Extended Sammon Projection and Wavelet Kernel Extreme Learning Machine for Gait-Based Legitimate User Identification on Smartphones

Muhammad Ahmad, *Member, IEEE,* Adil Mehmood Khan, *Member, IEEE,* ,

Abstract—**Smartphones have been ubiquitously integrated into our home and work environments, with one person having more than one device connected to the Internet at the same time. Normally, users rely on explicit but inefficient user identification processes in a controlled environment when the device is stolen, the attacker can have access to the users personal information and services against the stored password/s. As a result of this potential scenario, this work demonstrates the possibilities of legitimate user identification in a semi-controlled environment, through the built-in smartphones motion dynamics captured by two different accelerometers. We named this mechanism Gait based Legitimate User Identification (GUI). This is a two-fold process, sub-activity recognition based user identification, in which we first collected data from 20 users walking with their smartphones freely placed in one of their pants pockets (front right, front left, back right, and back left pocket devise placement). The collected raw signals are stored into micro SD cards, which later transfer this information to the computer for further analysis. Through extensive experimentations using overall and average-one-subject-cross-validation, we demonstrate that together, time and frequency domain features, are further optimized by applying the Extended Sammon projection (ESP) method to train the wavelet kernel based extreme learning machine, as an effective system to identify the legitimate user or an impostor. All experiments were carried out using MATLAB (2014b) on Intel Core i5 CPU 3.20 GHz with 8 GB of RAM with a 64-bit operating system machine.**

Index Terms—**Smartphone, Sensor, Feature Extraction, Feature Selection, Legitimate User, Imposture.**

I. Introduction

In the recent past, devices such as desktop computers and laptops were our best means for staying connected to the Internet community and to have access to online services. However, with enhanced capabilities, low cost and user-friendly interfaces, smartphones have become peoples first choice to stay connected to the Internet. This is equally credited to publicly available Internet which facilitates users to access their device contents regardless of their location. According to a recent study [1], more than 2.56 billion people are estimated to own smartphones by the end of 2018.

With this rapid growing trend in the usage of smartphones, device control, and data security have become extremely important. Not only personal and professional contact information is stored such as email IDs, passwords, banking details, credit and debit card numbers, photos, and videos, but users also store their sensitive and critical information in their smartphones [2]. If the device is stolen, the stored information can be used to create many troubles not only for the user, but also for the individuals in their contacts. In order to secure this access, it is important to develop fast and accurate methods for legitimate user identification and block-out impostors. Ideally, these methods should detect an impostor from the moment a device is stolen with acceptable accuracy within a minimum time span.

Current identification methods such as secret PIN number (SPN) or lock codes [3], are not only risky- since tools to extract SPNs are easily available on the Internet today, but also difficult to use - particularly for the elderly and physically impaired users who find entering PIN codes or screen patterns difficult. Another factor which restricts the security of SPNs based mechanisms, is that smartphones are mostly used in public places with many other people around. This increases the chances for the codes to be found-out by potential attackers. To overcome these issues, fast and secure methods are required to intelligently verify legitimate user and to block-out impostors.

In the literature hereby referred to, several solutions were proposed addressing implicit user identification without involving the user, such as keystroke based user identification [2], touch screen biometrics [4-5], application set fingerprints [6], hybrid user identification methods such as accelerometers and gyroscopes [7-9], and gait based user identification [10-11]. However, these solutions only discuss one aspect of user identification, either software or hardware.

The first thing attackers do after stealing a smartphone, is to walk away from the actual user. Considering this fact, the gait based legitimate user identification methods are most efficient, as they detect the impostor from their walking or running patterns at that same time and thus can trigger an alarm to keep the real user informed. This type of legitimate user identification method protects not only the smartphone itself, as well as the stored data when the device is stolen by swiftly triggering an alarm. However, due to several contributing factors, the implementation of such real-time identification is quite challenging. There are 2 key important features in a GUI system:

1) The user can perform the same ambulatory sub-activity differently at separate times.
2) Various users require a distinctive set of features for user identification: male and female have different physical

M. Ahmad, and A.M. Khan are with Machine Learning and Knowledge Representation (MlKr) Lab, at the Department of Computer Science, Innopolis University, Innopolis, 420500, Russia.

Manuscript received June, 2017; revised —-.

characteristics, therefore, will have explicit identification processes.

This study focuses on the idea of identifying a smartphone user by applying different walking patterns, hereby referred as sub-activities. Furthermore, it is assumed that the phone is freely placed without any particular orientation inside any of the users pants pockets. Data on walking patterns (with different sub-activities) is recorded using an embedded triaxial, where we intentionally limited the scope to just walking, in order to understand how fast and accurate can ambulatory sub-activity based legitimate user identification be.

The aim of this research, is to propose a semi-controlled environment system in which we overcome the limitations of our users age, gender, jeans style (either loose or tight) and walking style (we intentionally asked users to walk differently in various times to investigate the ambulatory activity performed by each legitimate user). In this regard, the aim of our current work is to investigate several research questions relevant to building a walking based legitimate user identification system in real life:

1) Does the ESP, a non-linear unsupervised feature selection method improve the identification accuracy more than the other existing and well-studied unsupervised feature selection methods such as principle component analysis (PCA)?
2) Is the kernel based extreme learning machine (KELM) an effective classifier for the non-linear signal based user identification method?
3) How to achieve real-time user identification in practice? Since our goal is to develop an algorithm which identifies the user in real time, thus computation complexity is extremely important. System performance measurements ought be considered to balance the trade-off between accuracy and computational cost.
4) Does the data variation affect the performance for the legitimate user identification process?

Our major research commitments are towards answering the above questions using the proposed ESP and KELM methods. In this work, we introduce a new two-fold average-one-subject-cross-validation based legitimate user identification (GUI) system, in a semi-controlled environment, thus addressing the above questions within a sub-activity recognition based legitimate user identification method on smartphones, in a real time environment. The most important aims in our work are to test the proposed ESP and KELM methods, neither of which have ever been tested for this purpose before together or individually.

The remainder of this paper is organized as follows: Section 2 explains related works; Section 3 describes the system design; Section 4 presents the system validation and the discussion on results; and finally section 5 concludes with future directions.

II. Related Work

The objective of this work is to provide convenience in using smartphones differently from explicit identification, by using sensor data information. Therefore, hereby we present some key related works on this field which can be categorized into two groups: implicit user identification and multiple modality biometrics.

W. Shi, et al., proposed a Senguard method for user identification in [8], offering continuous and implicit user identification service for smartphone users. This method leverages the sensors available on smartphones, e.g. voice, multi-touch and location; these sensors are processed together in order to get the users identification features implicitly. Explicit identification is performed only when there is an important evidence of change in the user activity. In recent years, several other implicit identification approaches have been proposed leveraging smartphones sensor devices such as accelerometer [12], touch screen [13], GPS [14] and microphone [15].

T. Feng, et al., in [16] proposed to extract finger motion speed and acceleration of touch patterns as features. A. De Luca, et al, suggested to directly compute the distance between pattern traces using the dynamic time warping algorithm in [17]. N. Sae-Bae, et al., in [18] present 22 special touch patterns for user identification, most of which involve all five fingers simultaneously. They then computed dynamic time warping distance and Frechet distance between multi-touch traces. M. Frank, et al., in [19] studied the correlation between 22 analytic features from touch traces and classified them using k nearest neighbors and support vector machines. M. Shahzad, et al, in [20] explained the use of touch screen patterns as a secure unlocking mechanism at the login screen.

Moreover, the idea behind the behavior based model is that the persons habits are a set of its attributes; therefore, each event (activity) has a correlation between two fundamental attributes: space and time. In addition, the architecture proposed in [21], utilizes the resources found in the smartphone devices, such as: user calls, user schedule, GPS, device battery level, user applications, and sensors. A similar methodology has also been adopted in [22].

