"I know it's still you": A study of using the PPG sensor to support zero re-authentications

Tanushree Banerjee
tanushree.banerjee@tcs.com
TCS Research
Kolkata, India

Kartik Muralidharan
kartik.m4@tcs.com
TCS Research
Bangalore, India

Dibyanshu Jaiswal
dibyanshu.jaiswal@tcs.com
TCS Research
Kolkata, India

Mithun Basaralu Sheshachala
mithun.bs@tcs.com
TCS Research
Banglore, India

Ramesh Kumar Ramakrishnan
ramesh.kumar@tcs.com
TCS Research
Banglore, India

Arpan Pal
arpan.pal@tcs.com
TCS Research
Kolkata, India

ABSTRACT

The Photoplethysmogram (PPG) sensor is found in most smart wearables and fitness trackers to support the physical wellness monitoring of it's user. The popularity of this sensor has encouraged the exploration of it's use in other domains particularly in the field of banking, education, training, wellness etc. as a form of biometric authentication. These studies are however limited in the evaluation of the sensor in the wild. We created several datasets of continuous in-the-wild PPG across multiple participants and devices and propose the use of different statistical, signal processing and machine learning based techniques to support zero re-authentications using *in-situ* PPG data.

CCS CONCEPTS

• **Human-centered computing** → **Usability testing**; • **Security and privacy** → *Vulnerability management*; • **Computing methodologies** → **Model development and analysis**.

KEYWORDS

Photoplethysmogram signal, wearable sensing, authentication, human-computer interactions

ACM Reference Format:
Tanushree Banerjee, Kartik Muralidharan, Dibyanshu Jaiswal, Mithun Basaralu Sheshachala, Ramesh Kumar Ramakrishnan, and Arpan Pal. 2021. "I know it's still you": A study of using the PPG sensor to support zero re-authentications. In *MobiSys '21: The 19th ACM International Conference on Mobile Systems, Applications, and Services, June 24–July 2, 2021.* ACM, New York, NY, USA, 6 pages.

1 INTRODUCTION

Wearable devices such as smart watches and fitness trackers are packed with a plethora of sensors and are increasingly gaining acceptance in healthcare solutions. More recently, these devices are also being used as a security token to perform payments, such as fitbit pay [4] as well as regarded as a trusted device to perform actions like automatically unlocking your smartphone [3]. While authentication mechanisms are necessary, it is also necessary to constantly validate the wearer within this authenticated session. This step will prevent any potential misuse of these devices **post authentication**.

Consider this possible scenario. *Alice owns a smart wearable device that allows her to make payments at her favourite grocery store with a simple hand wave. The device also seamlessly pairs with her smart phone keeping it unlocked as long as the wearable device is nearby. These features, while convenient, do support a possibility of unauthorized transactions and access of paired devices whenever the wearable is left unattended. To prevent such possibilities she needs to enter a pin to authenticate herself. While the pin makes the wearable slightly more secure, it does require her to constantly enter it for every transaction, perhaps when the device is removed-even for a brief moment, or whenever the authenticated-session, as set by her, times out - making her turn-off this feature altogether!.* So what we need is some form of a continuous and seamless authentication support that reduces the number of re-authentications required (for the genuine user) whilst preventing any fraudulent transactions.

The PPG sensor is found in most wearable devices including fitness trackers. The popularity of this sensor does make the possibility of using PPG information for zero authentication an interesting proposition. Further, amongst the various physiological signals, PPG is considered to have a unique signature for every individual [14, 15] making a stronger case for using it. In this work we therefore explore the use of the wrist worn PPG sensor in *maintaining* an authenticated session on a wearable device. Note we do not intend of using the PPG information to eliminate the need for authentication. Instead we advocate using the sensor to support zero (or minimize) re-authentications in an already authenticated session.

The PPG sensor is however prone to error. It is well known that the signal is greatly affected by motion artifact [7]. Any real-time solution involving this sensor would therefore have to be robust to these nuances in order to reduce false positives in user detection or in detecting certain events like watch removal.

