Hindawi
Security and Communication Networks
Volume 2019, Article ID 5452870, 20 pages
https://doi.org/10.1155/2019/5452870

Review Article

Authentication and Authorization for Mobile IoT Devices Using Biofeatures: Recent Advances and Future Trends

Mohamed Amine Ferrag,[1] **Leandros Maglaras**,[2,3] **and Abdelouahid Derhab**[4]

[1]*Department of Computer Science, Guelma University, B.P. 401, 24000, Algeria*
[2]*School of Computer Science and Informatics, De Montfort University, Leicester, UK*
[3]*National Cyber Security of Greece, General Secretariat of Digital Policy, Athens, Greece*
[4]*Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia*

Correspondence should be addressed to Leandros Maglaras; leandrosmag@gmail.com

Received 25 January 2019; Revised 4 April 2019; Accepted 22 April 2019; Published 5 May 2019

Guest Editor: Jorge B. Bernabe

Biofeatures are fast becoming a key tool to authenticate the IoT devices; in this sense, the purpose of this investigation is to summarise the factors that hinder biometrics models' development and deployment on a large scale, including human physiological (e.g., face, eyes, fingerprints-palm, or electrocardiogram) and behavioral features (e.g., signature, voice, gait, or keystroke). The different machine learning and data mining methods used by authentication and authorization schemes for mobile IoT devices are provided. Threat models and countermeasures used by biometrics-based authentication schemes for mobile IoT devices are also presented. More specifically, we analyze the state of the art of the existing biometric-based authentication schemes for IoT devices. Based on the current taxonomy, we conclude our paper with different types of challenges for future research efforts in biometrics-based authentication schemes for IoT devices.

1. Introduction

Biometric identification enables end-users to use physical attributes instead of passwords or PINs as a secure method of accessing a system or a database. Biometric technology is based on the concept of replacing "one thing you have with you" with "who you are," which has been seen as a safer technology to preserve personal information. The possibilities of applying biometric identification are really enormous.

Biometric identification is applied nowadays in sectors where security is a top priority [1], like airports, and could be used as a means to control border-crossing at sea, land, and air frontier [2]. Especially for the air traffic area, where the number of flights will be increased by 40% before 2013, the authentication of mobile IoT devices will be achieved when the biofeatures models become sufficiently mature, efficient, and resistant to IoT attacks.

Another area where biometric identification methods are starting to be adopted is electronic IDs. Biometric identification cards such as the Estonian and Belgian national ID cards were used in order to identify and authenticate eligible voters during elections. Moving one step further, Estonia has introduced the Mobile-ID system that allows citizens to conduct Internet voting [3] and combines biometric identification and mobile devices. This system that was quite innovative when it was initially introduced possesses several threats to the electoral procedure and was criticized for being insecure [4].

According to a survey by Javelin Strategy & Research, in 2014, $16 billion was stolen by 12.7 million people who were victims of identity theft in the US only [5]. This amount is calculated without taking into account the economic problems and psychological oppression that victims of this fraud suffer. From the banking sector and businesses to access to homes, cars, personal computers, and mobile devices, biometric technology offers the highest level of security in terms of privacy and privacy protection and secure access.

Mobile devices are nowadays an essential part of our everyday life, as they are used for a variety of mobile applications. Performing biometric authentication through mobile devices can provide a stronger mechanism for identity verification as the two authentication factors, "something you have" and "something you are," are combined. Several

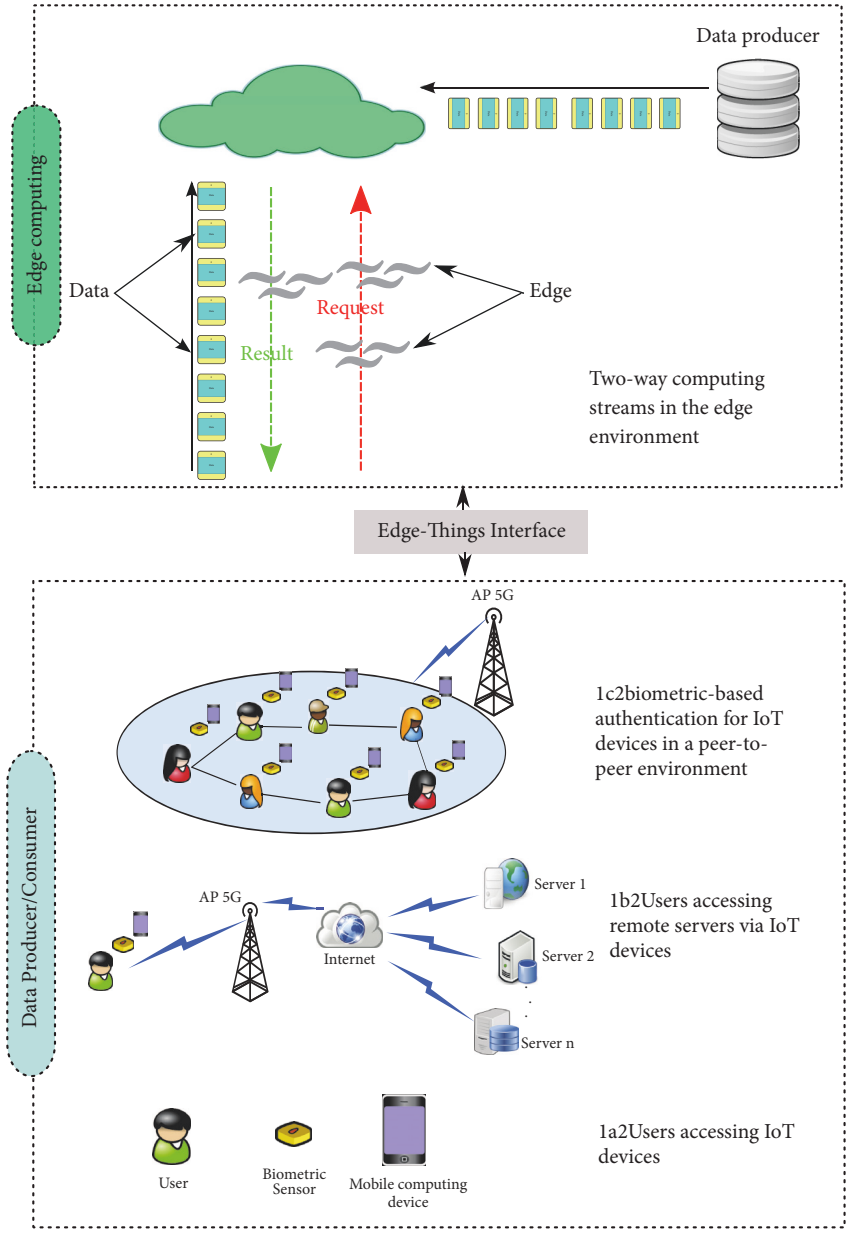

Figure 1: Types of communication for IoT devices in edge environments during the authentication and authorization. (a) Users accessing IoT devices, (b) users accessing remote servers via IoT devices, and (c) biometric-based authentication for IoT devices in a peer-to-peer environment.

solutions that include multibiometric and behavioral authentication platforms for telecom carriers, banks, and other industries were recently introduced [6].

