Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 113 (2017) 202–209

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017)

# Identifying Smartphone Users based on their Activity Patterns via Mobile Sensing

M. Ehatisham-ul-Haq[a], Muhammad Awais Azam[a,]*, Usman Naeem[b], Shafiq ur Rèhman[b,c], Asra Khalid[d]

[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, E16 2RD, United Kingdom*
[c]*Department of Applied Physics and Electronics, Umeå University, SE-90187, Sweden*
[d]*Department of Computer Science, COMSATS Institute of Information Technology, Wah Campus, Pakistan*

## Abstract

Smartphones are ubiquitous devices that enable users to perform many of their routine tasks anytime and anywhere. With the advancement in information technology, smartphones are now equipped with sensing and networking capabilities that provide context-awareness for a wide range of applications. Due to ease of use and access, many users are using smartphones to store their private data, such as personal identifiers and bank account details. This type of sensitive data can be vulnerable if the device gets lost or stolen. The existing methods for securing mobile devices, including passwords, PINs and pattern locks are susceptible to many bouts such as smudge attacks. This paper proposes a novel framework to protect sensitive data on smartphones by identifying smartphone users based on their behavioral traits using smartphone embedded sensors. A series of experiments have been conducted for validating the proposed framework, which demonstrate its effectiveness.

*Keywords:* Activity Recognition; Behavioral Biometrics; Continuous Sensing; Mobile Device Security; Data Privacy; Mobile Sensing; Ubiquitous Computing; User Identification;

## 1. Introduction

Smartphones are context-aware devices that are becoming more and more dominant with ever-growing computing, sensing and networking capabilities. They provide ubiquity and assist users in accomplishing their daily

* Muhammad Awais Azam. Ph: +92-312-5151200
*E-mail address:* awais.azam@uettaxila.edu.pk

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.08.349

routine tasks, including sending and receiving e-mails, playing games and socializing anytime and anywhere. The pervasiveness of smartphones has changed the entire structure of people's everyday lives even users with disabilities[1,2]. Market research on usage of smartphones depicts that the number of smartphones sold has surpassed the number of laptops sold worldwide[3]. Instead of using personal computers, people are now using smartphones for storing most of their personal data so that it can be accessed effortlessly at anytime and anywhere when required. With the progress in usage of smartphones, users have become anxious about the secrecy of their data and information available through these devices. Unfortunately, most widely used methods for protecting smartphones such as passwords, PINs, patterns locks and fingerprint scans provide limited security. They are exposed to many attacks, such as guessing[4] (passwords and PINs), spoofing[5] (fingerprint scans) and side channel attacks such as video capture[6], reflection[7] and smudge attacks[8]. They prompt users to deal with the device actively for entering some pieces of information for validation, which frustrates user. Also, these approaches are futile to use after login because of their failure in detecting and recognizing a user once he/she has passed the point of entry[9]. Therefore, it has become critical to find out viable solutions for these challenges to protect sensitive data available through these devices. Continuous and passive mobile sensing offers a way to use behavioral biometrics to identify a smartphone user continuously[11]. Behavioral biometrics schemes aim to identify the characteristics of a user behavior that possess a definite pattern over a period such as hand movements and waving patterns[13], voice[14], signature[15], touchscreen interactions[16] and gait patterns[17]. The major issues in developing a continuous mobile sensing system for identifying smartphone users are as follows:

- Orientation sensitivity of smartphone inertial sensors as shown in Fig. 1
- Efficiently learning activity patterns from noisy data
- Incorporating sensor data into a biometric authentication setup on a smartphone
- Adaption of the user identification model to a new user in real-time