The key contributions of this work are:

MobiSys '21, June 24–July 2, 2021,

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
DOI:10.1145/3469260.3469669

- Progressively conceptualizing multiple approaches in using the PPG sensor to support a zero re-authentication mechanism.
- Evaluation of each approach across multiple devices with a real-time system perspective in 1) how accurately can we differentiate between the user and an adversary and 2) how quickly can we do it.
- Identifying the limitations of the PPG sensor data in an in-situ setting.

2 RELATED WORK

Several publications have documented the vulnerabilities of smart wearable devices on aspects of security and privacy. In 2015, Hewlett-Packard (HP) published a research study highlighting the security issues in popular smart wearable devices [2], a lack of a secured authentication mechanism being a major issue. This concern is mirrored in recent research papers [6, 19].

To address this concern many studies have explored the feasibility of using physiological signals (especially the PPG) as a form biometric authentication for wearable devices. Yadav et al. [15] evaluated one such scheme collecting PPG on the finger across user activities and emotional states achieving an Equal Error Rate (EER) of 0.5-6%. Most of these works use a machine learning based approach extracting fiducial (time-domain, statistical) [13] and non-fiducial (working with the transformation of PPG data) [8, 10] features from the PPG signal. The extracted features are then used in a one-class or binary classifier [16] to test the accuracy. PPG based template matching and usage of thresholds are also often used to give the verdicts on user authenticity [12, 14]. Lee et al [11] reported an accuracy of 93-99% for identification of subjects using an ML technique. Authors in [17] reported a False Acceptance Rate of 4.2% and False Rejection Rate of 3.7% for PPG based biometric authentication. An EER of 9-14.5% was observed in [9] for a continuous PPG based biometric authentication system. Most of these works however attempt to use the PPG information to (1) determine the identity of the person wearing the device, (2) evaluate with a limited dataset of known users (and adversaries), and (3) operate under a controlled lab environment where signals from the same recording session are used for both enrollment and testing. In a real world environment it has been shown that EER values rise quickly (up to 23.2%) when the time interval between the enrollment and testing stages increases [14]. In this work we abstract the identity of the user and instead explore the use of the PPG sensor in maintaining an already authenticated session in an *in-situ* environment.

3 DESCRIPTION OF DATASETS USED

For this work multiple sessions of in-house data was collected following different data collection protocols. A total of six datasets were used to validate our proposed approaches. The data was collected using an Empatica E4 wearable device [1] and a Samsung Gear S3 [5].

3.1 Checking the PPG signal quality: A must

Since PPG signals are negatively impacted by motion artifacts [7] it is important to remove these to minimize any error; Figure 1 and 2 clearly establishes the effect of motion on the PPG signal.

Therefore any data collected needs to first pass through our PPG-quality-checker block. This block essentially performs a frequency domain analysis of the signal focussing on the components corresponding to the heart and breathing features in the frequency spectrum of the PPG signal. The frequency range corresponding to the heart rate is taken from $f = 0.6$ to 2 Hz, and similarly for respiration rate, $f = 0.2$ to 0.6 Hz. Note, in a 'clean' PPG, ideally the dominant frequencies are primarily for frequency components corresponding to the heart rate followed by breathing rate and then noise. In the case of a 'noisy' PPG, the frequency components are spread across the entire spectrum in an uneven manner. Each of the PPG segments (P) are low pass filtered (P_l), following which a threshold is set to check the percentage change in frequency components corresponding to the heart rate and respiration rate of P and P_l respectively. Based on this, segments with motion artifacts are detected and removed.

