Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey

Mohammed Abuhamad, Ahmed Abusnaina, *Graduate Student Member, IEEE*, Daehun Nyang, and David Mohaisen, *Senior Member, IEEE*

***Abstract*—Mobile devices and technologies have become increasingly popular, offering comparable storage and computational capabilities to desktop computers allowing users to store and interact with sensitive and private information. The security and protection of such personal information are becoming more and more important since mobile devices are vulnerable to unauthorized access or theft. User authentication is a task of paramount importance that grants access to legitimate users at the point of entry and continuously through the usage session. This task is made possible with today's smartphones' embedded sensors that enable continuous and implicit user authentication by capturing behavioral biometrics and traits. In this article, we survey more than 140 recent behavioral biometric-based approaches for continuous user authentication, including motion-based methods (28 studies), gait-based methods (19 studies), keystroke dynamics-based methods (20 studies), touch gesture-based methods (29 studies), voice-based methods (16 studies), and multimodal-based methods (34 studies). The survey provides an overview of the current state-of-the-art approaches for continuous user authentication using behavioral biometrics captured by smartphones' embedded sensors, including insights and open challenges for adoption, usability, and performance.**

***Index Terms*—Continuous authentication, mobile sensing, sensor-based authentication, smartphone authentication.**

I. Introduction

SMARTPHONES have been witnessing a rapid increase in storage and computational resources, making them an invaluable instrument for activities on the Internet and a leading platform for users' communication and interaction with data and media of different forms. Moreover, the current edge and cloud computing services available to users have increased the reliance on mobile devices for mobility and convenience, revolutionizing the landscape of technologies and methods of conducting transactions [1]. The continuous user authentication is an implicit process of validating the legitimate user based on capturing behavioral attributes by leveraging resources and built-in sensors of the mobile device. Users tend to develop distinctive behavioral patterns when using mobile devices, which can be used for the authentication task. These patterns are implicitly captured as users interact with their devices using behavioral features calculated from a stream of data, such as interaction and environmental information and sensory data. Continuous authentication methods are also called "transparent, implicit, active, nonintrusive, nonobservable, adaptive, unobtrusive, and progressive" techniques [2], [3]. Traditionally, continuous authentication methods operate as a support process to the conventional authentication methods, e.g., using secret-based authentication or physiological biometrics, such as prompting users to reauthenticate when adversarial or unauthorized behavior is detected.

Recently, the field of continuous authentication has been gaining increasing interest, especially with the expansion of storage and computational resources and the availability of sensors that can make the implicit authentication very accurate and effective. Using sensors-based authentication methods offers convenient and efficient access control for users. This article surveys recent and state-of-the-art methods for continuous authentication using behavioral biometrics. We aim to shed light on the current state and challenges facing the adoption of such methods in today's smartphones.

Conventional Versus Biometric Approaches: To date, vendors of mobile devices have adopted both knowledge-based schemes and physiological biometrics as the primary security method for accessing the device. Knowledge-based approaches rely on the knowledge of the user; i.e., the user must provide certain information, such as numeric password, PIN, graphical sequence, or a picture gesture [4], to access a device [5]. Despite their simplicity, ease of implementation, and user acceptance, such approaches suffer from several shortcomings, such as the inconvenience of frequent reentering (especially when the knowledge used is long enough to convey strong security) and several adversarial attacks (e.g., shoulder surfing and smudge attacks) [6]–[10]. Another issue with knowledge-based authentication is the underlying assumption of having equal security requirements for all

Manuscript received May 9, 2020; revised July 15, 2020; accepted August 21, 2020. Date of publication August 28, 2020; date of current version December 21, 2020. This work was supported in part by the CyberFlorida Collaborative Seed Award, and in part by NRF under Grant 2016K1A1A2912757 (Global Research Lab Initiative). *(Corresponding authors: Daehun Nyang; David Mohaisen.)*

Mohammed Abuhamad is with the Department of Computer Science, Loyola University Chicago, Chicago, IL 60660 USA.

Ahmed Abusnaina and David Mohaisen are with the Department of Computer Science, University of Central Florida, Orlando, FL 32816 USA (e-mail: mohaisen@ucf.edu).

Daehun Nyang is with the Department of Cyber Security, Ewha Womans University, Seoul 03760, South Korea (e-mail: nyang@ewha.ac.kr).

Digital Object Identifier 10.1109/JIOT.2020.3020076

TABLE I
SUMMARY OF THE RELATED SURVEYS IN THE FIELD OF USER AUTHENTICATION, HIGHLIGHTING THE FEATURES FOR EACH WORK

	Year	Refereces	System Design	Protocols and Security	Traditional Methods	Motion-based Modalities	Gait-based Modalities	Keystroke Dynamics-based Modalities	Touch Gestures-based Modalities	Voice-based Modalities	Multiple Modalities
[8]	2005	19	✗	✓	✓	✗	✗	✗	✗	✗	✗
[24]	2011	72	✓	✗	✗	✗	✗	✓	✗	✗	✗
[22]	2013	163	✓	✓	✓	✗	✗	✓	✗	✗	✗
[23]	2013	56	✗	✗	✓	✗	✗	✓	✗	✗	✗
[2]	2016	150	✓	✓	✓	✗	✗	✗	✗	✗	✓
[26]	2016	33	✗	✗	✓	✗	✗	✗	✗	✗	✗
[3]	2016	191	✓	✗	✓	✓	✓	✓	✓	✓	✓
[25]	2017	214	✓	✗	✗	✗	✗	✗	✗	✓	✗
[27]	2018	36	✓	✓	✓	✗	✗	✗	✗	✗	✗
Ours	2020	187	✓	✓	✓	✓	✓	✓	✓	✓	✓

applications [11]. For example, accessing financial records and texting are given the same level of security. Using a knowledge-based authentication on smartphones falls short on delivering application-specific security guarantees [12], especially observing the recent emergence of adaptable biometric authentication that account for environmental factors to adapt and select the suitable sensors for authentication (e.g., using fingerprint sensor when the lighting condition does not allow for face recognition) [13]. Even when using more complicated implementations of knowledge-based approaches, e.g., Yu *et al.*'s [14] implementation of 3-D graphical passwords that can be easier to remember and possibly providing larger password space, they still inherit the same drawbacks. In fact, in a study by Amin *et al.* [9], graphical sequences (2-D patterns) are shown to be as easier to predict as textual passwords since 40% of patterns begin from the top-left node and the majority of users use five nodes out of the nine nodes. Another example of sophisticated knowledge-based schemes is introduced by Shin *et al.* [15], which includes changing the colors of six circles by touching them repeatedly up to seven times. Once all the circles' colors fit the correct combination, user authentication is granted. Even though this allows for harder security (especially when enabling a larger number of circles and colors), it still requires memorizing such complex combinations, which is the main disadvantage in knowledge-based approaches. To overcome the need for memorizing complex combinations, Yang *et al.* [16] proposed free-form gestures (doodling) as a user validation scheme, where users are to enter any draw with any number of fingers. The authors showed that using free-form gestures enabled a log-in time reduction that reached 22% in comparison to textual passwords while maintaining higher usability and search space. However, the authors have not addressed other security concerns, such as shoulder surfing and smudge attacks.

Many researchers have attempted to overcome the core problems of knowledge-based authentication by coupling such methods with biometric-based methods. Using biometric information improves both the accuracy and usability of the authentication process. Such integration can be done by measuring the keystroke dynamics or gestures when connecting, changing the order, or selecting images [17]. The shortcomings of knowledge-based authentication approaches motivate for using stronger and easier authentication schemes such as biometrics. Physiological biometrics provide unquestionable precision of user authentication with a convenient and simple approach. For example, most current smartphones are equipped with a fingerprint recognition module as reliability and a cost-effective method for user authentication [3], [18], [19].

Physiological biometrics-based authentication techniques show high efficiency, accuracy, and user acceptance [3], [12], [20]. However, all of these techniques necessitate the user's knowledge of the service since the user must interact with the biometric sensor and be aware of the biometric capturing process. Similar to knowledge-based authentication schemes, physiological biometrics, e.g., face, fingerprint, periocular, and iris, can provide point-of-entry authentication and fall short of offering implicit and transparent authentication.

Motivation: It is obvious that knowledge-based and physiological biometric-based methods are successful for user validation, but they fall short on delivering continuous and transparent authentication. Moreover, physiological biometrics are mostly hardware dependent. Behavioral biometrics show higher potential to meet all requirements for an efficient authentication system. In addition to all benefits of adopting behavioral biometrics, they are a suitable solution for "user abandonment" [21] protection, or when the legitimate user of the unlocked device is not present. These many advantages of behavioral biometrics-based authentication have shown to be influential for user adoption since a survey by Crawford and Renaud [10] demonstrated that 90% of the study's participants favored behavioral biometrics-based transparent authentication. Hence, the literature shows a remarkable interest in adopting various behavioral modalities, such as keystroke dynamics, touch gestures, motion, voice, etc., for transparent user authentication on mobile devices.

This article focuses on behavioral continuous authentication and multimodal methods that may incorporate physiological biometrics to harden security and boost the performance of the authentication scheme. Table I shows a summary of features of several surveys in the field of user authentication, highlighting scope, and modalities. For readability, we list the abbreviations used in this article in Table II.

Other Related Surveys: There are several surveys that have addressed specific modalities, e.g., keystroke dynamics [22]–[24], voice-based speaker identification [25], and multimodal authentication [2]. Moreover, there are surveys that address traditional biometric based, i.e., [8] and [26], general

TABLE II
LIST OF ABBREVIATIONS IN ALPHABETICAL ORDER

Term	Definition
Ac	Accelerometer
ANN	Artificial Neural Network
Ca	Camera
CC	Cross-correlation
CI	Confidence Interval
CNN	Convolutional Neural Network
Co	Compass
CPANN	Counter Propagation Artificial Neural Network
CRM	Cyclic Rotation Metric
DAE-SR	Deep Auto Encoder and Softmax Regression
DSP	Digital Signal Processing
DTW	Dynamic Time Wrapping
EEH	Electromagnetic Energy Harvester
EER	Equal Error Rate
El	Elevation
FA-NN	Fast Approximate Nearest Neighbor
FAR	False Acceptance Rate
FC	Fuzzy Commitment
FFT	Fast Fourier Transform
FLD	Fisher Linear Discriminant
FPOS	Frequent Pattern Outlier Score
FRR	False Rejection Rate
FSR	Force Sensing Resistor
GA	Genetic Algorithm
GMM	Gaussian Mixed Model
GPS	Global Positioning System
Gr	Gravity sensor
Gy	Gyroscope
HMM	Hidden Markov Model
HWS	Healthcare Wearable Sensors
I-F	Isolation Forest
KL	Kullback-Leibler
k-NN	k-Nearest Neighbor
KRR	Kernel Ridge Regression
LDA	Linear Discriminant Analysis
Li	Light sensor
LMC	Leap Motion Controller
LSTM	Long Short Term Memory
Ma	Magnetometer
MCF	Multi-Classifier Fusion
MGGN	Multivariate Gaussian Generative Model
MHD	Modified Hausdorff Distance
Mi	Microphone
MLP	Multilayer Perceptron
MRC	Cyclic Rotation Metric
Or	Orientation
PCA	Principle Component Analysis
PEH	Piezoelectric Energy Harvester
Pr	Pressure
PSO	Particle Swarm Optimization
RBF	Radial Basis Function
RBFN	Radial Basis Function Network
RF	Random Forest
SOM	Self Organizing Maps
Sp	Speaker
SRC	Sparse Representation Classification
SVM	Support Vector Machine
To	Touch
VR	Virtual Reality

authentication schemes, i.e., [2] and [3], and authentication protocols and OS-related security [27]. This study provides a contemporary survey for sensor-based continuous authentication on smartphones, differing in scope, time, and range of surveyed works. Table I shows a summary of features of several surveys in the field of user authentication, highlighting scope, and modalities.

Contribution: This work contributes to the mobile continuous user authentication in several aspects.

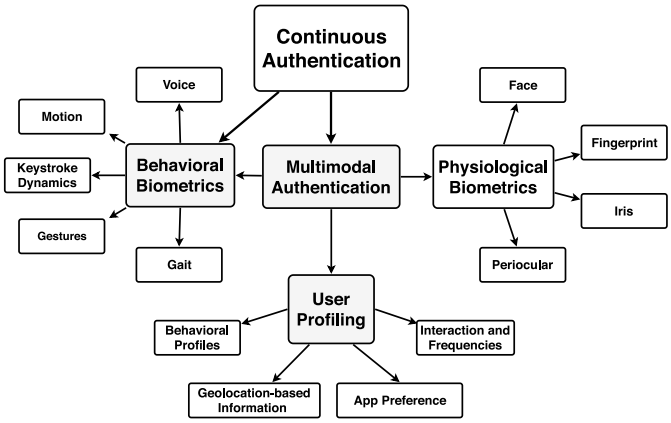

Fig. 1. Biometric-based authentication modalities are categorized into physiological biometrics, behavioral biometrics, and user profiles.

1) Survey more than 140 works on continuous user authentication methods, categorizing them into six behavioral and physiological biometrics groups (motion, gait, keystroke dynamics, gesture, voice, and multimodal).
2) Present the studies of each biometric modality in a table format, comparing works by the modality, sensors, and the used authentication algorithm, in addition to the data collected, user sample size, and six evaluation metrics. Such comparison provides ease in understanding each work and how it compares to others in the field.
3) Give insights and challenges for different biometric methods, highlighting the possible future work and existing common gaps within the literature.

Organization: The remainder of this survey is organized as follows. We discuss the system design of continuous user authentication, including biometric modalities, user enrollment, and verification techniques, and evaluation metrics in Section II. The user authentication system is categorized into six groups: motion-based authentication is discussed in Section III, gait-based authentication in Section IV, and followed by keystroke dynamics-based authentication in Section V. Touch gesture-based and voice-based authentication methods are described in Sections VI and VII, respectively. The multimodal-based authentication is described in Section VIII. Finally, we conclude in Section IX.

II. CONTINUOUS AUTHENTICATION: DESIGN

Numerous studies have explored various methods for continuous user authentication leveraging modern mobile technologies and embedded sensors to model users' behavior. The deployment of sensors on today's mobile devices has enabled a variety of applications, such as modeling human behavior [28], [29], user authentication [30]–[34], activity and action recognition [28], [35], [36], and healthcare monitoring [37], [38], among others [39], [40]. In this article, we show recent user authentication methods that use mobile sensory data to capture users' behavioral biometrics.

A. Used Biometric Modalities

Several modalities are used for biometric-based authentication, including physiological biometrics (e.g., face, fingerprint,

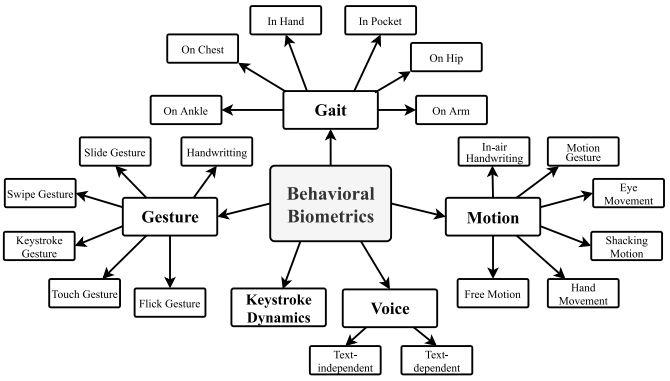

Fig. 2. Behavioral biometrics are categorized into several modalities. The combination of the modalities provides a multimodal user authentication.

iris, etc.) and behavioral biometrics (e.g., keystroke dynamics, touch gestures, voice, motions, etc.). Fig. 1 shows a categorization of used modalities for user authentication tasks. Fig. 2 shows the modalities and features of several behavioral biometrics that are commonly used for user authentication tasks. All these modalities are made possible by the embedded mobile sensors, e.g., camera, microphone, accelerometers, and gyroscopes, which contribute to the enrolment phase and the verification part of the authentication process. Such sensors provide sufficient information for accurate and secure authentication, and adopting the proper utilization mechanism would play an essential role in delivering efficient and usable user authentication [41]. Using biometrics for authentication, there are enormous studies that demonstrated the benefits and security aspects of using such information to explore "on-the-move biometry" [42].