N. L. Clarke, et al., proposed smartphones user perception of identification in [23],in which results showed the system implicitly and continuously performing user identification in the background. J. Koreman, et al., recommended a continuous multiple model based approach for user identification [in 24]. J. Mantyjarvi, et al., in [12] used an accelerometer in television remote controls to identify individuals. D. Gafurov, et al., and K. R. Cuntoor, et al., suggested an experimented user identification using gait analysis and recognition in [25-26]. M. Jakobsson, et al., put forward another unique implicit user identification framework by using recorded phone call history and location for continuous user identification in [27]. Therefore, these approaches present several propositions for legitimate user identification, but to some extent, all required some additional information and source.

P. Casale, et al., proposed a user verification and authentication method using gait as a biometric unobtrusive pattern in [28]. A four-layer architecture was built around the geometric concept of a convex hull. This was a twofold method, in which first, a general activity identification based classifier is personalized for a specific user based on their walking patterns, and second, where the author verifies whether the user is authorized or not by using the one-class classification method.

The proposed architecture is able to improve robustness to the outliers, account for temporal coherence information and most importantly for non-convex shapes. The most important fact of this system was not its non-user-friendliness, thus the user can only operate this system in specific and controlled environments.

J. Mantyjarvi studied a users identification utilizing portable devices from gait signals acquired with three-dimensional accelerometers in [29]. They originally proposed three approaches: data distribution statistics, correlation, and frequency domain to identify the subject while walking at different speeds: fast, normal and slow, where the accelerometer device was placed on the users belt only at the back. The identification process by this method was novel, but only limited for walking by the same users and with limited variations. Similar studies for user identification were proposed in [30-34] using external accelerometers. To some extent, these studies are innovative but solely rely on external accelerometers with limited activity or sub-activities.

Conclusively, all previous works require users to either perform predefined touch patterns, or for the data to be collected under controlled experimental environments, which might not be a real representation of common user interactions. For this situation, the proposed gait based legitimate user identification work is an interesting application alternative for the process of identifying explicit and continuous legitimate user or impostor in a semi-controlled environment;hence, overcomes the smartphones limitations in power consumption and cost. Moreover, todays research is towards the smartphones emergence of these kinds of identification mechanisms.

Our team has worked on combining different approaches to deliver a more reliable legitimate user identification model using a built-in accelerometer for different sub-activities in semi controlled environment. In short, several studies have experimented user identification using gait recognition as a possible identification method. Our proposed approach, utilizes acceleration signals and detects users by their way of walking under different sub-activities in a semi-controlled environment, and for this, a motion-recording device is used in order to measure the acceleration according to the three axes outlined in [35-36].

III. System Design

Now-a-days, smartphones are equipped with a variety of motion sensors which are useful for monitoring the devices movements such as: tilt, rotation, shaking and swinging. Two of these are the accelerometer (ACC) and the linear acceleration (LACC) sensors. This work explores built-in sensors to validate the sensors capacities for legitimate user identification processing. To this end, the first task of our proposed system is to collect data using two different enabled sensors. The second task is the feature extraction and analysis based on both the time and frequency domain features. The third task is feature selection and the fourth task is the classification for legitimate user identification based on performed sub-activities while walking. Finally, the fifth task is towards the evaluation of our proposed method on a publicly available dataset.

A. Data Collection

The first data is collected using an android smartphone, collecting raw signals from sensors, as the user performed daily sub-activities. These sub-activities included walking while the smartphone was intentionally placed in one of the subjects pants pockets: back right pocket (BRP), back left pocket (BLP), front right pocket (FRP) and front left pocket (FLP). We recorded these sub-activities without any constraints on the smartphones orientation inside of any of the users pockets. From literature, one can find that an accelerometer placed on the thigh gives a more powerful performance.

The first dataset was gathered from four users each one performing individual sub-activities each day; each sub-activity was performed at least twice a day. Thus, the compiled data is from one same user, doing the same activity on different days, for an entire month. For this activity, we requested users to wear different types of pants: tight and loose styles. Initially, we stored these raw signals in a micro SD card, which we later transferred to a computer for further analysis. It is worth pointing out, since different smartphone models have different sampling rates, therefore, in order to control the data collection process and better validation, generalization and reproducibility, we have used 50Hz sampling rate instead to use highest sampling rate within different smartphones. In order to identify the legitimate user, each behavior should be presented in a simple structure: feature extraction process [37].

The second dataset was acquired from 16 healthy users between the ages of 19 to 48 years old. The dataset was gathered from all users by using a linear acceleration sensor (LACC) with a constant rate of 50Hz while they were wearing a smartphone on their waist. The dataset was preprocessed by applying noise filters, using a 2.56 sec windows with a 50% overlap. The second experimental dataset is an extended version of the UCI human activity recognition process using a smartphone dataset and can be freely download from UCI website [38].

B. Feature Extraction

The accelerometer sensor generates time series signals which are highly fluctuating and oscillatory in nature [37-39], thus making the legitimate user identification more difficult. Therefore, it is compulsory to gather the nontrivial signals from the raw data through the feature extraction process. Particularly, we divided the raw signal into several equal size windows to control the flow rate, hence passing less data to the system to be able to extract all meaningful information. Given a sampling rate of 50Hz, we initially chose a window size of 50 samples, which is almost equal to a one second slot for both sensors as shown in Figure 1(A-B). A selected window size provides enough data to be able to extract the quality features while at the same time, ensuring a fast response [37].

Our research analyzed the individuals user data applying time series modeling techniques to understand the behavior in each of the users physical patterns. Time series analysis reveals unusual observations as well as particular data patterns[40]. There are three commonly used models to perform time series analysis: moving average [41], autoregressive [42] and a combination of both the moving average and the autoregressive models [37]. We explored with the use of autocorrelation (AC) and partial autocorrelation (PAC) coefficients to identify the model for our data. These coefficients revealed the pattern of each datum and indicated the best model for our data. Each data model is determined based on the characteristics of the theoretical AC and PAC. Samples of AC and PAC for both sensors are shown in Figure 2 (A-B). The fitting process for the time series model is calculated by estimating the parameter values based on a previously selected model. Moving average and autoregressive parameter estimations requires an iteration process [43], and for that, we follow the box Jenkins model estimation due to its flexibility for the inclusion of both the moving average and the autoregressive models [44]. The parameters and the model need to be verified to ensure that the estimated results are statistically significant [45].

Detailed analysis revealed that the time domain features, including the coefficients from the time series model provided the same accuracy as the frequency domain features at a lower sampling rate [11, 46]. Therefore, in our work we have used both the time and frequency domain features.

The extracted features are: mean, median, variance, standard deviation, interquartile, autocorrelation, partial correlation, coefficients of autoregressive model, coefficients of moving average model, coefficient of moving average autoregressive model and wavelet coefficients. These features are extracted from each axis of the three-dimensional acceleration signals. In total 72 features were extracted from each window. Prior to the feature extraction, a moving average filter of order three was employed for noise reduction purposes.

C. *Feature Selection*

The output of an embedded motion sensor depends upon the position of the smartphone while walking. This could result in a high within class variance [47]. Therefore, it is at the same time desirable to improve both the discriminatory power of the features and achieve dimensionality reduction, by employing an optimum method. Hence, our third important step towards legitimate user identification is feature selection. The advantages of the feature selection process are to avoid the curse of dimensionality [48], as well as to reduce the abundant, irrelevance, misleading and noisy features, but above all, to be able to reduce the systems cost pertaining to run-time applications [49]. In addition to the above, the main purpose is to increase the accuracy of the resulting model within a short time.

In recent years, several feature selection algorithms have been proposed, including: the filter based approach, the wrapper method, the principal components analysis (PCA), the linear discriminant analysis (LDA) [50], a kernelized version of the LDA (KLDA) [47] and the stepwise linear discriminant analysis (SWLDA) [11].

