Hindawi
Mobile Information Systems
Volume 2018, Article ID 5107024, 14 pages
https://doi.org/10.1155/2018/5107024

Research Article

Smartwatch-Based Legitimate User Identification for Cloud-Based Secure Services

Muhammad Ahmad[1,2] **Mohammed A. Alqarni,**[3] **Asad Khan,**[4] **Adil Khan,**[1] **Sajjad Hussain Chauhdary,**[3] **Manuel Mazzara,**[5] **Tariq Umer**[6] **and Salvatore Distefano**[2]

[1]*Institute of Robotics, Innopolis University, Innopolis, 420500 Kazan, Tatarstan, Russia*
[2]*University of Messina, Messina, Italy*
[3]*Faculty of Computing and Information Technology, University of Jeddah, Saudi Arabia*
[4]*Graphic and Computing Lab, School of Computer Science, South China Normal University, Guangzhou, China*
[5]*Director of Institute of Technologies and Software Development, Head of Service Science and Engineering Lab, Innopolis University, Innopolis, 420500 Kazan, Tatarstan, Russia*
[6]*Department of Computer Science, COMSATS University, Wah Campus, Islamabad, Pakistan*

Correspondence should be addressed to Muhammad Ahmad; mahmad00@gmail.com

Received 15 May 2018; Accepted 5 July 2018; Published 14 August 2018

Academic Editor: Syed Hassan Ahmed

Smartphones are ubiquitously integrated into our home and work environment and users frequently use them as the portal to cloud-based secure services. Since smartphones can easily be stolen or coopted, the advent of smartwatches provides an intriguing platform legitimate user identification for applications like online banking and many other cloud-based services. However, to access security-critical online services, it is highly desirable to accurately identifying the legitimate user accessing such services and data whether coming from the cloud or any other source. Such identification must be done in an automatic and non-bypassable way. For such applications, this work proposes a two-fold feasibility study; (1) activity recognition and (2) gait-based legitimate user identification based on individual activity. To achieve the above-said goals, the first aim of this work was to propose a semicontrolled environment system which overcomes the limitations of users' age, gender, and smartwatch wearing style. The second aim of this work was to investigate the ambulatory activity performed by any user. Thus, this paper proposes a novel system for implicit and continuous legitimate user identification based on their behavioral characteristics by leveraging the sensors already ubiquitously built into smartwatches. The design system gives legitimate user identification using machine learning techniques and multiple sensory data with 98.68% accuracy.

1. Introduction

We are living in an era of context-aware systems whose aim is to acquire a user's context and reason on it to change a system's behavior to match the user's changing situation [1]. Making user's context information available to such systems is a critical task, and one such information is the identity of the user. Furthermore, today's era is an era of smart devices such as smartphones (SP), smartwatches (SW), smart TVs, and even smarthomes (SHs). The modern SWs consist of extensive computing power, different sensors, and the ability to communicate with other smart devices, for example, SH and SP via Bluetooth or the WIFI. SWs are a comparatively new expansion and probably the first SW to be truly modern and smart "The Pebble" became available in early 2013 [2].

In 2014, many other SWs were released, and almost all of these operate with Android phones and run the Android Wear subsystem. These SWs include the Moto 360, Sony SW 3, LG G, and Samsung Gear. While the sale of these SWs has recently been modest, the introduction of the Apple watch in 2015 greatly increased interest in such devices. It is now clear

that SWs have become as ubiquitous as SPs, and current market projections indicate that nearly 400 million SWs will ship by 2020 which is 25 times greater than 2014 sales [2, 3].

Modern SWs are equipped with a variety of motion sensors that are useful for monitoring device movements like tilt, rotate, and shake. Some of these sensors are the ambient light sensor, accelerometer, compass, gyroscope, magnetometer, and GPS sensors. These sensors support similar capabilities and applications of smartphones such as healthcare applications that require physical activity recognition (PAR). The accelerometer, linear accelerometer, magnetometer, and gyroscope sensors are ideal for PAR and gait-based legitimate user identification over SPs [4–7]. This work will show that SWs are equally capable of performing PAR and gait-based legitimate user identification.

The proposed legitimate user identification model uses a personal (single predictive) model to identify a user within a group of users. Finally, the identification model uses a predictive model to determine if an unknown user is a legitimate user or is an impostor. This work utilizes SWs and SPs to collect and store sensor data from three different sensors. These sensors include accelerometer, magnetometer, and gyroscope sensors. The data collected by these sensors were ultimately sent to the computer for further processing. This work utilizes the Android-based SPs and SWs because these devices are easily available in the market at low price.

Gait-based legitimate user identification on SWs has several advantages over the SPs, for example, portability, location, and orientation that almost remain stable which are quite important advantages over SPs. Both the location and orientation of SP may diverge, depending on the user's style of wearing and on the activity that the user is performing. Change in any of the above-discussed issues will reduce the effectiveness. Furthermore, some locations and positions simply do not generate the appropriate signatures for legitimate identification. Explicitly, the issue of orientation and location occurs with females because they frequently bring their SPs off the body, but in case of SW, the device will be carried in a fix position such as on the wrist almost all the time. Above all, a SW can easily transmit the data to other paired devices using Internet or Bluetooth which is evident that the SWs are superior for user identification for cloud-based secure applications like Internet banking or to access SHs.

To support the above-said discussion, we found that recently a South Korean telecommunication company named SK Telecommunication started working towards a system meant to use SW to provide legitimate user identification, in order to access a secure online banking application [8]. However, banking applications normally use security similar to that of most other applications, where accessing your bank online requires a special randomized key from your bank or a special USB drive or any other secure identification means. A custom-designed user identification application will simply allow customers to tap on their registered SW to access their online banking system without much effort. In addition to this, the online system is subject to powerful encryption at both ends to secure the user personal information.

Keeping in mind the computational sources of SWs, the proposed system will be fairly simple as the user only needs to register the SW to use it in conjunction with any digital banking portals to authorize legitimate user access. Once a user is registered, it presumably involves some sort of verification and identification or the user's SW can be given a tap while running the correct software for identification as a legitimate user. If the SW is lost or stolen, the user can pass a kill command to nullify the online access by SW. This system has a number of different possible ways in which it could pair up and identified a legitimate user on SW, and our proposed solution can be a foundation for such secure applications.

In addition to the above, SW-based legitimate user identification can support many other real-life applications, for example, acting as the foundation for a delegated identification system for SH. More specifically, while a legitimate user is approaching their SH, their SW transmits its sensor signal to the SH which would compare it with the previously sent signals, and if sensor signal matched, then it would open the door. The proposed solution can also be used for such kind of secure systems to identify a legitimate user with an acceptable accuracy with least computational power and time.

The rest of the paper is organized as follows: Section 2 describes the related work. Section 3 presents the procedure for collecting the raw signals from the six users performing five different activities and how the raw signal is transformed into a suitable format for machine learning algorithms. The results of these experiments are presented in Section 4. Section 5 discusses the immediate future extensions to the current research. Finally, Section 6 concludes the work.

2. Related Work

Recently, wearable devices like SWs have emerged in our daily lives. However, limited research has been done on legitimate user identification by these wearable devices. Besides, these several traditional legitimate user identification approaches have been proposed based on passwords such as secret information possession and physiological biometrics such as iris patterns and fingerprints. More recently, behavior-based legitimate user identification utilizes the distinct behavior of users such as gestures and gaits [5, 7].

Different physiological biometrics for legitimate user identification systems are out there, such as iris patterns [9], fingerprints [10], and face patterns. However, such legitimate user identification requires user interactions. For example, fingerprint identification needs users to put their finger on the scanner. Hence, these approaches requiring user compliance cannot achieve continuous and implicit identification [11] which was an ultimate goal of our proposed system to overcome.

In contrast to above-discussed solutions, behavior-based legitimate user identification assumes that the people have distinct but stable patterns for a certain behavior such as gait [5, 7, 12], handwriting patterns [13, 14], and GPS patterns [15]. Such legitimate user identification exploits users' behavioral patterns to identify a legitimate user. Some

important and classical works from the literature in the area that specifically use built-in sensors for legitimate user identification are discussed below.