In the literature, many authentication schemes based on biofeatures models for mobile IoT devices have been proposed. As shown in Figure 1, the schemes can perform two different authentication operations: they either (a) authenticate the users to access the mobile devices or (b) authenticate the users to access remote servers through mobile devices. The main challenges that are facing biometric-based authentication schemes are (1) how to design an authentication mechanism that is free from vulnerabilities, which can be exploited by adversaries to make illegal accesses, and (2) how to ensure that the user's biometric reference templates are not compromised by a hacker at the device level or the remote-server level. This paper extends the work we have presented in [7].

Our contributions in this work are the following:

(i) We classify the related surveys according to several criteria, including deployment scope, focus biometric area, threat models, countermeasures, and ML/DM algorithms.

(ii) We present the machine learning and data mining methods used by authentication and authorization

Table 1: Related surveys on biometric authentication.

Reference	Deployment scope	Focus biometric area	Threat models	Countermeasures	ML and DM
Gafurov (2007) [8]	Not mobile	Gait recognition	No	No	No
Revett et al. (2008) [9]	Not mobile	Mouse dynamics	No	No	No
Yampolskiy and Govindaraju (2008) [10]	Not mobile	Behavioral-based	No	No	No
Shanmugapriya and Padmavathi (2009) [11]	Not mobile	Keystroke dynamics	No	No	Yes
Karnan et al. (2011) [12]	Not mobile	Keystroke dynamics	No	No	Yes
Banerjee and Woodard (2012) [13]	Not mobile	Keystroke dynamics	No	No	Yes
Teh et al. (2013) [14]	Not mobile	Keystroke dynamics	No	No	Yes
Bhatt et al. (2013) [15]	Not mobile	Keystroke dynamics	No	No	Yes
Meng et al. (2015) [16]	Mobile device	All	Yes	Yes	Partial
Teh et al. (2016) [17]	Mobile device	Touch dynamics	No	No	Yes
Mahfouz et al. (2017) [18]	Smartphone	behavioral-based	No	No	Yes
Mahadi et al. (2018) [19]	Not mobile	behavioral-based	No	No	Yes
Sundararajan and Woodard (2018) [20]	Not mobile	All	No	No	Yes
Rattani and Derakhshani (2018) [21]	Mobile device	Face recognition	Yes	Yes	Yes
Our survey	Mobile IoT device	All	Yes	Yes	Yes

ML and DM: machine learning (ML) and data mining (DM) algorithms

schemes for mobile IoT devices, including unsupervised, semisupervised, and supervised approaches.

(iii) We present all the biofeatures used by authentication and authorization schemes for mobile IoT devices.

(iv) We provide a comprehensive analysis and qualitative comparison of the existing authentication and authorization schemes for mobile IoT devices.

(v) We emphasize the challenges and open issues of authentication and authorization schemes for mobile IoT devices.

The rest of this paper is organized as follows. Section 2 gives the related surveys on biometric authentication. In Section 3, we present the different machine learning and data mining algorithms used by authentication and authorization schemes for mobile IoT devices. In Section 4, we provide the new trends of biometric technologies including human physiological (e.g., face, eyes, fingerprints-palm, and electrocardiogram) and behavioral features (e.g., signature, voice, gait, or keystroke). In Section 5, we clearly highlight the pros and cons of the existing authentication and authorization schemes for mobile IoT devices. Then, we discuss the challenges and suggest future research directions in both Sections 6 and 7. Lastly, Section 8 presents conclusions.

2. Related Surveys on Biometric Authentication

In the literature, there are different related surveys that deal with user authentication. Although some of them covered different authentication methods [103–105], we only consider those that were fully dedicated for biometric authentication. As shown in Table 1, we classify the surveys according to the following criteria:

(i) *Deployment scope:* it indicates whether the authentication scheme is deployed on mobile devices or not.

(ii) *Focus biometric area:* it indicates whether the survey focused on all/specific biometric features.

(iii) *Threat models:* it indicates whether the survey considered the threats against the authentication schemes.

(iv) *Countermeasures:* it indicates whether the survey focused on and considered the countermeasures to defend the authentication schemes.

(v) *Machine learning (ML) and data mining (DM) algorithms:* they indicate whether the survey mentions for each solution the used machine learning or data mining method.

Some surveys described the authentication schemes that only consider specific biofeatures. For instance, the surveys in [11–15] only focused on the keystroke dynamics. On the other hand, Gafurov [8] presented biometric gait recognition systems. Revett et al. [9] surveyed biometric authentication systems that rely on mouse movements. Yampolskiy and Govindaraju [10] presented a comprehensive study on behavioral biometrics. Mahadi et al. [19] surveyed behavioral-based biometric user authentication and determined the set of best classifiers for behavioral-based biometric authentication. Sundararajan and Woodard [20] surveyed 100 different approaches that leveraged deep learning and various biometric modalities to identify users. Teh et al. [17] presented different authentication solutions that rely on touch dynamics in mobile devices. Rattani and Derakhshani [21] provided the state of the art related to face biometric authentication schemes that are designed for mobile devices. They also discussed the spoof attacks that target mobile face biometrics as well as the antispoofing methods. Mahfouz et al. [18] surveyed the behavioral biometric authentication schemes that are applied on smartphones. Meng et al. [16] surveyed the

authentication frameworks using biometric user on mobile phones. They identified eight potential attack against these authentication systems along with promising countermeasures. Our survey and [16] both focus on authentication schemes that are designed for mobile device and consider all the biometric features and deal with threat models and countermeasures. However, [16] does not give information related to the used machine learning or data mining method of all the surveyed solutions. In addition, [16] only covers papers up to 2014, whereas the coverage of our survey is up to 2018. To the best of our knowledge, this work is the first that thoroughly covers threats, models, countermeasures, and the machine learning algorithms of the biometric authentication schemes.

3. Machine Learning and Data Mining Algorithms

In this section, we list the different machine learning and data mining algorithms used by biometric-based authentication schemes for IoT devices, as presented in Table 2.

3.1. Support Vector Machine (SVM). The SVM is a popular and powerful binary classifier, which aims to find a hyperplane within the feature space that separates between two classes. SVM is used by seven authentication schemes for IoT devices in edge environments using biofeatures [24, 32–34, 72, 78, 92].

In [24], Frank et al. used two classifiers, k-nearest-neighbors (kNN) and SVM, with an RBF kernel. In this study, two classes are chosen, namely, (i) user of interest and (ii) the rest of users. In the training data phase, this study tunes the two relevant parameters, that is, γ and C of the RBF-SVM, which are tuned under fivefold cross-validation. The first parameter γ is used for controlling the Gaussian radial-basis function. The second parameter C is used for controlling the trade-off between maximizing the margin and minimizing the number of exceptions.