Filter methods are based on discriminating criteria which are relatively independent of classification and use minimum redundancy and maximum relevance for feature selection. These methods are comparatively fast, scalable and provide good computational complexity, but ignore the interaction with the classifier. Alternatively, wrapper methods utilize the classifier as a black box to obtain a subset of features based on their predictive power. These methods interact with the classifier to optimize the features subset. The main disadvantages of these methods are their dependency on the classifier, who makes the classifier selection a key important process. In different prospects, the LDA seeks a linear combination of features and characterizes two or more types. Among the three different discriminant analysis approaches, the number of dimensions returned by both the LDA and KDA depend on the number of classes, which limit the use of LDA and KDA.

For this purpose, our current work considers only unsupervised non-linear feature selection methods. In this regard, the most commonly used method is the PCA. Through this work we have introduced an unsupervised and fully automatic feature selection method named extended Sammon projection (ESP). The ESP is one of the most successful non-linear metric multidimensional scaling methods and it projects the high dimensional space into a lower dimensional space, while preserving the structure of inter-point distances in a high dimensional space within a lower dimensional space. Consequently, let us assume $d_{i,j}$ be the distance between two adjacent samples x_i and $x_j, i \neq j$ from the original space and $d^*_{i,j}$ be the distance between two samples x^*_i and x^*_j in the mapped space; thus, the Sammon stress measure, which is also known as the Sammon error or simple error function E can be defined as;

$$E = \frac{1}{\sum_{i=1}^{n-1} \sum_{j=i+1}^{n} d_{i,j}} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \frac{d^*_{i,j} - d_{i,j}}{d^*_{i,j}} \tag{1}$$

where $d_{i,j}$ is the Euclidean distance and this error measurement is minimized by using the steepest and gradient decent methods, respectively.

$$x^*_{ik}(t+1) = x^*_{ik}(t) - \alpha \frac{\partial E(t) \setminus \partial x^*_{ik}(t)}{\mid \partial^2 E(t) \setminus \partial^2 x^*_{ik}(t) \mid} \tag{2}$$

$$x^*_{ik}(t+1) = x^*_{ik}(t) - \alpha \frac{\partial E(t)}{\partial x^*_{ik}(t)} \tag{3}$$

In both cases x^*_{ik} is the k^{th} coordinate of the position of point x^*_i in the lower dimensional space. Since the Steepest descent method has issues at the inflection points, where the second order derivative appears to quit small [51], therefore, we set α between 0.3 0.4 as the optimal value using a grid operation between [0, 1], but there is no reason to expect this given range to be optimal for all problems and datasets.

D. *Classifier*

Neural networks have quite diverse real-life applications and among different neural network approaches, extreme learning machines (ELM) have better generalization capabilities and a fast learning speed [52]. An ELM is a single hidden layer feed-forward neural network which randomly determines the initial parameters of weights input and hidden biases with simple activation functions [53]. Among the factors influencing

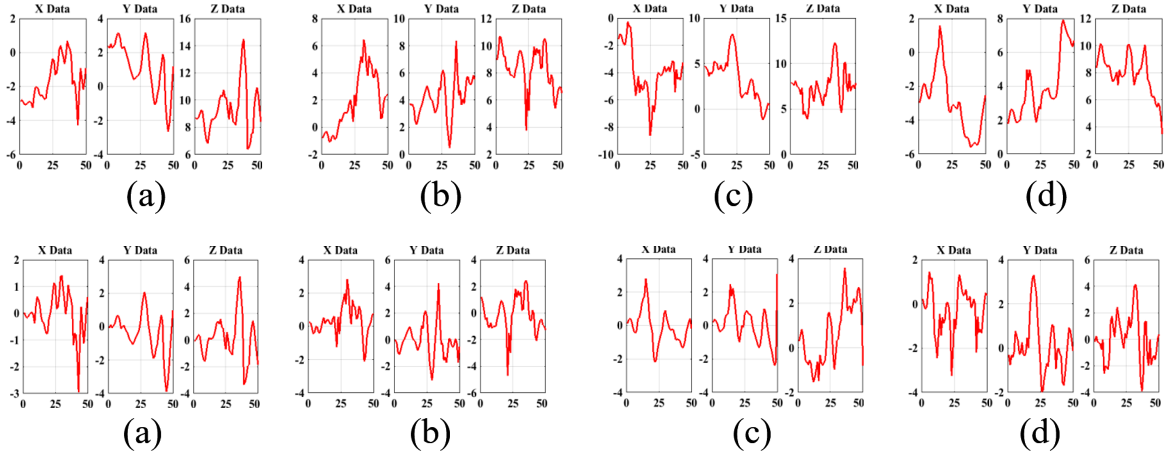


Fig. 1: **(A)-(B)**: Representative raw signals obtained by ACC and LACC sensors for one subject doing activity while the smartphone is freely placed in: (a) Back left pocket, (b) Back right pocket, (c) Front left pocket, and (d) Front right pocket.

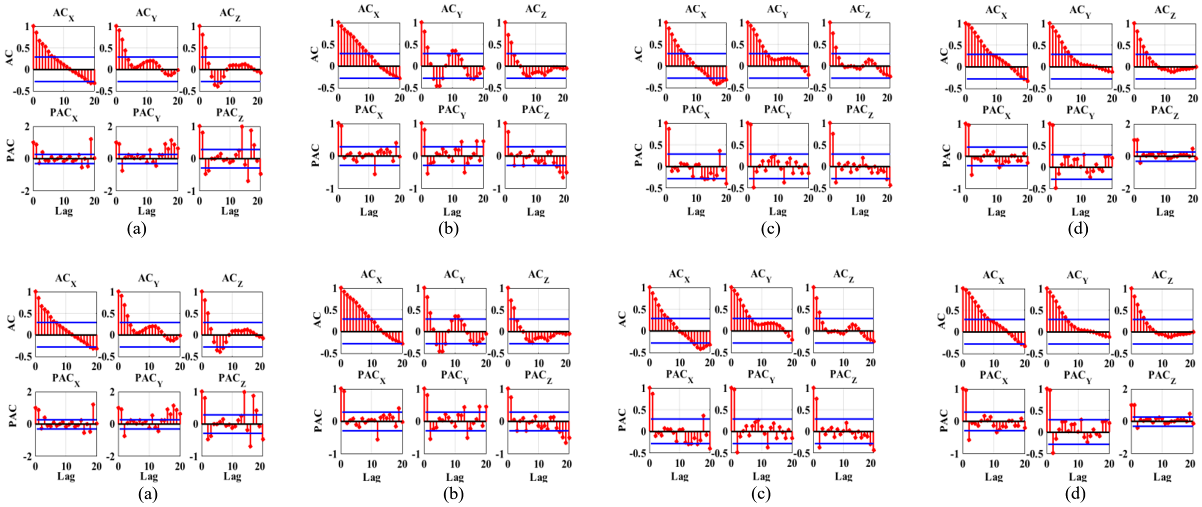


Fig. 2: **(A)-(B)**: Autocorrelation (AC) and Partial autocorrelation (PAC) coefficients from ACC and LACC sensors: (a) Back Left pocket, (b) Back Right pocket (c) Front Left pocket, and (d) Front Right pocket signals

learning performance, the hidden neurons are very important to improve generalization capabilities.

Moreover, ELMs with a tunable activation function were proposed to handle the data dependency on hidden neurons. However, the selection of suitable combinations for activation functions is still a big question within the research community. Therefore, kernelized ELMs are known to improve the generalization capabilities, when the feature mapping function of hidden neurons is unknown. However, the parameters for the kernel function need to be selected carefully to improve generalization performance. In order to improve the generalization performance for real-time applications, such as smartphone-based legitimate user identification, the kernel parameters need to be tuned carefully. In our work, the parameters are optimized through the swarm optimization based method [54].