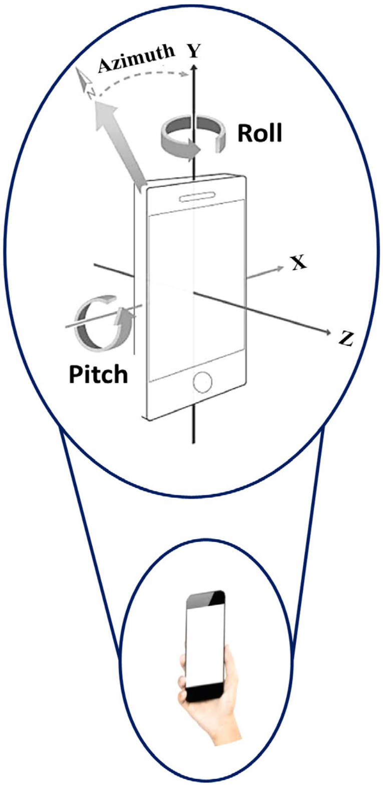

Fig. 1. Smartphone inertial sensors are orientation sensitive. The axes of the smartphone inertial sensors change their directions if the orientation of the smartphone is changed. Hence, the readings of these sensors are different for varying orientations of the smartphone.

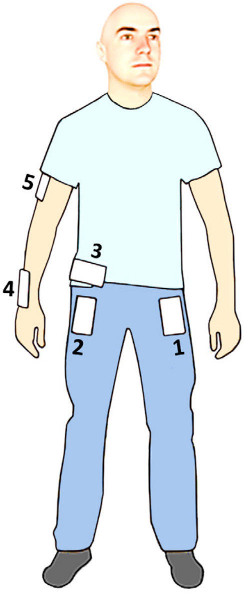

Fig. 2. Five positions are selected in this study for placing a smartphone on human body while performing an activity. These body positions include: (1) Left Thigh, (2) Right Thigh, (3) Waist, (4) Wrist, and (5) Upper Arm.

Keeping in view all these challenges, the problem of continuous and passive identification of smartphone users is addressed in this study, and a novel framework is proposed for smartphone user identification based on physical activity recognition. The objective is to recognize users by learning their behavioral patterns for different activities while interacting with the smartphone. For this purpose, six activities of daily living (ADL) are considered in this study, which include walking, sitting, standing, running, walking upstairs and walking downstairs. Three smartphone sensors (accelerometer, gyroscope and magnetometer) are used for capturing data of users while performing these activities. The position of a smartphone on human body is not always fixed and usually varies in real time while performing any activity. Therefore, five different positions are considered for the placement of a smartphone on human body while performing the activities selected in the study. These body positions include right wrist, right upper arm, left thigh, right thigh and waist position towards right leg as shown in Fig. 2. The smartphone is assumed to be found in one of these positions while performing any activity. An existing dataset for physical activity recognition[18,19] has been used for this study. The data is preprocessed and several features are extracted from it, which are further utilized by three different machine learning algorithms i.e., K-Nearest Neighbor (K-NN), Bayes Net (BN) and Support Vector Machine (SVM) for identifying different users based on their activity patterns.

## 2. Related Work

With the advancement in computing and sensing capabilities of smartphones and mobile devices, researchers have started to make use of different types of sensory data available through these devices for a wide range of purposes. Smartphone sensors have been enormously utilized for activity recognition[17,18,19,20]. In an existing study[24], the authors used smartphone sensors along with wrist-mounted motion sensors for identifying complex human activities such as smoking, eating, drinking etc. Activity recognition has been utilized for detecting bad habits in a person using smart-watch sensors along with smartphone embedded sensors[25]. Numerous schemes have been proposed for validating and identifying smartphone users based on behavioral biometrics using smartphone sensing. In an existing study[21], the authors identified users based on their walking patterns using accelerometer. OpenSesame[13], a new authentication approach, locks and unlocks a smartphone based on the user's hand waving patterns. Draffin et al. proposed KeySens[10], an approach that authenticates a user by learning the user's behavior while interacting with the device keyboard. Frank et al.[12] and Zheng et al.[16] discussed the use of touchscreen input as a behavioral biometric for smartphone users' authentication.

