IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON CYBER-PHYSICAL-SOCIAL COMPUTING AND NETWORKING

Received April 18, 2018, accepted May 16, 2018, date of publication May 28, 2018, date of current version June 29, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2841347

Sensor-Based Continuous Authentication Using Cost-Effective Kernel Ridge Regression

YANTAO LI[1,2], HAILONG HU[1], GANG ZHOU[2], (Senior Member, IEEE), AND SHAOJIANG DENG[3]

[1]College of Computer and Information Sciences, Southwest University, Chongqing 400715, China
[2]Department of Computer Science, College of William and Mary, Williamsburg, VA 23185, USA
[3]Department of Computer Science, Chongqing University, Chongqing 40044, China

Corresponding author: Yantao Li (yantaoli@foxmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grants 61672119, 61528206, and 61402380, in part by the Natural Science Foundation of CQ CSTC under Grant cstc2015jcyjA40044, and in part by the U.S. National Science Foundation under Grants CNS-1253506 (CAREER) and CNS-1618300.

ABSTRACT People prefer to store important, private, and sensitive information on smartphones for convenient storage and fast access, such as photos and emails. To prevent information leakage and smartphone illegal access, we propose a novel sensor-based continuous authentication system, *SensorCA*, for continuously monitoring users' behavior patterns, by leveraging the accelerometer, gyroscope, and magnetometer ubiquitously built-in smartphones. We are among the first to exploit the data augmentation approach of the rotation, which creates additional data by applying it on the collected raw data and improves the robustness of the proposed system. With the augmented data, *SensorCA* extracts sensor-based features in both time and frequency domains within a time window, then utilizes the kernel ridge regression with truncated Gaussian radial basis function kernel (KRR-TRBF) to train the classifier, and finally authenticates the current user as a legitimate user or an impostor. We evaluate the authentication performance of *SensorCA* in terms of different classifiers including KRR-TRBF, KRR-POLY, and SVM-RBF, and the data augmentation approach rotation on KRR-TRBF6 and SVM-RBF. The experimental results show that under the KRR-TRBF6 classifier, *SensorCA* reaches the lowest median equal error rate of 3.0% with dataset size 8000 and consumes the shortest training time of 0.054 seconds with dataset size 1000.

INDEX TERMS Continuous authentication, rotation, KRR-TRBF, accelerometer, gyroscope and magnetometer, equal error rate (EER).

I. INTRODUCTION

Most of people prefer to store their important, private, and sensitive information in smartphones, because smartphones have become personal computing platforms that provide convenient storage and fast access to stored valuable information, such as photos, emails, online banking and Android pay. However, information leakage and smartphone illegal access become severe concerns for smartphone users since the abuse of leaked personal information in smartphones has caused great adverse effects [1]–[3]. To prevent the critical information in smartphones from leaking or being accessed by other people, use authentication mechanisms have been researched and developed, and some have been deployed on smartphones, such as one-time user authentication mechanisms.

One-time user authentication mechanisms have been widely applied to current smartphone operating systems, such as Android OS and iOS. The most popular and important authentication mechanism is passcode, which is required when users initiate their cell phones. This authentication mechanism can prevent people who have no idea about the passcode from getting access to the phone. Then, when it comes to a smartphone, the user authentication mechanisms evolve to graphical patterns, fingerprints (such as Touch ID) and even face patterns (such as Face ID). However, these one-time authentication mechanisms authenticate users only at the time of initial login. Since they do not perform authentication after login, unauthorized users can easily gain access to unattended smartphones.

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. Within behavioral biometrics based approaches, we briefly categorize these approaches into sensor-based smartphone continuous authentication, touchscreen-based smartphone continuous authentication, and continuous authentication with wearable devices. More specifically, continuous authentication based on sensor data has been significantly investigated [4]–[14]. Continuous authentication based on touch gestures on smartphone screens has been deeply researched [15]–[24]. Continuous authentication based on contexts has been well developed [25]–[29]. However, most of the above studies highly rely on the originally collected data, which requires more time on data collection. We are different in that we are among the first to apply the data augmentation approach of the rotation to the raw data, which creates additional data and improves the robustness of the system.

In this paper, we propose a novel sensor-based continuous authentication system, *SensorCA*, for continuously monitoring users' behavior patterns. More specifically, *SensorCA* consists of modules of the data collection, data rotation, feature extraction, classifier, and authentication. The operation of *SensorCA* includes the enrollment phase for data and classifier training (including Data Rotation, Feature Extraction, and Classifier training) and the continuous authentication phase for testing (involving Feature Extraction, Classifier testing, and Authentication). Data collection captures users' behavioral patterns by leveraging three ubiquitously built-in sensors of the accelerometer, gyroscope and magnetometer on smartphones. We are among the first to apply the data rotation augmentation approach on a continuous authentication system, which creates additional data based on the raw data from data collection and improves the robustness of the system. Then, 135 sensor-based features are extracted in both time and frequency domains within a time window on the augmented data. From these features, the most discriminable ones are selected by the minimum-Redundancy Maximum-Relevance (mRMR), and with the selected features, we use the kernel ridge regression with truncated Gaussian radial basis function kernel (KRR-TRBF) to train the classifier in the enrollment phase. With the trained classifier and testing features, *SensorCA* classifies the current user as a legitimate user or an impostor in the continuous authentication phase. We evaluate the authentication performance of *SensorCA* in terms of different classifiers including KRR-TRBF, KRR-POLY and SVM-RBF, and the data augmentation approach rotation on KRR-TRBF6 and SVM-RBF, respectively. For the different classifiers, we evaluate the EER of KRR-POLY and KRR-TRBF across various degrees, EER comparison between KRR-TRBF and SVM-RBF, training time for KRR-TRBF and KRR-POLY with various degrees, training time comparison between KRR-TRBF and SVM-RBF. Based on the rotation, we evaluate the EER of KRR-POLY and KRR-TRBF across various degrees, EER comparison between KRR-TRBF and SVM-RBF, training time for KRR-TRBF and KRR-POLY with various degrees, training time comparison between KRR-TRBF and SVM-RBF. The experimental results show that under the KRR-TRBF6 classifier, *SensorCA* reaches the lowest median equal error rate (EER) of 3.0% with dataset size 8000 and costs the shortest training time of 0.054 seconds with dataset size 1000.

The main contributions of this work are summarized as follows:

- We design *SensorCA*, a novel sensor-based authentication system that continuously monitors users' behavior patterns using the accelerometer, gyroscope, and magnetometer in smartphones. *SensorCA* is composed of the data collection, data rotation, feature extraction, classifier, and authentication.
- We are among the first to exploit the data augmentation approach of the rotation, which creates additional data by applying it on the collected raw data and improves the robustness of *SensorCA*. We explore the KRR-TRBF to train the classifier of *SensorCA* in the enrollment phase and the trained classifier classifies the current user as a legitimate user or an impostor in the continuous authentication phase.
- We evaluate the authentication performance of *SensorCA* in terms of different classifiers including KRR-TRBF, KRR-POLY and SVM-RBF, and the data augmentation approach rotation on KRR-TRBF6 and SVM-RBF. The experimental results show that under the KRR-TRBF6 classifier, *SensorCA* reaches the lowest median EER of 3.0% with dataset size 8000 and consumes the shortest training time of 0.054 seconds with dataset size 1000.

The remainder of this paper is organized as follows: Section II reviews the background and the existing literature on the behavioral biometrics based continuous authentication. We present the detailed *SensorCA* architecture consisting of data collection, data rotation, feature extraction, classifier, and authentication in Section III. In Section IV, we elaborate the learning algorithm of KRR-TRBF. Then, we describe our experiment setup in terms of dataset, parameter selection, classifier training and testing, and metrics in Section V. In Section VI, we evaluate the authentication performance of *SensorCA* on different classifiers and on the data augmentation approach rotation, and conclude this work in Section VII.