In ELMs, the initial parameters of hidden layer need not to be tuned and almost all nonlinear, piece-wise continuous functions can be used as hidden neurons. Therefore, for N distinct samples $(x_i, t_i) \mid x_i \in R^n, t_i \in R^m, i \in 1,2,3,...,N$, and the output function with L hidden neurons can be expressed as;

$$f_L(x) = \sum_{i=1}^{L} \beta_i h_i(x) = h(x)\beta \tag{4}$$

where $\beta = [\beta_1, \beta_2, ..., \beta_L]$ be the output weights between the hidden layer and the output neurons; $h(x) = [h_1(x), h_2(x), ..., h_L(x)]$ be the output vector of the hidden layer that maps the input space to the feature space [55]. The output weights and training error should be minimized to enhance the generalization capabilities. The least square solution to the minimization problem can be expressed as:

$$\beta = H^T\left(\frac{1}{C} + HH^T\right)^{-1} T \tag{5}$$

where H be the hidden layer output matrix and T is the expected output matrix, and C is the regularization coefficient. Thus, the training model output can be expressed as:

$$f(x) = h(x)H^T\Big(\frac{1}{C} + HH^T\Big)^{-1}T \tag{6}$$

For the unknown mapping $h(x)$, the kernel and the output function $f(x)$ can be defined as;

$$M = HH^T; m_{i,j} = h(x_i)h(x_j) = \kappa(x_i, x_j) \tag{7}$$

$$f(x) = \Big[\kappa(x, x_1), ..., \kappa(x, x_N)\Big]\Big(\frac{1}{C} + M\Big)^{-1}T \tag{8}$$

where $\kappa(x, y)$ is the kernel function and can be expressed as in expression (9), where a and b are adjustable kernel parameters, which play an important role in generalization performance and are updated using the cross validation process.

$$\kappa(x, y) = cos\bigg(\frac{\|x - y\|^2}{a}\bigg)exp\bigg(\frac{\|x - y\|^2}{b}\bigg) \tag{9}$$

IV. EXPERIMENTAL RESULTS AND DISCUSSION

To validate the proposed system, we conducted different experiments on two different datasets as explained in the previous section. Based on our own dataset, our first experiment presents the results obtained using average-one-subject-cross-validation on sub-activities for a legitimate user identification system, in which we conducted a detailed comparison on two different unsupervised feature selection methods (PCA and ESP). Our second experiment explains the identification behavior with different numbers of windows within the best settings obtained from our first experiment. Finally, our third experiment shows the computational cost for our proposed system.

Based on publicly available smartphone-based physical activity recognition (PAR) data, our first experiment presents a user identification method using a one-subject-cross-validation process during a walking activity, with different numbers of windows, in which the features are processed through an ESP method. The second experiment explains the confidence interval for the computational cost of our proposed legitimate user identification system.

A. Experimental Settings

The values utilized for the different parameters pertaining to the ESP, PCA, and KELM methods were optimized using across-validation process; these optimized parameters were the ones used for our research work. These optimized setting were used during each case for each sub-activity, as they provided the best results. In all cases, the wavelet kernel is used and the kernel parameters updated, according to the practical swarm method. For the feature Selection process, and in order to keep both methods consistent, the same numbers of PCs are selected as the number of features selected by the ESP. The intention behind to select the same number of features was to make this model reliable and consistent for replicability of our work in future use. Prior to the classification, all obtained features are normalized and bounded within [0, 1].

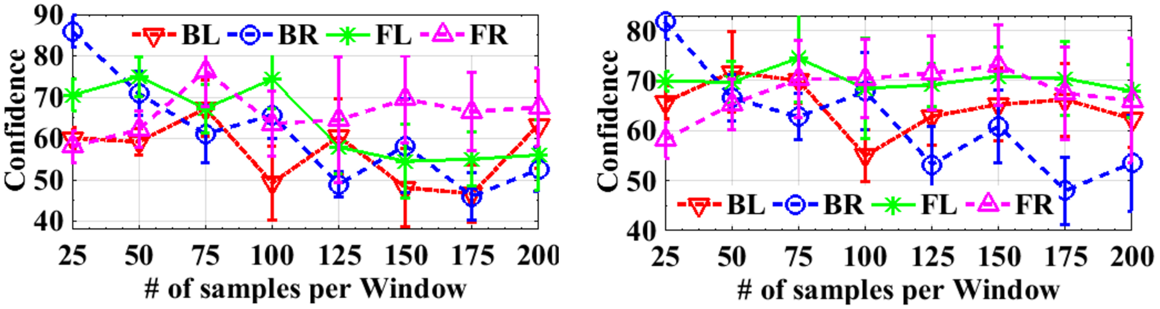
B. Results and Discussion

In the introduction part we have stated four important research questions for legitimate user identification on smartphone and based on our findings, we know it is definitely possible to identify a smartphones legitimate user by analyzing their walking patterns when the device is freely placed in any of their pants pockets. Furthermore, the proposed unsupervised ESP features selection process significantly boosts identification performance. The KELM method uses 72 features for user identification when the case is without feature selection; both feature selection methods are thus able to reduce this number down to a different number of features (5, 10, 15, 20, 25, 30, 35, and 40) keeping always the most informative features. Based on our findings we observe that the ESP feature selection method, together with the KELM classifier, is more robust and accurate than the existing well studied unsupervised feature selection method such as the PCA.

Our first experiment details the process of our proposed scheme for analyzing the behavior of different numbers of samples per window (i.e. 25, 50, 75, 100, 125,150, 175, and 200), on a legitimate user identification process within each sub-activity without a feature selection method. Figure 3 shows the legitimate user identification confidence of a legitimate user being identified with a different number of samples per window, for both sensors' data processed without selecting the feature. From these results, we observe that the BR pocket produced better results with 25 samples per window (80% to 88% confidence interval with the LACC and ACC sensors respectively). On average, we can see the ACC sensor performed better than the LACC for legitimate user identification within each sub-activity without feature selection method.

In our second experiment, we investigated the average-one-subject-cross-validation for all users and each sub-activity within a fixed size window (50 samples per window), for both feature selection methods with a different number of features. Table 1 lists the results (user identification accuracy across all users and each sub-activity with a 99% confidence interval) for the case of the PCA-KELM and the proposed ESP-KELM. According to the results obtained on Table 1, the best performance was obtained by the KELM classifier when the normalized features were extracted by both sensors and processed with the proposed ESP method. The PCA performed slightly better than without the feature selection process, but in average, there was no such difference with and without the feature selection process for the PCA case. All these results were obtained by using 50 samples per window during the feature extraction process.

Figure 4 displays the average accuracy obtained through ESP using different number of windows as explained earlier and 30 number of selected features as 30 number of features provide best average results in our previous experiments for all pockets data. For all subsequent experiments, we have fixed 30 number of features selected by the ESP method. From Figure 4, we can observe that the performance has significantly improved for the legitimate user identification for both sensors, each with a different number of samples.



(a): ACC Sensor

(b): LACC Sensor

Fig. 3: Average Accuracy (confidence) for one-subject-cross-validation based legitimate user identification. The data was collected by both sensors (ACC and LACC) and processed without selecting any features.

