Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing

Research Paper

Continuous Authentication of Smartphone Users Based on Activity Pattern Recognition Using Passive Mobile Sensing

Muhammad Ehatisham-ul-Haq [a,*], Muhammad Awais Azam [a], Usman Naeem [b], Yasar Amin [a], Jonathan Loo [c]

[a] Faculty of Telecom and Information Engineering, University of Engineering and Technology, Taxila, Punjab, Pakistan.

[b] School of Architecture, Computing and Engineering, University of East London, UK.

[c] School of Computing and Engineering, University of West London, London, UK.

***** ***Corresponding author:*** ehatishamuet@gmail.com

Abstract: Smartphones are inescapable devices, which are becoming more and more intelligent and context-aware with emerging sensing, networking and computing capabilities. They offer a captivating platform to the users for performing a wide variety of tasks including socializing, communication, sending or receiving emails, storing and accessing personal data etc. at anytime and anywhere. Nowadays, loads of people tend to store different types of private and sensitive data in their smartphones including bank account details, personal identifiers, accounts credentials, and credit card details. A lot of people keep their personal e-accounts logged in all the time in their mobile devices. Hence these mobile devices are prone to different security and privacy threats and attacks from the attackers. Commonly used approaches for securing mobile devices such as passcode, PINs, pattern lock, face recognition, and fingerprint scan are vulnerable and exposed to several attacks including smudge attacks, side-channel attacks, and shoulder-surfing attacks. To address these challenges, a novel continuous authentication scheme is presented in this study, which recognizes smartphone users on the basis of their physical activity patterns using accelerometer, gyroscope, and magnetometer sensors of smartphone. A series of experiments are performed for user recognition using different machine learning classifiers, where six different activities are analyzed for the multiple locations of smartphone on the user's body. SVM classifier achieved the best results for user recognition with an overall average accuracy of 97.95%. A comprehensive analysis of the user recognition results validates the efficiency of the proposed scheme.

Keywords: Activity Pattern Recognition, Behavioral Biometrics, Continuous Authentication, Mobile Sensing, Smartphone User Recognition, Ubiquitous Computing

1. Introduction

Smartphone and mobile technologies have become much popular in a very short span of time. We have moved from larger phones to very slim yet powerful smartphones. These devices have aided people with internet connectivity and enabled them to do their routine tasks at anytime and anywhere. At the moment, 68% of the entire world's inhabitants possesses a mobile phone and this number is anticipated to reach up to 72% by 2019 ("The Statistic Portal", 2017). Smartphones have started to replace personal computers and laptops. A market research has shown that mobile phone shipments worldwide are projected to add up to 1.93 billion in 2019 (Gartner, 2017). Due to the increased use of smartphones, more and more data is being produced, stored, accessed, and analyzed on these devices at homes, offices, and workplaces on daily basis. This data also includes sensitive and confidential information including personal identifiers, bank account details, and credit card information etc. As much as these mobile devices have become popular and improved worker's output, the security and privacy of sensitive data stored on these devices is still a key problem to be resolved (Krupp et al., 2017). The ever growing popularity of smartphones and mobile devices has resulted in several incentives for the attackers. The attackers are shifting their focus on mobile and hand-held devices as these devices can be stolen easily and victims' confidential data can be compromised. By stealing mobile devices, the attackers can easily reach and contaminate more machines and earn more money by misusing individuals' private details or by

selling their details via the black market ("Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes", 2018). Therefore, ensuring the privacy of sensitive information being stored on these portable devices has now become critical. Unluckily, most extensively used validation methods for smartphones and mobile devices including password, PIN (Personal Identification Number), and pattern locks provide weak authentication and have certain limitations. These schemes are subjected to several attacks, which include side-channel attacks (Spreitzer et al., 2016), smudge attacks (Meng et al., 2016), and shoulder-surfing attacks (Wakabayashi et al., 2017). Passwords and PINs need to be remembered all the time and the length of time required for their input is also frustrating (Mayron, 2015). Pattern locks may be drawn by others because of the distinctive traces of fingertip left on the phone screen after drawing a pattern. Biometric authentication schemes for mobile devices, such as face recognition and iris recognition, are influenced by the environmental conditions such as light and shelter. Fingerprint scans are subjected to spoofing and require additional hardware for their operation. Furthermore, these frequently used authentication schemes only provide entry point authentication and fail to detect and recognize a challenger after the point of entry. Hence, these methods are ineffective to apply for authenticating and recognizing a smartphone user in a continuous way.

To enhance the security of mobile devices and provide potential solutions to existing challenges in smartphone authentication, researchers have come up with numerous schemes, which perform authentication on the basis of behavioral biometrics (Alzubaidi and Kalita, 2016). These authentication schemes offer a way to continuously and passively authenticate different smartphone users by identifying their behavioral traits while interacting with smartphone. (Wu et al., 2016) utilized keystrokes and gestures as behavioral biometrics for continuous authentication of smartphone users. (Meng et al., 2016) proposed a touch movement based method for improving the security of pattern locks. The authors identified the users on the basis of touch movements while unlocking patterns. (Yang et al., 2015) utilized handwaving as a behavioral biometric for user authentication. (Shen et al., 2016) proposed a method to authenticate users through the action of passcode input by utilizing orientation sensors and accelerometers. (Zhang et al., 2015) identified gait pattern by using five body-worn accelerometers on different locations and utilized gait pattern as a behavioral biometric for identifying users. (Zeng, 2016) proposed the possibility of utilizing dynamic behavior based on simple activities such as walking, running, climbing, and jumping for identifying users using wearable sensors. (Cola et al., 2016) used motion data of the walking activity collected from a wrist-mounted device for user authentication. These wearable sensors and devices become a cause of interference for the users in performing their activities. Therefore, a few researchers have made use of smartphone motion sensors to develop efficient schemes for user authentication based on behavioral biometrics (Sitova et al., 2016; Neverova et al., 2016). However, the performance of these schemes is compromised by the position and orientation sensitivity of smartphone motion sensors. Moreover, the research on continuous user authentication is still very challenging due to the difficulty in collecting real time data in open and dynamic environments (Neverova et al., 2016). Therefore, it is the need of the hour to develop more efficient and reliable solutions for continuous and non-intrusive user authentication to ensure the security of mobile device.

In this research work, an intelligent scheme is proposed for the unobtrusive authentication and validation of smartphone users to address existing challenges in continuous authentication. The proposed scheme is based on recognition of physical activity patterns of different smartphone users for their identification. Once a user is identified, he/she can easily be validated and authorized. Our idea is to learn the activity patterns of a smartphone user to differentiate him/her from other users on the basis of his/her behavioral traits. As the authentication needs to be done in real time, therefore we have selected six real life activities of daily living for user recognition purpose. These activities include walking, sitting, standing, running, walking upstairs, and walking downstairs. These activities are likely to be performed by every normal human being for multiple times in their routine life. Moreover, people usually perform these activities in a different way from each other owing to their behavioral traits. Three smartphone embedded sensors i.e., accelerometer, gyroscope, and magnetometer, are selected to provide data corresponding to six selected activities performed by the users. These inertial sensors provide a way to recognize smartphone users based on their activity patterns as shown in Fig. 1. As in real time, the placement of smartphone on the human body is not always fixed; therefore user recognition is analyzed for five different smartphone positions on the user's body. These positions include left thigh (left jeans pocket), right thigh (right jeans pocket), waist, upper arm, and wrist position. A smartphone needs to be in one of these positions on the user's body for his/her recognition based on the proposed scheme. An existing dataset for physical activity recognition (Shoaib et al., 2014, 2013) is utilized for this study, which fulfills all necessary experimentation requirements. A number of time domain features are extracted from the

data after its preprocessing. These features are then further utilized for recognizing ten different users on the basis of six individual activities selected in this study. For the purpose of experimentation, three different classifiers i.e., Support Vector Machine (SVM), Decision Tree (DT), and K-Nearest Neighbors (K-NN), are used for user recognition.

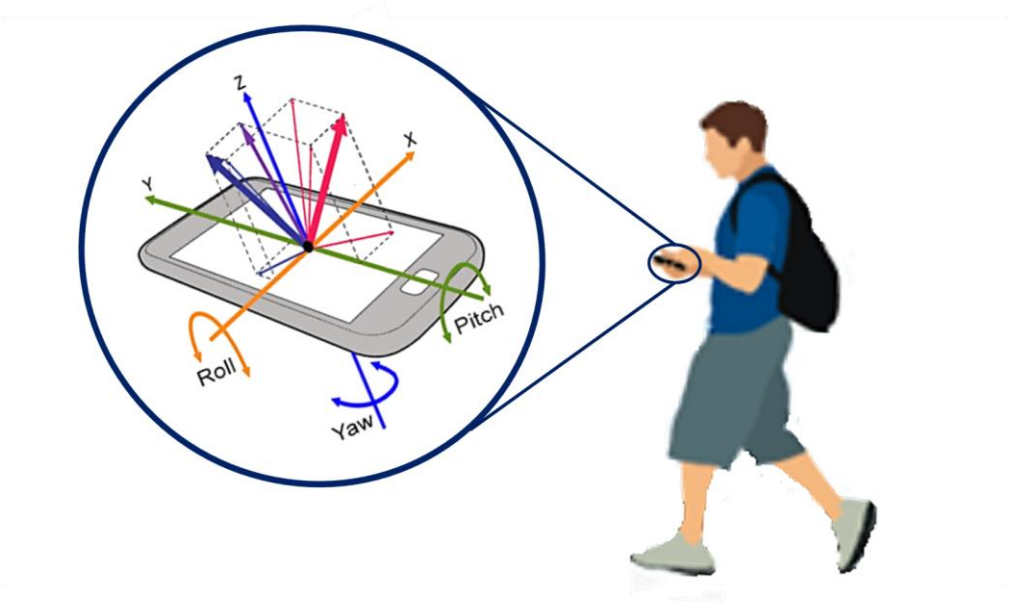

Fig. 1. Smartphone inertial sensors track the physical activity pattern of a user and provide a way to identify that user based on activity pattern recognition

The significant achievements of this research work are as follow:

1. An innovative scheme is presented for continuously authenticating smartphone users, which is based on the recognition of physical activity patterns of individual users for their identification.
2. The issue of position sensitivity of smartphone motion sensors is addressed in this study to reduce false positives for user authentication. For this purpose, five different smartphone positions on the user's body are analyzed for user recognition.
3. The experiments for user recognition are performed using three prevalent machine learning classifiers and a detailed comparison is presented amongst these classifiers performance for recognizing users. The best one provides efficient results for user identification based on activity patter recognition.
4. As the proposed scheme is based on activity pattern recognition, a detailed analysis is presented for six different activities, which shows the best activities and the phone positions that can be utilized for efficient user recognition.

