WearIA: Wearable Device Implicit Authentication based on Activity Information

Yunze Zeng, Amit Pande, Jindan Zhu, Prasant Mohapatra
Department of Computer Science, University of California, Davis, CA, USA
{zeng, pande, jdzhu, pmohapatra}@ucdavis.edu

***Abstract*—Privacy and authenticity of data pushed by or into wearable devices are of important concerns. Wearable devices equipped with various sensors can capture user's activity in fine-grained level. In this work, we investigate the possibility of using user's activity information to develop an implicit authentication approach for wearable devices. We design and implement a framework that does continuous and implicit authentication based on ambulatory activities performed by the user. The system is validated using data collected from 30 participants with wearable devices worn across various regions of the body. The evaluation results show that the proposed approach can achieve as high as 97% accuracy rate with less than 1% false positive rate to authenticate a user using a single wearable device. And the accuracy rate can go up to 99.6% when we use the fusion of multiple wearable devices.**

I. Introduction

Recent hardware advances have led to the development and consumerization of wearable computing devices ranging from exercise and sleep tracking bracelets [3], vital signs (e.g. heart rate and blood pressure) monitoring devices [1] to augmented reality glasses [2]. Building on top of these wearable devices, many personalized applications have been developed for providing easy-to-use service and convenient user experience. These new technologies open enormously vast opportunities in sensing user context and monitoring health status, as well as providing plethora of new services. While enabling a spectrum of new applications, they also introduce unexplored paradigms in security and privacy.

Wearable devices can create new forms of interactions between humans and machines. Users' physical environment and context can be efficiently sensed by wearable devices. The ECG, heart-rate, ultraviolet, infrared, accelerometer and many other type of sensors can sense context and record data for an individual, which can be used to understand human activity [15], energy expenditure [21], personal health monitoring [24], etc. Wearable devices equipped with these sensors can sense, collect and upload personal health and activity related information (e.g. heart rate and steps) to the Electric Health Record(EHR)/cloud for further record and analysis. Meanwhile, wearable devices can also be used to create new types of immersive human-machine interactions with products such as smartwatch or smartglass. These interactions can be used for the applications of smart home and office. Moreover, different personal notifications, such as emails, text messages and reminders can be pushed to wearable devices

978-1-5386-2723-5/17/$31.00

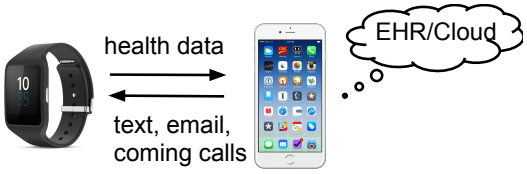


Fig. 1. Wearable devices application scenarios

through the smartphones or directly from the cloud though WiFi connection for convenient viewing. Personal notifications often contain a brief viewing of the message content. Such notifications are highly private and people usually do not want others to see these contents. Figure 1 shows us the roles of wearable devices in our daily life using an example of smartwatch. Here we name the first case of service (sensing context) that a wearable can provide us as *upload* service and the second case (notifications) as *download* service.

Almost all the smart functions available on mobile/wearable devices require user authentication as the first step. Usually, smartphone like devices use traditional explicit authentication methods, such as inputting PIN code or graphic pattern and using fingerprint. However, such ways can not be easily used on wearable devices due to the small form factor or lack of screens. Wearable devices have limited input method and feedback modality, which make it even harder to use traditional authentication methods designed for smartphone. Moreover, PIN code-based ways are not user-friendly and sometimes not fully secure. Due to aforementioned reasons, current wearable devices only rely on the BLE (Bluetooth Low Energy) pairing process to authenticate a user. However, the paring process only requires password for the first time and the device will automatically be paired for the rest of times without checking the user's identity. Such one-time authentication manner cannot ensure that there is no mishap or misbonding between the device and the user. An implicit and continuous authentication service is needed, which will allow the user to save the intervention required in the pairing process as well as ensure that there is no mishap or misbonding in the rest time of usage.

For both *upload* and *download* services, security and privacy concerns are important to be ensured. It is commonplace to imagine a child, spouse or friend wearing a user's wearable device for some short time period. Family members sharing the same medical wearable device, such as non-invasive glucose monitoring device, is also common to happen. Ideally, such

wearable device must be able to automatically recognize the person wearing it and provide services catered to her. This is applicable to both *upload* and *download* services. For example, it is necessary to make sure that the pushed notifications are not *downloaded* when the actual person wearing the device is not the owner. Similarly, the vital signs collected by the wearable may be integrated to her EHR and such data should be *uploaded* corresponding to the right user.

It is pertinent to secure such wearable devices using an implicit and continuous authentication way, which provides the ability to authenticate users based on actions they would carry out anyway. Such authentication framework provides a delicate balance between usability and security by implicitly verifying the genuineness of the user using the device without any explicit PIN or password requests but only using the user's patterns of activity. Similar ideas has been proved in smartphones using feature-tuned application centric [12] and touch-based [9] approaches. We argue that wearable devices will benefit more through such implicit authentication approach. However, there are unique challenges for designing such approach on wearable platforms. For instance, there are limited patterns and computing resources we can leverage. Moreover, we need to focus on the user-friendly and effortless design for wearable applications. These and many other challenges will be discussed and addressed in our work. Some of the main requirements of this framework are: *passive and continuous* monitoring of the user (and data), *accurate* authentication and low outliers, *user-friendliness* and minimum burden to users and *energy-efficiency* (low computational cost).

Inertial sensors, such as accelerometer and gyroscope, are becoming essential parts of various mobile and wearable platforms. Usually, these sensors have high sampling rate capability with low cost to capture users' activities [19]. Google Fit and Apple HealthKit are recently released for easy accessing to these sensor information on Android and IOS platforms respectively for developers. Among all the existing apps, the major functions by using these sensors are heath related, such as physical activities prediction, and anomaly detection and diagnosis [5].