B. User Authentication

Biometric-based user authentication leverages users' behavioral patterns for the identification or/and validation task using a pattern recognition method. The authentication is commonly referred to as a verification task in mobile security since the authentication method validates the legitimate user given certain biometrics. The general framework for the authentication system is illustrated in Fig. 3.

Enrolment: There are two common approaches for user enrollment in the user authentication system. For simplicity purposes, we categorize enrollment techniques to: 1) template-based enrollment and 2) model-based enrollment. For template-based enrollment, the user submits several samples to establish templates for future comparison. This method is popular among authentication methods using physiological biometrics, where features can be more robust to intraclass variations and more distinctive and scalable for a large population. Once users' templates are established, a similarity-based technique is used to validate users after passing a similarity threshold. Many considerations should be taken to ensure the quality of templates for supporting the performance of the system, such as the robustness and distinguishability of features across users, removing outliers, and reducing noise and redundancy. Moreover, security concerns should be addressed to ensure the security and privacy of users' templates, whether during enrollment and template registration, storing, retrieving, and processing for user authentication. For model-based enrollment, users' biometrics are collected for training a machine learning model for user authentication, where the authentication model decides whether the input data belong to the legitimate user. The common machine learning approaches are used to establish users' models, including data acquisition and preprocessing, feature extraction and selection, and modeling. The quality of features plays a significant role in the performance of model-based authentication. Therefore, most efficient methods include a feature evaluation and selection process to extract the most distinctive features across a large population. Recently, model-based approaches have been gaining success for the user authentication task. However, several challenges should be tackled for efficient adoption, such as data collection size, training time, model size, and robustness against possible adversarial attacks.

User Verification: After the user enrollment, the system validates the legitimate user based on extracted features. The verification can be at the point of entry and continuously through the usage session. For continuous authentication, the user verification process occurs periodically to grant access to the legitimate user and to deny access to impostors. The frequency of verification should be carefully selected to allow sufficient biometric data acquisition and features extraction process and to manage energy consumption. Depending on the enrolment approach, the authentication algorithm follows a similarity-based or probability-based scheme for user validation. The similarity-based techniques are used for measuring the similarity of input data in comparison to a stored template for a certain user. Traditionally, the verification implies a match between a given data and a stored template to a certain degree. The authentication system is responsible for giving access to the legitimate user when presenting a biometric data that matches the supposed template with a similarity check higher than a predefined threshold. The threshold is for accounting for environmental and processing errors that could affect reading or calculating of the biometric data. Mathematically, a verification process can be viewed as $C = True$ if $f(x, y) \geq t$ and $False$ otherwise, where f is a similarity measurement between an input x and a template y, and t is a predefined threshold. The genuine match is shown when C evaluates to $True$ while the impostor match is when C is $False$.

Probability-based algorithms are used for model-based enrolment, where the authentication model signals a probability for granting access to the legitimate user based on the input data, the verification process is similar to the template-based algorithm, except for using a pretrained model for decision making. The decision of the model $C = True$ if $g(x) \geq th$ and $False$ otherwise, where g is the objective function of the probability-based algorithm and th is a predefined threshold. The user verification process runs periodically for continuous user authentication, however, the frequency f_{req} higher bound is limited by minimum verification time t_o, where $f_{\text{req}} = (1/t_o)$, and $t_o = t_d + t_p + t_c$, where t_d is the time needed to acquire sufficient data for verification, t_p refers to the time

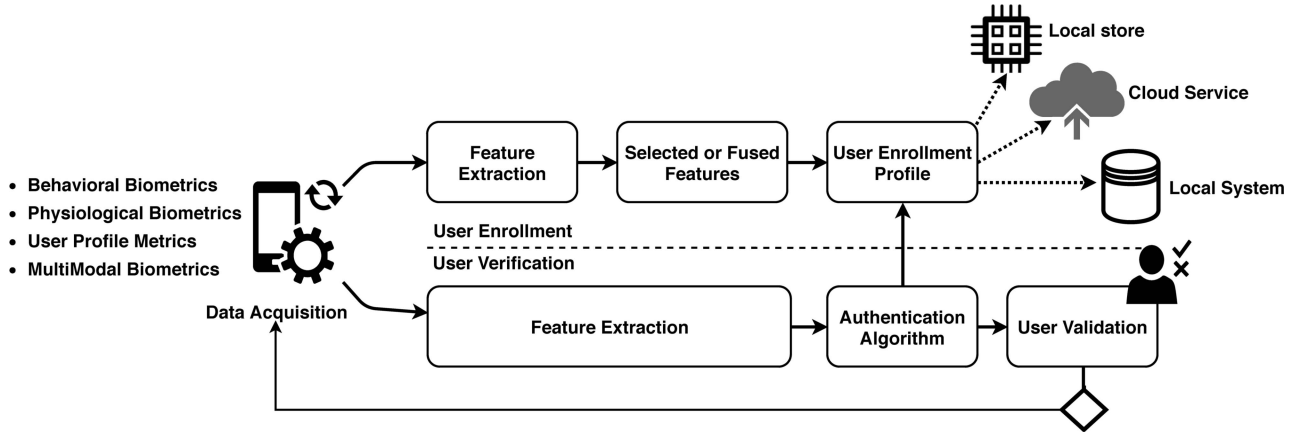

Fig. 3. General framework of the biometric-based authentication system. The framework includes two operations: 1) user enrollment and 2) user verification. Both operations require data acquisition and feature extraction. User enrollment includes modeling of the extracted data and storing while user verification feeds the extracted features to the authentication algorithm to grant access for legitimate users periodically.

required for data preprocessing, and t_c is classification period. While t_c can be mitigated by overlapping t_d and t_p with t_c, it should be taken into account the computational power and battery consumption needed for the verification process.

C. Authentication Evaluation Metrics

Biometric-based authentication systems are evaluated by their ability to be generalized to a large population. This emphasis becomes more obvious when addressing mobile security since the authentication system should account for a very large and different population. There are several evaluation metrics for evaluating authentication system performance. The three most common metrics are the false accept rate (FAR), the false reject rate (FRR), and the equal error rate (EER). For the authentication task on a mobile device, a false accept indicates that false access is granted to an intruder while a false reject indicates that the legitimate user is denied access to the device. FAR is represented as (*Number of False Acceptance/Total Number of Attempts*) and FRR is equal to (*Number of False Rejections/Total Number of Attempts*). The EER is where the FAR is roughly similar to FRR, and it is a very popular metric for interpreting system error.

Additional evaluation metrics for the authentication system include true positive rate, true negative rate, false positive rate, false negative rate, accuracy, precision, recall, and F1-score. The true positive rate and true negative rate indicate the rate of correctly validating a legitimate user and denying an impostor, respectively. The false positive rate and false negative rate are the rate of which the system denies access for the legitimate user and allows access for the impostor, respectively. Accuracy is the proportion of true positives and negatives to the overall tested data, including true positives, true negatives, false positives, and false negatives. Precision indicates how frequently the system correctly produces positive classifications, which is calculated as the ratio of true positives to both true and false positives. Recall indicates how frequently the system correctly validates positive data, which is calculated as the ratio of true positives to both true positives and false negatives.

D. Behavioral Biometrics and Smartphones' Capabilities

Behavioral biometrics enable efficient implementation of an authentication system that operates beyond the point-of-entry access and continuously authenticate users without explicitly asking their input. Therefore, behavioral biometrics improve mobile security by providing user continuous and transparent authentication process throughout the entire routine session. Various techniques have been proposed for mobile user authentication using behavioral usage and features by taking advantage of the embedded sensors. Using sensory data, a background process continuously and implicitly captures user's behavior to perform an active and transparent authentication, e.g., using motion patterns [28], [43]–[47], gait [35], [48]–[52], touch gestures [43], [53]–[57], electrocardiography (ECG) [33], keystroke dynamics [19], [55], [58], [59], voice [60]–[62], signature [63]–[65], and profiling [29], [31], [66].

Since today's smartphones are well equipped with a variety of embedded sensors, such as motion sensors (e.g., gravity, accelerometer, gyroscope, and magnetometer), environmental sensors (e.g., light, temperature, barometer, and proximity), and position sensors (e.g., GPS and compass), numerous studies have leveraged these sensors for user authentication [28], [31], [67], [68]. A study by Crawford *et al.* [69] shows that behavioral biometrics reduce the demand for legitimate authentication by 67% in comparison to knowledge-based methods, i.e., adding a remarkable improvement in usability. In terms of exploiting access privilege, the authors showed that an intruder could perform more than 1000 tasks if successfully gain access to a mobile device using a knowledge-based authentication scheme; however, the intruder can hardly achieve one task if the mobile device uses a multimodal behavioral biometrics-based method [69].

Smartphone Hardware and Software Capabilities: The rapid advancements in mobile technologies have increased the performance of smartphones by multiple folds in recent years. The computational capabilities of mobile devices, including multicore processors, GPUs, and Gigabytes of memory, are comparable to those of normal-use desktop computers.

Hardware acceleration units, which are available on most smartphones' chipset platforms, e.g., Qualcomm, HiSilicon, MediaTek, and Samsung, have enabled smartphones to run sophisticated applications that go far beyond the standard and built-in phone functions. Moreover, today's smartphones are equipped with a variety of sensors, e.g., motion sensors, environmental sensors, and position sensors, which can provide accurate usage profiling for enhanced user experience. While standard applications are no longer a challenge with such capabilities, there are many performance requirements and challenges related to adopting continuous behavioral-based authentication on smartphones, especially when using machine learning approaches. Such challenges include the following.

1) *OS-Related Development Tools:* The availability of such tools to access and take advantage of the embedded processing acceleration units plays a key role in developing continuous authentication methods. Most the of surveyed systems are implemented on Android-based platforms for the ease of access to a variety of developing tools. Studying the effects of the running OS system on obtaining and analyzing behavioral biometrics for continuous authentication is an interesting direction for future work that is out of the scope of this study.
2) *Machine Learning-Based Authentication:* While the current computational and memory power of smartphones allow for model inference, the enrolment phase can be a challenge and may require a server-side training phase. Through our survey of behavioral-based continuous authentication methods using different modalities, we highlight insights and challenges to advance the application of the addressed modality. We note that an efficient implementation of behavioral biometric-based authentication method should account for hardware- and software-independent operation and network connectivity differences to allow for successful system adoption [84].

Built-in Methods: Most of the built-in authentication methods are intended for point-of-entry level, as continuous implicit authentication is still evolving to meet a specific level of standards. To the best of our knowledge, and based on our survey, there has not been any commercial offering of a dedicated built-in continuous authentication method in customer-grade smartphones, making the development of such methods a possible gap to fill with research and development. We note the barrier to the mass production of built-in authentication capabilities in smartphones is that they need to meet a high standard of security (e.g., FAR of 0.01% in the European Union), which is not met by the current technology. In our survey, we highlight a variety of challenges that can be pursued to improve the current methods to rise to this level of standards. As standards are clearly outlined for point-of-entry authentication, there is still a lack of guidelines for adopting continuous behavioral biometrics as an integral component of the smartphone. However, many of the covered methods are applicable as a running application, given today's devices' resources, such as sensors, multicore processors, and GPUs.

III. Motion-Based Authentication

Most of today's mobile devices are equipped with motion sensors, such as accelerometers and gyroscopes, which can be a valid source for modeling users' behavior. The accelerometer provides the gravitational acceleration in three spatial dimensions (axes), x, y, and z, measured in meter per second squared, where the axes denote the vertical, and left-to-right dimensions [85]. The gyroscope measures the angular rotation in three dimensions, x, y, and z, in radians per second along the axes [76]. Such sensory data provide a feature space that enables modeling of users' movement and usage; therefore, a variety of methods revolve around utilizing such data for authentication and security.

Early exploitation of motion sensors includes air-written signatures [44], [77] for which the user holds the device and performs an air-written signature as the application is running and recording the user's motion. Traditionally, signatures are well-known behavioral biometric commonly used for conducting official or commercial transactions [86]–[88]. However, air-written signatures, while providing a valid method for user authentication, they operate as a point-of-entry authentication and fail to offer covert, transparent, or continuous authentication. Laghari *et al.* [44] showed that a motion-based signature had achieved a 1.46% FAR and 6.87% FRR when tested on a data set collected from motion sensors of ten participants' smartphones. While such methods are robust against shoulder surfing attacks [89], they: 1) require the user input and engagement once authentication is required; 2) fail to offer a continuous transparent authentication; and 3) are secret based and knowledge based since the user must memorize the used signature. Similar implementations include waving gestures [70], free-form gestures [76], and "picking-up" movement (i.e., picking the phone and raising it for answering a call) [71].

Ehatisham-ul Haq *et al.* [28] proposed a continuous authentication system that identifies mobile users based on their activity patterns using embedded sensors, i.e., accelerometer, gyroscope, and magnetometer. The authors reported an analysis of the system performance when the smartphone is placed at five different locations on the user's body. Amini *et al.* [67] introduced *DeepAuth*, an LSTM-based user authentication method, which uses sensory data extracted from the accelerometer and gyroscope to model users' behavioral patterns. The experiments, which were carried out on data collected from 47 users with 10–13 min each, have shown an average accuracy of 96.7% for 20-s authentication window. Zhu *et al.* [90] introduced a technique based on users' phone-skating behavior captured by motion sensors. The experiments reported an average EER of 1.2% using data of 20 users. Lee and Lee [81] introduced an SVM-based system for user authentication using readings from three motion sensors to achieve an average accuracy of 90% when using data collected from four participants.