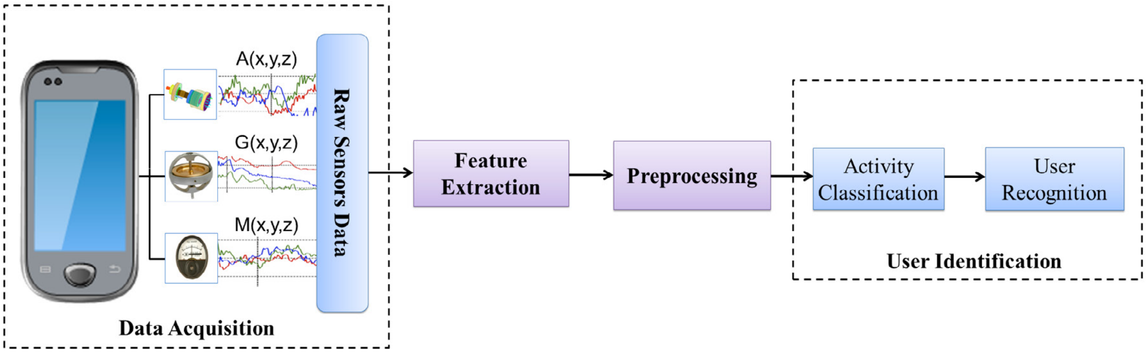

Fig. 3. Proposed methodology for identifying smartphone users.

The existing work on smartphone users' identification and authentication has certain limitations. Gait or walking pattern of a person may vary by wearing different footwear, which can lead to incorrect user identification. Also, the typing patterns of a user vary considerably during a day with his/her state of mind such as sad, happy, excited etc. Moreover, an extensive time is required to learn keystroke and touchscreen interaction patterns for new users. Owing to these limitations, these approaches are futile to use for continuous and passive authentication of a smartphone user in real time.

## 3. Methodology

The proposed methodology for identifying smartphone users based on their behavioral traits consists of four steps as shown in Fig. 3. These steps include: data acquisition, preprocessing, feature extraction and user identification.

### *3.1. Data Acquisition*

To conduct the experiments for user identification according to the proposed scheme, an existing dataset for physical activity recognition[18,19] was used. The dataset contained data of 10 participants for six different physical activities including walking, sitting, standing, running, walking upstairs and walking downstairs. Each activity was performed by a participant for 3-5 minutes. All participants were male, aged between 25 and 30. Three smartphone sensors (accelerometer, gyroscope and magnetometer) were used to collect data at a sampling rate of 50 Hz.

### *3.2. Preprocessing*

The data collected from the smartphone inertial sensors also contained unwanted noise generated from the participants and the sensors themselves. To mitigate the effect of unwanted noise from the sensors data, an average smoothing filter was applied on the recorded data along every axis. The orientation sensitivity of smartphone inertial sensors influences the performance of recognition algorithms because readings of these sensors change by changing the orientation of smartphone[22] as shown in Fig. 1. To overcome this issue, a fourth dimension i.e., magnitude, was added to the existing three dimensions of each sensor as the magnitude of a vector is not sensitive to its direction.

### *3.3. Feature Extraction*

For feature extraction, a fixed-width sliding window of 5 seconds in time (250 samples at 50 Hz sampling rate) with 50% overlap between the samples was selected for dividing whole sensors data along every axis into small segments. After data segmentation, eight different features from both time and frequency domains, were extracted for each partitioned data segment. These features are given in Table 1. Only two features i.e., energy and entropy, are extracted from frequency domain because of the high computational complexity of Fourier Transform as discussed in existing studies[18,20,22].

### *3.4. User Identification*

User identification was carried out in two steps: Firstly, the activity performed by the user was classified into one of the six activities selected in this study using a machine learning classifier. After that, the classified activity pattern was compared with trained activity patterns of all the users to identify the smartphone user possessing the device while performing that activity. For activity classification, three prevalent classifiers (K-Nearest Neighbor (K-NN), Bayes Net (BN) and Support Vector Machine (SVM)) were used so that an efficient comparison can be made among the performance of these classifiers for user identification.

Table 1. A set of features extracted from time and frequency domains for user identification.

| Feature | Mathematical Transformation |
|---|---|
| Max. | $s_{max} = \max\left\{s\left(t\right)\right\}$ |
| Min. | $s_{min} = \min\left\{s\left(t\right)\right\}$ |
| Mean | $\mu = \frac{1}{N}\Sigma s\left(t\right)$ |
| Variance | $\sigma^2 = \frac{1}{N}\Sigma\left(s\left(t\right)-\mu\right)^2$ |
| Kurtosis | $K = (m_4)/\left(m_2^2\right)$ |
| Skewness | $S = (m_3)/\left(m_3^{3/2}\right)$ |
| Energy | $E_f = \sum\left\lvert S\left(f\right)\right\rvert^2$ |
| Entropy | $H(S(f)) = -\sum_{i=1}^{N} p_i\left(S\left(f\right)\right)\log_2 p_i\left(S\left(f\right)\right)$ |