The remaining part of the paper is structured as follows: Section 2 provides a brief description of the background and related work. Section 3 explains the methodology of research in details. Section 4 presents and discusses the results of user recognition comprehensively and analyzes the performance of selected machine learning algorithms for user recognition. Section 5 determines the findings of this research study and gives recommendations for further future work.

2. Background and Related Work

With the dominant increase in computing, networking, and sensing capabilities of smartphones, researchers have started to make use of the sensory data available from these devices to model human behavior (Cho and Lee, 2017; Kwapisz et al., 2011; Miluzzo et al., 2010; van Deursen et al., 2015; Zhitomirsky-Geffet and Blau, 2016) and infer certain contexts. Context-awareness has become increasingly significant as being aware of people surroundings is very beneficial for a wide variety of pervasive applications. Human-centric contexts, such as indoor or outdoor, at home or in office etc., have been studied extensively by the researchers (Hoseini-Tabatabaei et al., 2013; Khan et al., 2013; Miluzzo et al., 2008; Otebolaku and Andrade, 2016). A few

efforts have been made on context-awareness from phones' perspective also. Sherlock framework (Yang et al., 2014) collects data from smartphone sensors and recognizes the near surroundings of the smartphone. Table 1 shows a set of smartphone sensors that have been utilized in different research studies. The data acquired from these sensors have been utilized for activity recognition (Su et al., 2014; Wannenburg and Malekian, 2016) and many other aspects related to health monitoring (Lee et al., 2012; Mun et al., 2009; Pludwinski et al., 2016), social activities monitoring (Gesell et al., 2013; Harari et al., 2016; Min et al., 2013), and crowdsourcing (Chatzimilioudis et al., 2012; Consolvo et al., 2008). On-body wearable sensors have also been utilized to learn human movements and actions (Bulling et al., 2014; Ellis et al., 2013; Shoaib et al., 2016). But these wearable on-body sensors create inconvenience for the users in performing their activities. Moreover, it is hard and takes a lot of time to adjust these wearable sensors on right positions. As a result, mobile sensing has been employed for human activity recognition (Avci et al., 2010; Lockhart et al., 2012; Incel et al., 2013; Lara and Labrador, 2013), which has a diversified range of significant application areas. In (Shoaib et al., 2015a), the authors provided a comprehensive survey of online activity recognition using mobile sensing. (Albert et al., 2012) utilized mobile sensing for activity recognition of Parkinson's patients. The CenceMe system (Miluzzo et al., 2008) recognizes simple physical activities like idle, walking, and running with the help of an accelerometer. Activity recognition has been further used for different applications, such as human behavior modeling (Miluzzo et al., 2010; Pei et al., 2013) and health monitoring (Mun et al., 2009). (Shoaib et al., 2015b) utilized activity recognition for the detection of bad and unusual habits of different persons. Our study aims to utilize activity pattern recognition for validating smartphone users.

The research on smartphone authentication is progressing and researchers have come up with some dominant work in recent years. In literature, there exist different approaches for reliable and efficient recognition of smartphone users using physiological and behavioral biometrics. (Song et al., 2016) presented a novel framework for smartphone user authentication called EyeVeri, which is based on tracking human eye movement using front camera of smartphone. The authors explored different gaze patterns i.e., volitional and non-volitional, using pattern matching algorithms to provide access authentication. An in-depth analysis of the evaluation results showed that the proposed scheme works effectively. (Alzubaidi and Kalita, 2016) provided a detailed review of seven different types of behavioral biometrics, including walking style, touchscreen interaction, signature, handwaving, keystroke dynamic, voice, and behavior sketching. (Yang et al., 2015) proposed OpenSesame, a scheme to authenticate users on the basis of handwaving patterns. SVM classifier was used for classifying a user as authorized or unauthorized. (Shrestha et al., 2013) proposed a scheme called Wave-to-Access, which is based on recognition of handwaving gestures. An embedded smartphone sensor i.e., ambient light sensor, was used to examine phone dialing behavior for authentication purposes. Using handwaving scheme for authentication purposes has certain limitations, for example, it cannot authenticate a user continuously and passively all the time. (Papadopoulos et al., 2017) addressed the challenges of shoulder-surfing attacks in their study. The authors proposed IllusionPin (IPIN) for user authentication, which utilized hybrid images for blending two keypads for keypad illusion. (Sitova et al., 2016) introduced a behavioral authentication scheme based on Hand Movement, Orientation, and Grasp (HMOG) features for continuous and unobtrusive user authentication. HMOG features keep track of how a user grasps, holds, and taps on the smartphone. The authors achieved an EER (Equal Error rate) as minimum as 7.16%, which shows the effectiveness of their proposed scheme. (Draffin et al., 2014) presented KeySens, in which the behavior of the user was learnt by utilizing the pattern of user's interaction with the keyboard. The authors examined touchscreen interactions of the smartphone users based on the movement of fingers, touch force, and the area enclosed by the fingers. (Feng et al., 2013) came up with Typing Authentication and Protection (TAP) scheme for user authentication. TAP included login and post log-in phases to validate a user by exploiting the password and biometric information. The experimental results were validated using three different classifiers out of which Random Forest gave lowest False Acceptance Rate (FAR) of 8.93%. (Frank et al., 2013) also validated the use of touchscreen interactions as a behavior biometric for user verification. (Trojahn and Ortmeier, 2013) used a combination of keystroke and handwriting analysis for authentication purpose. (Zheng et al., 2014) utilized a combination of smartphone inertial and touchscreen sensors for validating a smartphone user. (Shahzad et al., 2013) proposed a gesture based user authentication approach to provide safe unlocking facility for touchscreen devices. Different features including finger velocity, device acceleration, and stroke time were used to learn how a user input data. The authentication schemes based on keystrokes and touchscreen interactions take a lot of time for training and learning the keystroke and touchscreen interaction patterns for a user. Moreover, keystrokes or touchscreen patterns of a user change with the passage of time as the behavior of the user changes.

184 **Table 1.** A set of smartphone embedded sensors

Sensor	Description
Accelerometer	Measures the acceleration force applied to the device including the force of gravity
Linear Accelerometer	Measures the acceleration force applied to the device excluding the force of gravity
Gyroscope	Measures the device rotation by using the roll, pitch, and yaw motions of the smartphone along three axes (x, y, z)
Magnetometer	Measures the ambient geomagnetic field in three axes (x, y, z)
Light Sensor	Measures the ambient light level i.e., illumination
Humidity Sensor	Measures the humidity of ambient environment
Proximity Sensor	Measures the closeness of an object relative to device screen
Barometer	Measures the ambient air pressure

185 A few researchers have worked on utilizing physiological sensors for identity authentication. (Camara et
186 al., 2015) formulated a scheme that identifies a user by utilizing Electrocardiogram (ECG) signals. Different
187 features were extracted from ECG signals and K-NN classifier was applied for the purpose of user
188 identification. The experiments reported that their proposed scheme achieved a mean accuracy of 97%. Another
189 identity authentication approach was proposed by (Hejazi et al., 2016), where the authors used a multi-class
190 SVM for user identification after applying Discrete Wavelet Transform (DWT) on ECG signals. The
191 experiments reported 3.97% false match rate. (Kang et al., 2016) utilized smartwatch sensors for recording the
192 ECG signals of different participants. The participants were kept in an exact motion state, which restricted the
193 practical application of the proposed scheme. The experimental results presented an FAR of around 5%. These
194 research studies proved that the ECG signals provide an impending solution of user authentication problem.
195 However, the placement of ECG sensors and equipment on the user's body, such as at chest or hand, creates
196 inconvenience for the user.
197 Another approach for validating smartphone users is the use of smartphone inertial sensors for obtaining
198 data related to behavioral traits of different users. (Zhu et al., 2017) proposed a novel user authentication
199 scheme called ShakeIn, which learns how a smartphone user shakes the phone to lock/unlock it. The biometric
200 features of the users' shaking behavior were captured with the help of embedded motion sensors of the
201 smartphone. The experiments were performed on 20 participants with 530,555 shaking samples in total. The
202 results described an Equal Error Rate (EER) of 1.2% on average. (Buriro et al., 2017) made use of user's hand
203 movement patterns for authentication purpose. The data was collected using smartphone embedded sensors and
204 Random Forest (RF) classifier was used for evaluating the results. An EER rate of 96% was achieved by the
205 system. Gait recognition with motion sensors provides a gateway for user authentication. It tends to identify and
206 recognize the walking pattern of a person, e.g. walking style of a user under different conditions. (Damaševičius
207 et al., 2016; Fernandez-Lopez et al., 2016) utilized smartphone internal motion sensors for validating users
208 based on gait characteristics. (San-Segundo et al., 2016) used smartphone inertial sensors to develop a
209 Gait-based Person Identification (GPI) scheme based on a Gaussian Mixture Model-Universal Background
210 Model (GMM-UBM). The results showed a User Recognition Error Rate (URER) of 34%. (Derawi et al., 2010)
211 exploited smartphone motion sensors for extracting information about walking cycles. They achieved an EER
212 of 20.1%. (Mäntyjärvi et al., 2005) recognized users by utilizing their walking style using data from
213 accelerometer. The research work on gait recognition and walking pattern detection is extended to recognize
214 more physical activities for user identification. A number of studies focused on recognizing activities and
215 gestures using motion sensors, including approaches based on deep learning. (Neverova et al., 2016) proposed a
216 scheme for learning human identity based on their motion patterns using deep neural networks. This scheme
217 achieved and EER of 20%.
218 In our study, we analyzed the existing challenges in smartphone user authentication and presented a
219 reliable and applicable solution for continuous user authentication. We used smartphone inertial sensors for
220 learning and recognizing the physical activity patterns of individual users for six different activities of daily
221 living. Hence, the users are identified on the basis of their behavioral traits.