In this paper, we investigate the possibility of using ambulatory activities as unique markers of the user to design an implicit authentication method. Here, we present WearIA, a **Wear**able device **I**mplicit **A**uthentication framework. WearIA is based on the unique patterns derived from wearable sensors when the user is performing different activities. We design and implement a framework of collecting and processing the information from inertial sensors on the wearable platform to authenticate the user implicitly and continuously. We evaluate our proposed framework using real world data and experiment. We asked 30 users to perform common ambulatory activities (e.g. walking, running) and conducted measurements using inertial sensors from wearable devices on different body parts of the users to verify the accuracy of our proposed approach. The main contributions of this work are as follows:

1) We investigate the problem of implicitly authenticating a user on wearable devices. We design and implement an implicit authentication framework for wearable devices based on the user's activity information available from inertial sensors.
2) We demonstrate that we can increase the authentication accuracy by predicting the activity type, knowing the device placement and fusion of multiple on body sensors. We quantify the impact and performance improvement for each of above steps.
3) We collected a dataset which involves 30 participants with 5 wearable devices in different on body locations. We conducted extensive evaluation for our system using the dataset. We also implemented our system on a real wearable platform.

The rest of the paper is summarized as follows: Section II provides an overview about related work. We discuss the detailed system design components in Section III. In Section IV, we talk about experiment setup and data collection. We then evaluate the performance of our system in Section V. Section VI discusses the further works and conclusions.

II. Related Work

There has been recent interest in implicit authentication (IA) in smartphones. Shi et al. [23] models user's recent behavior using a Gaussian Mixture Model to identify current active user of mobile phone. Implicit authentication is obtained using keystroke dynamics and typing patterns, geo-location, file system activity and network access [26], proximity information and touch-sensitivity and pressure applied while touching smartphone [9], [18]. De Luca et al. [9] use dynamic time warping on user's touch pressure sensitivity to improve performance of pattern-based phone unlocks. TIPS [11] extends the use of touch screen to ubiquitiously monitor and implicitly authenticate smartphone user. ITUS [12] framework supports different behavioral classifiers but it is focused on Android OS for smartphones. ZEBRA [17] framework involves smartwatch sensors for IA but uses smartwatch to authenticate the user's inputs on a smartphone. A good study of different IA schemes is provided by [13]. However, these work are limited to smartphone, and not considering the case for wearable devices. Moreover, Khan et al. [14] shows that current touch input based IA solutions suffer from shoulder surfing and offline training attacks. Recent work has been proposed to use different methods of IA for smart glasses [7], [16], [20], [27] and IoT devices [22]. However, these solutions cannot be generalized for wearable devices with different body placements.

Some work have been done in gait-based user authentication using wearable devices and other type of sensing media (e.g. RF signals) [10], [28]. However, such authentication is based on gait-detection, and restricted to walking. Gait detection involves finding gait cycle and matching gait properties among users. But the attacker can be trained to impersonate other person's gait. Our work considers generic activity-based IA, which is more robust and practical. Moreover, we also elaborate the impact of sensor placement and generalization of different activities to IA.

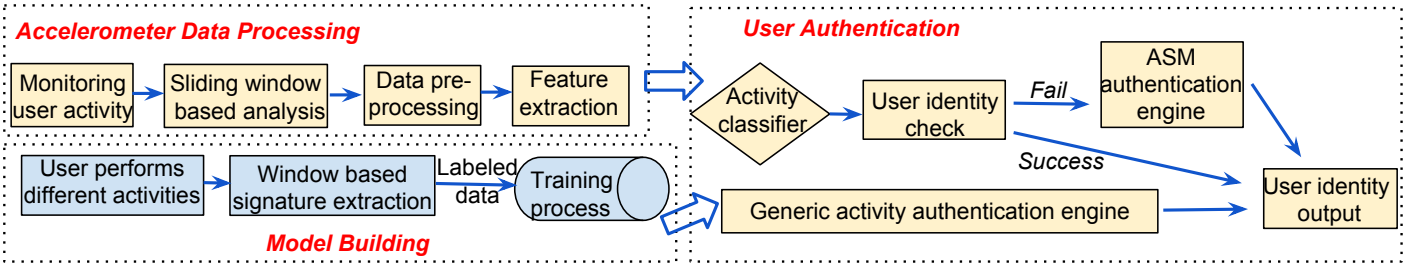


Fig. 2. Overview of WearIA

III. Design

In this section, we first discuss motivation and application scenarios of continuous and implicit authentication for wearable devices. Then, we present the design goals and an overview of WearIA. We also describe each component in detail.

A. Motivation: User Scenarios

Different kinds of wearable devices are being equipped on people for fitness tracking and convenient message viewing and human-computer interaction. Typically, a wearable device will be paired with a gateway device (e.g. smartphone) to provide its full functionality. Here, we use smartwatch as an example to illustrate the usage scenarios of various wearable devices. Before the first time of use, the user needs to perform pairing process for a smartwatch. To start paring, the user needs to enable Bluetooth for both devices and make sure they are in transmission range. Usually, the pairing needs a code or pattern generated from the smartwatch and the smartphone will use the code or pattern to identify the smartwatch to pair with. The pairing will only happen once and the smartwatch will automatically be paired with the smartphone in its vicinity for the rest of times. We call such authentication as one time authentication.

The information exchanged between smartwatch and smartphone include sensor data collected by the smartwatch and notifications and message briefings generated by the smartphone. Although such wearable devices are designed mainly for one user, there are certain circumstances that the devices are used by other users for a short period of time. One time authentication manner cannot guarantee the sensor data are from the intended user. Moreover, it cannot make sure that the notifications and message briefings are viewed by the intended user. In this way, a continuous and implicit authentication is needed to protect data on wearable devices. Such authentication can benefit in the following three ways.

