Using Data Augmentation in Continuous Authentication on Smartphones

Yantao Li, *Member, IEEE*, Hailong Hu, and Gang Zhou, *Senior Member, IEEE*

***Abstract*—As personal computing platforms, smartphones are commonly used to store private, sensitive, and security information, such as photos, emails, and Android Pay. To protect such information from adversaries, continuous authentication on smartphone users becomes more and more important. In this paper, we present a novel authentication system, *SensorAuth*, for continuous authentication of users based on their behavioral patterns, by leveraging the accelerometer and gyroscope ubiquitously built into smartphones. We are among the first to exploit five data augmentation approaches including permutation, sampling, scaling, cropping, and jittering to create additional data by applying them on training data. With the augmented data, *SensorAuth* extracts sensor-based features in both time and frequency domains within a time window, then utilizes the one-class SVM to train the classifier, and finally authenticates users. We evaluate the authentication performance of *SensorAuth* in terms of the impact of window size, accuracy on each of and combinations of data augmentation approaches, time efficiency, energy consumption, and comparisons with the representative classifiers and with the existing approaches, respectively. The experimental results show that *SensorAuth* performs highly accurate and time-efficient continuous authentication, by reaching the lowest median equal error rate (EER) of 4.66%, and consuming a short authentication time of approximately 5 seconds.**

***Index Terms*—Continuous authentication, data augmentation, one-class Support Vector Machine (SVM), accelerometer and gyroscope, equal error rate (EER).**

I. Introduction

Smartphones are becoming the most commonly used devices in human daily life as personal platforms [1], [2]. People prefer to store important, private, sensitive, and security information, such as photos, emails, and credit card connected Android Pay, on smartphones for their convenience. However, information leakage and stolen smartphones become major concerns for smartphone users [3]. Therefore, to protect the critical information from adversaries who masquerade as legitimate users, researchers and developers have been exploring user authentication mechanisms on smartphones.

Current smartphone operating systems, such as Andorid OS and iOS, have been integrated with one-time user authentication mechanisms. One-time user authentication has been a dominant authentication mechanism on smartphones for decades, and includes passwords or personal identification numbers (PINs), graphical patterns, and fingerprints; however, they offer limited security since they are susceptible to guessing [5], video capture [4], and spoofing [6]. Moreover, since these mechanisms authenticate users only once at the time of initial login, unauthorized users are easily able to physically gain access to unattended smartphones after initial authentication has been performed, which can incur security issues. These security issues have excited the investigation of continuous authentication mechanisms, which can continuously monitor a user's interactions with the smartphone even after initial login to ensure that the initially-authenticated user is still the one using the phone.

Continuous authentication has been a promising mechanism to alleviate the above security issues, by frequently authenticating users via biometrics-based approaches. These authentication approaches can be broadly categorized into physiological biometrics based approaches and behavioral biometrics based approaches. More specifically, the former approaches rely on static physical attributes, such as face patterns [7]–[11], fingerprints [12], [13], iris patterns [14], [15], voice [16] and pulse [17], but they require user direct participation in the process of the authentication. Behavioral biometrics based approaches exploit user behavioral patterns, such as touch gestures [18]–[25], gait [26], [27], and GPS patterns [28]. These approaches identify invariant features of user interactions with the smartphones by using sampling data from built-in sensors and accessories, such as the accelerometer, gyroscope, megnetometer, and touch screen. However, to authenticate users with a high accuracy, they need a large amount of data to train classifiers, which consumes lots of time on data collection.

Data augmentation has been widely used in the field of image recognition, which leverages limited data by transforming existing samples to create new ones [29]. In image recognition, operations such as permutation, scaling, cropping, and jittering on an image that do not change its label, can be used as label-preserving data augmentation methods. These approaches can expand data sets and enhance robustness. However, in the field of sensor data, data augmentation approaches have not been studied. We are among the first to apply data augmentation technology to the field of wireless sensors, which is the major contributions of this work.

In this paper, we present a novel sensor-based authentication system, *SensorAuth*, for continuous authentication of users based on their behavioral patterns. More specifically, *SensorAuth* consists of data collection, data augmentation, feature extraction, classifier, and authentication. The operation of *SensorAuth* includes the enrollment phase for data and classifier

Y. Li and H. Hu are with the College of Computer and Information Sciences, Southwest University, Chongqing 400715 China (e-mail: yantaoli@foxmail.com, corresponding author: Yantao Li)

Y. Li and G. Zhou are with the Department of Computer Science, College of William and Mary, Williamsburg, VA 23185 USA.

training (including Data Augmentation, Feature Extraction, and Classifier training) and the continuous authentication phase for testing (involving Feature Extraction, Classifier testing, and Authentication). Data collection captures behavioral patterns of users by leveraging two sensors of accelerometer and gyroscope ubiquitously built into smartphones. We are among the first to exploit five data augmentation approaches including permutation, sampling, scaling, cropping, and jittering to create additional data by applying them on training data. Then, 32 sensor-based features are extracted in both time and frequency domains from the augmented data within a time window. From these features, the most discriminable ones are selected by the Fisher score ranking, and with the selected features, we use the one-class Support Vector Machine (SVM) to train the classifier in the enrollment phase. With the trained classifier and testing features, *SensorAuth* classifies the current user as a legitimate user or an impostor in the continuous authentication phase. We evaluate the authentication performance of *SensorAuth* in terms of the impact of window size, accuracy on each of the data augmentation approaches, and accuracy on the combinations of data augmentation approaches, time efficiency, energy consumption, and comparisons with the representative classifiers and with the existing approaches, respectively. The experimental results show that *SensorAuth* performs highly accurate and time-efficient continuous authentication, by reaching the lowest median equal error rate (EER) of 4.66%, 12.11% lower than solutions without data augmentation, and costing a short authentication time of approximately 5 seconds.

The main contributions of this work are summarized as follows:

- We design *SensorAuth*, a novel continuous authentication system on smartphones that exploits ubiquitously built-in sensors of accelerometer and gyroscope to capture users' behavioral patterns running as background service. *SensorAuth* consists of data collection, data augmentation, feature extraction, classifier, and authentication.
- We are among the first to explore five data augmentation approaches of permutation, sampling, scaling, cropping, and jittering on training data, which create additional data by applying these transformations on the training data.
- We evaluate the authentication performance of *SensorAuth* in terms of the impact of window size, accuracy on each of and combinations of data augmentation approaches, and time efficiency, energy consumption, and comparisons with the representative classifiers and with the existing approaches. The experimental results show that *SensorAuth* reaches the lowest median EER of 4.66%, and consumes 5-second authentication time.

The remainder of this paper is organized as follows: Section II reviews the existing literature on continuous authentication on smart devices. We present the detailed *SensorAuth* architecture consisting of data collection, data augmentation, feature extraction, classifier, and authentication in Section III. In Section IV, we elaborate the data augmentation approaches of permutation, sampling, scaling, cropping, and jittering applied to the system. Then, we describe our experiment setup in terms of dataset, classifier, metrics and parameter in Section V. In Section VI, we evaluate the authentication performance of *SensorAuth* on window size, accuracy, time efficiency, energy consumption, and comparisons with representative classifiers and with existing approaches, respectively, and conclude this work in Section VII.

II. Related Work

There are a wide range of works focusing on continuous authentication on smart devices, which can be broadly categorized into two groups: physiological biometrics based approaches and behavioral biometrics based approaches.

A. Physiological biometrics based approaches

Physiological biometrics based approaches rely on static physical attributes, such as face patterns [7]–[11], fingerprints [12], [13], iris patterns [14], [15], voice [16] and pulse [17]. There are some significant works devoted to continuous authentication based on physiological biometrics. In [7], the authors propose a new sensor-assisted facial authentication method by using motion and light sensors to defend against 2D media attacks and virtual camera attacks without the penalty of authentication speed. The authors of [8] present an application of the scale invariant feature transform approach in the context of face authentication. In [9], the authors investigate the effectiveness of methods for fully-automatic face recognition in solving the active authentication problem for smartphones. The authors of [10] propose a part-based technique for real time detection of users' faces on mobile devices, which is specifically designed for detecting partially cropped and occluded faces captured using a smartphone's front-facing camera for continuous authentication. In [11], the authors consider face detection and authentication in mobile phones and experimentally analyze a face authentication scheme using Haar-like features with AdaBoost for face and eye detection, and local binary pattern approach for face authentication. The authors of [12] present a phase-only correlation method based on the phase component of images for matching, which is highly robust against noise, brightness change, and image shifting. The authors of [13] develop a prototype biometrics system which integrates face recognition and fingerprint verification. This system incorporates a decision fusion module to improve the identification performance. In [14], the authors investigate iris recognition by using gabor filters and multiscale zero-crossing representation. The authors of [15] propose a novel iris localization method and user-specific automatic iris authentication approach based on feature selection. In [16], the authors present a modular scheme of the training and test phases of a speaker verification system. The authors of [17] propose a new biometric based on the human body's response to an electric square pulse signal. They explore how this biometric can be used to enhance security in the context of two example applications: (1) an additional authentication mechanism in PIN entry systems, and (2) a means of continuous authentication on a secure terminal.

