Human-centric Computing and Information Sciences

RESEARCH Open Access

Identifying smartphone users based on how they interact with their phones

Mohammed A. Alqarni[1], Sajjad Hussain Chauhdary[2], Maryam Naseer Malik[3], Muhammad Ehatisham-ul-Haq[3*] and Muhammad Awais Azam[3]

*Correspondence: ehatishamuet@gmail.com
[3] Faculty of Telecom and Information Engineering, University of Engineering and Technology (UET), Taxila, Punjab 47050, Pakistan
Full list of author information is available at the end of the article

Abstract

The continuous advancement in the Internet of Things technology allows people to connect anywhere at any time, thus showing great potential in technology like smart devices (including smartphones and wearable devices). However, there is a possible risk of unauthorized access to these devices and technologies. Unfortunately, frequently used authentication schemes for protecting smart devices (such as passwords, PINs, and pattern locks) are vulnerable to many attacks. USB tokens and hardware keys have a risk of being lost. Biometric verification schemes are insecure as well as they are susceptible to spoofing attacks. Maturity in sensor chips and machine learning algorithms provides a better solution for authentication problems based on behavioral biometrics, which aims to identify the behavioral traits that a user possesses, such as hand movements and waving patterns. Therefore, this research study aims to provide a solution for passive and continuous authentication of smartphone users by analyzing their activity patterns when interacting with their phones. The motivation is to learn the physical interactions of a smartphone owner for distinguishing him/her from other users to avoid any unauthorized access to the device. Extensive experiments were conducted to test the performance of the proposed scheme using random forests, support vector machine, and Bayes net. The best average recognition accuracy of 74.97% is achieved with the random forests classifier, which shows the significance of recognizing smartphone users based on their interaction with the phones.

Keywords: Activity recognition, Behavioral biometric, Gesture recognition, Mobile sensing, Machine learning, User identification

Introduction

In recent years, with the continuous evolvement in Artificial Intelligence (AI) and Information and Communication Technologies (ICTs), including Internet-of-Things (IoT) and cloud computing (CC), computers are anticipated to replace human beings in almost all fields of life. Smartphones and other handheld devices have evolved from simple communication devices to personal computers. They have gained popularity due to their convenient use in everyday life for accessing various online services, social networks, and e-banking, etc. People use smartphones for not only personal use but also take advantage of these devices in their business-related tasks. Consequently, increasing amounts of private and sensitive information are being generated and stored in our smartphones. According to a study, 92.8% of people use a smartphone to store their private information [1, 2]. These smart devices are potentially occupying the center stage in smart environments. People can easily control their lighting systems, TVs, refrigerators, and doors through their smartphones for easy accessibility. Smartphones have also been used to control health-related instruments, such as audiovisual aids, thus becoming the focus of the imminent technological paradigm swing. However, incorporating smartphone-based tracking and control in different systems is leading to severe security and privacy issues as well. Users are now more hesitant in sharing their smartphones with others as smartphones have become an attractive target for the attackers to gain illegal access and control to other smart devices and private information [3, 4]. Hence, an implicit authentication mechanism is essential for preserving user's access and control that has been made accessible through smart devices.

Currently, passwords and Personal Identification Numbers (PINs) are the most widely used user identification and access control strategies in smartphone operating systems. These methods use explicit authentication yet not provide continuous authentication. There are other explicit authentication mechanisms such as fingerprints [5], face recognition [6, 7], Iris scanning [8], etc. However, these explicit mechanisms are not convenient for smartphone users as they require users to participate with the device. Also, re-authentication actively requires each time users try to access sensitive private information. Similarly, after an initial login, these mechanisms do not continuously authenticate users again, thus creating a risk for adversaries to access control on users' smartphone and act as a legitimate user. Also, password and PINs are vulnerable to various attacks such as side-channel attacks [9], spoofing [10], and guessing attacks [11]. Facial recognition using a smartphone camera is another strategy to identify the actual owner of the smartphone, but it is inconvenient due to the unreliability of the technique with the changing environment. Also, the frequent image capturing consumes more power this preventing this technique for continuous authentication use. Similarly, multiple challenges are associated with camera-based gesture recognition techniques as it is difficult to collect an ample training set for personalized gestures for existing statistical models such as Hidden Marvok Model (HMM) [12]. A more suitable approach can be adopted by using smartphones inertial sensors (accelerometer, gyroscope, and magnetometer) to perform user identification, which provides the advantage that recognition can be done within the device. Thus the power and cost consumptions are lower [13]. If physical sensors are used, they require some external power source, whereas the embedded smartphone sensors use the battery as a power source. As a result, the smartphone-embedded inertial sensors have stimulated research towards user identification by detecting behavioral characteristics [14]. As an example, TapPrints detects user behavior though sensors data by examining tapping behavior on different locations on the touch screen [15]. Moreover, the users have their own behavioral patterns to interact with the device, and the motion sensors assist in characterizing the behavioral pattern to identify the user. The current work in authenticating smartphone users mainly focuses on the Activities of Daily Living (ADLs). Most of these activities consist of longer duration, which are then segmented to smaller chunks to recognize activities effectively. But there is a need for exploring strategies that consider the activities of relatively short duration to authenticate smartphone users.