Kayacik et al. [16] proposed a temporally and spatially aware user behavioral lightweight model based on hard and soft sensors. For some reason, they did not quantitatively show the legitimate identification performance, but they have shown that the attackers can be detected in 717 seconds. Buthpitiya et al. [15] proposed a GPS sensor-based system that could detect abnormal activities by analyzing legitimate users' location history. Trojahn and Ortmeier [14] and Shahzad et al. [13] have developed a mixture of a handwriting and keystroke-based method to achieve legitimate user identification through the screen sensor. Zhu et al. [17] proposed a system which constantly collects the data from three different built-in sensors namely the gyroscope, magnetometer, and accelerometer to construct gesture models while a legitimate user is using the device. Nickel et al. [12] proposed an accelerometer-based behavior recognition system for legitimate user identification using a k-nearest neighbor-based classification algorithm. Lee et al. [18, 19] empirically proved that using more sensors can improve legitimate user identification performance by using a support vector machine (SVM) as a final classification algorithm. Li et al. [20] proposed five basic movements, namely, sliding up, sliding down, sliding right, sliding left, and tapping and their related combinations as legitimate user behavioral patterns with which to perform legitimate user identification.

In regards to the works discussed above, Riva et al. [21] proposed a prototype using voice recognition, phone placement, and face recognition proximity to progressively identify a legitimate user. However, their objectives were just to decide when to identify the legitimate user and thus not match to the proposed framework. Furthermore, their scheme requires access to sensors that need users' permissions, which limiting their application for implicit legitimate user identification in a real-time environment. Mare et al. [22] proposed a two-fold legitimate user identification model in which the signals sent from a bracelet worn on the user's wrist are correlated with the operations of the terminal to confirm the continued presence of the user if the two movements correlate according to a few coarse-grained actions. Lee and Lee [11] proposed a legitimate user identification system named iAuth for implicit but continuous user identification in which the end user is identified based on their behavioral characteristics by leveraging the built-in sensors. They have built a system which gives better identification than previously possible using sensor data from multiple devices and machine learning techniques. Their system was able to consume only 2% of the battery to produce 92.1% accuracy.

To the best of our knowledge, there is no SW gait-based legitimate user identification research proposed in the literature that works in the way this one does including the ones discussed above. This study takes the advantage of the idea of identifying a legitimate user on SW by employing different activity patterns. Data on different activities are recorded using the embedded triaxial without limiting the scope only to a controlled environment. The aim of this work is to propose a semicontrolled environment system in which the proposed system overcomes the limitations of users' age, gender, SW wearing style (left or right hand), and regular activity style while wearing a SW. The user was enforced to perform daily activity differently at different times because the goal was to investigate the ambulatory activity performed by any user towards legitimate user identification in real-time scenarios.

Thus, this work introduces a novel two-fold legitimate user identification system in which the proposed system first recognizes the activity and then the identification process comes in to decide whether the recognized activity has been performed by a legitimate user or imposture. Additionally, this work experiments with a single-subject-cross-validation process to further validate a legitimate user identification. The proposed system is a semicontrolled environment-based activity recognition and legitimate user identification system.

3. System Modeling

This section describes the process for collecting the raw signals from different users performing different physical activities under study. This section also explains the process for extracting the meaningful features. Furthermore, we will explain the process of transforming the time series raw sensor signals into examples that can be handled by different classifiers from machine learning literature, for example, Decision Tree (DT), K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and Naive Bayes (NB).

3.1. Data Collection. The raw signals were collected for five different activities from six users (three female and three male) having a mean age of twenty-five years old. The criterion for selecting the subjects was based on gender because different genders exhibit different patterns when performing the same activity. These activities include walking, walking upstairs, walking downstairs, running, and jogging. All subjects performed these activities twice each day for more than a month. Therefore, the proposed system utilizes the collected raw data from the same users for the same activity but performed on different days.

The participants enrolled in this study were approved by the laboratory head. This is a formal prerequisite because the experiments involved human subjects although there was a negligible risk of injury. The involved subjects were asked to answer a few nontechnical questions about their gender, age, height, weight, left-or-right handedness, and so on, which were used as characteristics in the proposed study. Then the subjects were asked to fasten the SW on their wrist and place a Bluetooth paired SP in their pocket. Both devices run a simple custom-designed application that controls the data collection process and instructs the participant to add their name and select the activity from the list of five different activities and the sensor from three different sensors. Once the initial instructions have been completed, the SP screen is turned off and placed into the pants pocket. The SP

instructs the SW running the paired data collection application to collect the raw signal at a rate of 20 Hz. Each of these sensors generates 3-dimensional signals and appends a timestamp to the values. After every five minutes, the SW sends the data to the SP, and after a successful transmission, the SP vibrates to notify the user that the data collection process has been successfully completed and they can stop the current activity.

3.2. Feature Extraction. SW sensor measurements are of the form (X, Y, Z) where X, Y, and Z are, respectively, the X, Y, and Z components of the acceleration relative to the smartwatch. The proposed system systematically removes the gravity component from each of the X, Y, and Z measurements. Raw accelerometer measurements are quite noisy since even a SW in a fixed position could return sensor measurements depicting bursts of acceleration. To minimize the effect of noise, the proposed system used a simple moving average based on a window of 3 points for each of the X, Y, and Z components. For each component, the smoothed time series was then broken into windows.

There are plenty of ways to prepare the raw sensor signals prior to using them for legitimate user identification. Some gait-based works utilized the data within the time domain [23–25] but other systems map the time series sensor data onto examples using a sliding window approach. This technique permits the use of traditional machine learning classification approaches to handling the time series data. Our proposed study also utilizes the same sliding window approach employed in the prior work [2, 5–7].

The discussed windowing process initially partitions the time series raw signal into 30 seconds non-overlapping windows. Then, from each window, the system generates relatively simple features (together with time and frequency) for each sensor individually but uses the same encoding technique [2]. Each feature is calculated from each axis of the raw signal. Since the data are sampled at 20 Hz and the window size is 30 seconds (which includes 25 samples within each iteration), there are 600 time series values per axis per window and 1800 values per window for three sensors. During the feature extraction process, the proposed system changes the window size from 25 samples per window to up to 400 samples per window in different experiments to further validate the behavior of window size for legitimate user identification.

The said process holds for all three sensors' data, and each of these time series values is transformed into 72 features using the feature encoding. The extracted features are average acceleration, average absolute difference, standard deviation, and average resultant acceleration, in which 1 feature for each axis is obtained (in total 4 features per axis), the average difference between peaks (10 features for each axis). Our system also calculates the binned distribution in which the proposed system determines what fraction of readings fall within a 10 equal-sized bins, and this function generates 10 features for each axis individually.

3.3. Classifiers. This work leverages the different classifiers available in Matlab. The literature has highlighted that each classifier will have varying results depending on what the proposed system is predicting. The training process involves learning in relation to the label user wants to predict [26]. For experimental setup, the proposed system involved four different types of classifiers, for example, DT, KNN, SVM, and NB in order to compare the performance.

3.3.1. Decision Tree (DT). In DTs, the input space is first separated by class regions to determine the DTs. Nodes are generated with decision functions that branch depending on the output of a decision. As one traverses from root to leaf, the classifier effectively narrows the prediction space until it reaches its final prediction at the leaf. Decision trees bring scalable and fast implementation with the need to tune many parameters [26].

3.3.2. K-Nearest Neighbors (KNN). When classifying a given unseen feature vector, KNN will find the k-nearest points given a distance function, look at all k training labels, and predict the label as the majority of the k labels. An advantage of KNN is its robustness against noisy data, and there is only the number of nearest neighbors which needs to carefully tune [26]. It is an instance-based classifier which is also one of the most popular classifiers used for SP-based PAR and is found to be the best in terms of performance and computational complexity as compared to the decision trees [27].

3.3.3. Support Vector Machine (SVM). SVM recognizes a diverse set of physical activities using motion and other sensors, and the literature has highlighted that their performance is superior to that of the other classifiers [28].

3.3.4. Naive Bayes (NB). NB is a simple and well-known classification method. NB is a probabilistic classifier [30], and Bayes' rule contains probabilistic models. Bayes' rule relies on the statistical properties of data and the accuracy of data. To begin with, it finds the solution from statistics as well as by data mining [29]. All of these classification methods are suitable for real-time legitimate user identification because they can be generated and evaluated rapidly.

The values used for the different parameters of the classification methods are as follows: SVM is used with a quadratic kernel function; KNN is used with a Euclidean distance function, and nearest neighbors are set to 10; DT is used with 85 as the number of trees. All the said parameters are carefully tuned and optimized prior to the final experimental setups. All the experiments are carried out using Matlab R2014b and installed on core i5 and 8 GB of RAM machine.

4. System Setup

The output of each classifier result is a strong indicator of the system's ability to predict the legitimate user of the SW. 10-fold-cross-validation has been performed to extract the meaningful information for each legitimate user. In each experiment, the user's data are split into 10 subsets in which

a single subset is chosen as a validation set towards legitimate user identification and the rest of the 9 subsets are used as training data to be fed into each classifier individually. Classifier results are generated with the given setup with every instance in the validation set being classified against the training sets. This entire process is repeated for every activity and each user and for all three sensors by picking each subsequent subset as a validation set with the reaming as the training set. Leading to a total of 30 experiments for a single sensor's data, 90 experiments for all 3 sensors and 360 experiments for all four classifiers which are weighted for the final results to identify either a legitimate user or imposture.