However, physiology biometrics based authentication requires user direct participation in the process of the authentication. We are different in that our system solely makes use

of two common sensors, the accelerometer and gyroscope, on smartphones without any additional hardware devices. Also, we differ in that the system does not require root permissions to obtain sensor data for protecting users' privacy.

B. Behavioral biometrics based approaches

Behavioral biometrics based approaches aim at identifying invariant features of human behaviors during different activities, such as touch gestures, gait, and GPS patterns. There are some valuable works focusing on continuous authentication based on behavioral biometrics.

Continuous authentication based on touch gestures with features extracted from touching screen data is significantly investigated [18]–[20]. In [18], the authors adopt a continuous and passive authentication mechanism based on a user's touch operations on the touchscreen. The authors of [19] present a touch based identity protection service that implicitly and unobtrusively authenticates users in the background by continuously analyzing touch screen gestures in the context of a running application. In [20], the authors propose a novel biometric-based system to achieve continuous and unobservable re-authentication for smartphones by using a classifier to learn the owner's finger movement patterns and checking the current user's finger movement patterns against the owner's.

Continuous authentication based on touch gestures with features extracted from sensor data during a touch event is deeply researched [21]–[24]. The authors of [21] present a framework to authenticate users silently and transparently by exploiting the user touch behavior biometrics and leveraging the integrated sensors to capture the micro-movement of the device caused by user's screen-touch actions. In [22], the authors propose a new mobile system framework using passive sensory data to ensure the security of applications and data on mobile devices. Specifically, they provide a probabilistic approach to model user's gesture patterns using a generative continuous n-gram language model. The authors of [23] present a new set of behavioral biometric features of hand movement, orientation, and grasp (HMOG). HMOG uses accelerometer, gyroscope, and magnetometer readings to unobtrusively capture subtle hand micro-movements and orientation patterns generated when a user taps on the screen. In [24], the authors propose an implicit and continuous authentication system based on a user's behavioral characteristics, by leveraging the sensors already ubiquitously built into smartphones.

Continuous authentication based on gait and GPS patterns is developed [26]–[28]. In [26], the authors present a new identification method for personal devices using the acceleration signal characteristics produced by walking. The authors of [27] extract several features from the gait data and use the k-Nearest Neighbour algorithm for classification. In [28], the authors present an n-gram based model for a user's mobility patterns, which models the user's idiosyncratic location patterns through a collection of n-gram geo-labels, each with estimated probabilities.

Behavioral biometrics based authentication exploits users' behavioral patterns to authenticate their identities by collecting a large amount of sensor data for training, and needs to train a new model based on fresh sensor data obtained at certain intervals in order to maintain reliability. However, our work differs in that we utilize data augmentation approaches to create additional sensor data, thereby greatly reducing the time on data collection, which can enhance the robustness and generalization ability of the system.

III. System Design

In this section, we present the architecture of our continuous authentication system, *SensorAuth*, as illustrated in Fig. 1. As shown in Fig. 1, *SensorAuth* consists of five modules: Data Collection, Data Augmentation, Feature Extraction, Classifier, and Authentication. The operation of *SensorAuth* includes two phases for learning and classifying user's behavioral patterns: the enrollment phase (including Data Augmentation, Feature Extraction, and Classifier training) and the continuous authentication phase (involving Feature Extraction, Classifier testing, and Authentication). *SensorAuth* learns a profile of the legitimate user in the enrollment phase and then authenticates users in the continuous authentication phase. In particular, the Data Augmentation module can create additional data by applying transformations to the limited raw sensor data in the enrollment phase, which is detailed in Section IV. In the remainder of this section, we introduce the other four modules: Data Collection, Feature Extraction, Classifier, and Authentication, respectively.

A. Data Collection

To collect data for our authentication system, we select the two sensors in smartphones: the accelerometer, and the gyroscope. The reasons are that: (1) the two sensors are commonly embedded in the current smartphones and do not need any support from external sensors; (2) the accelerometer and the gyroscope provide different levels of information about users' behavior, respectively. The accelerometer records larger motion patterns of users, such as how they move their arms or walk, while the gyroscope records fine-grained motions of users, such as how they hold their smartphones; (3) the two sensors do not require user permission when requested by mobile applications, which makes them useful for background monitoring; (4) the two sensor data usually do not contain private or sensitive information of users, such as GPS and voice. In the system, the Data Collection module captures every subtle movement during the user's operation of the smartphone, and records the instantaneous readings of the two sensors when the screen is on. The recorded sensor readings of the accelerometer and gyroscope are the values in x, y, and z axes, respectively. In our system, this module is implemented as a listener which listens to all user events on smartphones, and the collected raw data are either stored in a protected buffer for Data Augmentation as training data in the enrollment phase or used for Feature Extraction as testing data in the continuous authentication phase (see Fig. 1).

B. Feature Extraction

The Feature Extraction module consists of feature construction and feature selection. We first propose sensor-based

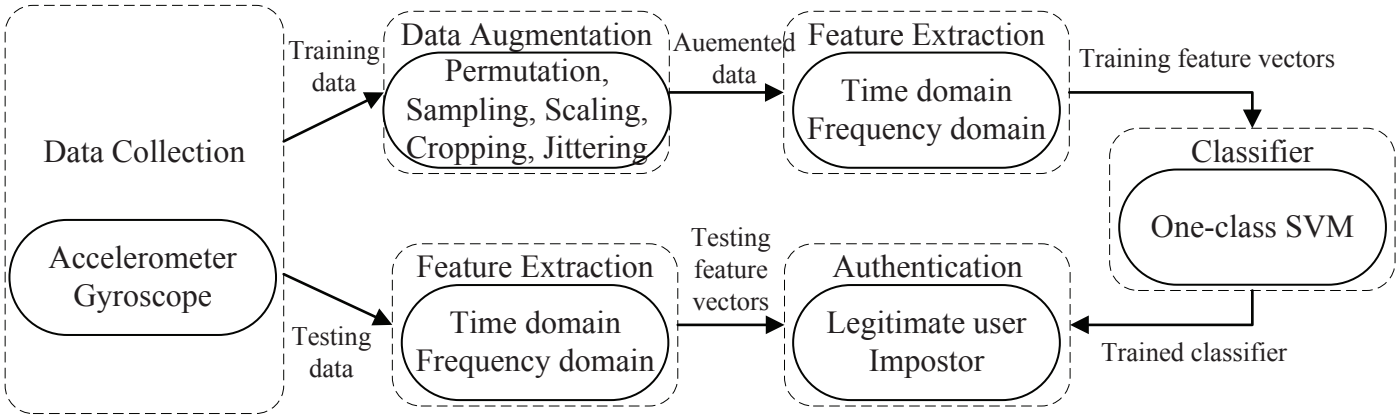

Fig. 1. Architecture of *SensorAuth*

features in time and frequency domains, and then describe how to conduct feature selection.

1) Feature construction: We segment sensor readings into a series of time windows. In each window, we extract sensor-based features from the time domain and the frequency domain. Let x, y, and z be sensor readings (accelerometer or gyroscope) in three axes and we calculate the magnitude $mag = \sqrt{x^2 + y^2 + z^2}$. Discarding direct use of sensor readings, we extract our features based on the magnitude of sensor readings.

Time domain features characterize the motion patterns of users with meaningful statistics during the operation of the smartphones. In the time domain, we extract eleven statistical features of the magnitude for each sensor in a time window, including the mean, median, standard deviation, maximum, minimum, range, kurtosis, skewness, and 25%, 50%, 75% quartiles of magnitude of sensor readings. In particular, the range of the magnitudes in a time window indicates the difference between the maximum magnitude and the minimum one, which can differentiate users with different ranges of the magnitudes. The kurtosis feature represents the width of peak for magnitudes in a time window, and the skewness feature indicates the orientation of peak for magnitudes.

Frequency domain features depict the frequency domain information of user actions in the process of operating the smartphones, and frequency domain information is obtained by implementing the Fast Fourier Transform (FFT) on sensor readings. In the frequency domain, we extract five features, involving energy, entropy, peak1, peak2f, and peak2.

Combining the features from the time domain and frequency domain, we have 32 sensor-based features (2 sensors $\times$ 16 features) in total. In order to save space, we only list the 16 features based on one set of sensor readings (accelerometer or gyroscope) in a time window in Table I.

2) Feature selection: Given the extracted 32 features based on the sensor readings of the accelerometer and gyroscope, Feature Extraction then conducts feature selection to remove poor features and select features with high discriminability. We exploit Fisher score ranking to do feature selection, where a higher Fisher score indicates higher discriminability of the corresponding feature. In our experiment, using ten-fold cross validation, we test feature subsets whose sum of Fisher scores accounted for 90% of the sum of Fisher scores for all features.

TABLE I
SENSOR-BASED FEATURES.