II. BACKGROUND AND RELATED WORK

User authentication mechanisms can be broadly organized into three principles: (i) ''what you know'' approaches (such as PINs and graphical patterns), (ii) ''what you have'' approaches (such as cards, tokens, and keys), and (iii) ''what you are'' approaches (such as biometric characteristics [15], [30]). The former two principles are susceptible to guessing and device theft while biometric-based approaches utilize users' personal traits that are hard to reproduce or mimic. Within the ''what you are'' category, there are two classes of biometrics-based approaches: physiological biometrics (such as fingerprints [31] and voices [28]) and behavioral biometrics (such as touch gestures [29], [32] and gait [4], [5]). The former class that relies on static

physical attributes has some defects. These physiological characteristics are prone to duplicate (fingerprints are easily recreated in plastic [6]), are easily distorted or changed (scars or burns can change the fingerprints [33]), and need special hardware supports (accelerometer chip and Bluetooth transmitter are applied to the wearable [28]). In addition, it requires user direct participation in the process of the authentication. Behavioral biometrics based approaches aim at identifying invariant features of human behaviors during different activities, which show a promising research area and have been widely investigated [34]. Within behavioral biometrics based approaches, we briefly review previous studies on smartphone continuous authentication based on sensors, touchscreens, and wearable devices, respectively.

A. SENSOR-BASED SMARTHPONE CONTINUOUS AUTHENTICATION

Continuous authentication based on sensor data has been significantly investigated. In [4], Mantyjarvi *et al.* present an identification method for personal devices using the acceleration signal characteristics produced by walking. Nickel *et al.* [5] propose an accelerometer-based biometric gait recognition to authenticate users on their mobile devices by extracting several features from the gait data. In [6], Tanviruzzaman *et al.* provide an adaptive solution to secure the authentication of cellular phone users by using gait and location tracks. Buthpitiya *et al.* [7] present an n-gram based model for learning a user's movement pattern using the GPS sensor to detect abnormal activities by analyzing historical GPS tracks. In [8], Conti *et al.* propose a biometric measure to authenticate the movement of the user when answering (or placing) a phone call, which leverages commercial features of the accelerometer and orientation sensors in smartphones. The authors of [10] present a probabilistic approach to model user's gesture patterns using passive sensory data from the accelerometers, gyroscopes and magnetometers. In [11], Lee and Lee propose a multi-sensors-based system to achieve continuous and implicit authentication by leveraging sensor data collected by the accelerometer, orientation sensor and magnetometer on smartphones. Yang *et al.* [12] provide a hand waving biometric-based authentication to lock or unlock the smartphones by utilizing the accelerometer. In [13], Centeno *et al.* propose an approach based on a deep learning autoencoder, relying on accelerometer data. Chen *et al.* [14] propose a framework and performance analysis of using onboard-sensor behavior for continuous user authentication on smartphones, which can implicitly and continuously verifies the presence of a smartphone user.

B. TOUCHSCREEN-BASED SMARTPHONE CONTINUOUS AUTHENTICATION

Continuous authentication based on touch gestures on smartphone screens has been deeply researched. Chen *et al.* [15] propose a continuous authentication system with behavioral biometrics from six types of touch gestures (single-tap, swipe forward, swipe backward, swipe down, two-finger swipe forward, and two-finger swipe backward). In [17], Feng *et al.* introduce a finger gesture authentication system using touchscreen by extracting touch data from touchscreen equipped smartphones. Trojahn and Ortmeier [18] develop a mixture of a keystroke-based and a handwriting-based authentication method using capacitive displays. In [20], Frank *et al.* propose a foundational work for continuous authentication schemes that rely on the data source of touchscreen input. Li *et al.* [21] provide a re-authentication system that utilizes the finger movement as a biometric characteristic to authenticate a smartphone user. Xu *et al.* [22] present a continuous and passive authentication mechanism based on a user's touch operations on the touchscreen. In [23], Zheng *et al.* propose a non-intrusive user verification mechanism to substantiate whether an authenticating user is the true owner of the smartphone or an impostor who happens to know the passcode. Zhang *et al.* [24] present an approach for active user authentication using screen touch gestures by building linear and kernelized dictionaries based on sparse representations and associated classifiers.

C. CONTINUOUS AUTHENTICATION WITH WEARABLE DEVICES

Continuous authentication based on contexts has been well developed. In [25], Mare *et al.* propose a zero-effort bilateral recurring authentication with the user wearing a bracelet on the wrist. Feng *et al.* [28] provide a continuous authentication system for voice assistants, consisting of the wearable device and the voice assistant extension, where the wearable device is responsible for collecting and uploading the accelerometer data. In [29] and [26], the authors design an implicit authentication system by combining a user's sensor information recorded in the smartphone and the wearable device smartwatch, which continuously monitors the user's behavior and authenticates the user in an stealthy manner. Song *et al.* [27] present a secure and trustworthy continuous user authentication scheme via non-contact cardiac motion sensing based on the smart DC-coupled continuous-wave radar.

III. SYSTEM DESIGN

In this section, we elaborate the architecture of our continuous authentication system, *SensorCA*, as depicted in Fig. 1. As illustrated in Fig. 1, *SensorCA* comprises five modules: Data Collection, Data Rotation, Feature Extraction, Classifier, and Authentication. To learn and classify users' behavioral patterns, *SensorCA* operates in two phases: the enrollment phase (including Data Rotation, Feature Extraction, and Classifier training) and the continuous authentication phase (involving Feature Extraction, Classifier testing, and Authentication). In this way, *SensorCA* learns a profile of the legitimate user in the enrollment phase and then authenticates users in the continuous authentication phase.

A. DATA COLLECTION

Data Collection module collects all users' sensor data from the accelerometer, gyroscope, and magnetometer

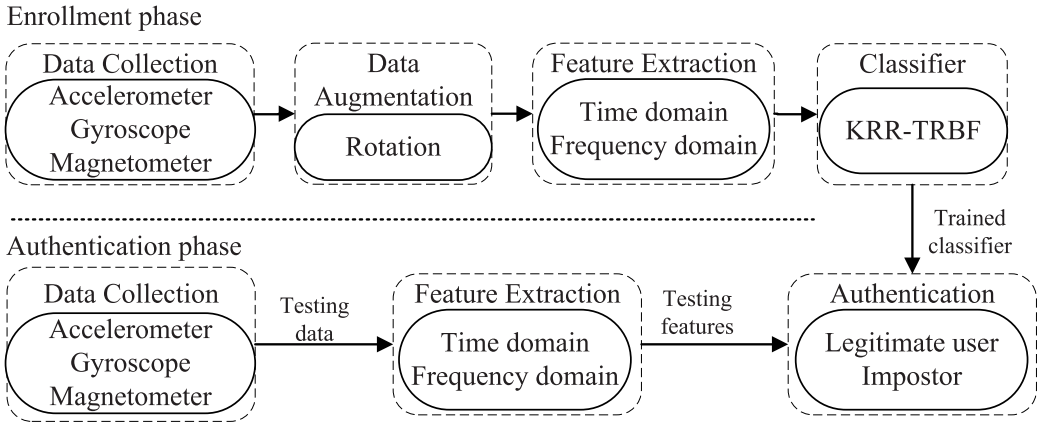


FIGURE 1. Architecture of *SensorCA*.

on smartphones. When a user starts using the smartphone, the accelerometer records larger motion patterns of the user such as how to move the arms or how to walk, the gyroscope records fine-grained motions of the user such as how to hold the smartphone, and the magnetometer records the ambient geomagnetic filed of the user. The three sensors do not require root permissions when requested by mobile applications, which makes them useful for background monitoring. In the system, the Data Collection module captures every subtle movements during the user's operation on the smartphone, and records the instantaneous readings of the three sensors when the screen is on. Since the raw readings may contain abnormal values or missing values, the module processes outliers and fills missing values. More specifically, the values of a time window from the first to the fourth quartiles are removed in the training or testing data, and the missing values will be replaced by the latest previous values. Then, the collected data are either stored in a protected buffer for data rotation in the enrollment phase or used for Feature Extraction in the authentication phase.

B. DATA ROTATION

Users may prefer their own ways holding the smartphones, and the sensors may generate non-diverse data for each user. By simulating different smartphone holding gestures for users, we apply rotation to the collected raw data to achieve data augmentation.

