Hand Dynamics for Behavioral User Authentication

***Abstract*—We propose and evaluate a method to authenticate individuals by their unique hand dynamics, based on measurements from wearable sensors. Our approach utilises individual characteristics of hand movement when opening a door. We implement a sensor-fusion machine learning algorithm to classify individuals based on their hand movement and conduct a lab study with 20 participants to test the feasibility of the concept in the context of accessing physical doors as found in office buildings. Our results show that our approach yields an accuracy of 92% in classifying an individual and thus highlights the potential for behavioral hand dynamics for authentication.**

I. Introduction

Passwords are still the most widely used approach to authenticate a user towards a system. As highlighted in the scientific literature, knowledge-based authentication methods have several shortcomings in both security and privacy [31], [23], [5]. On the one hand, users find it difficult to choose and remember complex and secure passwords. On the other hand, passwords may be lost, forgotten or stolen.

In security research, physiological biometrics relying on static physical attributes of an individual ('something you are'), such as face, iris or fingerprints have been proposed as alternative means of authentication. However, also these systems have been proven to be potentially infeasible and, besides their usability issues, are also considered as privacy invading as they often involve high-resolution cameras [26], [29]. Furthermore, leaked biometric information and misuse may have significant impact on the affected individual. If biometric information is compromised, it is also hard yet impossible to renew an account.

Behavioral biometrics ('something you do') are often considered as an alternative solution as they are based on the combination of a number of weak invariant feature that are strong in combination and hard to impersonate [14], [1]. So far, different activities such as walking or keystroke and touchscreen interaction have been proposed in the scientific literature.

To the best of our knowledge, we are the first to consider hand dynamics for authentication based on movement characteristics when opening a door. Our approach is solely based on sensor data from built-in sensors in wearable devices, such as smartwatches. The movement description is based on information obtained from sensors such as gyroscope, magnetometer and accelerometer. To classify individuals based on their movement characteristics, we propose a machine learning based approach, comprising of various statistical and physical features and Support Vector Machines (SVM).

In addition, we explore manufacturer-dependent and -independent characteristics of commercial sensors as used in smartphones and wearables. To evaluate our approach, we collected data from 20 participants that each opened a door 10 times. Our lab study shows that our solution allows to classify individuals with an accuracy of 92% based on their hand movement. Despite the tremendous advances in biometric technology, the recognition systems based on the measurement of single modality cannot guarantee 100% accuracy. In fact, these factors laid the foundation of the systems which use multiple independent evidences of biometric information from either single or different biometric modalities, very often termed as multi-modal biometric systems [30]. We consider our approach to be a reliable part of such a multi-modal system.

The remainder of the paper is organized as follows: Section II describes the sensors used for this paper in detail. Section III reports on state of the art methods for behavioral biometrics and available datasets based on information obtained from accelerometers, gyroscope and magnetometer sensors. Section IV details the method to obtain our dataset, and the characteristics thereof. Section V explains our authentication method. The experimental results revealing the efficacy of the method are described in Section VI. The paper concludes with discussions and future work in Section VII.

II. Sensors measurements

Today's smartphones are equipped with a variety of sensors: GPS, motion sensors, magnetometers, proximity sensors, microphones, cameras, and radio (cellular, Bluetooth, Wi-Fi, RFID, NFC) antennas. Moreover, sensors are still a fast growing segment of these devices. We therefore expect even more sensors to be part of future devices. According to The Wall Street Journal, Samsung will embed iris scanners into future mobile devices [20]; and Google will produce a 3D imaging tablet based on infrared sensors [21].
The rich set of built-in sensors enable a wide range of applications [19]. For instance, Michalevsky et al. [24] used an MEMS gyroscope as found in smartphones to extract speech. This highlights the rich capabilities of these sensors. In this paper, we use motion sensors and the magnetometer embedded in Google Nexus 4 smartphone to authenticate a user based on hand movement when opening a door. This smartphone first appeared on the market in November 2012. The key specification is given in Table I. In the following, we will describe the device's motion sensors (accelerometer

TABLE I
KEY SPECIFICATIONS OF GOOGLE NEXUS 4

Processor	Qualcomm $Snapdragon^{TM}$ S4 Pro CPU
Operating System	Android 4.2 (Jelly Bean)
Memory	2GB RAM, 16GB flash memory
Display	4.7" WXGA (1280x768)
Battery	2100mAh
Senors	GPS LGE Accelerometer Sensor LGE Gyroscope Sensor LGE Magnetometer Sensor LGE Proximity Sensor LGE Barometer Sensor LGE Light Sensor LGE Gravity Sensor LGE Linear Acceleration Sensor LGE Microphone

and gyroscope) and the magnetometer capabilities to measure movement data in detail.

A. Accelerometer, Gyroscope and Magnetometer

Our movement data is based on sensor data from an accelerometer, gyroscope and magnetometer embedded in Google Nexus 4.

The *accelerometer* sensor measures the amount of force applied on the smartphone trying to move it. For instance, when the smartphone is laying flat with its back on a table, the acceleration value of phone's Z axis should be the gravity force (9.81m/s^2) and the other two axes (X and Y) should be 0m/s^2.

The *gyroscope* sensor measures the rotation speed around X, Y and Z axis. For instance, when the smartphone is at rest, the gyroscope measurements should be 0°/s.

The *magnetometer* measures the ambient magnetic field force in the X, Y and Z axis. If there is not magnet or large metal object nearby, it indicates the magnetic field of the earth.

Android uses a standard 3-axis coordinate system to express values for the acceleration, gyroscope and the uncalibrated magnetometer (Figure 1). When the phone is held in an upright position with the screen facing the user, the Z axis points to the outside of the screen, the X axis is horizontal and points to the right, the Y axis is vertical and points up.

Table II shows the specifications of the accelerometer, gyroscope and magnetometer sensors of Google Nexus 4: the minimum delay allowed between two events in microsecond, the resolution of the sensor in the sensor's unit, and the maximum range of the sensor in the sensor's unit. Both the delay and the resolution are adequate to capture the movement of the hand with a sufficient detail and precision.