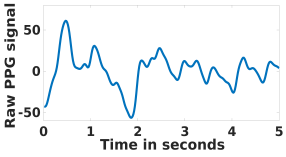

Figure 1: A PPG signal *with motion artifact.*

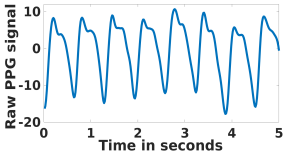

Figure 2: A PPG signal *post motion artifact removal.*

3.2 Dataset A: The need for detecting watch removal

In order to support zero re-authentications using the PPG sensor, some of our approaches (Section 4.2 to 4.4) utilize PPG data from the most recent past as input. Therefore it was important to identify the portions where the wearable was not worn as these cannot be used as input to our system. We initially presumed that the sensor would output incoherent data during this phase as it was no longer in contact with the skin. However, during our data collection we observed that when the wrist wearable device was removed, the PPG sensor continued to provide data albeit with a smaller amplitude (Figure 4). An amplitude based threshold technique to identify these segments where the device was not worn unfortunately did not work as this range varied based on *how* the device was placed post removal. The placement of the device altered the amount of light reflecting off the PPG sensor thereby altering the amplitude range. This made it necessary to come up with a smarter way of detecting the 'remove' and 'worn' events in order to discard this segment of data from our input.

For this exercise we collected data from two subjects (subject 1 provided 5 sessions with E4 device and subject 2 provided 4 sessions with Samsung Gear S3) under different conditions to emulate possible situations of wearable device removed from wrist. These include conditions of varying ambient light (dim, bright), varying

sensor positions (device left open with the sensor facing up, side and downwards).

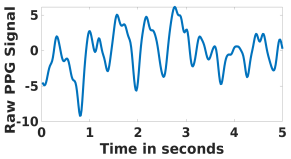

Figure 3: A sample wearable PPG signal when worn on wrist.

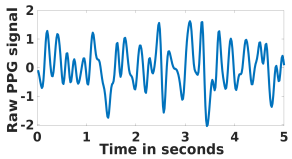

Figure 4: A sample PPG signal when the device is removed from wrist.

A random forest based binary classifier was trained with 38 time domain and statistical features extracted from the PPG data with both device worn (dataset B1 & B2) and removed (as mentioned above) scenarios . The classifier could identify watch removed areas correctly with an average F_{score} of 0.95.

3.3 Other Datasets

- **B1**: For this dataset we emulated the scenario described in Section 3.2 where a user would remove their wrist worn wearable post which it would either be reworn by the same user or an unauthorized person (user 2). A total of 7 sessions were captured from two subjects wearing the Samsung S3 with varying times of device-worn (5min/3min) and device-removed (2min/1min/30s) durations. An example data collection session would involve the user wearing the device for 5 minutes, remove it for 2 minutes, post which another user wears it for 5 minutes and so on. The data collection protocol is captured in Figure 5. Figure 6 shows the plot of the PPG signal collected following this protocol.
- **B2**: It was collected using the same protocol captured in Figure 5. Here the participants wore the Empatica E4 device. 13 sessions of data was collected from 6 subjects.
- **C**: In-situ data was collected from 7 participants wearing the Empatica E4 device. Participants wore the device (without removing) for 7 hours across a typical working day.
- **D**: Two training datasets were created to build a subject specific authentication model. Subject 1 provided 20 hours of continuous PPG data worn over the entirety of a day while subject 2 provided 6.5 hours of continuous PPG data. Both datasets were collected using the E4.
- **E**: In-situ PPG data was collected across 13 participants wearing the E4 through a normal working day. Each participant provided data for a different number of days ranging from 1 to 8 with an average of 3 days of data per subject.

4 PPG: HYPE OR HOPE FOR ZERO RE-AUTHENTICATION?

We investigated 4 different approaches for using the PPG sensor for a zero re-authentication scenario. With each approach we attempt to mitigate some of the constraints we observed when using the PPG in an *in-situ* scenario to maintain an authenticated session. The proposed techniques are implemented using MATLAB 2019a and Python 3.7.5.