Aspect	Feature	Explanation
Time domain	Mean	Mean value of the magnitudes of sensor readings
	Median	Median value of the magnitudes of sensor readings
	Standard deviation	Standard deviation of the magnitudes of sensor readings
	Maximum	Maximum value of the magnitudes of sensor readings
	Minimum	Minimum value of the magnitudes of sensor readings
	Range	Difference between the maximum value and minimum value of the magnitudes of sensor readings
	Kurtosis	Width of peak of the magnitudes of sensor readings
	Skewness	Orientation of peak of the magnitudes of sensor readings
	Quartiles	25%, 50%, 75% quartiles of magnitudes of sensor readings
Frequency domain	Energy	Intensity of the magnitudes of sensor readings
	Entropy	Dispersion of spectral distribution of the magnitudes of sensor readings
	Peak1	Amplitude of the first highest peak of the magnitudes of sensor readings
	Peak2f	Frequency of the second highest peak of the magnitudes of sensor readings
	Peak2	Amplitude of the second highest peak of the magnitudes of sensor readings

C. Classifier

After features are extracted and selected, they are passed to Classifier for training and testing, respectively. We implement the one-class SVM classifier [30]–[32], which exploits a kernel function to map data into a high dimensional space, and considers the origin as the only sample from other classes. In the enrollment phase, the classifier is established by using training feature vectors of the owner's data with a radial basis function (RBF) kernel. In the continuous authentication phase, the trained classifier projects the testing feature vectors onto

the same high-dimensional space, and classifies the testing feature vectors from all users.

To do the user authentication, the classifier only needs to classify whether the current user is the owner. When training, one-class SVM classifier just requires the owner's features, rather than other users'. When testing, the classifier compares the trained features of the owner with the current user's to do the classification. We select one-class SVM because it provides high accuracy, is effective in high dimensional spaces, and is flexible in modeling diverse sources of data [33], [34]. Moreover, it is demonstrated that SVM performs well in detecting user patterns in various applications, such as motion pattern [35].

D. Authentication

Based on the testing feature vectors and the trained classifier, Authentication classifies the current user as a legitimate user or an impostor. In the continuous authentication phase, the legitimate user's profile generated from the training data in the enrollment phase is compared against the current user's features. If the current user is classified as an impostor, *SensorAuth* will require initial login inputs; otherwise, it will continuously authenticate the user.

IV. Data Augmentation

In image processing, operations such as scaling, cropping, and jittering on an image do not change its label, which can be used as label-preserving data augmentation methods. We use data augmentation methods to create additional data by transforming the collected raw data, which can be considered as an injection of prior knowledge about the invariant properties of the data against certain transformations. With data augmentation, *SensorAuth* can save time on data collection for classifier training in the enrollment phase. Moreover, augmented data can cover unexplored input space, prevent overfitting, and improve the generalization ability of the SVM model [29]. Therefore, such additional data improve the accuracy of the continuous authentication. In this section, to augment sensor data, we apply five data augmentation approaches on the training data: permutation, sampling, scaling, cropping, and jittering.

Before describing these methods, we first introduce the structure of the collected raw data. In our Data Collection, the collected data are stored in a format of a matrix in smartphone buffers, and the readings of the accelerometer and gyroscope are saved as $n \times 3$ matrices M_a and M_g, respectively:

$$M_a = \begin{bmatrix} x_1^a & y_1^a & z_1^a \\ x_2^a & y_2^a & z_2^a \\ \vdots & \vdots & \vdots \\ x_n^a & y_n^a & z_n^a \end{bmatrix} \quad \text{and} \quad M_g = \begin{bmatrix} x_1^g & y_1^g & z_1^g \\ x_2^g & y_2^g & z_2^g \\ \vdots & \vdots & \vdots \\ x_n^g & y_n^g & z_n^g \end{bmatrix}.$$

For convenience, we take matrix M_a of accelerometer readings as an instance to describe data augmentation approaches.

A. Permutation

Permutation randomly perturbs the temporal location of within-window events, which relates to the act of arranging all the elements of a dataset into some sequence or order. Permutation of sensor data can reduce the dependency of the element location and obtain weakly-invariant features over various locations of the elements.

In order to perturb the location of the sensor data within a time window, we first slice matrix M_a by row into s same-length segments with each segment n/s rows as:

$$M_a' = \begin{bmatrix} M_a(1) \\ M_a(2) \\ \vdots \\ M_a(s) \end{bmatrix}, \quad \text{where} \quad M_a(i) = \begin{bmatrix} x_{(i-1)n/s+1}^a & y_{(i-1)n/s+1}^a & z_{(i-1)n/s+1}^a \\ x_{(i-1)n/s+2}^a & y_{(i-1)n/s+2}^a & z_{(i-1)n/s+2}^a \\ \vdots & \vdots & \vdots \\ x_{in/s}^a & y_{in/s}^a & z_{in/s}^a \end{bmatrix}, (i \in [1, s]).$$

There are $s!$ number of permutation sequences for M_a' and we randomly select one of the permutations shown as:

$$M_a^{pt} = \begin{bmatrix} M_a(t1) \\ M_a(t2) \\ \vdots \\ M_a(ts) \end{bmatrix}, \text{ where } t1, t2, ..., ts \text{ is a permutation order}$$

of $1, 2, ..., s$. In our experiment, we set $s = 4$.

Then, after data are augmented by the permutation approach, we obtain a new data matrix of accelerometer readings, as shown in Eq. (1)

$$M_a^{apt} = \begin{bmatrix} M_a \\ M_a^{pt} \end{bmatrix} \tag{1}$$

B. Sampling

Sampling samples from a time window can be regarded as perturbing the data with local translations. That is, irregular intervals by random sampling distort the timestamps between the samples, thus, introducing variability due to local translations in time.

For convenience, we take the z axis of the accelerometer as an instance and use Z_a to denote the readings of the z axis of the accelerometer in a time window, expressed as: $Z_a = \{z_1^a, z_2^a, ..., z_n^a\}$. In our experiments, we sample m samples in a time window n, where we set $m = 90\% \times n$. Supposing ζ_i is uniformly distributed within [1, n], denoted as $\zeta_i \sim U(1, n)$, m samples in z axis are sampled as: $Z_a^{sp} = \{z_{\zeta_1}^a, z_{\zeta_2}^a, ..., z_{\zeta_i}^a, ..., z_{\zeta_m}^a\}$. Then, the sampling matrix of the accelerometer readings can be written as: $M_a^{sp} = [(X_a^{sp})^\top, (Y_a^{sp})^\top, (Z_a^{sp})^\top]$, where $\top$ denotes the transpose of a vector.

Then, after data are augmented by the sampling approach, we obtain a new data matrix of accelerometer readings, as shown in Eq. (2):

$$M_a^{asp} = \begin{bmatrix} M_a \\ M_a^{sp} \end{bmatrix} \tag{2}$$

C. Scaling

Since sensor data gathered from the accelerometer or gyroscope may contain sensor noise, scaling introduces window-wise multiplicative noise to the training data, thereby increasing robustness against noise.

Scaling is applied to a time-window data of sensor readings. In a time window, the augmented data by scaling can be expressed as: $M_a^{sc} = \zeta M_a = \begin{bmatrix} \zeta x_1^a & \zeta y_1^a & \zeta z_1^a \\ \zeta x_2^a & \zeta y_2^a & \zeta z_2^a \\ \vdots & \vdots & \vdots \\ \zeta x_n^a & \zeta y_n^a & \zeta z_n^a \end{bmatrix}$, where $\zeta \sim U(a, b)$. In our experiment, we set $a = 0.99$ and $b = 1.01$.

Then, after data are augmented by the scaling approach, we obtain a new data matrix of accelerometer readings, as shown in Eq. (3)

$$M_a^{asc} = \begin{bmatrix} M_a \\ M_a^{sc} \end{bmatrix} \tag{3}$$

D. Cropping

Cropping is a primitive approach to diminish the dependency on the event location, which can reduce the length of time-series input, and thus decrease the variability due to different event locations.

In a t-second time window, we crop m samples. Supposing $\zeta_i \sim U(1, b)$ and $b = t - m$, we obtain the cropped samples: $Z_a^{cp} = \{z_{\zeta_i}^a, z_{\zeta_{i+1}}^a, ..., z_{\zeta_{i+m}}^a\}$. Then, the matrix of the accelerometer readings by cropping can be written as: $M_a^{cp} = [(X_a^{cp})^\top, (Y_a^{cp})^\top, (Z_a^{cp})^\top]$. Finally, a new data matrix M_a^{acp} can be obtained by cropping, as shown in Eq. (4):

$$M_a^{acp} = \begin{bmatrix} M_a \\ M_a^{cp} \end{bmatrix} \tag{4}$$

E. Jittering

Due to noise in sensor data, jittering can introduce element-wise additive noise to increase robustness against noise.