B. Empirical Sensor Data

To verify and augment the device characteristics given by the specification, we discuss in the following some of the findings presented by Ma et al.[22] in a performance

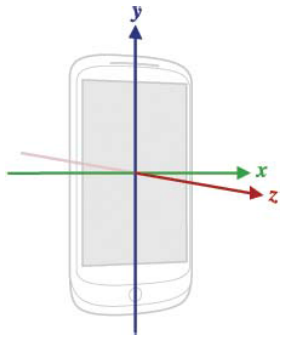

Fig. 1. Coordinate system (relative to a device).

TABLE II
SPECIFICATIONS OF THE ACCELEROMETER, GYROSCOPE AND MAGNETOMETER OF THE GOOGLE NEXUS 4

Sensor	Min. Delay(μs)	Resolution	Max. Range
LGE Accelerometer(m/s^2)	5000	0.0012	39.23
LGE Gyroscope(rad/s)	5000	0.0011	17.45
LGE Magnetometer(μT)	20000	0.1495	4912

TABLE III
GYROSCOPE AND ACCELEROMETER SAMPLING FREQUENCY

	Average	Max	Min	StdDev
Gyroscope (fast)	0.00503	0.00583	0.00424	0.000034
Gyroscope (normal)	0.201	0.202	0.201	0.000068
Accelerometer (fast)	0.00503	0.00536	0.00496	0.00001

evaluation of the accelerometer, gyroscope and orientation of the Google Nexus 4. In case the orientation is not provided by a real sensor, it is a software sensor that combines accelerometer and magnetometer measurements and hence provides orientation information.

Table III shows the maximum possible frequency of the gyroscope and accelerometer, indicating that there is relatively little variation in the sampling frequency. It further shows that the fastest sampling rate for the accelerometer and gyroscope sensors are 0.00496s and 0.00424s respectively, approximately equal to 0.005s of the specifications (Table II).

The sampling frequencies with the normal sampling rate are approximately 0.201s for both sensors, which is a quarter of the sampling frequency under faster rate. The variation reported for the gyroscope at medium sampling rate is similar to the fast sampling rate.

Table IV shows the stability of the accelerometer output.

Ma et al. [22] conclude: (1) the accelerometer and gyroscope sensor are very stable, (2) the derivation error of the digital compass is about 170 degrees under the faster rate, which shows that it is unstable and therefore unreliable under certain circumstances, (3) the standard deviation of the accelerometer under normal sampling rate (0.2s) is higher than

TABLE IV
ACCELEROMETER STABILITY MEASUREMENTS

		Average	Max	Min	Std Deviation
Fastest Sampling	X(m/s^2)	0.0697	0.1725	-0.0262	0.0274
	Y(m/s^2)	0.0187	0.1278	-0.0781	0.0253
	Z(m/s^2)	9.6603	9.8920	9.3742	0.0441
Normal Sampling	X(m/s^2)	0.0113	0.1142	-0.0548	0.0308
	Y(m/s^2)	-0.0634	-0.0031	-0.1269	0.0289
	Z(m/s^2)	9.7541	9.9015	9.5920	0.0524

TABLE V
ACCELEROMETER AT REST

ACCELEROMETER (SAMPLING 0.1S)				
Glove				
	Average	Max	Min	Std Deviation
X(m/s^2)	0.0041	0.0225	-0.0226	0.0106
Y(m/s^2)	-0.0018	0.0272	-0.0190	0.0125
Z(m/s^2)	10.2996	10.3281	10.2732	0.0100
Handle				
X(m/s^2)	0.0028	0.0229	-0.0080	0.0067
Y(m/s^2)	-0.0014	0.0160	-0.0228	0.0102
Z(m/s^2)	10.8233	10.8529	10.7900	0.0132

the standard deviation under fastest rate for each axis (cf. Table IV), and (4) the standard deviation of sampling frequency under normal rate is the double of the one under the fastest rate. We can thus expect to achieve sufficient accuracy and precision for measuring our hand movements with the selected device, at the highest sampling rate.

C. Sensors Differences Between Devices

During fabrication, subtle imperfections arise in sensors, which yields different responses to the same stimulus. Several studies investigated the effect and magnitude of these imperfections; [11] uses the accelerometers, [4] analyze the frequency response of the speakerphone-microphone plus the accelerometer calibration errors, and [8] uses the microphones and speakers to provide unique fingerprints of the devices -[11], [4] and [8] use these imperfections in the sensors to identify the devices.

We evaluate the differences and the stability of our two Google Nexus 4, which we use to collect the data. One phone is used to collect the data from the user's hand movement – it is mounted on a glove (cf. Figure 5). The other phone collects the data of the door handle movement - it is mounted on the door handle (cf. Figure 6). Figures 2-4 show the values of the accelerometers, gyroscopes and magnetometers of the two phones phone located in the glove and in the handle, respectively, when both phones are at rest – laying flat with the back on the table.

Tables V-VII shows the average, maximum, minimum and standard deviation of the sensors (accelerometer, gyroscope and magnetometer) of both phones at rest, and with a sample rate equal to 0.1s . The sampling frequency is closer to the

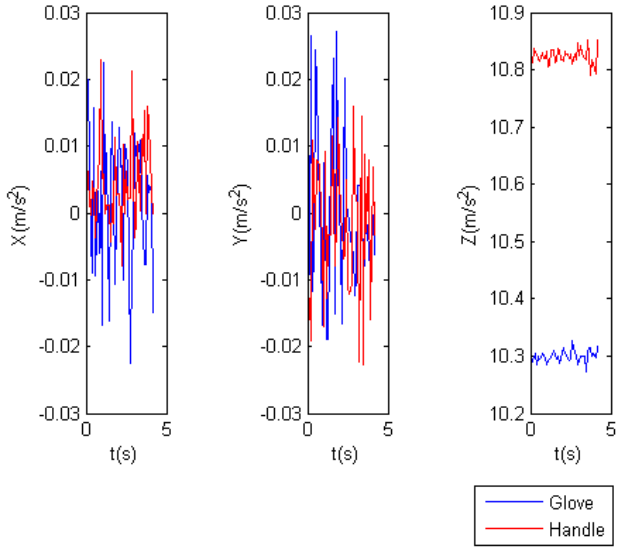

Fig. 2. Accelerometer at rest.