In this work, we investigate the feasibility of utilizing the behavioral biometrics extracted from smartphone inertial sensors for user authentication based on machine learning. A passive and implicit authentication scheme is proposed, which analyzes the behavioral patterns of the user when they interact with the smartphone. The user identification component is based on the recognition of different activities performed by the users. A total of 12 activities are experimented, which are categorized into two groups: short-term activities and gestures. Short-term activities are those activities in which a user uses a smartphone while gestures are those activities which user performs while holding a smartphone (not actually using the smartphone). Two smartphone sensors, accelerometer and gyroscope, are used to collect data from different smartphone users while performing activities. The collected data is pre-processed, and then different time domain and frequency domain features are extracted. Three different prevalent classifiers i.e., support vector machine, Bayes net, and random forests, are employed for classification purposes to identify the actual user of the smartphone.

The key contributions of this research work are given below.

- Collection of dataset composed of different short-term activities and gestures from 26 users by utilizing smartphone's inertial sensors and avoiding any additional hardware
- Design of implicit and passive authentication scheme that continuously monitors the user's interaction patterns with the smartphone to recognize a smartphone user
- Selection of a set of computationally efficient features for user identification based on the selected activities
- Extensive experimental evaluation and analysis to test and validate the performance of the proposed scheme

The remaining part of the paper is organized as follows: "Literature review" section presents the literature review for smartphone authentication and user identification schemes. "Proposed methodology" section provides details regarding the proposed method and its main steps. "Experimental results and analysis" section provides an analysis of the obtained results and discusses the performance of the selected classifiers for user identification. Finally, "Conclusion" section concludes this research work and provides recommendations and suggestions for future works.

Literature review

Traditional smartphone authentication or user identification methods are based on passwords and PINS for protecting the smartphone user's privacy [16]. Although they are widely used authentication mechanisms but choosing the right password is not an easy task [17]. Similarly, they are weak and vulnerable to guessing attacks [18, 19]. To avoid the limitations associated with passwords, tokens and hardware keys were adopted broadly as a second-factor authentication to enhance security [20]. Different physiological biometrics approaches used different human features for user identification, such as fingerprints, iris recognition, face recognition [21]. Fingerprint hardware is embedded in modern devices and smartphones as a security mechanism. Although this technology has been used extensively, it cannot be considered definitive. Several research studies have revealed the vulnerability of fingerprint readers, including spoofing attacks [22]. Also, fingerprints can be altered by molting human fingers. Similarly, fake fingerprints can be made by using a putty or high-quality scanner. Similar to fingerprint-based methods, user authentication using face recognition schemes have also been used widely, but they can be compromised even through simple attacks using a 3D printed mask. Also, a facial recognition system is susceptible to spoofing attacks that the photo of a legitimate user can be used to gain access to a system. Face recognition is influenced by lighting conditions and shelter. Moreover, most of the existing authentication mechanisms for the smartphone are based on a one-time manner, i.e., once a user is declared as legal, he/she could be considered as the legitimate user for an extended period of time without re-verification [23].

Keystroke dynamic based authentication schemes are the oldest ones, introduced to identify a user as the owner of the device. This method is later adopted in smartphones as touch strikes. Nader et al. [24] proposed a hybrid authentication scheme based on touch gestures by combining continuous authentication (CA) and implicit authentication (IA) schemes. The results were tested using neural network classifier and practical swarm optimization (PSO)–radial basis function network (RBFN) classifier. The error rate obtained is 1.9% when only the CA scheme is used and reduces nearly to zero when combined with the IA scheme. In [25], the authors presented Touchstroke that uses participants's hand movements when holding the smartphone and text-independent 4-digit touch-type patterns for bimodal verification. The experimental results indicate that the solution is highly accurate. Similarly, the authors in [26, 27] analyzed the distinctness of touch dynamics for mobile authentication system. Trojahn et al. [28] proposed an authentication scheme that is a combination of keystroke and handwriting based mechanisms through a touchscreen sensor. They presented their results in terms of the False Acceptance Rate (FAR) and False Rejection Rate (FRR) as 11% and 16%, respectively. In [29], the authors proposed a feasibility study based on keystroke analysis, which authenticates a user by examining their typing characteristics. Fang et al. [30] proposed a state-of-the-art method based on keystrokes dynamics to achieve both FAR and FRR as low as 1.0% by using three classifiers, including decision trees (J48), Bayesian network, and random forests. Attaullah et al. [31] presented a method which is a mixture of keystroke dynamics with inertial measurement unit readings to enhance user recognition capabilities. Gesture-based authentication methods have been used as primary or secondary security measures for the device. Most of the time, the way of performing gestures is different, which reflects the user's distinct behavior. Feng et al. [32] analyzed the gesture behavior analysis of different users for user authentication and achieved FAR below 5% and FRR as 0.13%. Frenk et al. [33] identified a user via distinct analytic features from sliding traces and achieved an Equal Error Rate (EER) of 4%.