In our Data Collection, the collected data are stored in a format of a matrix in smartphone buffers, and the readings of the accelerometer, gyroscope and magnetometer are saved as $n \times 3$ matrices M_a and M_g, respectively:

$$M_a = \begin{bmatrix} x_1^a & y_1^a & z_1^a \\ x_2^a & y_2^a & z_2^a \\ \vdots & \vdots & \vdots \\ x_n^a & y_n^a & z_n^a \end{bmatrix}$$

$$M_g = \begin{bmatrix} x_1^g & y_1^g & z_1^g \\ x_2^g & y_2^g & z_2^g \\ \vdots & \vdots & \vdots \\ x_n^g & y_n^g & z_n^g \end{bmatrix}$$

$$M_m = \begin{bmatrix} x_1^m & y_1^m & z_1^m \\ x_2^m & y_2^m & z_2^m \\ \vdots & \vdots & \vdots \\ x_n^m & y_n^m & z_n^m \end{bmatrix}$$

We use rotation matrices to perform a rotation in Euclidean space. A basic rotation is a rotation about one of the axes of a coordinate system. In three dimensions, there are three basic rotation matrices as illustrated as $R_x(\alpha)$, $R_y(\beta)$ and $R_z(\gamma)$, where $R_x(\alpha)$ can rotate our matrix (M_a or M_g) by an angle α about the x-axis, $R_y(\beta)$ can rotate our matrices by an angle β about the y-axis, and $R_z(\gamma)$ can rotate our matrices by an angle γ about the z-axis, respectively.

$$R_x(\alpha) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{bmatrix}$$

$$R_y(\beta) = \begin{bmatrix} \cos\beta & 0 & \sin\beta \\ 0 & 1 & 0 \\ -\sin\beta & 0 & \cos\beta \end{bmatrix}$$

$$R_z(\gamma) = \begin{bmatrix} \cos\gamma & -\sin\gamma & 0 \\ \sin\gamma & \cos\gamma & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

We use matrix multiplication to realize rotations in three dimensions, as shown in Eq. (1):

$$R = R_z(\gamma) \times R_y(\beta) \times R_x(\alpha) \tag{1}$$

where R is a 3×3 rotation matrix.

We take accelerometer matrix M_a as an instance to illustrate the data augmentation by rotation. By premultipling M_a with rotation matrix R, we generate the augmented data

matrix M_a^{rt}, as shown in Eq. (2):

$$M_a^{rt} = R \times M_a^T \tag{2}$$

where "T" indicates the transpose of matrix M_a, and M_a^{rt} is a $3 \times n$ data matrix.

Then, after data augmentation by rotation, we obtain the new data matrix of accelerometer readings, as shown in Eq. (3)

$$M_a^{art} = \begin{bmatrix} M_a \\ (M_a^{rt})^T \end{bmatrix} \tag{3}$$

where M_a^{art} is a $2n \times 3$ data matrix with double data amount.

C. FEATURE EXTRACTION

The Feature Extraction module is composed of feature construction and feature selection. We first propose sensor-based features extracted in both time and frequency domains, and then describe how to conduct feature selection.

1) FEATURE CONSTRUCTION

We first segment the signals of the sensor data into a series of discrete time windows. In each time window, we extract sensor-based features from the time domain and the frequency domain, respectively. Let x, y, and z be the three-axis sensor readings of the accelerometer, gyroscope or magnetometer. We extract our features sequentially based on sensor readings from each axis of each sensor.

Time domain features depict the users' motion patterns with meaningful statistics during the operation of the smartphones. In the time domain, we extract ten statistical features for each axis of each sensor in a time window, involving the mean, standard deviation, maximum, minimum, range, kurtosis, skewness, and 25%, 50%, 75% quartiles of sensor readings. In particular, the range of the sensor readings in a time window indicates the difference between the maximum sensor reading value and the minimum sensor reading value, which can differentiate users with different range of the sensor readings. The kurtosis feature represents the width of peak for sensor readings in a time window and the skewness feature indicates the orientation of peak for sensor readings.

Frequency domain features characterize 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, including energy, entropy, P1, P2f, P2.

Combining the features from the time domain and the frequency domain, we have 135 sensor-based features (3 sensors $\times$ 3 axes $\times$ 15 features) in total. In order to save space, we only list the 15 features based on one axis of the sensor readings for one sensor data (accelerometer, gyroscope or magnetometer) in Table 1.

TABLE 1. Sensor-based features.

Aspect	Feature	Explanation
Time domain	Mean	Mean value of one-axis sensor readings
	Standard deviation	Standard deviation of one-axis sensor readings
	Maximum	Maximum value of one-axis sensor readings
	Minimum	Minimum value of one-axis sensor readings
	Range	Difference between the maximum value and minimum value of one-axis sensor readings
	Kurtosis	Width of peak of one-axis sensor readings
	Skewness	Orientation of peak of one-axis sensor readings
	Quartiles	25%, 50%, 75% quartiles of one-axis sensor readings
Frequency domain	Energy	Intensity of one-axis sensor readings
	Entropy	Dispersion of spectral distribution of one-axis sensor readings
	P1	Amplitude of the first highest peak of one-axis sensor readings
	P2f	Frequency of the second highest peak of one-axis sensor readings
	P2	Amplitude of the second highest peak of one-axis sensor readings

2) FEATURE SELECTION

Given the extracted 135 features based on the sensor readings of the accelerometer, gyroscope, and magnetometer, Feature Extraction then conducts feature selection to remove poor features and selects features with high discriminability. We exploit minimum-Redundancy Maximum-Relevance (mRMR) to do feature selection in the enrollment phase. The ultimate goal of mRMR is to maximize the correlation between feature subsets and category tags while minimizing the redundancy of the feature subsets. In our experiment, we conduct mRMR by FEAST, which provides implementations of common mutual information based filter feature selection algorithms.

D. CLASSIFIER

After features are extracted and selected, they are passed to Classifier training and testing. We apply kernel ridge regression with truncated Gaussian radial basis function kernel (KRR-TRBF) for classification, since it offers computational advantages over the traditional Support Vector Machine with Gaussian radial basis function (SVM-RBF) kernel, while retains similar, even lower error-rate performances. In the enrollment phase, the classifier is established by using training feature vectors. 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. The learning algorithm KRR-TRBF is detailed in Section IV.

E. AUTHENTICATION

Based on the testing feature vectors and the trained KRR-TRBF classifier, Authentication classifies the current user as a legitimate user or an impostor. If the current user is classified as an impostor, *SensorCA* will require initial login inputs; otherwise, it will authenticate the user continuously.

IV. LEARNING ALGORITHM

In this section, we first describe the kernel ridge regression with truncated Gaussian radial basis function kernel (KRR-TRBF) in terms of KRR and TRBF kernel

that is a simple Taylor expansion approximation of Gaussian radial basis function (RBF). Then, we introduce a comparable classifier Support Vector Machine with Gaussian radial basis function (SVM-RBF).

In this work, we consider the authentication task as a two-class classification problem (a legitimate user and an impostor). Therefore, the positive (the legitimate user) class comprises of samples from the owner, while the negative (the impostor) class is composed of samples from all users other than the owner.

Given a set of labeled training data $\mathcal{D} = \{(\mathbf{x_1}, y_1), (\mathbf{x_2}, y_2), \ldots, (\mathbf{x_i}, y_i), \ldots, (\mathbf{x_n}, y_n)\}$ where n is the number of samples, $\mathbf{x_i} \in \mathbb{R}^P$ is the feature vector and $y_i \in \{\pm 1\}$ is the label, indicating that the sample either belongs to the positive class ($y_i = +1$) or negative class ($y_i = -1$).

