WhoAmIOn: A Technique To Determine Whether All Devices Are Being Used By The Same Person

Anuja Achyut Pinge,† Amey Damle,† Rishav Mukherji,† Bhargav Nagaraj,† Surjya Ghosh,†‡ Sougata Sen†‡
†*Department of Computer Science and Information Systems, and* ‡*APPCAIR*
BITS Pilani K.K. Birla Goa Campus, Goa, India.

2024 IEEE Smart World Congress (SWC) | 979-8-3315-2086-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/SWC62898.2024.00155

***Abstract*—Wearable devices, with a plethora of sensors, can measure physical and physiological signals from various on-body locations, and log the information against a device owner's profile. However, when another person uses the same wearable device, the other person's activities and health-related information are also logged into the owner's profile, causing mis-logging. One approach to prevent mis-logging is by enabling the owner's wearable devices to communicate amongst themselves to determine if the same person is using them.**

In this work, we also explore the possibility of using heart rate and inertial sensor data from multiple devices to determine their co-existence with the same user. We developed the WhoAmIOn system that uses machine learning techniques (as compared to correlation approaches that are currently used) to determine whether the same person is using the devices. Overall, we observed that with the inertial sensor, we achieved an accuracy of 52%, while with a heart rate sensor the accuracy increases substantially to 85% in determining whether the same user is wearing or using the devices at the same time instant in a free-living setting. This demonstrates that, it is indeed possible to use heart rate sensors to determine if devices are on the same body.

***Index Terms*—Wearable Devices, Tracking, Multi-sensor Correlation, Heart Rate Monitoring, Security.**

I. Introduction

Wearable devices, nowadays, are available in various shapes, sizes, and form factors, and many users wear multiple wearable devices in various on-body positions. Many companies are progressively developing novel wearables, primarily for health tracking and activity monitoring [Apple(2024)], [Samsung(2024)], [Garmin(2024)], [Polar(2024)], [Movsense(2024)]. These companies embed these devices with multiple sensors that collect physical, physiological, and contextual information such as physical activities, heart rate, blood-oxygen levels, and ambient temperature, to name a few. Application developers taking advantage of these sensors usually assume that these devices are worn or carried by a particular user – the device owner. These applications sometimes request a passcode to verify whether the owner is using the application. Most such applications do not usually verify if the owner continues to wear *all* their device – a multi-device Continuous Authentication (CA) task [Zhao et al.(2020)]. If multiple users share a device, the manufacturer might expect the non-owner to change the profile, a cognitive task the non-owner might not perform [Plass et al.(2010)]. Thus, a seamless and automatic CA approach among the owner's devices is necessary.

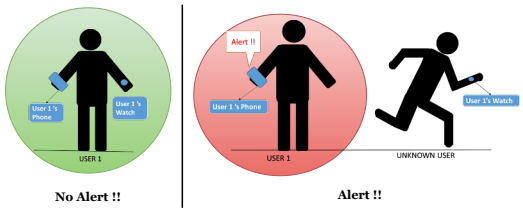


Fig. 1: WhoAmIOn is a technique to determine if all devices are on the same user. WhoAmIOn runs on all devices and processes sensor data to determine if all the devices are worn or carried by the same user (Scenario 1). WhoAmIOn raises an alert if the devices are not on the same user (Scenario 2).

This paper answers the following question "*Can multiple devices of the owner collaborate to determine whether the devices' owner is using them?*". In this paper, we monitor multiple devices of the "owner" to determine whether all the devices are *on the same body at the same time*. If all the devices are not on the same user simultaneously, then we notify the device owner about the same. Thus, the primary goal of this work is to determine whether the same person is using all the owner's wearable devices simultaneously. We aim to achieve this goal by finding a relationship between sensor data from the user's devices. Although this task might appear similar to a CA task, most existing research in CA focuses on continuously authenticating a single device [Mare et al.(2014)], [Zhao et al.(2020)].

In the past, researchers have used inertial sensors to determine movement-based correlations; they hypothesized that inertial sensor streams from devices moving in a similar pattern will produce similar readings [Coskun et al.(2015)], [Mayrhofer and Gellersen(2007)]. However, with wearable devices placed on different on-body positions, the movement correlation might not be obvious. For example, inertial sensor reading from a wrist-worn smartwatch might exhibit movement when a person is working on the laptop, but the in-pocket smartphone's inertial data might not exhibit any movement. Thus, relying on inertial sensor individually for this multi-device CA task might not be a viable solution. It is well known that physiological signals such as human heart rate are often correlated, even when measured at different body locations [Pinge et al.(2022)]. Similarly, environmental signals like air pressure levels are often correlated

2993-396X/24/$31.00 ©2024 IEEE
DOI 10.1109/SWC62898.2024.00155

even when measured by sensors attached to various body parts [Meier and Holz(2023)]. In this paper, we focus specifically on body-generated signals and develop a technique, *WhoAmIOn*, that validates the possibility of *using the heart rate signal* to determine if the devices are on the same body. Figure 1 presents the conceptual idea of WhoAmIOn.