TABLE I: Average Accuracy, Confidence Intervals and Time taken for Legitimate User Identification for 50 Sample Per Window With Different Feature Selection Methods and Different Number of Features on Both Sensors Data

Features	Metric	Back Left Pocket				Back Right Pocket				Front Left Pocket				Back Right Pocket			
		ACC		LACC		ACC		LACC		ACC		LACC		ACC		LACC	
		PCA	ESP	PCA	ESP	PCA	ESP	PCA	ESP	PCA	ESP	PCA	ESP	PCA	ESP	PCA	ESP
5	Accuracy	55±5.1	50±3.2	50±4.5	53±5.7	52±4.9	53±3.8	51±3.6	50±2.7	54±3.6	55±2.9	57±2.9	54±3.9	54±4.6	63±2.9	54±3.8	52±4.5
	Time	0.140	0.138	0.209	0.243	0.265	0.261	0.553	0.527	0.175	0.173	0.268	0.270	0.164	0.133	0.201	0.202
10	Accuracy	74±6.3	85±3.3	67±4.8	85±3.8	63±4.5	77±2.3	63±3.4	84±3.9	66±2.9	90±4.6	72±4.1	81±3.9	69±3.8	74±5.9	64±4.7	77±4.8
	Time	0.140	0.142	0.209	0.214	0.255	0.252	0.535	0.523	0.177	0.178	0.270	0.271	0.131	0.131	0.194	0.188
15	Accuracy	72±6.2	98±1.1	75±4.6	89±4.1	76±5.5	99±0.9	78±3.9	96±2.0	70±5.8	95±3.4	77±4.1	95±2.1	74±4.1	98±1.3	71±5.7	98±1.0
	Time	0.142	0.142	0.211	0.238	0.255	0.254	0.536	0.517	0.177	0.178	0.269	0.273	0.135	0.132	0.197	0.203
20	Accuracy	73±6.1	97±1.4	73±4.9	97±2.0	76±4.6	99±0.4	82±2.5	98±1.6	76±3.6	99±0.7	76±6.7	98±2.6	71±7.1	95±2.4	73±5.8	94±4.2
	Time	0.142	0.142	0.216	0.219	0.259	0.256	0.538	0.529	0.178	0.189	0.269	0.281	0.132	0.132	0.194	0.212
25	Accuracy	78±3.8	99±0.5	74±4.9	98±2.7	72±4.4	96±3.4	80±4.6	98±1.6	75±6.7	98±1.2	76±4.9	94±2.3	73±6.7	96±3.9	73±8.3	90±4.9
	Time	0.148	0.140	0.221	0.219	0.258	0.257	0.532	0.528	0.180	0.179	0.254	0.270	0.134	0.133	0.200	0.203
30	Accuracy	**78±3.8**	**97±0.4**	**76±4.3**	**98±1.8**	**73±6.9**	**98±1.5**	**76±3.6**	**98±1.4**	**76±6.7**	**94±3.2**	**76±6.4**	**99±0.3**	**74±3.7**	**99±0.5**	**68±7.8**	**91±4.1**
	Time	**0.148**	**0.143**	**0.216**	**0.217**	**0.260**	**0.258**	**0.539**	**0.532**	**0.179**	**0.179**	**0.268**	**0.284**	**0.132**	**0.149**	**0.197**	**0.181**
35	Accuracy	77±5.4	99±0.5	71±6.2	94±4.7	72±4.5	99±0.3	74±5.9	87±6.2	75±4.5	97±1.7	73±5.5	97±3.6	76±7.2	99±0.8	69±7.9	54±4.9
	Time	0.143	0.143	0.216	0.208	0.258	0.259	0.536	0.548	0.180	0.179	0.267	0.275	0.134	0.133	0.194	0.201
40	Accuracy	**74± 5.9**	**98± 0.6**	**70± 6.4**	**99± 0.4**	**71± 4.2**	**98± 0.8**	**72± 5.9**	**99± 0.4**	**73± 4.6**	**50± 2.8**	**71± 4.9**	**75± 5.9**	**69± 8.2**	**98± 1.1**	**69± 6.3**	**99± 0.4**
	Time	**0.144**	**0.142**	**0.216**	**0.212**	**0.262**	**0.259**	**0.537**	**0.532**	**0.180**	**0.172**	**0.276**	**0.278**	**0.133**	**0.148**	**0.196**	**0.196**

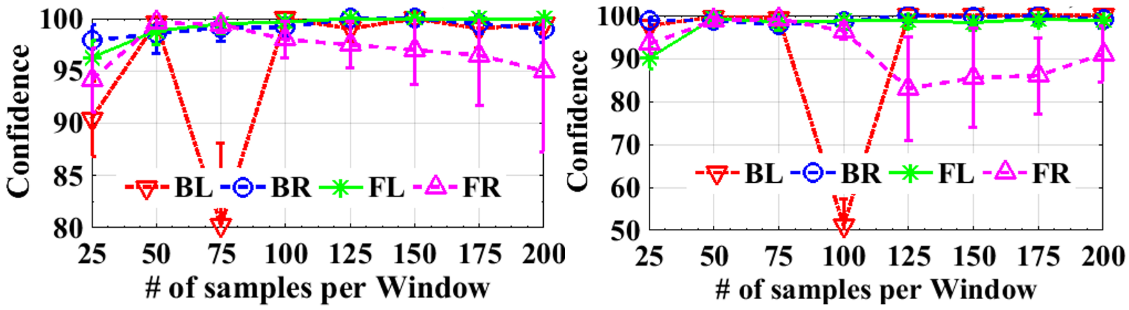
The average accuracy increased from 70% to 99% for 50 samples per window, which is a significant improvement for any legitimate user identification system. From these results, we conclude that the back left and front right pockets had some variations according to the number of samples per window; however, this variation is not enough to exclude these sub-activities from our experimental setup, except the ones with 75 and 100 numbers of samples per window. This degradation might happens due to the sudden change in the users walking patterns. In future research, we will further investigate legitimate user behaviors, while performing the same sub-activity to minimize the ambiguity to the legitimate user identification method.

In our third experiment, we detailed the computational cost in terms of time comparison, pertaining to our previous experiments presented in Figures 3 and 4. Figures 5 and 6 show the computational time for KELM with and without using the ESP method; with different numbers of samples per window for each sub-activity and sensors individually.

As shown in these results, the different number of samples per window (25 to 50 samples per window) for both sensors, the computational cost exhibits the huge difference, thus, indicating that identification has strong influence on the computational time of KELM with the number of samples. However, when we increased the size of samples from 50 to 75 or even to 100, 125, 150, 175, and 200, both systems took almost the same time to complete the legitimate user identification process.

As shown in Figures 7 and 8, the computational cost gradually increases as the size of the windows decrease. Therefore, dealing with such high computational time becomes an important issue. There are certain possibilities which can be used to overcome this problem. One way is to use a lightweight feature selection method such as the PCA, although the problem with the PCA is its incompetency for statistical results. There is another solution for such problems, and it is to further divide each window into other sub-windows. However, this presents another challenge, how to conduct the windowing process, so that it does not decrease the performance of the legitimate user identification process.

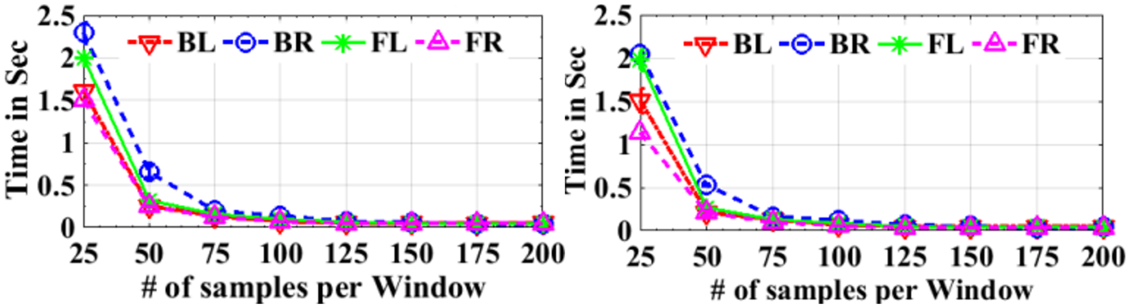
We conducted our last experiment on a publicly available LACC sensor based dataset, hereby this experiment, we again investigated the one-subject-cross-validation within different size of windows. Table 2 lists the results of user identification and computational time to identify individual users where features are selected through the proposed ESP method and the selected features are classified through the KELM method. Our obtained results corroborate the effectiveness of our proposed