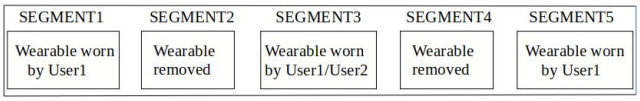

Figure 5: Dataset B1/B2 collection protocol. Three time combinations were used across the 5 segments to collect the data: 5min-*2min*-5min-*2min*-5min OR 3min-*1min*-3min-*1min*-3min OR 3min-*30s*-3-*30s*-3min.

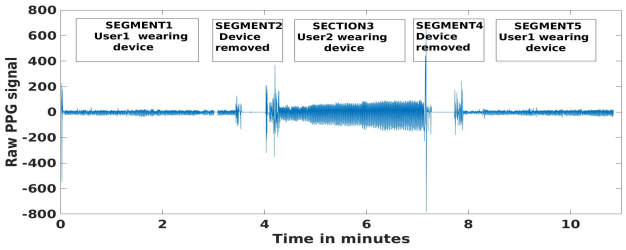

Figure 6: A PPG session collected from Empatica E4 wearable device following the Figure 5 protocol

4.1 Technique 1: Template matching

In our first approach templates of PPG pulses are matched to determine segments that belong to the authenticated user. To identify the templates, we use a simplified procedure compared to the approach found in [14]. Here, in each template, the troughs are first identified. Next, trough-to-trough PPG data are extracted such that each cycle has a systolic and a diastolic peak.

4.1.1 Data. Dataset C was used to evaluate this approach.

4.1.2 Algorithm. Synchronised accelerometer data is used to track the PPG windows (of size 5 seconds) with motion artifacts. The segments identified as corrupted with motion (refer Figure 1) are removed. The individual PPG pulses are then stretched in time to a nominal width of 625 ms (40 samples at a sampling rate of 64 Hz) and normalized in area. As observed in [14], and as captured in Figure 9, these templates match well with each other.

Let there be I pulses, $p_i, i \in \{0, \ldots, I-1\}$ in a test-segment and J pulses, $r_j, j \in \{0, \ldots, J-1\}$ in the reference segment. Typically, I, J are in the range of $[30, 40]$. We compute for the i^{th} pulse, its minimum distance from the reference as:

$$d_{\text{test}}[i] = \min_{j \in \{0,\ldots,J-1\}} \text{dist}(p_i, r_j) \quad (1)$$

where $\text{dist}(x, y)$ is the Euclidean distance metric. The distances d_{ref} are also computed as in (1) with $j \neq i$. Next, the distributions of the distances d_{ref} and d_{test} are computed. An example of these distributions is given in Figures 7 and 8. To determine if the test segment belongs to the same user as the reference segment, first a threshold t_1 is needed. We then find d_1, such that t_1-percentile of the distance vector in d_{ref} falls below d_1. The test segment is treated to be of the same user if the percentage of distances in $d_{\text{test}} > d_1$ is less than a second threshold t_2. Such a test segment is treated as the reference segment for the computation with next segment.

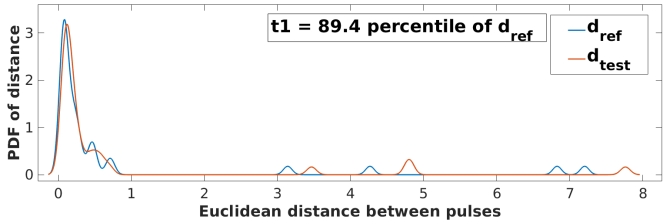

Figure 7: For this user, FN is minimum at the stated t_1

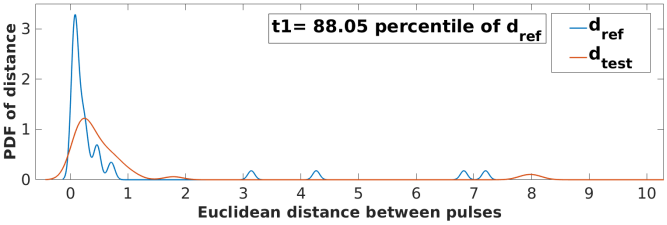

Figure 8: For this user, FP=FN at the stated t_1

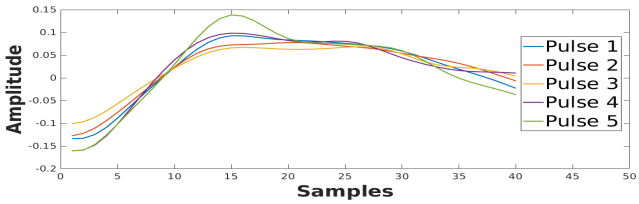

Figure 9: Examples of aligned, normalized PPG pulses.