Nowadays, the analysis of behavioral patterns has widely been used in implicit and continuous authentication. These methods have improved the accuracy in identifying and verifying users based on their activity patterns. In this regard, an authentication scheme has been proposed by Conti et al. [34], which authenticates a user based on the hand movements when he tries to answer or place a call. They analyzed accelerometer and orientation sensors data and achieved and 4.4% FAR and 9.3% FRR. In [35], the authors proposed an authentication scheme that validates a user continuously and unobtrusively based on his/her interactions with the user interface of the mobile application. The proposed scheme is tested using a support vector machine-based ensemble classifier that achieved an EER of 7% and a median accuracy of 93%. In [36], the authors presented a framework that identifies user continuously from remote servers by analyzing user interactions with the smartphone. The obtained results showed FAR and FRR of 23% and 22%, respectively in the case of a single scroll gesture. In [37], the authors utilized neural networks and extreme value analysis for implementing a gait recognition-based fuzzy authentication system. Sensec [38] presented a sensor-based user authentication model by collecting data from three smartphone sensors: accelerometer, gyroscope, and magnetometer. The data was based on the gestures model developed when the users were interacting with the device. Their approach showed 75% accuracy in identifying users. Amin et al. [39] presented an implicit authentication scheme for smartphone user authentication based on built-in sensors of the device. The experimental analysis shows an accuracy of 96.5%. In [40], the authors recognize the touchscreen interactions based on web browsing for authenticating smartphone users. Nickle et al. [41] recognize the user's behavior patterns and to authenticate smartphone user. They used accelerometer data and used the k-nearest neighbor classifier to obtain FAR of 3.97% and FRR of 22.22%. Lee et al. [42] analyzed the user's daily living activities and showed that using more sensors can significantly improve the accuracy of the authentication scheme. Their results showed an accuracy of 90% when support vector machine classifier was used. A system proposed by Yang et al. [43] utilizes the accelerometer data of the hand waving pattern when used for locking and unlocking of the smartphone, which achieved FAR of 15% and FRR of 10%. The existing work mainly focuses on the activities of daily living or utilizes only single behavioral biometric for authentication. However, this study uses a fair number of short-term activities and gestures for user identification, which is performed by the participants when interacting with their smartphones.

Proposed methodology

This section explains the step-wise process of the proposed methodology, as shown in Fig. 1.

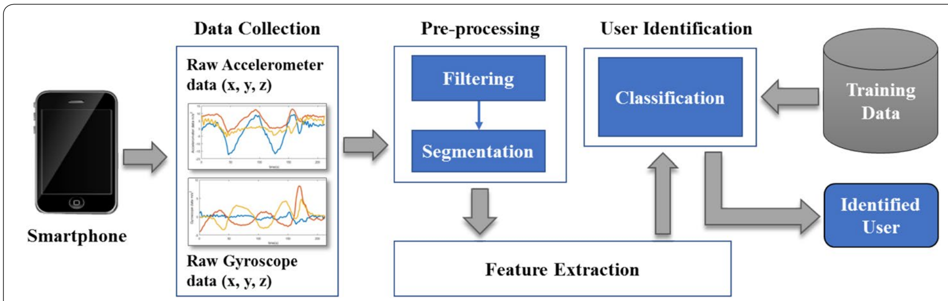

Fig. 1 Methodology of the proposed user identification scheme

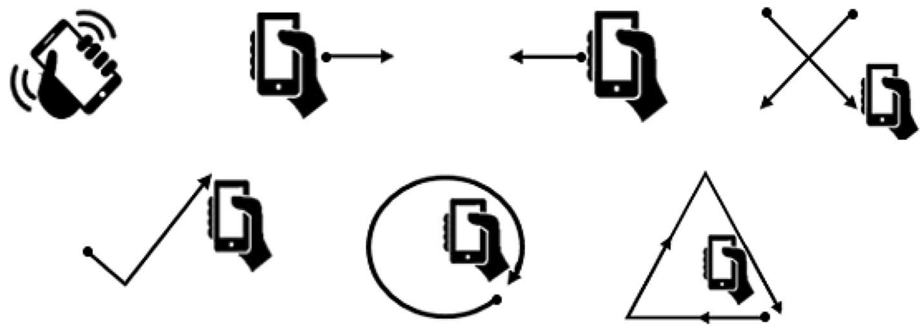

Fig. 2 A graphical representation of the selected gestures for user identification. Starting from left to right and top to bottom, these graphical symbols represent the following gestures: **a** Handwaving, **b** Right arm swipe to right, **c** Right arm swipe to left, **d** Right-hand draw cross, **e** Right-hand draw tick, **f** Right-hand draw circle, and **g** Right-hand draw triangle

Table 1 Details of short-term activities selected for user identification

Code	Short-term activities	Trials	Duration (s)
S1	Pick up device from table and putting it back	5	2.5 ± 4
S2	Unlock the device by pressing power button and unlock pattern	5	3 ± 4
S3	Keystroke pattern: "In a meeting call you later"	5	5 ± 10
S4	Dialing a number and make a call	5	5 ± 10
S5	Pull down phone from ear to lock	5	2 ± 4

Dataset description

Stimuli

The dataset includes smartphone data when different types of activities are performed by participants. The activities considered are those which define the user interaction with the device, thus making it suitable for identifying smartphone users. The dataset encompasses a total of 12 activities, which are divided further into two groups, namely *short-term activities* and *gestures*. Short-term activities can be defined as those activities which are performed while the user is using the smartphone. They are named as short-term activities because their duration of performing a single trail is relatively short as compared to the most commonly used ADLs. The activities that fall into the category of gestures represent some specific type of gestures performed by the user while holding a smartphone in hand. The graphical representation of these gestures is presented in Fig. 2. Tables 1 and 2 summarize the necessary details related to all the captured activities with their time duration in seconds.