Exploring the effects of using different sensory data augmentation process, Li *et al.* [82] examined five data augmentation methods to authenticate users with *SensorAuth*. The

TABLE III
SUMMARY OF THE RELATED WORK FOR MOTION-BASED USER AUTHENTICATION. EACH WORK IS IDENTIFIED BY THE USED MODALITIES, UTILIZED SENSORS, DATA SET, MODELING ALGORITHM, AND THEIR PERFORMANCE

Study	Modalities	Sensors	Methods	# Users	EER	FAR	FRR	TPR	Accuracy	Auth. Time	Platform
[70]	Motion Gesture	Ac	SVM	8	✗	3.67%	✗	✗	92.83%	✗	GoogleG3 (A-4.4)
[71]	Picking-up Motion	Ac, Gy, Ma	SVM	31	6.13%	✓	✓	✗	✗	✗	✗
[55]	Motion & keystroke	Ac, Gy, Pr	SVM	100	1.25%	✓	✓	✗	99.13%	✗	✗
[72]	Motion Gesture	Ac	SVM	8	✗	✗	✗	✗	95.83%	✗	GoogleNexus5 (A-4.0)
[73]	In-air Handwriting	LMC	SVM	100	0.6%	✓	✓	✗	✗	✗	✗
[74]	In-air Handwriting	Ac, Gy	RF	5	✗	✗	✗	✗	32.8†%	✗	LG R Watch (A-Wear)
[75]	Shacking Motion	Ac, Gy	DTW-LSTM	150	✗	0.1%	✗	✗	96.87%	✗	GoogleNexus4 (A-5.1)
[76]	Free-form Gesture	Ac, Gy	DTW	✗	3%	0.02%	10%	✗	✗	✗	SamsungGalaxyS3 (A-4.3)
[77]	In-air Handwriting	Ac	DTW*	34	2.5%	✓	✓	✗	✗	✗	✗
[78]	In-air Handwriting	Ac, Gy, Or	MLP	✗	✗	✗	✗	84.5%	✗	✗	GoogleNexus6 (A-7.1.1)
[44]	Pick-up Motion	Ac	CC	10	✗	1.46%	6.87%	✗	✗	✗	HTC-x
[79]	Motion Gesture	Ac, Gy	Naïve Bayes	10	✗	✗	✗	✗	83.6%	✗	MotorolaMotoG (A-10.0)
			k-NN	10	✗	✗	✗	✗	89.8%	✗	MotorolaMotoG (A-10.0)
			MLP	10	✗	✗	✗	✗	92.7%	✗	MotorolaMotoG (A-10.0)
			SVM	10	✗	✗	✗	✗	92.2%	✗	MotorolaMotoG (A-10.0)
[80]	Hand-movement	Ac, Gy	Naïve Bayes	50	✗	2%	✗	✗	89%	✗	✗
		Ma, Or, Gy	SVM	50	✗	18%	✗	✗	74%	✗	✗
			I-F	50	✗	0%	✗	✗	93%	✗	✗
[81]	Free motion	Ac, Ma, Or	SVM	4	✗	✗	✗	✗	90%	20s	GoogleNexus5 (A-4.4)
[28]	Free motion	Ac, Ma, Gy	SVM	10	✓	✗	✗	✓	97.95%	180s	SamsungGalaxyS2 (A-2.3)
[67]	Free motion	Ac, Gy	LSTM	47	✗	✓	✓	✓	96.7%	20s	GoogleNexus5X (A-8.1)
[82]	Free motion	Ac, Gy	SVM	100	8.33%	✗	✗	✗	✗	5s	SamsungGalaxyS4 (A-4.4)
[47]	Free motion	Ac, Gy, Ma	LSTM	84	0.09%	0.96%	8.08%	✓	97.52%	0.5s	✗
[83]	Eye movement	Ca	SVM	20	10.61%	✓	✓	✓	88.73%	10s	GoogleNexus4 (A-5.1)
[32]	Eye movement	Ca	SRC	30	6.9%	✓	✓	✓	93.1%	130s	RaspberryPi3ModelB

Ac: Accelerometer, Gy: Gyroscope, Ma: Magnetometer, Pr: Pressure, LMC: Leap Motion Controller, Or: Orientation, RF: Random Forest, SVM: Support Vector Machine, DTW: Dynamic Time Wrapping, LSTM: Long Short Term Memory, MLP: Multilayer Perceptron, CC: Cross-correlation, k-NN: k-Nearest Neighbor, I-F: Isolation Forest, SRC: Sparse Representation Classification.

overall results of *SensorAuth* have shown an EER of 4.66% when using a 5-s window.

Using different motion-based modality, Zhang *et al.* [32] introduced an eye movement-based implicit authentication method based on eye movement in response to visual stimuli when using a VR headset. The authors reported imposters' detection accuracy of 91.2% within 130 s. Song *et al.* [83] conducted a similar study on smartphones to track individual eye movement with the built-in front camera to investigate using gaze patterns for user authentication [83]. The authors reported an average system accuracy of 88.73% when tracking users' eye movement for 10 s.

The summary of the related work associated with motion-based user authentication is listed in Table III. In this table, the performance metrics and authentication time are reported based on the original referenced paper. We follow this approach for all the following tables. Most of the studies use embedded motion sensors, such as accelerometer, gyroscope, and orientation sensors. Using motion-based methods for user authentication allowed an authentication accuracy of up to 99.13% using SVM trained on sensory data collected from motion sensors [55].

Insights and Challenges: While motion-based user authentication methods can detect and classify legitimate users, it has been shown that using the motion-based authentication alone achieves a relatively lower accuracy (up to 96.87%) in comparison with methods that incorporate multiple modalities. For example, using the keystroke dynamics along with motion sensors, i.e., as an indication of active usage of the device, enables a higher authentication accuracy [55]. Note that some motion-based modalities, e.g., waving gestures, free-form gestures, motion-based signature, and in-air writing, fail to offer a covert continuous authentication. Therefore, numerous studies have explored other modalities that rely on behavioral biometrics captured by the motion sensors and wearable devices to implement a transparent continuous authentication. Handling information from multiple sensors and sources, e.g., wearable devices, for an implicit authentication is a challenging task that requires several on-device data preprocessing techniques, temporal data alignment, and accurate modeling and matching.

Common open challenges of using motion-based continuous authentication on smartphones include the following.

1) *Power Consumption:* Intuitively, continuous authentication schemes, in general, consume power. This consumption is due to multiple processing components of the adopted method, data collection and sampling, feature extraction, model inference, and matching algorithms. For example, a study by Lee and Lee [68] shows that continuously querying of sensors data at a 50-Hz sampling rate for 12 h can consume up to 5% of the battery life even without active usage (i.e., the device is locked). Using a higher sampling rate can result in significantly higher power consumption [68], [107]. Note that power consumption varies from a device to another, considering the hardware configurations and processing units. For example, a study by Zhu *et al.* [107] shows that the power consumption of running *RiskCog* for 3 h with a 50-Hz data sampling rate on three devices as follows: Samsung N9100 (4.4%), Sony Xperia Z2 (3.6%), and MI 4 (4.2%).
2) *Computation and Memory Overhead:* Motion-based continuous authentication requires continuous collection and processing of data as well as high-frequency authentication via model or matching algorithm inference.

Moreover, data records within the collection timeframe and predefined operational thresholds increase the memory overhead. Optimizing the computational and memory requirements for motion-based schemes is considered an open challenge.

3) *Adversarial Attacks:* Motion-based authentication schemes can be vulnerable to attacks, including observation-based attacks (e.g., observing and reproducing in-air handwriting and gestures) [108]–[110] and sensor-based inference attacks (e.g., sensor-based side-channel inference attacks) [111]–[115]. While behavioral biometrics can be accurately captured by sensors, sensors' data can be collected by a variety of applications that may present a threat to the adopted modality. Addressing such attacks is an interesting and open research direction.

IV. Gait-Based Authentication

Gait recognition has gained increased interest in recent years, especially with the vast adoption of mobile and wearable sensors. Gait recognition is defined as the process of identifying an individual by the manner of walking using computer vision and/or sensory data collected from environmental and wearable sensors [116]. Computer vision approaches for gait recognition include segmenting the individual's images while walking and capturing the features that enable accurate recognition [91]. While using sensory data, including: 1) adopting floor sensors, where the gait-related features are captured once the person walks on them [92], [93] and 2) adopting wearable sensors, which aims to collect information that enables gait recognition [92]. For mobile security and authentication, gait recognition is usually done using wearable sensors, especially the reading of the motion sensors (e.g., accelerometer) of the mobile device, to enable continuous transparent authentication.

The general approach to gait recognition includes four steps: 1) data acquisition step in which the device is placed in a certain way that enables the walk activity recording; 2) data preprocessing step for reducing the introduced noise by the data collection method or other environmental factors; 3) walk detection step using either traditional cycle or machine learning techniques; and 4) analysis step [85]. Handling the data acquisition process requires accurate readings from motion sensors as the user places the device in a predefined manner, such as carrying the device inside of a pouch [99], in the pants pocket [85], [100], or in hand [101]. The studies conducted for mobile security using gait-based biometrics usually include data collection from a population of size equal to or less than 50 participants [99]–[101], and processed in controlled conditions to minimize the effects of outside factors [102]. Even though some studies have attempted to capture gait-related metrics from a real-world collection of sensory data, such as the study by Nickel and Busch [102], generally, the data collection requires an ideal setting at least in one aspect (e.g., walking patterns or floor condition) [3].

The second step after acquiring the data, the preprocessing step takes place to clean, reduces the noise, and normalizes the data. The major task in this regard is the noise reduction considering various possible noise sources, such as environmental and gravitational factors, floor conditions, and the users' shoes or other wearable materials. Since the gait-related features rely heavily on readings from motion sensors, such as the accelerometer, which are very sensitive, the adopted method should account for further noise [100]. Such noises can be handled using linear interpolation and filtering techniques, while environmental noise adds much complexity to the walk detection task, which can be minimized using activity recognition to remove any irrelevant data [99]. For the walk detection, cycles (i.e., the time between two paces bounded by maximum and minimum threshold across the three axes) or machine learning techniques are both utilized in the literature. Cycle-based approaches are commonly used since the average cycle length is easily and simply calculated to detect cycles by moving forward or backward in intervals of the average cycle length with some correction measurement. On the other hand, machine learning-based approaches have shown to be accurate for automatic walk detection [102]. Such techniques require: 1) data collection module for sensory data readings; 2) data preprocessing stage for handling and reducing possible noise; and 3) walk detection model.

The final step of gait recognition is the analysis of time intervals, frequencies, or both. Using time intervals analysis, some metrics can be extracted and studied, such as cycle statistics, including the minimum, average, and maximum acceleration values, and cycle lengths and frequencies. Moreover, cycle variance and stability are measured by acceleration moments [85], [116]. Using frequency analysis, usually conducted using discrete or fast Fourier transforms, it has been shown that the first few coefficients resulting from each conversion are highly relevant for detecting distinctive gait patterns [85].

Wang *et al.* [91] and Gafurov and Snekkenes [92] used a *k*-NN model to classify legitimate users using gait-based features, where Wang *et al.* used the camera to capture the user movement, and Gafurov *et al.* captured the user movement using cyclic rotation metric device attached to different places of the body (ankle, hip, pocket, and arm). Both studies achieved an accuracy of above 85%, with EER of 3.54% and 5%, respectively. Multiple studies used accelerometer as a standalone sensor to capture user movement for user authentication task [85], [94]–[102].

Both Thang *et al.* [94] and Hoang *et al.* [95] collected data of 11–14 users and used SVM-based models for capturing user patterns, achieving nearly the same accuracy of 92%. In addition, Hoang *et al.* [100] achieved an EER of 3.5% by using a fuzzy commitment algorithm on a study sample of 38 users, outperforming its counterparts. Others [103]–[106] incorporated different sensors to capture the motion aspects of the users, achieving an accuracy of up to 96% by using accelerometer, gyroscope, compass, piezoelectric energy harvester, and electromagnetic energy harvester [103]. The summary of the gait-based user authentication methods is shown in Table IV.

Insights and Challenges: Similar to motion-based user authentication methods, gait-based methods do not achieve a high relative accuracy nor precision in user authentication

TABLE IV
SUMMARY OF THE RELATED WORK FOR GAIT-BASED USER AUTHENTICATION. EACH WORK IS IDENTIFIED BY THE USED MODALITIES, UTILIZED SENSORS, DATA SET, MODELING ALGORITHM, AND THEIR PERFORMANCE

Study	Modalities	Sensors	Methods	# Users	EER	FAR	FRR	TPR	Accuracy	Auth. Time	Platform
[91]	Gait	Camera	k-NN	20	3.54%	✓	✓	✗	87.5%	✗	✗
[92]	Gait	MRC – ankle	k-NN	21	5%	✓	✓	✗	85.7%	✗	✗
		MRC – hip	k-NN	100	13%	✓	✓	✗	73.2%	✗	✗
		MRC – pocket	k-NN	50	7.3%	✓	✓	✗	86.3%	✗	✗
		MRC – arm	k-NN	30	10%	✓	✓	✗	71.7%	✗	✗
[93]	Gait	FSR	FLD	10	✗	5.07%	✗	✗	88.8%	0.127s	ComputerSimulation
[85]	Gait	Ac	Guidelines	✗	✗	✗	✗	✗	✗	✗	✗
[94]	Gait	Ac	SVM	11	✗	✗	✗	✗	92.7%	✗	GoogleNexusOne (A-2.1)
[95]	Gait	Ac	SVM	14	✗	✗	✗	✗	$91.33 \pm 0.67\%$	✗	LGOptimusG (A-4.1.2)
[96]	Gait	Ac	CC	36	7%	✓	✓	✗	✓	✗	✗
[97]	Gait	Ac	DTW-SVM	51	33.3%	✓	✓	✓	53%	✗	GoogleG1 (NA)
[98]	Gait	Ac	CRM	48	21.7%	✓	✓	✓	53%	30s	MotorolaMilestone (A-2.2)
[99]	Gait	Ac	k-NN	36	8.24%	✗	✗	✗	✗	1.7m	MotorolaMilestone (A-2.2)
[100]	Gait	Ac	FC	38	3.5%	0	16.18%	✗	✗	✗	✗
[101]	Gait	Ac–In-hand	CC	31	17.2%	✗	✗	✗	✗	✗	✗
		Ac–Chest	CC		14.8%	✗	✗	✗	✗	✗	✗
		Ac–Hip	CC		14.1%	✗	✗	✗	✗	✗	✗
		Ac–In-hand	FFT		14.3%	✗	✗	✗	✗	✗	✗
		Ac–Chest	FFT		13.7%	✗	✗	✗	✗	✗	✗
		Ac–Hip	FFT		16.8%	✗	✗	✗	✗	✗	✗
[102]	Gait	Ac	HMM	48	6.15%	✓	✓	✓	✗	33s	MotorolaMilestone (A-2.2)
[103]	Gait	Ac, Gy, Co, PEH, EEH	PMSSRC	20	6–12.1%	✓	✓	✓	96%	1.6ms	SensorTag (Contiki-3.0)
[104]	Gait	Ac, Gy, Camera	Matching	10	✗	✓	✓	✓	91%	15-75s	ComputerSimulation
				20	20.8%	✓	✓	✓	81.3%		
				30	✗	✓	✓	✓	✗		
[105]	Gait	Ac, Gy, Ma	SVM & RF	50	✗	✗	✗	✗	✓	6.4s	GoogleNexus5 (A-4.4)
[106]	Gait	Ac, Gy, Ma	CC–FC	15	5.5%	✓	✓	✗	95%	12s	ComputerSimulation

MRC: Cyclic Rotation Metric, FSR: Force Sensing Resistor, Ac: Accelerometer, Gy: Gyroscope, Co: Compass, PEH: Piezoelectric Energy Harvester, EEH: Electromagnetic Energy Harvester, Ma: Magnetometer, SVM: Support Vector Machine, RF: Random Forest, DTW: Dynamic Time Wrapping, CC: Cross-correlation, k-NN: k-Nearest Neighbor, FLD: Fisher Linear Discriminant, CRM: Cyclic Rotation Metric, FC: Fuzzy Commitment, FFT: Fast Fourier Transform, HMM: Hidden Markov Model, PMSSRC: Probability-based Multi-Step Sparse Representation Classification.

tasks. Generally, gait-based user authentication methods are feasible in specific applications, which requires capturing the user's gait traits while moving, e.g., player detection in a team-based sport via wearable sensing devices. Applying gait-based authentication for smartphone users requires addressing a variety of challenges, such as the following.

1) *Data Sources:* Collecting gait-related sensory data requires visual information as well as motion information from multiple sensors.
2) *Sensors Placement:* As changing the placement of the device can significantly change the sensory readings.
3) *Adopting Alternatives:* As gait-based authentication fails to provide continuous authentication when the user is not moving.
4) *Usability:* As the user state at the enrollment stage may differ from the state the inference stage. Moreover, the gait-based traits are highly dependent on the user's physical state when capturing the data. Such challenges may explain the relatively low accuracy of the gait-based authentication methods.