In Sitova et al.'s work [32], an SVM classifier with scaled Manhattan (SM) and scaled Euclidian (SE) is used to perform verification experiments. For parameter tuning, the RBF kernel was selected to perform a grid search to find the parameter.

In order to detect faces of a particular size, Sarkar et al. [33] introduced a face detection algorithm, which is based on deep feature combined with a SVM classifier. Specifically, the study passes the image through a deep convolutional neural network; then they used train SVMs of different sizes in order to achieve scale invariance. During training step, Sarkar et al.'s scheme uses 5202 images from the UMD-AA database, which is a database of 720p videos and touch gestures of users on a mobile device (iPhone). The experimental results showed that the proposed idea can detect the partial or the extremely posed faces in IoT environment.

The approach described by Mahbub et al. [92] is a framework for authentication and authorization of users' faces on mobile IoT devices. Their approach trains a linear SVM with statistical features. The study used the Active Authentication Dataset, which contains the front-facing camera face video for 50 iPhone users (43 males and 7 females) with three different ambient lighting conditions: well-lit, dimly-lit, and natural daylight. Compared to Viola-Jones face detector, Mahbub et al.'s framework can achieve superior performance.

In another study, the SVM classifier was attempted as the learning algorithm by Gunasinghe and Bertino [34], face as the biofeature, and eigenfaces as the feature extraction algorithm. The trained SVM classifier helps to the artifacts stored in the mobile IoT devices. Compared to Mahbub et al.'s [92] approach, the protocol in [34] considers privacy-preserving of the training data, which uses three secrets ($S_i : i \in \{1, 2, 3\}$) in different phases of the scheme: S_1 of size 128 $bits$, S_2 of size 160 $bits$, and S_3 of size 256 $bits$.

Chen et al. [72] introduced a two-factor authentication protocol using rhythm, which can be applied for mobile IoT devices. Specifically, Chen et al.'s protocol employs SVM as a machine learning classifier and LibSVM in the implementation phase. The false-positive and false-negative rates achieve 0.7% and 4.2%, respectively. In general, there are two behavioral biometric modalities in the construction of an authentication scheme based on the biofeature: (1) using one behavioral biometric model, which does not need any additional hardware to capture data, and (2) using a combination of the behavioral biometric models.

3.2. Deep Learning Approach. Actually, deep learning is used to authenticate low-power devices in the IoT networks. Deep learning approach is based on an artificial neural network (ANN), consisting of many layers of neurons, referred to as hidden layers, between two other layers: input and output. Each layer receives and interprets information from the previous layer. Unlike SVM, the learning runtime increases when the number of features in an ANN increases. Ferdowsi and Saad [39] proposed a deep learning method based on the long short-term memory (LSTM), which uses the fingerprints of the signal y generated by an IoT mobile device. In addition, LSTM algorithm is used to allow an IoT mobile device updating the bit stream by considering the sequence of generated data. The paper expressed that the findings reported that dynamic LSTM watermarking is able to detect some attacks such as eavesdropping.

Das et al. [40] used a deep learning-based classifier to have a faster system against high-power adversaries. Similar to the work in [39], this study uses the long short-term memory (LSTM). The experiments used a testbed of LoRa low-power wireless, which consists of 29 Semtech SX1276 chips as LoRa transmitters and a Semtech SX1257 chip as the receiver. The experimental results showed that the classification performance is more promising with respect to state-of-the-art LoRa transmitters.

The work by Bazrafkan and Corcoran [106] used a deep U-shaped network with 13 layers for the segmentation task. The study used a 3x3 kernel that maps the input to the first convolutional hidden layer in order to enhance iris authentication for mobile IoT devices. They used two databases: (1) CASIA Thousand, which contains 20k images, and (2)

Table 2: Machine learning and data mining methods used by authentication and authorization schemes for mobile IoT devices.

Machine learning and data mining methods	Schemes	EER	Accuracy	FAR	FRR
Agglomerative complete link clustering approach	[22]	19.68%	n/a	n/a	n/a
Support vector distribution estimation	[23]	0.52%	n/a	n/a	n/a
	[24]	0 - 4%	n/a	n/a	n/a
Gaussian mixture model	[25]	2.13%	n/a	n/a	n/a
k-nearest-neighbors (kNN)	[24]	0% - 4%	n/a	n/a	n/a
	[26]	n/a	87.8%	18.3%	6.1%
	[27]	n/a	n/a	0.37%	1.12%
	[28]	n/a	96.4%	3.6%	0%
	[29]	n/a	96.86%	n/a	n/a
	[30]	3.7%	n/a	n/a	n/a
	[31]	0.5%	n/a	n/a	n/a
Support vector machine (SVM)	[24]	0 - 4%	n/a	n/a	n/a
	[32]	7.16%	n/a	n/a	n/a
	[33]	n/a	96.0%	n/a	n/a
	[34]	n/a	n/a	0.023%	0.044%
	[35]	n/a	n/a	2.10%	2.24%
	[36]	n/a	n/a	0.004%	0.01%
	[26]	n/a	87.8%	18.3%	6.1%
	[27]	n/a	n/a	0.37%	1.12%
	[37]	1.3%	n/a	2.96%	0.86%
	[35]	n/a	n/a	2.61%	2.51%
	[29]	n/a	98%	n/a	n/a
A computation efficient statistical classifier	[38]	10.00%	n/a	9.78%	10.00%
Deep learning	[39]	0.02%	n/a	n/a	n/a
	[40]	n/a	99.58%	n/a	n/a
	[41]	n/a	98.55-99.71%	n/a	n/a
	[42]	n/a	99.10%	n/a	n/a
	[43]	n/a	97.5%	n/a	n/a
Local binary patterns algorithm	[44]	0.1-0.13%	n/a	n/a	n/a
Mel-frequency cepstral coefficients	[45]	n/a	80.6%	0.01%	15%
Pupillary light reflex	[46]	11.37%	n/a	n/a	n/a
Euclidean distance, hamming distance	[47]	n/a	0.9992%	0%	0.0015%
Deep convolutional neural network	[33]	n/a	96.0%	n/a	n/a
	[48]	n/a	n/a	1.5%	n/a
	[49]	8.6%	91.4	n/a	n/a
	[50]	n/a	93.2	n/a	n/a
	[51]	3.1%	n/a	n/a	n/a
Genetic algorithm	[52]	0.46%	n/a	n/a	n/a
Artificial neural network (ANN)	[53]	2.13%	n/a	n/a	n/a
	[54]	2.46%	n/a	n/a	n/a
Gauss-Newton based neural network	[55]	4.1%	n/a	3.33%	3.33%
Radial integration transform	[56]	10.8%	n/a	n/a	n/a

Table 2: Continued.