3. Methodology of Research

This research study primarily focuses on learning, identifying, and recognizing behavioral patterns of different users whilst they are using their smartphones. In this work, six different daily living activities i.e., walking, running, standing, sitting, walking upstairs, and walking downstairs, are used for the purpose of user validation. Numerous researches have been carried out on identifying and recognizing these activities from each other (Su et al., 2014; Anguita et al., 2013; Avci et al., 2010; Lockhart et al., 2012; Incel et al., 2013), where the motivation is to learn and differentiate between these individual activities. This research work focuses on recognizing the pattern of these activities for individual users. The aim is to recognize the differences among the behavioral patterns of different users for the same activity. For this purpose, we trained the system to learn the behavioral patterns of individual users for six different activities. Smartphone users are then identified by the system on the basis of the way they perform a certain activity. To avoid false positives occurring because of the changing location of smartphone on the user's body, we trained the system to identify users for five different and commonly used smartphone positions. These positions are shown in Fig. 2. As behavioral authentication involves continuous collection of a user's motion data from the device, therefore, the proposed system continuously collects and processes small portion of sensors data in a passive way in order to authenticate a user in real time scenarios. The proposed system recognizes the user from the collected portion of data on the basis of his/her activity pattern. The proposed research methodology is shown in Fig.3, which consists of following steps: raw data collection, preprocessing (data-denoising and segmentation), feature extraction, and user recognition.

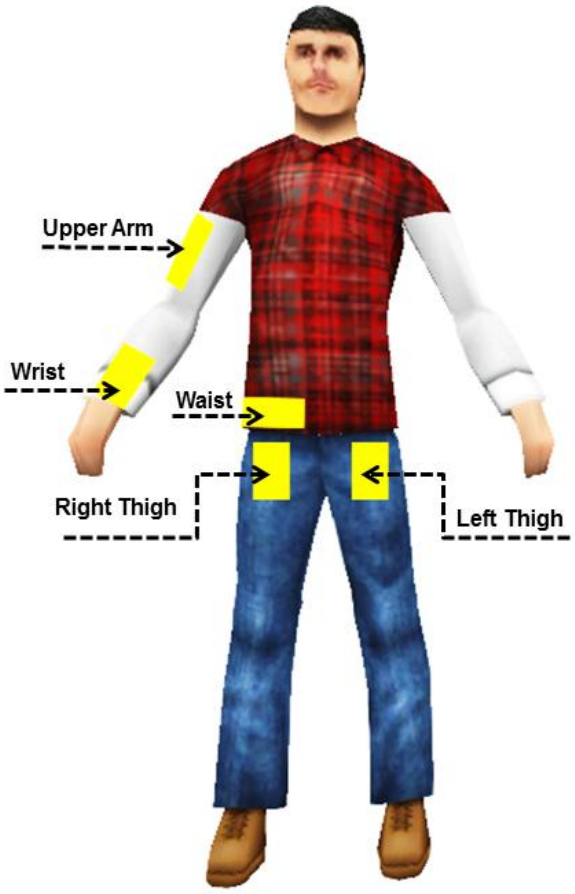

Fig. 2. Possible positions for the placement of smartphone on the user's body. A smartphone user is required to place his/her phone in one of these body positions to get identified according to the proposed scheme.

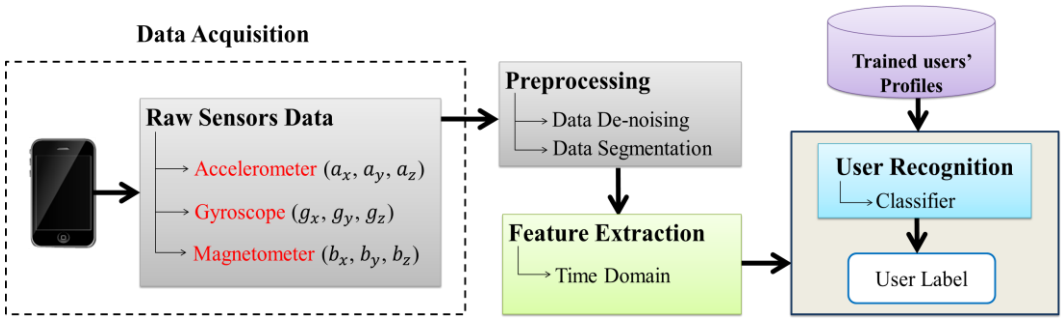

Fig. 3. Proposed scheme for smartphone user recognition

Table 2. Details of the dataset selected in this study for experimentation

Property	**Details**						
Activities	**Total**			**Activity names**			
	06	Walking	Sitting	Standing	Running	Walking upstairs	Walking downstairs
Actors	**Total**		**Gender**			**Age**	
	10		Male			25-30	
Activity duration	03 minutes per actor for a single position of smartphone on actor's body						
Smartphone positions	**Total**			**Position names**			
	05	Left pocket	Right pocket	Waist	Upper arm	Wrist	
Data collection device	Samsung Galaxy S-II (i9100) smartphones						
Sampling rate	50 Hz						
sensors	Accelerometer, Gyroscope, and Magnetometer						

3.1. Raw Data Collection : Dataset

To validate the proposed scheme, an existing dataset for physical activity recognition (Shoaib et al., 2013, 2014) was used. This dataset was selected because it was consistent to the pipeline of the proposed scheme. Table 2 describes the properties of this dataset. Three sensors were used for the purpose of data collection as shown in Table 2. The accelerometer was used to measure acceleration in meter per second square (m/s^2), the magnetometer was employed to report magnetic field in micro tesla (μT), and the gyroscope was used to measure the angular rotation in radians per second (rad/s) along each axis. The data collected from smartphone sensors had the form $\{a_x, a_y, a_z, g_x, g_y, g_z, b_x, b_y, b_z\} \in \mathbb{R}^9$, where 'a' and 'g' represent the acceleration, and rotation respectively whereas, 'b' represents the strength of the magnetic field along x, y and z axes.

3.2. Preprocessing : Data De-noising and Segmentation

Inertial sensors of the smartphone are sensitive to interferences such as noise. The signals acquired from these sensors are subjected to undesirable noise produced by unanticipated and vibrant movements of the participants. This noise corrupts useful information contained in the signal. Therefore, the removal of unwanted noise from the signal is necessary before further processing. In our case, the noisy data obtained from smartphone inertial sensors was de-noised using an average smoothing filter of size 1×3. Noise was removed from whole sample data by applying the averaging filter separately along all three dimensions of accelerometer, gyroscope, and magnetometer. As smartphone inertial sensors are orientation sensitive, therefore the magnitude

of the sensor that is independent of the sensor orientation was also concatenated with the existing three dimensions of each sensor. After adding fourth dimension, each sensor data was of the form (x, y, z, mag). For each sensor, magnitude is simply calculated as: $mag = \sqrt{x^2 + y^2 + z^2}$.

Before feature extraction from the preprocessed data, the sensors data was divided into smaller segments using a fixed-size sliding window. The selection of the length of sliding window is crucial as the final accuracy of recognition is affected by the length of the sliding window. Different researchers (Shoaib et al., 2013; Anjum and Ilyas, 2013) have shown that simple physical activity patterns can be recognized within 5 seconds duration. This led us to use a fixed-size slicing window having a length of 5 seconds in time with 250 samples at the rate 50 Hz. A 50% overlap was selected between the samples during the segmentation and the whole sensors data along each dimension was divided into small chunks of 5 seconds for feature extraction.

Table 3. A set of time domain features for user recognition

Features	**Formula**
Maximum Amplitude	$s_{max} = \max\{s(n)\}$
Minimum Amplitude	$s_{min} = \min\{s(n)\}$
Mean	$\mu = \frac{1}{N}\sum s(n)$
Variance	$\sigma^2 = \frac{1}{N}\sum (s(n) - \mu)^2$
Kurtosis	$K = (m_4/m_2^2)$, where m_2 and m_4 are the 2nd and 4th moment about the mean
Skewness	$S = (m_3)/\left(m_3^{\frac{3}{2}}\right)$, where m_3 is the 3rd moment about the mean
Energy	$E = \sum \lvert S(n)\rvert^2$
Entropy	$H(S(n)) = -\sum_{i=1}^{N} p_i(S(n))\ \log_2 p_i(S(n))$
Mean of Absolute Value of First Difference	$\mu_\nabla = \frac{1}{N}\sum \lvert s(n) - s(n-1)\rvert$
Mean of Absolute Value of Second Difference	$\mu_\Delta = \frac{1}{N}\sum \lvert s(n+1) - 2s(n) + s(n-1)\rvert$
Peak-to-Peak Signal Value	$s_{pp} = s_{max} - s_{min}$
Maximum Latency	$n_{s_{max}} = \{n \lvert s(n) = s_{max}\}$
Minimum Latency	$n_{s_{min}} = \{n \lvert s(n) = s_{min}\}$
Peak-to-Peak Time	$t_{pp} = n_{s_{max}} + n_{s_{min}}$
Peak-to-Peak Slope	$s_{pps} = \frac{s_{pp}}{t_{pp}}$
Absolute Latency to Amplitude Ratio	$ALAR = \left\lvert \frac{n_{s_{max}}}{s_{max}} \right\rvert$

3.3. Feature Extraction

Once the data was preprocessed, next step was to extract suitable features that can discriminate between the activity patterns of different users so that the users can be identified accurately. For this purpose, we selected sixteen different features from the time domain. Most of these features have been utilized by the earlier studies for physical activity recognition (Anjum and Ilyas, 2013; Incel et al., 2013; Shoaib et al., 2014, 2013; Su et al., 2014). These studies have demonstrated the excellent performance of these features for recognizing the activity patterns. First and second difference of the signal highlights the varying information in the signal and provides the edges and sharp changes in the signal. Similarly, maximum and minimum latency, peak-to-peak time, peak-to-peak slope, and latency to amplitude ratio also gives us useful information about the signal. Hence these features are useful descriptors of the signal and helpful in recognizing different activity patterns. Table 3 provides the details of the features selected in this study. All of these features were extracted for each partitioned data segment i.e., s[n], along all four channels of three sensors.