Using sensor correlation to determine whether the devices are on the same person has several inherent challenges that we must address to ensure that the technique is reliable. First, users wear devices on different body parts or carried differently. A device's on-body position (and sensor data from the device) should not affect WhoAmIOn's performance. Furthermore, the signal might attenuate when captured at different body locations. For example, the heart rate captured by the Electrocardiography (ECG) sensor near the chest captures voltage readings that enable detection of finer-grain details of the heart activity [Sörnmo and Laguna(2006)]. In comparison, a Photoplethysmography (PPG) sensor captures heart rate information using changes in blood volume [Castaneda et al.(2018)]. PPG usually captures coarser heart-related activities. WhoAmIOn should be robust to these differences and be able to determine if the same user is using the devices continuously. Second, the sensitivity and resolution of the same sensor type (e.g., two different PPG sensors from other manufacturers) might vary. This variation should not affect WhoAmIOn's performance. Third, various changes might affect a sensor's readings – for example, the PPG-based heart rate data might be affected by user motion or loose skin contact of the device. WhoAmIOn should not be affected by such external changes while performing continuous detection of whether the same person is using all the owner's devices. Fourth, a misused device might induce wrong information (e.g., logging in wrong activity information for the user). If WhoAmIOn considers short windows, then the difference in the two devices' data in those windows might be minimal. Longer windows will allow observing the differences better. However, a longer window will increase wrong information logging onto the users' profile.

Overall, while addressing these challenges, we develop WhoAmIOn, a technique that allows determining if all devices are worn by or carried by the same person. In contrast to the traditional approach of using inertial sensors for device correlation, WhoAmIOn experiments with heart rate sensor data to identify whether the same person is using the device. Inertial sensors can be sensitive towards their position on the body[Lu et al.(2010)], whereas, physiological signals such as heart rate do not vary drastically when collected from different body parts[Pinge et al.(2022)]. Hence, the heart rate sensor data can be considered robust towards body position compared to the inertial sensors. Traditionally, researchers have experimented with finding correlations between the sensor data. WhoAmIOn uses machine learning techniques to determine the same. Furthermore, when the devices are on a different person, there should be minimal latency in informing the owner about the possible misuse. WhoAmIOn uses a windowing technique to quickly identify misuse and share the same with the owner. The key contributions of this work are:

- In this paper, we present the design and development approach for the WhoAmIOn technique. We experimented using multiple machine learning approaches on two datasets – a publicly available Extrasensory dataset [Vaizman et al.(2017)], and our own dataset and observed that WhoAmIOn is capable of addressing the previously mentioned challenges and yet determine whether the devices are on the same person accurately.
- We demonstrate that while there is substantial correlation between inertial sensor readings obtained from mobiles and certain wearable devices, however the correlation is strongly tied to the position of the device. Deep learning techniques perform reasonably well, even with coarse-grained heart rate information obtained from PPG sensors. Overall, we can accurately determine whether the same user is using the device with an accuracy of 85% in both Extrasensory dataset, as well as our dataset.

Overall, WhoAmIOn will be helpful in various scenarios where a user might be interested in knowing if someone else is using their device, or a medical practitioner might be interested in knowing if their patient is actually using the device.

II. Related Work

Determining sensor correlations is useful for applications such as regular communication [Roy et al.(2015)], device authentication [Mayrhofer and Gellersen(2007)], crypto key generation [Wang et al.(2016)], or multi-device synchronization [Meier and Holz(2023)]. Over the years, researchers have experimented with various devices and sensors, to determine application-specific correlation patterns. Inertial sensors, due to their low cost, ubiquity, and diverse functionalities, are popularly used for performing these multi-device correlations [Mayrhofer and Gellersen(2007)], [Roy et al.(2015)], [Sen and Kotz(2021)]. In early wearable sensing days, accelerometer sensors have been used to synchronize multiple body-worn inertial sensors. Two accelerometers, when shaken together produce almost similar signals – researchers used this property to determine whether two sensors were shaken together [Mayrhofer and Gellersen(2007)].

Numerous novel applications that rely on these correlations have been proposed by various researchers over the years. One field that often benefits from sensor correlation is the field of security research. Several security-based works focus on exchanging a secret key via an out-of-band channel to enable secure communication [Mayrhofer and Gellersen(2007)], [Sen and Kotz(2021)]. One common approach for sharing this secret is is via correlating homogeneous sensors, especially the inertial sensor. Inertial sensor data have been used in the past to authenticate users based on their gait [Ngo et al.(2014)], based on specific action pattern that the user performs [Rahman et al.(2018)]. These works primarily focus on instantaneous authentication. Inertial sensor data has also been used by researchers for continuous authentication purposes. Mare et al. used the correlation across inertial sensors of a smartwatch and the keyboard typing and

mouse movement to determine if the intended user was using a specific terminal [Mare et al.(2014)]. In contrast to Mane et al.'s work, we primarily focus on using a novel sensor – the heart rate sensor, which captures a user's physiological response, an area that they have not explored. Using the heart rate sensor for user authentication is not novel, however [Zhao et al.(2020)]. We advances this work by correlating across multiple un-related sensors. Correlation across sensors has also been used be researchers for multi-device synchronization. Recently, Manuel and Holz explored the idea of multi-device correlation to synchronize between multiple devices [Meier and Holz(2023)]. They used the barometer data in collaboration with the accelerometer data to synchronize across devices worn on different body positions. This reveals a recent interest of using additional sensors for synchronization.