## 4. Results and Performance Analysis

To evaluate the performance of the proposed scheme for user identification, three classifiers (K-NN, BN and SVM) were trained and evaluated on the selected dataset. The dataset was divided into 10 folds such that the data of each participant was represented by a different fold. For example, Fold-1 contained data of all six activities performed by User-1 for all five body positions; Fold-2 represented the data of User-2 and so forth. In every fold, each activity data was split in such a way that 30% data participated in training the classifiers for user identification and the remaining 70% data was used for testing purpose. For every user, all six activities corresponding to five different body positions were used for training of the selected classifiers. Only the average results of user identification computed over all 10 participants/users are included in this section. The metrics used for evaluating the performance of the proposed scheme for user identification are accuracy percentage, precision, recall, f-measure, Root Mean Squared Error (RMSE) and computational time.

Table 2 provides the results of user identification based on activity recognition while placing the smartphone at five different body positions. The results are shown separately for different classifiers. As f-measure is the harmonic mean of precision and recall, therefore, only f-measure values are shown in the table. Table 3 provides the average results of these performance metrics. It can be observed from these tables that Bayes Net classifier provides the best accuracy rate and f-measure value for user identification at all body positions as compare to K-NN and SVM classifiers. The average accuracy rate for BN classifier is 94.57%, which is 0.33% and 4.59% higher than the accuracy rate provided by SVM and K-NN classifiers, respectively. The error rate value for SVM classifier is 0.63, which is indeed much higher as compare to the error rate values provided by BN and K-NN classifiers.

Table 2. Comparison of K-NN, BN and SVM classifiers for user identification based on activity recognition at selected body positions.

| Body Position | Classifier | Accuracy % | F-measure | RMSE |
|---|---|---|---|---|
| Waist | K-NN | 89.26 | 0.88 | 0.47 |
| | BN | 95.58 | 0.94 | 0.42 |
| | SVM | 94.31 | 0.93 | 0.63 |
| Left Thigh | K-NN | 91.96 | 0.91 | 0.44 |
| | BN | 95.34 | 0.95 | 0.38 |
| | SVM | 95.30 | 0.94 | 0.61 |
| Right Thigh | K-NN | 92.61 | 0.91 | 0.44 |
| | BN | 95.20 | 0.94 | 0.40 |
| | SVM | 94.74 | 0.92 | 0.63 |
| Upper Arm | K-NN | 88.81 | 0.91 | 0.47 |
| | BN | 93.48 | 0.91 | 0.42 |
| | SVM | 93.18 | 0.89 | 0.63 |
| Wrist | K-NN | 87.66 | 0.87 | 0.49 |
| | BN | 94.28 | 0.93 | 0.40 |
| | SVM | 93.84 | 0.93 | 0.63 |

Table 3. Average performance metrics for user identification based on activity recognition

| Classifier | Accuracy % | F-measure | RMSE |
|---|---|---|---|
| K-NN | 89.65 | 0.90 | 0.46 |
| BN | 94.57 | 0.94 | 0.40 |
| SVM | 94.24 | 0.93 | 0.63 |

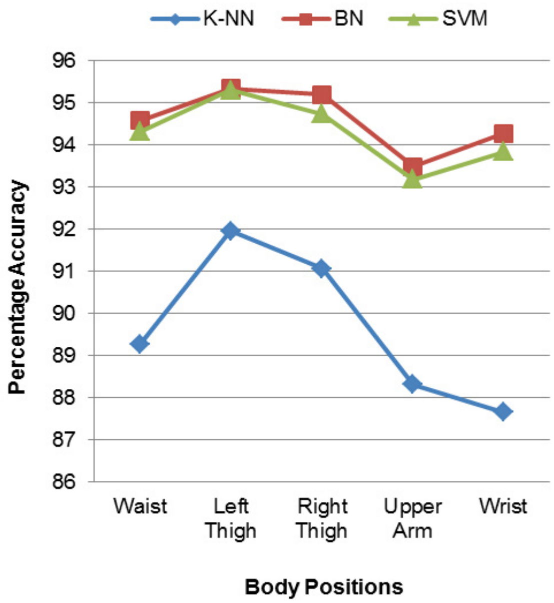

Fig. 4. A comparison among the accuracies of K-NN, BN and SVM classifiers for user identification at five different body positions.