3.4. User Recognition

After feature extraction, next step was to choose a suitable classifier for the purpose of user recognition based on extracted features. In this work, different supervised machine learning approaches were used. As there were ten participants in the experiment, therefore the recognition of each individual participant was a multi-class classification problem. Three prevalent classifiers i.e., Support Vector Machine (SVM), Decision Tree and K-Nearest Neighbors (K-NN) were used to recognize individual users from their activity patterns. These classifiers were trained separately for different activity patterns of all the participants. The main reason for the selection of these classifiers was their efficient performance in existing studies pertinent to physical activity recognition (Anjum and Ilyas, 2013; Incel et al., 2013; Shoaib et al., 2014, 2013; Su et al., 2014). Moreover, we intended to provide a performance comparison of these classifiers for recognizing users from their activity patterns, which is given in Section 4. These classifiers are described in the following sections.

3.4.1. Decision Tree

Decision Tree (Kohavi, 1996) is a non-parametric supervised machine learning approach used for classification and regression. This approach aims to build up a model that envisages the value of a target variable by learning simple rules for decisions. These rules are deduced from the features extracted from the input data. Decision tree uses an if-then-else structure for making decisions about classification. It is computationally cheap with excellent interpretation, therefore it is considered as one of the key classifiers in numerous activity recognition studies (Su et al., 2014; Shoaib et al., 2013). The problem in using Decision Tree as a classifier lies in updating the already built model to accommodate new training samples as it might be very expensive (Su et al., 2014).

3.4.2. K-Nearest Neighbors

K-Nearest Neighbors (Guo et al., 2003) is an instance-based classifier, which is based on the majority voting of its neighbors (Peterson, 2009). It is one of the most commonly used algorithms for recognizing patterns. It works by assigning a feature vector extracted from the input data to a class according to its nearest neighbor(s). The neighbor can be a class prototype or a feature vector from the training set. The nearest neighbor is determined by calculating the distance between the feature vectors. It is a discriminative non-linear classifier. A number of distance measures can be used in K-NN classification like Chebyshev, Manhattan or Minkowski but Euclidean distance is usually the default measure used.

3.4.3. Support Vector Machine

Support Vector Machine (Cortes and Vapnik, 1995) is a non-probabilistic classifier that has successful applications in classification and regression. Support Vector Machine utilizes decision planes for outlining decision boundaries. A decision plane is capable of separating a set of objects with different class associations. Given a set of labeled training examples for the two classes, the training algorithm of SVM formulates a model that allocates new samples to one of the two classes. An SVM model denotes different examples as points in space, which are dispersed such that the examples pertaining to different classes are separated by a clear gap using support vectors. New examples are then mapped into the same space and assigned to a class depending upon which side of the gap they fall. SVM resists the overtraining problem and ultimately achieves a high generalization performance.

4. Experimental Results

In order to perform continuous authentication of smartphone users, the proposed scheme performed the recognition of activity patterns for individual users. Hence, the users were identified based on their activity patterns. The performance of the proposed scheme was evaluated using three different classifiers: SVM, DT, and KNN. These classifiers were trained and tested on the dataset for six activities. The dataset was pre-labeled for all six activities performed by ten different users. The users who performed these activities were labeled as well. It means that the ground truth was available for the activities as well as for the users performing those activities. So, our idea was to exploit the dataset for recognizing individual users from this labeled activity data. For this reason, we combined the data of all the users related to same activity at the same body position and assigned user labels to the data according to the ground truth. For example, the labeled data of the walking activity for a single body position was combined for all the participants and the user labels were assigned to the data. These user labels were representing the walking activity patterns of different participants. This process was repeated for each activity data for all body positions. It was done in order to train the selected classifiers for activity patterns of individual users. For every activity, the classifiers were trained for all five body positions separately to recognize ten different users. For this purpose, sixteen different features (as described in Table 3) were extracted for all four dimensions of accelerometer, gyroscope, and magnetometer. These sixteen features, extracted from four dimensions of three sensors, were concatenated into a single feature vector of size $16 \times 4 \times 3 = 192$ computed over a data segment of 5 seconds (250 samples with 50 Hz sampling rate) in time. As mentioned earlier, the duration of each activity data was 3 minutes (180 seconds), therefore using a 50% overlapping sliding window, total $\frac{180}{2.5} - 1 = 71$ feature vectors were computed related to each activity for a single body position. For total ten participants, 71 x 10 = 710 feature vectors were computed for each activity. The feature vectors computed for each activity were passed as input to the selected classifiers along with the user labels for classifiers training to recognize users from their activity patterns.

4.1. Evaluation Approach and Performance Metrics

To validate the performance of different classifiers, the data was divided into training and testing splits using k-fold cross validation scheme with k=10, and the classifiers were evaluated. For K-NN classifier, the nearest neighbor parameter K was set equal to 1 and Euclidean distance metric with equal weight was used for similarity measure. In case of DT classifier, the standard Classification and Regression Trees (CART) algorithm (Breiman et al., 1984) was used for creating the decision tree and the nodes were split using Gini's diversity index as a split criterion. A linear kernel was used for SVM classifier and one-vs-one multi-class method was used for classification. In Table 4, different performance metrics are given on the basis of which the performance of these classifiers was measured for user recognition. These performance measures are computed separately pertaining to each activity for five different body positions. .

Table 4. Performance metrics for evaluating classifiers performance for user recognition are: Accuracy (A), Precision (P), Recall (R), F-measure (F), and Error Rate (E). Here tp , tn , fp , and fn represent true positives, true negatives, false positives, and false negatives respectively.

Metric	Formula
Accuracy	$A = \frac{t_p + t_n}{t_p + t_n + f_p + f_n}$
Precision	$P = \frac{t_p}{t_p + f_p}$
Recall	$R = \frac{t_p}{t_p + f_n}$
F-measure	$F = 2\left(\frac{P \cdot R}{P + R}\right)$
Error Rate	$E = 1 - A$

4.2. Performance Analysis of User Recognition

This section provides the results of user recognition based on six selected activites. For every activity, the results are presented for five different positions of the smartphone on the user's body. To make a comparison between the classifiers performance in recognizing the users, the results are computed for each selected classifier i.e., DT, K-NN, and SVM. Table 5 to Table 10 summarizes the results of user recogntion based on walking, running, standing sitting, walking upstairs, and walking downstairs activity respectively. It can be observed from these tables that overall performance of SVM classifier is better than DT and K-NN classifiers in recognizing the users from their activity patterns.

Table 5. Performance measures of selected classifiers for user recognition based on *walking* activity

Classifier	Accuracy	Precision	Recall	F-measure	Error Rate	Phone Position
DT	0.989	0.989	0.989	0.989	0.011	
K-NN	0.989	0.989	0.989	0.989	0.011	Waist
SVM	0.996	0.996	0.996	0.996	0.004	
DT	0.966	0.966	0.966	0.966	0.034	
K-NN	0.976	0.976	0.976	0.976	0.024	Left Pocket
SVM	1	1	1	1	0	
DT	0.986	0.986	0.986	0.986	0.014	
K-NN	0.974	0.975	0.973	0.974	0.026	Right Pocket
SVM	1	1	1	1	0	
DT	0.945	0.946	0.945	0.946	0.055	
K-NN	0.973	0.973	0.973	0.973	0.027	Upper Arm
SVM	0.994	0.994	0.994	0.994	0.006	
DT	0.983	0.983	0.983	0.983	0.017	
K-NN	0.989	0.989	0.989	0.989	0.011	Wrist
SVM	0.994	0.994	0.994	0.994	0.006	

Table 6. Performance measures of selected classifiers for user recognition based on *running* activity

Classifier	Accuracy	Precision	Recall	F-measure	Error Rate	Phone Position
DT	0.982	0.982	0.982	0.982	0.018	
K-NN	0.972	0.972	0.972	0.972	0.028	Waist
SVM	0.997	0.997	0.997	0.997	0.003	
DT	0.972	0.972	0.972	0.972	0.0280	
K-NN	0.989	0.989	0.989	0.989	0.011	Left Pocket
SVM	0.999	0.999	0.999	0.999	0.001	
DT	0.966	0.967	0.966	0.967	0.034	
K-NN	0.983	0.983	0.983	0.983	0.017	Right Pocket
SVM	1	1	1	1	0	
DT	0.975	0.975	0.975	0.975	0.025	
K-NN	0.975	0.975	0.975	0.975	0.025	Upper Arm
SVM	0.993	0.993	0.993	0.993	0.007	
DT	0.963	0.963	0.963	0.963	0.037	
K-NN	0.975	0.975	0.975	0.975	0.025	Wrist

SVM	0.996	0.996	0.996	0.996	0.004	

369 **Table 7.** Performance measures of selected classifiers for user recognition based on *standing* activity