Machine learning and data mining methods	Schemes	EER	Accuracy	FAR	FRR
Weibull distribution	[57]	2-10%	n/a	n/a	n/a
Online learning algorithms	[58]	0.04%	96%	n/a	n/a
Random forest (RF)	[59]	7.5%	n/a	17.66%	n/a
Neural network (NN)	[27]	n/a	n/a	0.37%	1.12%
	[28]	n/a	96.4%	3.6%	0%
	[60]	n/a	n/a	15%	0%
Circular integration transform	[56]	10.8%	n/a	n/a	n/a
Decision tree (DT)	[26]	n/a	86.4%	16.1%	11.0%
	[35]	n/a	n/a	2.10%	2.24%
	[61]	n/a	n/a	0.88%	9.62%
	[62]	n/a	n/a	0.005%	3.027%
	[29]	n/a	91.72%	n/a	n/a
Learning Algorithm for Multivariate Data Analysis (LAMDA)	[63]	n/a	n/a	0%	0.36%
Bayesian network (BN)	[35]	n/a	n/a	2.47%	2.53%
	[29]	n/a	95.02%	n/a	n/a
Naive Bayes	[29]	n/a	93.7%	n/a	n/a
	[36]	n/a	n/a	0.004%	0.01%
	[64]	8.21%	n/a	n/a	n/a
Pearson product-moment correlation coefficient (PPMCC)	[28]	n/a	96.4%	3.6%	0%
Keyed random projections and arithmetic hashing	[65]	7.28%	n/a	n/a	n/a
One-dimensional multiresolution local binary patterns	[66]	7.89%	n/a	1.57%	0.39%

EER: equal error rate; FAR: false acceptance rate, FRR: false rejection rate; n/a: not available.

Bath 800, which contains 24156 images. The segmentation results are reported as 98.55% for the Bath 800 and 99.71% for CASIA Thousand. The paper also states the benefits of the deep learning technique such as efficient segmentation on large data sets.

In their study, Bayar and Stamm [42] use a universal forensic approach using deep learning in order to detect multiple types of image forgery. For image recognition, the convolutional neural networks (CNNs) are used as tool from deep learning. Specifically, the CNN proposed contains eight layers: the proposed new convolutional layer, two convolutional layers, two max-pooling layers, and three fully connected layers. The first layer of the network is 227×227 grayscale image. The proposed CNN is evaluated as a binary and multiclass classifier. Although the false-positive rate is not reported, the Caffe deep learning framework is used, which shows that the CNN proposed model can distinguish between unaltered and manipulated images with at least 99.31% and 99.10% accuracy for a binary and multiclass classifier, respectively.

3.3. Deep Convolutional Neural Network. The deep convolutional neural networks (DCNNs) for face detection were attempted by Ranjan et al. [107], which can be classified into two categories: the region-based approach and the sliding-window approach. The DCNN can identify whether a given proposal contains a face or not.

Based on deep learning and random projections, Liu et al. [48] proposed a novel finger vein recognition algorithm, named FVR-DLRP, which could be used for mobile IoT devices. The FVR-DLRP algorithm uses four main phases, namely, (1) feature extraction, (2) random projection, (3) training, and (4) matching. The finger vein feature extraction is based on 3×3 regions. The Johnson–Lindenstrauss theorem is used for the random projections. In the training phase, the deep belief network is applied to generating the biometric template. The experimental results on finger vein laboratory database, named FV_NET64, involving 64 people's finger vein image and each of them contributing 15 acquisitions, show that the FVR-DLRP algorithm achieves 91.2% for recognition rate (GAR) and 0.3% for false acceptance rate (FAR). In

the study by Sarkar et al. [33], a deep convolutional neural network is proposed for mobile IoT devices. According to the study, the OpenCL and RenderScript based libraries for implementing deep convolutional neural networks are more suitable for mobile IoT devices compared to the CUDA based schemes.

3.4. Decision Tree (DT). DTs are a type of learn-by-example pattern recognition method, which were used by five studies [26, 35, 61, 62, 108]. In [61], Sheng et al. proposed a parallel decision trees-based system in order to authenticate users based on keystroke patterns, which could be applied for mobile IoT devices. According to the study, a parallel DT alone cannot solve the authentication on keystroke patterns. The training data contains 43 users; each of them typed a given common string of 37 characters. The study achieves 9.62% for FRR and 0.88% for FAR. Therefore, Kumar et al. [62] presented a fuzzy binary decision tree algorithm, named FBDT, for biometric-based personal authentication. The FBDT was able to be detected with FAR=0.005% and FRR=3.027% on palm print and FAR=0.023% and FRR=8.1081% on iris and FAR=0% and FRR=2.027% on the bimodal system. To enhance the network authentication in ZigBee devices, Patel et al. [108] presented an authentication system that employs ensemble decision tree classifiers. Specifically, the study applied multiclass AdaBoost ensemble classifiers and nonparametric random forest on the fingerprinting arena.

3.5. k-Nearest-Neighbors (kNN). The kNN algorithm identifies the k training observations to belong to a group among a set of groups based on a distance function in a vector space to the members of the group [28]. In our study, we found that it is always combined with other classifiers in order to provide a fast classification. The study in [24] uses the kNN algorithm and a support vector machine with an RBF kernel. The study in [26] combines three classifiers, namely, the kNN algorithm, support vector machines, and decision trees. The study in [27] combines three models: (1) a nearest-neighbor-based detector model, (2) a neural network detector model, and (3) a support vector machine model. The study by Jagadeesan and Hsiao [28] incorporates statistical analysis, neural networks, and kNN algorithms, in which the experimental results show that the identification accuracy is 96.4% and 82.2% for the application-based model and the application-independent model, respectively.

3.6. Statistical Models. In order to perform authentication of the user's identity on mobile IoT devices, Tasia et al. [38] used a computation efficient statistical classifier, which has low computational complexity compared to fuzzy logic classifiers and does not require comparison with other users' samples for identification. Therefore, hidden Markov model is a statistical model where Kim and Hong [25] used an embedded hidden Markov model algorithm and the two-dimensional discrete cosine transform for teeth authentication. For the voice authentication on mobile IoT devices, the study uses pitch and mel-frequency cepstral coefficients as feature parameters and a Gaussian mixture model algorithm to model the voice signal. In the experiment section, Kim's study used an HP iPAQ rw6100 mobile device equipped with a camera and sound-recording device. The study reported an ERR of 6.42% and 6.24% for teeth authentication and voice authentication, respectively.

3.7. Naive Bayes. To map from the feature space to the decision space, Fridman et al. [36] used the Naive Bayes classifier, which is based on the so-called Bayesian theorem. In the experiment section, the study reached a false acceptance rate of 0.004 and a false rejection rate of 0.01 after 30 seconds of user interaction with the device. Therefore, Traore et al. [64] considered two different biometric modalities, namely, keystroke and mouse dynamics. Their study used a Bayesian network to build the user profile and then used it to classify the monitored samples. The experimental results show that the mouse dynamics model has a reached an equal error rate (EER) of 22.41%, which is slightly lower than the keystroke dynamics that reached an EER of 24.78%. In addition, Bailey et al. [35] used a Bayesian network with two machine learning algorithms: LibSVM and J48. The results achieved a full-fusion false acceptance rate of 3.76% and a false rejection rate of 2.51%.