4.1.3 Evaluation Criteria. For our deployment scenario, using the PPG to maintain an authenticated session, minimizing the False-Negative rate (FN) is of importance - a low false negative rate essentially translates to fewer re-authentication requests to the user. Thus, we perform a grid search to obtain the values of t_1 and t_2 that minimize the FN that is FN_{t_1} and FN_{t_2}. Note we also envisage optimizing these values for each user.

In order to compare with state of the art techniques, we also report the rates at which FN and False Positive rate (FP) are equal, i.e. Equal Error Rate (EER). In this case too, a grid search is performed to obtain the values of t_1 and t_2 that minimize the EER, namely EER_{t_1} and EER_{t_1}, respectively. In a deployment scenario, re-authentication may be made mandatory on watch removal, and it is thus acceptable to minimize FN and EER independently.

4.1.4 Result. Table 1 shows the minimum FN for the seven users of our database. We observe that across users the values of FN_{t_1} range from 60 to 90-percentile, and those of FN_{t_2} range from 9 to 13%. For the same users, the EER ranges from 0.41% to 10% which is in the same range reported by [14]. However their data was collected in a controlled environment, with very little motion artifact, unlike ours. The corresponding ranges for EER_{t_1} and EER_{t_2} are 80 to 90 percentile and 7 to 11% respectively.

Table 1: Minimum False Negative rates (%) and the Equal error rates(%) with corresponding thresholds t_1 (percentile) and t_2 (percentage) for seven users.

User ID	FN	FN_{t_1}	FN_{t_2}	EER	EER_{t_1}	EER_{t_2}
1	0.41	89.4	9	1.67	88.05	11
2	0.41	93.45	13	9.2	82.65	11
3	0.41	58.35	13	0.83	89.4	7
4	0.83	94.8	11	0.41	94.8	11
5	0.41	93.45	9	1.67	89.4	9
6	0.41	97.5	9	0.83	96.15	9
7	0.41	86.7	13	10.04	92.1	9

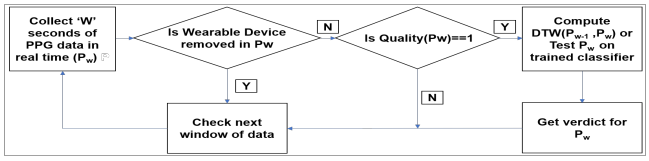

Figure 10: Flowchart of proposed approach.

4.2 Technique 2: Using Dynamic Time Warping (DTW) between PPG segments

The previous technique, despite having a good EER and being functional using in-situ data, is a threshold based approach. These thresholds are computed using both the authorized and unauthorized users data which means for an unknown adversary, this approach will not work. Moreover, the thresholds are device specific. This compelled us to move to a more real-time approach. In this technique we investigate utilizing the DTW computation between PPG windows to keep a check on users authenticity over time.

4.2.1 Data. Dataset B1 & B2 are used.

4.2.2 Algorithm. The algorithm flowchart is shown in Figure 10. The first step is to detect if there is a device-removed event. This is to ensure that only the recent past window of PPG data P_{w-1}, of an individual is always compared to the current window P_w for performing seamless re-authentication.