Classifier	Accuracy	Precision	Recall	F-measure	Error Rate	Phone Position
DT	0.990	0.991	0.990	0.990	0.010	
K-NN	0.879	0.880	0.879	0.880	0.121	Waist
SVM	0.994	0.994	0.994	0.994	0.006	
DT	0.975	0.975	0.975	0.975	0.025	
K-NN	0.766	0.770	0.766	0.768	0.234	Left Pocket
SVM	0.959	0.963	0.959	0.961	0.041	
DT	0.954	0.954	0.954	0.954	0.046	
K-NN	0.845	0.847	0.845	0.846	0.155	Right Pocket
SVM	0.966	0.967	0.966	0.967	0.034	
DT	0.951	0.951	0.951	0.951	0.049	
K-NN	0.734	0.755	0.734	0.744	0.266	Upper Arm
SVM	0.954	0.955	0.954	0.954	0.046	
DT	0.952	0.953	0.952	0.952	0.048	
K-NN	0.841	0.840	0.841	0.841	0.159	Wrist
SVM	0.970	0.970	0.970	0.970	0.030	

370 **Table 8.** Performance measures of selected classifiers for user recognition based on *sitting* activity

Classifier	Accuracy	Precision	Recall	F-measure	Error Rate	Phone Position
DT	0.991	0.991	0.991	0.991	0.009	
K-NN	0.811	0.817	0.811	0.814	0.189	Waist
SVM	0.989	0.989	0.989	0.989	0.010	
DT	0.992	0.992	0.992	0.992	0.008	
K-NN	0.904	0.906	0.904	0.905	0.096	Left Pocket
SVM	0.993	0.993	0.993	0.993	0.007	
DT	0.986	0.986	0.986	0.986	0.014	
K-NN	0.934	0.936	0.934	0.935	0.066	Right Pocket
SVM	0.992	0.992	0.992	0.992	0.008	
DT	0.955	0.955	0.955	0.955	0.045	
K-NN	0.844	0.849	0.844	0.846	0.156	Upper Arm
SVM	0.983	0.983	0.983	0.983	0.017	
DT	0.945	0.945	0.945	0.945	0.055	
K-NN	0.863	0.870	0.863	0.867	0.137	Wrist
SVM	0.968	0.968	0.968	0.968	0.032	

371 **Table 9.** Performance measures of selected classifiers for user recognition based on *walking upstairs* activity

Classifier	Accuracy	Precision	Recall	F-measure	Error Rate	Phone Position
DT	0.963	0.963	0.963	0.963	0.0370	Waist

K-NN	0.966	0.968	0.966	0.967	0.0340	
SVM	0.986	0.986	0.986	0.986	0.0140	
DT	0.903	0.905	0.903	0.904	0.0970	
K-NN	0.911	0.913	0.911	0.912	0.0890	Left Pocket
SVM	0.986	0.986	0.986	0.986	0.0140	
DT	0.901	0.903	0.901	0.902	0.0990	
K-NN	0.925	0.926	0.925	0.926	0.0750	Right Pocket
SVM	0.987	0.988	0.987	0.988	0.0130	
DT	0.858	0.865	0.858	0.861	0.142	
K-NN	0.883	0.891	0.883	0.887	0.117	Upper Arm
SVM	0.975	0.977	0.975	0.976	0.0250	
DT	0.862	0.865	0.862	0.864	0.138	
K-NN	0.858	0.860	0.858	0.859	0.142	Wrist
SVM	0.969	0.970	0.969	0.970	0.0310	

Table 10. Performance measures of selected classifiers for user recognition based on *walking downstairs* activity

Classifier	Average	Precision	Recall	F-measure	Error Rate	Phone Position
DT	0.911	0.914	0.911	0.912	0.0890	
K-NN	0.918	0.919	0.918	0.919	0.0820	Waist
SVM	0.952	0.954	0.952	0.953	0.0480	
DT	0.901	0.903	0.901	0.902	0.0990	
K-NN	0.877	0.888	0.877	0.883	0.123	Left Pocket
SVM	0.959	0.961	0.959	0.960	0.0410	
DT	0.904	0.905	0.904	0.904	0.0960	
K-NN	0.863	0.866	0.863	0.864	0.137	Right Pocket
SVM	0.965	0.968	0.965	0.966	0.035	
DT	0.811	0.820	0.811	0.815	0.189	
K-NN	0.813	0.818	0.813	0.815	0.187	Upper Arm
SVM	0.927	0.931	0.927	0.929	0.073	
DT	0.794	0.804	0.794	0.799	0.206	
K-NN	0.841	0.850	0.841	0.846	0.159	Wrist
SVM	0.937	0.937	0.937	0.937	0.063	

In case of walking activity, SVM classifier achieved an accuracy of 100% in recognizing the users when the smartphone was placed in their left jeans pocket or right jeans pocket. For the same activity, DT and K-NN classifiers achieved 96.6% and 97.6% accuracy for the left pocket position and an accuracy of 98.6% and 97.3% for the right pocket position respectively. The values of other performance metrics i.e., precision, recall, and f-measure were also better for SVM classifier. For the waist and wrist positions, SVM classifier achieved 99.6% accuracy. However, the recognition accuracies obtained for DT and K-NN classifiers are 98.9% for the waist position, and 98.9% and 98.3% for the wrist position respectively. The worst accuracy achieved by SVM, DT, and K-NN classifiers in recognizing users from walking activity is for upper arm position as shown in Table 5. These results state that recognizing users from their walking activity is easier if the phone is kept in their left or right pocket as compare to other positions. Keeping phone at upper arm position makes it difficult to recognize

a user based on walking pattern. The same thing can be said for identifying users on the basis of running activity as indicated by the results in Table 6.

On the basis of standing activity, the users are best recognized for the case when the smartphone was hanged with a belt clipper. The best accuracy rate achieved in this case is 99.4% for the waist position using SVM classifier. The accuracy rate obtained using DT and K-NN classifier for the same position is 99% and 87.6% respectively as given in Table 7. Table 8 shows that for sitting activity, the best accuracy rate achieved is 99.3% for the left pocket position using SVM classifier. On the other hand, DT and K-NN classifier achieved 99.2% and 90.4% accuracy for the left pocket position. The worst accuracy rate achieved by SVM for standing activity is 95.4% for the upper arm position, whereas in case of sitting activity it is 97% for the wrist position. These results depict that it is possible to identify a user based upon standing and sitting activities. In case of these two activities, the users are distinguished from each other because of the differences in their standing and sitting postures. This difference is detected by the inertial sensors of the smartphone placed on the user's body. The orientation of smartphone inertial sensors changes when a user stands or sits in a different pattern/posture as compare to other persons. Hence, the readings of these sensors change, which leads to identification of that user. From the results obtained from Table 7, it can be said that it is easier to recognize a user on the basis of his/her standing posture/stance if the smartphone is hanged near waist position. On the other hand, it is very hard to recognize the user if the smartphone is placed on the upper arm position. Similarly, results from Table 8 report that the identification of a user based on sitting activity is easier if the phone is placed in the jeans pocket as compare to other phone positions.

For the case of recognizing users from walking upstairs and walking downstairs activities also, the best results are also obtained using SVM classifier. The highest accuracy achieved for walking upstairs and walking downstairs activity is 98.7% and 96.5% respectively for the right pocket position using SVM classifier as shown in Table 9 and Table 10 respectively. The accuracy achieved by DT and K-NN classifier for walking upstairs activity is 90.1% and 92.5% respectively for the right pocket position. For downstairs activity for similar phone position, DT and K-NN classifiers attained an accuracy rate of 90.4% and 86.3% respectively. The results of these activities, i.e., walking upstairs and walking downstairs, obtained for the waist position are comparable to the results obtained for pocket positions as given in Table 9 and Table 10. Moreover, it can be observed from the results reported in these tables that upper arm and wrist position provides lower user recognition accuracies. Hence, it can be stated that the recognition of a user on the basis of walking upstairs and walking downstairs activity is easier if the smartphone is kept in pocket of the user or hanged at the waist position.

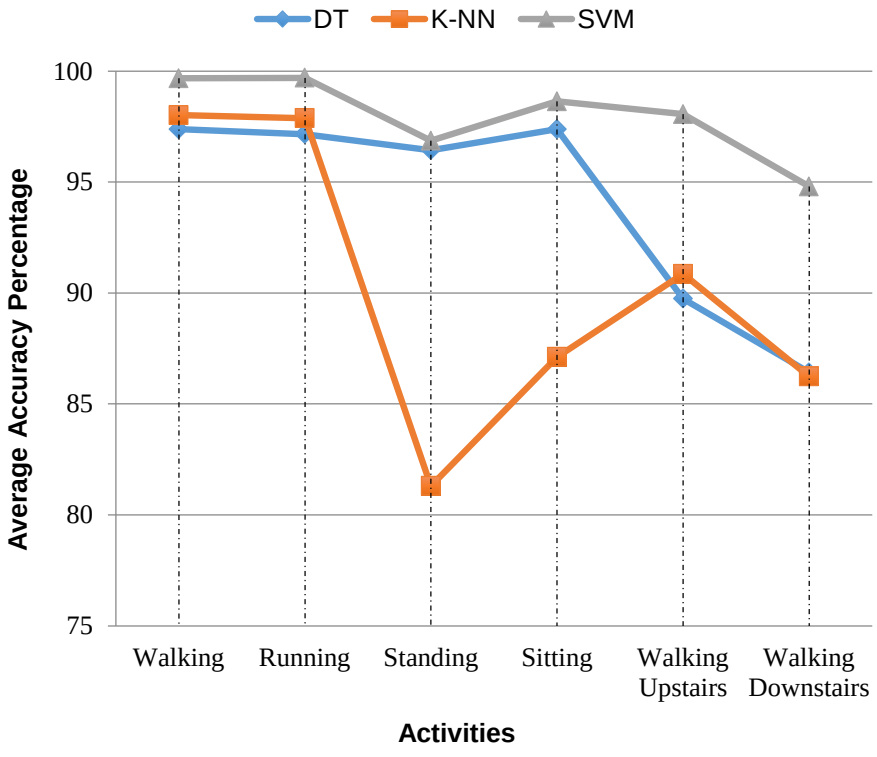

Fig. 4. Comparison of selected classifiers performance for user recognition based on six selected activities