III. WHOAMION

The intuition behind WhoAmIOn is that the physiological signals produced by the body are similar during a time window, even when one measures this signal at different on-body locations. For example, the heartbeat measured via ECG on the chest will produce an equivalent change in the PPG reading measured on the wrist (with a slight delay – accounting for the time for the blood to flow from the heart to the body location). If we can measure any body-generated physiological signal during a short time window, we can use the data measured at different body locations to determine if the devices are worn by the same user. This correlation should be unique and difficult to forge. Thus, the overall goal of WhoAmIOn is to determine whether the same user is using (or wearing) all the devices belonging to the same owner at any particular time window. This problem can be formulated as a CA problem. Similar to other CA systems [Mare et al.(2014)], WhoAmIOn continuously checks whether the device owner is continuously using *all* their devices. In this section, we discuss the assumptions made while developing WhoAmIOn, the system model, and the adversary model of WhoAmIOn.

System Overview: Overall, this problem can be difficult as it involves aligning two recordings obtained from two devices based on the similarities in measurements contained in the sensor traces. These devices can exist at various on-body locations. WhoAmIOn must obtain data from these devices, align the data, frame it and determine if there is high cross correlation in the data. Formally, WhoAmIOn consists of a set of devices D that are connected to a hub device – H. A device $d_i \in D$ as well as H has a set of sensors S_i. $s_i \in S_i$ sample at a constant sampling rate and this data is sent to the hub device at a specific rate. We describe the system overview of WhoAmIOn to perform this task.

Figure 2 presents the overall system details of WhoAmIOn. The WhoAmIOn system executes on H, a smartphone (or another similar hub device) of the owner. We assume that H is a proxy for the user – it is always on the user or somewhere near the user. The user authenticates H using a technique that is beyond the scope of WhoAmIOn. H is

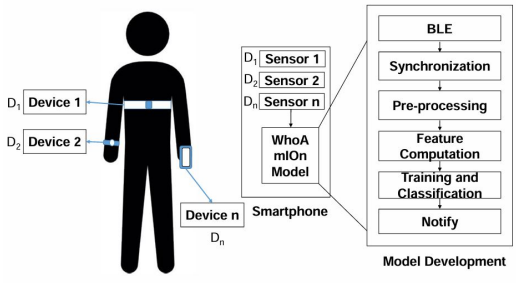


Fig. 2: Overall system architecture of WhoAmIOn. User's devices are connected to the user's smartphone via BLE. All sensor data is transferred to the phone where the sensor data are correlated to determine if all devices are on the same user.

capable of connecting with D over a RF channel, such as Bluetooth Low Energy (BLE). The pairing and usage (in case of BLE) step acts as a validation that a particular device belongs to the smartphone's owner. WhoAmIOn assumes that these paired devices are independent devices that share sensor data with H – the WhoAmIOn system execution location. The connected devices can be heterogeneous – each device providing data from one of more sensor channels. WhoAmIOn aggregates data collected from D on H. Additionally, the WhoAmIOn system executing on H to extract sensor data from H. The WhoAmIOn module on H pre-processes the data obtained from D to remove any outliers and to impute missing data. The sensor stream S_{ij} (i is the i^{th} device from which data is obtained, and j is the j^{th} sensor stream in device i) is windowed independently. These windows are aligned and features are computed. A pre-built model exist on the phone that is used to test the data obtained from the J sensors on the I devices exists. WhoAmIOn assumes that if all devices are on the same user, then the pattern will be similar to the pattern recorded in the model. In case any one of the devices' sensor data does not follow the pattern, then WhoAmIOn reports the same to the user in the form of a smartphone alert.

System Model: We envision that specific modules of WhoAmIOn will be executing on all the devices of the user. The set of sensor data collected by each device can vary based on the device's capabilities. Currently, we assume that the devices can collect either the heart rate data, the inertial data (accelerometer and gyroscope), or both heart rate and inertial sensor data. However, WhoAmIOn will work with any other time series data obtained from the devices. All devices will share the sensor data with H, which can commonly be the user's smartphone. Since a user's personal devices are already connected to the smartphone, additional bonding and pairing steps will not be necessary. Furthermore, this pairing is a proxy of the device belonging to the owner of the hub device. In case d_i is not in range of H, it can locally store the data, and once it is in the proximity of H, it can share the data that can be analyzed at H. H already contains a machine learning model to determine whether all d_i are on the same

person. This model is created by collecting sensor data from all the user's devices in an offline manner, prior to the real-time tracking. When new data arrives from the user's devices, they are preprocessed, fused together, and passed through the classifier. In case the classifier determines that the devices are not on the same user, it notifies the smartphone's owner.

Assumptions and Limitations: We make the following assumptions while developing WhoAmIOn. First, we assume that the user has already authenticated the devices they use. WhoAmIOn does not explicitly authenticate users; its goal is to determine if all the devices are on the same user. Several existing continuous authentication works do make similar assumptions of a one-time in-session authentication using password or PINs [Mare et al.(2018)]. Second, we assume that the hub device is always with the owner. This device will be used to obtain the initial authentication, and will use this authentication to continuously authenticate all other devices. It is obvious that a misplaced hub device will be easily observable to the owner, even without WhoAmIOn. Third, smartphones are not in contact with the user's skin and thus cannot take PPG readings. We currently use only the inertial sensors from the smartphone. However, in future, with RF-based heart rate measurement systems [Gromert and Alnasser(2022)] can be integrated into WhoAmIOn.

Adversary Model: WhoAmIOn is primarily concerned about the misuse of personal devices to manipulate the outcome of a system or application that is concerned with user-task mapping such as what activities were performed by the user [Zeni et al.(2014)]. In such a scenario, a mischievous adversary aims to manipulate the data of the user-task mapping by providing data that is not of the truthful owner (e.g., the adversary uses the owner's wearable camera intended for food journaling or other similar application [Thomaz et al.(2013)], [Mamish et al.(2024)] to provide wrong food consumption information). The adversary has the authentication details of D and can log into D and use it as it is intended to be used. However, the adversary does not have physical access to H or the privilege to modify the sensor data stream collected and transferred by D.