In this technique, the last N consecutive windows, from the most recent past prior to the device removal event are individually compared to current N consecutive windows post device worn event to compute the dynamic time warping distance between the two windows. Say W is the most recent past PPG segment (refer to Figure 5) having l windows,and W' is the current segment. Next, T_1, T_2 and T_3 are computed as shown below:

$$T_1 = \sum_{i=1}^{N} \sum_{k=N-1}^{0} \phi(W'_i, W_{l-k}) \tag{2}$$

$$T_2 = \sum_{k=N-1}^{0} \sum_{j=N-1}^{0} \phi(W_{l-k}, W_{l-j}) \tag{3}$$

$$T_3 = \sum_{k=1}^{N} \sum_{j=1}^{N} \phi(W'_k, W'_j) \tag{4}$$

Table 2: Instances in the data

Device	User change instances	Same user instances
Samsung	4	10
E4	18	8

Table 3: The DTW Approach, *average precision*=0.75 and *average recall*=0.56. 'U' and 'A' refer to the user and adversary.

		$W=3, O=2, N=4$		$W=4, O=3, N=4$	
	Predicted	U	A	U	A
Actual	U	6	12	8	10
	A	2	20	2	20

where $\phi(A, B)$ gives the DTW distance between windows A and B. Finally, verdict V is given by:

$$V1 = \begin{cases} 1, & \text{if } (abs(T1/T2) \leq 0.7 \vee abs(T1/T2) \geq 2) \\ 0, & \text{otherwise} \end{cases}$$

$$V2 = \begin{cases} 1, & \text{if } (abs(T1/T3) \leq 0.7 \vee abs(T1/T3) \geq 2) \\ 0, & \text{otherwise} \end{cases}$$

$$V = \begin{cases} 1, & \text{if } V1 \vee V2 = 1 \\ 0, & \text{otherwise} \end{cases}$$

Note, for this approach to work, the N consecutive windows in both segments W and W' should be free of motion artifacts. Out of the 20 sessions, 7 of them are collected using Samsung Gear S3 and 13 using the E4. Each session has two watch removal events, resulting in a total of 40 re-authentication events. A break up of the re-authentication events where the same/different user wore the device are mentioned in Table 2.

4.2.3 Evaluation Criteria. As before, the primary goal of this work is to ensure an adversary wearing the device is detected (minimize false positives) as well as reduce the number of user re-authentications (minimize false negatives). We use the measures of precision and recall to evaluate our approaches.

4.2.4 Result. A grid search is performed with multiple combinations of window sizes ($W = 3 - 12s$), overlap between windows ($O = 2 - 11$) and the number of consecutive windows ($N = 3 - 5$), prior to and post wearing the device, being compared. The top two results are tabulated in Table 3. The key benefit of this approach is that it is device independent. Note, the total time taken to detect an unauthorized access in this approach would be $t + W + (W - O) * N$ seconds, where t is the time taken to wear the device (which was observed to be around 14-18 seconds).

4.3 Technique 3: One class classification

While the DTW approach provides a real-time device and ML independent solution, we observed that the technique had certain limitations. A significant change in breathing pattern as well the way the device is worn, varying the amount of contact the sensor has with the body, is reflected in the PPG signal. Comparing PPG signals under these conditions using DTW is one of the reasons for the high false positives and false negatives observed in the previous approach. This compelled us to take a step deeper and explore PPG pulse morphology features by building a subject specific model.

Table 4: One class classification, *average precision*= 0.3, *average recall*= 0.95. 'U' and 'A' refer to the user and adversary.

		Subject $1_{Classifier}$		Subject $2_{Classifier}$	
	Predicted	U	A	U	A
Actual	U	14	0	9	1
	A	25	0	29	0

Table 5: Top selected pulse specific features

Feature Number	Feature Name
F3	Dicrotic Notch Amplitude
F8	Ratio F2/F6
F9	Ratio F2/Total pulse width

4.3.1 Data. Dataset B2, & D are used.

4.3.2 Algorithm. Dataset D was used to create a subject specific model. Since the PPG morphology changes based on the users emotional and physical activities, we collected a longer baseline to capture this variation in the data. Quality-checked data was used to extract pulse morphology based features (Table 5) and build the classifiers. A window size of 5 seconds are used for feature extraction, both in the training and testing phases. Support Vector Machine (SVM) based one-class classifier were used to build the model. Dataset B2 was used only for testing the model.