A. KRR-TRBF

Kernel ridge regression is to learn a model that assigns the correct label to an unseen testing sample. The optimal classifier can be obtained analytically according to Eq. (4):

$$\omega^* = \arg\min_{\omega \in \mathbb{R}^d} \rho \|\omega\|^2 + \sum_{i=1}^{n} \left(\omega^T \mathbf{x_i} - y_i\right)^2 \tag{4}$$

where N is the data size, x_k^P is the selected features, and P is the dimension of the feature vector. ρ is a penalty parameter and "$\|.\|$" is the Euclidian distance measure. Let $\vec{\phi}(x_i)$ denote a kernel function, which maps the original data x_i into a higher-dimensional (J) space. We define $\Phi = [\vec{\phi}(x_1), \vec{\phi}(x_2) \ldots \vec{\phi}(x_N)]$ and $K = \Phi^T \Phi$. The objective function has an analytic optimal solution as shown in Eq. (5):

$$\omega^* = \Phi \left[K + \rho I_N\right]^{-1} y \tag{5}$$

Kernel methods are able to nonlinearly transform patterns into some high-dimensional feature space, where various learning methods apply. The high-dimensional feature space and the nonlinear mapping are determined by a kernel function that describes the similarity between pairwise samples, where the kernel function should satisfy Mercer condition. By Mercer's Theorem [35], a kernel function that satisfies Mercer condition can be represented as the inner product in a kernel-induced feature space $\mathcal{H}$: $k(\mathbf{x}, \mathbf{x}') \leq \langle \phi(\mathbf{x}), \phi(\mathbf{x}') \rangle_{\mathcal{H}}$, where $\phi(\mathbf{x})$ is some fixed mapping to $\mathcal{H}$. The Gaussian RBF kernel can be expressed as in Eq. (6):

$$k_{RBF}(\mathbf{x}, \mathbf{x}') = \exp\left(-\frac{\left\|\mathbf{x} - \mathbf{x}'\right\|^2}{2\sigma^2}\right) \tag{6}$$

and the ploynomial kernel can be written as in Eq. (7):

$$k_{POLY\_P}(\mathbf{x}, \mathbf{x}') = \left(1 + \frac{\mathbf{x^T x}'}{\sigma^2}\right)^P \tag{7}$$

In our experiment, we denote the pth order polynomial kernel as $POLY\_P$, and the basis function is shown as in Eq. (8):

$$\phi^{(j)}(\mathbf{x}) = \sqrt{\frac{p!}{(p-\ell)!}} \prod_{m=1}^{M} \frac{1}{\sqrt{d_m!}} \left(\frac{x^{(m)}}{\sigma}\right)^{d_m}$$
$$0 \leq \ell \leq p, \quad \ell = d_1 + \ldots + d_M \tag{8}$$

There are $J = J^{(p)} = \frac{(M+p)!}{M!p!}$ different combinations.

Based on RBF, the TRBF kernel [36] can be defined as in Eq. (9):

$$\begin{aligned} k_{TRBF}(\mathbf{x}, \mathbf{x}') &= \exp\left(-\frac{\|\mathbf{x}\|^2}{2\sigma^2}\right)\left(\sum_{\ell=1}^{p} \frac{1}{\ell!}\left(\frac{\mathbf{x^T x}'}{\sigma^2}\right)\right)\exp\left(-\frac{\|\mathbf{x}\|^2}{2\sigma^2}\right) \\ &= \phi(\mathbf{x})^{\mathbf{T}} \phi(\mathbf{x}') \end{aligned} \tag{9}$$

where each basis function has the form as shown in Eq. (10):

$$\phi^{(j)}\mathbf{x} = exp\left(-\frac{\|\mathbf{x}\|^2}{2\sigma^2}\right) \prod_{m=1}^{M} \frac{1}{\sqrt{d_m!}} \left(\frac{x^{(m)}}{\sigma}\right)^{d_m}$$
$$0 \leq d_1 + \ldots + d_M \leq p \tag{10}$$

The tradeoff between accuracy performance and computation efficiency highly depends on order p and its intrinsic dimension $J = J(p)$, which is identical to that of polynomial kernels. Note that TRBF is simply a Taylor expansion approximation of RBF [36]–[40].

B. SVM-RBF

For comparison, we select another popular classifier Support Vector Machine with Gaussian radial basis function (SVM-RBF), to train the user's model. The SVM finds a hyperplane in the training data matrix to separate the positive (the legitimate user) class and the negative (the imposter) class such that the margin is maximized [41]–[43]. The regularized empirical risk function can be written as:

$$\underset{\omega, b, \xi \in \mathbb{R}^n}{\text{minimize}} \left\{\frac{\rho}{2}\|\omega\|^2 + \sum_{i=1}^{n} \xi_i\right\}$$
$$\text{subject to } y_i \varepsilon + \xi \geq 0.$$

where $\varepsilon_i \equiv \omega^T \phi(x_i) + b - y_i$, and $\xi \geq 0$

V. EXPERIMENTS

In this section, we first describe the dataset used by *SensorCA*. Then, we discuss how to select parameters, and how to train the classifier. Finally, we introduce the metrics for evaluating the proposed *SensorCA*.

A. DATASET

To demonstrate the effectiveness of the proposed system, we exploit sensor data from a public multi-modal dataset [44]. The dataset included sensor readings of the accelerometer, gyroscope and magnetometer with the sampling rate of $100Hz$ and the screen touching data collected by an Android-based software system from 100 subjects typing on a virtual keyboard (53 male, and 47 female) on ten

Samsung Galaxy S4 smartphones. Each subject devoted to approximately 2 to 6 hours of behavior traits. The data were recorded and stored on smartphones according to three usage scenarios involving document reading, text production, and navigation. In this work, we only exploit the sensor data of the accelerometer, gyroscope and magnetometer from 98 subjects to perform user authentication, since the data of 2 subjects were extremely abnormal. Specifically, among all the 98 users, to ensure that every user provides the same amount of data, we select the first 100 minutes of sensor data for each user with an approximately 1-second time window size (exactly 1.28 seconds). According to the sensor sampling rate of 100Hz, a 1-second time window should have 100 samples (exactly 128 samples). To create inputs with the same length and calculate the frequency domain feature conveniently, we use 128 samples for each time window in our experiments.

B. PARAMETER SELECTION

We use the five-fold cross validation on training data to select the appropriate parameter values for different classifiers. More specifically, for the SVM-RBF classifier, we conduct a grid search to find the parameters σ and ρ with the best performance, by searching through [3, 4, 5, 6]. For the KRR-TRBF and KRR-POLY classifiers, we use the same grid search to find the parameters σ and ρ with the best performance, where we search through $[2^{-19}, 2^{-18}, 2^{-17}, 2^{-16}]$ for σ, and [2, 3, 4, 5] for ρ. Note that the grid search scope is very small, because we first conduct a coarse-grained search in a relatively large range, and then perform a fine-grained grid search after a suitable range of parameters is obtained.

C. TRAINING AND TESTING

We first specify one of the 98 users as the legitimate user and the remaining 97 users as impostors; Thus, we have positive feature samples from one legitimate user and negative feature samples from 97 impostors. To keep samples balanced, we randomly select the same number of samples from 97 impostors as the legitimate user. Based on these samples, we use 90% of the total amount of the data to train the classifiers in the enrollment phase and 10% of the data to test the classifiers in the authentication phase. We then repeat the above procedure until each of the subjects is designated as a legitimate user once. We also utilize five-fold cross validation to tune the parameters of the classifiers. Note that 10% of the data are approximately 800 samples in the experiments (without data augmentation).

D. METRICS

We explore three representative metrics FAR, FRR, and ERR to quantify the accuracy of authentication performance of *SensorCA*:

- FAR (False Acceptance Rate): the ratio of the number of false acceptance of 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 [45].

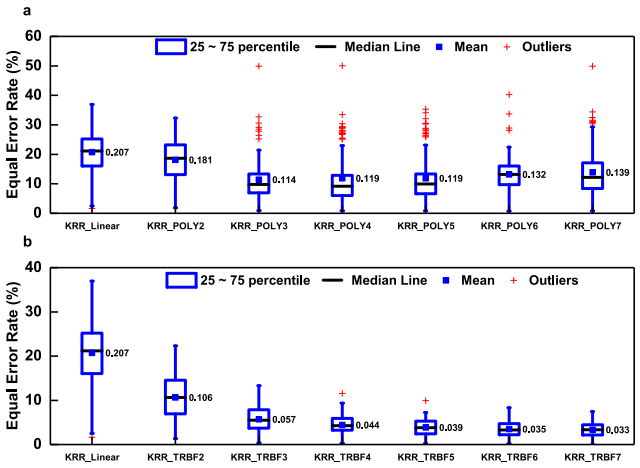


FIGURE 2. EER of KRR-POLY and KRR-TRBF across different degrees.