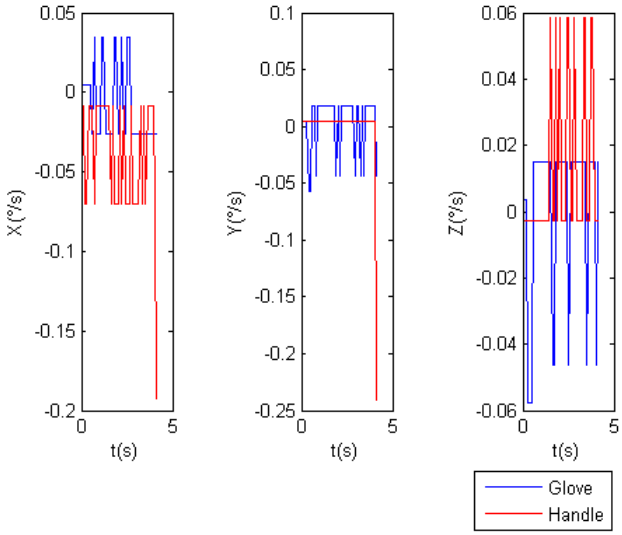

Fig. 3. Gyroscope at rest.

TABLE VI
GYROSCOPE AT REST

GYROSCOPE(SAMPLING 0.1S)				
Glove				
	Average	Max	Min	Std Deviation
X(°/s)	-0.0262	0.0350	-0.0262	0.0246
Y(°/s)	0.0175	0.0175	-0.0568	0.0264
Z(°/s)	0.0149	0.0149	-0.0577	0.0259
Handle				
X(°/s)	-0.0087	-0.0087	-0.1923	0.0388
Y(°/s)	0.0044	0.0044	-0.2404	0.0378
Z(°/s)	-0.0026	0.0586	-0.0026	0.0264

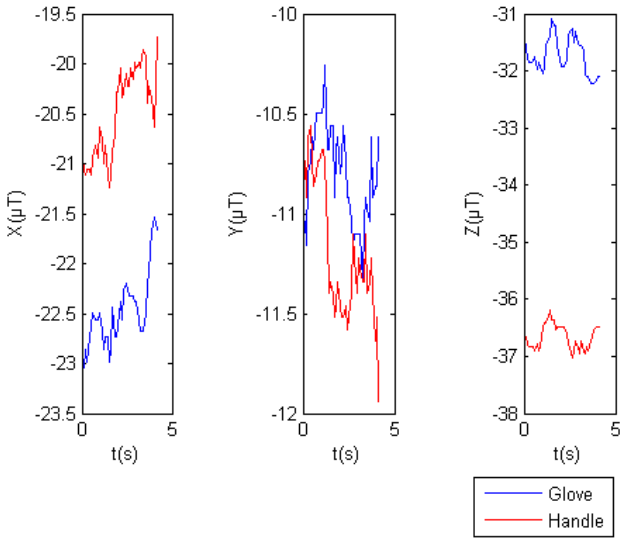

Fig. 4. Magnetometer at rest.

TABLE VII
MAGNETOMETER AT REST

MAGNETOMETER (SAMPLING 0.1S)				
Glove				
	Average	Max	Min	Std Deviation
X(μT)	-22.5586	-21.5393	-23.0392	0.3673
Y(μT)	-10.7986	-10.2585	-11.3388	0.2484
Z(μT)	-31.7695	-31.0791	-32.2189	0.3234
Handle				
X(μT)	-20.4293	-19.7388	-21.2387	0.4472
Y(μT)	-11.3388	-10.5591	-11.9385	0.3405
Z(μT)	-36.6889	-36.1786	-37.0193	0.2131

0.2s of the normal sampling rate than to 0.005s of the fastest sampling rate. We note that the standard deviations of the phone located in the glove are smaller than the one located in the door handle. Meanwhile the average values of the phone located on the handle are closer to zero than the other one. But most of the standard deviations and the average values are smaller in both cases than the obtained values for the fastest sampling rate by Ma et al. [22]. However, at this point it must be mentioned that we only used a subset of their test cases.

III. RELATED WORK

The potential of human behavior for user authentication using wearable sensors has already been discussed in the scientific literature. One of the human behaviors considered unique is arm's flex. Negara et al. [25] were the first to examine the uniqueness of arm movements when answering calls. They conduct their experiments with a tri-axial accelerometer embedded in a Pantech Sky Racer smartphone. They evaluate the cosine similarity and the euclidean distance of the acceleration pattern in 6 users and with 10 repetitions per user. They achieve 87.8% accuracy when the phone is picked from the table, and 90% accuracy when the phone is picked from the pocket.

Biometric gait recognition using smartphones has recently gained attention: Derawi et al. [10] and [9] use the low-grade accelerometers embedded in commercially available mobile devices to collect the data. [10] calculates the average step cycle of the users and use Dynamic Time Warping to compare them. They considered 51 users and they obtained an error rate of 20.1%. They say that biometric gait recognition can be run in smartphones but it is not yet ready for practical use, because the sensors embedded in the smartphones contain a lower sample rate. In [9] the authors use the accelerometer embedded in a Samsung Nexus S smartphone to implement an application for activity and gait recognition in the Samsung Nexus S smartphone. They extract the cycles of the users and they use the Manhattan (L1) distance to compare them. They consider 5 users and they correctly identify 89.3% of the users.