1) User A uses a smartwatch to record and track his daily activity. User B borrows the device for two hours to measure her energy expenditure. Continuous and implicit authentication will automatically detect that this two hours data is not from user A and prevent it to be uploaded to user A's health profile.
2) User A has a smartwatch and use it to receive notifications. Some of the notifications contain private information. User B wears it occasionally. Continuous and implicit authentication can know when the device is not worn by user A and stop sending notifications to the device.
3) User A owns a smartwatch which is paired with her smartphone. Continuous and implicit authentication process on the smartwatch can constantly verify the wearer's identity. Applications (e.g. bank APPs) on her smartphone can leverage the proximity of the smartwatch to enable a convenient two-factor authentication. In this way, smartwatch can help her better secure the smartphone applications.

B. Design Goals

To design a system which can provide continuous and implicit authentication for wearable devices, we need to consider both practicability and applicability of the proposed system. Based on the identified challenges for wearable devices, the proposed authentication framework should meet the following design goals:

1) **Implicity and continuity:** Different from the existing one-time authentication approach, the main purpose of our system is to continuously authenticate the users without explicitly asking users to provide any information. We should build the framework to implicitly collect available information from wearable devices and use that to design the authentication engine.
2) **Effortlessness and user-friendliness:** The system should not require the user to perform additional actions in order to make the authentication process as effortless as possible. It is expected that the user wear the device and use it naturally. No proactive interaction from the user will be necessary to get identified.
3) **Low computational cost:** We are targeting different wearable platforms with limited battery and computing resources. The solution should be low cost. Such low cost solution comes form two folds. The sampling rate required for the data collection should be as low as possible and the authentication algorithms should involve only low computational calculation.

C. System Overview

Our central idea in this work is to design a user activity-based authentication framework for wearable devices. In order

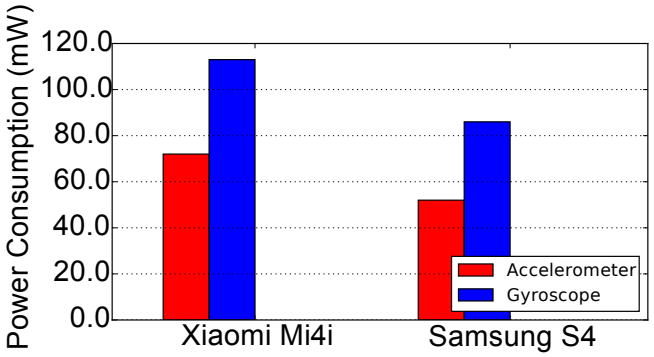


Fig. 3. Power consumption comparision between accelerometer and gyroscope

to meet the above design goals, we propose WearIA, a system design which can be applied on wearable platforms to conduct continuous and implicit authentication. Figure 2 shows the outline diagram of WearIA. WearIA requires a separate training phase which can be conducted when the user uses her wearable device for the first time. The user just needs to perform certain activities to train the model. Our training phase is conducted offline. We then constantly monitor and collect user's activity data (e.g. accelerometer) from the wearable device. We divide the time series data into small window chunks and pre-process the data in each window to remove the noise, where we apply a low pass filter with a cutoff frequency at 20Hz [25] to remove the high frequency noise caused by the vibration which cannot infer any activity status. Note that we use low pass/band pass filters with different cutoff frequencies for feature calculation, but for the pre-processing, we use the fixed 20Hz cutoff threshold. After the data pre-processing, we extract a number of activity features from each window and select the significant features for authentication. We evaluate two approaches for the user authentication module. Both approaches need separate training phases conducted offline to generate the authentication models. One simple and naive approach is to directly run a generic authentication engine without predicting the user's activity type. The other approach is to first classify user's activity type and then check if it is the default user(e.g. the owner of the device or the most recent user) by running a binary classification model. If it is not the default user, a pre-trained Activity Specific Model (ASM) will be used based on the activity type to predict the user's identity and further authenticate the user.

D. Wearable Sensor Selection

Current wearable devices have been equipped with many sensors including accelerometer, gyroscope, heart rate and ambient light sensors. WearIA is based on activity information observed from wearable devices. User's activity information can be directly captured by accelerometer and gyroscope sensors. Heart rate sensor can also capture the activity indirectly, however it cannot provide us fine-grained level of activity information. Both accelerometer and gyroscope are widely used for understanding and classifying user's different activities. Due to the design differences, the power consumption of these two sensors are quite different. From our measurement, we found that gyroscope consumes much more power than accelerometer at the same sampling rate. Figure 3 shows us the power consumption of accelerometer and gyroscope for two smartphones at 200Hz sampling rate. We can see that gyroscope consumes 20mW to 30mW more power. In order to meet the low cost desigh goal, we choose to use accelerometer for WearIA.

TABLE I
SELECTED TIME DOMAIN FEATURES FOR ACTIVITY EXTRACTION

Features for individual axis
- Mean, Minimum, Maximum, Median, Absolute Mean - Variance, Standard Deviation, DC Mean - DC Area: The area under the signal after a low-pass filter(1Hz). $$DCArea = \sum_{i=1}^{window\_size} acceleration_i \quad (1)$$ - 90th percentile, 10th percentile, Signal Range - Cumulative sum over absolute signal value(AbsACArea) - Zero crossing rate, Mean crossing rate, Auto correlation - Pitch: The magnitude of the second peak of auto-correlation function. - Skewness (3rd moment): Measuring the asymmetry of the signal. - Kurtosis (4th moment): Measuring the peakedness of the signal. - Quartiles (first, second and third), Inter quartile range - Coefficient of variation over absolute value of signal
Features across 3 axis
- Total DC Mean across X, Y and Z axis - Total area under the absolute signals values across X, Y and Z - Total signal vector magnitude across X, Y and Z axis - DC Posture Dist: The difference value between means of X-Y, X-Z and Y-Z after a low-pass filter(1Hz). - Correlation across X, Y and Z axis