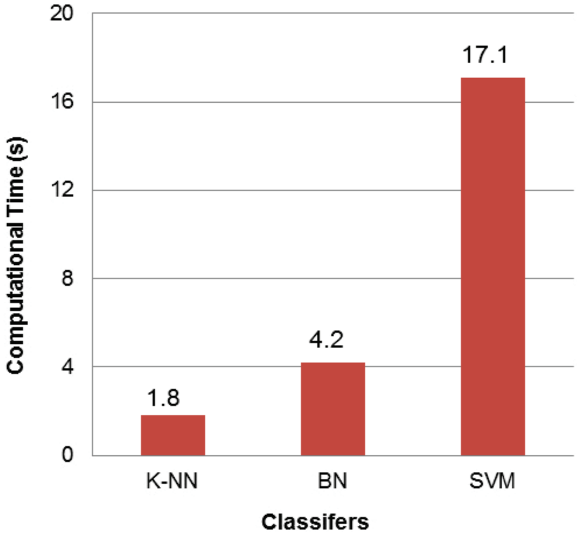

Fig. 5. Average computational time taken by K-NN, BN and SVM classifiers for user identification.

Figure 4 shows a comparison among the performance of the selected classifiers for user identification at five different body positions. BN classifier provides the best accuracy rate for user identification at all body positions. Also, the results of user identification are better for left thigh, right thigh and waist positions as compare to other body positions. Figure 5 shows a comparison of the computational time taken by the selected classifiers for user identification based on activity recognition. The time taken by SVM classifier for user identification is 17.1s, which is 9.5 times and 4.07 times more than the time taken by K-NN and BN classifiers for user identification respectively. On the other hand, BN classifier takes a reasonable time of 4.2s time for user identification. Based on these results, the overall performance of Bayes Net classifier performs better than the other classifiers in identifying users given their activity patterns. As a smartphone is equipped with limited processing power, memory and storage, therefore, it is feasible to use BN classifier for on-device user identification in real time as Bayes Net classifier is based on a simple probabilistic model that is computationally very cheap[23].

## 5. Conclusion and Future Work

In this paper, we have focused on identifying smartphone users based on their physical activity patterns, using smartphone inertial sensors. Different features have been extracted from the sensors data to learn and recognize six different activities for all participants individually. These activities include walking, standing, sitting, running, walking upstairs and walking downstairs. It is observed that these activities are smartphone position dependent and can be recognized in a better way if the smartphone is placed in the left or right jeans pocket, or hanged with a belt clipper at waist position. Therefore, it is easy to identify a smartphone user if the smartphone is placed in one of these positions while performing any selected activity. Furthermore, it is concluded that Bayes Net classifier provides the best performance for on-device user identification in terms of accuracy, error rate and computational time taken, which makes it an optimal choice for real-time identification of smartphone users based on physical activity recognition. This work will be extended to detect and recognize more complex activities for user identification. More sensors will be used for this purpose including virtual sensors. The work in this paper provides the opportunity to develop a smartphone access control framework that provides different levels of access to a wide range of users once they have been identified based on their behavioral traits.