- FRR (False Rejection Rate): the ratio of the number of false rejection of 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 [46], [47].
- EER (Equal Error Rate): the point where FAR equals to FRR. The FAR or FRR cannot provide the whole picture, because there is a trade-off between them. We use the EER as a metric to evaluate the accuracy of *SensorCA* [48]–[50].

VI. EXPERIMENTAL RESULTS

In this section, we present the performance evaluation of *SensorCA* in terms of the accuracy on different classifiers including the KRR-TRBF, KRR-POLY and SVM-RBF, and the accuracy with the data augmentation approach of the rotation on the KRR-TRBF6 and SVM-RBF, respectively.

A. EVALUATION ON DIFFERENT CLASSIFIERS

In this section, we evaluate the performance of *SensorCA* on different classifiers, in terms of the EER of KRR-POLY and KRR-TRBF across various degrees, EER comparison between KRR-TRBF and SVM-RBF, training time for KRR-TRBF and KRR-POLY with various degrees, training time comparison between KRR-TRBF and SVM-RBF.

1) EER OF KRR-POLY AND KRR-TRBF ACROSS VARIOUS DEGREES

Fig. 2 shows the box plots of the EER of KRR-POLY and KRR-TRBF across different degrees. As illustrated in Fig. 2a, the EER decreases from POLY2 to PLOY3 and increases from POLY4. The reason is that it may be over-fitting in POLY kernel function with larger degrees. In Fig. 2b, the EER gradually decreases with the increase of TRBF degrees and becomes saturated. This trend shows that the authentication accuracy comes close to an optimum. Table 2 lists the EER, mean (with standard deviations (SDs) in parentheses) and median value of the two classifiers KRR-POLY and KRR-TRBF across different degrees. From Table 2, the best

TABLE 2. EER of KRR-POLY and KRR-TRBF across different degrees.

Classifier	EER (%)	
	Mean (SD)	Median
KRR-Linear	20.7 (7.2)	21.2
KRR-POLY2	18.1 (6.3)	18.6
KRR-POLY3	11.4 (7.6)	9.8
KRR-POLY4	11.9 (9.2)	9.2
KRR-POLY5	11.9 (8.2)	9.9
KRR-POLY6	13.2 (6.4)	13.2
KRR-POLY7	13.9 (8.2)	12.2
KRR-TRBF2	10.6 (4.8)	10.7
KRR-TRBF3	5.7 (2.7)	5.5
KRR-TRBF4	4.4 (2.1)	4.3
KRR-TRBF5	3.9 (1.9)	3.8
KRR-TRBF6	3.5 (1.7)	3.3
KRR-TRBF7	3.3 (1.6)	3.3
SVM-RBF	3.7 (01.9)	3.7

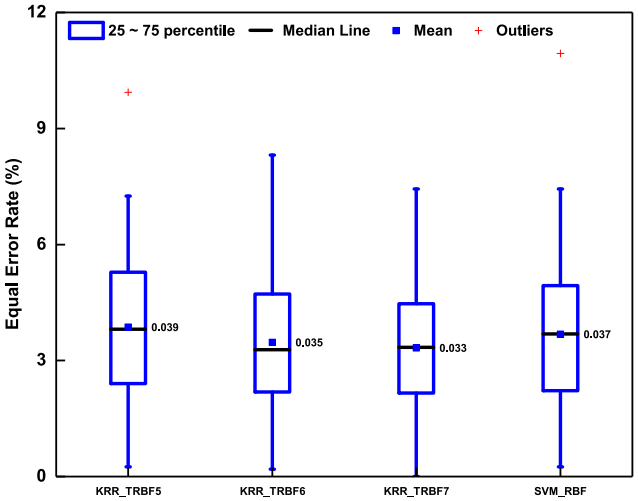


FIGURE 3. EER comparison between the classifiers KRR and SVM.

mean EER in various degrees of KRR-POLY is greater than 11% while the worst mean EER in various degrees of KRR-TRBF is less than 11%, which indicates that KRR-TRBF can be a promising authentication classifier in continuous authentication area. Moreover, the KRR-TRBF7 classifier shows the best performance (3.3% mean EER) among all the classifiers.

2) EER COMPARISON BETWEEN THE KRR AND SVM

Fig. 3 illustrates the box plots of EER between KRR with kernels of TRBF5, TRBF6, and TRBF7, and SVM-RBF. As shown in Fig. 3, KRR-TRBF6 (3.5% mean EER) and KRR-TRBF7 (3.3% mean EER) shows better accuracy than SVM-RBF (3.7% mean EER).

3) TRAINING TIME FOR THE KRR-TRBF AND KRR-POLY WITH VARIOUS DEGREES

We describe how to calculate the training time for different classifiers: let $t_{train}^{(i)}$ be the time required to train the samples from legitimate user i, and then the average training time can be expressed as: $T_{train\_avg} = \frac{1}{N}\sum_{i=1}^{N} t_{train}^{(i)}$, where N indicates the total number of the users.

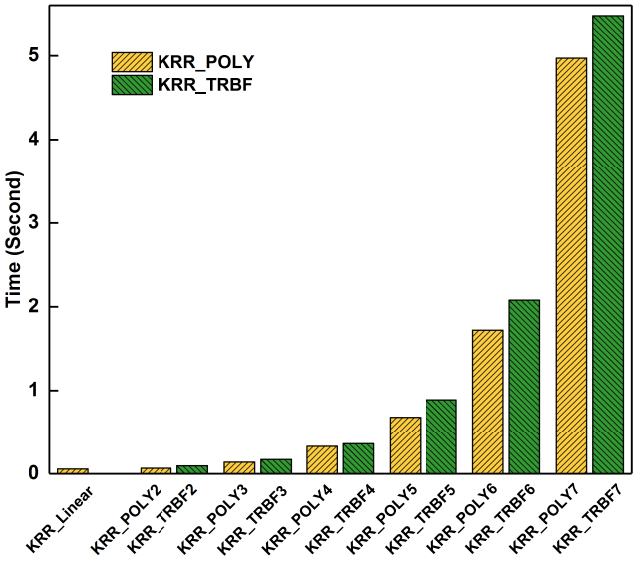


FIGURE 4. Training time for KRR-TRBF and KRR-POLY over various degrees.

TABLE 3. Training time for KRR-TRBF and KRR-POLY over various degrees.

Classifier	Training time (s)
KRR-linear	0.056
KRR-POLY2	0.067
KRR-POLY3	0.138
KRR-POLY4	0.330
KRR-POLY5	0.679
KRR-POLY6	1.719
KRR-POLY7	4.974
KRR-TRBF2	0.095
KRR-TRBF3	0.170
KRR-TRBF4	0.363
KRR-TRBF5	0.891
KRR-TRBF6	2.077
KRR-TRBF7	5.477
SVM-RBF	3.849

Fig. 4 and Table 3 show the training time of the KRR classifier with TRBF kernel and POLY kernel over various degrees, respectively. As illustrated in Fig. 4, the training time for both KRR-TRBF and KRR-PLOY grows with their degrees increase. The higher the degree is, the more training time the classifier takes. In particular, the training time of KRR-TRBF is a little bit higher than that of KRR-PLOY on each degree. However, the performance of KRR-TRBF is relatively better than that of KRR-PLOY, as shown in Fig 2.

4) COMPARISON OF THE TRAINING TIME BETWEEN THE KRR-TRBF AND SVM-RBF

Fig. 5 illustrates the training time for the KRR classifier with TRBF5, TRBF6 and TRBF7 kernels, and the SVM-RBF classifier. As shown in Fig. 5, both KRR-TRBF5 and KRR-TRBF6 take significantly less training time than SVM-RBF, while KRR-TRBF7 has a slightly higher training time than SVM-RBF. Considering that both KRR-TRBF6 and KRR-TRBF7 show relatively higher accuracy than

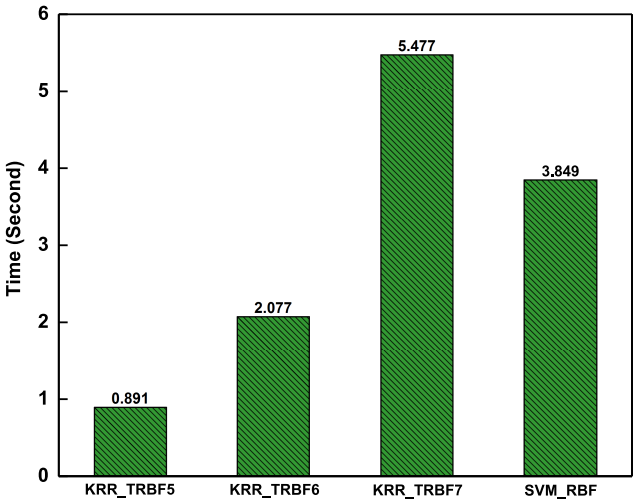


FIGURE 5. Comparison of the training time between KRR-TRBF and SVM-RBF.