(a): ACC Sensor

(b): LACC Sensor

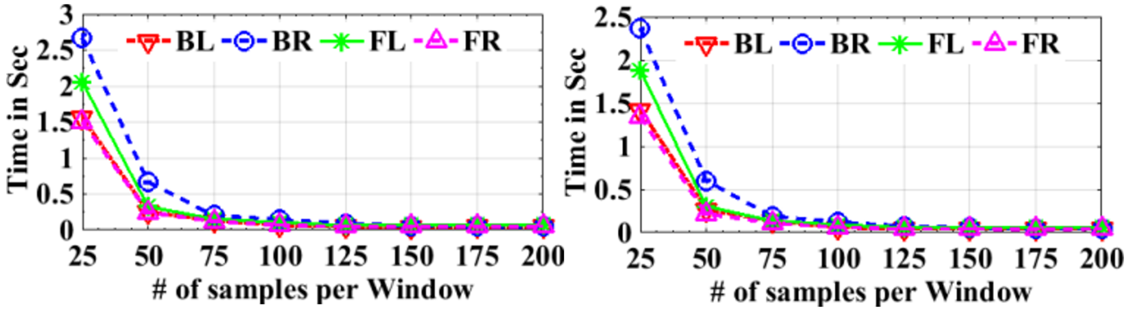
Fig. 4: Average Accuracy (confidence) for one-subject-cross-validation based legitimate user identification. The data was collected by both sensors (ACC and LACC) and processed through ESP-KELM.



(a): Without feature selection

(b): With feature selection

Fig. 5: Computational Time for Legitimate User Identification on the ACC Sensor Data, with and without feature selection through ESP.



(a): Without Feature Selection

(b): With Feature Selection

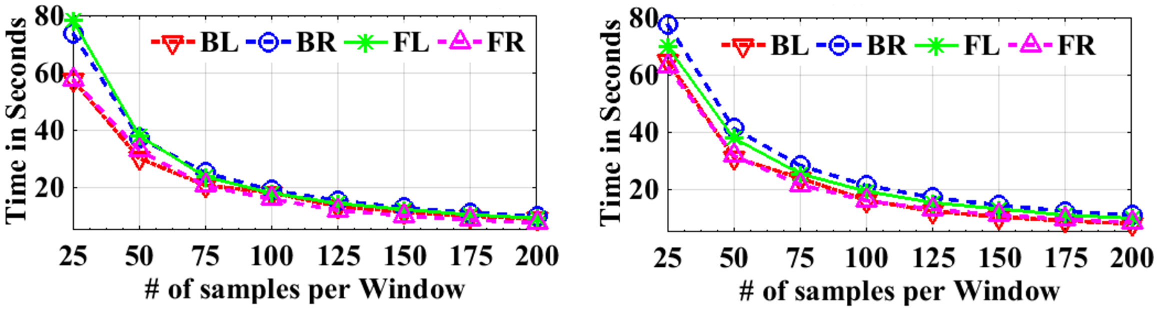
Fig. 6: Computational Time for Legitimate User Identification on the LACC data, with and without feature selection through ESP.

methodology for real-time applications.

From these results, we observe that the proposed feature selection and classification methods significantly increases the accuracy for legitimate user identification within each sub-activity for both sensors; additionally, outperforming on publicly available smartphone-based physical activity recognition (PAR) datasets.

Figure 4 presents the 99% confidence intervals, pertaining to the average legitimate user identification by using the pairwise T-test between groups with and without feature selection data at the 99% confidence level. Looking at Figure 4, significant statistical results are clearly seen, showing that the KELM method performs much better when selected features of data are used in all cases: an 80% and 88% to 99% performance increase. This leads us to prefer the use of the feature selection method in future applications.

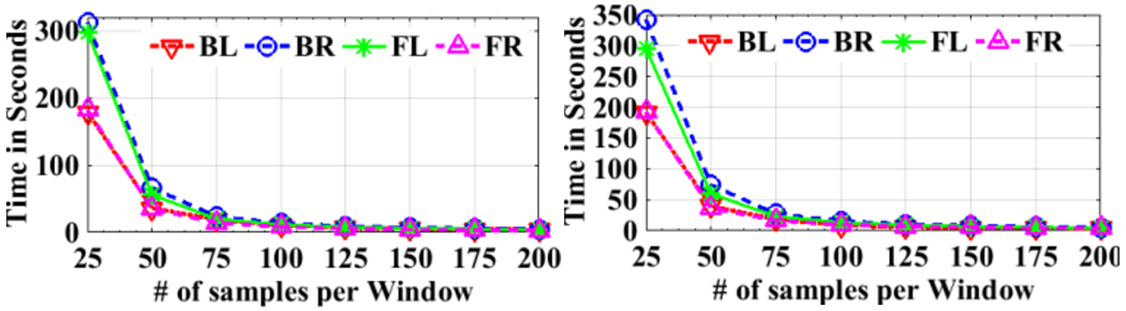
The KELM method provides acceptable performance and has numbers of other attractive features to its applicability.



(a): ACC Sensor

(b): LACC Sensor

Fig. 7: Computational Time for the feature extraction process for both sensors.



(a): ACC Sensor

(b): LACC Sensor

Fig. 8: Computational Time for the feature selection process for both sensors.

In term of the applicability within a smartphone system, the KELM has smaller confidence intervals, implying it has more reliability in training models. Since the structure of the network in the KELM is fixed, it has a better training and lower variance. This implies that systems using a connected network should keep a fixed connective structure, in order to increase its reliability. Holding a constant connective structure is a good feature for the network due to hardware constraints. Any potential manufacturer to capture this method into a chip, as trainable network, needs such a constant size structure. These chips could take away from the phones main CPU, thus increasing the speed of the legitimate user identification process. This, would allow for greater device security, by not allowing for software-based attacks on this method, only hardware based manipulations. These hardware operations would require access to the smartphone, hence making such attacks subject to the devices defense.

V. Conclusion and Future Work

This study substantiates the idea to be able to detect a legitimate smartphone user based on their walking patterns through various sub-activities in a semi-controlled environment. Having used a commonly available mass-market consumer hardware, such as our experimental platform, we have demonstrated its global applicability of our proposed method with minimal accuracy variations. The KELM requires minimal battery consumption, and in order for us to run it as a practical application, we need to limit the number of required samples; based on our results we observed that the KELM together with the ESP are the best methods in terms of accuracy and computational cost to a certain extent. However,the KELM is found to be the best examination method, in order to reduce battery consumption when performing checks to the sensor array.

Our future work will involve furthering the scope of this research by introducing new methodologies for feature selection, with better statistical significance. Another future direction for our current work will be to split the size of the smallest windows (25 or 50 samples per window) in to even smaller windows within the classification process for the KELM method, but for this, there is another challenge: how to maintain performance, within each sub-window, and how to control the computational complexity during real-time deployment.

References

1) Consumers Worldwide. Available online: Online: http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694, accessed on January 2017.
2) S. Zahid, et al., Keystroke-based user identification on smartphones, in Recent Advances in Intrusion Detection, ser. Lecture Notes in Computer Science, Springer, 2009, vol. 5758, pp. 224-243.