TABLE II
SELECTED FREQUENCY DOMAIN FEATURES FOR ACTIVITY EXTRACTION

Features for individual axis
- Normalized-Entropy: Measuring the disorder of the signal in frequency domain(V_i is the normalized FFT coefficients). $$H = -\sum_{i=1}^{window\_size/2} V_i \cdot \log_2(V_i) \quad (2)$$ - Normalized-Energy: Measuring the sum of energy without DC component in frequency domain(V_i is the normalized FFT coefficients). $$E = \sum_{i=1}^{window\_size/2} V_i^2 \quad (3)$$ - FFT Peaks, Ratio of energy in dominant frequency - AC Band Energy: Normalized activity band energy(0.2-3.5Hz). - AC Low Energy: Normalized energy of low intensity physical activity(0-0.7Hz). - AC Mod Vig Energy: Normalized energy of moderate to vigorous physical activity(0.71-10Hz).

E. Feature Extraction and Selection

We extract a number of time and frequency domain features from each window (all three axis of each accelerometer). A total of 102 features are extracted which are summarized in

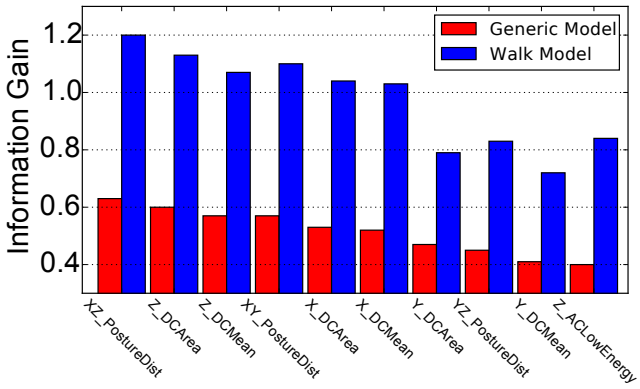


Fig. 4. Information Gain for selected features

Table I and II. A detailed description of these features is given in [25].

From all the candidate features shown in Table I, we further select a subset of most useful features for the authentication purpose. To determine how well a given feature can be used to identify the user, we use Information Gain (IG) to evaluate and selection the feature set. IG was calculated using GainRatio criterion. It is equal to the total entropy for an attribute if for each of the attribute values a unique classification can be made for the result attribute. In this case, the relative entropy subtracted from the total entropy is 0. Let FV denote a feature vector.

$$\text{GainRatio}(C, FV) = (H(C) - H(C|FV))/H(FV) \quad (4)$$

where C is the set of all training examples, and $H()$ denotes entropy. The missing merge scheme is used to distribute counts for missing values. Counts are distributed across other values in proportion to their frequency. Otherwise, the missing is treated as a separate value.

Figure 4 shows the ten features with highest IG values. Here the top ten features are the same for generic as well as walking data (as well as running data). Next, we use a feature selection algorithm to find the independent features which can give high predictive power. Feature selection aims at reducing the number of attributes to be used in the model, while trying to retain the predictive power of the original set of attributes in the pre-processed data. We use the Correlation Feature Selection (CFS) strategy to identify a subset of attributes which were highly correlated with the outcome variable while having low inter-correlation among themselves. The CFS technique was used in conjunction with a greedy step wise search to find the subset S with the best average merit, which is given by:

$$Merit_s = \frac{n\overline{r_{fo}}}{\sqrt{n + n(n-1)\overline{r_{ff}}}} \quad (5)$$

where n is the number of features in S,$\overline{r_{fo}}$ is the average value of feature- outcome correlations, and $\overline{r_{ff}}$ is the average value of all feature-feature correlations.

TABLE III
SENSOR PLACEMENT

Placement	Sensor Node
Wrist (left)	Shimmer 6DoF IMU
Ankle (right)	Shimmer 6DoF IMU
Hip/Torso (center right)	Samsung Galaxy S4 i9500
Thigh/Front Pocket (left)	Samsung Galaxy Nexus i9250
Upper Arm (right)	Samsung Galaxy Nexus i9250

TABLE IV
USER INFO. (MEAN±STDEV (MIN/MAX))

Number of Subjects	30 (20 males & 10 females)
Age(year)	$27.8 \pm 6.9(19/45)$
Height(cm)	$168.9 \pm 10.8(150/189)$
Weight(kg)	$66.9 \pm 15.1(48/105)$
BMI ($\mathbf{kg/m^2}$)	$22.7 \pm 3.4(18/30)$

TABLE V
ACTIVITY SEQUENCE

Timed	Activity (Part1)	Timed	Activity (Part2)
0	Jumping	0	Walking
1	Walking	1	Standing
2	Turning/Walking	2	Sitting
3	U-Turn/Walking	3	Standing
4	Turning/Walking	4	Walking
11	Walking (repeat)	5	Elevator (up)
12	...	6	Elevator (down)
13	Stairs climbing(up)	7	Walking
14	Stairs climbing(down)	9	Running

F. Authentication Classifier

We use sliding window based method to buffer the sensor data and calculate features. The feature calculation and model checking need to be performed periodically. Because our target platform for the authentication classifier is a wearable device which has limited computational resource and small capacity battery, we would like to choose a light-weight and energy efficient classifier. For the authentication engines, we use Random Forest [6] which is a decision-tree based classifier and only needs implement simple if-else conditions to do the classification. Our system requires separate training phases for both generic and ASM authentication engines. To train the models, we ask the user to perform a set of pre-defined activities and label the data for training. Note that our model building is conducted in the cloud which does not consume any resource from wearable devices. To evaluate the performance, we divide the overall data for the model into n = 10 folds, where, n-1 folds are for supervised learning and one fold is used to test the model for errors. The errors obtained in a fold are added to the weights of nodes of next fold in the training set. Such 10-fold cross validation was used to evaluate the model in order to ensure that the model was tested on data that it had not seen while training, to minimize chance for over-fitting. Considering the fact that most wearable devices are frequently used only by the owner (the default user) of the device, we design a user identity check module, where we use a binary classifier to first check if the current user is the owner. For the binary classification, we use Support Vector Machine (SVM) with the Radial Basis Function (RBF) kernel