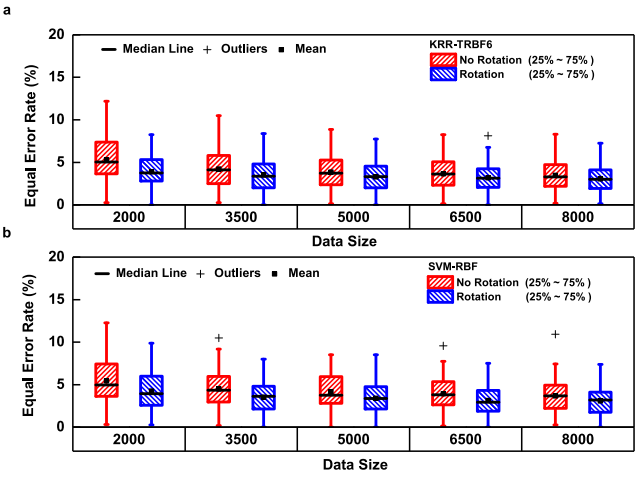


FIGURE 6. EER of the KRR-TRBF6 and SVM-RBF with rotation on different data sizes.

SVM-RBF as demonstrated in Fig. 3, we choose KRR-TRBF6 as our training and testing classifier in *SensorCA*.

B. EVALUATION ON THE ROTATION

In this section, we evaluate the performance of *SensorCA* on the data augmentation approach rotation with different dataset sizes, in terms of the EER of KRR-TRBF6 and SVM-RBF, training time of KRR-TRBF6 and SVM-RBF, and EER for KRR-TRBF6 and SVM-RBF on different rotation angles. In the experiments, we choose the rotation angle as 1 or -1 degree, which indicates that $\alpha = \beta = \gamma = 1$ or -1 in the three basic rotation matrices.

1) EER OF KRR-TRBF6 AND SVM-RBF WITH DIFFERENT DATASET SIZES

Fig. 6 shows box plots of the EER of the KRR-TRBF6 and SVM-RBF with rotation approach on different dataset sizes. For the rotation approach, we vary the dataset size ranges from 2000 to 8000. For each dataset size, we plot boxes of the EER with no augmentation (red box plot) and the EER with the rotation approach (blue box plot), respectively, for comparison. In particular, Fig. 6a illustrates box plots of the EER of the KRR-TRBF6 on different dataset sizes. More specially, with the increase of the dataset size, the EER decreases. Moreover, the EER with the rotation approach shows significantly lower values than that without rotation. Fig. 6b demonstrates box plots of the EER of the SVM-RBF on different dataset sizes, which exhibit the same trend with the EER of the KRR-TRBF6. However, the KRR-TRBF6 shows lower EERs than the SVM-RBF on different dataset sizes. Table 4 and 5 list the mean, SD, and median of EERs for the KRR-TRBF6 and SVM-RBF with and without rotation approach on different dataset sizes, respectively. For both the classifiers, the mean, SD, and median of the EERs with the rotation approach are less than that without the rotation, which ensures the advantage of the rotation approach and motivates us to apply this approach to our authentication system. More specifically, comparing Tables 4 with 5, the KRR-TRBF6 classifier performs a better median EER of 3.0% than the SVM-RBF classifier with dataset size 8000.

TABLE 4. EER of the KRR-TRBF6 with (without) rotation on different data sizes.

Dataset size	EER (%) with (without) rotation		
	Mean	SD	Median
2000	3.9 (5.3)	1.9 (2.6)	3.8 (5.0)
3500	3.5 (4.2)	1.8 (2.1)	3.4 (4.1)
5000	3.3 (3.9)	1.7 (1.9)	3.3 (3.7)
6500	3.2 (3.7)	1.6 (1.8)	3.1 (3.6)
8000	3.1 (3.5)	1.6 (1.7)	3.0 (3.3)

TABLE 5. EER of the SVM-RBF with (without) rotation on different data sizes.

Dataset size	EER (%) with (without) rotation		
	Mean	SD	Median
2000	4.2 (5.4)	2.1 (2.5)	3.9 (5.0)
3500	3.5 (4.5)	1.8 (2.2)	3.6 (4.3)
5000	3.4 (4.2)	1.9 (2.2)	3.4 (3.8)
6500	3.1 (3.9)	1.7 (2.0)	2.9 (3.8)
8000	3.1 (3.7)	1.7 (1.9)	3.2 (3.7)

It is worth noting that the performance of SVM-RBF on a small dataset is still acceptable. However, as the dataset size increases, the EER of KRR-TRBF6 gradually shows more competitive advantages. In the following time performance comparison, the advantages of the KRR-TRBF6 will be more prominent.

2) TRAINING TIME OF KRR-TRBF6 AND SVM-RBF WITH DIFFERENT DATASET SIZES

Fig. 7 and Table 6 show the training time of the KRR-TRBF6 and SVM-RBF with rotation approach on different dataset sizes ranging from 1000 to 16000. As shown in Fig. 7, the training time increases as the dataset size increases for both the KRR-TRBF6 and SVM-RBF. However, the KRR-TRBF6 takes less training time than the SVM-RBF on each dataset size. In particular, the

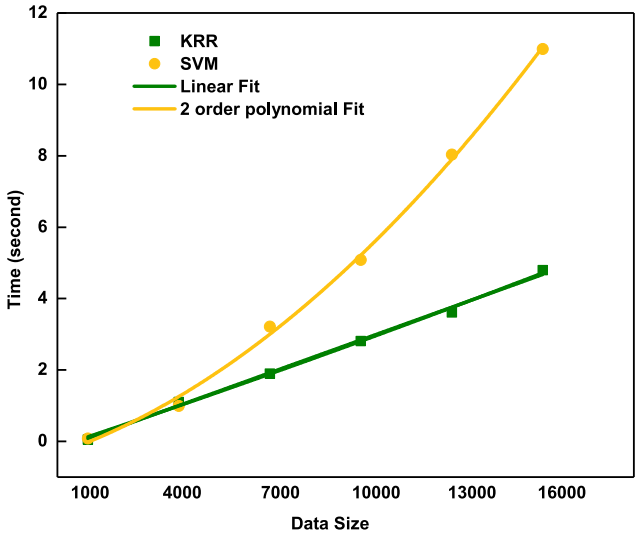


FIGURE 7. Training time of KRR-TRBF6 and SVM-RBF with rotation on different dataset sizes.

TABLE 6. Training time of KRR-TRBF6 and SVM-RBF with rotation on different dataset sizes.

Dataset size	Training time (s)	
	KRR-TRBF6	SVM-RBF
1000	0.054	0.081
4000	1.108	0.995
7000	1.902	3.213
10000	2.808	5.806
13000	3.612	8.036
16000	4.801	10.989

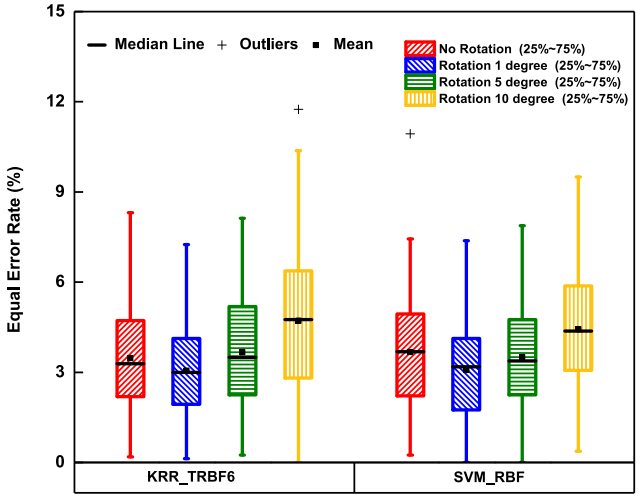


FIGURE 8. EER of the KRR-TRBF6 and SVM-RBF under different rotation degrees.