## References

1. Réhman SU, Liu L. iFeeling: Vibrotactile Rendering of Human Emotions on Mobile Phones. In: *WMMP*. 2008. p. 1–20.
2. Réhman SU, Liu L, Li H. Vibrotactile Rendering of Human Emotions on the Manifold of Facial Expressions. Journal of Multimedia. 2008 Jul;**3**:18-25.
3. Gartner. Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 Billion Units in 2013, a press release published April 4, 2013. Gartner. 2013. p. 1. Available from: http://www.gartner.com/newsroom/id/2408515 [Accessed 5th June 2017].
4. Data Genetics: Pin Analysis. 2012. Available from: http://www.datagenetics.com/blog/september32012 [Accessed 5th June 2017].
5. SRLabs: Spoofing Fingerprints. 2013. Available from: https://srlabs.de/spoofing-fingerprints [Accessed 5th June 2017].
6. Shukla D, Kumar R, Serwadda A, Phoha V V. Beware, Your Hands Reveal Your Secrets! In: CCS - ACM Conference on Computer and Communications Security. 2014. p. 904–17.
7. Xu Y, Heinly J, White AM, Monrose F, Frahm J. Seeing double: Reconstructing Obscured Typed Input from Repeated Compromising Reflections. Proc 2013 ACM SIGSAC Conf Comput Commun Secur - CCS '13. 2013;1063–74.
8. Aviv AJ, Gibson K, Mossop E, Blaze M, Smith JM. Smudge Attacks on Smartphone Touch Screens. USENIX Conf Offensive Technol. 2010;1–7.
9. Mayron LM. Biometric Authentication on Mobile Devices. *IEEE Secur Priv*. 2015;**13**:70–3.
10. Draffin B, Zhu J, Zhang J. KeySens : Passive User Authentication through Micro-behavior Modeling of Soft Keyboard Interaction. *Mob Comput Appl Serv*. 2014;**130**:184–201.
11. Alzubaidi A, Kalita J. Authentication of smartphone users using behavioral biometrics. *IEEE Commun Surv Tutorials*. 2016;**18**:1998–2026.
12. Frank M, Biedert R, Ma E, Martinovic I, Song D. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Trans Inf Forensics Secur*. 2013;**8**:136–48.
13. Yang L, Guo Y, Ding X, Han J, Liu Y, Wang C, et al. Unlocking Smart Phone through Handwaving Biometrics. *IEEE Trans Mob Comput*. 2015;**14**:1044–55.
14. Lu H, Bernheim Brush AJ, Priyantha B, Karlson AK, Liu J. SpeakerSense: Energy efficient unobtrusive speaker identification on mobile phones. In: Lecture Notes in Computer Science. 2011. p. 188–205.
15. Blanco-Gonzalo R, Miguel-Hurtado O, Mendaza-Ormaza A, Sanchez-Reillo R. Handwritten signature recognition in mobile scenarios: Performance evaluation. In: Proceedings - International Carnahan Conference on Security Technology. 2012. p. 174–9.
16. Zheng N, Bai K, Huang H, Wang H. You are how you touch: User verification on smartphones via tapping behaviors. In: Proceedings - International Conference on Network Protocols, ICNP. 2014. p. 221–32.
17. Su X, Tong H, Ji P. Activity recognition with smartphone sensors. *Tsinghua Sci Technol*. 2014;**19**:235–49.
18. Shoaib M, Scholten H, Havinga PJM. Towards Physical Activity Recognition Using Smartphone Sensors. 2013 IEEE 10th Int Conf Ubiquitous Intell Comput 2013 IEEE 10th Int Conf Auton Trust Comput. 2013;80–7.
19. Shoaib M, Bosch S, Durmaz Incel O, Scholten H, Havinga PJM. Fusion of smartphone motion sensors for physical activity recognition. *Sensors (Switzerland)*. 2014;**14**:10146–76.
20. Anguita D, Ghio A, Oneto L, Parra X, Reyes-Ortiz JL. 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. 2013.
21. Mäntyjärvi J, Lindholm M, Vildjiounaite E, Mäkelä SM, Ailisto H. Identifying users of portable devices from gait pattern with accelerometers. In: ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings. 2005.
22. Sun L, Zhang D, Li B, Guo B, Li S. Activity recognition on an accelerometer embedded mobile phone with varying positions and orientations. In: Lecture Notes in Computer Science. 2010. p. 548–62.
23. Friedman N, Geiger D, Goldszmidt M. Bayesian Network Classifiers. *Mach Learn*.1997;**29**:131–63.
24. Shoaib M, Bosch S, Incel OD, Scholten H, Havinga PJM. Complex human activity recognition using smartphone and wrist-worn motion sensors. *Sensors*. 2016;**16**.
25. Shoaib M, Bosch S, Scholten H, Havinga PJM, Incel OD. 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. 2015. p. 591–6.