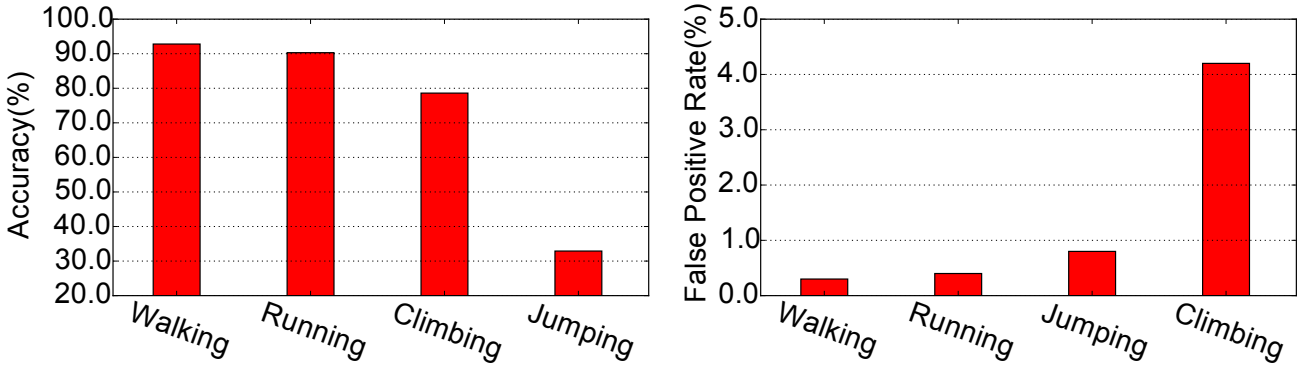


Fig. 5. The overall performance with ASMs

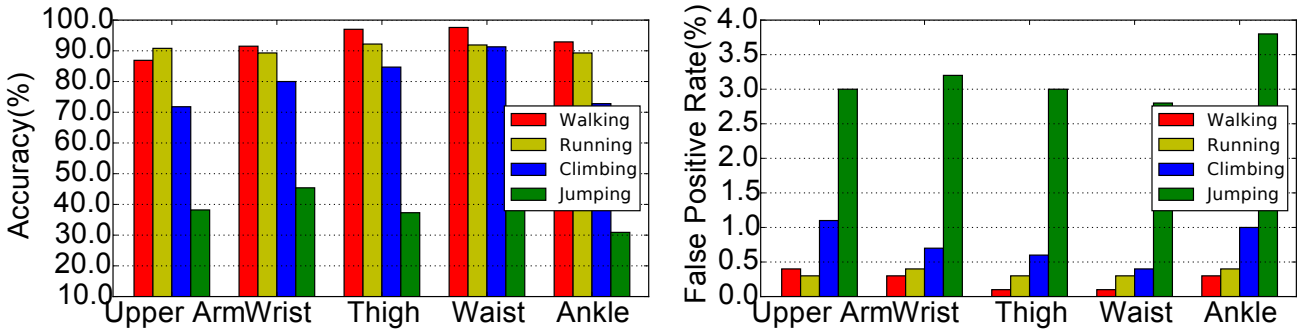


Fig. 6. Overall performance with known device placement

to perform the non liner separation. A similar 10-fold cross validation method is used for the evaluation.

IV. Experiment Setup

A. Implementation and Platform

A platform of 5 wearable sensors are used for the data collection and evaluation, including 2 wearable Shimmer IMU nodes and 3 smartphones. Nodes are attached to different body parts as described in Table III, and continuously collect accelerometer samples at a fixed frequency of 50Hz. All devices are time synchronized before collection. During the collection, Shimmer units stream real-time sensing data to controlling smartphone via a Bluetooth connection, while smartphones will store all data locally for later processing. We also implemented our system on a Shimmer device with a Android smartphone to demonstrate the real-time authentication based on the user's activities.

B. Subjects

We recruited a total of 30 participants (10 females and 20 males) for the study. All participants are physically fit for performing typical ambulatory activities of a normal person, as described below. Physical characteristics of all participants are summarized in Table IV. The study is approved by Institutional Review Board (IRB) at our university. Participants are recruited from the university campus and the medical center, and all have given oral consent prior to the experiment in accord with IRB regulation.

C. Data Collection Protocol

We designed a semi-controlled protocol for the data collection. Participants were asked to perform a sequence of pre-defined types of ambulatory activities, following specified routes. However, the environment where the collection is conducted is inside a regular office building and the courtyard outside, with moderate traffic. The activity sequence is broken into two parts, as described in Table V, designed to emulate ordinary behavior of a person in such environment. The participants are asked to perform the activities as natural as possible, and no rest between activities in each part. Completion of the whole sequence will take each participant approximately 30 minutes. A supervisor accompanying the participant will manually time the instance when an activity transition happens. Annotation of the activities is performed offline. Data from all participants was combined to create a dataset. Each person wore the same set of sensors and the experiment was carried in the lab over a couple of days.

V. Performance Evaluation

In this section, we evaluate our system using the real-world dataset we have collected from 30 users. Meanwhile, we summarize our findings in order to provide insights for developing better implicit authentication for wearable devices.