To solve the problem of verifying a user, Buriro et al. [29] proposed AnswerAuth, an authentication mechanism, which is based on the extracted features from the data recorded using the built-in smartphone sensors. In effect, the AnswerAuth mechanism is tested using a dataset composed of 10,200 patterns (120 from each sensor) from 85 users and six classification techniques are used: Bayes network, naive Bayes, SVM, kNN, J48, and random forest. According to the study, random forest classifier performed the best with a true acceptance rate of 99.35%.

3.8. Observations Related to Performance Metrics. There are several performance metrics by which the machine learning and data mining methods for authentication could be compared: equal error rate (EER), accuracy, false acceptance rate (FAR), and false rejection rate (FRR).

The EER of 19.68% is obtained by Maiorana et al.'s scheme [76] when using all the first E = 10 acquisitions of each user for enrollment. The BEAT scheme [23] achieves an average equal error rate of 0.5% with 3 gestures and one of 0.52% with single signature using only 25 training samples. The Touchalytics framework [24] trains user profiles based on vertical and horizontal strokes using a k-nearest neighbor classifier and a Gaussian RBF kernel support vector machine, in which these classifiers achieve EER between 0% and 4%, depending on the application scenario. Kim and Hong's method [25] is evaluated using 1000 teeth images and voices, which achieves an EER of 2.13%. Shen et al.'s approach [27] achieves a practically useful level of performance with FAR of 0.37% and FRR of 1.12% obtained by the SVM detector, which shows that mouse characteristics extracted from frequent behavior segments are much more stable. The average accuracy of application-based user reauthentication system proposed by Jagadeesan and Hsiao [28] is 96.4% with 0% FRR and 3.6% FAR for 2-, 3-, 4-, and 5-user sets. Compared to the work in [109], the HMOG scheme [32]

achieves the lowest EERs (7.16% in walking and 10.05% in sitting).

Based on the mouse data from 48 users, Nakkabi et al's scheme [63] achieves a false acceptance rate of 0% and a false rejection rate of 0.36%. Compared to Nakkabi et al.'s scheme [63], Zheng et al.'s scheme [37] achieves an equal error rate of 1.3% with just 20 mouse clicks under two sets of data: one set of 30 users under controlled circumstances and another set of over 1,000 users on a forum website. The EBDL scheme [35] produces a FAR of 2.24% and FRR of 2.10%, which are in line with previous singular modality work. On the full dataset, the authentication system proposed by Fridman et al. [36] achieved FAR of 0.004% and FRR of 0.01% after 30s of user interaction with the device. The study by Abate et al. [44] uses the local binary patterns (LBPs) algorithm for authenticating the users on mobile devices through ear shape and arm gesture, which achieved EER values of 0.1 for the combined ear-arm and 0.13 for the single-arm gesture. Annapurani et al. [47] use the Euclidean method, in which the authentication rate is 99.8% and 99.7% for the fused one and the tragus compared to the shape of the ear which has 99.55%.

Ferdowsi and Saad [39] proposed a deep learning algorithm using long short-term memory (LSTM) which is trained on accelerometer data, and the testing error is close to 0.02%, which is acceptable for an IoT application. Therefore, Das et al. [40] used an LSTM unit of length 2048 and with $N_p = 21$ *layers*, which archives the classification accuracy of 99.58%. The study by Bazrafkan and Corcoran [41] enhances iris authentication on handheld devices using deep learning, which trained the network on the augmented databases (Bath 800 and CASIA Thousand). The segmentation results for the test set on these two databases were 98.55% for Bath 800 and 99.71% for CASIA Thousand. Bayar and Stamm [42] trained multiclass convolutional neural networks (CNN) over 56 000 iterations, which achieve an accuracy of 99.10% of detecting the different four types of forgery. Alhussein and Muhammad [43] show that the voice pathology detection accuracy reaches up to 97.5% using the transfer learning of CNN models. The results obtained by the FBDT scheme [62] validate the effectiveness of the biometric-based authentication, in which the best error rates are reported as FAR 0.005% and FRR 3.027% on palm print, FAR 0.023% and FRR 8.1081% on the iris, and FAR 0% and FRR 2.027% on the bimodal system.

The study by Taigman et al. [49] proposed a DeepFace framework, which reaches an accuracy of 97.35% on the Labeled Faces in the Wild (LFW) dataset, reducing the error of the current state of the art by more than 27%. In addition, the DeepFace framework reports an accuracy of 91.4% on the YouTube Faces (YTF) dataset, which reduces the error of the previous best methods including MBGS+SVM [110] and APEM+FUSION [111]. Similar to Taigman et al. [49], the study by Sun et al. [50] reaches an accuracy of 99.47% on the LFW dataset and 93.2% on the YTF dataset. For more information about deep learning for understanding faces, we refer the reader to the study by Ranjan et al. [107].

The Gaithashing scheme [56] achieves EER=0% for type 1 and 3 impostors (i.e., type 1 impostor uses his/her own gait features and his/her own token, while type 3 impostors use compromised gait features and they own token for authentication). In addition, the Gaithashing scheme achieves very high accuracy (EER=10.8%) for type 2 impostors (i.e., an impostor that uses a compromised token and his/her own gait features for authentication). Therefore, Alpar [55] proposed a novel frequency based authentication method and a Gauss-Newton based neural network classifier in order to provide the foundations of frequency authentication to enhance keystroke authentication protocols. The conducted experiments are 3.33% FAR, 3.33% FRR, and 4.1% EER, which all are promising. Khalifa et al.'s system [52] uses genetic algorithm, which shows that the fusion of the three unimodal systems has improved significantly the performance of the multimodal system. In addition, the EER has increased from 2.51% to 0.46%.

Table 3: Bio-features used by authentication schemes for IoT devices in edge environments.

Biofeature	Schemes
Gaze gestures	[67–69]
Electrocardiogram	[70, 71]
Voice recognition	[25, 43, 72, 73]
Signature recognition	[23]
Gait recognition	[74]
Behavior profiling	[23, 24, 32, 75]
Keystroke dynamics	[38, 53, 61, 64, 76–78]
Touch dynamics	[17, 69]
Fingerprint	[62, 79–84]
Smart card	[85–87]
Multitouch interfaces	[88, 89]
Graphical password	[90]
Face recognition	[33, 34, 91–93]
Iris recognition	[41, 91, 94, 95]
Rhythm	[72]
Capacitive touchscreen	[96]
Ear shape	[44]
Arm gesture	[44]
Plantar biometrics	[97]
Mouse dynamics	[27, 35, 37, 64, 78]
Slap fingerprints	[98]
Palm dorsal vein	[98]
Hand geometry	[98]
Behavioral biometric	[58]

4. Biofeatures

The biofeatures used by authentication and authorization schemes for mobile IoT devices can be classified into two types: human physiological (e.g., face, eyes, fingerprints-palm, or electrocardiogram) and behavioral features (e.g., signature, voice, gait, or keystroke). Table 3 presents the biometrics-based authentication schemes for mobile IoT devices with biofeatures used as a countermeasure.