Jittering is applied to each element of sensor readings. Supposing ζ_i is Gaussian noise and conforms $\zeta_i \sim N(\mu, \sigma^2)$, we add noise to z axis sensor readings of the accelerometer as: $Z_a^{jt} = \{z_1^a + \zeta_1, z_2^a + \zeta_2, ..., z_n^a + \zeta_n\}$. Then, the matrix of the accelerometer readings by jittering can be written as: $M_a^{jt} = [(X_a^{jt})^\top, (Y_a^{jt})^\top, (Z_a^{jt})^\top]$. Finally, a new data matrix M_a^{ajt} can be obtained, as shown in Eq. (5):

$$M_a^{ajt} = \begin{bmatrix} M_a \\ M_a^{jt} \end{bmatrix} \tag{5}$$

V. Experiments

In this section, we first describe the dataset used by *SensorAuth*. We then discuss the experimental process of classifier training and testing, and present different metrics that we use to evaluate the proposed system.

A. Dataset

To investigate the accuracy of *SensorAuth*, we use sensor data from a public multi-modal dataset [23]. The dataset contains sensor readings of the accelerometer and gyroscope collected by ten Samsung Galaxy S4 smartphones with the sampling rate of 100Hz from 100 users (53 male, and 47 female), and the same user might receive a different device during each visit. In data collection, each user devotes to approximately 2 to 6 hours of behavior traits including document reading, text production, and navigation on a map locating a destination.

Among all 100 users, there were 2 users whose data were manually discarded due to extremely abnormal values. Among the remaining 98 users, to ensure that users have the same amount of data, we select the first 100 minutes of data for each user with a 6-second window size. Accordingly, a 6-second window should have 600 sample data; however, some windows have fewer sample data due to data missing. To create same-length inputs and calculate the frequency domain feature conveniently, we use 512 samples for each time window and these samples are extracted from an approximately 5-second time window in our experiments.

B. Parameter selection

Since we use RBF kernel for one-class SVM classifier, we perform a grid search to find the values for parameters γ and μ. For both γ and μ, we first search through $0.01, 0.02, ..., 0.1, 0.2, ..., 0.5$, and then use ten-fold cross validation on training data to select the appropriate parameter values.

C. Classifier training

We utilize ten-fold cross validation to train the one-class SVM classifier, since it can properly avoid overfitting. We specify one of the 98 users as a legitimate user and the rest as impostors. That is, we have positive feature samples from one legitimate user and negative feature samples from 97 impostors. Based on these samples, we train the classifier as follows:

Step 1: We randomly divide all positive samples into k ($k = 10$) equal-size subsets, where $k - 1$ positive subsets are used to train the one-class SVM model, and one subset to test the model.

Step 2: We randomly select negative samples with the same size as positive ones from all the negative samples, which are also divided into k ($k = 10$) equal-size subsets. One of the 10 negative subsets is exploited to test the model.

Step 3: The above 2 steps are repeated 10 times until each subset of negative samples and each subset of positive samples are tested exactly once.

Step 4: We repeat steps 1, 2, and 3 twenty times to account for the effect of the randomness.

D. Metrics

We describe three metrics that we used for analyzing the authentication accuracy of *SensorAuth*.

- False acceptance rate (FAR): the ratio of the number of falsely accepted unauthorized users to the total number of invalid requests made by impostors trying to access the system. A lower FAR is preferred in cases where security is very important [36].
- False rejection rate (FRR): the ratio of the number of falsely rejected requests to the total number of valid requests made by legitimate users trying to access the system. A lower FRR is preferred for user convenience [37].

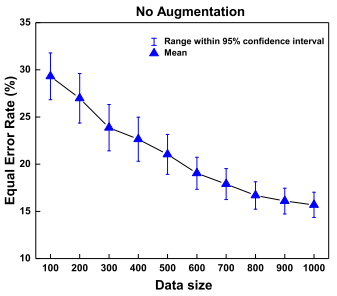

Fig. 2. Accuracy with different data sizes.

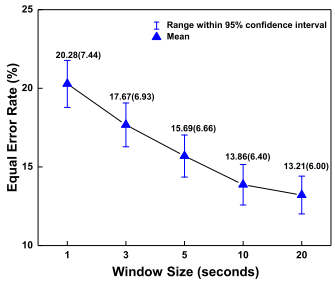

Fig. 3. Accuracy on time window size.

• Equal error rate (EER): the point where FAR equals to FRR. FAR or FRR cannot provide the whole picture, because there is a trade-off between them. We use EER as a metric to evaluate the accuracy of *SensorAuth* [38], [39].

VI. Experimental Results

In this section, we present the experimental results on the authentication performance of *SensorAuth*. More specifically, we first explore the impact of training dataset size on raw data (no data augmentation) as a baseline, and then investigate the impact of time window size on the performance. Next, we present the authentication accuracy on each of and the combinations of the proposed data augmentation approaches, respectively, the time efficiency, and energy consumption of the system. Finally, we compare our approach with the representative classifiers and with the existing approaches, respectively.

A. Impact of dataset size

Training dataset size is of importance and has a significant impact on authentication accuracy. We evaluate the impact of training dataset size on authentication accuracy, with sizes ranging from 100 to 1000. This experiment is conducted on raw data, without data augmentation, which is considered baseline. Fig. 2 shows the experimental results of EERs with mean points connected against variable training data sizes. As shown in Fig. 2, the EER decreases as the dataset size increases. More specifically, the mean EER achieves up to 29.3% with 100 samples in the dataset, while with 800 samples the mean EER reaches down to 16.68%, approximately a 12.62% reduction. The lowest EER is approximately 15.69%, when the training sample size comes to 1000.

We observe that the authentication accuracy gradually becomes saturated as training dataset size increases. However, we notice that the larger the training dataset size is, the longer the training process will take. Therefore, there is a tradeoff between authentication accuracy and user applicability in practice.

B. Impact of time window size

The size of the time window is a significant system parameter for determining the time that the system requires to perform user authentication.

We vary the window size from 1 second to 20 seconds to select the appropriate window size for *SensorAuth*. Given each window size, for each of 98 users, we utilize ten-fold cross-validation for training and testing. We plot the EER with mean points connected against different window sizes in Fig. 3, with standard deviations (SDs) in the parentheses, where the training dataset size is 1000. As illustrated in Fig. 3, the EER gradually decreases as the time window size increases, and when the time window size is larger than 10 seconds, little performance improvement can be obtained. Moreover, the standard deviation decreases as the window size increases, which indicates the EER corresponding to each window size tends to be stable as the window size increases. However, the smaller the time window size is, the higher the frequency of user authentication is. Taking the authentication accuracy and the experience of user authentication into account, we set the time window size as 5 seconds.

C. Accuracy on data augmentation approaches

In this section, we investigate the authentication accuracy on each of the data augmentation approaches that consist of permutation, sampling, scaling, cropping, and jittering.

Fig. 4 shows box plots of EERs with different data augmentation approaches on different dataset sizes. For each data augmentation approach, we vary the dataset size from 100 to 800. For each dataset size, we plot boxes of EERs with no augmentation (red box plot) and that with augmentation approach (blue box plot), respectively, for comparison. As illustrated in Fig. 4, for all the five data augmentation approaches, the EERs with data augmentation approaches show significant lower values than those without data augmentation for all dataset sizes.

Table II lists the medians with SDs in parentheses of EERs with different data augmentation approaches on different dataset sizes, where the standard deviations indicate robustness of the system. As shown in Table II, the worst median EER is 11.56% (when dataset size is 500), which indicates that all the five data augmentation approaches exhibit certain improvements in authentication accuracy. In particular, the permutation approach achieves the best performance among other data augmentation approaches, with a 7.85% median EER and 4.85% SD at the best circumstances. As described in Section IV-A, the reason why the permutation approach achieves the best performance is that it diminishes the dependency of the event location, and consequently acquires weakly-invariant features over various locations of the events. Moreover, the best median EERs of jittering, scaling, sampling and cropping approaches reach about 11.56%, 10.41%, 8.33% and 10.09%, respectively.