Every pulse having a systolic and a diastolic peak within the 5 second window of test data was normalized followed by extraction of pulse morphology based features which are then fed to the classifier. The classifier outputs a verdict for each pulse. The final output is the majority verdict for a window.

4.3.3 Evaluation Criteria. Refer Section 4.2.3.

4.3.4 Result. The results are tabulated in Table 4. We measured the system output prediction at different intervals - 30s, 1min & the entire segment (Refer Figure 5). Although the average recall rate is very high, minimising the false re-authentication queries, the precision is low suggesting poor adversary detection. For all three intervals, the same result was obtained indicating that waiting for a longer duration does not improve the classifier prediction.

4.4 Technique 4: Tree Bagger based binary classification

While we wanted to avoid building an adversary dataset, clearly using a unary classification results in high unauthorized access. However, using pulse morphology features does recognize the user to a high degree despite the interval between enrollment and testing. In this approach we investigate a binary classification mechanism

Table 6: Classifier$_{Subject1}$ Confusion Matrix, V_{th}=0.2, Y=120 minutes

Test Duration		*30 seconds*		*1 minute*		*Entire segment*	
	Predicted	U	A	U	A	U	A
Actual	U	2	12	2	12	2	12
	A	3	22	4	21	5	20

Table 7: Classifier$_{Subject2}$ Confusion Matrix, V_{th}=0.08, Y=20 minutes

Test Duration		*30 seconds*		*1 minute*		*Entire segment*	
	Predicted	U	A	U	A	U	A
Actual	U	1	9	1	9	1	9
	A	6	23	6	23	6	23

with an adversary dataset to increase the variety of PPG morphology information.

4.4.1 Data. Dataset B2, D & E are used.

4.4.2 Algorithm. For this approach, we consider a two step model building process. In the first step a 2-class subject-specific classifier is built following which a personalised threshold value is calculated for that subject. We build a classifier for each subject in dataset D and use dataset E to build the adversary class.

The fiducial features (refer Table 5) are extracted from both the datasets. An MIC based feature selection [18] suggested F3, F8 and F9 as the top features, which are then used to train the model (say M), and build a subject specific Tree Bagger classifier. Note, of the subject data used to build the model, around 30% of this data (Y) is set aside to compute the personalized threshold.

Personalized Threshold: In the previous attempt we observed that a subject specific model using PPG morphology features provided a high recall value but with low precision. To improve this measure we introduce a personalised adversary threshold value (say V_{th}) where $V_{th} = 1 - V_r$ and V_r is the recall value of Y tested on the model $M_{Subject}$. The values of Y and V_{th} for each subject classifier are mentioned in Table 6 and 7.

Dataset B2 is used for testing the classifier's performance. Majority voting based verdict is given for each window of 5 seconds duration as described in Section 4.3.2. The Testing is done on 30 seconds, 60 seconds and for the entire segment (Refer Figure 5) to understand the performance-time tradeoff. In the test segment, if the percentage of windows predicted as an adversary >=V_{th}, the segment is considered to belong to the adversary. The confusion matrices using this technique are presented in Table 6 and 7.

4.4.3 Evaluation Criteria. Refer Section 4.2.3.

4.4.4 Result. While a cost sensitive classifier, where more weight is given to the detection of an adversary, clearly reduces the false positives, it increases the number of re-authentications to the user. While this tradeoff cannot be eliminated, there is perhaps a possibility of finding a sweet spot between the number of re-authentications to the user and the detection of an unauthorized access.

5 CONCLUSION

Smartwatches and other wrist worn devices are increasingly becoming part of our circle of trusted devices allowing us to not only use it as an authentication token to access other devices but to also perform financial transactions. Authentication mechanisms are then needed on these devices to prevent any misuse of this trust. Since constant authentications can damper user experience, there is a need to address this.