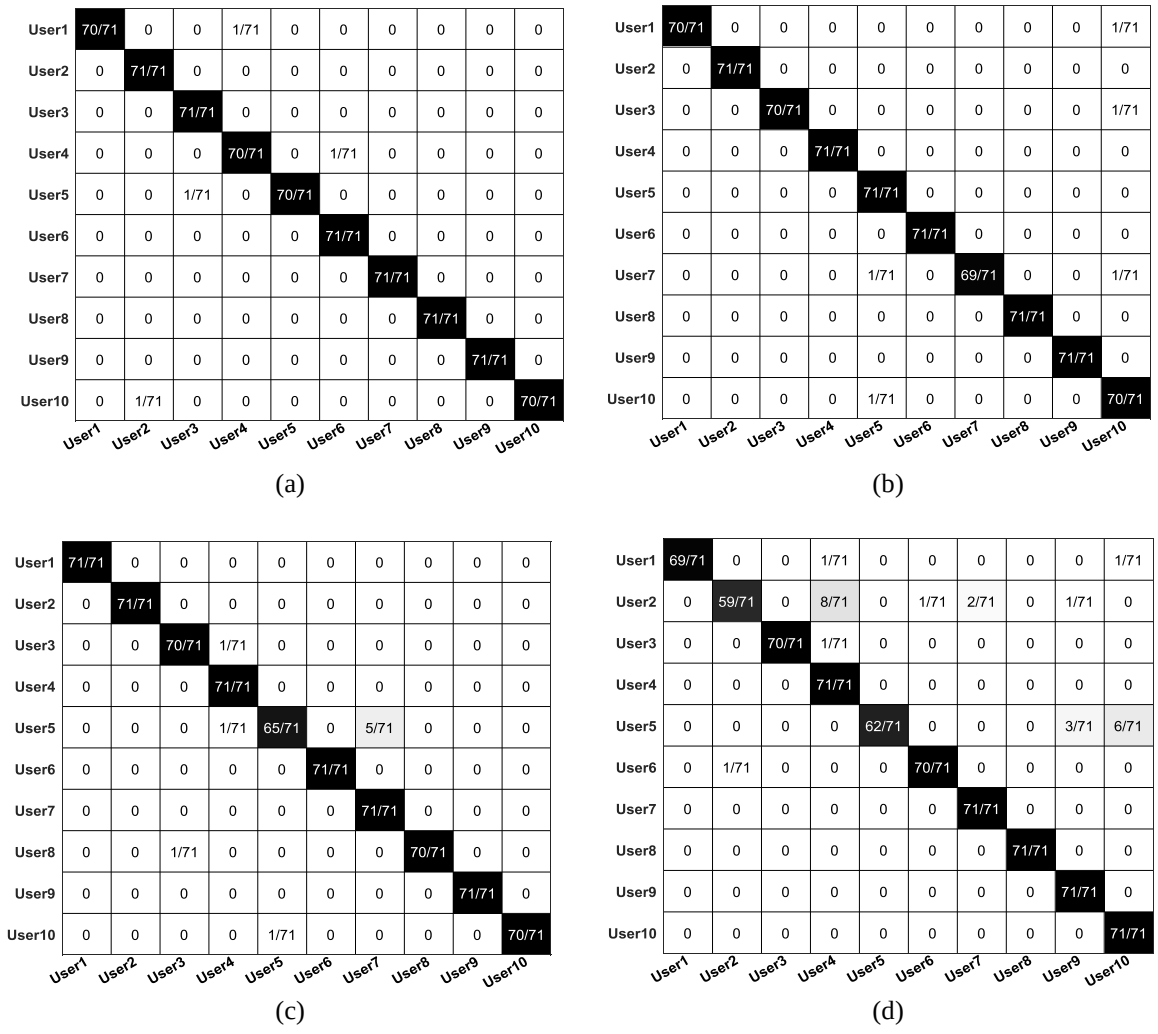

Fig. 5. Confusion matrices of user recognition (performed using SVM classifier) based on four different activities: (a) standing with phone at waist position, accuracy = 99.4%, (b) sitting with phone in left pocket position, accuracy = 99.3% (c) walking upstairs with phone in right pocket, accuracy = 98.7 (d) walking downstairs with phone in right pocket, accuracy = 96.5%.

Fig. 4 shows and compares the average accuracy rate achieved by the selected classifiers in recognizing the users on the basis of six different activities. For each activity, average accuracy percentage calculated over five body positions is shown in the figure. It can be observed that for all six activities, SVM classifier obtained the best average accuracy percentage for user recognition. The overall performance of K-NN classifier was better than DT classifier in recognizing the users based on walking, running and walking upstairs activities. For the remaining activities i.e., sitting, standing, walking downstairs, DT classifiers achieved better results than K-NN classifier. The overall average recognition accuracy achieved for SVM classifier is 97.95%, which is 3.87% and 7.72% more than the overall average accuracy obtained for DT and K-NN classifiers respectively. Moreover, the precision, recall, f-measure, and error rate are also better for SVM classifiers as depicted in Table 5 to Table 10. So, it can be concluded based on the above results and discussions that the performance of SVM classifier is better for user recognition based on activity patterns recognition. It suggests SVM classifier as the best choice for on-device user recognition based on recognizing the activity patterns for individual users.

To find out the best individual accuracies of recognition for different users, the confusion matrices for user recognition are provided in Fig. 5 ((a)-(d)). For every activity except walking and running, only one confusion matrix is shown for the position where the best performance metrics were achieved for user recognition using SVM classifier. In case walking and running activities, the best value of accuracy, precision, recall, and f-measure obtained for user recognition using SVM classifier is 100% for each (as shown in Table 5 and Table 6). It means that no user was misclassified or wrongly identified as any other user; hence the individual recognition accuracy achieved for every user is 100%. From Table 7 to Table 10, it is clear that for recognizing

a user based on the walking upstairs and walking downstairs activity, the best position to keep smartphone is the right jeans pocket. On the other hand, for standing and sitting activities, the best positions are waist and left pocket respectively. As discussed earlier, there were total 71 samples for all individual users corresponding to each activity for a single position. Therefore the confusion matrices in Fig. 5 ((a)-(d)) are presented in terms of recognized over total number of samples (i.e. 71) for the all the users. The rows of the confusion matrices are representing actual users while columns are representing the predicted users. It can be seen from Fig. 5 ((a)-(d)) that there are a few misclassifications where the actual user of the smartphone is identified as any other user. However, for each user, the value of correctly classified samples is very high. It means that every user is correctly identified with a very high accuracy. From these promising results, it is worth mentioning that it is possible to efficiently recognize different users on the basis of their activity patterns because of their behavioral differences.

Typically, there is only a single owner of a smartphone who is called as the authenticated user of that phone. The owner of the phone has full access to each and everything on his/her phone. However, a smartphone is not necessarily to be used by a single person only. An owner of a mobile device may share his/her phone with other people, who can use that phone for performing any of their tasks as allowed by the phone owner. All such users of the phone are supplementary users. The device owner may set different levels of access to his/her smartphone data and services for different supplementary users. Other than authenticated and supplementary users, any other user of the phone is treated as an impostor with no access given to phone data. To ensure the privacy of any confidential information and data stored on the owner phone, it is necessary to identify the phone user. The proposed system for user recognition identifies a user on the basis of his/her behavioral traits while using smartphone. Once the user is identified by the system, the system assigns the user a respective level of access privileges. The system can only identify a user on the basis of the activities for which the system is trained. In real time, if a user performs a random activity for which is unknown to the system, the system is improbable to be capable of identifying the user in an accurate way as there is no training of the system. However, the proposed system can be trained for the new activity by collecting raw data from the motion sensors of the smartphone. The system can then quickly learn the behavioral patterns of different users for the new activity and adapt itself to identify users based on new activity. In this way, adaptive behavioral authentication is also incorporated in the proposed system.

5. Conclusions

In this paper, we analyzed continuous authentication of smartphone users based on their behavioral traits using activity pattern recognition. For this purpose, we proposed a novel scheme for validating smartphone users, which identifies the users based on the way they perform certain activities using mobile sensing. Six activities of daily life i.e., walking, running, sitting, standing, walking upstairs, and walking downstairs, are used to distinguish between different users based on sixteen different features extracted from the time domain. For each activity, five different positions are employed for keeping a smartphone on the user's body and the user recognition results are analyzed for all these positions. It is noted that the performance of the user recognition based on a particular activity is different for varying positions of the smartphone on the user's body. A user can be easily and efficiently recognized on the basis of his/her walking pattern if the phone is placed in his/her jeans pocket. In contrast, keeping the phone at the upper arm position makes it very difficult to recognize a user based on the walking activity. Similarly, on the basis of standing posture, a user can be easily recognized if he/she keeps the phone at the waist position, whereas in case of sitting activity, the jeans pocket is the best place for user recognition. In the same way, the activities of walking upstairs and walking downstairs can easily distinguish between different users if the phone is kept in the jeans pocket or hanged with a belt clipper at the waist. Three different machine learning algorithms i.e., Decision Tree, K-Nearest Neighbors, and Support Vector Machine, are used for the purpose of user recognition. It is observed that Support Vector Machine classifier provides the best performance for on-device user identification. Hence, it is an ideal choice for on-device user identification based on activity pattern recognition.

To further extend this work, more sensors and activities can be incorporated into the system for recognizing users. Physiological sensors can be used along with the motion sensors for identity authentication. The emotional state of the users can also be recognized along with activity pattern recognition using physiological sensors. As the behavior of the user may change in a random way in different settings; hence an un-supervised machine learning approach can be used for user recognition, which will be helpful in adapting the system to random activity patterns. Contextual information is of very much importance while recognizing a user based on

his/her behavioral traits as the behavior of the user changes with different contexts. Hence, context-awareness can be incorporated into the system to efficiently recognize a smartphone user keeping in view the contextual information. Once a user is identified, we can keep track of his/her activities for health monitoring, social interaction monitoring, and behavior prediction and modeling.