In addition, the EER in raw data gradually decreases and ultimately becomes stable as the dataset size increases; however, the EER in data augmentation initially shows an obvious growth, and then exhibits a slight rise as the dataset size increases. That is, the EERs under data augmentation approaches are still smaller than those without data augmentation. A reasonable explanation is that data will become more and more complex as the dataset size increases, which further illustrates

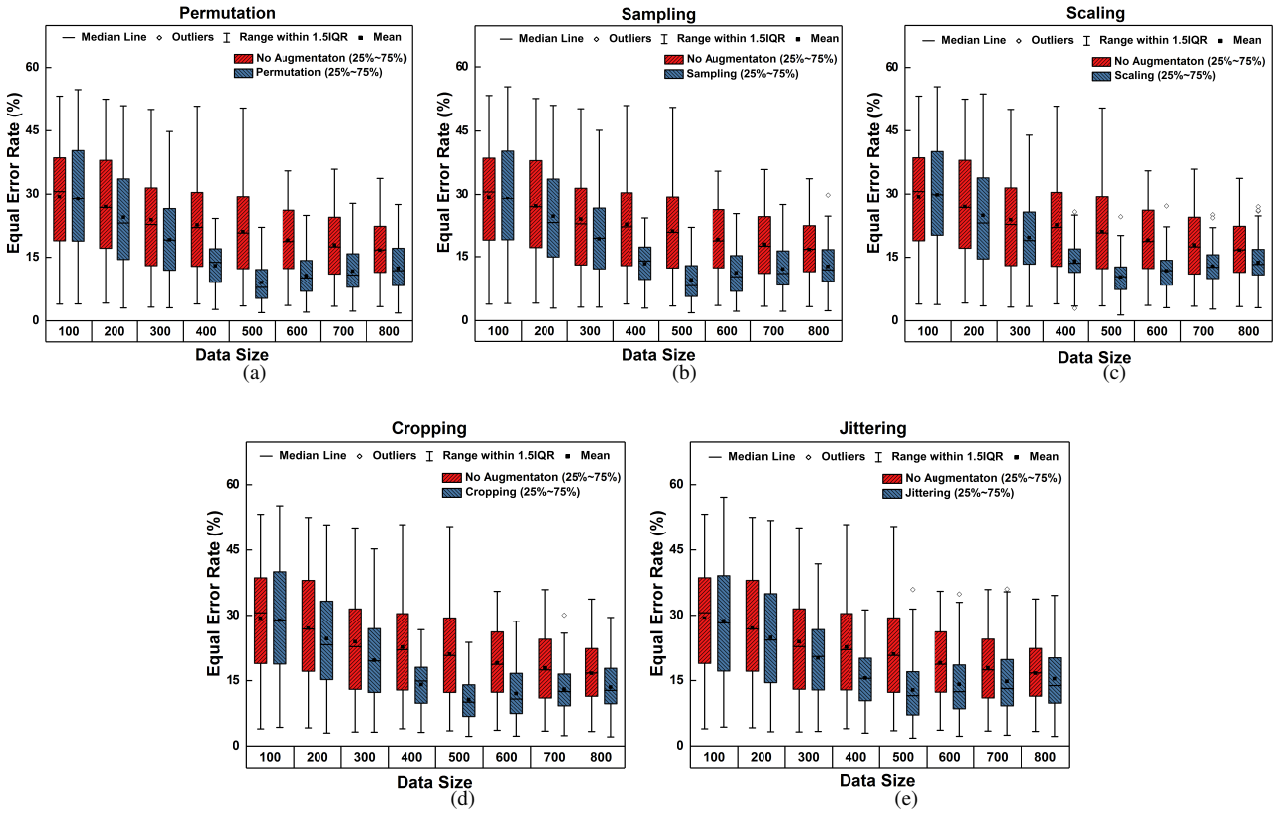

Fig. 4. EER with different data augmentation approaches on different dataset sizes: (a) Permutation. (b) Sampling. (c) Scaling. (d) Cropping. (e) Jittering.

TABLE II
MEDIAN (SD) EER (%) WITH DIFFERENT DATA AUGMENTATION APPROACHES ON DIFFERENT DATASET SIZES.

Approach \ Dataset size	100	200	300	400	500	600	700	800
No Augmentation	30.58 (12.35)	26.82 (13.09)	22.76 (12.25)	22.05 (11.67)	**20.76 (10.54)**	18.72 (8.48)	17.46 (8.17)	16.77 (7.21)
Permutation	28.90 (12.57)	23.12 (12.20)	19.08 (9.18)	13.84 (5.16)	**7.85 (4.85)**	10.14 (5.35)	10.82 (5.57)	11.85 (5.79)
Sampling	28.99 (12.53)	23.08 (12.17)	19.35 (9.19)	13.97 (5.19)	**8.33 (4.82)**	10.27 (5.43)	11.01 (5.57)	11.86 (5.57)
Scaling	29.83 (12.60)	23.14 (12.16)	18.96 (8.76)	13.57 (4.77)	**10.41 (4.13)**	11.83 (4.46)	12.64 (4.77)	13.29 (5.18)
Cropping	28.92 (12.64)	23.19 (12.20)	19.52 (9.38)	14.92 (5.55)	**10.09 (5.21)**	10.80 (5.81)	12.53 (6.04)	12.78 (6.16)
Jittering	28.21 (13.21)	24.79 (12.57)	20.53 (9.45)	15.54 (6.86)	**11.56 (7.21)**	12.47 (7.60)	13.19 (7.76)	13.85 (7.96)

that data augmentation approaches can be applied at certain circumstances with small datasets, such as difficulties in data collection and limited data collection time.

Discussion: Data augmentation technology could increase errors on data, because the raw data collected by sensors could include errors. In fact, as shown in Fig. 4, the average EERs under the five data augmentation approaches obviously decrease comparing with that without data augmentation. That is, the error caused by data augmentation technology introduces less impact on authentication results. The reason could be that data augmentation technology cancels the errors caused by data collection to some extent. Therefore, data augmentation technology can achieve sufficient performance for *SensorAuth* with practical values. In addition, the influence brought by data augmentation can be regarded as a balance between the augmentation technology and the system accuracy. This is because there is a parameter that controls each of the data augmentation approach, such as the segment length for permutation, sample rate for sampling, scale factor for scaling, length of crop sample for cropping, and Gaussian noise for jittering.

D. Accuracy on combinations of different data augmentation approaches

In this section, we investigate the authentication accuracy on combinations of data augmentation approaches that include permutation + sampling, permutation + jittering, scaling + cropping, permutation + sampling + scaling, permutation + sampling + scaling + cropping, and permutation + sampling + scaling + cropping + jittering. These combinations are mainly determined by the performance of each data augmentation approach in Section VI-C.

Fig. 5 and Table III present box plots and medians (with SDs in parentheses) of EERs against the combinations of different data augmentation approaches on different dataset sizes. As depicted in Fig. 5 and Table III, the EERs decrease as the number of the combinations of data augmentation approaches increases; however, there is a slight drop when all the data

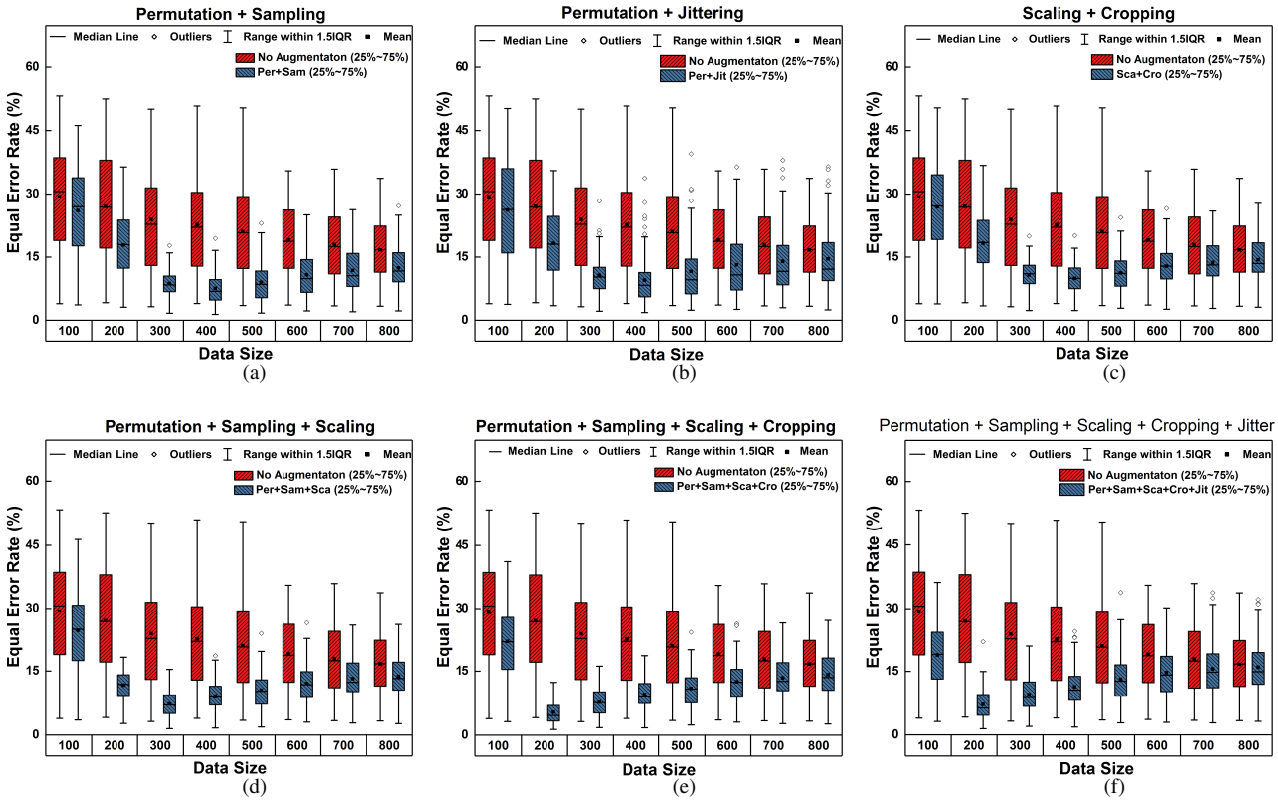

Fig. 5. EER with combinations of different data augmentation approaches on different dataset sizes: (a) Combination of permutation and sampling. (b) Combination of permutation and jittering. (c) Combination of scaling and cropping. (d) Combination of permutation, sampling and scaling. (e) Combination of permutation, sampling, scaling, and cropping. (f) Combination of permutation, sampling, scaling, cropping and jittering.

augmentation approaches are combined. More specifically, the best performance in all approaches is achieved by permutation + sampling + scaling + cropping, where the median EER achieves as low as 4.66%, 12.11% lower than that with no augmentation. The median EERs of permutation + sampling + scaling approach and permutation + sampling + scaling + cropping + jittering approach reach 7.13% and 6.29%, respectively.