4.1. Experimental Setup. The first experimental setup compared the performance of four different classifiers for three different sensors data for a fixed number of samples per window, after which each classifier was chosen and tested multiple times while changing the number of samples per window, that is, 25, 50, 75, 100, 125, 150, 175, 200, 225, 250, 275, 300, 325, 350, 375, and 400 samples. The main goal of our second experiment was to measure the effect of changing the window size on the performance of each classifier. In both experimental setups, the training and testing data are randomly divided, and classification results are obtained using a 10-fold-cross-validation process.

4.2. Experimental Results. The SW gait-based legitimate user identification task is first to identify a user from a pool of users and then to verify that specific user can access the device based on a sample of the user's performed activities taken from the selected sensor. This process requires the training data from all the users and their performed activities. Such experiments seem fairly simple, such as the transformed data associated with the sensor data are individually used to train and evaluate using 10-cross-validation. In the identification process, each user has its own classification model, and when a sample is provided, the model determines whether the sample belongs to the legitimate user or to an imposter. This identification experiments and evaluates a model for each of the 6 participants in the study, and in each case, each activity is considered independently.

Here, we turn to the first experimental results, in which we used a fixed sample size in each window. Table 1 shows the raw accuracy for legitimate user identification for three different sensors and four classifiers based on the performed activities. Straight walking activity-based legitimate user identification using the accelerometer sensor performed better than the other activity-based methods over a DT classifier with an accuracy of 98.68%.

These results show that even 400 samples per window are sufficient to identify a user most of the time especially if one uses the accelerometer data with a classifier other than NB. Here, one can note that the accelerometer sensor data are clearly more informative and helpful in identifying a legitimate user than the magnetometer and gyroscope data.

The gait-based legitimate user identification process explained above involves building a single predictive model to first identify a specific user from a set of users and then deciding whether the identified user is legitimate or an impostor. At the lowest level, the results are based on identifying an individual user based on 400 samples per window of data for different activities performed at different times. However, one can improve the proposed model by using more data and then employing a majority voting scheme to identify a legitimate user from the pool of different users.

In order to demonstrate how this scheme works and to provide greater insight into the results, confusion matrices are generated for each user which is presented in the following tables. Due to space limitations, Table 1 shows the overall results only for legitimate user identification based on different activities performed by the legitimate user or impostor. The results shown in the tables are based on an identification model generated from three sensors' data and four different classifiers.

The columns in Tables 2 and 3 correspond to the predicted users and the rows correspond to the actual users. Thus, the values in the diagonal in boldface correspond to correct identification of the legitimate user while the rest of the values correspond to identification of an impostor as a legitimate user or vice versa. The obtained results clearly indicate the ability of the proposed model to correctly identify the legitimate user. Based on the stated results, one can compute the accuracy for identifying a legitimate user or accuracy for aggregated overall six users. For example, the accuracy for correctly identifying the legitimate user 1 is almost 97.81% while the accuracy for identifying the legitimate user 2 is 98.26%. Whereas, the overall accuracy would be simply the total number of correct predictions divided by the total number of predictions in the case of a DT classifier using accelerometer sensor data.

The corresponding results interpreted with the most predicted legitimate user strategy are shown in Tables 1–3 within a fixed size of the window for each activity. This strategy always leads to perfect results except for the case of NB classifier. Based on a visual inspection of the confusion matrices and based on the fact that there is usually no second user who gets nearly as many votes as the actual user. We believe that for the population used in this experiment, one could get perfect legitimate user identification accuracy using fairly small samples of data.

For trusted external judgments and for statistical analysis of any legitimate user identification system, true positive, true negative, false positive, and false negative are usually compared. The terms true and false refer to whether the prediction corresponds to the external judgment or not and the terms positive and negative refer to the classifier's prediction. The test names in Tables 4 and 5 are abbreviated as TPR = true positive rate, TNR = true negative rate, FPR = false positive rate, FNR = false negative rate, PPV = positive predictive values, NPV = negative predictive values, SEN = sensitivity, SEP = specificity, FDR = false discovery rate, FOR = false omission rate, and ACC = individual user identification accuracy.

Table 1: Average accuracy for legitimate user identification with 400 samples per window.

Sensor	Activities	Classifiers			
		DT	SVM	KNN	NB
Acc.	Walking	**0.9868 ± 0.0094**	0.9391 ± 0.0181	0.9375 ± 0.0171	0.7616 ± 0.0201
	Walking up	**0.8753 ± 0.0327**	0.8005 ± 0.0422	0.7874 ± 0.0388	0.5876 ± 0.0540
	Walking down	**0.8835 ± 0.0383**	0.8447 ± 0.0534	0.7831 ± 0.0598	0.5619 ± 0.0909
	Running	**0.8168 ± 0.0363**	0.6381 ± 0.0554	0.5969 ± 0.0477	0.5311 ± 0.0325
	Jogging	**0.9572 ± 0.0147**	0.8816 ± 0.0163	0.9260 ± 0.0236	0.6234 ± 0.0384
Gyr.	Walking	**0.9638 ± 0.0115**	0.9177 ± 0.0268	0.9504 ± 0.0066	0.5149 ± 0.0367
	Walking up	**0.8575 ± 0.0389**	0.8362 ± 0.0333	0.8313 ± 0.0181	0.5423 ± 0.0683
	Walking down	**0.8983 ± 0.0453**	0.8062 ± 0.0339	0.8126 ± 0.0225	0.5476 ± 0.0595
	Running	**0.8521 ± 0.0651**	0.6737 ± 0.0390	0.7359 ± 0.0220	0.5866 ± 0.0483
	Jogging	**0.9424 ± 0.0163**	0.8964 ± 0.0272	0.8903 ± 0.0095	0.6629 ± 0.0376
Mag.	Walking	**0.9193 ± 0.0208**	0.7699 ± 0.0259	0.8551 ± 0.0339	0.6777 ± 0.0339
	Walking up	**0.7600 ± 0.0549**	0.5951 ± 0.0486	0.7107 ± 0.0405	0.5907 ± 0.0674
	Walking down	**0.8298 ± 0.0543**	0.7233 ± 0.0486	0.7055 ± 0.0671	0.5826 ± 0.0716
	Running	**0.6384 ± 0.0611**	0.5768 ± 0.0339	0.5916 ± 0.0481	0.3524 ± 0.0589
	Jogging	**0.7056 ± 0.0461**	0.4637 ± 0.0419	0.5873 ± 0.0361	0.3340 ± 0.0287

Table 2: Confusion matrix according to the users using 400 samples per window with accelerometer and gyroscope sensors.

Users	Accelerometer sensor						Gyroscope sensor					
	User 1	User 2	User 3	User 4	User 5	User 6	User 1	User 2	User 3	User 4	User 5	User 6
DT classifier												
User 1	**1710**	2	6	40	1	42	**1246**	1	0	12	3	44
User 2	0	**1796**	48	9	35	6	29	**1889**	42	1	78	17
User 3	0	40	**1774**	31	125	0	1	19	**1772**	30	123	15
User 4	12	13	11	**1695**	18	45	32	7	19	**1699**	7	31
User 5	18	24	40	2	**1457**	0	0	21	69	0	**1476**	4
User 6	121	16	3	49	1	**1880**	140	2	4	30	0	**1895**
SVM classifier												
User 1	**1473**	16	27	76	28	135	**1511**	32	9	63	1	100
User 2	9	**1597**	91	40	84	9	53	**1787**	51	10	110	40
User 3	14	165	**1568**	51	163	0	18	36	**1576**	26	181	20
User 4	26	81	75	**1644**	22	68	69	3	37	**1627**	1	33
User 5	50	48	134	9	**1346**	0	4	39	119	0	**1344**	29
User 6	152	0	8	53	16	**1781**	185	4	4	69	5	**1862**
KNN classifier												
User 1	**1514**	11	15	59	19	113	**1428**	13	18	17	0	79
User 2	1	**1679**	131	24	132	23	52	**1779**	109	29	238	88
User 3	10	113	**1616**	12	111	7	0	12	**1638**	37	184	36
User 4	41	56	11	**1575**	5	83	97	16	27	**1680**	8	87
User 5	15	46	89	3	**1332**	0	4	37	53	21	**1282**	3
User 6	238	13	10	68	7	**1888**	183	4	6	43	0	**1749**
NB classifier												
User 1	**1008**	49	108	178	24	205	**593**	83	4	12	62	102
User 2	1	**1370**	112	35	169	2	79	**1264**	28	12	244	68
User 3	40	230	**1069**	32	218	35	131	94	**974**	191	96	44
User 4	221	211	157	**1079**	29	127	364	50	561	**1104**	601	106
User 5	190	83	350	28	**1472**	119	74	177	193	41	**611**	23
User 6	338	10	58	438	52	**1566**	487	202	132	485	82	**1693**

PPVs are the scores of the positive statistical results based on true positive and true negative values. PPV shows the performance of a statistical measure and in the proposed model it has been used to confirm the probability of positive and negative results. A higher value of PPV indicates that fewer positive results are false. False Omission Rate and False Discovery Rate is a statistical method used in multiple hypothesis testing to correct for multiple comparisons. It measures the proportion of false negatives which are incorrectly rejected. FOR is computed by using false negative and true positive and it can also be computed by taking the complement of NPVs. FDR measures the proportion of actual positives that are incorrectly identified. FDR is also one way to abstracting the rate of type I errors in null

Table 3: Confusion matrix according to the users using 400 samples per window and magnetometer sensor.