References

Albert, M. V., Toledo, S., Shapiro, M., Kording, K., 2012. Using mobile phones for activity recognition in Parkinson's patients. Front. Neurol. NOV. doi:10.3389/fneur.2012.00158

Alzubaidi, A., Kalita, J., 2016. Authentication of smartphone users using behavioral biometrics. IEEE Commun. Surv. Tutorials 18, 1998–2026. doi:10.1109/COMST.2016.2537748

Anguita, D., Ghio, A., Oneto, L., Parra, X., Reyes-Ortiz, J.L., 2013. A Public Domain Dataset for Human Activity Recognition Using Smartphones, in: 21th European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, ESANN 2013.

Anjum, A., Ilyas, M.U., 2013. Activity recognition using smartphone sensors, in: 2013 IEEE 10th Consumer Communications and Networking Conference, CCNC 2013. pp. 914–919. doi:10.1109/CCNC.2013.6488584

Avci, A., Bosch, S., Marin-Perianu, M., Marin-Perianu, R., Havinga, P., 2010. Activity Recognition Using Inertial Sensing for Healthcare, Wellbeing and Sports Applications: A Survey. Archit. Comput. Syst. (ARCS), 2010 23rd Int. Conf. 1–10.

Breiman, L., Friedman, J.H., Olshen, R.A., Stone, C.J., 1984. Classification and Regression Trees, The Wadsworth statisticsprobability series. doi:10.1371/journal.pone.0015807

Bulling, A., Blanke, U., Schiele, B., 2014. A tutorial on human activity recognition using body-worn inertial sensors. ACM Comput. Surv. 1, 1–33. doi:http://dx.doi.org/10.1145/2499621

Buriro, A., Crispo, B., Zhauniarovich, Y., 2017. Please hold on: Unobtrusive user authentication using smartphone's built-in sensors, in: 2017 IEEE International Conference on Identity, Security and Behavior Analysis, ISBA 2017. doi:10.1109/ISBA.2017.7947684

Camara, C., Peris-Lopez, P., Tapiador, J.E., 2015. Human Identification Using Compressed ECG Signals. J. Med. Syst. 39. doi:10.1007/s10916-015-0323-2

Chatzimilioudis, G., Konstantinidis, A., Laoudias, C., Zeinalipour-Yazti, D., 2012. Crowdsourcing with smartphones. IEEE Internet Comput. 16, 36–44. doi:10.1109/MIC.2012.70

Cho, K.S., Lee, J.M., 2017. Influence of smartphone addiction proneness of young children on problematic behaviors and emotional intelligence: Mediating self-assessment effects of parents using smartphones. Comput. Human Behav. 66, 303–311. doi:10.1016/j.chb.2016.09.063

Cola, G., Avvenuti, M., Musso, F., Vecchio, A., 2016. Gait-based authentication using a wrist-worn device, in: Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services - MOBIQUITOUS 2016. pp. 208–217. doi:10.1145/2994374.2994393

Consolvo, S., McDonald, D.W., Toscos, T., Chen, M.Y., Froehlich, J., Harrison, B., Klasnja, P., LaMarca, A., LeGrand, L., Libby, R., Smith, I., Landay, J.A., 2008. Activity Sensing in the Wild: A Field Trial of UbiFit Garden. Chi 2008 26Th Annu. Chi Conf. Hum. Factors Comput. Syst. Vols 1 2, Conf. Proc. 1797–1806. doi:10.1145/1357054.1357335

Cortes, C., Vapnik, V., 1995. Support-Vector Networks. Mach. Learn. 20, 273–297. doi:10.1023/A:1022627411411

Damaševičius, R., Maskeliunas, R., Venčkauskas, A., Woźniak, M., 2016. Smartphone user identity verification using gait characteristics. Symmetry (Basel). 8. doi:10.3390/sym8100100

534 Derawi, M.O., Nickely, C., Bours, P., Busch, C., 2010. Unobtrusive user-authentication on mobile phones using
535 biometric gait recognition, in: Proceedings - 2010 6th International Conference on Intelligent Information
536 Hiding and Multimedia Signal Processing, IIHMSP 2010. pp. 306–311. doi:10.1109/IIHMSP.2010.83
537 Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes.
538 http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101 (accessed on 30.01.
539 2018)
540 Ellis, K., Godbole, S., Chen, J., Marshall, S., Lanckriet, G., Kerr, J., 2013. Physical activity recognition in
541 free-living from body-worn sensors, in: Proceedings of the 4th International SenseCam & Pervasive
542 Imaging Conference on - SenseCam '13. pp. 88–89. doi:10.1145/2526667.2526685
543 Feng, T., Zhao, X., Carbunar, B., Shi, W., 2013. Continuous mobile authentication using virtual key typing
544 biometrics, in: Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in
545 Computing and Communications, TrustCom 2013. pp. 1547–1552. doi:10.1109/TrustCom.2013.272
546 Fernandez-Lopez, P., Liu-jimenez, J., Sanchez-Redondo, C., Sanchez-reillo, R., 2016. Gait Recognition Using
547 Smartphone. Carnahan 8. doi:10.1109/CCST.2016.7815698
548 Frank, M., Biedert, R., Ma, E., Martinovic, I., Song, D., 2013. Touchalytics: On the applicability of touchscreen
549 input as a behavioral biometric for continuous authentication. IEEE Trans. Inf. Forensics Secur. 8, 136–
550 148. doi:10.1109/TIFS.2012.2225048
551 Gartner, 2017. Gartner Says Worldwide Device Shipments Will Increase 2 Percent in 2018, Reaching Highest
552 Year-Over-Year Growth Since 2015. http://www.gartner.com/newsroom/id/3816763 (accessed on
553 30.01.2018)
554 Gesell, S.B., Barkin, S.L., Valente, T.W., 2013. Social network diagnostics: A tool for monitoring group
555 interventions. Implement. Sci. 8. doi:10.1186/1748-5908-8-116
556 Guo, G., Wang, H., Bell, D., Bi, Y., Greer, K., 2003. kNN Model-Based Approach in Classification. Move to
557 Meaningful Internet Syst. 2003 CoopIS, DOA, ODBASE 2888, 986–996. doi:10.1007/b94348
558 Harari, G.M., Lane, N.D., Wang, R., Crosier, B.S., Campbell, A.T., Gosling, S.D., 2016. Using Smartphones to
559 Collect Behavioral Data in Psychological Science: Opportunities, Practical Considerations, and
560 Challenges. Perspect. Psychol. Sci. 11, 838–854. doi:10.1177/1745691616650285
561 Hejazi, M., Al-Haddad, S.A.R., Singh, Y.P., Hashim, S.J., Abdul Aziz, A.F., 2016. ECG biometric
562 authentication based on non-fiducial approach using kernel methods. Digit. Signal Process. 52, 72–86.
563 doi:10.1016/j.dsp.2016.02.008
564 Hoseini-Tabatabaei, S.A., Gluhak, A., Tafazolli, R., 2013. A survey on smartphone-based systems for
565 opportunistic user context recognition. ACM Comput. Surv. 45, 1–51. doi:10.1145/2480741.2480744
566 Incel, O.D., Kose, M., Ersoy, C., 2013. A Review and Taxonomy of Activity Recognition on Mobile Phones.
567 Bionanoscience 3, 145–171. doi:10.1007/s12668-013-0088-3
568 Kang, S.J., Lee, S.Y., Cho, H. Il, Park, H., 2016. ECG Authentication System Design Based on Signal Analysis
569 in Mobile and Wearable Devices. IEEE Signal Process. Lett. 23, 805–808.
570 doi:10.1109/LSP.2016.2531996
571 Khan, W.Z., Xiang, Y., Aalsalem, M.Y., Arshad, Q., 2013. Mobile Phone Sensing Systems: A Survey. IEEE
572 Commun. Surv. Tutorials 15, 402–427. doi:10.1109/SURV.2012.031412.00077
573 Kohavi, R., 1996. Scaling Up the Accuracy of Naive-Bayes Classifiers: A Decision-Tree Hybrid. Proc. Second
574 Int. Conf. Knowl. Discov. Data Min. 7, 202–207. doi:citeulike-article-id:3157868
575 Krupp, B., Sridhar, N., Zhao, W., 2017. SPE: Security and Privacy Enhancement Framework for Mobile
576 Devices. IEEE Trans. Dependable Secur. Comput. 14, 433–446. doi:10.1109/TDSC.2015.2465965