TABLE II: Average Accuracy and Confidence Intervals for Legitimate User Identification on Publically Available Dataset With Different Number of Sample Per Window

User	Metric	Samples Per Window							
		25	50	75	100	125	150	175	200
User 1	**Accuracy**	97.343±0.133	98.134±0.262	98.725±0.256	97.471±0.427	98.029±0.412	98.662±0.272	98.407±0.294	98.881±0.486
	Time	26.369±0.524	9.968±0.031	6.290±0.127	4.776±0.081	4.025±0.233	3.188±0.081	2.634±0.033	2.435±0.036
User 2	**Accuracy**	97.162±0.189	97.848±0.219	97.572±0.166	98.350±0.345	99.085±0.213	99.317±0.164	98.984±0.153	98.784±0.221
	Time	37.635±1.684	21.510±0.646	11.758±0.081	8.326±0.057	9.055±0.789	5.711±0.0937	5.007±0.173	4.311±0.137
User 3	**Accuracy**	97.302±0.135	97.652±0.189	97.686±0.257	98.394±0.189	99.364±0.193	98.849±0.341	98.719±0.261	98.229±0.389
	Time	27.128±0.494	11.413±0.478	6.881±0.052	4.896±0.047	3.916±0.025	3.104±0.009	2.702±0.060	2.551±0.061
User 4	**Accuracy**	96.955±0.129	97.906±0.224	98.522±0.216	98.492±0.251	98.661±0.204	98.420±0.334	98.250±0.218	98.301±0.544
	Time	26.321±0.759	11.244±0.207	6.172±0.025	4.554±0.014	3.568±0.031	3.265±0.147	2.673±0.027	2.529±0.087
User 5	**Accuracy**	97.906±0.123	98.529±0.250	98.268±0.168	98.822±0.219	98.504±0.315	99.090±0.145	98.609±0.349	98.909±0.274
	Time	22.744±0.054	9.908±0.036	7.089±0.045	6.436±0.229	3.945±0.025	3.322±0.061	2.907±0.036	2.603±0.028
User 6	**Accuracy**	97.607±0.124	98.180±0.165	97.926±0.125	97.939±0.203	98.426± 0.245	98.327±0.266	98.578±0.334	98.372±0.332
	Time	24.464±0.183	10.699±0.355	6.619±0.147	4.911±0.152	3.994±0.143	3.138± 0.039	2.729±0.036	2.356±0.009
User 7	**Accuracy**	96.953±0.195	97.718±0.241	98.107±0.168	98.617±0.175	98.984±0.161	98.193±0.235	98.453±0.260	98.354±0.489
	Time	24.884±0.746	9.903±0.089	6.281±0.101	4.646±0.123	3.736±0.109	3.107±0.028	2.827±0.057	2.459±0.037
User 8	**Accuracy**	97.672±0.158	97.803±0.141	97.418±0.254	98.769±0.194	98.259±0.231	98.246±0.339	98.516±0.391	99.016±0.344
	Time	23.326±0.052	10.892±0.489	6.509±0.201	4.629±0.135	3.591±0.028	3.212±0.074	2.660±0.018	2.359±0.012
User 9	**Accuracy**	97.233±0.135	97.598±0.230	98.087±0.208	98.243±0.346	99.754±0.149	98.046±0.254	98.109±0.352	98.837±0.438
	Time	23.169±0.179	9.925±0.064	6.508±0.237	4.614±0.052	3.573±0.011	3.130± 0.006	2.828±0.029	2.444±0.028
User 10	**Accuracy**	97.358±0.139	97.701±0.201	97.98±0.253	98.145±0.345	98.560±0.197	98.139±0.390	98.406±0.269	98.766±0.344
	Time	24.652±0.698	10.447±0.333	6.305±0.034	4.542±0.037	3.709±0.012	3.055±0.012	2.808±0.113	2.485±0.058
User 11	**Accuracy**	97.331±0.106	97.785±0.268	97.371±0.241	97.743±0.208	98.471±0.149	98.527±0.253	98.578±0.443	98.497±0.240
	Time	23.785±0.125	11.418±0.287	6.889±0.169	4.900±0.114	3.810±0.029	3.257±0.031	2.892±0.115	2.464±0.013
User 12	**Accuracy**	98.193±0.135	98.088±0.159	98.054±0.185	98.519±0.252	98.929±0.157	97.912±0.361	98.688±0.426	98.784±0.303
	Time	25.832±0.332	10.129±0.127	6.239±0.135	4.424±0.022	3.568±0.026	2.998±0.005	2.886±0.037	2.481±0.019
User 13	**Accuracy**	98.071±0.165	97.442±0.171	98.033±0.177	98.234±0.206	98.583±0.201	98.434±0.332	98.625±0.312	98.873±0.335
	Time	22.773±0.214	11.175±0.043	7.054±0.310	4.891±0.093	3.913±0.055	3.448±0.098	2.972±0.065	2.473±0.017
User 14	**Accuracy**	97.331±0.167	97.963±0.183	98.328±0.199	97.806±0.262	98.471±0.284	98.005±0.229	98.563±0.257	97.567±0.536
	Time	23.38±0.444	11.361±0.167	6.584±0.252	4.812±0.095	3.818±0.018	3.296±0.067	2.809 ±0.016	2.513±0.034
User 15	**Accuracy**	97.607±0.102	98.837±0.122	98.662±0.239	98.805±0.221	98.672±0.256	98.554±0.284	98.953±0.277	98.426±0.442
	Time	23.563±0.259	9.801±0.029	8.238±0.128	4.999±0.111	3.543±0.026	3.234±0.032	2.888±0.045	2.517±0.020
User 16	**Accuracy**	97.603±0.192	98.476±0.157	97.766±0.209	98.689±0.147	98.281± 0.318	98.876±0.245	98.484±0.278	98.623±0.384
	Time	24.384±0.752	10.9± 0.037	6.077±0.033	4.649±0.068	3.679±0.064	3.122±0.016	2.815±0.056	2.385±0.008

3) X. Wang, An intrusion-tolerant password authentication system, In proc. of 19th IEEE annual Computer Security Applications, IEEE, pp. 110-118, 2003.
4) J. Angulo, and E. Wastlund, Exploring touch-screen biometrics for user identification on smartphones, In proc. of Springer, IFIP Advances in Information and Communication Technology, pp. 130-143, 2012.
5) T. Feng,et al., TIPS: Contextaware implicit user identification using touch screen in uncontrolled environments, In proc. ACM-HotMobile, 15th Workshop on Mobile Computing Systems and Applications, ACM, pp. 1-6, 2014.
6) N. Fukumoto, et al.,Passive smart phone identification and tracking with application set fingerprints, In proc. of the APAN-Network Research Workshop, vol. 36, pp. 41-48, 2013.
7) A. Dandachi, A novel identification/verification model using smartphones sensors and user behavior, In proc. of IEEE, 2nd International Conference on Advances in Biomedical Engineering, IEEE, pp. 235-238, 2013.
8) W. Shi, et al., Senguard: Passive user identification on smartphones using multiple sensors, In proc. of 7th IEEE International Conference on Wireless and Mobile Computing (WiMob), Networking and Communications, IEEE, pp. 141-148, 2011.
9) C. Bo, et al., Silentsense: Silent user identification via dynamics of touch and movement behavioral biometrics, In proc. of ACM, 19th annual International Conference on Mobile computing and networking, ACM, pp. 187-190, 2013.
10) M. Boyle, et al, Gait-based smartphone user identification,In proc. of ACM MobiSys, ACM, pp. 395-396, 2011.
11) M. Ahmad, et al, Gait Fingerprinting based User Identification on Smartphones, In proc. of IEEE, International Joint Conference on Neural Networks (IJCNN) in Conjunction with World Congress on Computational Intelligence (WCCI), IEEE, pp. 3060-3067, 2016.
12) J. Mantyjarvi, et al, ”Identifying users of portable devices from gait pattern with accelerometers”, In proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing, IEEE, vol. 2, pp. 973-976, 2005.
13) N. Sae-Bae, et al, Biometric rich gestures: a novel approach to authentication on multi-touch devices, In proc. of ACM, SIGCHI Conference on Human Factors in Computing Systems, ACM, pp. 977-986, 2012.
14) P. Marcus, et al, Securing mobile device-based machine interactions with user location histories, In proc. springer, 4th International Conference on MobiSec, Springer, vol. 107, pp. 81-92, 2012.
15) H. Lu, et al, Speakersense: Energy efficient unobtrusive speaker identification on mobile phones,In proc. of Springer, 9th International Conference on Pervasive Computing, Springer, vol. 6696, pp. 188-205,2011.
16) T. Feng, et al, Continuous mobile authentication using touch screen gestures, In proc. of IEEE Conference on Technologies for Homeland Security (HST), IEEE, pp. 451-456, 2012.
17) A. De Luca, et al, Touch me once and i know its you: implicit authentication based on touch screen patterns, In proc. of

ACM Conference on Human Factors in Computing Systems (SIGCHI), ACM, pp. 987-996, 2012.