Users	User 1	User 2	User 3	User 4	User 5	User 6
DT classifier						
User 1	**1230**	48	17	151	21	184
User 2	39	**1499**	63	49	89	43
User 3	29	136	**1551**	110	282	9
User 4	160	101	125	**1476**	84	79
User 5	51	63	188	17	**1138**	1
User 6	263	22	3	37	3	**1696**
SVM classifier						
User 1	**1005**	73	19	168	52	302
User 2	137	**1244**	292	69	72	110
User 3	56	284	**1124**	167	511	15
User 4	147	220	184	**1166**	107	94
User 5	48	68	238	24	**914**	29
User 6	343	28	23	178	26	**1521**
KNN classifier						
User 1	**1300**	41	21	233	45	318
User 2	78	**1423**	168	93	132	47
User 3	34	182	**1311**	134	353	48
User 4	198	103	167	**1248**	87	178
User 5	45	79	226	45	**998**	4
User 6	168	24	29	64	2	**1425**
NB classifier						
User 1	**763**	99	49	201	72	354
User 2	149	**1047**	224	103	75	200
User 3	135	339	**1003**	190	511	65
User 4	343	258	269	**1050**	298	368
User 5	109	44	186	54	**594**	0
User 6	879	108	139	175	121	**1078**

hypothesis testing when conducting multiple comparisons between classes. FDR is computed by using FP and TP.

The second experimental study is based on varying the window size for the legitimate user identification process. The window size is an important system parameter which determines the time that the system needs to perform an identification, that is, window size directly determines the system's identification frequency. In this experiment, the system varies the window size from 25 samples per window to 400 samples per window with 25 sample blocks within each window. Given a fix window size for each targeted user, the model is learned using 10-fold-cross-validation for training, validation, and testing. Here, we utilize the average accuracy across all activities stated before. In these experiments, we investigate the influence of the window size on average accuracy in choosing a proper window size. Within each window, another important system parameter is the total number of samples from the 3-dimensional signal which affects the average and overall accuracy because a larger training set provides the system more information but allows more chances for the system to be overwhelmed and degrades the classifier's generalization performance. According to the observations; the largest number of samples per window produces the maximum accuracy in almost all cases and for each activity, particularly, when the number of samples per window exceeds 200 samples or more. The accuracy decreases when the training set size is lower than 200 because a larger training set is likely to cause over-fitting so that the constructed training model would introduce more errors than expected. The detailed results over a different number of samples per windows with a 99% confidence interval are shown in Figures 1–3.

5. Discussion

The outcomes of the activity recognition and identification experiments described above provide the overall results for the proposed identification model. Recall that the results presented in Tables 1–3 have been aggregated over all identification models, that is, one per subject and all identification decisions presented here are based on multiple instances, that is, 25–400 samples per window of data. The results in Figures 1–3 indicate that SW-based identification can be relatively accurate when using only 400 samples per window of data from different activities performed by each user. Form the identification results, one can confirm that the accelerometer sensor data performs slightly better than the gyroscope sensor data and together the accelerometer and gyroscope sensors produce much higher identification results than the magnetometer sensor. In terms of classifiers, DT outperforms the KNN, SVM, and NB classifiers. In this sequence, KNN outperforms the SVM and NB but performs less well than Dts. SVM slightly underperforms against KNN but performs much better than NB classifier.

Activity recognition-based user identification models perform much better for almost all activities except for running. The overall accuracy for the proposed activity recognition-based identification is almost 98% for walking

Table 4: Statistical results for four different classifiers using accelerometer and gyroscope sensors data.

Metric	Method	Accelerometer sensor						Gyroscope sensor					
		User 1	User 2	User 3	User 4	User 5	User 6	User 1	User 2	User 3	User 4	User 5	User 6
TPR	DT	0.9495	0.9483	0.9005	0.9448	0.9455	0.9083	0.9540	0.9188	0.9041	0.9465	0.9401	0.9150
	SVM	0.8393	0.8727	0.7996	0.8580	0.8481	0.8861	0.8805	0.8713	0.8487	0.9192	0.8756	0.8746
	KNN	0.8746	0.8437	0.8646	0.8893	0.8969	0.8489	0.9183	0.7752	0.8589	0.8773	0.9157	0.8811
	NB	0.6412	0.8111	0.6583	0.5917	0.6566	0.6361	0.6927	0.7457	0.6366	0.3963	0.5460	0.5495
TNR	DT	0.9837	0.9897	0.9882	0.9859	0.9811	0.9897	0.9786	0.9942	0.9848	0.9919	0.9770	0.9872
	SVM	0.9730	0.9664	0.9632	0.9749	0.9669	0.9766	0.9648	0.9873	0.9761	0.9819	0.9687	0.9751
	KNN	0.9673	0.9736	0.9722	0.9821	0.9714	0.9745	0.9646	0.9906	0.9767	0.9839	0.9555	0.9677
	NB	0.9197	0.9400	0.9198	0.9258	0.9464	0.9455	0.8888	0.9354	0.9037	0.9105	0.8909	0.9570
FPR	DT	0.0505	0.0517	0.0995	0.0552	0.0546	0.0918	0.0459	0.0812	0.0959	0.0535	0.0599	0.0849
	SVM	0.1607	0.1273	0.2004	0.1419	0.1519	0.1139	0.1195	0.1287	0.1513	0.0808	0.1244	0.1254
	KNN	0.1254	0.1563	0.1354	0.1107	0.1030	0.1511	0.0817	0.2248	0.1411	0.1227	0.0843	0.1189
	NB	0.3588	0.1889	0.3417	0.4084	0.3434	0.3639	0.3072	0.2543	0.3634	0.6037	0.4539	0.4505
FNR	DT	0.0164	0.0104	0.0119	0.0141	0.0189	0.0103	0.0214	0.0057	0.0152	0.0081	0.0229	0.0128
	SVM	0.0269	0.0336	0.0368	0.0250	0.0330	0.0234	0.0352	0.0127	0.0239	0.0181	0.0313	0.0248
	KNN	0.0326	0.0263	0.0278	0.0178	0.0286	0.0255	0.0354	0.0094	0.0234	0.0161	0.0445	0.0323
	NB	0.0803	0.0599	0.0802	0.0741	0.0536	0.0545	0.1112	0.0647	0.0963	0.0895	0.1091	0.0429
PPV	DT	0.9495	0.9483	0.9005	0.9448	0.9455	0.9082	0.9541	0.9188	0.9041	0.9465	0.9401	0.9150
	SVM	0.8393	0.8727	0.7996	0.8580	0.8481	0.8861	0.8805	0.8713	0.8487	0.9192	0.8756	0.8746
	KNN	0.8746	0.8437	0.8646	0.8893	0.8969	0.8489	0.9183	0.7752	0.8589	0.8773	0.9157	0.8811
	NB	0.6412	0.8111	0.6582	0.5916	0.6566	0.6361	0.6928	0.7457	0.6366	0.3963	0.5460	0.5495
NPV	DT	0.9837	0.9896	0.9881	0.9859	0.9811	0.9897	0.9786	0.9942	0.9848	0.9919	0.9770	0.9872
	SVM	0.9730	0.9664	0.9632	0.9749	0.9669	0.9765	0.9648	0.9873	0.9761	0.9819	0.9687	0.9751
	KNN	0.9673	0.9737	0.9722	0.9821	0.9714	0.9745	0.9646	0.9906	0.9767	0.9839	0.9555	0.9677
	NB	0.91975	0.9400	0.9198	0.9259	0.94643	0.9455	0.8888	0.9353	0.9037	0.9105	0.8909	0.9570
SEN	DT	0.9189	0.9498	0.9426	0.9283	0.8900	0.9529	0.8605	0.9742	0.9297	0.9588	0.8749	0.9447
	SVM	0.8544	0.8374	0.8239	0.8777	0.8113	0.8936	0.8212	0.9400	0.8775	0.9064	0.8185	0.8935
	KNN	0.8323	0.8754	0.8632	0.9047	0.8293	0.8931	0.8095	0.9559	0.8849	0.9195	0.7488	0.8565
	NB	0.5606	0.7015	0.5766	0.6028	0.7495	0.7624	0.3432	0.6759	0.5148	0.5984	0.3603	0.8315
SPE	DT	0.9901	0.9893	0.9787	0.9893	0.9911	0.9791	0.9936	0.9811	0.9788	0.9893	0.9896	0.9799
	SVM	0.9698	0.9745	0.9571	0.9704	0.9744	0.9747	0.9778	0.9712	0.9697	0.9846	0.9797	0.9702
	KNN	0.9765	0.9660	0.9725	0.9789	0.9838	0.9625	0.9863	0.9439	0.9708	0.9745	0.9874	0.9738
	NB	0.9413	0.9662	0.9419	0.9226	0.9185	0.9043	0.9718	0.9531	0.9394	0.8176	0.9458	0.8463
FDR	DT	0.0505	0.0517	0.0995	0.0552	0.0545	0.0918	0.0459	0.0812	0.0959	0.05349	0.0599	0.0849
	SVM	0.1607	0.1273	0.2004	0.1419	0.1519	0.1139	0.1195	0.1287	0.1513	0.0808	0.1244	0.1254
	KNN	0.1254	0.1563	0.1354	0.1107	0.1030	0.1511	0.0817	0.2248	0.1411	0.1227	0.0843	0.1189
	NB	0.3588	0.1889	0.3417	0.4084	0.3434	0.3639	0.3072	0.2543	0.3634	0.6037	0.4539	0.4505
FOR	DT	0.0163	0.0104	0.0119	0.0142	0.0189	0.0103	0.0214	0.0057	0.0152	0.0081	0.0229	0.0128
	SVM	0.0269	0.0336	0.0368	0.0250	0.0330	0.0234	0.0352	0.0127	0.0239	0.0181	0.0313	0.02486
	KNN	0.0327	0.0263	0.0278	0.0179	0.0286	0.0255	0.0354	0.0094	0.0233	0.0161	0.0445	0.0323
	NB	0.0803	0.0599	0.0802	0.0741	0.0536	0.0545	0.1112	0.0647	0.0963	0.0895	0.1091	0.0429
ACC	DT	0.9781	0.9826	0.9725	0.9792	0.9762	0.9744	0.9756	0.9798	0.97007	0.9843	0.9716	0.9733
	SVM	0.9518	0.9509	0.9342	0.9547	0.9499	0.9601	0.9517	0.9658	0.9547	0.9719	0.9558	0.9558
	KNN	0.9528	0.9503	0.9540	0.9672	0.9614	0.9492	0.9581	0.9459	0.9564	0.9655	0.9504	0.9522
	NB	0.8814	0.9209	0.8826	0.8724	0.8894	0.8787	0.8737	0.9063	0.8668	0.7811	0.8561	0.8436