V. KEYSTROKE-BASED AUTHENTICATION

One of the earliest behavioral authentication methods is based on studying the keystroke dynamics. Most keystroke dynamics-based methods are cost effective and do not require additional modules to operate [24]. During the usage of the device, when a key input is required (e.g., texting), the keystroke dynamics-based authentication method continuously validates the user since behavioral dynamics can be distinctive across users. Conducting authentication via keystroke dynamics requires analyzing and capturing the distinctive features and patterns of users' keystrokes when using the device [22], [23]. Common features include: 1) keypress frequency, which calculates the frequency of keypress events; 2) key release frequency, which calculates the frequency of key release events; 3) latency and hold time, which calculates the rates of press-to-press, press-to-release (which is also known as the hold time), release-to-release, and release-to-press events; 4) finger's pressure while touching the screen; 5) pressed area size by the user's fingers; and 6) error rate, which is the frequency of using backspaces or deletion option.

Using keystroke dynamics for authentication or user validation has been adopted on traditional computers before their application to smartphones [117]. Even though it seems to be an easier task to implement a keystroke dynamics-based authentication on computers due to the less complex feature space, Joyce and Gupta [118] showed the uniqueness of both written signatures and typing behavior is originated from the physiology of the neurological system.

The recent application of keystroke dynamics takes advantage of embedded sensors (e.g., motion sensors on smartphones) to improve the authentication accuracy, especially when the key-based input is unavailable there [114], [128]. Another distinction between applying keystroke dynamics-based methods on smartphones and computers is the large space of key-based input in the smartphone since it includes touches and swipes that are meant for interacting with the applications without typing textual content [119]. Several studies have addressed the generalization of these methods to different types of input. For instance, McLoughlin *et al.* [119] showed that using key press and release frequencies and the

TABLE V
SUMMARY OF THE RELATED WORK FOR KEYSTROKE DYNAMICS-BASED USER AUTHENTICATION. EACH WORK IS IDENTIFIED BY THE USED MODALITIES, UTILIZED SENSORS, DATA SET, MODELING ALGORITHM, AND THEIR PERFORMANCE

Study	Modalities	Sensors	Methods	# Users	EER	FAR	FRR	TPR	Accuracy	Auth. Time	Platform
[117]	Keystroke Dynamics	NA	k-NN	63	✗	✗	✗	✗	83.22–92.14%	✗	✗
[118]	Keystroke Dynamics	NA	Matching	33	✗	0.25%	16.36%	✗	✗	✗	✗
[119]	Keystroke Dynamics	NA	Distance & CI	3	✗	✓	✓	✗	✗	✗	RenesasH8S-2377
[120]	Keystroke Dynamics	NA	RBFN	25	✗	36%	26.6%	✗	✗	✗	✗
			Fuzzy	25	✗	18.6%	19%	✗	✗	✗	✗
			PSO-Fuzzy	25	✗	8.09%	7.58%	✗	✗	✗	✗
			GA-Fuzzy	25	✗	8.79%	7.94%	✗	✗	✗	✗
			PSO-GA Fuzzy	25	✗	2.07%	1.73%	✗	✗	✗	✗
[121]	Keystroke Dynamics	NA	Distance	15	✗	12.97%	2.25%	✗	✗	✗	✗
[122]	Keystroke Dynamics	NA	Distance	25	4%	✗	✗	✗	✗	632-2151ms	SamsungSCH-V740 (NA)
[123]	Keystroke Dynamics	NA	SVM	10	✗	✗	✗	98.7%	98.6%	✗	✗
[124]	Keystroke Dynamics	Ac, Gy	k-NN	20	0.08%	✗	✗	✗	✗	200ms	✗
[125]	Keystroke Dynamics	NA	MLP	32	✗	6.33%	4.89%	95.11%	94.81%	✗	SamsungGalaxyS5 (A-4.4.2)
[19]	Keystroke Dynamics	NA	SVM	24	1.42%	2%	1%	99%	99%	✗	SamsungGalaxyS5 (A-4.4.2)
[126]	Keystroke Dynamics	Ac	SVM	5	5.1%	✗	✗	✗	97.9%	✗	HuaweiP10 (A-7.0)
[127]	Keystroke Dynamics	NA	DAE-SR	10	5%	✗	✗	91.8%	95%	✗	✗
[43]	Keystroke Dynamics	NA	MLP	13	✗	14%	2.2%	✗	86%	✗	✗
[58]	Keystroke Dynamics	NA	MCF	64	✗	✗	✗	✗	89.7%	✗	✗

Ac: Accelerometer, Gy: Gyroscope, CI: Confidence Interval, RBFN: Radial Basis Function Network, PSO: Particle Swarm Optimization, k-NN: k-Nearest Neighbor, GA: Genetic Algorithm, DAE-SR: Deep Auto Encoder and Softmax Regression, MCF: Multi-Classifier Fusion, SVM: Support Vector Machine, MLP: Multilayer Perceptron.

latency between two presses contribute greatly to establishing distinctive keystroke behavior for users. The authors showed that the application should account for the inconsistencies in recorded data by introducing weights based on the variance of data (i.e., lower variance gets higher weights). Their results show an accuracy of more than 90%, establishing the validity of using keystroke dynamics as a biometric for authentication with minimal computational overhead and increased usability.

Buriro *et al.* [129] designed an authentication scheme based on the user's hand movements and timing features as they enter ten keystrokes. The authors conducted experiments using data collected from 97 participants and reported an authentication accuracy of 85.77% and FAR of 7.32%. Similarly, Zahid *et al.* [120] studied the keystroke behavior of 25 users including features, such as the hold time, error rate, and latency. The authors suggested a fuzzy classifier to account for the diffused features space and argued that presenting the classification task of keystroke behavior as an optimization problem benefits the robustness of the model when compared to similarity-based methods [121]. Using a fuzzy classifier with particle swarm optimization and genetic algorithms, their proposed method showed 0% FRR and 2% FAR, suggesting high security and usability potential. However, keystroke dynamics are often incorporated with other modalities for improving performance and accuracy. For instance, Hwang *et al.* [122] suggested, including rhythm and tempo as components for studying keystroke dynamics, i.e., a user is required to follow a distinct and consistent timing pattern for accurate keystroke-based authentication. For example, a given term can be entered digit by digit separated with subsequent short and long pauses that are controlled by tempo cues, e.g., a metronome for counting pause intervals. In their study, the authors showed an average improvement of about 4% in the EER evaluation metric when using artificial rhythmic input with tempo cues in comparison to natural rhythms. However, adopting such methods adds complexity to the usability aspect.

Using smartphone-embedded sensors to support keystroke dynamics-based authentication has been repeatedly suggested to improve the performance and to provide transparent authentication. Wu *et al.* [123] proposed incorporating velocity-related metrics to reach an accuracy of 98.6% for classifying data from ten users using an SVM classifier. Similarly, Giuffrida *et al.* [124] proposed incorporating keystroke data with motion sensors data, namely, accelerometer and gyroscope, to conclude that metrics obtained from the accelerometer data are more useful than those obtained from the gyroscope. The authors showed that combining features from motion sensors with keystroke metrics provides similar results as adopting only the motion sensors-related features alone, i.e., the study shows that sensor-related features can be more useful than keystroke dynamics in terms of authentication. However, obtaining and analyzing high-frequency sensory data can be power consuming. Table V shows a list of authentication methods based on keystroke dynamics. The proposed approaches show a promising direction for using this modality for user authentication, achieving an accuracy of up to 99% by Cilia and Inguanez [19].

Insights and Challenges: Keystroke dynamics-based methods have several advantages, such as: 1) their high authentication accuracy that can reach up to 99%; 2) high power-efficiency in comparison with other methods; and 3) hardware independence since these methods can operate with either physical or on-screen keyboards. However, implementing a keystroke dynamics-based approach can be challenging for several reasons.

1) *User Behavioral Changes:* Capturing keystroke dynamics as a behavioral modality under uncontrolled conditions, e.g., user's activity (standing, walking, etc.), user's emotional or physical state change, and the in-use application, is challenging and requires testing under these nontrivial scenarios.
2) *Feature Extraction and Selection:* The extracted metrics should be robust against noise and behavioral changes. Considering the limited space of features, recent studies

have considered incorporating other modalities to extend the feature space, thus allowing for the selection of a distinctive user representation that can be generalized to a relatively large population.

3) *Adopting Alternatives:* Since these methods operate only when the user interacts with the keyboard, the implicit authentication module should allow for possible alternatives when the user uses the device without typing (e.g., watching a video, placing a call, etc.). Other challenges can be related to typing with different languages and whether the user's typing behavior changes across languages, which require further attention through further research.

VI. Touch Gesture-Based Authentication

Using touch gestures as a biometric modality extend the landscape of transparent authentication applications to include a variety of devices with touchscreen unit (e.g., smartwatches, digital cameras, navigation systems, and monitors) [3]. Several studies have investigated the touch gestures as a behavioral biometrics for continuous authentication since it can be convenient and cost-effective. Touch gestures include swipes [130], [147], flicks [131], [132], [135], slides [133], and handwriting [148]. The distinction between keystroke dynamics and touch gestures can be summarized in the input form for users and the method of input. The commonalities between the two modalities are the space of improvement when accounting for motion sensors [131], [134]. Therefore, many studies have incorporated motion-based features to gesture-based methods [135]. Considering features from touch gestures enables accurate authentication with an accuracy reaching 99% and minimal EER such as 0.03% when applying the *k*-nearest neighbor classifier or other distance-based classifiers [134].

Leveraging the abundance of information generated by the operating system of smartphones, a large number of features can be extracted from touch gestures such as reading from the accelerometer, pressure, gravity, velocity, touch area, and time-related measurements. Such features allow for accurate calculation of the gesture statistics and developing patterns for user authentication [115], [136]–[139]. Antal and Szabó [140] extended the feature space of swipe gestures to include touch duration, trajectory length, acceleration, average speed, touch pressure, touch area, and gravity readings. Using data from 40 users, including 58 samples, the authors performed one- and two-class classifications using multiple classifiers, such as Bayes Net, *k*-nearest neighbor, and random forests. The authors reported that random forests showed an EER of 0.004%. Their results showed that the device motion and positioning are important factors in distinguishing users.

Since touch gestures are commonly known as soft biometrics that could enable the recognition of gender and proportional measures such as physical attributes, including hand size, forearm length, and height, they are beneficial in criminal investigations. Miguel-Hurtado *et al.* [149] proposed studying the swipe gesture for gender prediction using a variety of features, including the swipe's length, width, touch area, pressure, velocity, acceleration, start-to-end angle, and others. The authors showed that applying a multilinear logistic regression classifier for gender prediction achieves an accuracy of 71% when the direction of the swipe is down to up. Using a fusion of swipe direction-based decision, the accuracy reaches 78%. Similarly, Bevan and Fraser [150] investigated the relationship between swipe gestures, thumb length, and gender. Using data from 178 users performing one-hand gestures using the thumb, the authors collected 21 360 samples of swipes in various directions. Among the calculated features, the results showed a strong correlation between thumb length and gestures, and they reflected in the velocity, acceleration, and completion time. Moreover, the study also showed that male users completed the gestures at a higher speed than female users.

The landscape of using touch gestures as behavioral biometrics for user authentication includes devices designed for users with disabilities. For example, Azenkot *et al.* [151] proposed PassChords, which was designed for authenticating users with vision impairments using a predefined sequence of screen taps. Another application is proposed by Zaliva *et al.* [53] for users with finger injuries, which uses the finger's trajectory and posture before touching the screen using its positioning and proximity. For this application, the direct touch gesture (i.e., the contact with the screen) is not fully required, and only the proximity-related measurement is possibly feasible to authenticate users.

Several studies have shown that gesture-based authentication schemes are application dependent, and gesture-based data can vary significantly from one application to another, which makes the generalization aspect of gesture-based schemes for continuous authentication across different applications is limited [141]–[143], [152]. Therefore, a "context-aware" approach is a potential solution to generalize gesture-based methods. Khan and Hengartner [12] showed that the performance of gesture-based methods could be improved by allowing context-aware implementation, where different applications control the tuning of features. To this end, the authors used the Kullback–Leibler (KL) divergence metric, which is shown to differ by application indicating the importance of accounting and tuning the features based on the used application. Using data of 32 users who were instructed to use four different applications during the data collection process, the experimental results showed that using the "context-aware" approach improves the accuracy of the device-centric approach.

Table VI shows a list of proposed gesture-based authentication methods using varieties of touch gestures and machine learning models. Random forest, in particular, is among the top achieving and adopted models in this modality-based method, with an accuracy above 99% as shown in [145] and [53].

Insights and Challenges: Similar to keystroke dynamics-based methods, gesture-based authentication methods have several advantages, including: 1) their high authentication accuracy, which can reach up to 99.9%; 2) operating efficiently in terms of both power and computation; and 3) conveying high resilience against mimicry attacks since gesture-based modality incorporates multiple independent features, restricting the ability of an impostor to successfully reproduce one

TABLE VI
SUMMARY OF THE RELATED WORK FOR GESTURE-BASED USER AUTHENTICATION. EACH WORK IS IDENTIFIED BY THE USED MODALITIES, UTILIZED SENSORS, DATA SET, MODELING ALGORITHM, AND THEIR PERFORMANCE

Study	Modalities	Sensors	Methods	# Users	EER	FAR	FRR	TPR	Accuracy	Auth. Time	Platform
[130]	Swipe Gesture	NA	ANN-CPANN	71	✗	0.08%	0	✗	✗	✗	✗
[131]	Flick Gesture	AC, Gy	SOM	NA	✗	✗	✗	✗	92.8%	✗	✗
[132]	Flick Gesture	Or	k-NN	16	6.85%	✓	✓	✗	✗	<100ms	HTCWildfire (A-2.2)
[133]	Slide Gesture	NA	SVM	60	0.01–0.02%	0.03%	0.05%	✗	✗	0.3s	MotorolaME525 (A-2.2)
[134]	Swipe Gesture	Ac, Or	MHD	104	0.31%	✓	✗	✓	✗	✗	SamsungGalaxyS2 (A-2.3)
			DTW	104	1.55%	✓	✗	✓	✗	✗	SamsungGalaxyS2 (A-2.3)
[135]	Flick Gesture	Ac	Naïve Bayes	10	✗	1.3%	8%	92%	98%	✗	HTCDesire600 (A-4.3)
[136]	Touch & keystroke	NA	k-NN	10	1%	✗	✗	✗	99%	20ms	SynapticTouchpad (NA)
[137]	Keystrokes/Touch/Handwriting	NA	SVM-RBF	32	0.75–8.67%	✗	✗	✗	✓	✗	SamsungGalaxyS2 (A-4.1.2)
[138]	Gesture	NA	MGGM	20	✓	✗	✗	✗	89%	53ms	GoogleNexus4 (A-4.3)
[139]	Gesture	NA	PSO-RBFN	20	8.1%	2%	8.2%	✗	✗	✗	SamsungGalaxyS2 (A-4.0.1)
[140]	Swipe Gesture	Or	RF	40	0.2%	✗	✗	✗	✗	✗	GoogleNexus7 (A-4.1.2)
[53]	Touch Gesture	NA	RF	14	✗	✗	✗	99.9%	99.9%	12.6s	SamsungGalaxyS4 (A-4.4)
[141]	Swipe Gesture	NA	RF	34	16.22–22.94%	✗	✗	✗	✗	✗	✗
[142]	Touch Gesture	NA	DTW-k-NN	23	✓	✗	✗	91%	✗	✗	SamsungGalaxyS3 (A-4.3)
[143]	Touch Gesture	NA	RF	71	1.8%	0.1%	18.52%	✗	✗	0.77s	HuaweiAscendMate (A-4.4)
[144]	Touch Gesture	NA	RF	71	5.4%	✗	✗	✗	✗	✗	SamsungTab210 (A-4.1)
[145]	Touch Gesture	NA	RF	NA	✗	2.54%	1.98%	✗	99.68%	✗	✗
[146]	Touch Gesture	NA	Matching	30	✗	✗	✗	93.01%	93.76%	✗	✗

Ac: Accelerometer, Gy: Gyroscope, Or: Orientation, ANN: Artificial Neural Network, CPANN: Counter Propagation Artificial Neural Network, RBFN: Radial Basis Function Network, SOM: Self Organizing Maps, k-NN: k-Nearest Neighbor, SVM: Support Vector Machine, MHD: Modified Hausdorff Distance, RF: Random Forest, DTW: Dynamic Time Wrapping, RBF: Radial Basis Function, MGGN: Multivariate Gaussian Generative Model, PSO: Particle Swarm Optimization.

feature given another. Moreover, using a high sampling rate (i.e., small timeframe) makes it difficult to observe and replicate the touch gestures. However, several challenges should be considered, including understanding users' temporal behavioral changes, application preferences, users' activity, users' mobility, etc.