Dataset acquisition protocol

The dataset for smartphone user identification was collected at the University of Engineering and Technology, Taxila, Pakistan. The experiments were performed in a controlled environment of video and image processing lab in the Computer Engineering department. The lab was dedicated to data collection purpose and kept free from

Table 2 Details of hand gestures selected for user identification

Code	Gestures	Trials	Duration (s)
G1	Handwaving gesture	5	4
G2	Right arm swipe to the right	5	4
G3	Right arm swipe to the left	5	4
G4	Right-hand draw cross	5	4
G5	Right-hand draw tick	5	4
G6	Right-hand draw circle	5	4
G7	Right-hand draw triangle	5	4

external interruptions. The users were provided with a chair to sit and perform the selected activities. Data were recorded from the accelerometer and gyroscope sensor of the Lenovo Vibe K5 Plus smartphone. The gyroscope was calibrated prior to data recording using the device's integrated tool. An existing android application, "Linear-DataCollector," was used for raw data acquisition of the smartphone sensors at the sampling rate of 50 Hz. The application can be downloaded from the following link: https://www.utwente.nl/en/eemcs/ps/research/dataset/. For each sample, the timestamp value was recorded along with the sensor's values for segmentation purposes. The subjects were asked to perform activities in sequential order with 05 trials of each activity, where the gestures were performed, followed by the selected short-term activities. After performing all trials of one activity, the users were asked to take rest for the 1-min duration before performing the next activity. In this way, approximately 25–30 min were taken by each user in the completion of his/her experimental study.

Participants

For dataset generation, 26 participants (14 male and 12 female) from the same department have voluntarily recorded their data when performing the predefined activities. The average age of the participants was 21 years, with a standard deviation of 03 years. Neither of the participants was forced to perform activities in a specific position. All the participants have successfully completed their experiment.

Data pre-processing

The data acquired from smartphone sensors are affected by noise due to the unnecessary participant motion or sudden device movements. Before further processing of the sensory data, it is essential to minimize unwanted noise from the data to produce accurate results. Hence, the accelerometer and gyroscope data were passed through an average smoothing filter for signal denoising. The duration of all activities is less than 5 s except for S3 and S4 activities, so only these two activities were segmented when required. If the duration of these two activities is higher than 4 s, then filtered data of these activities is further divided into smaller chunks of 4 s.

Feature extraction

The filtered data can further be used for feature extraction. Several commonly used features from the existing studies [44–46] were selected to test the proposed scheme

Table 3 Set of features extracted to test the proposed scheme performance

Domain	Feature	Equation*
Time	Arithmetic mean	$\bar{s} = \frac{1}{N}\sum_{i=1}^{N} s_i$
Time	Minimum amplitude	$s_{min} = min(s_i)$
Time	Maximum amplitude	$s_{max} = max(s_i)$
Time	Standard deviation	$std(s) = \sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(s_i - \bar{s})^2}$
Time	kurtosis	$kurtosis(s) = \sum_{i}^{N}\frac{(s_i-\bar{s})^4}{N\sigma^4}$
Time	Skewness	$skewness(s) = \sum_{i}^{N}\frac{(s_i-\bar{s})^3}{N\sigma^3}$
Time	Signal magnitude area	$sma(s) = \frac{1}{3}\sum_{i=1}^{3}\sum_{j=1}^{N}\lvert s_{i,j}\rvert$
Time	Median absolute deviation	$mad(s) = median_i\left(\left\lvert s_i - median_{j(s_j)}\right\rvert\right)$
Time	Interquartile range	$iqr(s) = Q3(s) - Q1(s)$
Time	Autoregression	$a = arburg(s,4)a\epsilon\mathbb{R}^4$
Time	Sum vector magnitude	$\lvert s\rvert = \sqrt{s_{i,x}^2 + s_{i,y}^2 + s_{i,z}^2}$
Time	Angle between z-axis and vertical	$\theta 1 = atan2\left(\sqrt{s_{i,x}^2 + s_{i,y}^2}, s_{i,z}\right)$
Time	Orientation of a person's trunk	$\theta 2 = \mathrm{atan}\left(\sqrt{s_{i,x}^2 + s_{i,y}^2}/s_{i,z}\right)$
Time	Angle between device and ground	$\theta 3 = \sin(s)$
Frequency	Maximum frequency index	$maxFreqInd(S) = arg\,max_i(S_i)$
Frequency	Mean frequency	$mean\,freq(S) = \sum_{i=1}^{N}(iS_i)/\sum_{j=1}^{N}S_j$
Frequency	Energy	$E_f = \sum \lvert S(f)\rvert^2$
Frequency	Entropy	$H(S(f)) = -\sum_{i=1}^{N}p_i(S(f))\log_2 p_i(S(f))$

*Here s. represents a 3D signal, i and j signify the signal index, $s_{i,x}$., $s_{i,y}$, and $s_{i,z}$ denote the signal value along x, y, and z-axis of the sensor, respectively,$Q1$ and $Q3$ represent the first and third signal quartile, N is the total number of samples in a data chunk, S is the Fourier transform of signal s, and p is the probability

performance, which are listed in Table 3 along with their mathematical equations. Different variables and subscripts/superscripts used in these equations are defined as footnote (*) of Table 3. These features include both time and frequency domain features, including statistical signal attributes, auto-regression coefficients, and angular features. Overall, eighteen (18) different features were extracted, where the size of the final feature vector obtained was [1 × 145], containing all the extracted features on three dimensions, i.e., x, y, and z, of the accelerometer and gyroscope.