KRR-TRBF6 costs the shortest training time of 0.054 seconds with dataset size 1000. More specifically, with the increase of the dataset size, the training time of the KRR-TRBF6 grows slower than that of the SVM-RBF. When dataset size comes to 16000, the KRR-TRBF6 just takes 4.801 seconds which are significantly less than 10.989 seconds SVM-RBF does.

TABLE 7. EER of the KRR-TRBF6 and SVM-RBF under different rotation degrees.

Classifier	EER (%)	Rotation degree			
		No rotation	1 degree	5 degree	10 degree
KRR-TRBF6	Mean	3.5	3.1	3.7	4.7
	SD	1.7	1.6	1.9	2.4
	Median	3.3	3.0	3.5	4.8
SVM-RBF	Mean	3.7	3.1	3.5	4.4
	SD	1.9	1.7	1.8	2.1
	Median	3.7	3.2	3.4	4.4

3) EER OF KRR-TRBF6 AND SVM-RBF UNDER DIFFERENT ROTATION DEGREES

To further understand the impact of the rotation on the proposed system, we discuss the effect of the rotation angle on the EER performance. Fig. 8 shows box plots of the EER with the KRR-TRBF6 and SVM-RBF on different range of the rotation angles (such as no rotation, 1 degree, 5 degrees and 10 degrees). As illustrated in Fig. 8, for both the KRR-TRBF6 and SVM-RBF, the EER increases with the increase of the rotation degree. The reason is that a large rotation angle may cause the augmented sensor data to have a very different distribution from the raw sensor data, complicating the entire dataset and resulting in an increased EER. Hence, we choose rotation degree as 1 or -1 in the experiments.

Table 7 lists the mean, SD, median of the EER for the KRR-TRBF6 and SVM-RBF under different rotation angles. As shown in Table 7, the EER of the KRR-TRBF6 is less than that of the SVM-RBF under any rotation degree.

VII. CONCLUSION

In this paper, we propose a novel sensor-based continuous authentication system, *SensorCA*, for continuously monitoring users' behavior patterns, by leveraging the accelerometer, gyroscope, and magnetometer ubiquitously built-in smartphones. We are among the first to exploit the data augmentation approach of the rotation, which creates additional data by applying it on the collected raw data and improves the robustness of the proposed system. With the augmented data, *SensorCA* extracts sensor-based features in the time and frequency domains, then utilizes the KRR-TRBF to train the classifier, and finally authenticates the current user as a legitimate user or an impostor. We evaluate the authentication performance of *SensorCA* in terms of the different classifiers including KRR-TRBF, KRR-POLY and SVM-RBF, and the data augmentation approach rotation on KRR-TRBF6 and SVM-RBF. The experimental results show that under the KRR-TRBF6 classifier, *SensorCA* reaches the lowest median EER of 3.0% with dataset size 8000 and costs the shortest training time of 0.054 seconds with dataset size 1000.

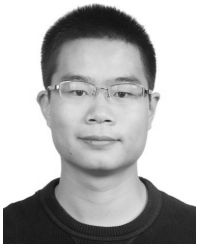
REFERENCES

[1] Y. Kim, T. Oh, and J. Kim, "Analyzing user awareness of privacy data leak in mobile applications," *Mobile Inf. Syst.*, vol. 2015, pp. 1–12, Nov. 2015, Art. no. 369489.

[2] Y. Li, F. Xue, X. Fan, Z. Qu, and G. Zhou, "Pedestrian walking safety system based on smartphone built-in sensors," *IET Commun.*, vol. 12, no. 6, pp. 751–758, Apr. 2018.