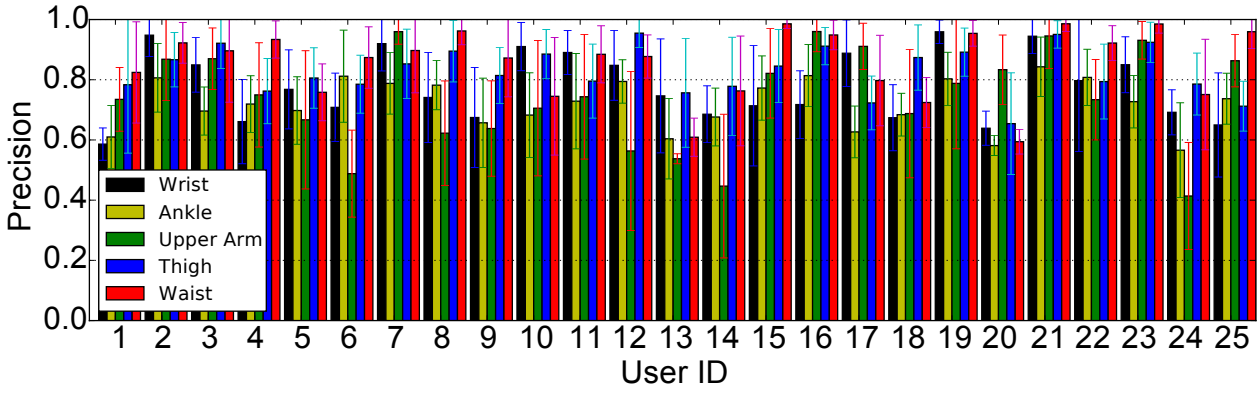


Fig. 7. The detailed precision comparison for 25 users

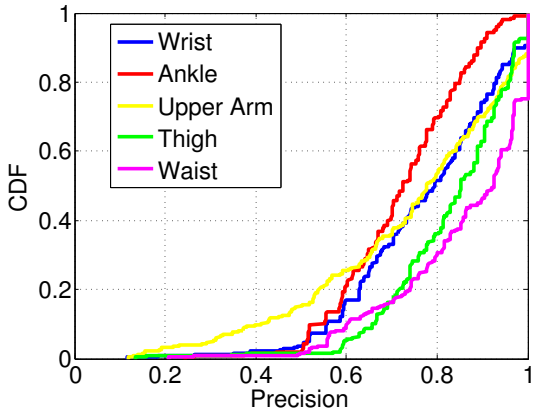


Fig. 8. CDF of authentication precision for user identity check module

A. Evaluation Metrics

To evaluate our system, we consider the following metrics.

1) True Positive (TP) rate (accuracy): TP rate is the fraction of instances of user A that are correctly identified as user A. The overall accuracy is the weighted average of TP rate of all the users.
2) False Positive (FP) rate: FP rate is the fraction of instances that are incorrectly identified as user A. The overall FP rate is the weighted average of FP rate of all the users.
3) Precision: It is defined as the number of true positives over the number of true positives plus the number of false positives.

B. Accuracy using Generic Model

We first consider the most robust case where we use a generic model without classifying the activities and the sensor placement on body is unknown. In this scenario, the user picks up a wearable device, puts it on any position (within five positions considered in this work) of the body and performs a certain activity. The accuracy to identify the user with a simple generic model is 80.9% and FP rate is less than 1%. The time window of 2 seconds is used in this setup to process sampled data. Note that using the generic model we do not identify activity types as the first step. 80.9% of TP rate shows us that WearIA can find the unique pattern existed in different activity types of the same user.

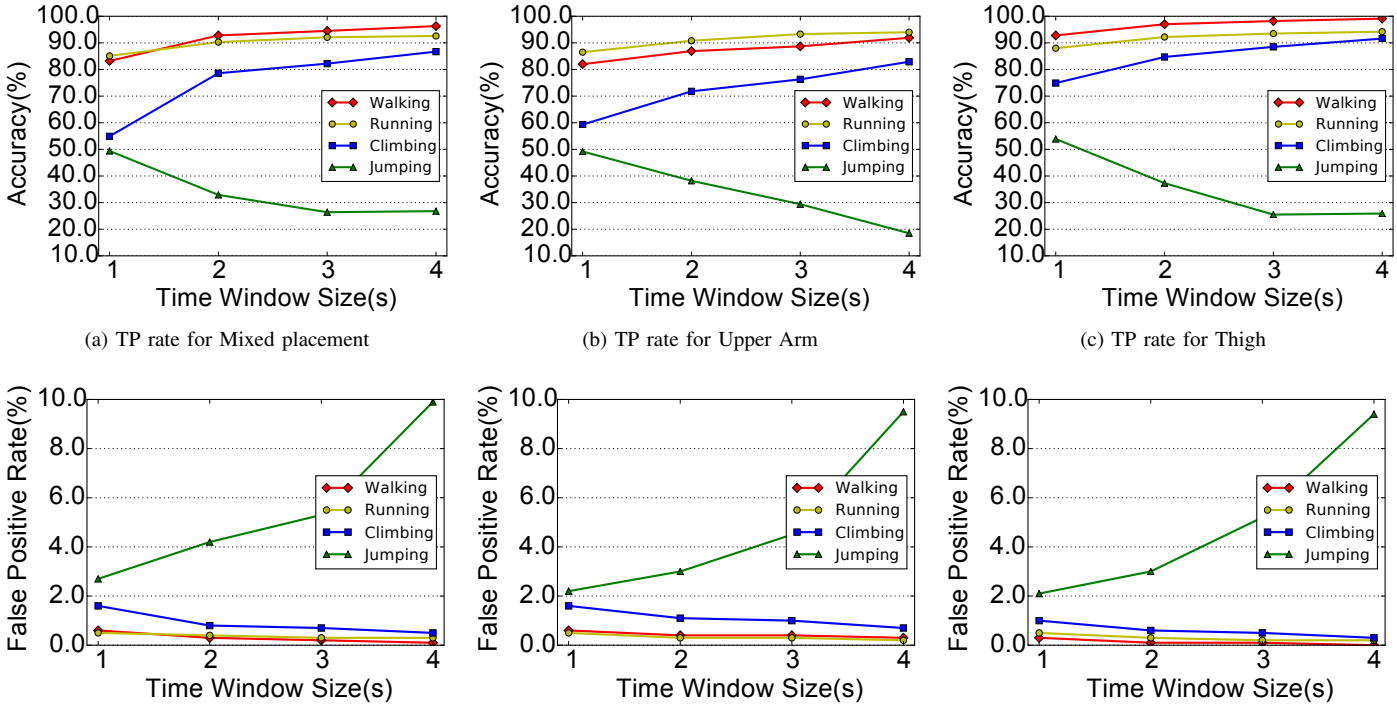
C. Improvements with Activity Specific Models (ASMs)