User Identification

To identify smartphone users based on their interaction with a smartphone, three prevalent classifiers Support Vector Machine (SVM), Random Forests (RF), and Bayes Net (BN) were used. The classifiers were selected because of their frequent use and excellent performance in the existing studies. The activities performed by the user were classified into different groups, where the identified activity patterns were used for user classification. A detailed experimental analysis was conducted to test the performance of three different classifiers for the proposed scheme.

Experimental results and analysis

This section depicts the results of the performed experiments to explore whether the collected measurements can be used for user authentication or not. The results are presented separately for two different groups of activities.

Classification methods

According to the dataset, the user authentication is a multi-class classification problem. Three commonly used machine learning algorithms, including SVM, RF, and BN, are considered for training and testing purposes. A cross-validation method with k-folds is applied to the dataset where k is set equal to 10. The activities performed by the user were labeled, and the user who performed those activities was also labeled. The training and testing procedure has been applied for each activity. For SVM, the linear algorithm of Sequential Minimal Optimization was used.

Performance metrics

For evaluating the performance of the proposed scheme, four different performance metrics have been used, which include: accuracy, F-measure, kappa statistic, and Root Mean Square Error (RMSE). Kappa statistic is a statistical measure that is independent of total classes. In kappa statistic, when $k_p = 0$, it means that there is a chance-level classification. If the value of k_p increases from zero and reaches to 1, it then represents perfect classification. In contrast, the value of k_p going below zero represents that the result of classification is poorer than the chance-level classification.

Table 4 User identification results for activities S1–S5 based on chosen performance metrics

Short-term activities	Classifier	Accuracy %	F-measure	Kappa	RMSE
S1	SVM	71.79	0.716	0.706	0.186
	Random forests	71.15	0.701	0.700	0.141
	Bayes net	60.89	0.595	0.593	0.163
S2	SVM	45.39	0.450	0.431	0.187
	Random forests	57.23	0.668	0.554	0.162
	Bayes net	28.28	0.243	0.253	0.209
S3	SVM	75.56	0.754	0.744	0.186
	Random forests	76.20	0.748	0.751	0.133
	Bayes net	60.45	0.595	0.586	0.160
S4	SVM	60.36	0.587	0.587	0.187
	Random forests	59.75	0.580	0.580	0.151
	Bayes net	50.00	0.470	0.479	0.175
S5	SVM	59.75	0.588	0.579	0.187
	Random forests	54.26	0.516	0.520	0.162
	Bayes net	38.41	0.323	0.355	0.179

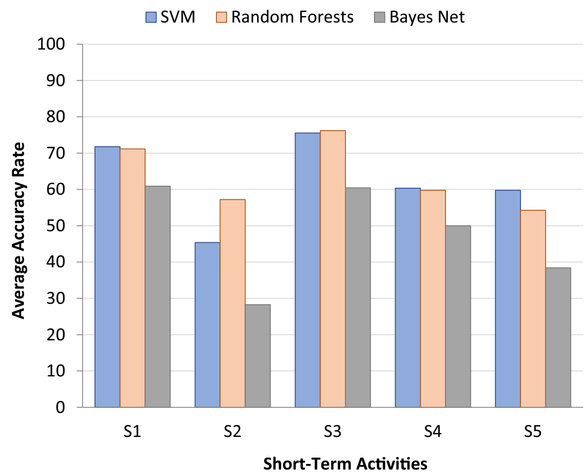

Fig. 3 Average accuracy percentage for user identification based on short-term activities

User Identification based on Short-term Activities

This section shows the identification performance of the short-term activities that participants performed when they were using the smartphone. Table 4 represents the detailed user identification results for activities S1–S5. The highest accuracy is achieved in the case of S3 activity by RF classifier, which is the keystroke pattern. It means that most of the users are correctly identified based on their keystroke patterns. The highest average accuracy is achieved by the RF classifier, which is 63.72%, and the worst accuracy is achieved by BN classifier, i.e., 47.61%.

Figure 3 provides a comparison of the average accuracy rate obtained for user identification based on short-term activities using SVM, RF, and BN classifier. It can be observed from the figure that for most of the activities, RF classifier provides better performance than SVM and BN classifiers.

User identification based on hand gestures

This section represents the user identification performance of the hand gestures performed by the user when holding the smartphone in hand. The inertial sensors were recording data unobtrusively, which is used for identifying smartphone users. Table 5 shows the user recognition results for activities G1–G7. The highest accuracy is achieved in the case of G6 and G7, which represent "right hand draw circle" and "right hand draw triangle" gesture, respectively. The accuracy of SVM and RF classifiers is the same for these two gestures. However, the overall average accuracy is higher in the case of RF, which is 74.97% for all the gestures. The worst classification results were obtained using the BN classifier with an average accuracy of 64.38%. Figure 4 compares of the average accuracy rate obtained for user identification based on hand gestures using SVM, RF, and BN classifier, which show that RF classifier outperforms SVM and BN classifiers in most of the cases.