Touch screen gestures have recently gained popularity as a new behavioral biometric for user authentication [13]. This is because the data is indicative of the user hand geometry and muscle behavior. Such biometric characteristic variations have the potential to provide user discrimination. Feng et al. [13] consider 23 smartphone users. They extract the following features: how fast a user performs a swipe/zoom gesture; the time difference between two clicks; contact surface area; swipe location preference; length of the swipe or zoom gestures; slope of a user's swipe or zoom gestures; and the running application context. They compare the features with the combination of the nearest neighbor (1-NN) classifier and Dynamic Time Warping (DTW). They correctly identify 90% of the users, in real-life naturalistic conditions.

A. Available Datasets

To be able to better compare our results to previous work, we investigated datasets containing biometrical data previously collected and published. We present an overview in the following. However, the vast majority of the research works and available datasets using body worn inertial sensors focus on recognizing human activity instead of classifying individuals.

[33] models and recognizes human activity using wearable sensors. The authors record the data using a multimodal sensing platform called MotionNode [16], which is packed firmly into a mobile phone pouch and attached to the users' front right hip. The resolution is equal to 0.0019m/s$^2 \pm 5\%$ for the accelerometer, 0.07°/s for the gyroscope and 0.1μT for the magnetometer sensors. The sample rate is equal to 0.01s for the accelerometer, gyroscope and the magnetometer sensors.

Bao et al. [3] use a two-axis accelerometers sensor (ADXL210E) with a sample rate equal to 0.05s. The accelerometers are attached on the limbs (upper arm, lower arm, upper leg and lower leg), plus the right hip to 20 users. The users perform random sequences of 20 activities (e.g., walking, eating and drinking, reading, etc.)

Ravi et al. [27] use a a triaxial accelerometer CDXL04M3 marketed by Crossbow Technologies with a sample rate equal

to 0.02s. The accelerometer is attached on the pelvic region to two users. The users perform eight different activities (e.g., walking, running, sit-ups, etc.) in multiple rounds over different days.

Banos et al. [2] use inertial measurement units (Xsens MTx) with a sampling rate 0.02s. The inertial measurement units are attached on the left calf, left thigh, right calf, right thigh, back, left lower arm, left upper arm, right lower arm and right upper arm of 17 users. The volunteers perform warm up, cool down and fitness exercises considered for the activity set, where there are some activities with the arms like arm frontal crossing, arms lateral elevation, etc.

Bulling et al. [6] present a tutorial on human activity recognition using body worn inertial sensors. They conduct a small user study with three Inertial Measurement Units (IMUs) with a sampling rate 0.03s. The inertial measurements units are attached on the right hand, as well as on the right lower and upper arm to two volunteers. The volunteers performs 26 activities repetitions of some activities, such as opening window, closing a window, cutting with a knife, etc.

No one of the dataset place the sensors in the hand, except for [6]. We therefore tested that dataset for user authentication and we got different accuracy for the sensors located in the lower arm and in the hand. For example, for the closing window activity we achieved an authentication accuracies of 93% with the sensors in the hand and 85% with the sensors in the lower arm, respectively. However, these results, and the dataset in general, are not useful because the dataset has only two users.

As there was no fitting dataset available for our task, we collected and make publicly available the dataset described in the following Section IV).

IV. Construction of the Dataset

Although there exist multiple datasets which describe human movements based on information obtained from sensors such as gyroscope, magnetometer and accelerometer, there is no single dataset that investigates the hand dynamics and the door handle movement when opening a door [33], [3], [27], [2]. Bulling et al. [6] investigate the hand dynamics when opening and closing windows, but the dataset has only two users.

This is why we collect our own dataset with 20 participants. The size of our dataset is comparable to previous studies in behavioral biometrics. We utilise two Google Nexus 4 phones to collect accelerometer, gyroscope and magnetometer data. In Section II we discussed the characteristics of these phones. In Section IV-A we describe our protocol for collecting the raw data from the sensors, and in Section IV-B we describe the resulting data files.

A. Sensor Data Collection

We used the AndroSensor app[1] to collect and store the sensor measurements in a data file (csv file). This app allows to choose the sampling interval among normal, fast and very fast, and the recording interval between 0.005s and 1s. We choose a sampling interval equal to 0.1s, as settings less than 0.1s have caused frequent crashes in our Google Nexus 4 smartphones.

[1]http://www.fivasim.com/androsensor.html

Fig. 5. User opening the door with the smartphone attached to the glove.

The hand and door handle movements were tracked using different devices. One phone is used to collect the data from the user's hand movement when he opens a door. It was located in the right hand of the right-handed users and in the left-hand of the left-handed users, as can be seen in Figure 5. The phone was fixed in a non-intrusive way on the outside of a glove, thus providing as little disturbance to normal hand movement as possible. Figure 5 shows a user opening the door with the Google Nexus 4 attached to the glove. The other phone was placed on the door handle, but on the other side of the door, to ensure that users do not displace it when they open the door, as depicted in Figure 6.

We recorded the hand and the door handle movements of 20 participants when they opened the same door. 19 participants were right-handed, and one was left-handed. They repeated the movement ten times in a continuous sequence. To synchronize the collected data and to extract individual attempts from the continuous sequence, the participants raised and lowered the arm before and after opening the door.

B. Activity Labels

For each participant we extract the periods of time when they were opening the door. Therefore we have 20 data files, 10 data files with the data of the hand movements (e.g., hand1d1.csv) and 10 data files with the data of the door handle (e.g., door1d1.csv). Moreover, the data of the hand and of

Fig. 6. Sensor setup in the door handle.

the door handle have been synchronized regarding the starting time.

The median time to perform the door opening activity varies between the minimum median time 3.131s of *participant #18* and the maximum median time 4.9878s of *participant #2*. The minimum variance of the time to open the door is 0.505s of the *participant #10*, the maximum variance of the time to open the door is 2.828s of *participant #2* and the mean-variance for all the 20 participants is 1.3905s. The sensors sampling rate was set to 0.1s, and the recording interval in the data files is 0.101s.