Next, we investigate whether it is possible to improve the authentication accuracy using ASMs. ASMs have been widely used to improve the Caloric energy expenditure estimation using mobile sensors [4], [8]. We consider that knowing the activity type will help to find the unique pattern for the user. Here, we use a two-step approach to conduct the authentication. For the same scenario (robust case), we train a custom classifier for each activity type and use activity-specific classifier to identify a user. We first apply an activity classifier (which is also a random forest based model) to classify user's activity. The activities we have considered are walking, running, climbing and jumping. The accuracy of activity classification is close to 95%. Then we apply a activity-specific authentication model (ASM) after detecting the user's activity. Figure 5 shows the performance for each activity model. Walking and running models can achieve 92.8% and 90.3% accuracy which improve the performance by 15% and 12%. We can see from Figure 5 that climbing model slightly performs worse than generic model and jumping activity cannot infer user's identity information. Walking and running are the most common activities in our daily life, hence it is reasonable to assume that we trigger the authentication process when we detect that the user is walking or running. Walking and running involves movements unique to the users, while jumping is an activity in free air. This may be the reason for low performance of jumping activity.

Summary: With a generic model, we have a fair accuracy rate for the user authentication. However, ASMs can significantly improve the accuracy.

D. Improvements using Device Placement

The placement of wearable devices is usually fixed. For example, we prefer to wear the smartwatch on our wrist and hang the Fitbit or smartphone around waist or pant pockets. So it is reasonable to assume that we know the device placement everytime when we want to authenticate the current user. Here



(a) TP rate for Mixed placement (b) TP rate for Upper Arm (c) TP rate for Thigh

(d) FP rate for Mixed placement (e) FP rate for Upper Arm (f) FP rate for Thigh

Fig. 9. The performance with different authentication window size for selected placement cases

TABLE VI
AVERAGE PRECISION OF SVM CLASSIFIER

	Wrist	Ankle	Upper Arm	Thigh	Waist
Precision	0.78	0.72	0.74	0.83	0.86

we use a similar approach to build separate classifiers for each activity type with different device placement. Figure 6 shows us the performance if we know the placement of the wearable device, for each activity. Note that we assume the users to provide the device placement information. We can always check whether the device is remaining on the target placement by simply applying a placement classification algorithm, since different placement will observe the same activity in different ways. From Figure 6, we can observe that putting the device on thigh or waist can achieve the highest accuracy (with more than 97%) while walking. The average accuracy we can achieve by applying a placement-specific model is 93.2% and 90.7% for walking and running respectively.

Summary: We need to build different models for different sensor placements in order to achieve a very high accuracy rate.

E. Performance of User Identity Check Module

The user identity check module runs a SVM binary classifier to check if current user is the default user. Since walking is the most common activity during our daily life, WearIA triggers the SVM binary classification once it detects a walking activity. The overall average precision for user identity checking is 0.78 based on walking activity. Table VI and Figure 8 shows us the average precision and CDF of all precision among 30 users for each device placement. We can see that placing the device on thigh or waist can achieve relatively better performance. However, through the analysis we found that different users have different authentication results. To understand the detailed precision for each individual user with different device placements, Figure 7 shows us the results of comparison for 25 users. The actual performance varies from user to user, but placing the device on waist can have the highest precision for most of users.

F. Changing Authentication Window Size

To allow real time implementation, we adopt a sliding window based approach to analyze the sensor data from wearable devices in real time. All the features are calculated based on samples collected in one time window. The window size determine how long the user needs to maintain in a certain activity before we can authenticate the user. In the other words, the window size determines how fast we can identify and authenticate a user. Figure 9 shows us the performance with different window sizes. Obviously, with a larger window size we can always get more activity data from the user and achieve a better accuracy. However, from Figure 9, we can see that using 2 seconds window size can give us more than 90% accuracy for most cases. Requiring a user to wear a device for only 2 seconds makes WearIA a practical system. The performance of jumping activity reduces for larger time window because jumping is usually accompanied by seconds of inactivity.

G. Improvements with Sensor Fusion

Here we consider an extreme case where a user carries five devices with different placement and we fuse the data from all five devices to authenticate the user. The accuracy rates of ASMs and generic model are all greater than 99%. In this way, some cloud services can identify a user with nearly 100% accuracy using multiple data sources from the user at the same time.

Summary: With fusion of multiple devices of a user, we can achieve nearly 100% *accuracy rate.*

VI. Discussion and Conclusions

This work is limited to the use of accelerometer sensor, however we would like to investigate the impact of fusing information from gyroscope as well as compass sensor in the next step. Heart rate sensor may also be used as an indicative of user activity and it would be interesting to see how that feed improves the accuracy of user authentication. In a real-world setting, the wearable shifts its placement in human body because of slips or re-adjustments by user which will introduce additional challenges. To guard against data-replay attacks, it is also possible to use strong mathematical models which are able to draw correlations between multiple sensor data.