577 Kwapisz, J., Weiss, G., Moore, S., 2011. Activity recognition using cell phone accelerometers. ACM SIGKDD
578 Explor. … 12, 74–82. doi:10.1145/1964897.1964918
579 Lara, O.D., Labrador, M. a., 2013. A Survey on Human Activity Recognition using Wearable Sensors. IEEE
580 Commun. Surv. Tutorials 15, 1192–1209. doi:10.1109/SURV.2012.110112.00192
581 Lee, Y.-G., Jeong, W.S., Yoon, G., 2012. Smartphone-Based Mobile Health Monitoring. Telemed. e-Health 18,
582 585–590. doi:10.1089/tmj.2011.0245
583 Lockhart, J.W., Pulickal, T., Weiss, G.M., 2012. Applications of mobile activity recognition. Proc. 2012 ACM
584 Conf. Ubiquitous Comput. - UbiComp '12 1054. doi:10.1145/2370216.2370441
585 Mäntyjärvi, J., Lindholm, M., Vildjiounaite, E., Mäkelä, S.M., Ailisto, H., 2005. Identifying users of portable
586 devices from gait pattern with accelerometers, in: ICASSP, IEEE International Conference on Acoustics,
587 Speech and Signal Processing - Proceedings. doi:10.1109/ICASSP.2005.1415569
588 Mayron, L.M., 2015. Biometric Authentication on Mobile Devices. IEEE Secur. Priv. 13, 70–73.
589 doi:10.1109/MSP.2015.67
590 Meng, W., Li, W., Wong, D.S., Zhou, J., 2016. TMGuard: A touch movement-based security mechanism for
591 screen unlock patterns on smartphones, in: Lecture Notes in Computer Science (Including Subseries
592 Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 629–647.
593 doi:10.1007/978-3-319-39555-5_34
594 Miluzzo, E., Cornelius, C.T., Ramaswamy, A., Choudhury, T., Liu, Z., Campbell, A.T., 2010. Darwin Phones :
595 the Evolution of Sensing and Inference on Mobile Phones. Darwin 14, 5–20.
596 doi:10.1145/1814433.1814437
597 Miluzzo, E., Lane, N.D., Fodor, K., Peterson, R., Lu, H., Musolesi, M., Eisenman, S.B., Zheng, X., Campbell,
598 a T., 2008. Sensing meets mobile social networks: the design, implementation and evaluation of the
599 cenceme application. Proc. 6th ACM Conf. Embed. Netw. Sens. Syst. 337–350.
600 doi:10.1145/1460412.1460445
601 Min, J.-K., Wiese, J., Hong, J.I., Zimmerman, J., 2013. Mining smartphone data to classify life-facets of social
602 relationships, in: Proceedings of the 2013 Conference on Computer Supported Cooperative Work -
603 CSCW '13. p. 285. doi:10.1145/2441776.2441810
604 Mun, M., Boda, P., Reddy, S., Shilton, K., Yau, N., Burke, J., Estrin, D., Hansen, M., Howard, E., West, R.,
605 2009. PEIR, the personal environmental impact report, as a platform for participatory sensing systems
606 research. Proc. 7th Int. Conf. Mob. Syst. Appl. Serv. - Mobisys '09 55. doi:10.1145/1555816.1555823
607 Neverova, N., Wolf, C., Lacey, G., Fridman, L., Chandra, D., Barbello, B., Taylor, G., 2016. Learning Human
608 Identity from Motion Patterns. IEEE Access 4, 1810–1820. doi:10.1109/ACCESS.2016.2557846
609 Otebolaku, A.M., Andrade, M.T., 2016. User context recognition using smartphone sensors and classification
610 models. J. Netw. Comput. Appl. 66, 33–51. doi:10.1016/j.jnca.2016.03.013
611 Papadopoulos, A., Nguyen, T., Durmus, E., Memon, N., 2017. IllusionPIN: Shoulder-Surfing Resistant
612 Authentication Using Hybrid Images. IEEE Trans. Inf. Forensics Secur. 12, 2875–2889.
613 doi:10.1109/TIFS.2017.2725199
614 Pei, L., Guinness, R., Chen, R., Liu, J., Kuusniemi, H., Chen, Y., Chen, L., Kaistinen, J., 2013. Human behavior
615 cognition using smartphone sensors. Sensors (Switzerland) 13, 1402–1424. doi:10.3390/s130201402
616 Peterson, L., 2009. K-nearest neighbor. Scholarpedia 4, 1883. doi:10.4249/scholarpedia.1883
617 Pludwinski, S., Ahmad, F., Wayne, N., Ritvo, P., 2016. Participant experiences in a smartphone-based health
618 coaching intervention for type 2 diabetes: A qualitative inquiry. J. Telemed. Telecare 22, 172–178.
619 doi:10.1177/1357633X15595178

San-Segundo, R., Cordoba, R., Ferreiros, J., D'Haro-Enríquez, L.F., 2016. Frequency features and GMM-UBM approach for gait-based person identification using smartphone inertial signals. Pattern Recognit. Lett. 73, 60–67. doi:10.1016/j.patrec.2016.01.008

Shahzad, M., Liu, A.X., Samuel, A., 2013. Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures – You can see it but you can not do it. Proc. of MobiCom 39. doi:10.1145/2500423.2500434

Shen, C., Yu, T., Yuan, S., Li, Y., Guan, X., 2016. Performance analysis of motion-sensor behavior for user authentication on smartphones. Sensors (Switzerland) 16. doi:10.3390/s16030345

Shoaib, M., Bosch, S., Durmaz Incel, O., Scholten, H., Havinga, P.J.M., 2014. Fusion of smartphone motion sensors for physical activity recognition. Sensors (Switzerland) 14, 10146–10176. doi:10.3390/s140610146

Shoaib, M., Bosch, S., Incel, O., Scholten, H., Havinga, P., 2015a. A Survey of Online Activity Recognition Using Mobile Phones. Sensors 15, 2059–2085. doi:10.3390/s150102059

Shoaib, M., Bosch, S., Incel, O.D., Scholten, H., Havinga, P.J.M., 2016. Complex human activity recognition using smartphone and wrist-worn motion sensors. Sensors (Switzerland) 16. doi:10.3390/s16040426

Shoaib, M., Bosch, S., Scholten, H., Havinga, P.J.M., Incel, O.D., 2015b. Towards detection of bad habits by fusing smartphone and smartwatch sensors, in: 2015 IEEE International Conference on Pervasive Computing and Communication Workshops, PerCom Workshops 2015. pp. 591–596. doi:10.1109/PERCOMW.2015.7134104

Shoaib, M., Scholten, H., Havinga, P.J.M., 2013. Towards Physical Activity Recognition Using Smartphone Sensors. 2013 IEEE 10th Int. Conf. Ubiquitous Intell. Comput. 2013 IEEE 10th Int. Conf. Auton. Trust. Comput. 80–87. doi:10.1109/UIC-ATC.2013.43

Shrestha, B., Saxena, N., Harrison, J., 2013. Wave-to-access: Protecting sensitive mobile device services via a hand waving gesture, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 199–217. doi:10.1007/978-3-319-02937-5_11

Sitova, Z., Sedenka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P., Balagani, K.S., 2016. HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users. IEEE Trans. Inf. Forensics Secur. 11, 877–892. doi:10.1109/TIFS.2015.2506542

Song, C., Wang, A., Ren, K., Xu, W., 2016. EyeVeri: A secure and usable approach for smartphone user authentication, in: Proceedings - IEEE INFOCOM. doi:10.1109/INFOCOM.2016.7524367

Spreitzer, R., Moonsamy, V., Korak, T., Mangard, S., 2016. SoK: Systematic Classification of Side-Channel Attacks on Mobile Devices. arXiv1611.03748 [cs].

Su, X., Tong, H., Ji, P., 2014. Activity recognition with smartphone sensors. Tsinghua Sci. Technol. 19, 235–249. doi:10.1109/TST.2014.6838194

The Statistics Portal. http://www.statista.com/statistics/274774/forecast-of-mobile- phone-users-worldwide (accessed on 30.01. 2018)

Trojahn, M., Ortmeier, F., 2013. Toward mobile authentication with keystroke dynamics on mobile phones and tablets, in: Proceedings - 27th International Conference on Advanced Information Networking and Applications Workshops, WAINA 2013. pp. 697–702. doi:10.1109/WAINA.2013.36

van Deursen, A.J. a. M., Bolle, C.L., Hegner, S.M., Kommers, P. a. M., 2015. Modeling habitual and addictive smartphone behavior. Comput. Human Behav. 45, 411–420. doi:10.1016/j.chb.2014.12.039

Wakabayashi, N., Kuriyama, M., Kanai, A., 2017. Personal authentication method against shoulder-surfing attacks for smartphone, in: 2017 IEEE International Conference on Consumer Electronics, ICCE 2017.

663 pp. 153–155. doi:10.1109/ICCE.2017.7889266
664 Wannenburg, J., Malekian, R., 2016. Physical Activity Recognition From Smartphone Accelerometer Data for
665 User Context Awareness Sensing. IEEE Trans. Syst. Man, Cybern. Syst. 1–8.
666 doi:10.1109/TSMC.2016.2562509
667 Wu, J.S., Lin, W.C., Lin, C.T., Wei, T.E., 2016. Smartphone continuous authentication based on keystroke and
668 gesture profiling, in: Proceedings - International Carnahan Conference on Security Technology. pp. 191–
669 197. doi:10.1109/CCST.2015.7389681
670 Yang, L., Guo, Y., Ding, X., Han, J., Liu, Y., Wang, C., Hu, C., 2015. Unlocking Smart Phone through
671 Handwaving Biometrics. IEEE Trans. Mob. Comput. 14, 1044–1055. doi:10.1109/TMC.2014.2341633
672 Yang, Z., Shangguan, L., Gu, W., Zhou, Z., Wu, C., Liu, Y., 2014. Sherlock: Micro-environment sensing for
673 smartphones. IEEE Trans. Parallel Distrib. Syst. 25, 3295–3305. doi:10.1109/TPDS.2013.2297309
674 Zeng, Y., 2016. Ph.D. Forum Abstract: Activity-Based Implicit Authentication for Wearable Devices, in: 2016
675 15th ACM/IEEE International Conference on Information Processing in Sensor Networks, IPSN 2016 -
676 Proceedings. doi:10.1109/IPSN.2016.7460684
677 Zhang, Y., Pan, G., Jia, K., Lu, M., Wang, Y., Wu, Z., 2015. Accelerometer-Based Gait Recognition by Sparse
678 Representation of Signature Points with Clusters. IEEE Trans. Cybern. 45, 1864–1875.
679 doi:10.1109/TCYB.2014.2361287
680 Zheng, N., Bai, K., Huang, H., Wang, H., 2014. You are how you touch: User verification on smartphones via
681 tapping behaviors, in: Proceedings - International Conference on Network Protocols, ICNP. pp. 221–232.
682 doi:10.1109/ICNP.2014.43
683 Zhitomirsky-Geffet, M., Blau, M., 2016. Cross-generational analysis of predictive factors of addictive behavior
684 in smartphone usage. Comput. Human Behav. 64, 682–693. doi:10.1016/j.chb.2016.07.061
685 Zhu, H., Hu, J., Chang, S., Lu, L., 2017. ShakeIn: Secure User Authentication of Smartphones with
686 Single-Handed Shakes. IEEE Trans. Mob. Comput. 16, 2901–2912. doi:10.1109/TMC.2017.2651820

687