VII. VOICE-BASED AUTHENTICATION

Speaker identification using voice-related features has been investigated extensively in [25] and [86]. Voice-related features combine both physiological aspects (e.g., vocal tract and lips characteristics) and behavioral traits (e.g., emotion- or age-related tones), allowing the speak/voice analysis over large feature space [161]. Based on [162], there are two approaches for using voice to authenticate/identify the speaker, which are as follows.

1) Text-dependent approach, in which users are authenticated based on the matching of speaking a predefined phrase. Since the users speak a certain phrase for authentication, this method is straightforward and very accurate. However, it does not allow for transparent or continuous authentication, and it is not a secret-based method.
2) Text-independent approach, in which users are authenticated based on features extracted from the voice regardless of the spoken words. This approach allows higher flexibility, especially in offering transparent authentication, where users are unaware of the service. However, accurate text-independent authentication accuracy faces different challenges due to the dynamic changes in the feature space of voice input accounting for the user condition and other environmental factors.

Speaker recognition using voice features follows the typical pattern recognition system, starting from data collection and preprocessing, going through the feature extraction and selection, and ending with the modeling and pattern recognition. Similar to conventional machine learning-based systems, the quality of features contributes considerably to the accuracy of speaker recognition. Such features include short-term spectral features, temporal and rhythmic, voice source, prosodic, and conversation-level features [3]. Short-term spectral characteristics represent the resonance attributes of the vocal tract and are often extracted with high frequency from 20- to 30-ms timeframes. Prosodic and temporal traits include intonation and rhythmic patterns extracted from long timeframes. Conversation-level features are high-level properties extracted from the textual contents of spoken words, such as word or phrase frequencies.

The quality of features is measured by their distinctive nature and their robustness against possible introduced noise (e.g., the user condition and environment) [163]. In this regard, a study by Reynolds [162] showed that spectral features provide high-quality, simple, and discriminative feature space.

Using the extracted features, a variety of models are utilized for voice/speaker recognition, such as SVM and Gaussian mixture models [163]. Early applications for voice recognition include access control, personalization, and forensic and criminal investigations [162]. The application landscape has increased to include online banking (i.e., conducting a transaction via voice communication as the voice recognition system transparently and continuously authenticates the customer) [3]. While voice-based user authentication methods capture the voice using the microphone, different works can be distinguished by data preprocessing and the utilized machine learning algorithm. Zhang *et al.* [154] achieved an accuracy of 99.34% with EER and FAR of 1% using the cross-correlation method with an authentication time of half a second on a sample size of 21 users. Additionally, using the Gaussian mixed model, Kim and Hong [158] and Johnson *et al.* [159] achieved similar EER of around 6% on a sample size of 50 and 48, respectively. Similarly, Lu *et al.* [155] achieved an accuracy of 95% and TPR of 99% in conducting user authentication tasks using the Gaussian mixed model with a sample size of 104 users. Multiple machine learning methods may be incorporated for user authentication tasks, Wang *et al.* [156] used principle

TABLE VII
SUMMARY OF THE RELATED WORK FOR VOICE-BASED USER AUTHENTICATION. EACH WORK IS IDENTIFIED BY THE USED MODALITIES, UTILIZED SENSORS, DATA SET, MODELING ALGORITHM, AND THEIR PERFORMANCE

Study	Modalities	Sensors	Methods	# Users	EER	FAR	FRR	TPR	Accuracy	Auth. Time	Platform
[153]	Voice	Ca, Mi	Matching	27	✗	✗	3%	✗	93%	< 24.7s	iPhone5S (iOS7)
[154]	Voice	Sp, Mi	CC	21	1%	1%	✗	✗	99.34%	0.5s	SamsungGalaxyNote5 (A-6.0)
[155]	Voice	Sp, Mi	GMM	104	✗	✗	✗	99%	95%	✗	SamsungGalaxyS6 (A-5.0)
[156]	Voice	Mi	PCA-SVM	18	5.4%	2%	✗	93%	93.5%	✗	ComputerSimulation
[157]	Voice	Mi	DTW	15	✗	1%	15%	✗	88.6%	✗	XiaomiRedmiNote3 (A-5.5)
[62]	Voice	Mi	HMM	54	21.58%	✗	✗	✓	✗	0.07s	SamsungGalaxyS5 (A-4.4)
[158]	Voice	Mi	GMM	50	6.24%	✓	✓	✗	✗	10.76s	ComputerSimulation
[159]	Voice	Mi	GMM	48	6%	✓	✓	✗	✗	✗	ComputerSimulation
[160]	Voice	Mi	Similarity	12	1.01%	1%	✗	99%	99.3%	✗	SamsungGalaxyNote3 (A-6.0)

Ca: Camera, Mi: Microphone, Sp: Speaker, GMM: Gaussian Mixed Model, PCA: Principle Component Analysis, CC: Cross-Correlation, SVM: Support Vector Machine, DTW: Dynamic Time Wrapping, HMM: Hidden Markov Model.

components analysis with support vector machine to train data collected from 18 users, achieving an EER of 5.4% and the overall accuracy of 93.5%. Using a simple approach may outperform powerful machine learning algorithms in user authentication tasks, as Zhang *et al.* [160] achieved an accuracy of 99.3% with EER of 1.01% and FAR of 1% using the sample similarity method. Table VII shows several voice-based user authentication methods. The listed voice-based methods show the validity of using this modality for the user authentication task.

Insights and Challenges: The high availability of voice recognition systems enables simple and accurate implementation of voice-based authentication schemes. However, there are many shortcomings when relying solely on the voice-based modality for user authentication. Therefore, many studies have employed voice in multimodal authentication approaches [18], [62], [65], [158], [164]. These shortcomings include the following.

1) *Background Noise:* Voice samples captured by mobile devices usually contain noises, considering the mobility and uncontrolled environmental conditions.
2) *User Physical and Emotional State:* Changes in the voice caused by emotions or illness (i.e., throat-related conditions) may affect the performance of the system.
3) *Adversarial Attacks:* The rise of adversarial examples suggests the possibility of successfully crafting samples to fool the authentication model and force it to grant access to imposters.
4) *System Overhead:* Continuous voice-based user authentication methods require voice commands and signatures to be captured and analyzed periodically through a sophisticated system with multiple stages that include data collection, noise reduction, and voice recognition. Such processes introduce overhead in terms of both power and computation.
5) *Usability:* Considering the user and environmental changes and the variety of possible noise sources, voice-based methods may result in high false acceptance and false rejection rates. Depending on the sampling rate, the high false rejection rates can degrade the usability and user experience. All of those issues require further attention through additional research efforts.

VIII. MULTIMODAL AUTHENTICATION

Multimodal authentication systems have become increasingly popular since relying on multiple modalities on offer robust and accurate results in comparison to unimodal systems, which consider only a single biometric modality. Such systems offer hardened security, especially against adversarial attacks, and deliver a flexible method for authentication considering possible changes of the input data that result in problems in the enrollment and validation phase [86], [182].

The implementation of multimodal authentication could require a fusion of multiple data sources, extracted features, or/and used algorithms and models. The literature shows that multimodal biometric-based authentication schemes have used different fusion approaches, such as feature-level fusion, used modeling algorithms fusion, and decision-level fusion.

1) Feature-level fusion includes combining features from different modalities to be considered together as an input to the modeling algorithm. Accounting for possible heterogeneous resulting feature space from different sources, a normalization process usually takes place.
2) Algorithm-level fusion includes constructing an ensemble of models that are built based on an individual of multiple biometric modalities. The ensemble combines outputs by considering matching scores or voting mechanism to help with the decision.
3) Decision-level fusion occurs when decisions are generated by individual modalities separately. The final decision considers all outputs and adopts certain rules or voting to generate the final output.

Using multimodal authentication on smartphones is a feasible solution since today's devices are equipped with a variety of sensors that support the reading of several biometrics [164]. However, several challenges should be considered when implementing multimodal authentication, such as the input data quality generated by different sources since poor data result in poor performance, and the inclusion of multiple data sources requires reading from different sensors, which could be computationally hungry and energy expensive [183]. Addressing such challenges effectively allows multimodal authentication to offer robust and secure access control [184].

Vildjiounaite *et al.* [101] proposed combining gait and voice biometrics to increase the performance of user validation.

Using data samples of 31 users, the authors reported a decrease in the error rates from 2.82%–43.09% and 13.7–17.2% using the individual voice and gait recognition, respectively, to 1.97%–11.8% for adopting a multimodal system incorporating both biometrics. However, the proposed method is event dependent and performs differently when the user motion or speaking is different since the results show that such a method is ineffective if the user is not speaking or speaking. Zhu *et al.* [107] proposed an SVM-based method called *RiskCog* that can validate users within 3.2 s using sensory data collected from mobile and/or wearable devices, including readings of the accelerometer, gyroscope, and gravity sensors. The authors reported an average system accuracy of 93.8% and 95.6% for steady and moving users, respectively, using a large data set of 1513 users. Lee and Lee [68] proposed combining sensors' readings from the user's smartphone and other wearable devices to improve authentication accuracy. Their experiments on a data set of 35 users have shown an accuracy of 98.1%, FRR of 0.9%, and FAR of 2.8% by combining data from users' smartphones and smartwatches when adopting an authentication window of 6 s.

Gofman *et al.* [164] suggested using face and voice biometrics to tackle input data quality and training data scarcity for mobile authentication. Considering the nature of the data acquisition process on mobile devices, the authors argued that data quality is usually in poor condition due to environmental factors or the utilization of low-cost sensors. Moreover, the authors stated mobile authentication systems face a training data scarcity problem since users tend to provide small training samples during the enrolment phase. Using a multimodal system, the authors addressed these issues and enhanced the potential of acquiring high-quality data samples during user enrollment. The proposed approach incorporated the Fisherface method for face recognition since it is shown to be effective under changing environmental conditions, and hidden Markov models (HMMs) and linear discriminant analysis (LDA) for voice recognition (HMM was used for algorithm score-level fusion and LDA was used for feature-level fusion). The authors used a quality-based weighting method to adjust to samples' quality and limit the impact of poor-quality samples on the performance of the system. The results showed a decrease in error rates from 4.29% for the face recognition module and 34.72% for the voice recognition module to 2.14% for the feature-level fused multimodal system. Similar work has been proposed by Morris *et al.* [65] for combining voice, face, and signature modalities for personal digital assistant devices. The authors reported a decrease in error rates when combining all three modalities from 3.38%–29.87% to 0.56%, which is considered a considerable improvement in the system performance. Their implementation adopts a text-dependent voice authentication approach since text independent can bring much complexity when addressing phonetic variations, which can computationally expensive and energy draining when running locally on the device.

Kayacik *et al.* [174] proposed a data-driven approach with an ensemble of classifiers to enable the authentication system to be temporally and spatially aware of the user behavioral usage and surroundings by taking advantage of several hard and soft sensors, such as the accelerometer, Wi-Fi, light sensor, and others. The proposed method requires more than 122 s to allow the data to be collected for authenticating users and about 717 s to detect an imposter. However, the experiments report a high authentication accuracy of 99.4%. Similar work has been proposed by Li and Bours [185] that incorporates sensory data of smartphones and Wi-Fi information for enabling users to access an application within 3 s, with an average EER of 9.19%. Similar studies combinations of multiple biometrics to incorporate face, iris, and periocular recognition [168], [186], eye gaze, and touch gestures [165], and user behavioral profiling, keystroke dynamics, and linguistic features [166]. Another direction of research studied users' behavioral patterns using their usage of applications and Wi-Fi traffic [167]. Table VIII shows the multimodal-based user authentication methods by using multiple modalities and machine learning algorithms.

Insights and Challenges: Multimodal-based user authentication methods are designed by implementing several modalities that can include both behavioral and physiological biometrics (e.g., face, voice, and keystroke dynamics) to conduct user authentication tasks. Recent trends in the authentication space show that multimodal methods are the favorable choice for implementing authentication schemes due to their performance and added security. Since multimodal authentication schemes incorporate multiple modalities, they intrinsically inherit some of the shortcomings and challenges of their integrated components. However, adopting a multimodal authentication scheme for continuous authentication on mobile devices adds several additional challenges, among which we mention the following.

1) *Computation and Memory Overhead:* Incorporating multiple modalities requires continuous collection and processing of data at a high sampling rate, which can increase the computation and memory overhead of the device. Moreover, combining the output of multiple modalities for the authentication decision requires the inference of multiple models or matching algorithms to generate the final output. Considering continuous authentication at a high frequency can introduce major resources bottlenecks, in terms of computations. Fortunately, current mobile devices are equipped with multicore processors, GPUs, and even Gigabytes of RAM, making it feasible to run a wide range of sophisticated applications such as multimodal-based continuous authentication schemes. Recent trends to secure in-device operations take advantage of machine learning libraries that utilize hardware acceleration units, using GPUs or digital signal processor (DSP), which are available in most of today's mobile devices, to implement local inference of authentication models.
2) *Biometric Samples Quality Assurance:* The performance of a system is related to the quality of the collected samples, as a biometric sample with high quality is essential for accurate identification. Due to the unreliable features that could be obtained from a single biometric (i.e., the changing emotional or physical state of the user or poor data acquisition), and to overcome performance degradation caused by these limitations, researchers

TABLE VIII
SUMMARY OF THE RELATED WORK FOR MULTIMODAL-BASED USER AUTHENTICATION. EACH WORK IS IDENTIFIED BY THE USED MODALITIES, UTILIZED SENSORS, DATA SET, MODELING ALGORITHM, AND THEIR PERFORMANCE