activity and 93% accuracy for jogging and 82% to 86% for the rest of the activities-based user identification model. The results of the proposed two-fold activity recognition and legitimate user identification model are presented in Figures 1–3 and Tables 1–5 which show the ability to efficiently recognize the individual activity and identification based on the recognized activity of the individual user.

As we earlier explained, there is no research in the literature as similar to the work presented in this paper. However, we found two closely related works, and their comparison results are presented in Table 6. These methods have exactly been tested as the settings mentioned in their respective works. Based on the results, one can conclude that the activity recognition-based legitimate user identification framework performed better because we used a single predictive model and ambiguity activity recognition analysis that significantly help the model to perform better in the identification process.

We also measured the time for doing activity recognition and user identification in the proposed system which is less than 5 seconds in extreme case of 400 samples per window as shown in Figure 4. One can also observe that as we decrease

Table 5: Statistical results for four different classifiers using magnetometer sensor data.

Metric	Method	User 1	User 2	User 3	User 4	User 5	User 6
TPR	DT	0.7450	0.8412	0.7326	0.7289	0.7805	0.8379
	SVM	0.6206	0.6465	0.5211	0.6079	0.6919	0.7178
	KNN	0.6639	0.7331	0.6358	0.6299	0.7144	0.8324
	NB	0.4961	0.582	0.4472	0.4060	0.6018	0.4312
TNR	DT	0.9424	0.9601	0.9557	0.9597	0.9501	0.9650
	SVM	0.9226	0.9263	0.9151	0.9337	0.9211	0.9385
	KNN	0.9425	0.9529	0.9320	0.9373	0.9359	0.9363
	NB	0.8403	0.9139	0.9079	0.9203	0.8990	0.8922
FPR	DT	0.2549	0.1588	0.2674	0.2711	0.2195	0.1621
	SVM	0.3793	0.3534	0.4789	0.3921	0.3081	0.2822
	KNN	0.3361	0.2669	0.3642	0.3700	0.2856	0.1676
	NB	0.5039	0.4177	0.5528	0.5939	0.3982	0.5688
FNR	DT	0.0576	0.0399	0.0443	0.0403	0.0499	0.0349
	SVM	0.0774	0.0737	0.0849	0.0663	0.0789	0.0615
	KNN	0.0575	0.0471	0.0679	0.0627	0.064	0.0637
	NB	0.1597	0.0861	0.0921	0.0797	0.1009	0.1078
PPV	DT	0.7450	0.8411	0.7326	0.7289	0.7805	0.8379
	SVM	0.6208	0.6466	0.5211	0.6079	0.6919	0.7178
	KNN	0.6639	0.7331	0.6358	0.6299	0.7144	0.8324
	NB	0.4961	0.5823	0.4472	0.4060	0.6018	0.4312
NPV	DT	0.9424	0.9601	0.9557	0.9597	0.9501	0.9650
	SVM	0.9226	0.9263	0.9151	0.9337	0.9211	0.93847
	KNN	0.9425	0.9529	0.9320	0.9373	0.9359	0.9363
	NB	0.8403	0.9139	0.9078	0.9203	0.8990	0.8922
SEN	DT	0.6941	0.8020	0.7966	0.8022	0.7038	0.8429
	SVM	0.5789	0.6489	0.5979	0.6580	0.5434	0.7344
	KNN	0.7131	0.7684	0.6821	0.6868	0.6172	0.70545
	NB	0.3209	0.5525	0.5364	0.5922	0.3555	0.5220
SPE	DT	0.9547	0.9692	0.9379	0.9404	0.9661	0.9637
	SVM	0.9341	0.9256	0.8874	0.9190	0.9566	0.9335
	KNN	0.9287	0.9437	0.9177	0.9206	0.9577	0.9682
	NB	0.9164	0.9230	0.8732	0.8445	0.9606	0.8517
FDR	DT	0.2549	0.1588	0.2674	0.2711	0.2195	0.1621
	SVM	0.3792	0.3534	0.4789	0.3921	0.3081	0.2822
	KNN	0.3361	0.2669	0.3642	0.3700	0.2856	0.1676
	NB	0.5039	0.4177	0.5528	0.5939	0.3982	0.5688
FOR	DT	0.0576	0.0399	0.0443	0.0403	0.0499	0.0349
	SVM	0.0774	0.0737	0.0849	0.0663	0.0789	0.0615
	KNN	0.0575	0.04709	0.0679	0.0627	0.064	0.0637
	NB	0.1597	0.0861	0.0921	0.0797	0.1009	0.1078
ACC	DT	0.9129	0.9409	0.9129	0.9174	0.9277	0.9418
	SVM	0.8784	0.8777	0.8382	0.8772	0.8937	0.8962
	KNN	0.8931	0.9143	0.8768	0.8822	0.9079	0.9202
	NB	0.7949	0.8628	0.8192	0.8061	0.8738	0.7933

the size of the window (i.e., we increase the number of samples for training model), the time for doing an implicit activity recognition and user identification increases slowly at first and then sharply increases when the size of the window decreases from 150 samples per window. One can also observe from identification results that the higher the window size, the better the identification results. Therefore, the proposed system can achieve acceptable performance in terms of accuracy and computational time which makes the proposed system efficient and applicable in real-world scenarios.