The average accuracy rate (i.e., 74.97%) of the RF classifier is the highest among all three classifiers in identifying the smartphone user. SVM has the second-best performance with a 74.78% accuracy rate, and the worst recognition accuracy of 64.38% is

Table 5 User identification results for activities G1–G7 based on chosen performance metrics

Gestures	Classifier	Accuracy %	F-measure	Kappa	RMSE
G1	SVM	69.75	0.699	0.6851	0.1867
	Random forests	73.45	0.720	0.7238	0.1445
	Bayes net	65.43	0.628	0.6403	0.1519
G2	SVM	70.46	0.745	0.6925	0.1866
	Random forests	67.78	0.677	0.6646	0.1471
	Bayes net	59.73	0.581	0.5808	0.1585
G3	SVM	85.90	0.858	0.8534	0.1861
	Random forests	83.22	0.824	0.8254	0.1327
	Bayes net	73.82	0.736	0.7277	0.1317
G4	SVM	89.87	0.900	0.8947	0.1861
	Random forests	87.34	0.872	0.8684	0.1271
	Bayes net	83.54	0.833	0.8289	0.1085
G5	SVM	84.17	0.838	0.8353	0.1862
	Random forests	83.54	0.830	0.8288	0.1397
	Bayes net	70.88	0.705	0.6972	0.1385
G6	SVM	92.15	0.918	0.9184	0.186
	Random forests	92.81	0.922	0.9252	0.1218
	Bayes net	90.19	0.901	0.898	0.0836
G7	SVM	92.15	0.921	0.9184	0.1861
	Random forests	92.81	0.925	0.9252	0.1178
	Bayes net	90.84	0.904	0.9048	0.0786

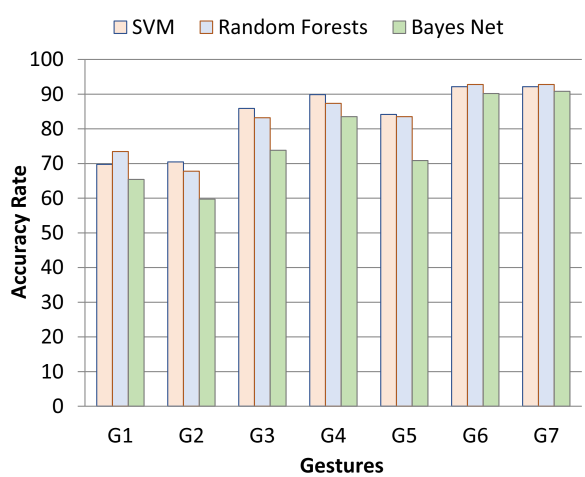

Fig. 4 Average accuracy percentage for user identification based on hand gestures

obtained for the BN classifier. Figure 5 shows the overall average accuracy for user identification based on all the selected activities using RF classifier. The results demonstrate that the average accuracy is higher in the case of gestures as compare to short-term activities performed by the user. This is because while performing the gesture, the user makes frequent movements that assist in recognizing every user and distinguish them

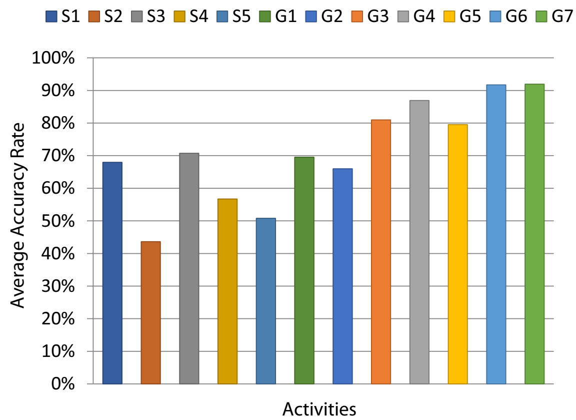

Fig. 5 Overall average accuracy obtained for user identification based on RF classifier

well. Hence, based on the overall results, the proposed scheme provides a viable solution for smartphone user identification.

Conclusion

In this paper, a passive and implicit smartphone user identification scheme is proposed for smartphone security, which is purely based on the behavioral biometrics of the user, i.e., how a user interacts with his/her device. A set of 12 different activities have been used for experimentation purpose, which is divided into two groups, named as short-term activities and gestures. The experimental results for user identification based on short-term activities revealed that the best performance is achieved by RF classifier in the case of keystroke pattern activity. Similarly, in the case of gestures, the best authentication results were also obtained using the RF classifier. The overall average recognition results are better in the case of gestures as compare to short-term activities because the user performs more frequent actions when performing gestures. For future work, the accuracy can be significantly improved by using a large dataset with more sensors. Feature selection methods can also be applied to enhance the recognition performance as well. Similarly, the effects of temporal and permanent behavioral changes need to be considered in order to test the identification accuracy. Open-set recognition can be applied to classify between a valid and invalid set of activities. In the same way, the classification between impostors and an authenticated user can be performed to achieve smartphone authentication. Wearable sensors can be used to identify a user based on the way how he/she interacts with an object.