18) N. Sae-Bae, et al, Investigating multi-touch gestures as a novel biometric modality, In proc. of IEEE, 5^{th} International Conference of Biometrics, Theory, Applications and Systems (BTAS), pp. 156-161, 2012.
19) M. Frank, et al, Touch analytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication, IEEE Transactions on Information Forensics and Security, 2013, vol. 8(1), pp. 136-148.
20) M. Shahzad, et al, Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you cannot do it, In proc. of ACM, 19^{th} International Conference on Mobile Computing and Networking (MobiCom), ACM, pp. 39-50, 2013.
21) J. C. D. Lima, et al, A Context aware recommendation system to behavioral based authentication in mobile and pervasive environments, In proc. of 9^{th} IEEE International Conference on Embedded and Ubiquitous Computing (IFIP), IEEE, pp. 312-319, 2011.
22) C. C. Rocha, et at, A2BeST: An adaptative authentication service based on mobile user's behavior and spatio temporal context, In proc. of IEEE Symposium on Computers and Communications (ISCC), IEEE, pp. 771-774, 2011.
23) N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis", International Journal of Information Security, vol. 6(1), pp. 1-14, 2007.
24) J. Koreman, et al, Multi-modal biometric authentication on the secure phone pda, In proc. of MMUA Workshop on Mult-Modal User Authentication, 2006.
25) D. Gafurov, et al, Biometric gait authentication using accelerometer sensor, Journal of Computers, 2006, vol. 1(7), pp. 51-59.
26) K. R. Cuntoor, et al, Gait-based recognition of humans using continuous hmms, In proc. of 5^{th} IEEE International Conference on Automatic Face and Gesture Recognition, IEEE, pp. 321-326, 2002.
27) M. Jakobsson, et al, Implicit authentication for mobile devices, In proc. of 4^{th} USENIX Workshop on Hot Topics in Security (HotSec), pp. 9, 2009.
28) P. Casale, et al, Personalization and user verification in wearable systems using biometric walking patterns, Personal and Ubiquitous Computing, 2012, vol. 16(5), pp. 563-580.
29) J. Mantyjarvi, et al, Identifying users of portable devices from gait pattern with accelerometers, In proc. of Acoustics, Speech, and Signal Processing (ICASSP), vol. 2, pp. ii 973, 2005.
30) L. Rong, Z. Jianzhong, L. Ming, H. Xiangfeng, A wearable acceleration sensor system for gait recognition, In proc. of 2^{nd} IEEE Conference on Industrial Electronics and Applications (ICIEA), IEEE, pp. 2654-2659, 2007.
31) M. O. Derawi, et al, Unobtrusive user authentication on mobile phones using biometric gait recognition, In proc. of 6^{th} International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 306-311, 2010.
32) D. Gafurov, et al, Improved gait recognition performance using cycle matching, In proc. of 24^{th} IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA), IEEE, pp. 836-841, 2010.
33) M. O. Derawi, et al, Improved cycle detection for accelerometer based gait authentication, In proc. of 6^{th} International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 312-317, 2010.
34) P. Bours, and R. Shrestha, Eigensteps: a giant leap for gait recognition, In proc. of 2^{nd} international Workshop on Security and Communication Networks (IWSCN), pp. 1-6, 2010.
35) D. Gafurov, E. Snekkenes and P. Bours, Gait Authentication and Identification Using Wearable Accelerometer Sensor, In proc. of IEEE Workshop on Automatic Identification Advanced Technologies, IEEE, pp. 220-225, 2007.
36) G. Dandachi, et al, A novel identification/verification model using smartphone's sensors and user behavior, In proc. of 2^{nd} IEEE International Conference on Advances in Biomedical Engineering, IEEE, pp. 235-238, 2013.
37) T.R.D. Saputri, et al, User Independent Activity Recognition via Three-Stage GA-Based Feature Selection, International Journal of Distributed Sensor Networks, 2014, vol 2014.
38) J. L. R. Ortiz, et al, Transition-Aware Human Activity Recognition Using Smartphones, Neurocomputing, vol. 171, pp. 754-767, 2015.
https://archive.ics.uci.edu/ml/datasets/Human+Activity +Recognition+Using+Smartphones, Accessed on January, 2017.
39) M. Fahim, et al, EFM: evolutionary fuzzy model for dynamic activities recognition using a smartphone accelerometer, Applied Intelligence, 2013, vol. 39(3), pp. 475-488.
40) W. S. William and S. Wei, Time Series Analysis: Univariate and Multivariate Methods, 1990.
41) R. P. Haining, The moving average model for spatial interaction, Transactions of the Institute of British Geographers, 1978, vol. 3(2), pp. 202-225.
42) V.Cuomo, et al, Autoregressive models as a tool to discriminate chaos from randomness in geo electrical time series: an application to earthquake prediction, Journal of Annals of Geophysics, 1997, vol. 40(2), pp. 385-400.
43) C. Chatfield, The Analysis of Time Series: An Introduction, CRC Press, 2003.
44) G. E. Box, et al, Time Series Analysis: Forecasting and Control, John Wiley and Sons, 2013.
45) O. D. Anderson, Time series analysis and forecasting: another look at the Box-Jenkins approach, Journal of Royal Statistical Society Series D the Statistician, 1977, vol. 26(4), pp. 285-303.
46) A. M. Khan, M. H. Saddiqi, and S.-W. Lee, Exploratory Data Analysis of Acceleration Signals to Select Light-Weight and Accurate Features for Real-Time Activity Recognition on Smartphones, 2013, Sensors, vol. 13(10), pp. 13099-13122.
47) A. M. Khan, et al, Activity Recognition on Smartphones via Sensor-Fusion and KDA-Based SVMs, International Journal of Distributed Sensor Networks, 2014, vol. 2014, Article ID 503291, pp.14.
48) L. Ladha and T. Deepa, Feature selection methods and algorithms, International Journal on Computer Science and Engineering, 2011, vol. 3(5), pp. 1787-1797.
49) B. Yu and B. Yuan, A more efficient branch and bound algorithm for feature selection, Pattern Recognition, 1993, vol. 26(6), pp. 883-889.
50) A. M. Khan, et al., A triaxial accelerometer-based physical-activity recognition via augmented-signal features and a hierarchical recognizer, IEEE Transactions on Information Technology in Biomedicine, 2010, vol. 14(5), pp. 1166-1172.
51) Kohonen, Self-Organizing Maps, Springer Series in Information Sciences. Springer, Berlin, 1995.
52) Al Jeroudi, et al, Online sequential extreme learning machine algorithm based human activity recognition using inertial data, In proc. of 10^{th} IEEE Control Conference (ASCC), IEEE, pp. 1-6, 2015.
53) G. B. Huang, D. H. Wang, and Y. Lan, Extreme Learning Machines: a Survey, International journal of Machine Learning and Cybernetics, 2011, vol. 2(2), pp. 107-122.
54) R. C. Eberhart and J. Kennedy, New optimizer using particle swarm theory, in proc. of 6^{th} International Symposium on Micro Machine and Human Science, pp. 39-43, 1995.
55) G. B. Huang, et al, Extreme Learning Machine for Regression and Multi class Classification, IEEE transactions on systems, man and cybernetics, 2012, vol 42(2), pp. 513-529.