The columns of the data files are show in Table VIII, the rows representing the different time instants.

V. Authentication Method

The act of open a door is mainly one of the involuntary control of hand and arm movements, we had reason to believe at the start of this investigation that opening a door would be different enough between individuals. Furthermore, previous researches have shown that the arm bending action results in various unique traits due to various force strength exerted from various posture and biological muscular structure [25]. Further, the hand-pressure pattern when a user grips a gun [28] or the dynamics of the signature have been already used for user authentication.

Fig. 7 provides a graphical overview of our authentication method. The method is divided into two phases, the training and the classification phase.

The training phase consists of the following steps:

- Data segmentation stage identifies those segments of the data streams that contain the open door activity.
- Features are extracted from each data stream to form the feature vector.
- The training returns a model which is used for the classification task.

TABLE VIII
Columns of the CSV file

Column#	Data
1	Accelerometer X (m/s^2)
2	Accelerometer Y (m/s^2)
3	Accelerometer Z (m/s^2)
4	Gravity X (m/s^2)
5	Gravity Y (m/s^2)
6	Gravity Z (m/s^2)
7	Linear Acceleration X (m/s^2)
8	Linear Acceleration Y (m/s^2)
9	Linear Acceleration Z (m/s^2)
10	Gyroscope X (°/s)
11	Gyroscope Y (°/s)
12	Gyroscope Z (°/s)
13	Magnetometer X (μT)
14	Magnetometer Y (μT)
15	Magnetometer Z (μT)
16	Orientation X (°)
17	Orientation Y (°)
18	Orientation Z (°)
19	Time since start (ms)

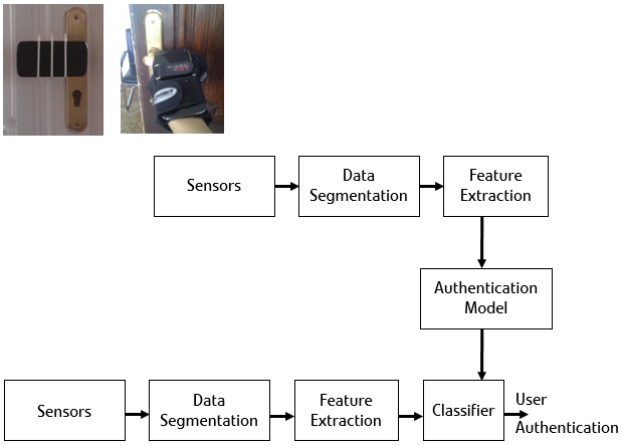

Fig. 7. Block diagram of our authentication method.

The classification phase (authentication phase) consists as well of a segmentation and feature extraction phase, as in the training phase. Finally, the trained model is used for user authentication.

A. Feature Extraction

Feature extraction methodologies are used to filter relevant information and to obtain quantitative measures that allow signals to be compared. They transform the raw time series dataset into a set of feature vectors. It is well understood that high quality features are essential to improve the classification accuracy of the machine learning method.

There are studies focusing on exploring the best features that can be extracted from human activity signals. In this work, we evaluate two features sets: statistical features and

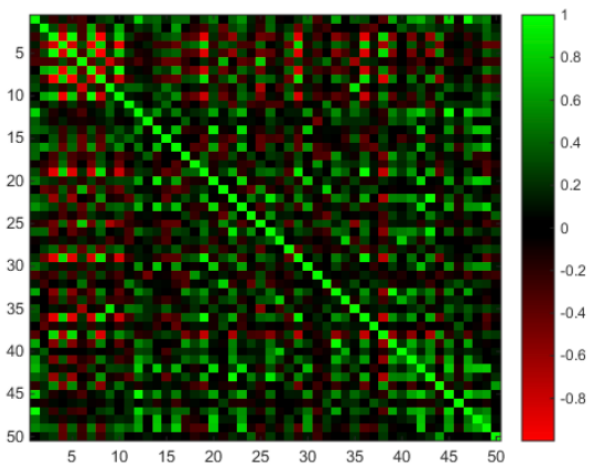

Fig. 8. Correlation coefficients of pairs of features.

physical features. Statistical features have been intensively investigated in previous studies and proved to be useful for activity recognition [3], [27], [17]. The physical features were originally designed by [32].

Overall we have a feature set of 170 features, where 85 features are determined by the door handle and 85 from the glove. We will describe them in the following. Figure 8 illustrates the correlation coefficients of all pairs of features in a color-coded plot.

1) Statistical Features: The statistical features are computed from each axis (channel) of the accelerometer, gyroscope and magnetometer over the segments of the data streams that contain the open door activity. We consider statistical features that have been successfully applied in similar recognition problems. Examples are zero crossing rate, mean crossing rate, and first-order derivative. These features have been heavily used in human speech recognition and handwriting recognition problems. We thus extract the following statistical features:

- *Mean:* The DC component (average value), (dimensionality: 9, feature index: 1-9)
- *Median:* The median signal value, (dimensionality: 9, feature index: 10-18)
- *Root Mean Square Level:* The quadratic mean value, (dimensionality: 9, feature index: 19-27)
- *Averaged derivatives:* The mean value of the first order derivatives, (dimensionality: 9, feature index: 37-45)
- *Interquartile Range:* Measure of the statistical dispersion, (dimensionality: 9, feature index: 46-54)
- *Zero Crossing Rate:* Total number of changes from positive to negative or vice versa normalized by the length of the data segment. (dimensionality: 9, feature index: 55-63)
- *Mean Crossing Rate:* The total number changes from below average to above average or vice versa normalized by the length of the data segment, (dimensionality: 9, feature index: 64-72)

2) Physical Features: The physical features are derived based on the physical interpretations of human motion [32]. It should be noted that the way to compute physical features is different from statistical features. For statistical features, each feature is extracted from each sensor axis (channel) individually. In contrast, the physical features are the combination of multiple sensor axis. We extract the following physical features:

- *Movement intensity:* The Euclidean norm of the total acceleration vector after removing the static gravitational acceleration. This feature is independent of the orientation of the sensing device, and measures the instantaneous intensity of human movements. We compute the mean (AI) and the variance (VI):
  - Mean (AI) (dimensionality: 1, feature index: 73)
  - Variance (VI) (dimensionality: 1, feature index: 74)
- *Normalized signal magnitude area:* The acceleration magnitude summed over three axes normalized by the length of the data segment, (dimensionality: 1, feature index: 75)
- *Dominant frequency:* The maximum of the squared discrete Fast Fourier transform (FFT) component magnitudes from each sensor axis.
- *Energy:* The sum of the squared discrete FFT component magnitudes from each sensor axis, normalized by the length of the data segment. (dimensionality: 9, feature index: 76-84)
- *Averaged acceleration energy:* The mean value of the energy over three acceleration axes. (dimensionality: 1, feature index: 85)

B. Classification Algorithm

In order to authenticate users, we propose a classification approach that uses the features and the trained model to classify the user into one of the previously-observed users.

After initial tests with various machine learning models, for our final setup, we use *Support Vector Machines (SVM)*, a popular machine learning method for classification that has shown good results in many application domains.SVM was originally designed for binary classification. For multi-class classification we use the Library LIBSVM [7]. LIBSVM implements the 'one-against-one' approach [18] for multi-class classification. Even though many other methods are available for multi-class SVM classification, Hsu et al.[15] performed a detailed comparison of them and concluded that the 'one-against-one' is a competitive approach.

Chang et al. [7] propose to combine the individual one-against-one binary classification results: each binary classification is considered to be a voting where votes can be cast for all data points x - in the end a point is designated to be in a class with the maximum number of votes. In case that two classes have identical votes, though it may not be a good strategy, now we simply choose the class appearing first in the array of storing class names.

VI. Experimental Evaluation

In this section we describe our experiments and then present and discuss our results for the authentication task.

A. Methodology

Our experiments first requires a collection of labelled raw sensor (accelerometer, gyroscope and magnetometer) data and then transform to a feature vectors. This process was described in Section V-A. We combine the features with an early fusion scheme which combines features before performing classification – obtaining 85 features per user. Our dataset consists of 20 individuals (users). Every user opened the door 10 times. 50% of the data (i.e. opening the door 5 times) is used for training and the other 50% of the data for testing. Note that the data in the training set are not present in the test set.

Once the data set was prepared and the features extracted, we used multi-class classification techniques from the the Library LIBSVM [7]. We choose the following parameters when learning the SVM:

- Type of the SVM: C-SVC.
- Kernel function: linear (u'$*$ v).
- Degree in kernel function: 3.
- Gamma in kernel function: 1/k (k means the number of attributes in the input data).
- coef0 in kernel function: 0.
- Parameter C of C-SVC: 1.
- Tolerance of termination criterion: 0.001.
- Parameter C of class i to weight$*$C in C-SVC: 1.

The training provides us with a model, which is subsequently used for the classification task (the future prediction). We tested a linear, a polynomial and a radial kernel function. For all the three kernels we varied the soft margin constant C in powers of ten between 1 and 1000. The polynomial kernel was used with degrees between 2 and 5. For the polynomial and the radial kernel the values of parameter are between 0.00001 and 1, similar to Eberz et al. [12]. The best result were achieved with rbf-kernel with C=10 and =0.0001, where we obtained an accuracy equal to 97.5%.

B. Adversary Model

Our adversary model is based on an insider threat scenario. Therefore, we consider every subject as potential imposter of every other subject. Hence, for our evaluation we also consider the class distance, which measures the distance between the probability to be a determinate user and the most successful out of the potential impostors.

C. Results

The summary results for our authentication experiments are presented in Table IX. This table specifies the predictive accuracy associated with each user, for the sensors located in the glove (Figure 5), the sensors located in the door handle (Figure 6), and the combination of the sensors from the glove and the door handle.

Table IX demonstrates that in most cases we can achieve a high level of accuracy. For the combination of the sensors from the glove and those from the door handle, we achieve the 100% accuracy for 14 users (70% of the total number of users), 80% (that is, one misclassification and four correctly identified samples) for four users (20% of the total number of users) and 60% for two users (10% of the total number of users). The average accuracy predicted with the combination of both sensors (glove and door handle) is 92%.

We observe that the achieved accuracies for the sensors from the glove and the door handle individually are similar and lower than for the combination of both: for the sensors located in the door handle is 84%; and for the sensors in the glove is 83%. We achieve the 100% accuracy for nine users (45% of the total number of users) and ten users (50% of the total number of users) with the glove and the door handle respectively. The lowest accuracies are 40% for two users (10% of the total number of users) for both cases.

More detailed results for the individual users are presented in the confusion matrices in Tables X-XII).

The *user #1* is the only one with an accuracy lower than 80% for the both individual configuration of sensors. *User #1* is mostly predicted as *user #6* and *#15* in the case of the sensors located in the glove, and as *user #4* in the case of the sensors located in the door handle.

For the sensors located in the door handle we observe that the classifier confuses *user #4* with *user #1* and *#19*, and vice-versa. *Uuser #4* has an accuracy equal to 100% in the case of the sensors located in the glove and with combination of the sensors from the glove and from the door handle. *Uuser #19* has an accuracy equal to 80% in the case of the sensors located in the glove, but he is confused with *user #15* in this case. And *user #19* has an accuracy of 100% with combination of the sensors from the glove and from the door handle.

Uuser #11 is mostly predicted as *user #5* in the case of the sensors located in the glove, while he has an accuracy of 100% in the case of the sensors located in the door handle and with combination of the sensors from the glove and from the door handle.

User #12 is mostly predicted as users *#6* and *#4* in the case of the sensors located in door handle. He has an accuracy of 100% in the case of the sensors located in the glove, but and accuracy of only 60% with combination of the sensors from the glove and from the door handle.