IV. Dataset collection and Feasibility Study

To detect whether multiple devices are on the same body, we analyzed sensor data from two datasets – the publicly available Extrasensory dataset [Vaizman et al.(2017)], and the MultiDevice dataset that we collected in a controlled setting.

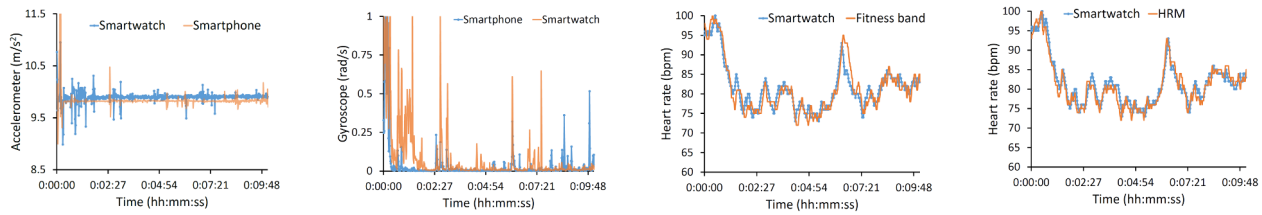
Extrasensory Dataset: The Extrasensory dataset consists of data from 60 participants in a free-living condition. Participants wore a smartwatch and carried a smartphone while carrying out their everyday activities. For our analysis, we used the inertial sensor data collected when the participant was either Walking or Running. Although we would have liked to use a physiological sensor for the analysis, the data set did not have the same. We considered only these activities for two reasons. First, as we will see in Section IV-A, when a person is sitting and performing a task, the correlation between inertial sensor data is low. Second, these two activities make up the majority of the dataset. We analyzed over 125 hours of data to evaluate WhoAmIOn.

MultiDevice Dataset: The Extrasensory dataset does not provide heart rate (or other physiological) data. However, as we wanted to examine whether we could use the heart rate data for correlation purposes, we also collected data in a controlled lab setting. We call this in-lab collected dataset as the *Multi-Device Dataset*. The MultiDevice dataset captures the resting condition (sitting still), physical activities (walking, ice bucket task), and psychological activities (mental arithmetic, public speaking). Overall, we collected data from 12 participants (6 males and 6 females) who individually performed tasks in a specified order: public speaking, mental arithmetic, an ice bucket task, and finally, walking. All tasks were performed for 5 minutes, and there was a break of 5 minutes between each of these tasks) for 45 minutes in an IRB-approved study. Participants wore three devices, namely (i) Polar H10 Chest Heart Rate Monitor [Polar(2024)], (ii) Samsung Watch 4 [Samsung(2024)], and (iii) Garmin Vivosmart 4 Fitness Band [Garmin(2024)] along with carrying a Samsung M32 smartphone in their pocket. The Polar H10 Chest Heart Rate Monitor was worn by participants on the chest and it collected heart rate via ECG technique. The Samsung Watch 4 was worn on the wrist, and it collected accelerometer, gyroscope, and heart rate via PPG technique. The Garmin Vivosmart 4 was also worn on the wrist, and the heart rate was collected using the PPG technique. The collected data was transferred to the smartphone over BLE. We also collected accelerometer and gyroscope data from the smartphone (placed in the participant's pant pocket).

A. Feasibility Study

We initially performed a feasibility study with sensor data to determine the correlation between various devices and sensors. We experimented with our collected dataset. The sampling frequency of the inertial sensors is 100 Hz, while we collected the heart rate data at 1 Hz. For the inertial sensor data, we computed a 1-second average of the data using a tumbling window approach. As there is linear relationship amongst sensor data obtained from different devices and this data did not have any outlier (we removed in the pre-processing step), Person's correlation is a well-suited technique for correlation. We computed the Pearson's correlation value for each device-sensor combination by computing a person-wise Pearson correlation, taking the absolute of the correlation coefficient and then taking an average across all 'N' participants' data (N=12).

Overall, we observed that although prior research has shown that inertial sensors are well suited for correlating devices or generating secret keys based on the movement pattern [Mayrhofer and Gellersen(2007)], [Sen and Kotz(2021)], they assumed the devices will move similarly. However, different devices will experience different movements when worn on different body parts. For example, when a person is sitting and working on their laptop, the sensor data collected by the accelerometer on the smartphone and smartwatch will be



(a) Comparison of accelerometer sensor signals obtained from Samsung Watch and Samsung Phone.

(b) Comparison of gyroscope sensor signals obtained from Samsung Watch and Samsung Phone.

(c) Comparison of heart rate from the PPG sensor of Samsung Watch and Garmin fitness band.

(d) Comparison of heart rate from Samsung Watch's PPG signals and Polar HRM's ECG signal.

Fig. 3: Comparison of various signals from a participant's data. The signals are obtained from four different devices that were worn by the participant. The correlation between the heart rate data obtained from the devices is evident. Interestingly, the correlation does not depend on the device type or the sensing approach (PPG or ECG).