Study	Modalities	Sensors	Methods	# Users	EER	FAR	FRR	TPR	Accuracy	Auth. Time	Platform
[62]	Face/Voice	Ca, Mi	LDA-HMM	54	21.58%	✗	✗	✓	✗	0.39s	SamsungGalaxyS5 (A-5.0)
[158]	Teeth Images/voice	Ca, Mi	HMM⊕GMM	50	2.13%	✓	✓	✗	✗	10.76s	Computer Simulation
[164]	Face/Voice	NA	LDA-Matching	54	2.14%	✗	✗	✗	✗	1.57s	SamsungGalaxyS5 (A-5.0)
[65]	Face/Voice/Signature	NA	GMM	60	0.56%	0.97%	0.69%	✗	✗	✗	✗
[165]	Touch/Gaze	To, Ca	✗	13	✗	✗	✗	✗	65%	3.1s	Computer (NA)
[166]	Keystroke/Linguistic/Behavior	NA	MLP⊕RBF	30	3.3%	✗	✗	✗	✗	2–10m	✗
[167]	App/Bluetooth/Wi-Fi	NA	k-NN	200	✗	✗	✗	✗	85%	✗	✗
[114]	Keystroke/Sensor dynamics	To, Ac, Gy	k-NN	20	0.14%	✗	✗	✗	✗	✗	GoogleNexusS (A-2.3)
[128]	Keystroke/Motion/Orientation	To, Ac, Gy	PCA-SVM	20	7.16%	✓	✓	✗	✗	20s	SamsungGalaxyS4 (A-4.4)
[168]	Face/Periocular/Iris	Ca	FA-NN	78	0.68%	✓	✗	✗	✓	✗	SamsungGalaxyS5 (A-4.4.2)
[169]	Face/Periocular	Ca	Matching	73	1.34%	0.01%	✗	✗	94.66%	✗	SamsungGalaxyS5 (A-5.0)
[170]	Face/Periocular	Ca	CNN	246	✗	✗	✗	✓	98.5%	✗	✗
[171]	Keystroke/Gait	To, Ac	MLP	20	1%	0.68%	7%	✗	99.11%	✗	Xiaomi2S (A-5.0.2)
[172]	App/Bluetooth/Wi-Fi/other	NA	FPOS	33	✗	✓	✗	✓	98.3%	2.3s	Nokia7Plus (A-8.0.1)
[173]	Touch/Motion/App/other	To, Ac, Gy, Ma, Li	SVM	48	✓	✓	✓	✗	97.1%	✗	✗
[174]	App/Motion/Wi-Fi/other	Ac, Wi-Fi, Li, other	Ensemble	7	✗	✗	✗	✗	99.4%	122s	Nokia6600 (Symbian-7.0)
[175]	Motion/Gesture	Ac, Gr, Or, Ma	n-gram	20	✗	31.1%	✗	71.30%	✗	4.96s	✗
[176]	Face/Touch/Motion	Ca, To, Ac,Gy, Ma	Ensemble	100	0.8-3.6%	✗	✗	✗	✗	✓	ComputerSimulation
[177]	Touch/Motion/other	To, Ac, Gy, Ma, other	Compound-Voting	30	✗	0	0	✗	100%	✗	VivoX6 (A-5.0)
[178]	Touch/Motion	To, Ac, Gy	SVM	100	15%	✗	✗	✗	88%	✗	SamsungGalaxyS4 (A-4.4)
[179]	Touch/Motion	To, Ac, Gy	SVM	48	✓	5.01%	6.85%	✗	✗	✓	SamsungN7100 (A-4.4)
[18]	Face/Voice	Ca, Mi	CNN-SVM	10	✗	✗	✗	88.84%	94.07%	30ms	SamsungGalaxyS9 (A-8.0)
[180]	Touch/Motion	Ac, Gy, Ma	CNN-SVM	90	✗	✓	✓	✗	97.8%	1s	SamsungGalaxyS4 (A-4.4)
[47]	Touch/Motion	Ac, Gy, Ma, El	LSTM	84	0.37%	1.72%	8.47%	✓	97.84%	1s	✗
[31]	Touch/Motion	To, Ac, Gy, Ma, Or	HMM	102	4.74%	3.98%	5.03%	✗	✗	8s	SamsungG9208 (A-5.0.2)
[68]	Wearable/Sensor dynamics	Ac, Gy, Ma, Or, Li	KRR	35	✓	2.8%	0.9%	✓	98.1%	✓	GoogleNexus5 (A-4.0)
[107]	Wearable/Sensor dynamics	Ac, Gy, Gr	SVM	1,513	✗	✗	✗	73.28%	95.57%	3.2s	ComputerSimulation
[181]	Healthcare readings	HWS	SVM-RBF	37	2.6%	7.6%	9.6%	✓	✗	✓	✗
			AdaBoost	37	2.4%	7.6%	8.4%	✓	✗	✓	✗

Ca: Camera, Mi: Microphone, To: Touch, Ac: Accelerometer, Gy: Gyroscope, Ma: Magnetometer, Li: Light sensor, Gr: Gravity sensor, El: Elevation
HWS: Healthcare Wearable Sensors, LDA: Linear Discriminant Analysis, HMM: Hidden Markov Model, GMM: Gaussian Mixed Model,
MLP: Multilayer Perceptron, RBF: Radial Basis Function, k-NN: k-Nearest Neighbor, PCA: Principal Component Analysis, SVM: Support Vector Machine,
FA-NN: Fast Approximate Nearest Neighbor, CNN: Convolutional Neural Network, FPOS: Frequent Pattern Outlier Score, KRR: Kernel Ridge Regression.

have moved from the unimodal to multimodal biometrics. For instance, combining face recognition and keystroke dynamics for user authentication enhances the performance of each modality when considered alone. However, recent trends in adopting biometric-based authentication show it is also necessary to add a sample-quality assessment module to the authentication system, after the data collection and acquisition module, in order to guarantee the processing of valid samples in further processes.

3) *Machine Learning-Based Authentication:* Recent studies show the increasing reliance on machine learning techniques to implement authentication systems. For multimodal-based methods, researchers utilize an ensemble of machine learning models to enable multiple pattern recognition per legitimate user. This can result in a longer training time (i.e., extending the user enrolment phase), greater model size and memory overhead, and inference time (i.e., user authentication phase). All of those are open directions worth exploring. Especially, future authentication schemes should consider using hardware acceleration units, such as GPUs or DSPs that are available in most of today's mobile devices.

IX. CONCLUSION

Mobile devices have become the most common platform for communication and accessing the Internet. The rapid enhancements of embedded technologies and resources of mobile devices have enabled users to conduct varieties of activities and transactions. Therefore, secure and accurate access control is essential. To date, mobile devices' manufacturers have implemented knowledge-based and physiological biometric-based authentication methods as the primary access control scheme. While both approaches offer simplicity, efficiency, and precision, they assume the same level of security to all applications and fall short on delivering authentication beyond the point of entry. Moreover, these approaches require overt recognition, where the user explicitly enters the pass secret or the used biometrics, making them fail in delivering implicit, transparent, and continuous authentication. Recently, behavioral biometrics are used to offer efficient continuous authentication on smartphones by leveraging the readings of a variety of embedded sensors. This survey aims to highlights methods, approaches, benefits, and challenges associated with using behavioral biometrics for user authentication. We surveyed around 150 studies that conducted a behavioral-based authentication and pointed out their used techniques, sensors, performance measurements, and time needed for authentication. As this field is rapidly evolving, there is still a need to explore security-related aspects and implementation considerations beyond familiar standards.

REFERENCES

[1] C. Jung, J. Kang, A. Mohaisen, and D. Nyang, "Digitalseal: A transaction authentication tool for online and offline transactions," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2018, pp. 6956–6960.

[2] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and transparent multimodal authentication: Reviewing the state of the art," *Clust. Comput.*, vol. 19, no. 1, pp. 455–474, Mar. 2016.

[3] T. J. Neal and D. L. Woodard, "Surveying biometric authentication for mobile device security," *J. Pattern Recognit. Res.*, vol. 11, no. 1, pp. 74–110, 2016.

[4] Z. Zhao, G.-J. Ahn, and H. Hu, "Picture gesture authentication: Empirical analysis, automated attacks, and scheme evaluation," *ACM Trans. Inf. Syst. Security*, vol. 17, no. 4, p. 14, 2015.

[5] D. Nyang, A. Mohaisen, and J. Kang, "Keylogging-resistant visual authentication protocols," *IEEE Trans. Mobile Comput.*, vol. 13, no. 11, pp. 2566–2579, Nov. 2014.

[6] D. Nyang *et al.*, "Two-thumbs-up: Physical protection for pin entry secure against recording attacks," *Comput. Security*, vol. 78, pp. 1–15, Sep. 2018.

[7] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and I know it's you!: Implicit authentication based on touch screen patterns," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2012, pp. 987–996.

[8] N. L. Clarke and S. M. Furnell, "Authentication of users on mobile telephones—A survey of attitudes and practices," *Comput. Security*, vol. 24, no. 7, pp. 519–527, 2005.

[9] R. Amin, T. Gaber, G. ElTaweel, and A. E. Hassanien, "Biometric and traditional mobile authentication techniques: Overviews and open issues," in *Bio-Inspiring Cyber Security and Cloud Services: Trends and Innovations*. Berlin, Germany: Springer, 2014, pp. 423–446.

[10] H. Crawford and K. Renaud, "Understanding user perceptions of transparent authentication on a mobile device," *J. Trust Manag.*, vol. 1, no. 1, p. 7, 2014.

[11] S. Furnell, N. Clarke, and S. Karatzouni, "Beyond the PIN: Enhancing user authentication for mobile devices," *Comput. Fraud Security*, vol. 2008, no. 8, pp. 12–17, 2008.

[12] H. Khan and U. Hengartner, "Towards application-centric implicit authentication on smartphones," in *Proc. 15th Workshop Mobile Comput. Syst. Appl.*, 2014, p. 10.

[13] A. Wójtowicz and K. Joachimiak, "Model for adaptable context-based biometric authentication for mobile devices," *Pers. Ubiquitous Comput.*, vol. 20, no. 2, pp. 195–207, 2016.

[14] Z. Yu, I. Olade, H.-N. Liang, and C. Fleming, "Usable authentication mechanisms for mobile devices: An exploration of 3D graphical passwords," in *Proc. Int. Conf. Platform Technol. Service (PlatCon)*, 2016, pp. 1–3.

[15] K. I. Shin, J. S. Park, J. Y. Lee, and J. H. Park, "Design and implementation of improved authentication system for android smartphone users," in *Proc. 26th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, 2012, pp. 704–707.

[16] Y. Yang, G. D. Clark, J. Lindqvist, and A. Oulasvirta, "Free-form gesture authentication in the wild," in *Proc. CHI Conf. Human Factors Comput. Syst.*, 2016, pp. 3722–3735.

[17] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Active authentication for mobile devices utilising behaviour profiling," *Int. J. Inf. Security*, vol. 13, no. 3, pp. 229–244, 2014.

[18] B. Zhou, Z. Xie, and F. Ye, "Multi-modal face authentication using deep visual and acoustic features," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2019, pp. 1–6.

[19] D. Cilia and F. Inguanez, "Multi-model authentication using keystroke dynamics for smartphones," in *Proc. IEEE 8th Int. Conf. Consum. Electron. (ICCE)*, Berlin, Germany, 2018, pp. 1–6.

[20] C. A. Miles and J. P. Cohn, "Tracking prisoners in jail with biometrics: An experiment in a navy brig," *Nat. Inst. Justice J.*, vol. 253, p. 4, Jan. 2006.

[21] K. B. Schaffer, "Expanding continuous authentication with mobile devices," *Computer*, vol. 48, no. 11, pp. 92–95, 2015.

[22] P. S. Teh, A. B. J. Teoh, and S. Yue, "A survey of keystroke dynamics biometrics," *Sci. World J.*, vol. 2013, Nov. 2013, Art. no. 408280.

[23] S. Bhatt and T. Santhanam, "Keystroke dynamics for biometric authentication—A survey," in *Proc. Int. Conf. Pattern Recognit. Informat. Mobile Eng.*, Feb. 2013, pp. 17–23.

[24] M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," *Appl. Soft Comput.*, vol. 11, no. 2, pp. 1565–1573, 2011.

[25] S. S. Tirumala, S. R. Shahamiri, A. S. Garhwal, and R. Wang, "Speaker identification features extraction methods: A systematic review," *Expert Syst. Appl.*, vol. 90, pp. 250–271, Dec. 2017.

[26] R. Spolaor, L. QianQian, M. Monaro, M. Conti, L. Gamberini, and G. Sartori, "Biometric authentication methods on smartphones: A survey," *PsychNol. J.*, vol. 14, no. 2, pp. 87–98, 2016.

[27] D. Kunda and M. Chishimba, "A survey of android mobile phone authentication schemes," *Mobile Netw. Appl.*, vol. 23, pp. 1–9, Aug. 2018.

[28] M. Ehatisham-ul Haq, M. A. Azam, U. Naeem, Y. Amin, and J. Loo, "Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing," *J. Netw. Comput. Appl.*, vol. 109, pp. 24–35, May 2018.

[29] H. F. Nweke, Y. W. Teh, M. A. Al-Garadi, and U. R. Alo, "Deep learning algorithms for human activity recognition using mobile and wearable sensor networks: State of the art and research challenges," *Expert Syst. Appl.*, vol. 105, pp. 233–261, Sep. 2018.

[30] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-factor authentication for IoT with location information," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3335–3351, Apr. 2019.

[31] 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.

[32] Y. Zhang, W. Hu, W. Xu, C. T. Chou, and J. Hu, "Continuous authentication using eye movement response of implicit visual stimuli," *Proc. ACM Interact. Mobile Wearable Ubiquitous Technol.*, vol. 1, no. 4, p. 177, Jan. 2018.

[33] J. S. Arteaga-Falconi, H. A. Osman, and A. El-Saddik, "ECG authentication for mobile devices," *IEEE Trans. Instrum. Meas.*, vol. 65, no. 3, pp. 591–600, Mar. 2016.

[34] Z. Ba, S. Piao, X. Fu, D. Koutsonikolas, A. Mohaisen, and K. Ren, "ABC: Enabling smartphone authentication with built-in camera," in *Proc. 25th Annu. Netw. Distrib. Syst. Security Symp. (NDSS)*, 2018, p. 15.

[35] M. Zeng *et al.*, "Convolutional neural networks for human activity recognition using mobile sensors," in *Proc. 6th Int. Conf. Mobile Comput. Appl. Services (MobiCASE)*, 2014, pp. 197–205.

[36] G. Biegel and V. Cahill, "A framework for developing mobile, context-aware applications," in *Proc. 2nd IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, 2004, pp. 361–365.

[37] S. Das, D. Guha, and B. Dutta, "Medical diagnosis with the aid of using fuzzy logic and intuitionistic fuzzy logic," *Appl. Intell.*, vol. 45, no. 3, pp. 850–867, 2016.

[38] S. Choi *et al.*, "A multisensor mobile interface for industrial environment and healthcare monitoring," *IEEE Trans. Ind. Electron.*, vol. 64, no. 3, pp. 2344–2352, Mar. 2017.

[39] J. Wu and R. Jafari, "Orientation independent activity/gesture recognition using wearable motion sensors," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1427–1437, Apr. 2019.

[40] Z. Yu, E. Xu, H. Du, B. Guo, and L. Yao, "Inferring user profile attributes from multidimensional mobile phone sensory data," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5152–5162, Jun. 2019.

[41] N. Micallef, H. G. Kayacık, M. Just, L. Baillie, and D. Aspinall, "Sensor use and usefulness: Trade-offs for data-driven authentication on mobile devices," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, 2015, pp. 189–197.

[42] A. Drosou and D. Tzovaras, "Activity and event related biometrics," in *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht, The Netherlands: Springer, 2012, pp. 129–148.

[43] B. Draffin, J. Zhu, and J. Y. Zhang, "Keysens: Passive user authentication through micro-behavior modeling of soft keyboard interaction," in *Proc. 5th Int. Conf. Mobile Comput. Appl. Services (MobiCASE)*, 2013, pp. 184–201.

[44] A. Laghari, Waheed-ur-Rehman, and Z. A. Memon, "Biometric authentication technique using smartphone sensor," in *Proc. 13th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, 2016, pp. 381–384.

[45] Y. Shen *et al.*, "Securing cyber-physical social interactions on wrist-worn devices," *ACM Trans. Sensor Netw.*, vol. 16, no. 2, pp. 1–22, 2020.

[46] Y. Shen, F. Yang, B. Du, W. Xu, C. Luo, and H. Wen, "Shake-n-shack: Enabling secure data exchange between smart wearables via handshakes," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, 2018, pp. 1–10.

[47] M. Abuhamad, T. Abuhmed, D. Mohaisen, and D. H. Nyang, "AUToSen: Deep-learning-based implicit continuous authentication using smartphone sensors," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5008–5020, Jun. 2020.

[48] P. Fernandez-Lopez, J. Liu-Jimenez, C. Sanchez-Redondo, and R. Sanchez-Reillo, "Gait recognition using smartphone," in *Proc. IEEE Int. Carnahan Conf. Security Technol. (ICCST)*, 2016, pp. 1–7.