For the sensor located in the glove, the users with accuracies lower than 80% are: #1, #4 and #12.

For the sensor located in the glove, the users with accuracies lower than 80% are: #1, #8, #9, #11 and #13.

TABLE IX
ACCURACIES OF USER AUTHENTICATION

	% of Records Correctly Predicted		
ID	glove	handle	glove and handle
1	40	60	80
2	80	80	80
3	100	100	100
4	100	40	100
5	100	100	100
6	100	80	100
7	100	80	100
8	60	80	60
9	60	100	80
10	100	100	100
11	40	100	100
12	100	40	60
13	100	100	100
14	80	100	100
15	100	80	100
16	100	80	100
17	60	100	80
18	80	80	100
19	80	80	100
20	80	100	100
AVG	83	84	92

TABLE X
CONFUSION MATRIX FOR THE SENSORS LOCATED IN THE GLOVE.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	ID
2	0	0	0	0	**2**	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0	1
0	**4**	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0	2
0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4
0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5
0	0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6
0	0	0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0	7
0	**1**	0	**1**	0	0	0	**3**	0	0	0	0	0	0	0	0	0	0	0	0	8
0	0	0	0	0	0	0	0	**3**	**2**	0	0	0	0	0	0	0	0	0	0	9
0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	10
0	0	0	0	**3**	0	0	0	0	0	**2**	0	0	0	0	0	0	0	0	0	11
0	0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	0	0	0	12
0	0	0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	0	0	13
0	0	0	0	0	0	0	0	0	0	0	0	0	**4**	0	0	0	**1**	0	0	14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	16
0	0	0	0	**1**	0	**1**	0	0	0	0	0	0	0	0	0	**3**	0	0	0	17
0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0	0	**4**	0	0	18
0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	**4**	0	19
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	**4**	20

TABLE XI
CONFUSION MATRIX FOR THE SENSORS LOCATED IN THE DOOR HANDLE.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	ID
3	0	0	**2**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0	**4**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	2
0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
1	0	0	**2**	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	**1**	0	4
0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5
0	0	0	0	0	**4**	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	6
1	0	0	0	0	0	**4**	0	0	0	0	0	0	0	0	0	0	0	0	0	7
0	**1**	0	0	0	0	0	**4**	0	0	0	0	0	0	0	0	0	0	0	0	8
0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	9
0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	10
0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	11
0	0	0	**1**	0	**2**	0	0	0	0	0	**2**	0	0	0	0	0	0	0	0	12
0	0	0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	0	0	13
0	0	0	0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	0	14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	**4**	0	0	0	0	**1**	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**4**	**1**	0	0	0	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**4**	0	**1**	18
0	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**4**	0	19
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**5**	20

TABLE XII
CONFUSION MATRIX FOR THE COMBINATION OF THE SENSORS LOCATED IN THE GLOVE AND IN THE DOOR HANDLE

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	ID
4	0	0	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0	**4**	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0	2
0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4
0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5
0	0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6
0	0	0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0	7
0	**1**	0	**1**	0	0	0	**3**	0	0	0	0	0	0	0	0	0	0	0	0	8
0	0	0	0	0	0	0	0	**4**	**1**	0	0	0	0	0	0	0	0	0	0	9
0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	10
0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	0	0	0	0	11
0	0	**1**	0	0	0	0	0	0	0	0	**3**	0	0	0	0	0	0	**1**	0	12
0	0	0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	0	0	13
0	0	0	0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	0	14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	0	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**5**	0	0	0	0	16
0	0	0	0	0	0	**1**	0	0	0	0	0	0	0	0	0	**4**	0	0	0	17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**5**	0	0	18
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**5**	0	19
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**5**	20

We improve the accuracies with the combination of the sensors located in the glove and the sensors located in the door handle. The users *#8* and *#12* are the only users with an accuracies lower than 80% with the combination.

We study the characteristic of hand movement when opening a door in an uncontrolled scenario. For the experiment we did not regulate the distance to the door, thus the participants might have spent more time walking towards the door. This is a possible explanation for approximately equal accuracy with the sensors located in the glove than with the sensors located in the door handle. We obtain more information with the sensors located in the glove (the arm flex [25], hand muscle behavior, the relative users' high compared to the door high, etc.) but they introduce more degrees of freedom (e.g., *user #2* has a variance of 2.828s of the needed time to open the door).

The recognition systems based on the measurement of single behavioral modality cannot guarantee 100% accuracy. In fact, these factors laid the foundation of the systems which use multiple independent evidences of biometric information from either single or different biometric modalities, very often termed as multi-modal biometric systems [30].

Our lab study shows that our solution allows to classify individuals with an accuracy of 92% based on their hand movement only. Our authentication method shows a higher accuracy compared to other related work: Negara et al. [25] examined the uniqueness of arm movements when answering calls. They achieved 87.8% accuracy in picking up a phone from a table to answer a call; and 90% accuracy for picking

up a phone from a pocket. Compared to our study, they only considered 6 participants and 10 repetitions for each participant.

Derawi et al. [9] performed gait recognition using smartphones. They considered only 5 users and they were able to correctly identify 89.3% of the users which is justified by the lower sample rate of the smartphones.

Feng et al. [13] performed user identification using touch screen. They considered 23 smartphone users in real-life naturalistic conditions. They correctly identified 90% of the users.

To evaluate our approach towards the attacker model described in Section VI-B, we calculated the class distance for our 19 potential impostors. The lowest calculated class distance was 15.91% (mean = 67.22%).

VII. Conclusion and Future Work

In this paper, we proposed a novel authentication algorithm based on hand dynamics. Our machine learning-based approach relies on the richness of motion sensors in smartphones and smartwatches in particular. It also exploits the uniqueness of hand and arm movements and thus highlights the potential of hand movement biometrics for continuous authentication. To evaluate our approach, we collected hand movement data from 20 participants. We also selected a set of statistical and physical features that we then used to classify individuals. Our experiments have shown that our hand dynamics authentication method was able to classify individuals with an accuracy of 92%. As future work, we plan to perform experiments with smartwatches. We furthermore plan to consider security attacks, such as impersonation attacks by mimicking the behaviour of others; and to conduct an extensive usability study in order to evaluate the usefulness and feasibility in a real-world scenario, such as granting access to premises in office buildings.