Sensor1 (Device1)	Sensor2 (Device2)	Average Correlation
PPG (Garmin Vivosmart 4)	PPG (Samsung Watch 4)	0.77
ECG (Polar H10 HRM)	PPG (Garmin Vivosmart 4)	0.76
ECG (Polar H10 HRM)	PPG (Samsung Watch 4)	**0.80**
Accel. (Samsung Watch 4)	Accel. (Smartphone)	0.18
Gyro. (Samsung Watch 4)	Gyro. (Smartphone)	0.60

TABLE I: Correlation of sensor values from different devices. We observe that the ECG from the Polar H10 and the PPG from the Samsung Watch 4 have the highest correlation.

different. Table I presents the sensor-wise correlation that we observed for different sensors. From the table, we can observe that the inertial sensor correlation between the sensors on the smartphone and smartwatch is 0.18, which indicates extremely low correlation. On the contrary, the correlation between the heart rate sensors – both ECG and PPG type – collected from different body locations have a higher correlation. Overall, we observed a correlation between 0.76 to 0.80 for the PPG-PPG pairs, as well as ECG-PPG.

To visually confirm this finding, we plotted the magnitude of the accelerometer readings obtained from the smartphone and smartwatch (Figure 3a), the magnitude of the gyroscope readings obtained from the smartwatch and smartphone (Figure 3b), the PPG readings obtained from the smartwatch and the fitness band (Figure 3c), and the PPG reading obtained from the smartwatch and ECG reading obtained from the heart rate monitor (Figure 3d). All the data were collected from one participant during the user study. Although the participant provided longer data, we have trimmed it for a 10-minute duration. Overall, we can visually confirm the high correlation in the heart rate reading, while the correlation is less for the accelerometer reading. This indicates that it is possible to use the heart rate sensor data to correlate devices.

V. Methodology

We next describe the steps taken by WhoAmIOn to determine whether all devices are being used by the same user. At a high level, WhoAmIOn determines whether two devices are on the same user. If it identifies that the two devices are not on the same user, then it notifies the device owner. We have previously performed correlation using the raw signal and shown that there exists a correlation between specific sensors and devices, when the devices are on the same user. This indicates that if we consider a small window, then the sensor data in that window vary similarly. However, currently it is unknown if the correlation values are useful in distinguishing whether the devices are on the same user. We consider the task of determining whether the devices are on the same user as a machine learning task, where we will train models using data collected from multiple devices worn by the same user during particular activity – this is the positive class, and data collected when all the devices are not on the same person, but the people wearing the devices are performing the same task (either physical or physiological) – we call this the negative class. We use these two data groups and build a machine learning model that can realize WhoAmIOn in real-time.

To run the WhoAmIOn system, the sensor devices should be connected to the smartphone. We assume that the data reaches the smartphone via a RF module and the subsequent steps are performed on the smartphone. Smartphones have enough capability to perform the detection in real time. However, currently we assume that the data from these sensors have already been collected and we are processing them offline, on a more powerful device, a server. We thus focus on determining the performance of the generated models. The following steps are performed on the server.

Data Synchronization: In our current implementation, we assume that the available sensors are PPG, ECG, accelerometer and gyroscope, i.e., $\{PPG, ECG, accelerometer, gyroscope\} \in \cup S_i$. However, in future additional sensors can always be integrated into WhoAmIOn. For both the inertial sensors, we consider all three axis of the sensor. For the sensors, we organize them into smaller windows of 1 second.

Pre-processing: Loss of packets in wireless networks is common. In real-time evaluation, WhoAmIOn can either ignore those windows or extrapolate the previous readings to compute the subsequent readings. In our offline dataset, whenever a 'NA' field is encountered, WhoAmIOn drops those readings. With the available data, it is possible that erroneous readings

Sensor Signal	Features
Heart Rate	Maximum, Mean, Standard Deviation
Accelerometer, Gyroscope	Mean X, Mean Y, Mean Z, Variance X, Variance Y, Variance Z, Covariance(X, Y), Covariance(Y, Z), Covariance(X, Z)

TABLE II: Various features computed for sensor signals

creep into the dataset. For example, we assume that the users' heart rate will be between 55 and 220 bpm. Readings outside the range should be filtered [Mishra et al.(2020)]. We used a band pass filter on all sensor readings to remove outliers.

The remaining data is framed into windows of size w. We used a sliding window technique to create the frames such that there was an overlap ϕ between subsequent frames. These frames are next passed to either a feature extracting unit in case a shallow learning technique is used, or directly to the classifier in case of deep learning approaches.

Feature Computation: For each window, we computed sensor specific time series features. For the heart rate sensor (both ECG and PPG), we compute the 'mean', 'standard deviation' and the 'maximum' heart rate for that window. For the inertial sensors (both accelerometer and gyroscope), for each axis, we compute the 'mean', 'variance', and 'covariance'. Overall, for each inertial sensor, we extracted nine features for a particular value of w and ϕ. The exact computed features are summarized in Table II. These basic time domain features have been used in several activity recognition works [Gupta et al.(2020)].

Training and Classification: WhoAmIOn allows performing both train-test split of the data, as well as leave one person out cross validation. In case of train test split, the data for one participant is either present in the training set, or the testing set when performance is computed. Currently, we experimented with multiple classifiers (both deep learning and shallow learning ones). Specifically, from shallow machine learning algorithms, we considered XGBoost and Extra Tree classifier, while for deep learning, we chose the Long Short-Term Memory (LSTM). XGBoost and Extra Tree classifiers are ensemble machine learning methods that are based on decision trees when used for classification. Even though these classifiers work well with time-series data, they might fail to capture temporal details when irrelevant features are used.