We have also analyzed the model's ability to defend against impostures such as masquerading attacks. Recall that the goal of the proposed model was to prevent an imposture from getting access to the secure and sensitive information or services against the stored passwords. The obtained results also show that the proposed model is secure against the masquerading attacks. The term "secure" means that the imposture cannot cheat the system by performing these attacks in a short time. Therefore, the proposed system performed well in recognizing the adversary who is launching the masquerading attack. Thus, within several windows, the probability for imposture escaping detection is 0.038% only. Therefore, the proposed system shows good performance in defending against masquerading attacks too.

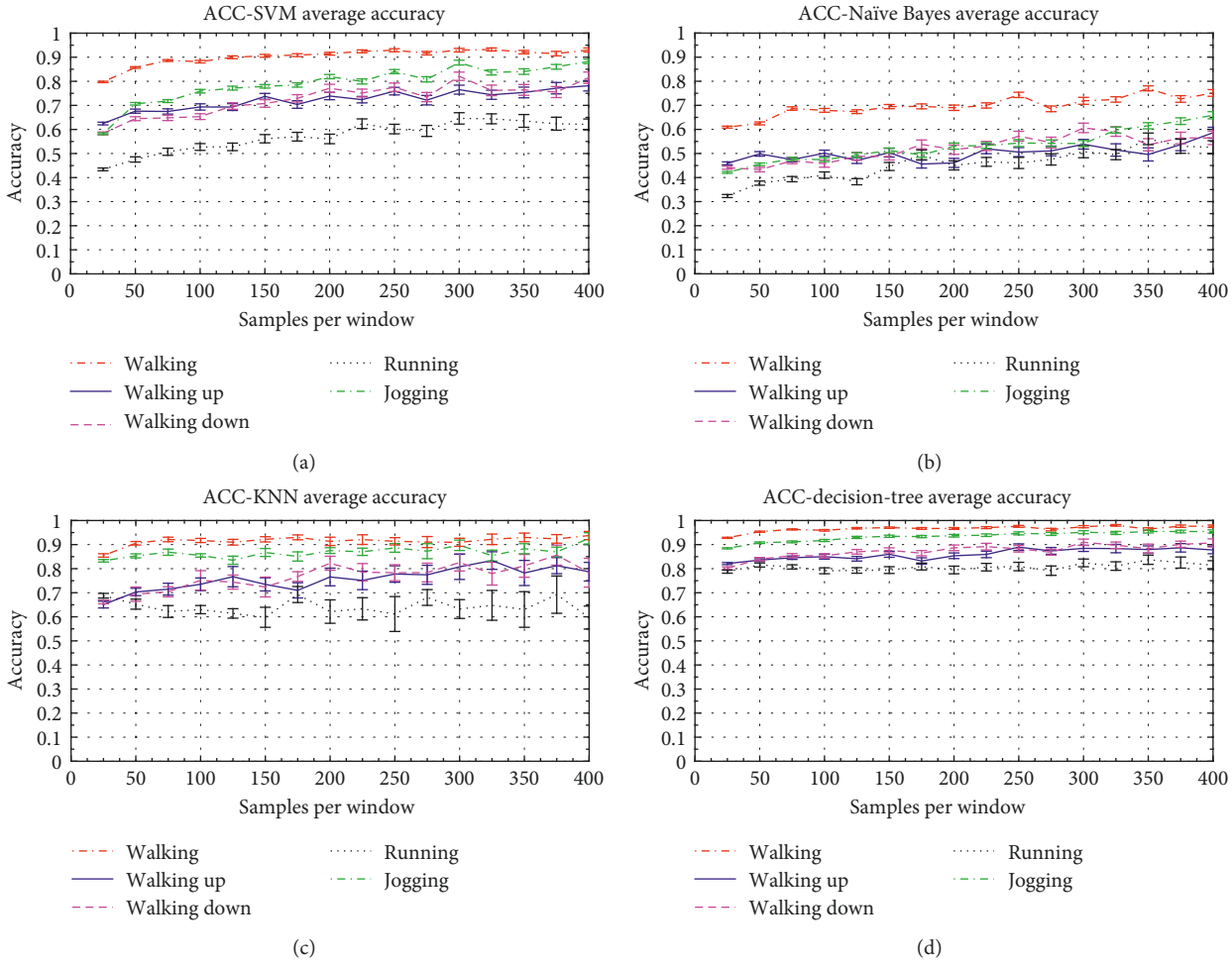

Figure 1: Accelerometer sensor-based accuracy for SVM, NB, KNN, and DT classifiers (a–d).

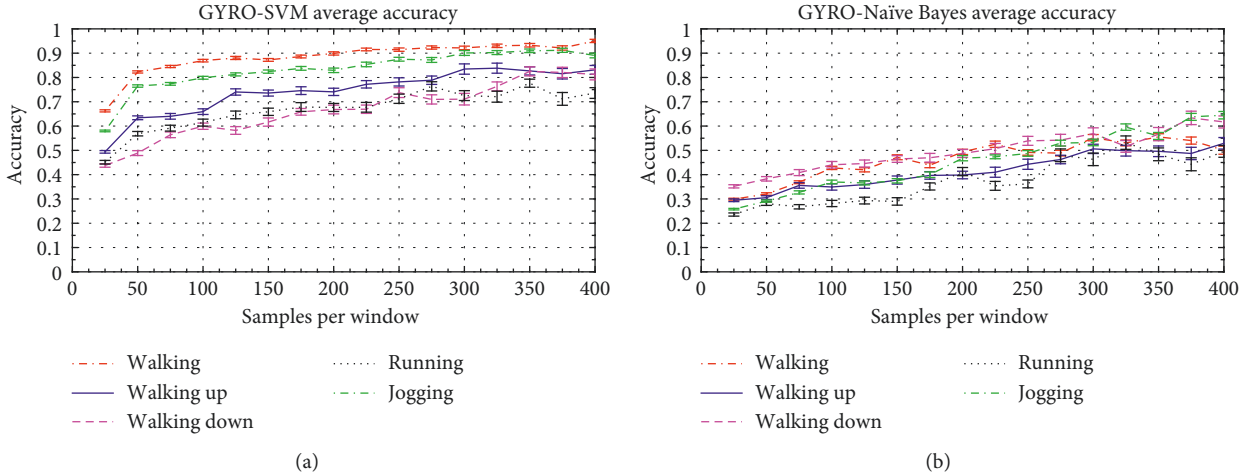

Figure 2: Continued.

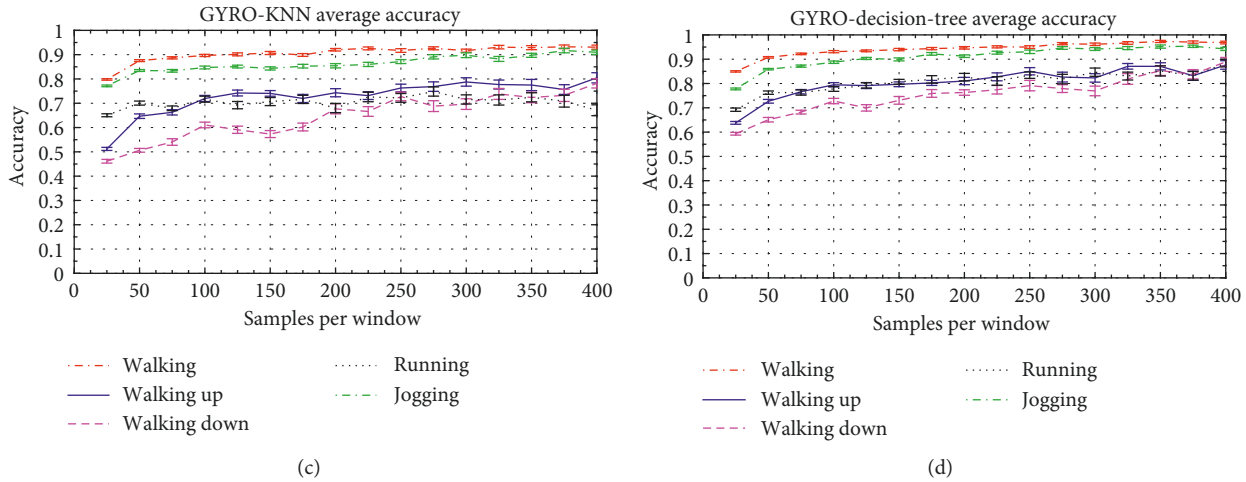

Figure 2: Gyroscope sensor-based accuracy for SVM, NB, KNN, and DT classifiers (a–d).