In addition, the combination of permutation and sampling exhibits the best performance within two-approach combinations, which achieves a median EER of 6.86%, 9.91% lower than that without data augmentation. The reason is that the permutation diminishes the temporal variability, and its generalization ability is improved in some degree due to a regularization effect by the complex data augmentation. Moreover, the median EERs of permutation + jittering approach and sampling + scaling approach reach about 8.26% and 9.99%, respectively.

We notice that the effectiveness of the combinations of different data augmentation approaches is extraordinarily distinct in small datasets, comparing with that without data augmentation approach.

E. Time efficiency

A practical continuous authentication system not only identifies the legitimate users and impostors with high accuracy, but also authenticates users in time efficiency. In this section, we analyze the time performance of *SensorAuth* at the enrollment and continuous authentication phases, respectively.

1) Time on enrollment phase: In the enrollment phase, *SensorAuth* spends time on data collection for training classifiers and data processing, denoted by T_{train_total}. Then, the total training time can be represented by: $T_{train\_total} = T_{train\_sensor} + T_{train\_processing}$, where T_{train_sensor} is the time that the system needs to collect sensor data (the accelerometer and gyroscope) for training classifiers, and $T_{train\_processing}$ denotes the time that the system needs to process sensor data including data augmentation, feature extraction and training.

In [24], the authors indicate that data collection time of their system is significantly larger than the processing time, and their data collection time T_{train_sensor} = 80 minutes. The training accuracy increases as T_{train_sensor} increases, but user experience quality declines. In our system, T_{train_sensor} = 16 minutes and $T_{train\_processing}$ = 20 seconds, with a 4.66% median EER by applying the data augmentation approach of the combination of permutation, sampling, scaling and cropping.

Therefore, the training time T_{train_total} for *SensorAuth* is roughly 16 minutes. Our training time is approximately 1/5 that of the training time for systems without data augmentation (16.77% of median EER and T_{train_sensor} = 80 minutes [24]).

TABLE III
MEDIAN (SD) EER (%) WITH AUGMENTATION APPROACH COMBINATIONS ON DIFFERENT DATASET SIZES.

Approach \ Dataset size	100	200	300	400	500	600	700	800
Per+Samp	26.92 (10.60)	17.95 (7.49)	8.35 (3.18)	**6.86 (3.85)**	8.47 (4.66)	9.94 (5.36)	10.61 (5.57)	11.72 (5.67)
Per+Jit	26.24 (11.75)	18.06 (7.84)	10.28 (4.56)	**8.26 (5.84)**	9.67 (7.29)	10.80 (7.75)	11.62 (7.97)	12.14 (8.02)
Scal+Crop	27.08 (10.93)	18.44 (7.32)	11.07 (3.37)	**9.99 (3.74)**	11.17 (4.41)	12.87 (4.85)	13.13 (5.11)	13.50 (5.42)
Per+Samp+Scal	24.94 (9.80)	11.86 (3.59)	**7.13 (3.11)**	8.99 (3.71)	10.23 (4.26)	11.75 (4.75)	12.36 (5.15)	13.22 (5.23)
Per+Samp+Scal+Crop	22.02 (8.62)	**4.66 (2.77)**	7.70 (3.17)	9.10 (3.69)	10.76 (4.48)	12.41 (5.02)	12.58 (5.21)	13.5 (5.53)
Per+Samp+Scal+Crop+Jit	19.04 (7.39)	**6.29 (3.48)**	8.74 (3.90)	10.56 (4.87)	12.66 (5.97)	14.15 (6.33)	14.79 (6.47)	14.92 (6.68)

2) Time on continuous authentication phase: In the continuous authentication phase, *SensorAuth* spends time on data collection for authenticating users and user authentication, denoted by T_{auth_total}. Then, the total authentication time can be expressed as: $T_{auth\_total} = T_{auth\_sensor} + T_{auth\_processing}$, where T_{auth_sensor} represents the time that the system needs to collect sensor data for user authentication, and $T_{auth\_processing}$ denotes the time that the system needs to process sensor data including feature extraction and user authentication.

The authentication accuracy increases as T_{auth_sensor} increases, but usability and security of users become worse. In our system, the measured authentication time $T_{auth\_processing}$ is less than 13 milliseconds. As we discussed in VI-B, T_{auth_sensor} corresponds to the time window size 5 seconds. Therefore, the authentication time T_{auth_total} for our system is approximately 5 seconds.

F. Energy consumption

To measure the energy consumption of *SensorAuth* on the smartphone, we consider two comparable testing scenarios that 1) the smartphone is under use and *SensorAuth* is off; 2) the smartphone is under use and *SensorAuth* is running. The testing smartphone is Mi 6 with a 5.15in screen, a 2.45GHz Snapdragon 835 processor, 6GB RAM and a 3350mAh battery. Note that *SensorAuth* is robust to some brands of smartphones, as we conduct experiments on different devices. For each testing scenario, the smartphone is fully charged. During the test, the user uses the smartphone for 20 minutes every other 5 minutes. The total testing time is two hours. For scenario 1 (*SensorAuth* off), the energy consumption is 25.5% and 30.9% for scenario 2 (*SensorAuth* on). Therefore, *SensorAuth* consumes 5.4% more battery power within 100 minutes, which is acceptable for daily usage.

G. Comparison with other classifiers

To investigate the advantage of our one-class SVM, we select two representative classifiers for comparison: kernel ridge regression (KRR) and k-nearest-neighbors (kNN).

1) KRR: The KRR is a regularized least square method for classification and regression [24], [40]. The goal of KRR is to learn a model that assigns the correct label to an unseen testing sample, which can be viewed as learning a function $f : X \rightarrow Y$ that maps each data x to a label y. The parameters for KRR are α and γ for training.

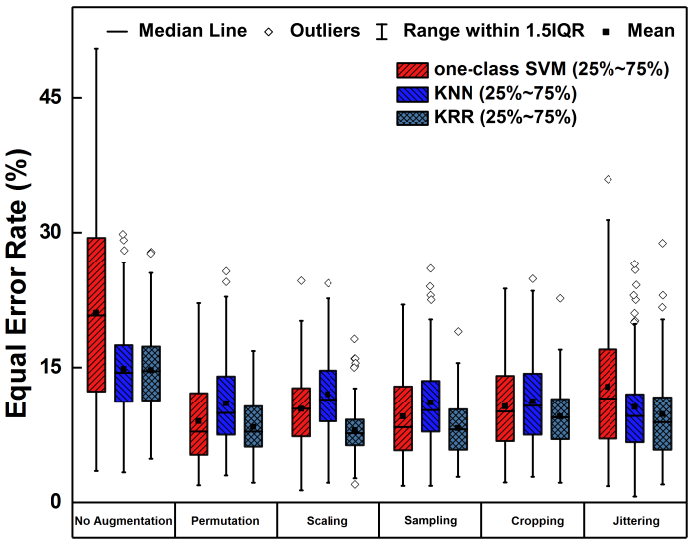

Fig. 6. Comparison with classifiers of KRR and kNN under five data augmentation approaches.

2) kNN: The kNN classifier takes every new observation and locates it in feature space with respect to all training observations. The classifier identifies the k training observations that are closest to the new observation. Then, it selects the label that the majority of the k closest training observations have [41], [42].

We choose data augmentation approaches of permutation, sampling, scaling, cropping, and jittering with dataset size 500 to train our one-class SVM classifier. We use the same training method (see Sec. V-C) to train the two classifiers KRR and kNN. The parameters α and γ for KRR are set in the range of [2,3,4], respectively, and the parameter k for kNN is set in the range of [2,3,4]. We show the average EERs for classifiers KRR and kNN under the five data augmentation approaches in Fig. 6. As depicted in Fig. 6, the one-class SVM shows the highest average EER when there is no data augmentation, but exhibits the lower or lowest EERs when data augmentation approaches apply (except jittering), comparing with the classifiers KRR and kNN. In addition, KRR and kNN are two-class classifiers, which require the training data from both legitimate user and impostors.

H. Comparison with existing authentication approaches

In order to show the difference between the proposed approach and the existing authentication approaches, we conduct a quantitative comparison and a qualitative comparison,

respectively, based on the dataset from [23]. We carefully selected the representative state-of-the-art approaches: Zhu *et al.* [22], Sitová *et al.* [23], Kayacik *et al.* [43], and Lee *et al.* [44]. Note that we choose our approach with data augmentation of sampling and data size 500 for comparison.