Techniques such as LSTM do not require hand-crafted features. LSTMs can capture and maintain the information contained in the long sequences. It can directly work with raw signals without the need for computing features. We thus trained our LSTM using the raw sensor signal. We use a LSTM architecture that has 36 hidden states, followed by a linear layer resulting in an intermediate state of 12 followed by another linear layer which then predicts a single output. We use a batch size of 32 for the training.

Post-processing and Output: The outcome of the classifier indicates whether the device is on a particular user at any point of time. We perform a smoothing to remove false positives. Overall, we perform a majority voting on a window size of 'k' windows to determine whether the devices are being used by the same person. Thus, we can determine the misuse of a device in $k \times w$ seconds, where w is the window size.

VI. Evaluation

We next describe our evaluation strategy for WhoAmIOn.

A. Dataset creation and model building

We created two fused datasets for each of the Extrasensory datasets and the MultiDevice dataset.

Extrasensory Dataset: The extrasensory dataset consists of an inertial sensor collected at a frequency of 1 minute. We used a window size $w = 5$ minutes, and overlap $\phi = 60\%$ We created two datasets using the Extrasensory dataset. In the first dataset (E_S), we combined all instances of the windows of the smartphone and smartwatch that were collected from the same user at the same timestamp. This emulates a scenario where all devices are on the same user at the same time. In the second dataset (E_D), we combined windows of data from the smartphone and smartwatch such that the data was not time-aligned. Specifically, we matched the data from the inertial sensors of the smartwatch collected at time t_0 with that of the data from the smartphone collected at $t_0 + 5$ minutes. E_D emulates a scenario where the same device is *not* on the same user at the same time. The final Extrasensory dataset consists of a combination of E_S and E_D, where E_S represents the positive class, and E_D represents the negative class. We evaluated the extrasensory dataset via a 80-20 split, where 80% of the data was used for training and tested on 20% data, i.e., with 12 participants' data.

MultiDevice Dataset: In the MultiDevice dataset, the heart rate was collected at a frequency of 1 Hz from the Garmin Vivosmart 4, the Polar H10, and the Samsung Watch 4, while the inertial sensors were collected at 16 Hz from the smartphone, and Samsung Watch 4. We used the mean of the inertial sensor readings to obtain 1 data point per second. We experimented with various values of w and ϕ for the MultiDevice dataset. Specifically, we experimented with $w = \{3, 5, 10, 20, 30, 40, 50, 60\}$ seconds with $\phi = \{0, 50\}\%$. We again created two datasets, M_S, and M_D for the MultiDevice dataset using the same approach used in the Extrasensory dataset. For M_S, all data collected at the same time window were included in that data instance. In case of M_D, as there were multiple devices and sensors, we used the following strategies: In case of inertial sensors (both accelerometer and gyroscope) the same strategy as E_D, i.e., one device's $\mathrm{t}_0 + 5$ minutes was aligned to the other device. In case of heart rate, as three devices collected heart rate, we misaligned only one device's data at a time by 5 minutes to train the negative class. We performed a leave one person out cross validation for this dataset as the dataset was smaller in size, and leave one person out cross validation provided a more generic result.

B. Evaluation metric

We evaluated WhoAmIOn using accuracy as the evaluation metric in determining whether the device is on the same

Classifier	Accuracy Accel-Accel
XGBoost	0.83
Extra-Tree	**0.84**
LSTM	0.56

TABLE III: Performance of classifiers on Extrasensory Dataset

Classifier	Accuracy HR-HR	Accel-Accel	Gyro-Gyro
XGBoost	0.79	0.52	0.67
Extra-Tree	0.66	0.62	0.68
LSTM	**0.85**	0.52	0.74

TABLE IV: Performance of classifiers on MultiDevice Dataset

Sensor Combination	Devices	Accuracy
PPG - PPG	Garmin Vivosmart 4, Samsung Watch 4	0.74
ECG- PPG	Polar H10 , Garmin Vivosmart 4	0.75
ECG-PPG	Polar H10, Samsung Watch 4	**0.84**

TABLE V: Evaluation of the system for heart rate sensor for device-wise performance using the MultiDevice Dataset.

user. One might argue that F1-score provides a more realistic performance. However, as we have equal-sized one positive and one negative class data in our dataset, the accuracy and the F1-score will result in the same outcome.

VII. Results

Comparison of the different sensing modalities for on-body detection: We first tested the inertial sensor-based *Extrasensory dataset* using the machine learning pipeline described in the previous sections. Table III presents the results for the accuracy of classification using the dataset. From the results, we observe that even though the correlation between the raw sensor data was not high (reported in Section IV), however machine learning techniques indeed detected certain patterns in the features extracted from the raw data. This is reflected in the improvised correlation values for the accelerometer data (accuracy of 0.84 in the best case). One must note several factors contributed towards these score improvements. Firstly, we consider only the two active states, i.e., when the person is walking or running. Secondly, rather than considering individual data points, we are looking at windowed data. One surprising observation in Table III is that the LSTM technique performed poorly as compared to the shallow learning approaches. Prior work has demonstrated that XGBoost works well with tabular data. Thus, the high performance of XGBoost is not surprising. Similarly, prior work has shown that LSTM works well with time series data. However, either the coarse-grained data (1 reading per minute) might have caused the poor performance of the dataset's outcome or there might not be a substantial correlation for the LSTM to learn.