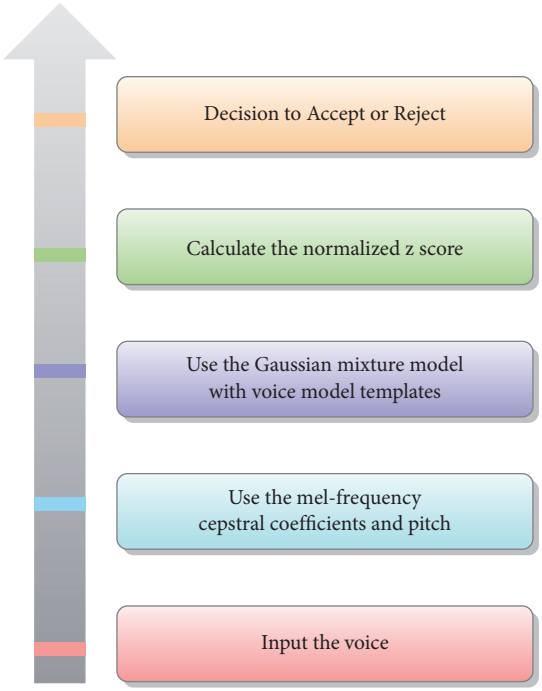

Figure 2: An authentication and authorization scheme using voice for mobile IoT devices.

(i) Gaze gestures: by combining gaze and touch, Khamis et al. [67] introduced multimodal authentication for mobile IoT devices, which is more secure than single-modal authentication against iterative attacks and side attacks.

(ii) Electrocardiogram: electrocardiogram methods can conceal the biometric features during authentication, which are classified as either electrocardiogram with the fiducial features of segmented heartbeats or electrocardiogram with nonfiducial features as discussed in [70, 71]. Both studies proved that the electrical activity of the heart can be a candidate of biofeatures for user authentication on mobile IoT devices.

(iii) Voice recognition: the voice signal can be used in voice authentication with a characteristic of single vowel. Kim and Hong [25] used mel-frequency cepstral coefficients and pitch as voice features and the Gaussian mixture model in the voice authentication process for speaker recognition, as shown in Figure 2. Note that voice-based authentication and authorization schemes for mobile IoT devices are vulnerable against attacks that use a prerecorded voice.

(iv) Signature recognition: according to Shahzad et al. [23], a signature is defined as the conventional handwritten depiction of one's name performed using a finger. Therefore, existing signature-based authentication and authorization schemes for mobile IoT devices can be divided into three categories, namely, offline, online, and behavior. With the category of offline, authentication and authorization schemes use the form on an image as input signatures. With the category of online, authentication and authorization schemes use the form of time-stamped data points as input signatures. With the category of behavior, authentication and authorization schemes use the behavior of doing signatures with a finger.

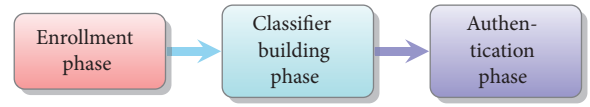

Figure 3: An authentication and authorization scheme using keystroke dynamics for mobile IoT devices. In the enrollment phase, users type their PINs by clicking the numeral buttons. Then, the system verifies the user's identity after obtaining the personal features in the classifier building phase. At the authentication phase, the system verifies the user's identity.

(v) Gait recognition: the gait templates can be used for user verification. Based on the biometric cryptosystem (BCS) approach with a fuzzy commitment scheme, Hoang et al. [74] introduced authentication and authorization scheme using gait recognition for mobile IoT devices.

(vi) Behavior profiling: behavior profiling aims at building invariant features of the human behavior during different activities. Frank et al. [24] proposed authentication and authorization scheme using a touchscreen input as a behavioral biometric for mobile IoT devices.

(vii) Keystroke dynamics: existing keystroke-based authentication and authorization schemes for mobile IoT devices can be classified into two types: (1) static, in which the keystroke analysis is performed only at specific times, and (2) continuous, in which the keystroke analysis is performed during a whole session. In order to improve the effectiveness of PIN-based authentication and authorization schemes, Tasia et al. [38] proposed three steps in the keystroke dynamics-based authentication systems, namely, (1) enrollment step, (2) classifier building step, and (3) user authentication step, as shown in Figure 3.

(viii) Touch dynamics: the process of measuring and assessing human touch rhythm on mobile IoT devices is called touch dynamics. According to Teh et al. [17], the design of a touch dynamics authentication system is performed in three steps, namely, (1) user enrollment step, (2) user authentication step, and (3) data retraining step, as shown in Figure 4.

(ix) Fingerprint: the fingerprint is used as a biokey, dynamically to secure a communication channel between client and server after successful authentication on mobile IoT devices. [79–82]. Currently, authentication and authorization schemes use public key infrastructure framework, such as elliptic curve cryptography, in order to protect the fingerprint biometric, as shown in Figure 5.

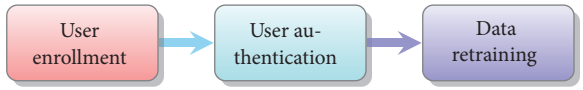

Figure 4: An authentication and authorization scheme using touch dynamics for mobile IoT devices. In the first phase, the touch dynamics data are acquired, processed, and stored. In the second phase, the system determines the similarity or dissimilarity. In the third phase, the reference template is updated (data adaptation).

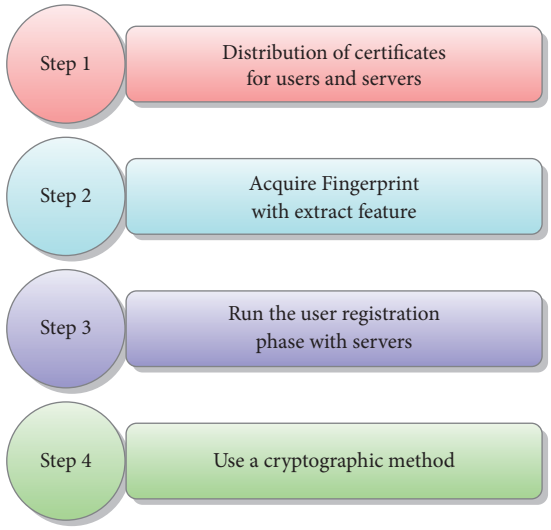

Figure 5: An authentication and authorization scheme using fingerprint for mobile IoT devices.

(x) Smart card: according to Li and Hwang [85], the authentication and authorization schemes for mobile IoT devices using smart cards are one of the simplest and the most effective schemes for IoT authentication compared to traditional password-based authentication schemes. Specifically, the user inputs his/her personal biofeatures on mobile IoT device during the registration step. Then, the registration center stores the personal biofeatures on the user's smart card.