In this paper, we design and implement WearIA which uses activity-sensing approach to implicitly authenticate users for wearable devices. The results are favorable and 97% accuracy was obtained in user identification using single sensor. Moreover, the accuracy was high even when we didn't know the exact location of the sensor, combine one or many sensors and without using ASMs. The decision trees based classifier and feature extraction are simple computations and easy to implement in existing wearable devices. The accuracy of 97% is high enough for tasks such as authentication for health records. It can be further improved by aggregating the results of classifiers over multiple consecutive time windows (we may require that the user to be recognized in two of the three consecutive time windows, which will increase the overall accuracy). This work has leveraged both binary and 1-out-of-N classification methods to authenticate users. Our system can be used in real-world to recognize and authenticate individual user and automatically detect $(N+1)^{th}$ user.

VII. Acknowledgments

We appreciate insightful comments from the anonymous reviewers. This work was supported in part by the NSF CRII 1464421 grant.

References

[1] "https://store.dexcom.com," [Online; accessed Dec. 2016].

[2] "https://www.oculus.com," [Online; accessed Dec. 2016].

[3] "http://www.fitbit.com/flex," [Online; accessed Dec. 2016].

[4] M. Altini, J. Penders, and O. Amft, "Energy expenditure estimation using wearable sensors: a new methodology for activity-specific models," in *Proceedings of ACM the conference on Wireless Health*, 2012.

[5] H. Banaee, M. U. Ahmed, and A. Loutfi, "Data mining for wearable sensors in health monitoring systems: a review of recent trends and challenges," *Sensors*, vol. 13, no. 12, pp. 17 472–17 500, 2013.

[6] L. Breiman, "Random forests," *Machine learning*, vol. 45, no. 1, pp. 5–32, 2001.

[7] J. Chauhan, H. J. Asghar, A. Mahanti, and M. A. Kaafar, "Gesture-based continuous authentication for wearable devices: The smart glasses use case," in *International Conference on Applied Cryptography and Network Security*. Springer, 2016, pp. 648–665.

[8] S. Chen, J. Lach, O. Amft, M. Altini, and J. Penders, "Unsupervised activity clustering to estimate energy expenditure with a single body sensor," in *IEEE International Conference on Body Sensor Networks*, 2013.

[9] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and i know it's you!: implicit authentication based on touch screen patterns," in *Proceedings of ACM CHI*, 2012.

[10] M. O. Derawi, "Accelerometer-based gait analysis, a survey," *Norsk informasjonssikkerhetskonferanse (NISK)*, 2010.

[11] T. Feng, J. Yang, Z. Yan, E. M. Tapia, and W. Shi, "Tips: Context-aware implicit user identification using touch screen in uncontrolled environments," in *Proceedings of ACM HotMobile*, 2014.

[12] H. Khan, A. Atwater, and U. Hengartner, "Itus: an authentication framework for android," in *Proceedings of ACM Mobicom*.

[13] ——, "A comparative evaluation of implicit authentication schemes," in *Research in Attacks, Intrusions and Defenses*. Springer, 2014, pp. 255–275.

[14] H. Khan, U. Hengartner, and D. Vogel, "Targeted mimicry attacks on touch input based implicit authentication schemes," in *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2016, pp. 387–398.

[15] O. D. Lara and M. A. Labrador, "A survey on human activity recognition using wearable sensors," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 3, pp. 1192–1209, 2013.

[16] S. Li, A. Ashok, Y. Zhang, C. Xu, J. Lindqvist, and M. Gruteser, "Whose move is it anyway? authenticating smart wearable devices using unique head movement patterns," in *Pervasive Computing and Communications (PerCom), 2016 IEEE International Conference on*. IEEE, 2016, pp. 1–9.

[17] S. Mare, A. M. Markham, C. Cornelius, R. Peterson, and D. Kotz, "Zebra: Zero-effort bilateral recurring authentication," in *IEEE Symposium on Security and Privacy (SP)*, 2014.

[18] S. Mondal and P. Bours, "Swipe gesture based continuous authentication for mobile devices," in *IEEE International Conference on Biometrics (ICB)*, 2015.

[19] A. Pande, Y. Zeng, A. K. Das, P. Mohapatra, S. Miyamoto, E. Seto, E. K. Henricson, and J. J. Han, "Energy expenditure estimation with smartphone body sensors," in *Proceedings of the 8th International Conference on Body Area Networks*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013, pp. 8–14.

[20] G. Peng, G. Zhou, D. T. Nguyen, X. Qi, Q. Yang, and S. Wang, "Continuous authentication with touch behavioral biometrics and voice on wearable glasses," *IEEE Transactions on Human-Machine Systems*, 2016.

[21] Á. Ruiz-Zafra, E. O. Gonzalez, M. Noguera, K. Benghazi, and J. M. H. Jiménez, "Energy expenditure analysis: A comparative research of based on mobile accelerometers," in *Ambient Assisted Living and Daily Activities*. Springer, 2014, pp. 38–45.

[22] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the internet of things," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2016 IEEE 17th International Symposium on A*. IEEE, 2016, pp. 1–3.

[23] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," in *Information Security*. Springer, 2011, pp. 99–113.

[24] J. Snoeck-Stroband, "Internet-based self-monitoring of physical activity (pa) in copd patients: a study of the usability of activity monitors and patients preferences," in *Medicine 2.0 Conference*. JMIR Publications Inc., Toronto, Canada, 2013.

[25] E. M. Tapia, "Using machine learning for real-time activity recognition and estimation of energy expenditure," Ph.D. dissertation, Citeseer, 2008.

[26] S. Yazji, X. Chen, R. P. Dick, and P. Scheuermann, "Implicit user re-authentication for mobile devices." in *UIC*. Springer, 2009.

[27] S. Yi, Z. Qin, E. Novak, Y. Yin, and Q. Li, "Glassgesture: Exploring head gesture interface of smart glasses," in *IEEE INFOCOM 2016*.

[28] Y. Zeng, P. H. Pathak, and P. Mohapatra, "Wiwho: wifi-based person identification in smart spaces," in *Proceedings of the 15th International Conference on Information Processing in Sensor Networks*. IEEE Press, 2016, p. 4.