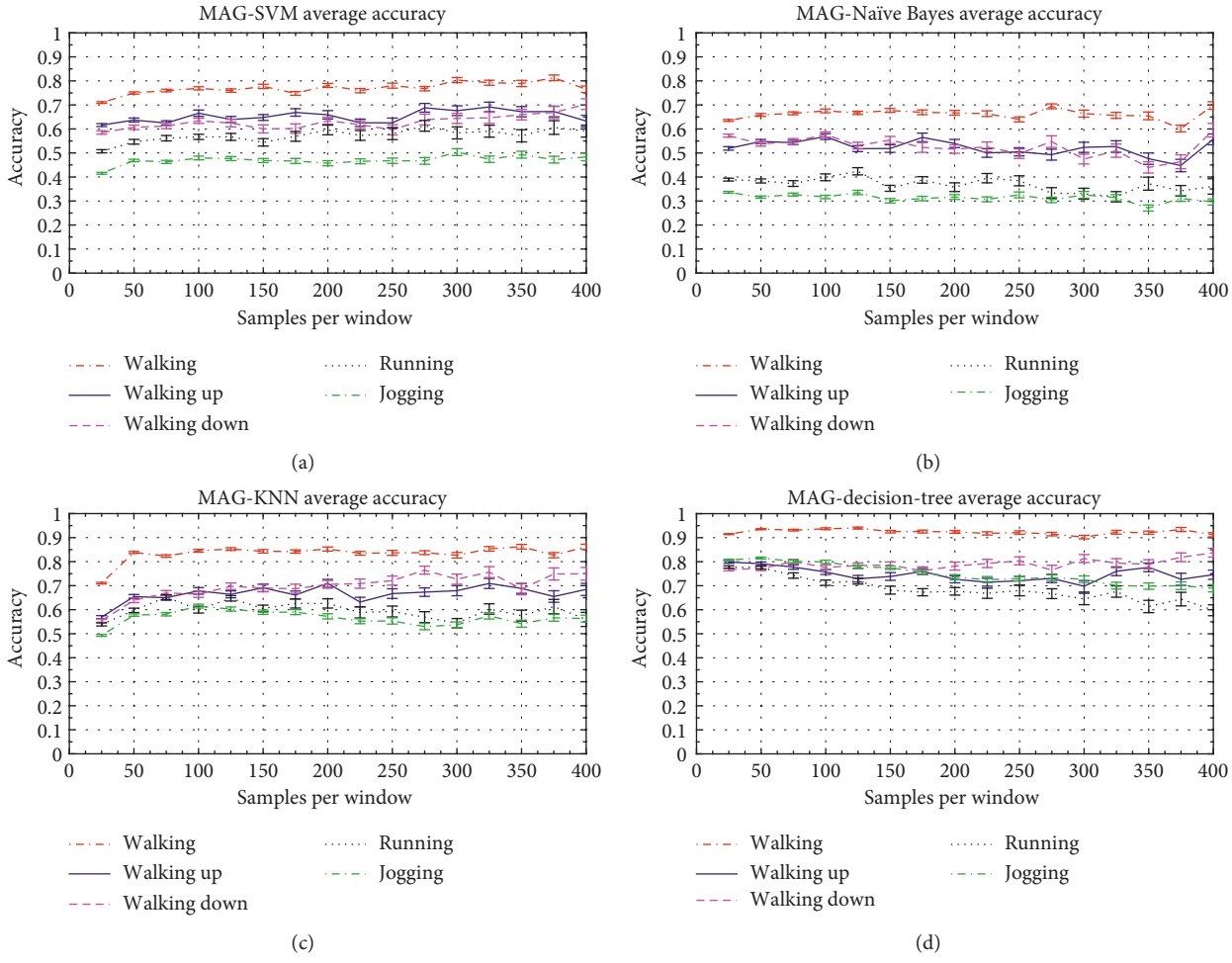

Figure 3: Magnetometer sensor-based accuracy for SVM, NB, KNN, and DT classifiers (a–d).

6. Future Work

The goal of this research was to show that activity recognition-based legitimate user identification is an effective approach in gait-based identification domain. As we have shown, it is possible to distinguish between both individuals performing the same activity. An immediate question we have for future work is to determine how identification time can be improved

Table 6: Comparison with state-of-the-art work.

Reference	Sensor		
	Accelerometer	Gyroscope	Magnetometer
[1]	97.2%	93.8%	—
[9]	92.1% combined		—
Proposed work	98.7%	96.4%	91.9%

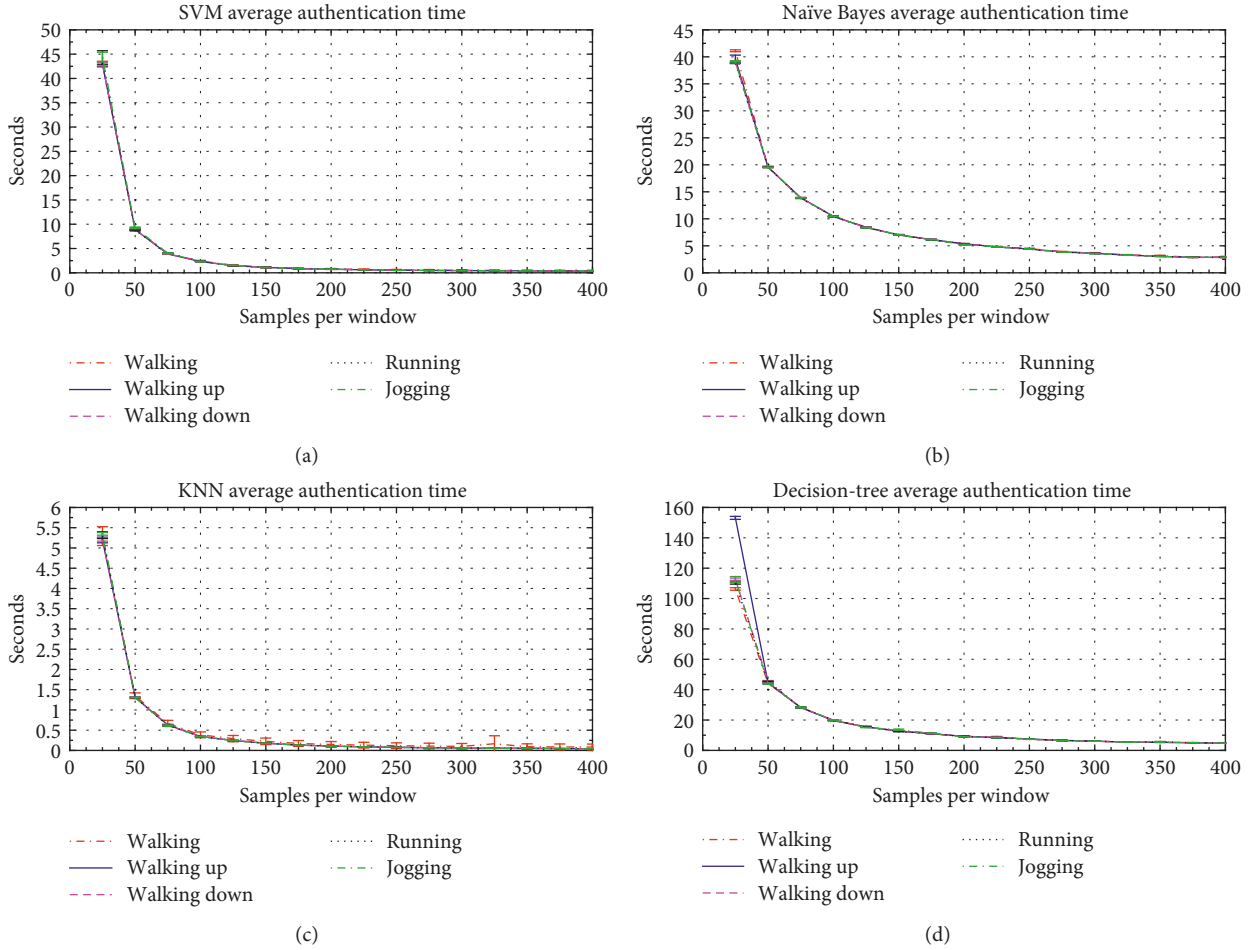

Figure 4: Identification time for SVM, NB, KNN, and DT classifiers (a–d).

within different activities as a first step. For this, the immediate solution is to use any lightweight feature selection method which somehow will help to improve the discriminative power and reduce the dimensions at the same time. To the best of our knowledge, this idea is relatively new in SW-based activity recognition and identification. The preliminary results indicate that this is indeed a promising area of research.

Additionally, as discussed above, a key limitation to activity recognition-based user identification is the variability of the signal. Our future work will focus on studying the potential of a further windowing process and feature selection. We will then use simple DT, KNN, and SVM classifiers. However, from the current results, one can observe that the DT classifier outperformed all other classifiers. When using the DT classifier, the results are promising for both activity recognition and user identification. However, this study was conducted on a relatively small set of users. The experimental dataset includes 5 activities performed by 6 six users per activity but the advantage is this dataset does not distribute classes uniformly. This has led to a set of results in line with other state-of-the-art works.