The MultiDevice dataset is a more realistic dataset as it consists of multiple activities' data collected from multiple devices. There are two devices that provide inertial sensor data readings and three devices that provide heart rate data (either ECG or PPG). We report the performance of the sensor using the machine learning technique described previously for two devices in the case of inertial sensors or all three devices in the case of heart rate. Table IV presents the results for the accuracy of classification using the MultiDevice dataset. For this dataset, we observe that there is a substantial drop in the performance of the shallow learning classifiers (XGBoost and Extra-Tree) on the inertial sensor data. However, the performance of LSTM is similar to that of the Extrasensory Dataset. This indicates that XGBoost might have learned something from the tabular information rather than the time series (the number of data points in the MultiDevice dataset is more than 60$\times$ that of the Extrasensory dataset). It is interesting to note that the performance of LSTM in detecting whether the data is on the same person using the heart rate data from three devices produces a high accuracy of 0.85. The best performance was obtained when we used a window size of 25 seconds. This indicates that WhoAmIOn can detect misplaced devices with an average delay of 25 seconds (considering the classification output obtaining delay is negligible). This indicates that although the physiological signal (heart rate) attenuates at a distance from the heart, yet it can be a strong candidate for performing CA.

Performance of device pair-wise heart rate signals: As evident from the experiments, the inertial sensors perform poorly in detecting whether the devices are on the same body, while the heart rate sensor is capable of detecting the same. In the previous section, we considered three heart rate devices and observed that the three devices could collaborate with each other and with an average performance of 0.85 detect if teh edvices were on the same person. However, one might argue that the performance might degrade when the number of heart rate devices are lesser. To answer this question, we performed a pair-wise comparison of accuracy for three devices to determine whether they could detect whether the devices are on the same user. Overall, we observed that (results in Table V) the accuracy drops sightly as compared to when using the data from the three devices. The drop in accuracy, however, is minimal (0.85 to 0.84) for the Polar H10 and the Samsung Watch 4 pair. One should note here that the Polar H10 is ECG-based, while the Samsung Watch 4 is PPG-based. Even with the different techniques, the performance is high. Surprisingly, the performance of the PPG-PPG pair is almost 10% lower. Overall, this indicates that the performance of WhoAmIOn improves when multiple devices are available.

VIII. Discussion and Future Work

Heart rate from various on-body locations: In this study, we considered capturing heart rate at the chest (ECG) and the wrist (PPG). We noted that the WhoAmIOn system provides reasonable performance even with ECG and PPG signals. One challenge with body-generated signals is that they can get attenuated as they travel across the body. We will experiment with data from other body parts to evaluate WhoAmIOn.

User Authentication: WhoAmIOn currently does not authenticate the devices' user. In future, we will introduce approaches

to authenticate the user. This will allow knowing which device is on the genuine user. There are several techniques for authentication purposes, the simplest one requiring the user to log into one device using a password or PIN, and we continue observing physical changes after the user authenticates.

Real-time processing: The current implementation of WhoAmIOn uses data from various devices, and determines whether the same users wore all the devices at the same time in an offline mode. Recent advances in machine learning for tiny embedded devices makes it possible to deploy machine learning models on low-powered embedded devices [Singh et al.(2023)]. In future, we will deploy the correlation mechanism on the wearable devices.

IX. Conclusion

In this paper, we present WhoAmIOn, a technique to determine whether the devices of the owner are on the same body. We evaluated WhoAmIOn on two datasets, one publicly available dataset and another dataset that we collected in a controlled setting. We experimented with both inertial sensors and heart rate sensors. Overall, we observed that WhoAmIOn could determine whether all devices were on the same body with an accuracy of 85% on the MultiDevice Dataset when we considered the heart rate sensor data and 84% when we considered the inertial sensor data from the Extrasensory Dataset. This demonstrates that WhoAmIOn can be used as an unobtrusive technique for detecting whether all the devices of the user are worn or carried by the same person.

Acknowledgment

This work is supported partly by the SURE grant (SUR/2022/002735) of SERB (Science and Engineering Research Board) of the Department of Science & Technology (DST), Government of India, and partly by BITS Pilani's CDRF grant (C1/23/173). All findings and recommendations are those of the authors and do not necessarily reflect the views of the funding institutes.

References

[Apple(2024)] Apple. 2024. Apple Vision Pro. https://www.apple.com/apple-vision-pro/. Accessed: 2024-07-13.

[Castaneda et al.(2018)] Denisse Castaneda et al. 2018. A review on wearable PPG sensors and their potential future applications in health care. *International journal of biosensors & bioelectronics* 4, 4 (2018), 195.

[Coskun et al.(2015)] Doruk Coskun et al. 2015. Phone position/placement detection using accelerometer: Impact on activity recognition. In *International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*. 1–6.

[Garmin(2024)] Garmin. 2024. Garmin Vivosmart 4. https://www.garmin.co.in/products/wearables/vivosmart-4-black-large/. Accessed: 2024-07-13.

[Gromert and Alnasser(2022)] L Gromert and M Alnasser. 2022. Heart Rate Measurement using a 60 GHz Pulsed Coherent Radar Sensor. (2022).

[Gupta et al.(2020)] Abhay Gupta et al. 2020. A survey on human activity recognition and classification. In *International conference on communication and signal processing (ICCSP)*. IEEE, 0915–0919.

[Lu et al.(2010)] Hong Lu et al. 2010. The jigsaw continuous sensing engine for mobile phone applications. In *8th ACM conference on embedded networked sensor systems*. 71–84.