(xi) Multitouch refers to the ability to sense the input simultaneously from more points of contact with a touchscreen [89]. According to Sae-Bae et al. [88], authentication and authorization schemes for mobile IoT devices using multitouch gesture are based on classifying movement characteristics of the center of the fingertips and the palm.

(xii) Graphical password: to withstand dictionary attacks, researchers proposed graphical-based password authentication schemes, which can be classified into two types: (1) authentication and authorization using recognition and (2) authentication and authorization using recall.

(xiii) Face recognition: Mahbub et al. [92] introduced an authentication and authorization scheme using face recognition, which can be applied for mobile IoT devices. Based on the support vector machine (SVM), Mahbub et al.'s scheme is based on three steps, namely, (1) step of segment clustering, (2) step of learning SVM, and (3) step of face detection, as shown in Figure 6.

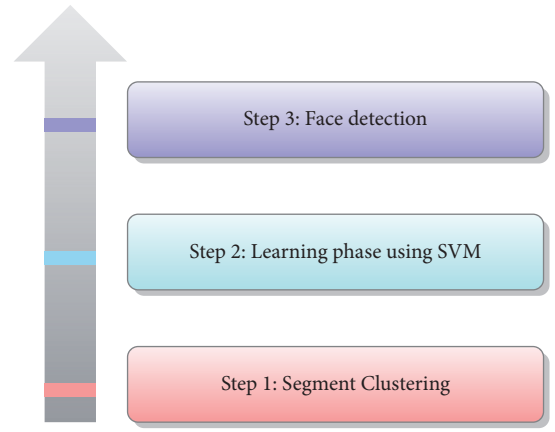

Figure 6: A face-based authentication and authorization scheme using the support vector machine (SVM) for mobile IoT devices. In Step 1, the system applies four substeps: training images, facial segments, clustering, and set of clusters. In Step 2, the system subset of clusters trains an SVM classifier. In Step 3, the system applies five substeps: clustering, a subset of clusters, statistical features, pretrained SVM, and score.

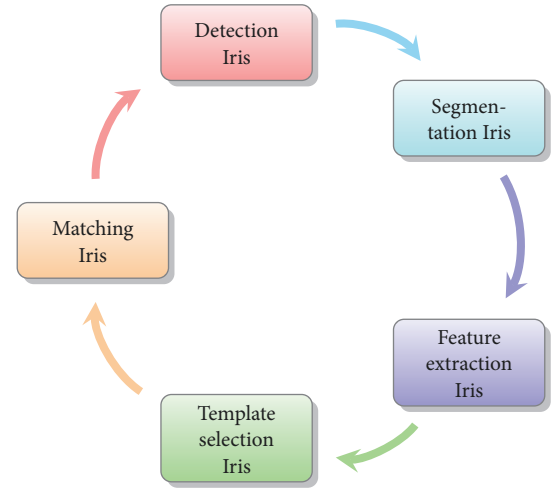

Figure 7: An authentication and authorization scheme using Iris for mobile IoT devices.

(xiv) Iris recognition: iris-based authentication scheme refers to a comparison with the iris template of the person owning the mobile computing device. This process could be used to unlock a mobile computing device or to validate banking transactions. According to De Marsico et al. [91], an iris-based authentication scheme can be repeated in a cyclic process to ensure continuous reidentification, as shown in Figure 7.

(xv) Rhythmic taps/slides: a rhythm-based authentication scheme refers to user identification by a series of

rhythmic taps/slides on a device screen. Chen et al. [72] proposed an authentication and authorization scheme using rhythmic taps/slides, which can be applied for mobile IoT devices. Chen et al.'s scheme is based on two steps, namely, (1) enrollment step and (2) verification step.

(xvi) Capacitive touchscreen: in order to scan body parts on mobile IoT devices, Holz et al. [96] introduced an authentication and authorization scheme using the capacitive touchscreen. Specifically, Holz et al.'s scheme appropriates the capacitive touchscreen as an image sensor.

(xvii) Ear shape: ear shape-based authentication scheme refers to capturing a sequence of ear images, which are used for extraction of discriminant features, in order to authenticate the users on mobile IoT devices [44].

(xviii) Arm gesture: the arm gesture is usually combined with a physical biometric to authenticate users for mobile IoT devices, for example, ear shape [44].

5. Authentication and Authorization Schemes for Mobile IoT Devices Using Biofeatures

The surveyed papers of authentication and authorization schemes for mobile IoT devices using biofeatures are shown in Table 4. In addition, threat models and countermeasures are shown in Table 5.

The manner and rhythm in which an individual types characters when writing a text message are called keystroke analysis, which can be classified as either static or continuous. For authenticating users based on the keystroke analysis, Clarke and Furnell [99] introduced an authentication and authorization scheme, which is based on three interaction scenarios, namely, (1) entry of 11-digit telephone numbers, (2) entry of 4-digit PINs, and (3) entry of text messages. Clarke and Furnell's scheme [99] not only can provide transparent authentication of the user but also is efficient in terms of FRR and FAR under three types of mobile IoT devices, namely, Sony Ericsson T68, HP IPAQ H5550, and Sony Clie PEG NZ90. To demonstrate the ability of neural network classifiers, the same authors in [100] proposed an authentication framework based on mobile handset keypads in order to support keystroke analysis. The three pattern recognition approaches used in this framework are (1) feedforward multilayered perceptron network, (2) radial basis function network, and (3) generalised regression neural network. Therefore, Maiorana et al. [76] proved that it is feasible to employ keystroke dynamics on mobile phones with the statistical classifier for keystroke recognition in order to employ it as a password-hardening mechanism. In addition, the combination of pressure and time features is proven by Tasia et al. in [38] that it is among the effective solutions for authentication and authorization.

The passwords have been widely used by the remote authentication schemes, which can be easily guessed, hacked, and cracked. However, to deal with the drawbacks of only-password-based remote authentication, Khan et al. [79] proposed the concept of chaotic hash-based fingerprint biometrics remote user authentication scheme. Theoretically, the scheme in [79] can prevent six attacks, namely, parallel session attack, reflection attack, forgery attack, impersonation attack, DoS attack, and server spoofing attack, but it is not tested on mobile devices and may be vulnerable to biometric template attacks.

In order to avoid the biometric template attack, Xi et al. [80] proposed an idea based on the transformation of the locally matched fuzzy vault index to the central server for biometric authentication using the public key infrastructure. Compared to [79, 80, 112], Chen et al. [81] proposed an idea that uses only hashing functions on fingerprint biometric remote authentication scheme to solve the asynchronous problem on mobile devices. In 2014, Khan et al. [82] improved Chen et al.'s scheme and Truong et al.'s scheme with quick wrong password detection, but location privacy is not considered.