Abbreviations

ADLs: activities of daily living; AI: Artificial Intelligence; BN: Bayes net; CA: continuous authentication; CC: cloud computing; EER: equal error rate; FAR: false acceptance rate; FRR: false rejection rate; HMM: Hidden Marvok Model; ICTs: Information and Communication Technologies; IA: implicit authentication; IoT: Internet-of-Things; PINs: Personal Identification Numbers; PSO: practical swarm optimization; RBFN: radial basis function network; RF: random forests; RMSE: root mean square error; SVM: support vector machine.

Acknowledgements

Not applicable.

Authors' contributions

MA and SHC designed the study and protocol for data acquisition. MNM, ME, and MAA performed data collection and provided an initial analysis of data. All the authors contributed in writing and reviewing the article to present the study in a better way. All authors took part in updating and revising the article. All authors read and approved the final manuscript.

Funding

Not applicable.

Availability of data and materials

The datasets used and analyzed during the current study are available from the corresponding author on reasonable request.

Competing interests

The authors declare that they have no competing interests.

Author details

[1] Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia. [2] Department of Computer Science and Artificial Intelligence, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia. [3] Faculty of Telecom and Information Engineering, University of Engineering and Technology (UET), Taxila, Punjab 47050, Pakistan.

Received: 17 October 2019 Accepted: 18 January 2020
Published online: 28 February 2020

References

1. Kim Y, Oh T, Kim J (2015) Analyzing user awareness of privacy data leak in mobile applications. Mob Inf Syst. https://doi.org/10.1155/2015/369489
2. Achara J, Castelluccia C, Lefruit J-D et al (2013) Mobilitics: analyzing privacy leaks in smartphones. https://ercim-news.ercim.eu/en93/special/mobilitics-analyzing-privacy-leaks-in-smartphones
3. Jung T, Mao X, Li XY, et al (2013) Privacy-preserving data aggregation without secure channel: multivariate polynomial evaluation. In: Proceedings—IEEE INFOCOM, pp 2634–2642
4. Jung T, Li XY, Wan Z, Wan M (2013) Privacy preserving cloud data access with multi-authorities. In: Proceedings—IEEE INFOCOM, pp 2625–2633
5. Mehboob R, Dawood H, Dawood H et al (2018) Live fingerprint detection using magnitude of perceived spatial stimuli and local phase information. J Electron Imaging 27:1. https://doi.org/10.1117/1.jei.27.5.053038
6. Xi K, Hu J, Han F (2012) Mobile device access control: an improved correlation based face authentication scheme and its Java ME application. Concurr Comput 24:1066–1085
7. Niinuma K, Park U, Jain AK (2010) Soft biometric traits for continuous user authentication. IEEE Trans Inf Forensics Secur 5:771–780. https://doi.org/10.1109/TIFS.2010.2075927
8. Qi M, Lu Y, Li J, et al (2008) User-specific iris authentication based on feature selection. In: Proceedings—international conference on computer science and software engineering, CSSE 2008, pp 1040–1043
9. Shukla D, Kumar R, Serwadda A, Phoha V V. (2014) Beware, your hands reveal your secrets! In: CCS—ACM conference on computer and communications security, pp 904–917
10. SRLabs: Spoofing fingerprints. https://srlabs.de/spoofing-fingerprints
11. Data genetics: pin analysis. https://www.datagenetics.com/blog/september32012/
12. Kela J, Korpipää P, Mäntyjärvi J et al (2006) Accelerometer-based gesture control for a design environment. Pers Ubiquitous Comput 10:285–299. https://doi.org/10.1007/s00779-005-0033-8
13. Niezen G, Hancke GP (2009) Evaluating and optimising accelerometer-based gesture recognition techniques for mobile devices. In: IEEE AFRICON conference
14. Bo C, Jian X, Li XY, et al (2013) You're driving and texting: detecting drivers using personal smart phones by leveraging inertial sensors. In: Proceedings of the annual international conference on mobile computing and networking, MOBICOM, pp 199–201
15. Miluzzo E, Varshavsky A, Balakrishnan S, Choudhury RR (2012) Tapprints: Your finger taps have fingerprints. In: MobiSys'12—Proceedings of the 10th international conference on mobile systems, applications, and services, pp 323–336
16. Buriro A, Crispo B, Conti M (2019) ANSWERAUTH: a bimodal behavioral biometric-based user authentication scheme for smartphones. J Inf Secur Appl 44:89–103. https://doi.org/10.1016/j.jisa.2018.11.008
17. Chiasson S, Oorschot P Van, Biddle R (2006) A usability study and critique of two password managers. 15th USENIX Secur … 1–16
18. Ma J, Yang W, Luo M, Li N (2014) A study of probabilistic password models. In: Proceedings—IEEE symposium on security and privacy, pp 689–704
19. Kelley PG, Komanduri S, Mazurek ML, et al (2012) Guess again (and again and again): measuring password strength by simulating password-cracking algorithms. In: Proceedings—IEEE symposium on security and privacy, pp 523–537
20. Ciolino S, Parkin S, Dunphy P (2019) Of two minds about two-factor: understanding everyday FIDO U2F usability through device comparison and experience sampling. In: Proc Fifteenth Symp Usable Priv Secur 339–356
21. Pentland A, Moghaddam B, Starner T (1994) View-based and modular eigenspaces for face recognition. In: Proceedings of the IEEE computer society conference on computer vision and pattern recognition, pp 84–91