[3] Y. Li and X. Li, "Chaotic hash function based on circular shifts with variable parameters," *Chaos, Solitons Fractals*, vol. 91, pp. 639–648, Oct. 2016.
[4] J. Mantyjarvi, M. Lindholm, E. Vildjiounaite, S.-M. Makela, and H. A. Ailisto, "Identifying users of portable devices from gait pattern with accelerometers," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, Philadelphia, PA, USA, Mar. 2005, pp. II973–II976.
[5] C. Nickel, T. Wirtl, and C. Busch, "Authentication of smartphone users based on the way they walk using k-NN algorithm," in *Proc. 8th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, Piraeus, Greece, Jul. 2012, pp. 16–20.
[6] M. Tamviruzzaman, S. I. Ahamed, C. S. Hasan, and C. O'Brien, "ePet: When cellular phone learns to recognize its owner," in *Proc. ACM Workshop Assurable Usable Secur. Configuration*, Chicago, IL, USA, 2009, pp. 13–18.
[7] 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.
[8] M. Conti, I. Zachia-Zlatea, and B. Crispo, "Mind how you answer me!: Transparently authenticating the user of a smartphone when answering or placing a call," in *Proc. ACM Symp. Inf., Comput. Commun. Secur. (ASIA CCS)*, Hong Kong, Mar. 2011, pp. 249–259.
[9] Q. Zhang, L. T. Yang, Z. Chen, P. Li, and M. J. Deen, "Privacy-preserving double-projection deep computation model with crowdsourcing on cloud for big data feature learning," *IEEE Intnet Things J.*, Jul. 2017, doi: 10.1109/JIOT.2017.2732735.
[10] 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, CA, USA, Jan. 2013, pp. 1128–1133.
[11] W.-H. Lee and R. B. Lee, "Multi-sensor authentication to improve smartphone security," in *Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP)*, Angers, France, Feb. 2015, pp. 1–11.
[12] L. Yang *et al.*, "Unlocking smart phone through handwaving biometrics," *IEEE Trans. Mobile Comput.*, vol. 14, no. 5, pp. 1044–1055, May 2015.
[13] M. P. Centeno, A. van Moorsel, and S. Castruccio, "Smartphone continuous authentication using deep learning autoencoders," in *Proc. Int. Conf. Privacy, Secur. Trust (PST)*, Calgary, AB, Canada, Aug. 2017, pp. 1–9.
[14] Y. Chen, C. Shen, Z. Wang, and T. Yu, "Modeling interactive sensor-behavior with smartphones for implicit and active user authentication," in *Proc. IEEE Int. Conf. Identity, Secur. Behav. Anal. (ISBA)*, New Delhi, India, Feb. 2017, pp. 1–6.
[15] G. Peng, G. Zhou, D. T. Nguyen, X. Qi, Q. Yang, and S. Wang, "Continuous authentication with touch behavioral biometrics and voice on wearable glasses," *IEEE Trans. Human-Mach. Syst.*, vol. 47, no. 3, pp. 404–416, Jun. 2017.
[16] W. Zhu *et al.*, "Co-occurrence feature learning for skeleton based action recognition using regularized deep LSTM networks," in *Proc. 13th AAAI Conf. Artif. Intell. (AAAI)*, Phoenix, AZ, USA, Feb. 2016, pp. 3697–3703.
[17] T. Feng *et al.*, "Continuous mobile authentication using touchscreen gestures," in *Proc. IEEE Conf. Technol. Homeland Security (HST)*, Waltham, MA, USA, Nov. 2012, pp. 451–456.
[18] M. Trojahn and F. Ortmeier, "Toward mobile authentication with keystroke dynamics on mobile phones and tablets," in *Proc. Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Barcelona, Spain, Mar. 2013, pp. 697–702.
[19] Q. Zhang, L. T. Yang, Z. Chen, and P. Li, "PPHOPCM: Privacy-preserving high-order possibilistic c-means algorithm for big data clustering with cloud computing," *IEEE Trans. Big Data*, May 2017, doi: 10.1109/TBDATA.2017.2701816.
[20] 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. Forensics Security*, vol. 8, no. 1, pp. 136–148, Jan. 2013.
[21] L. Li, X. Zhao, and G. Xue, "Unobservable re-authentication for smartphones," in *Proc. 20th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, Feb. 2013, pp. 1–16.
[22] 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 Secur. (SOUPS)*, Menlo Park, CA, USA, Jul. 2014, pp. 187–198.
[23] N. Zheng, K. Bai, H. Huang, and H. Wang, "You are how you touch: User verification on smartphones via tapping behaviors," in *Proc. IEEE Int. Conf. Netw. Protocols (ICNP)*, Raleigh, NC, USA, Oct. 2014, pp. 221–232.
[24] H. Zhang, V. M. Patel, M. Fathy, and R. Chellappa, "Touch gesture-based active user authentication using dictionaries," in *Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV)*, Waikoloa, HI, USA, Jan. 2015, pp. 207–214.
[25] S. Mare, A. M. Markham, C. Cornelius, R. Peterson, and D. Kotz, "ZEBRA: Zero-effort bilateral recurring authentication," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Jose, CA, USA, May 2014, pp. 705–720.
[26] W.-H. Lee and R. B. Lee, "Sensor-based implicit authentication of smartphone users," in *Proc. IEEE Int. Conf. Dependable Syst. Netw. (DSN)*, Denver, CO, USA, Jun. 2017, pp. 309–320.
[27] C. Song, F. Lin, Y. Zhuang, W. Xu, C. Li, and K. Ren, "Cardiac scan: A non-contact and continuous heart-based user authentication system," in *Proc. IEEE Int. Conf. Mobile Comput. Netw. (Mobicom)*, Snowbird, UT, USA, Oct. 2017, pp. 315–328.
[28] H. Feng, K. Fawaz, and K. G. Shin, "Continuous authentication for voice assistants," in *Proc. 23rd Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Snowbird, UT, USA, Oct. 2017, pp. 343–355.
[29] W.-H. Lee and R. Lee, "Implicit sensor-based authentication of smartphone users with smartwatch," in *Proc. Hardw. Archit. Support Secur. Privacy (HASP)*, Seoul, South Korea, Jun. 2016, Art. no. 9.
[30] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Evaluating behavioral biometrics for continuous authentication: Challenges and metrics," in *Proc. ACM Asia Conf. Comput. Commun. Secur. (ASIA CCS)*, Abu Dhabi, United Arab Emirates, Apr. 2017, pp. 386–399.
[31] N. Shabrina, T. Isshiki, and H. Kunieda, "Fingerprint authentication on touch sensor using Phase-Only Correlation method," in *Proc. 7th Int. Conf. Inf. Commun. Technol. Embedded Syst. (IC-ICTES)*, Bangkok, Thailand, Mar. 2016, pp. 1–5.
[32] W.-H. Lee and R. B. Lee, "Implicit smartphone user authentication with sensors and contextual machine learning," in *Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Denver, CO, USA, Jun. 2017, pp. 297–308.
[33] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.
[34] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," *IEEE Signal Process. Mag.*, vol. 33, no. 4, pp. 49–61, Jul. 2016.
[35] J. Mercer, "Functions of positive and negative type, and their connection the theory of integral equations," *Philos. Trans. Roy. Soc. London A, Math. Phys. Sci.*, vol. 209, pp. 441–458, Jan. 1909.
[36] S. Y. Kung and P.-Y. Wu, "On efficient learning and classification kernel methods," in *Proc. ICASSP*, Kyoto, Japan, Mar. 2012, pp. 2065–2068.
[37] P.-Y. Wu, C.-C. Fang, J. M. Chang, and S.-Y. Kung, "Cost-effective kernel ridge regression implementation for keystroke-based active authentication system," *IEEE Trans. Cybern.*, vol. 47, no. 11, pp. 3916–3927, Nov. 2016.
[38] Q. Zhang, L. T. Yang, Z. Chen, and P. Li, "A survey on deep learning for big data," *Inf. Fusion*, vol. 42, pp. 146–157, Jul. 2018.
[39] Q. Zhang, M. Lin, L. T. Yang, Z. Chen, and P. Li, "Energy-efficient scheduling for real-time systems based on deep Q-learning model," *IEEE Trans. Sustain. Comput.*, Aug. 2017, doi: 10.1109/TSUSC.2017.2743704.
[40] T.-T. Frieß and R. F. Harrison, "A kernel-based adaline," in *Proc. 7th Eur. Symp. Artif. Neural Netw. (ESANN)*, Bruges, Belgium, Apr. 1999, pp. 245–250.
[41] Y. Engel, S. Mannor, and R. Meir, "The kernel recursive least-squares algorithm," *IEEE Trans. Signal Process.*, vol. 52, no. 8, pp. 2275–2285, Aug. 2004.
[42] J. Kivinen, A. J. Smola, and R. C. Williamson, "Online learning with kernels," *IEEE Trans. Signal Process.*, vol. 52, no. 8, pp. 2165–2176, Aug. 2004.
[43] A. N. Tikhonov, "On the stability of inverse problems," *Doklady Akademii Nauk SSSR*, vol. 39, no. 5, pp. 195–198, 1943.
[44] Z. Sitová *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.
[45] 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.
[46] C. Shen, T. Yu, S. Yuan, Y. Li, and X. Guan, "Performance analysis of motion-sensor behavior for user authentication on smartphones," *Sensors*, vol. 14, no. 3, pp. 1–21, Mar. 2016.
[47] 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. Forensics Security*, vol. 13, no. 1, pp. 48–62, Jan. 2018.

[48] Q. Zhang and Z. Chen, "A distributed weighted possibilistic c-means algorithm for clustering incomplete big sensor data," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 5, pp. 1–8, 2014.
[49] 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.
[50] N. Neverova *et al.*, "Learning human identity from motion patterns," *IEEE Access*, vol. 4, pp. 1810–1820, 2016.



YANTAO LI received the Ph.D. degree from the College of Computer Science, Chongqing University, China, in 2012.

He is currently an Associate Professor with the College of Computer and Information Sciences, Southwest University, China, and has been a Postdoctoral Research Associate with the Department of Computer Science, College of William and Mary, USA, since 2016. From 2010 to 2012, he was a Visiting Scholar supported by China Scholarship Council with the College of William and Mary under the supervision of Prof. G. Zhou . His research area includes wireless communication and networking, sensor networks and ubiquitous computing, and information security.

Dr. Li was a recipient of the Outstanding Master's Thesis Award in Chongqing in 2011 and the Outstanding Ph.D. Thesis Award in Chongqing in 2014. He has served as a TPC member for several international conferences, such as the IEEE BigDataService from 2015 to 2018, and a Reviewer for several international journals, such as *ACM Transactions on Sensor Networks*, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE INTERNET OF THINGS, Elsevier *Computer Networks*, and Springer *Multimedia Tools and Applications*.

HAILONG HU received the B.S. degree from the College of Computer and Information Sciences, Southwest University, China, in 2016.

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

GANG ZHOU (M'07–SM'13) received the Ph.D. degree from the University of Virginia in 2007 under the supervision of Prof. John A. Stankovic. He served as the Graduate Program Director of this department from 2015 to 2017. He is currently an Associate Professor with the Computer Science Department, College of William and Mary. He has published over 90 papers in the areas of wireless networks, sensor systems, Internet of Things, smart health, and ubiquitous and mobile computing. There are in total 7070 citations of his papers per Google Scholar. He also has 11 papers each of which has been cited over 200 times since 2004. 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 was a recipient of the Best Paper Award of the IEEE ICNP 2010. He received NSF CAREER Award in 2013. He received the 2015 Plumeri Award for Faculty Excellence. He is an ACM/IEEE CHASE 2018 TPC Co-Chair. He serves on the Journal Editorial Board of *ACM Transactions on Sensor Networks*, the IEEE INTERNET OF THINGS, Elsevier *Computer Networks*, and Elsevier *Smart Health*.

SHAOJIANG DENG received the Ph.D. degree from the College of Computer Science, Chongqing University, in 2005.

He is currently a Professor with the College of Computer Science, Chongqing University, China. In 2007, he was a Visiting Scholar with the Institute of Applied Computer Science, Dresden University of Technology, Germany. His research interest focuses on digital chaotic cryptography, information security, and hash function construction.