References

[1] Sanjeev Acharya, Alexander Fridman, Philip Brennan, Patrick Juola, Rachel Greenstadt, and Moshe Kam. User authentication through biometric sensors and decision fusion. In *47th Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6. IEEE, 2013.

[2] O. Banos, M. A. Toth, M. Damas, H. Pomares, and I. Rojas. Dealing with the effects of sensor displacement in wearable activity recognition. *Sensors, vol. 14*, 2014.

[3] L. Bao and S. S. Intille. Activity recognition from user-annotated acceleration data. *Pervasive computing. Springer Berlin Heidelberg*, 2004.

[4] H. Bojinov, D. Boneh, and Y. Michalevsky. Mobile device identification via sensor fingerprinting. *arXiv preprint arXiv:1408.1416*, 2014.

[5] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 553–567. IEEE, 2012.

[6] A. Bulling, U. Blanke, and B. Schiele. A tutorial on human activity recognition using body-worn inertial sensors. *ACM Computing Surveys (CSUR) 46 (3)*, 2014.

[7] C. C. Chang and C.J. Lin. Libsvm : a library for support vector machines. *ACM Transactions on Intelligent Systems and Technology*, 2011.

[8] A. Das, N. Borisov, and M. Caesar. Do you hear what i hear?: Fingerprinting smart devices through embedded acoustic components. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2014.

[9] M. Derawi and P. Bours. Gait and activity recognition using commercial phones. *Computers and Security*, 2013.

[10] M. O. Derawi, C. Nickel, P. Bours, and C. Busch. Unobtrusive user-authentication on mobile phones using biometric gait recognition. *Intelligent Information Hiding and Multimedia Signal Processing*, 2010.

[11] S. Dey, N. Roy, W. Xu, R. R. Choudhury, and S. Nelakuditi. Accelprint: Imperfections of accelerometers make smartphones trackable. *In Proceedings of the Network and Distributed System*, 2014.

[12] Simon Eberz, Kasper B Rasmussen, Vincent Lenders, and Ivan Martinovic. Preventing lunchtime attacks: Fighting insider threats with eye movement biometrics. 2015.

[13] T. Feng, J. Yang, Z. Yan, E. M. Tapia, and W. Shi. Tips: Context-aware implicit user identification using touch screen in uncontrolled environments. *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications*, 2014.

[14] Alex Fridman, Ariel Stolerman, Sayandeep Acharya, Patrick Brennan, Patrick Juola, Rachel Greenstadt, and Moshe Kam. Decision fusion for multimodal active authentication. *IT Professional*, (4):29–33, 2013.

[15] W. Hsu and C. J. Lin. A comparison of methods for multi-class support vector machines. *IEEE Transactions on Neural Networks*, 2002.

[16] http://www.motionnode.com/.

[17] T. Huynh and B. Schiele. Analyzing features for activity recognition. *In Proceedings of the joint conference on Smart objects and ambient intelligence: innovative context-aware services: usages and technologies*, 2005.

[18] S. Knerr, L. Personnaz, and G. Dreyfus. Single-layer learning revisited: a stepwise procedure for building and training a neural network. *Neurocomputing: Algorithms, Architectures and Applications. Springer-Verlag*, 1990.

[19] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell. A survey of mobile phone sensing. *IEEE Commun. Mag., vol. 48, no. 9,*, 2010.

[20] M. J. Lee. Samsung looks to expand biometric sensors in mobile devices. *The Wall Street Journal*, 2014.

[21] L. Luk and R. Winkler. Google developing tablet with advanced vision capabilities. *The Wall Street Journal*, 2014.

[22] Z. Ma, Y. Qiao, B. Lee, and E. Fallon. Experimental evaluation of mobile phone sensors. *Signals and Systems Conference (ISSC)*, 2013.

[23] Michelle L Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 173–186. ACM, 2013.

[24] Yan Michalevsky, Dan Boneh, and Gabi Nakibly. Gyrophone: Recognizing speech from gyroscope signals. In *Proc. 23rd USENIX Security Symposium (SEC14), USENIX Association*, 2014.

[25] A. F. P. Negara, E. Kodirov, M. F. A. Abdullah, D. J. Choi, G. S Lee, and S. Sayeed. Arms flex when responding call for implicit user authentication in smartphone. *Int. J. Secur.*, 2012.

[26] Salil Prabhakar, Sharath Pankanti, and Anil K Jain. Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, (2):33–42, 2003.

[27] N. Ravi, N. Dandekar, P. Mysore, and M. L. Littman. Activity recognition from accelerometer data. *In IAAI*, 2005.

[28] X. Shang and R. Veldhuis. Local absolute binary patterns as image preprocessing for grip-pattern recognition in smart gun. *Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007. First IEEE International Conference on. IEEE*, 2007.

[29] Doroteo T Toledano, Rubén Fernández Pozo, Álvaro Hernández Trapote, and Luis Hernández Gómez. Usability evaluation of multi-modal biometric verification systems. *Interacting with Computers*, 18(5):1101–1122, 2006.

[30] J. A. Unar, W. C. Seng, and A. Abbasi. A review of biometric technology along with trends and prospects. *Pattern recognition*, 2014.

[31] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, et al. How does your password measure up? the effect of strength meters on password creation. In *USENIX Security Symposium*, pages 65–80, 2012.

[32] M. Zhang and A. A. Sawchuk. A feature selection-based framework for human activity recognition using wearable multimodal sensors. *6th International Conference on Body Area Networks*, 2011.

[33] M. Zhang and A. A. Sawchuk. Motion primitive-based human activity recognition using a bag-of-features approach. *In Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*, 2012.