In addition to the above, future work would entail bulking out the experimental dataset with more users (*more than 15*), activities (*more than 10*), and training runs. Finally, our experimental dataset was collected using Android SWs running in Android Wear OS. It would be useful to use different SWs running different operating systems. We believe it is useful to measure PAR-based user identification on a wide verity of SWs. One final goal of this study was to incorporate this technology into a real-time system.

7. Conclusion

Smartwatches are becoming increasingly popular. This popularity has forced the community to study the security implications of these small and powerful devices. It has been suggested that activity recognition and gait-based identification combined with SWs are possible. This study described an effective two-fold system for performing SW-based activity recognition and user identification. This study demonstrates that gait as measured by the commercial grade SW sensor is sufficient to identify an individual with modest accuracy. Furthermore, a simple sliding window approach is shown to be sufficient for representing the time series sensor data. Experimental results demonstrate the advantage of combining the time and frequency domain information. The proposed system can achieve user identification average accuracy up to 98.68% with negligible system overhead, minimum time, and power consumption. We hope that the proposed system can act as a key technique for implicit activity recognition-based legitimate user identification in real-world scenarios.

Data Availability

The experimental datasets will be provided upon reasonable requests to mahmad00@gmail.com.

Conflicts of Interest

The authors have no conflicts of interest to declare.

Authors' Contributions

The authors Mohammed A. Alqarni, Asad Khan, Adil Khan, Sajjad Hussain Chauhdary, Manuel Mazzara, Tariq Umer, and Salvatore Distefano contributed equally to this work.

References

[1] A. M. Khattak, N. Akbar, M. Aazam et al., "Context representation and fusion: advancements and opportunities," *Sensors*, vol. 14, no. 6, pp. 9628–9668, 2014.

[2] A. H. Johnston and G. M. Weiss, "Smartwatch-based biometric gait recognition," in *Proceedings of 7th IEEE International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–6, Washington, DC, USA, September 2015.

[3] J. Siegal, "Smartwatch sales set to explode, expected to top 100m within four years," September 2013, http://bgr.com/2013/09/27/smartwatch-sales-forecast-2020/.

[4] J. A. Hughes, J. A. Brown, and A. M. Khan, "Smartphone gait fingerprinting models via genetic programming," in *Proceedings of IEEE International Joint Conference on Neural Networks (IEEE IJCNN) in conjunction with IEEE World Congress on Computational Intelligence (IEEE WCCI)*, pp. 408–415, Vancouver, BC, Canada, July 2016.

[5] M. Ahmad, A. M. Khan, J. A. Brown, S. Protasov, and A. M. Khattak, "Gait fingerprinting-based user identification on smartphones," in *Proceedings of IEEE International Joint Conference on Neural Networks (IEEE IJCNN) in conjunction with IEEE World Congress on Computational Intelligence (IEEE WCCI)*, pp. 3060–3067, Vancouver, BC, Canada, July 2016.

[6] M. Ahmad and A. M. Khan, *Seeking Optimum System Settings for Physical Activity Recognition on Smartwatches* CoRR abs/1706.01720, Cornell University Library, Ithaca, NY, USA, 2017.

[7] M. Ahmad and A. M. Khan, *Extended Sammon Projection and Wavelet Kernel Extreme Learning Machine for Gait Based Legitimate User Identification on Smartphones (GUI)*, CoRR abs/1706.01720, Cornell University Library, Ithaca, NY, USA, 2017.

[8] April 2017 https://www.androidheadlines.com/2017/01/sk-telecom-outs-smartwatch-based-identification-system.html.

[9] M. Qi, "User-specific iris authentication based on feature selection," in *Proceedings of IEEE International Conference on Computer Science and Software Engineering*, pp. 1040–1043, Washington, DC, USA, 2008.

[10] L. Hong and A. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 12, pp. 1295–1307, 1998.

[11] W.-H. Lee and R. Lee, "Implicit sensor-based authentication of smartphone users with smartwatch," in *Proceedings of the Hardware and Architectural Support for Security and Privacy*, pp. 1–9, Seoul, Republic of Korea, June 2016.

[12] C. Nickel, T. Wirtl, and C. Busch, "Authentication of smartphone users based on the way they walk using k-NN algorithm," in *Proceedings of IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pp. 16–20, Piraeus-Athens, Greece, July 2012.

[13] M. Shahzad, A. X. Liu, and A. Samuel, "Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it," in *Proceedings of 19th Annual International Conference on Mobile Computing and Networking (MobiCom)*, pp. 39–50, Miami, FL, USA, January 2013.

[14] M. Trojahn and F. Ortmeier, "Toward mobile authentication with keystroke dynamics on mobile phones and tablets," in *Proceedings of IEEE Advanced Information Networking and Applications Workshops*, pp. 697–702, Barcelona, Spain, March 2013.

[15] S. Buthpitiya, Y. Zhang, A. K. Dey, and M. Griss, "n-gram geotrace Modeling," in *Proceedings of 9th International Conference on Pervasive Computing*, pp. 97–114, San Francisco, CA, USA, June 2011.

[16] H. G. Kayacik, M. Just, L. Baillie, D. Aspinall, and N. Micallef, "Data-driven authentication: on the effectiveness of user behavior modeling with mobile device sensors," in *Proceedings of the 3rd Workshop on Mobile Security Technologies (MoST)*, San Jose, CA, USA, May 2014.

[17] J. Zhu, P. Wu, X. Wang, and J. Zhang, "SenSec: mobile security through passive sensing," in *Proceedings of IEEE International Conference on Computing, Networking and Communications (IEEE ICNC)*, pp. 1128–1133, San Diego, CA, USA, January 2013.

[18] W.-H. Lee and R. B. Lee, "Multi-sensor authentication to improve smartphone security," in *Proceedings of Conference on Information Systems Security and Privacy (IEEE ICISSP)*, pp. 1–11, Angers, France, February 2015.

[19] W.-H. Lee and R. B. Lee, "Implicit authentication for smartphone security," in *Proceedings of International Conference on Information Systems Security and Privacy*, vol. 576, pp. 160–176, Angers, France, February 2015.

[20] L. Li, X. Zhao, and G. Xue, "Unobservable re-authentication for smartphones," in *Proceedings of IEEE NDSS Symposium (NDSS)*, San Diego, CA, USA, February 2013.

[21] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos, "Progressive authentication: deciding when to authenticate on mobile phones," in *Proceedings of 21st USENIX Security Symposium (USENIX 12)*, pp. 301–316, Bellevue, WA, USA, August 2012.

[22] S. Mare, A. M. Markham, C. Cornelius, R. Peterson, and D. Kotz, "Zebra: zero-effort bilateral recurring authentication," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 705–720, San Jose, CA, USA, May 2014.

[23] C. Nickel, H. Brandt, and C. Busch, "Classification of acceleration data for biometric gait recognition on mobile devices," *BIOSIG*, vol. 11, pp. 57–66, 2011.

[24] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user authentication on mobile phones using biometric gait recognition," in *Proceedings of 6th IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pp. 306–311, Darmstadt, Germany, October 2010.

[25] H. M. Thang, V. Q. Viet, T. D. Nguyen, and D. Choi, "Gait identification using accelerometer on a mobile phone," in *Proceedings of IEEE International Conference on Control, Automation and Information Sciences (ICCAIS)*, pp. 344–348, Ho Chi Minh City, Vietnam, November 2012.

[26] S. Davidson, D. Smith, C. Yang, and S. Cheah, "Smartwatch user identification as a means of authentication," 2016, https://cseweb.ucsd.edu/classes/wi16/cse227-a/report4.pdf.

[27] X. Su, H. Tong, and P. Ji, "Activity recognition with smartphone sensors," *Tsinghua Science and Technology*, vol. 19, no. 3, pp. 235–249, 2014.

[28] A. M. Khan, Y.-K. Lee, S. Y. Lee, and T.-S. Kim, "A triaxial accelerometer-based physical activity recognition via augmented-signal features and a hierarchical recognizer," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 5, pp. 1166–1172, 2010.

[29] A. Parnandi, "Coarse in-building localization with smartphones," in *Proceedings of International Conference on Mobile Computing, Applications, and Services (MobiCASE)*, pp. 343–354, San Diego, CA, USA, October 2009.

[30] I. Rish, "An empirical study of the naive Bayes classifier," in *Proceedings of Workshop on Empirical Methods in Artificial Intelligence (IJCAI-01)*, vol. 335, Seattle, WA, USA, August 2001.