[49] G. B. D. Pozo, C. Sanchez-Avila, A. De-Santos-Sierra, and J. Guerra-Casanova, "Speed-independent gait identification for mobile devices," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 26, no. 8, 2012, Art. no. 1260013.

[50] R. Damaševičius, R. Maskeliūnas, A. Venčkauskas, and M. Woźniak, "Smartphone user identity verification using gait characteristics," *Symmetry*, vol. 8, no. 10, p. 100, 2016.

[51] Y. Lu, Y. Wei, L. Liu, J. Zhong, L. Sun, and Y. Liu, "Towards unsupervised physical activity recognition using smartphone accelerometers," *Multimedia Tools Appl.*, vol. 76, no. 8, pp. 10701–10719, Apr. 2017.

[52] C. Nickel, H. Brandt, and C. Busch, "Classification of acceleration data for biometric gait recognition on mobile devices," in *Proc. Biometrics Special Interest Group (BIOSIG)*, 2011, pp. 57–66.

[53] V. Zaliva, W. Melicher, S. Saha, and J. Zhang, "Passive user identification using sequential analysis of proximity information in touchscreen usage patterns," in *Proc. 8th Int. Conf. Mobile Comput. Ubiquitous Netw. (ICMU)*, 2015, pp. 161–166.

[54] A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proc. 4th USENIX Workshop Offensive Technol. (WOOT)*, 2010, pp. 1–7.

[55] J. Wu and Z. Chen, "An implicit identity authentication system considering changes of gesture based on keystroke behaviors," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 6, pp. 470274:1–470274:16, 2015.

[56] A. Buchoux and N. L. Clarke, "Deployment of keystroke analysis on a smartphone," in *Proc. Aust. Inf. Security Manag. Conf.*, 2008, p. 48.

[57] C. X. Lu *et al.*, "Snoopy: Sniffing your smartwatch passwords via deep sequence learning," *Proc. ACM Interact. Mobile Wearable Ubiquitous Technol.*, vol. 1, no. 4, pp. 1–29, 2018.

[58] S. Mondal and P. Bours, "Person identification by keystroke dynamics using pairwise user coupling," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1319–1329, Jun. 2017.

[59] G. Kambourakis, D. Damopoulos, D. Papamartzivanos, and E. Pavlidakis, "Introducing touchstroke: Keystroke-based authentication system for smartphones," *Security Commun. Netw.*, vol. 9, no. 6, pp. 542–554, 2016.

[60] D. A. Reynolds, T. F. Quatieri, and R. B. Dunn, "Speaker verification using adapted Gaussian mixture models," *Digit. Signal Process.*, vol. 10, nos. 1–3, pp. 19–41, 2000.

[61] H. Lu, A. J. B. Brush, B. Priyantha, A. K. Karlson, and J. Liu, "Speakersense: Energy efficient unobtrusive speaker identification on mobile phones," in *Proc. 9th Int. Conf. Pervasive Comput.*, 2011, pp. 188–205.

[62] M. I. Gofman, S. Mitra, and N. Smith, "Hidden Markov models for feature-level fusion of biometrics on mobile devices," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, 2016, pp. 1–2.

[63] N. L. Clarke and A. Mekala, "The application of signature recognition to transparent handwriting verification for mobile devices," *Inf. Manag. Comput. Security*, vol. 15, no. 3, pp. 214–225, 2007.

[64] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia, "Towards mobile authentication using dynamic signature verification: Useful features and performance evaluation," in *Proc. 19th Int. Conf. Pattern Recognit.*, 2008, pp. 1–5.

[65] A. C. Morris *et al.*, "Multimodal person authentication on a smartphone under realistic conditions," in *Mobile Multimedia/Image Processing for Military and Security Applications*, vol. 6250. Bellingham, WA, USA: Int. Soc. Opt. Photon., 2006, Art. no. 62500D.

[66] A. Alzubaidi and J. Kalita, "Authentication of smartphone users using behavioral biometrics," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1998–2026, 3rd Quart., 2016.

[67] S. Amini, V. Noroozi, A. Pande, S. Gupte, P. S. Yu, and C. Kanich, "Deepauth: A framework for continuous user re-authentication in mobile apps," in *Proc. 27th ACM Int. Conf. Inf. Knowl. Manag. (CIKM)*, 2018, pp. 2027–2035.

[68] W.-H. Lee and R. B. Lee, "Implicit smartphone user authentication with sensors and contextual machine learning," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, 2017, pp. 297–308.

[69] H. Crawford, K. Renaud, and T. Storer, "A framework for continuous, transparent mobile device authentication," *Comput. Security*, vol. 39, pp. 127–136, Nov. 2013.

[70] F. Hong, M. Wei, S. You, Y. Feng, and Z. Guo, "Waving authentication: Your smartphone authenticate you on motion gesture," in *Proc. 33rd Annu. ACM Conf. Extended Abstracts Human Factors Comput. Syst.*, 2015, pp. 263–266.

[71] T. Feng, X. Zhao, and W. Shi, "Investigating mobile device picking-up motion as a novel biometric modality," in *Proc. IEEE 6th Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, 2013, pp. 1–6.

[72] F. Hong, S. You, M. Wei, Y. Zhang, and Z. Guo, "MGRA: Motion gesture recognition via accelerometer," *Sensors*, vol. 16, no. 4, p. 530, 2016.

[73] D. Lu, D. Huang, Y. Deng, and A. Alshamrani, "Multifactor user authentication with in-air-handwriting and hand geometry," in *Proc. Int. Conf. Biometrics (ICB)*, 2018, pp. 255–262.

[74] Q. Xia, F. Hong, Y. Feng, and Z. Guo, "Motionhacker: Motion sensor based eavesdropping on handwriting via smartwatch," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2018, pp. 468–473.

[75] J. Yan, Y. Qi, Q. Rao, and S. Qi, "Towards a user-friendly and secure hand shaking authentication for smartphones," in *Proc. 17th IEEE Int. Conf. Trust Security Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, 2018, pp. 1170–1179.

[76] A. L. Fantana, S. Ramachandran, C. H. Schunck, and M. Talamo, "Movement based biometric authentication with smartphones," in *Proc. Int. Carnahan Conf. Security Technol. (ICCST)*, 2015, pp. 235–239.

[77] J. G. Casanova, C. S. Ávila, A. de Santos Sierra, G. B. del Pozo, and V. J. Vera, "A real-time in-air signature biometric technique using a mobile device embedding an accelerometer," in *Proc. Int. Conf. Netw. Digit. Technol.*, 2010, pp. 497–503.

[78] M. Haring, D. Reinhardt, and Y. Omlor, "Pick me up and i will tell you who you are: Analyzing pick-up motions to authenticate users," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, 2018, pp. 472–475.

[79] J. Maghsoudi and C. C. Tappert, "A behavioral biometrics user authentication study using motion data from android smartphones," in *Proc. Eur. Intell. Security Informat. Conf. (EISIC)*, 2016, pp. 184–187.

[80] A. Eremin, K. Kogos, and Y. Valatskayte, "Touch and move: Incoming call user authentication," in *Proc. Int. Conf. Inf. Syst. Security Privacy*, 2018, pp. 26–39.

[81] W. Lee and R. B. Lee, "Multi-sensor authentication to improve smartphone security," in *Proc. 1st Int. Conf. Inf. Syst. Security Privacy (ICISSP)*, 2015, pp. 270–280.

[82] Y. Li, H. Hu, and G. Zhou, "Using data augmentation in continuous authentication on smartphones," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 628–640, Feb. 2019.

[83] C. Song, A. Wang, K. Ren, and W. Xu, "Eyeveri: A secure and usable approach for smartphone user authentication," in *Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, 2016, pp. 1–9.

[84] N. L. Clarke and S. Furnell, "Advanced user authentication for mobile devices," *Comput. Security*, vol. 26, no. 2, pp. 109–119, 2007.

[85] R. Ferrero, F. Gandino, B. Montrucchio, M. Rebaudengo, A. Velasco, and I. Benkhelifa, "On gait recognition with smartphone accelerometer," in *Proc. 4th Mediterranean Conf. Embedded Comput. (MECO)*, 2015, pp. 368–373.

[86] 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.

[87] P. Kartik, S. M. Prasanna, and R. V. Prasad, "Multimodal biometric person authentication system using speech and signature features," in *Proc. IEEE Region 10 Conf. (TENCON)*, 2008, pp. 1–6.

[88] I. Bhattacharya, P. Ghosh, and S. Biswas, "Offline signature verification using pixel matching technique," *Procedia Technol.*, vol. 10, pp. 970–977, Dec. 2013.

[89] A. Sahami Shirazi, P. Moghadam, H. Ketabdar, and A. Schmidt, "Assessing the vulnerability of magnetic gestural authentication to video-based shoulder surfing attacks," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2012, pp. 2045–2048.

[90] H. Zhu, J. Hu, S. Chang, and L. Lu, "Shakein: Secure user authentication of smartphones with single-handed shakes," *IEEE Trans. Mobile Comput.*, vol. 16, no. 10, pp. 2901–2912, Oct. 2017.

[91] L. Wang, H. Ning, T. Tan, and W. Hu, "Fusion of static and dynamic body biometrics for gait recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 2, pp. 149–158, Feb. 2004.

[92] D. Gafurov and E. Snekkenes, "Gait recognition using wearable motion recording sensors," *EURASIP J. Adv. Signal Process.*, vol. 2009, p. 7, Jan. 2009.

[93] G. Qian, J. Zhang, and A. Kidané, "People identification using gait via floor pressure sensing and analysis," in *Proc. Eur. Conf. Smart Sens. Context*, 2008, pp. 83–98.

[94] H. M. Thang, V. Q. Viet, N. D. Thuc, and D. Choi, "Gait identification using accelerometer on mobile phone," in *Proc. Int. Conf. Control Autom. Inf. Sci. (ICCAIS)*, 2012, pp. 344–348.

[95] T. Hoang, T. D. Nguyen, C. Luong, S. Do, and D. Choi, "Adaptive cross-device gait recognition using a mobile accelerometer," *J. Inf. Process. Syst.*, vol. 9, no. 2, pp. 333–348, 2013.

[96] 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. Acoust. Speech Signal Process. (ICASSP)*, vol. 2, 2005, pp. 973–976.

[97] M. Muaaz and R. Mayrhofer, "An analysis of different approaches to gait recognition using cell phone based accelerometers," in *Proc. Int. Conf. Adv. Mobile Comput. Multimedia*, 2013, p. 293.

[98] C. Nickel, M. O. Derawi, P. Bours, and C. Busch, "Scenario test of accelerometer-based biometric gait recognition," in *Proc. 3rd Int. Workshop Security Commun. Netw. (IWSCN)*, 2011, pp. 15–21.

[99] 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.*, 2012, pp. 16–20.

[100] T. Hoang, D. Choi, and T. Nguyen, "Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme," *Int. J. Inf. Security*, vol. 14, no. 6, pp. 549–560, 2015.

[101] E. Vildjiounaite *et al.*, "Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices," in *Proc. Int. Conf. Pervasive Comput.*, 2006, pp. 187–201.

[102] C. Nickel and C. Busch, "Classifying accelerometer data via hidden Markov models to authenticate people by the way they walk," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 28, no. 10, pp. 29–35, Oct. 2013.

[103] W. Xu *et al.*, "KEH-gait: Using kinetic energy harvesting for gait-based user authentication systems," *IEEE Trans. Mobile Comput.*, vol. 18, no. 1, pp. 139–152, Jan. 2019.

[104] N. Kolokas, S. Krinidis, A. Drosou, D. Ioannidis, and D. Tzovaras, "Gait matching by mapping wearable to camera privacy-preserving recordings: Experimental comparison of multiple settings," in *Proc. 6th Int. Conf. Control Decis. Inf. Technol. (CoDIT)*, 2019, pp. 338–343.

[105] A. Ferreira, G. Santos, A. Rocha, and S. Goldenstein, "User-centric coordinates for applications leveraging 3-axis accelerometer data," *IEEE Sensors J.*, vol. 17, no. 16, pp. 5231–5243, Aug. 2017.

[106] Y. Sun and B. Lo, "An artificial neural network framework for gait-based biometrics," *IEEE J. Biomed. Health Informat.*, vol. 23, no. 3, pp. 987–998, May 2019.

[107] T. Zhu *et al.*, "RiskCog: Unobtrusive real-time user authentication on mobile devices in the wild," *IEEE Trans. Mobile Comput.*, vol. 19, no. 2, pp. 466–483, Feb. 2020.

[108] F. Maggi, A. Volpatto, S. Gasparini, G. Boracchi, and S. Zanero, "A fast eavesdropping attack against touchscreens," in *Proc. 7th Int. Conf. Inf. Assurance Security (IAS)*, 2011, pp. 320–325.

[109] Y. Xu, J. Heinly, A. M. White, F. Monrose, and J.-M. Frahm, "Seeing double: Reconstructing obscured typed input from repeated compromising reflections," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2013, pp. 1063–1074.

[110] Q. Yue, Z. Ling, X. Fu, B. Liu, K. Ren, and W. Zhao, "Blind recognition of touched keys on mobile devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2014, pp. 1403–1414.

[111] B. Tang, Z. Wang, R. Wang, L. Zhao, and L. Wang, "Niffler: A context-aware and user-independent side-channel attack system for password inference," *Wireless Commun. Mobile Comput.*, vol. 2018, May 2018, Art. no. 4627108.

[112] L. Cai and H. Chen, "On the practicality of motion based keystroke inference attack," in *Proc. Int. Conf. Trust Trustworthy Comput.*, 2012, pp. 273–290.

[113] T. Nguyen, "Using unrestricted mobile sensors to infer tapped and traced user inputs," in *Proc. 12th Int. Conf. Inf. Technol. New Gener.*, 2015, pp. 151–156.

[114] V.-D. Stanciu, R. Spolaor, M. Conti, and C. Giuffrida, "On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks," in *Proc. 6th ACM Conf. Data Appl. Security Privacy*, 2016, pp. 105–112.

[115] L. Cai and H. Chen, "Touchlogger: Inferring keystrokes on touch screen from smartphone motion," in *Proc. 6th USENIX Conf. Hot Topics Security (HOTSEC)*, vol. 11, p. 9, 2011.

[116] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in *Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2010, pp. 306–311.

[117] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," *Future Gener. Comput. Syst.*, vol. 16, no. 4, pp. 351–359, 2000.

[118] R. Joyce and G. Gupta, "Identity authentication based on keystroke latencies," *Commun. ACM*, vol. 33, no. 2, pp. 168–176, 1990.

[119] I. V. McLoughlin *et al.*, "Keypress biometrics for user validation in mobile consumer devices," in *Proc. IEEE 13th Int. Symp. Consum. Electron.*, 2009, pp. 280–284.

[120] S. Zahid, M. Shahzad, S. A. Khayam, and M. Farooq, "Keystroke-based user identification on smart phones," in *Proc. Int. Workshop Recent Adv. Intrusion Detection*, 2009, pp. 224–243.

[121] E. V. C. Urtiga and E. D. Moreno, "Keystroke-based biometric authentication in mobile devices," *IEEE Latin America Trans.*, vol. 9, no. 3, pp. 368–375, Jun. 2011.

[122] S.-S. Hwang, S. Cho, and S. Park, "Keystroke dynamics-based authentication for mobile devices," *Comput. Security*, vol. 28, nos. 1–2, pp. 85–93, 2009.

[123] J.-S. Wu, W.-C. Lin, C.-T. Lin, and T.-E. Wei, "Smartphone continuous authentication based on keystroke and gesture profiling," in *Proc. Int. Carnahan Conf. Security Technol. (ICCST)*, 2015, pp. 191–197.