Prior attempts in using the PPG as of form of continuous biometric authentication fail to consider this sensor in the wild. In this work we therefore explored the possibility of using the PPG sensor in a more *in-situ* setting to support zero re-authentications.

To evaluate the four approaches proposed in this paper, we created several datasets of '*everyday*' PPG across multiple participants and devices. With each technique tried, we progressively learnt the morphology of the PPG signal better and it's limitations in maintaining an authenticated session in an everyday scenario.

REFERENCES

[1] 2013. E4 wristband Real-time physiological data streaming and visualization. https://www.empatica.com/en-eu/research/e4/ Accessed: 2021-05-20.

[2] 2015. HP Study Reveals Smartwatches Vulnerable to Attack. https://www.securityweek.com/all-smartwatches-vulnerable-attack-hp-study Accessed: 2021-05-20.

[3] 2018. *How to use Smart Lock to unlock your phone automatically.* https://www.androidcentral.com/smart-lock Accessed: 2021-05-20.

[4] 2021. *Make purchases easy with Fitbit Pay.* https://www.fitbit.com/in/fitbit-pay Accessed: 2021-05-20.

[5] 2021. Samsung Gear S3. https://www.samsung.com/global/galaxy/gear-s3/experience/ Accessed: 2021-05-20.

[6] Felton Blow, Yen-Hung Hu, and Mary Hoppa. 2020. A Study on Vulnerabilities and Threats to Wearable Devices. In *Journal of The Colloquium for Information Systems Security Education*, Vol. 7. 7–7.

[7] Anirban Dutta Choudhury, Aditi Misra, Arpan Pal, Rohan Banerjee, Avik Ghose, and Aishwarya Visvanathan. 2014. Heartsense: Estimating heart rate from smartphone photoplethysmogram using adaptive filter and interpolation. In *International Internet of Things Summit*. Springer, 203–209.

[8] Alotaiby et al. 2020. A Nonfiducial PPG-Based Subject Authentication Approach Using the Statistical Features of DWT-Based Filtered Signals. *Journal of Sensors* 2020 (2020).

[9] Bonissi et al. 2013. A preliminary study on continuous authentication methods for photoplethysmographic biometrics. In *2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications*. IEEE, 28–33.

[10] Karimian et al. 2017. Human recognition from photoplethysmography (ppg) based on non-fiducial features. In *ICASSP*. IEEE, 4636–4640.

[11] Lee et al. 2019. Wearable Bio-Signal (PPG)-Based Personal Authentication Method Using Random Forest and Period Setting Considering the Feature of PPG Signals. *JCP* 14, 4 (2019), 283–294.

[12] Spachos et al. 2011. Feasibility study of photoplethysmographic signals for biometric identification. In *2011 17th International Conference on Digital Signal Processing (DSP)*. IEEE, 1–5.

[13] Sarkar et al. 2016. Biometric authentication using photoplethysmography signals. In *BTAS*. IEEE, 1–7.

[14] Sancho et al. 2018. Biometric authentication using the PPG: a long-term feasibility study. *Sensors* 18, 5 (2018), 1525.

[15] Yadav et al. 2018. Evaluation of PPG biometrics for authentication in different states. In *2018 International Conference on Biometrics (ICB)*. IEEE, 277–282.

[16] Zhao et al. 2020. Trueheart: Continuous authentication on wrist-worn wearables using ppg-based biometrics. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 30–39.

[17] Anthony Lee and Younghyun Kim. 2015. Photoplethysmography as a form of biometric authentication. In *2015 IEEE SENSORS*. IEEE, 1–2.

[18] D. N Reshef and et al. 2011. Detecting novel associations in large data sets. *science* (2011).

[19] Chi Zhang, Hossain Shahriar, and ABM Kamrul Riad. 2020. Security and Privacy Analysis of Wearable Health Device. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 1767–1772.