," in *Proceedings of the 11th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, ser. Q2SWinet '15, 2015, pp. 165–172.

[17] D. van der Haar, "Canvis: A cardiac and neurological-based verification system that uses wearable sensors," in *Digital Information, Networking, and Wireless Communications (DINWC), 2015 Third International Conference on*. IEEE, 2015, pp. 99–104.

[18] J. C. Sriram, M. Shin, T. Choudhury, and D. Kotz, "Activity-aware ecg-based patient authentication for remote health monitoring," in *Proceedings of the 2009 international conference on Multimodal interfaces*. ACM, 2009, pp. 297–304.

[19] M. Derawi and I. Voitenko, "Fusion of gait and ecg for biometric user authentication," in *Biometrics Special Interest Group (BIOSIG), 2014 International Conference of the*, 2014, pp. 1–4.

[20] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "Ecg authentication for mobile devices," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 3, pp. 591–600, 2016.

[21] Y. N. Singh and S. K. Singh, "Evaluation of electrocardiogram for biometric authentication," *J. of Inf. Sec*, vol. 3, no. 1, pp. 39–48, 2012.

[22] "The clearsight system," http://www.edwards.com/eu/products/mininvasive/pages/clearsightsystem.aspx, accessed: 2016-02-09.

[23] "Abnormal EKGs and Corresponding Arterial Waveforms," http://www.dynapulse.com/educator/WebCurriculum/Chapter\%203/Abnormal\%20EKG\%20and\%20Waveform.htm.

[24] P. Geurts, D. Ernst, and L. Wehenkel, "Extremely randomized trees," *Machine learning*, vol. 63, no. 1, pp. 3–42, 2006.