1) Quantitative comparison with existing approaches: We first conduct a quantitative comparison with the four representative approaches as shown in Table IV. As illustrated in Table IV, we compare the sensors used, classifiers selected, the average FARs and FRRs of the approaches. More specifically, we select ubiquitously deployed sensors for data collection: the accelerometer and gyroscope, which could save certain energy on smartphone usage, and achieve the average FAR of 7.65% and the FRR of 9.01%, which performs better than others. Note that the table just provides the preliminary comparative results, and it is hard to conclude that a certain approach is better than another. Each approach has its own advantages and disadvantages under different conditions.

2) Qualitative comparison with existing approaches: We then conduct a qualitative comparison with the four representative approaches as shown in Table V. As demonstrated in Table V, we show the sensor sources, training data sources, participants in the experiments, and authentication results of all the approaches. In the table, Zhu *et al.* [22] and Sitová *et al.* [23] make the authentication decision in a short time period, but the accuracies are as low as 71.30% TPR and 13.10% FPR in [22], and 10.05% EER in [23]. Both Kayacik *et al.* [43] and Lee *et al.* [44] consider behavior data from the accelerometer, orientation and magnetometer for authentication and obtain 93.90% accuracy and the authentication time around 20 seconds, and 53.21%~99.49% detection rates in different attack cases and time larger than 122 seconds, respectively. Moreover, both the results are based on a relatively small number of participants with 7 users in [43] and 4 in [44]. In addition, it is not quite realistic in practice that [43] and [44] use data from both legitimate user and impostors to train the authentication models. However, our approach relying on the accelerometer and gyroscope, has less types of sensor data sources, a larger number of participants, a more carefully chosen set of behavioral metrics than the four approaches, but achieves a high authentication accuracy with an EER of 8.33% and a short authentication time of around 5 seconds.

VII. Conclusion

Most existing continuous authentication systems consume lots of time on data collection, in order to achieve a high authentication accuracy. To address the time consumption on data collection, we introduce a novel sensor-based authentication system, *SensorAuth*, for continuous authentication of users based on their behavioral patterns in this paper. *SensorAuth* is composed of data collection, data augmentation, feature extraction, classifier, and authentication. With sensor data collected by the built-in accelerometer and gyroscope on smartphones, our data augmentation module creates additional data by applying the proposed approaches on the collected data during the enrollment phase. The benefits are three-folds: 1) it greatly shortens the time for data collection; 2) it improves the generalization ability of the SVM and the authentication accuracy; 3) it prevents over-fitting and covers unexplored input space. Based on the augmented data, *SensorAuth* extracts and selects sensor-based features in both time and frequency domains for training one-class SVM classifier. With the trained classifier and the testing features, *SensorAuth* authenticates the testing user as a legitimate user or an impostor in the continuous authentication phase. For authentication performance, we evaluate our system in terms of the impact of window size, accuracy on each of and combinations of data augmentation approaches, time efficiency, energy consumption, and comparisons with the representative classifiers and with the existing approaches, respectively. The experimental results show that our system achieves a high accuracy with the lowest median EER of 4.66% and an efficient time of 5 seconds for continuous authentication.

Acknowledgment

This work is supported in part by the National Natural Science Foundation of China (Grant nos. 61672119, 61528206 and 61402380), the Natural Science Foundation of CQ CSTC (Grant no. cstc2015jcyjA40044), and U.S. National Science Foundation (Grant nos. CNS-1253506 (CAREER) and CNS-1618300).

References

[1] K. Wei, M. Dong, K. Ota and K. Xu, "CAMF: Context-aware message forwarding in selfish mobile social networks," *IEEE Trans. Parallel Distrib. Systs.*, vol. 26, no. 8, pp. 2178-2187, Aug. 2015.

[2] M. Dong, X. Liu, Z. Qian, A. Liu and T. Wang, "QoE-ensured price competition model for emerging mobile networks," *IEEE Wireless Commun.*, vol. 22, no. 4, pp. 50-57, Aug. 2015.

[3] Y. Kim, T. Oh, and J. Kim, "Analyzing user awareness of privacy data leak in mobile applications," *Mobile Info. Syst.*, vol. 2, Article ID 369489, 12 pages.

[4] D. Shukla, R. Kumar, A. Serwadda, and V.V. Phoha, "Beware, your hands reveal your secrets!," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, Scottsdale, AZ, USA, Nov. 2014, pp. 904-917.

[5] Data Genetics: PIN analysis. [Online]. Available: http://www.datagenetics.com/blog/september32012/, accessed on Sep. 25, 2017.

[6] Fingerprints are not fit for secure device unlocking, Security research labs. [Online]. Available: https://srlabs.de/bites/spoofing-fingerprints/, accessed on Sep. 25, 2017.

[7] S. Chen, A. Pande, and P. Mohapatra, "Sensor-assisted facial recognition: An enhanced biometric authentication system for smartphones," in *Proc. ACM 12th Int. Conf. Mobile System, Applications, and Services (MobySys)*, Bretton Woods, NH, USA, Jun. 2014, pp. 109-122.

[8] M. Bicego, A. Lagorio, E. Grosso, and M. Tistarelli, "On the Use of SIFT Features for Face Authentication," in *Proc. IEEE Conf. Computer Vision and Pattern Recogntion Workshop (CVPRW)*, New York, NY, USA, USA, Jun. 2006, pp. 1-7.

[9] M.E. Fathy, V.M. Patel, and R. Chellappa, "Face-based active authentication on mobile devices," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP)*, South Brisbane, Quessland, Australia, Apr. 2015, pp. 1687-1691.

[10] U. Mahbub, V.M. Patel, D. Chandra, B. Barbello, and R. Chellappa, "Partial face detection for continuous authentication," in *Proc. IEEE Int. Conf. Iamge Processing*, Phoenix, AZ, USA, Aug. 2016, pp. 2991-2995.

[11] A. Hadid, J. Heikkila, O. Silven, and M. Pietikainen, "Face and eye detection for persion authentication in mobile phones," in *Proc. ACM/IEEE Int. Conf. Distributed Smart Cameras (ICDSC)*, Vienna, Austria, Sep. 2007, pp. 101-108.

[12] N. Shabrina, T. Isshiki, and H. Kunieda, "Fingerprint authentication on touch sensor using Phase-Only Correlation method," in *Proc. 7th Int. Conf. Inf. Communi. Tech. Embedded Systems (IC-ICTES)*, Bangkok, Thailand, Mar. 2016, pp. 1-5.

TABLE IV
QUANTITATIVE COMPARISON WITH EXISTING APPROACHES

Approach	Sensor	Classifier	FAR (SD) (%)	FRR (SD) (%)
Zhu *et al.* [22]	Acc. & Ori. & Mag.	n-gram language model	13.15 (6.21)	15.29 (7.13)
Sitová *et al.* [23]	Acc. & Gyr. & Mag.	Scaled Manhattan	12.93 (6.57)	15.67 (7.24)
Kayacik *et al.* [43]	Acc. & Ori. & Mag. & Light	Temporal & spatia model	16.72 (7.97)	18.79 (9.98)
Lee *et al.* [44]	Acc. & Ori. & Mag.	SVM	8.07 (4.54)	9.97 (4.93)
This work (Sampling, 500)	Acc.& Gyr.	One-class SVM	7.65 (4.59)	9.01 (5.05)

TABLE V
QUALITATIVE COMPARISON WITH EXISTING APPROACHES

Approach	Sensor Source	Training Data Source	Participant	Authentication	
				Result	Time (s)
Zhu *et al.* [22]	Acc. & Ori. & Mag.	Owner	20	TPR: 71.30%, FPR: 13.10%	4.96
Sitová *et al.* [23]	Acc. & Gyr. & Mag. &Touch	Owner	100	EER: 7.16% (walk), 10.05% (sit)	~ 60
Kayacik *et al.* [43]	Acc. & Ori. & Mag. & Light	Owner& Impostors	7	Accuracy: 53.21~99.49%	≥122
Lee *et al.* [44]	Acc. & Ori. & Mag.	Owner& Impostors	4	Accuracy: 93.90%	~ 20
This work (Sampling, 500)	Acc. & Gyr.	Owner	100	EER: 8.33%	~5

[13] L. Hong and A. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Trans. Pattern Ayal. Mach. Intell.*, vol. 20, no. 12, pp. 1295-1307, Dec. 1998.

[14] C. Sanchez-Avila, and R. Sanchez-Reillo, "Two different approaches for iris recognition using Gabor filters and multiscale zero-crossing representation,", *Pattern Recogn.*, vol. 38, no. 2, pp. 231-240, Feb. 2005.

[15] M. Qi, Y. Lu, J. Li, X. Li, and J. Kong, "User-specific iris authentication based on feature selection," in *Proc. Int. Conf. Computer Science and Software Engineering*, Hubei, China, Dec. 2008, pp. 1040-1043.