[Mamish et al.(2024)] John Mamish et al. 2024. NIR-sighted: A Programmable Streaming Architecture for Low-Energy Human-Centric Vision Applications. *ACM Trans. Embed. Comput. Syst.* 23, 6, Article 101 (Sept. 2024), 26 pages. https://doi.org/10.1145/3672076

[Mare et al.(2014)] Shrirang Mare, Andrés Molina Markham, Cory Cornelius, Ronald Peterson, and David Kotz. 2014. Zebra: Zero-effort bilateral recurring authentication. In *2014 IEEE Symposium on Security and Privacy*. IEEE, 705–720.

[Mare et al.(2018)] Shrirang Mare, Reza Rawassizadeh, Ronald Peterson, and David Kotz. 2018. SAW: Wristband-based Authentication for Desktop Computers. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 3, Article 125 (sep 2018), 29 pages. https://doi.org/10.1145/3264935

[Mayrhofer and Gellersen(2007)] Rene Mayrhofer and Hans Gellersen. 2007. Shake Well Before Use: Authentication Based on Accelerometer Data. In *Pervasive Computing*. Springer.

[Meier and Holz(2023)] Manuel Meier and Christian Holz. 2023. BMAR: Barometric and Motion-Based Alignment and Refinement for Offline Signal Synchronization across Devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 7, 2, Article 69 (jun 2023), 21 pages.

[Mishra et al.(2020)] Varun Mishra et al. 2020. Continuous detection of physiological stress with commodity hardware. *ACM transactions on computing for healthcare* 1, 2 (2020), 1–30.

[Movsense(2024)] Movsense. 2024. Movsense. https://www.movesense.com/products/. Accessed: 2024-07-13.

[Ngo et al.(2014)] Thanh Trung Ngo, Yasushi Makihara, Hajime Nagahara, Yasuhiro Mukaigawa, and Yasushi Yagi. 2014. The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication. *Pattern Recognition* 47, 1 (2014), 228–237.

[Pinge et al.(2022)] Anuja Pinge, Soumyadip Bandyopadhyay, Surjya Ghosh, and Sougata Sen. 2022. A comparative study between ECG-based and PPG-based heart rate monitors for stress detection. In *International Conference on COMmunication Systems & NETworkS*. IEEE, 84–89.

[Plass et al.(2010)] Jan L Plass, Roxana Moreno, and Roland Brünken. 2010. Cognitive load theory. (2010).

[Polar(2024)] Polar. 2024. H10 Heart Rate Monitor. https://www.polar.com/en/sensors/h10-heart-rate-sensor. Accessed: 2024-07-13.

[Rahman et al.(2018)] Khandaker Abir Rahman, Dustyn J. Tubbs, and Md Shafaeat Hossain. 2018. Movement Pattern Based Authentication for Smart Mobile Devices. In *IEEE International Conference on Machine Learning and Applications (ICMLA)*. 1054–1058.

[Roy et al.(2015)] Nirupam Roy, Mahanth Gowda, and Romit Roy Choudhury. 2015. Ripple: Communicating through Physical Vibration. In *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*. USENIX Association, Oakland, CA, 265–278.

[Samsung(2024)] Samsung. 2024. Samsung Watch 4. https://www.samsung.com/in/watches/galaxy-watch/. Accessed: 2024-07-13.

[Sen and Kotz(2021)] Sougata Sen and David Kotz. 2021. VibeRing: Using vibrations from a smart ring as an out-of-band channel for sharing secret keys. *Pervasive and Mobile Computing* 78 (2021), 101505.

[Singh et al.(2023)] H. M. Singh, S. Agashe, S. Jain, S. Ghosh, A. Challa, S. Danda, and S. Sen. 2023. (POSTER) Insights from Executing TinyML Models on Smartphones and Microcontrollers. In *International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*. IEEE Computer Society, 89–92. https://doi.org/10.1109/DCOSS-IoT58021.2023.00026

[Sörnmo and Laguna(2006)] Leif Sörnmo and Pablo Laguna. 2006. Electrocardiogram (ECG) signal processing. *Wiley encyclopedia of biomedical engineering* (2006).

[Thomaz et al.(2013)] Edison Thomaz et al. 2013. Feasibility of identifying eating moments from first-person images leveraging human computation. In *International SenseCam & Pervasive Imaging Conference*. 26–33.

[Vaizman et al.(2017)] Yonatan Vaizman, Katherine Ellis, and Gert Lanckriet. 2017. Recognizing Detailed Human Context in the Wild from Smartphones and Smartwatches. *IEEE Pervasive Computing* 16, 4 (2017), 62–74. https://doi.org/10.1109/MPRV.2017.3971131

[Wang et al.(2016)] Wei Wang, Lin Yang, and Qian Zhang. 2016. Touch-and-Guard: Secure Pairing through Hand Resonance. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Heidelberg, Germany) *(UbiComp '16)*. 670–681.

[Zeni et al.(2014)] Mattia Zeni, Ilya Zaihrayeu, and Fausto Giunchiglia. 2014. Multi-device activity logging. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication* (Seattle, Washington) *(UbiComp '14 Adjunct)*. 299–302.

[Zhao et al.(2020)] Tianming Zhao, Yan Wang, Jian Liu, Yingying Chen, Jerry Cheng, and Jiadi Yu. 2020. Trueheart: Continuous authentication on wrist-worn wearables using ppg-based biometrics. In *IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 30–39.