22. Roy A, Memon N, Ross A (2017) MasterPrint: exploring the vulnerability of partial fingerprint-based authentication systems. IEEE Trans Inf Forensics Secur 12:2013–2025. https://doi.org/10.1109/TIFS.2017.2691658
23. Gupta S, Buriro A, Crispo B (2018) Demystifying authentication concepts in smartphones: ways and types to secure Access Mob Inf Syst 2018
24. Nader J, Alsadoon A, Prasad PWC et al (2015) Designing touch-based hybrid authentication method for smartphones. Procedia Comp Sci. 70:198–204
25. Buriro A, Crispo B, Frari F Del, Wrona K (2015) Touchstroke: Smartphone user authentication based on touch-typing biometrics. In: Lecture notes in computer science (including subseries Lecture notes in artificial intelligence and lecture notes in bioinformatics), pp 27–34
26. Teh PS, Zhang N, Tan S-Y et al (2019) Strengthen user authentication on mobile devices by using user's touch dynamics pattern. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-019-01654-y
27. Rehman AU, Awais M, Shah MA (2017) Authentication analysis using input gestures in touch-based mobile devices. In: ICAC 2017–2017 23rd IEEE international conference on automation and computing: addressing global challenges through automation and computing
28. Mäntyjärvi J, Lindholm M, Vildjiounaite E, et al (2005) Identifying users of portable devices from gait pattern with accelerometers. In: ICASSP, IEEE international conference on acoustics, speech and signal processing–Proceedings
29. Saini BS, Kaur N, Bhatia KS (2019) Authenticating mobile phone users based on their typing position using keystroke dynamics. Lecture notes in networks and systems. Springer, Singapore, pp 25–33
30. Feng T, Zhao X, Carbunar B, Shi W (2013) Continuous mobile authentication using virtual key typing biometrics. In: Proceedings—12th IEEE international conference on trust, security and privacy in computing and communications, TrustCom 2013. pp 1547–1552
31. Buriro A, Gupta S, Crispo B, Frari F Del (2018) Dialerauth: A motion-assisted touch-based smartphone user authentication scheme. In: CODASPY 2018—Proceedings of the 8th ACM conference on data and application security and privacy, pp 267–276
32. Feng T, Liu Z, Kwon KA, et al (2012) Continuous mobile authentication using touchscreen gestures. In: 2012 IEEE international conference on technologies for homeland security, HST 2012. pp 451–456
33. Frank M, Biedert R, Ma E et al (2013) Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans Inf Forensics Secur 8:136–148. https://doi.org/10.1109/TIFS.2012.2225048
34. Conti M, Zachia-Zlatea I, Crispo B (2011) Mind how you answer me! Transparently authenticating the user of a smartphone when answering or placing a call. In: Proceedings of the 6th ACM symposium on information, computer and communications security, pp 249–259
35. Sharma V, Enbody R (2017) User authentication and identification from user interface interactions on touch-enabled devices. In: Proceedings of the 10th ACM conference on security and privacy in wireless and mobile networks, WiSec 2017. pp 1–11
36. Velten M, Schneider P, Wessel S, Eckert C (2015) User identity verification based on touchscreen interaction analysis in web contexts. Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics). Springer, Cham, pp 268–282
37. Qin Z, Huang G, Xiong H et al (2019) A Fuzzy authentication system based on neural network learning and extreme value statistics. IEEE Trans Fuzzy Syst. https://doi.org/10.1109/TFUZZ.2019.2956896
38. Zhu J, Wu P, Wang X, Zhang J (2013) SenSec: Mobile security through passive sensing. In: 2013 international conference on computing, networking and communications, ICNC 2013, pp 1128–1133
39. Amin R, Gaber T, ElTaweel G (2015) Implicit authentication system for smartphones users based on touch data. Intelligent data analysis and applications. Springer, Cham, pp 251–262
40. Meng W, Wang Y, Wong DS et al (2018) TouchWB: touch behavioral user authentication based on web browsing on smartphones. J Netw Comput Appl 117:1–9. https://doi.org/10.1016/j.jnca.2018.05.010
41. Nickel C, Wirtl T, Busch C (2012) Authentication of smartphone users based on the way they walk using k-nn algorithm. In: 2012 Eighth international conference on intelligent information hiding and multimedia signal processing, pp 16–20
42. Lee W-H, Lee RB (2015) Multi-sensor authentication to improve smartphone security. In: 2015 International conference on information systems security and privacy (ICISSP), pp 1–11
43. Yang L, Guo Y, Ding X et al (2015) Unlocking Smart Phone through handwaving biometrics. IEEE Trans Mob Comput 14:1044–1055. https://doi.org/10.1109/TMC.2014.2341633
44. Hussain F, Hussain F, Ehatisham-ul-Haq M, Azam MA (2019) Activity-aware fall detection and recognition based on wearable sensors. IEEE Sens J 19:4528–4536
45. Ehatisham-ul-haq M, Awais M, Naeem U et al (2018) Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. J Netw Comput Appl 109:24–35. https://doi.org/10.1016/j.jnca.2018.02.020
46. Ehatisham-ul-Haq M, Azam MA, Naeem U et al (2017) Identifying smartphone users based on their activity patterns via mobile sensing. Procedia Comp Sci 113:202–209

Publisher's Note