[124] C. Giuffrida, K. Majdanik, M. Conti, and H. Bos, "I sensed it was you: Authenticating mobile users with sensor-enhanced keystroke dynamics," in *Proc. Int. Conf. Detection Intrusions Malware Vulnerability Assess.*, 2014, pp. 92–111.

[125] F. Inguanez and S. Ahmadi, "Securing smartphones via typing heat maps," in *Proc. IEEE 6th Int. Conf. Consum. Electron. (ICCE)*, Berlin, Germany, 2016, pp. 193–197.

[126] T. Anusas-amornkul, "Strengthening password authentication using keystroke dynamics and smartphone sensors," in *Proc. 9th Int. Conf. Inf. Commun. Manag.*, 2019, pp. 70–74.

[127] V. Shankar and K. Singh, "An intelligent scheme for continuous authentication of smartphone using deep auto encoder and softmax regression model easy for user brain," *IEEE Access*, vol. 7, pp. 48645–48654, 2019.

[128] 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.

[129] A. Buriro, B. Crispo, S. Gupta, and F. D. Frari, "DIALERAUTH: A motion-assisted touch-based smartphone user authentication scheme," in *Proc. 8th ACM Conf. Data Appl. Security Privacy*, 2018, pp. 267–276.

[130] S. Mondal and P. Bours, "Swipe gesture based continuous authentication for mobile devices," in *Proc. Int. Conf. Biometrics (ICB)*, 2015, pp. 458–465.

[131] T. Nohara and R. Uda, "Personal identification by flick input using self-organizing maps with acceleration sensor and gyroscope," in *Proc. 10th Int. Conf. Ubiquitous Inf. Manag. Commun.*, 2016, p. 58.

[132] C.-C. Lin, C.-C. Chang, D. Liang, and C.-H. Yang, "A new non-intrusive authentication method based on the orientation sensor for smartphone users," in *Proc. IEEE 6th Int. Conf. Softw. Security Rel.*, 2012, pp. 245–252.

[133] L. Lu and Y. Liu, "Safeguard: User reauthentication on smartphones via behavioral biometrics," *IEEE Trans. Comput. Social Syst.*, vol. 2, no. 3, pp. 53–64, Sep. 2015.

[134] A. Jain and V. Kanhangad, "Exploring orientation and accelerometer sensor data for personal authentication in smartphones using touchscreen gestures," *Pattern Recognit. Lett.*, vol. 68, pp. 351–360, Dec. 2015.

[135] D.-H. Shih, C.-M. Lu, and M.-H. Shih, "A flick biometric authentication mechanism on mobile devices," in *Proc. Int. Conf. Inf. Cybern. Comput. Social Syst. (ICCSS)*, 2015, pp. 31–33.

[136] H. Saevanee and P. Bhatarakosol, "User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device," in *Proc. Int. Conf. Comput. Elect. Eng.*, 2008, pp. 82–86.

[137] H. Xu, Y. Zhou, and M. R. Lyu, "Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones," in *Proc. 10th Symp. Usable Privacy Security (SOUPS)*, 2014, pp. 187–198.

[138] K. W. Nixon, X. Chen, Z.-H. Mao, and Y. Chen, "Slowmo-enhancing mobile gesture-based authentication schemes via sampling rate optimization," in *Proc. 21st Asia South Pac. Design Autom. Conf. (ASP-DAC)*, 2016, pp. 462–467.

[139] J. Nader, A. Alsadoon, P. Prasad, A. Singh, and A. Elchouemi, "Designing touch-based hybrid authentication method for smartphones," *Procedia Comput. Sci.*, vol. 70, pp. 198–204, Dec. 2015.

[140] M. Antal and L. Z. Szabó, "Biometric authentication based on touchscreen swipe patterns," *Procedia Technol.*, vol. 22, pp. 862–869, Oct. 2016.

[141] A. Primo and V. V. Phoha, "Music and images as contexts in a context-aware touch-based authentication system," in *Proc. IEEE 7th Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, 2015, pp. 1–7.
[142] T. Feng, J. Yang, Z. Yan, E. M. Tapia, and W. Shi, "TIPS: Context-aware implicit user identification using touch screen in uncontrolled environments," in *Proc. 15th Workshop Mobile Comput. Syst. Appl.*, 2014, pp. 9:1–9:6.
[143] C. Shen, Y. Zhang, X. Guan, and R. A. Maxion, "Performance analysis of touch-interaction behavior for active smartphone authentication," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 498–513, Mar. 2016.
[144] Z. Syed, J. Helmick, S. Banerjee, and B. Cukic, "Touch gesture-based authentication on mobile devices: The effects of user posture, device size, configuration, and inter-session variability," *J. Syst. Softw.*, vol. 149, pp. 158–173, Mar. 2019.
[145] Z. I. Rauen, F. Anjomshoa, and B. Kantarci, "Gesture and sociability-based continuous authentication on smart mobile devices," in *Proc. 16th ACM Int. Symp. Mobility Manag. Wireless Access*, 2018, pp. 51–58.
[146] R. Rocha, D. Carneiro, R. Costa, and C. Analide, "Continuous authentication in mobile devices using behavioral biometrics," in *Proc. Int. Symp. Ambient Intell.*, 2019, pp. 191–198.
[147] S. Mondal and P. Bours, "Continuous authentication and identification for mobile devices: Combining security and forensics," in *Proc. IEEE Int. Workshop Inf. Forensics Security (WIFS)*, 2015, pp. 1–6.
[148] F. A. Alsulaiman, J. Cha, and A. E. Saddik, "User identification based on handwritten signatures with haptic information," in *Proc. Int. Conf. Human Haptic Sens. Touch Enabled Comput. Appl.*, 2008, pp. 114–121.
[149] O. Miguel-Hurtado, S. V. Stevenage, C. Bevan, and R. Guest, "Predicting sex as a soft-biometrics from device interaction swipe gestures," *Pattern Recognit. Lett.*, vol. 79, pp. 44–51, Aug. 2016.
[150] C. Bevan and D. S. Fraser, "Different strokes for different folks? Revealing the physical characteristics of smartphone users from their swipe gestures," *Int. J. Human Comput. Stud.*, vol. 88, pp. 51–61, Apr. 2016.
[151] S. Azenkot, K. Rector, R. Ladner, and J. Wobbrock, "Passchords: Secure multi-touch authentication for blind people," in *Proc. 14th Int. ACM SIGACCESS Conf. Comput. Accessibility*, 2012, pp. 159–166.
[152] H. Khan, A. Atwater, and U. Hengartner, "Itus: An implicit authentication framework for android," in *Proc. 20th Annu. Int. Conf. Mobile Comput. Netw.*, 2014, pp. 507–518.
[153] O. Miguel-Hurtado, R. Blanco-Gonzalo, R. Guest, and C. Lunerti, "Interaction evaluation of a mobile voice authentication system," in *Proc. IEEE Int. Carnahan Conf. Security Technol. (ICCST)*, 2016, pp. 1–8.
[154] L. Zhang, S. Tan, and J. Yang, "Hearing your voice is not enough: An articulatory gesture based liveness detection for voice authentication," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2017, pp. 57–71.
[155] L. Lu *et al.*, "Lip reading-based user authentication through acoustic sensing on smartphones," *IEEE/ACM Trans. Netw.*, vol. 27, no. 1, pp. 447–460, Feb. 2019.
[156] Q. Wang *et al.*, "Voicepop: A pop noise based anti-spoofing system for voice authentication on smartphones," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2019, pp. 2062–2070.
[157] Z. Yan and S. Zhao, "A usable authentication system based on personal voice challenge," in *Proc. Int. Conf. Adv. Cloud Big Data (CBD)*, 2016, pp. 194–199.
[158] D.-S. Kim and K.-S. Hong, "Multimodal biometric authentication using teeth image and voice in mobile environment," *IEEE Trans. Consum. Electron.*, vol. 54, no. 4, pp. 1790–1797, Nov. 2008.
[159] R. Johnson, W. J. Scheirer, and T. E. Boult, "Secure voice-based authentication for mobile devices: Vaulted voice verification," in *Biometric and Surveillance Technology for Human and Activity Identification X*, vol. 8712. Bellingham, WA, USA: Int. Soc. Opt. Photon., 2013, Art. no. 87120P.
[160] L. Zhang, S. Tan, J. Yang, and Y. Chen, "Voicelive: A phoneme localization based liveness detection for voice authentication on smartphones," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, 2016, pp. 1080–1091.
[161] B. S. Atal, "Effectiveness of linear prediction characteristics of the speech wave for automatic speaker identification and verification," *J. Acoust. Soc. America*, vol. 55, no. 6, pp. 1304–1312, 1974.
[162] D. A. Reynolds, "An overview of automatic speaker recognition technology," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, vol. 4, 2002, pp. 4072–4075.
[163] T. Kinnunen and H. Li, "An overview of text-independent speaker recognition: From features to supervectors," *Speech Commun.*, vol. 52, no. 1, pp. 12–40, 2010.
[164] M. I. Gofman, S. Mitra, T.-H. K. Cheng, and N. T. Smith, "Multimodal biometrics for enhanced mobile device security," *Commun. ACM*, vol. 59, no. 4, pp. 58–65, 2016.
[165] M. Khamis, F. Alt, M. Hassib, E. von Zezschwitz, R. Hasholzner, and A. Bulling, "Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices," in *Proc. CHI Conf. Extended Abstracts Human Factors Comput. Syst.*, 2016, pp. 2156–2164.
[166] H. Saevanee, N. Clarke, S. Furnell, and V. Biscione, "Continuous user authentication using multi-modal biometrics," *Comput. Security*, vol. 53, pp. 234–246, Sep. 2015.
[167] T. J. Neal, D. L. Woodard, and A. D. Striegel, "Mobile device application, Bluetooth, and Wi-Fi usage data as behavioral biometric traits," in *Proc. IEEE 7th Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, 2015, pp. 1–6.
[168] K. B. Raja, R. Raghavendra, M. Stokkenes, and C. Busch, "Multi-modal authentication system for smartphones using face, iris and periocular," in *Proc. Int. Conf. Biometrics (ICB)*, 2015, pp. 143–150.
[169] M. Stokkenes, R. Ramachandra, K. B. Raja, M. K. Sigaard, and C. Busch, "Feature level fused templates for multi-biometric system on smartphones," in *Proc. 5th Int. Workshop Biometrics Forensics (IWBF)*, 2017, pp. 1–5.
[170] L. C. O. Tiong, S. T. Kim, and Y. M. Ro, "Multimodal face biometrics by using convolutional neural networks," *J. Korea Multimedia Soc.*, vol. 20, no. 2, pp. 170–178, 2017.
[171] I. Lamiche, G. Bin, Y. Jing, Z. Yu, and A. Hadid, "A continuous smartphone authentication method based on gait patterns and keystroke dynamics," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 11, pp. 4417–4430, 2019.
[172] X. Pang, L. Yang, M. Liu, and J. Ma, "Mineauth: Mining behavioural habits for continuous authentication on a smartphone," in *Proc. Aust. Conf. Inf. Security Privacy*, 2019, pp. 533–551.
[173] A. Acien, A. Morales, R. Vera-Rodriguez, J. Fierrez, and R. Tolosana, "Multilock: Mobile active authentication based on multiple biometric and behavioral patterns," in *Proc. 1st Int. Workshop Multimodal Understanding Learn. Embodied Appl.*, 2019, pp. 53–59.
[174] H. G. Kayacik, M. Just, L. Baillie, D. Aspinall, and N. Micallef, "Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors," 2014. [Online]. Available: arXiv:1410.7743.
[175] J. Zhu, P. Wu, X. Wang, and J. Zhang, "Sensec: Mobile security through passive sensing," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, 2013, pp. 1128–1133.
[176] G. Fenu and M. Marras, "Controlling user access to cloud-connected mobile applications by means of biometrics," *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 47–57, Jul./Aug. 2018.
[177] H. Lin, J. Liu, and Q. Li, "TDSD: A touch dynamic and sensor data based approach for continuous user authentication," in *Proc. PACIS*, 2018, p. 294.
[178] H. C. Volaka, G. Alptekin, O. E. Basar, M. Isbilen, and O. D. Incel, "Towards continuous authentication on mobile phones using deep learning models," *Procedia Comput. Sci.*, vol. 155, pp. 177–184, Aug. 2019.
[179] 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. 3, p. 345, 2016.
[180] M. P. Centeno, Y. Guan, and A. van Moorsel, "Mobile based continuous authentication using deep features," in *Proc. 2nd Int. Workshop Embedded Mobile Deep Learn.*, 2018, pp. 19–24.
[181] 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.
[182] Z. Ba, Z. Qin, X. Fu, and K. Ren, "CIM: Camera in motion for smartphone authentication," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2987–3002, Nov. 2019.
[183] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 125–143, Jun. 2006.
[184] F. Rahman, M. O. Gani, G. M. T. Ahsan, and S. I. Ahamed, "Seeing beyond visibility: A four way fusion of user authentication for efficient usable security on mobile devices," in *Proc. IEEE 8th Int. Conf. Softw. Security Rel. Companion*, 2014, pp. 121–129.
[185] G. Li and P. Bours, "Studying WiFi and accelerometer data based authentication method on mobile phones," in *Proc. 2nd Int. Conf. Biometric Eng. Appl.*, 2018, pp. 18–23.

[186] K. B. Raja, R. Raghavendra, M. Stokkenes, and C. Busch, "Fusion of face and periocular information for improved authentication on smartphones," in *Proc. 18th Int. Conf. Inf. Fusion (Fusion)*, 2015, pp. 2115–2120.

Mohammed Abuhamad received the M.S. degree in artificial intelligence from the National University of Malaysia, Bangi, Malaysia, in 2013, the first Ph.D. degree in computer science from the University of Central Florida, Orlando, FL, USA, in 2020, and the second Ph.D. degree in computer engineering from INHA University, Incheon, South Korea, in 2020.

He is currently an Assistant Professor with the Loyola University Chicago, Chicago, IL, USA. His research interests include software security, machine learning, authentication, privacy, and deep learning-based applications.

Ahmed Abusnaina (Graduate Student Member, IEEE) received the B.Sc. degree in computer engineering from the An-Najah National University, Nablus, Palestine, in 2018. He is currently pursuing the Ph.D. degree with the Department of Computer Science, University of Central Florida, Orlando, FL, USA.

His research interests include software security, and machine learning robustness applications in the field of security and privacy.

Daehun Nyang received the B.Eng. degree in electronic engineering from the Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 1994, and the M.S. and Ph.D. degrees in computer science from Yonsei University, Seoul, South Korea, in 1996 and 2000, respectively.

He has been a Senior Member of engineering staff with the Electronics and Telecommunications Research Institute, Gwangju, South Korea, from 2000 to 2003. From 2003 to 2020, he was a Full Professor with the Computer Information Engineering Department, Inha University, Incheon, South Korea, where he was also the Founding Director of the Information Security Research Laboratory. Since 2020, he has been a Full Professor with Ewha Womans University, Seoul. His research interests include AI-based security, network security, traffic measurement, privacy, usable security, and biometrics and cryptography.

Prof. Nyang is a member of the board of directors and an editorial board of *ETRI Journal* and also Korean Institute of Information Security and Cryptology.

David Mohaisen (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees from the University of Minnesota, Minneapolis, MN, USA, in 2012.

He was an Assistant Professor with SUNY Buffalo, Buffalo, NY, USA, from 2015 to 2017, and a Senior Research Scientist with Verisign Labs, Reston, VA, USA, from 2012 to 2015. He is currently an Associate Professor with the University of Central Florida, Orlando, FL, USA, where he directs the Security and Analytics Lab (SEAL). His research interests are in the areas of networked systems and their security, online privacy, and measurements.

Dr. Mohaisen is an Associate Editor of the IEEE TRANSACTIONS ON MOBILE COMPUTING, and IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and is a Senior Member of ACM in 2018.