[16] F. Bimbot, J.-F. Bonastre, C. Fredouille, G. Gravier et. al., "A tutorial on text-independent speaker verification," *EURASIP J. Adv.Signal Process.*, vol. 2004, pp. 430-451, 2004.

[17] I. Martinovic, K. Rasmussen, M. Roeschlin, and G. Tsudik, "Authentication using pulse-response biometrics," *Commun. ACM*, vol. 60, no. 2, pp. 108-115, Feb. 2017.

[18] H. Xu, Y. Zhou, and M. R. Lyu, "Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones," in *Proc. Symp. Usable Privacy Security (SOUPS)*, Menlo Park, CA, USA, Jul. 2014, pp. 187-198.

[19] T. Feng, J. Yang, Z. Yan, E. M. Tapia, and W. Shi, "Tips: Contextaware implicit user identification using touch screen in uncontrolled environments," in *Proc. 15th Workshop Mobile Comput. Syst. Appl. (HotMobile)*, Santa Barbara, CA, USA, Feb. 2014, Art. no. 9, pp. 1-6.

[20] L. Li, X. Zhao, and G. Xue, "Unobservable re-authentication for smartphones," in it Proc. 20th Annu. Netw. Distrib. Syst. Security Symp. (NDSS), San Diego, CA, USA, Feb. 2013, pp. 1-16.

[21] C. Bo, L. Zhang, X.-Y. Li, Q. Huang, and Y. Wang, "SilentSense: Silent user identification via touch and movement behavioral biometrics," in *Proc. 19th Annu. Int. Conf. Mobile Comput. Network (MobiCom)*, Miami, FL, USA, Sep. 2013, pp. 187-190.

[22] J. Zhu, P. Wu, X. Wang, and J. Zhang, "Sensec: Mobile security through passive sensing," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, San Diego, USA, Jan. 2013, pp. 1128-1133.

[23] Z. Sitova, J. sedenka, Q. Yang, et al., "HMOG: New behavioral biometric features for continuous authentication of smartphone users," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 877-892, May 2016.

[24] W.H. Lee, and R. Lee, "Implicit sensor-based authentication of smartphone users with smartwatch," in *Proc. Hardware and Architectural Support for Security and Privacy (HASP)*, Seoul, Republic of Korea, Jun. 2016, Art. No. 9, pp. 1-8.

[25] B. Zou and Y. Li, "Touch-based Smartphone Authentication Using Import Vector Domain Description," in *Proc. 29th Annual IEEE Int. Conf. Application-specific Systems, Architectures and Processors (ASAP)*, Milan, Italy, Jul. 2018, pp. 1-4.

[26] J. Mantyjarvi, M. Lindholm, E. Vildjiounaite, S.-M. Makela, and H. Ailisto, "Identifying users of portable devices from gait pattern with accelerometers," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing (ICASSP)*, Philadelphia, PA, USA, Mar. 2005, pp. II973-II976.

[27] C. Nickel, T. Wirtl, and C. Busch, "Authentication of smartphone users based on the way they walk using k-nn algorithm," in *Proc. 2012 8th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, Piraeus, Greece, Jul. 2012, pp. 16-20.

[28] S. Buthpitiya, Y. Zhang, A.K. Dey, and M. Griss, "n-gram geo-trace modeling," in *Proc. Int. Conf. Pervasive Comput.*, San Francisco, CA, USA, Jun. 2011, pp. 97-114.

[29] I. Goodfellow, Y. Bengio, and A. Courville, "Deep Learning," MIT Press, 2016. http://deeplearningbook.org

[30] L. Manevitz and M. Yousef, "One-class SVMs for document classification," *J. Machine Learning Research*, vol. 2, pp. 139-154, Dec. 2001.

[31] G. Peng, G. Zhou, D. Nguyen, X. Qi, Q. Yang, and S. Wang, "Continuous Authentication with Touch Behavioral Biometrics and Voice on Wearable Glasses," *IEEE Trans. Hum. Mach. Syst.*, vol. 47, no. 3, pp. 404-416, Jun. 2017.

[32] H. Feng, K. Fawaz, and K.G. Shin, "Continuous Authentication for Voice Assistants," *Proc. 23rd Annual Int. Conf. Mobile Computing and Networking (MobiCom)*, Snowbird, UT, USA, Oct. 2017, pp. 343-355.

[33] A. Ben-Hur and J. Weston, "A user's guide to support vector machines," *Data Mining Techn. Life Sci.*, vol. 609, pp. 223-239, 2010.

[34] B. Scholkopf, K. Tsuda, and J.-P. Vert, *Kernel Methods in Computational Biology*, Cambridge, MA, USA: MIT Press, 2004.

[35] R. Begg and J. Kamruzzaman, "A machine learning approach for automated recognition of movement patterns using basic, kinetic and kinematic gait data," *J. Biomechanics*, vol. 38, no. 3, pp. 401-408, 2005.

[36] S.P. Banerjee and D.L. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," *J. Pattern Recognit. Res.*, vol. 7, no. 1, pp. 116-139, 2012.

[37] C. Shen, T. Yu, S. Yuan, Y. Li, and X. Guan, "Performance Analysis of Motion-Sensor Behavior for User Authentication on Smartphones," *Sensors*, vol. 16, no. 345, pp. 1-21, 2016.

[38] A. Mosenia, S. Sur-kolay, A. Raghunathan, and N.K. Jha, "CABA: continuous authentication based on BioAura," *IEEE Trans. Comput.*, vol. 66, no. 5, pp. 759-772, May 2017.

[39] Y. Li, H. Hu, G. Zhou, and S. Deng, "Sensor-based Continuous Authentication Using Cost-Effective Kernel Ridge Regression," *IEEE Access*, vol. 6, pp. 1-12, May 2018.

[40] J. A. Suykens, T. Van Gestel, J. De Brabanter, B. De Moor, J. Vandewalle, J. Suykens, and T. Van Gestel, "Least squares support vector machines," World Scientific Press, 2002.

[41] C. Shen, Y. Li, Y. Chen, X. Guan, and R.A. Maxion, "Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication," *IEEE Trans. Inf. Forensis Security*, vol. 13, no. 1, pp. 48-62, 2018.

[42] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," *IEEE Trans. Inf. Forensis Security*, vol. 8, no. 1, pp. 136-148, 2013.

[43] H. Kayacik, M. Just, L. Baillie, D. Aspinall, and N. Micallef, "Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors," *Proc. 3rd Workshop Mobile Secur. Technol.*, San Jose, CA, USA, May 2014, pp. 1-10.

[44] W. Lee, and R. Lee, "Multi-sensor authentication to improve smartphone security," *Proc. Inf. Syst. Secur., Privacy*, Loire Valley, France, Feb. 2015, pp. 1-11.

Yantao Li received the PhD degree from the College of Computer Science at Chongqing University, China, in December 2012.

He is currently an Associate Professor in the College of Computer and Information Sciences at Southwest University, China, and has been a Postdoctoral Research Associate in the Department of Computer Science at the College of William and Mary, USA, since July 2016. From September 2010 to September 2012, he was a visiting scholar supported by China Scholarship Council working with Professor Gang Zhou at the College of William and Mary. His research area includes wireless communication and networking, sensor networks and ubiquitous computing, and information security.

Dr. Li was a recipient of the Outstanding Ph.D. Thesis Award in Chongqing in 2014, and the Outstanding Master's Thesis Award in Chongqing in 2011. He has served as a TPC member for several international conferences, such as *IEEE BigDataService* 2015-2018 and *ICUIA* 2019, and a Reviewer for several international journals, such as *ACM Transactions on Sensor Networks*, *IEEE Transactions on Systems, Man and Cybernetics: Systems*, *IEEE Internet of Things Journal*, *Elsevier Computer Networks*, and *Springer Multimedia Tools and Applications*.

Hailong Hu received the B.S. degree from the College of Computer and Information Sciences at Southwest University, China, in June 2016.

He is currently pursuing his master's degree in the College of Computer and Information Sciences at Southwest University, China. His research interests include ubiquitous sensing and mobile computing.

Gang Zhou (M'07-SM'13) is an Associate Professor in the Computer Science Department at William & Mary. He served as Graduate Program Director of this department during 2015~2017. He received his Ph.D. degree from the University of Virginia in 2007 under Professor John A. Stankovic. He has published more than 90 papers in the areas of wireless networks, sensor systems, internet of things, smart health, ubiquitous & mobile computing. There are in total 7200 citations of his papers per Google Scholar. He also has 11 papers each of which has been cited more than 200 times since 2004. He serves on the Journal Editorial Board of (1) ACM Transactions on Sensor Networks, (2) IEEE Internet of Things, (3) Elsevier Computer Networks, and (4) Elsevier Smart Health. He is ACM/IEEE CHASE 2018 TPC co-Chair. He served as NSF, NIH, and GENI proposal review panelists multiple times. He received an award for his outstanding service to IEEE Instrumentation and Measurement Society in 2008. He is a recipient of the Best Paper Award of IEEE ICNP 2010. He received NSF CAREER Award in 2013. He received a 2015 Plumeri Award for Faculty Excellence.