Biometric keys have some advantages, namely, (1) cannot be lost, (2) very difficult to copy, (3) hard to distribute, and (4) cannot be easily guessed. In 2010, Li and Hwang [85] proposed a biometric-based remote user authentication scheme using smart cards in order to provide nonrepudiation. Without using identity tables and storing password tables in the authentication system, Li and Hwang's scheme [85] can resist masquerading attacks, replay attacks, and parallel session attacks. Authors did not specify the application environment of their scheme, but it can be applied to mobile IoT devices as the network model is not too complicated. Note that Li and Hwang's scheme was cryptanalyzed for several times.

Touch dynamics for user authentication are initialed on desktop machines and finger identification applications. In 2012, Meng et al. [113] focused on authentication and authorization using user behavioral biofeatures such as touch duration and touch direction. Specifically, they proposed an authentication scheme that uses touch dynamics on touchscreen mobile IoT devices. To classify users, Meng et al.'s scheme performs an experiment with 20 users using Android touchscreen phones and applies known machine learning algorithms (e.g., decision tree and naive Bayes). Through simulations, the results show that Meng et al.'s scheme succeeds in reducing the average error rate down to 2.92% (FAR of 2.5% and FRR of 3.34%). The question we ask here is the following: is it possible to use the multitouch as an authentication mechanism? Sae-Bae et al. [88] in 2012 introduced an authentication approach based on multitouch gestures using an application on the iPad with version 3.2 of iOS. Compared with Meng et al.'s scheme [113], Sae-Bae et al.'s approach is efficient with 10% EER on average for single gestures and 5% EER on average for double gestures. Similar to Sae-Bae et al.'s approach [88], Feng et al. [114] proposed an authentication and authorization scheme using multitouch gesture for mobile IoT devices, named FAST, which incurs FAR=4.66% and FRR=0.13% for the continuous postlogin user authentication. In addition, the FAST scheme can provide a good postlogin access security, but the threat model is very limited and privacy-preservation is not considered.

Arteaga-Falconi et al. [70] introduced the concept of authentication and authorization using electrocardiogram for

Table 4: Biometric-based authentication schemes for mobile IoT devices.

Time	Scheme	Method	Goal	Mobile device	Performance (+) and limitation (-)	Complexity
2007	Clarke and Furnell [99]	(i) Keystroke analysis	(i) Introducing the concept of advanced user authentication	(i) Sony Ericsson T68; (ii) HP IPAQ H5550	+ Keystroke latency - Process of continuous and nonintrusive authentication	Low
2007	Clarke and Furnell [100]	(i) Keystroke analysis	(i) Enable continuous and transparent identity verification	(i) Nokia 5110	+ GRNN has the largest spread of performances - The threat model is not defined	High
2008	Khan et al. [79]	(i) Fingerprint	(i) Introducing the chaotic hash-based fingerprint	(i) N/A	+ Can prevent server spoofing attack - The proposed scheme is not tested on mobile devices	Low
2010	Li and Hwang [85]	(i) Smart card	(i) Providing the nonrepudiation	(i) N/A	+ Can prevent parallel session attacks - Storage costs are not considered	$10T_H$
2011	Xi et al. [80]	(i) Fingerprint	(i) Providing the authentication using biocryptographic methods	(i) Mobile device with Java Platform	+ Secure the genuine biometric feature - Server-side attack is not considered	at FAR=0.1%, GAR=78.69%
2012	Chen et al. [81]	(i) Fingerprint	(i) Using only hashing functions	(i) N/A	+ Solve asynchronous problem - Privacy-preserving is not considered	$7T_H$
2013	Frank et al. [24]	(i) Touchscreen	(i) Providing a behavioral biometric for continuous authentication	(i) Google Nexus One	+ Sufficient to authenticate a user - Not applicable for long-term authentication	11 to 12 strokes, EER=2%–3%
2014	Khan et al. [82]	(i) Fingerprint	(i) Improve Chen et al.'s scheme	(i) N/A	+ Quick wrong password detection - Location privacy is not considered	$18T_H$
2015	Hoang et al. [74]	(i) Gait recognition	(i) Employing a fuzzy commitment scheme	(i) Google Nexus One	+ Efficient against brute force attacks - Privacy model is not defined	Low

Table 4: Continued.

Time	Scheme	Method	Goal	Mobile device	Performance (+) and limitation (-)	Complexity
2016	Arteaga-Falconi et al. [70]	(i) Electrocardiogram	(i) Introducing the concept of electrocardiogram-based authentication	(i) AliveCor	+ Concealing the biometric features during authentication - Privacy model is not considered	TAR=81.82% and FAR=1.41%
2017	Abate et al. [44]	(i) Ear shape	(i) Implicitly authenticate the person authentication	(i) Samsung Galaxy S4 smartphone	+ Implicit authentication - Process of continuous and nonintrusive authentication	EER=1%–1.13%
2017	Khamis et al. [69]	(i) Gaze and touch	(i) Protect multimodality and authorization on mobile IoT devices	(i) N/A	+ Secure against the side attack model and the iterative attack model - Vulnerable to video attacks	$SSR = 68\%\ to\ 10.4\%$
2017	Feng et al. [87]	(i) Fingerprints or iris scans	(i) Introducing a biometrics-based authentication with key distribution	(i) Google Nexus One	+ Anonymity and unlinkability - Interest privacy in not considered	$C_1 = 8TE_{mul} + 24T_H$
2017	Ghosh et al. [83]	(i) Fingerprint	(i) Proposing a near-field communication with biometric authentication	(i) N/A	+ Authentication and authorization for P2P payment - Threat model is not defined	High
2017	Mishra et al. [101]	(i) Biometric identifier	(i) Removing the drawback of Li et al.'s scheme [102]	(i) N/A	+ Efficient password change + Offline password guessing - Location privacy is not considered	$C_1 = 8T_H + TE_{enc/dec} + 2TE_{mul}$
2018	Li et al. [84]	(i) Fingerprint	(i) Introducing three-factor authentication using fingerprint identification	(i) N/A	+ Quick detection of wrong password + Traceability of mobile user - Backward privacy is not considered	$C_1 = 9TE_{mul}+2T_e \quad +20T_H$
2018	Yeh et al. [97]	(i) Plantar biometrics	(i) Introducing critical characteristics of new biometrics	(i) Raspberry PI platform	+ High verification accuracy - Threat model is not defined	$RV = 83,88\%\ to\ 99,60\%$
2018	Bazrafkan and Corcoran [41]	(i) Iris	(i) Use deep learning for enhancing Iris authentication	(i) N/A	+ The iris segmentation task on mobile IoT devices - Privacy-preserving is not considered	$SA = 99.3\%$

TAR: true acceptance rate; FAR: false acceptance rate; FPR: false-positive rate; EER: equal error rate; GAR: genuine acceptance rate; T_H: time of executing a one-way hash function; SSR: shoulder surfing attack rate; C_1: computational cost of client and server (total); TE_{mul}: time of executing an elliptic curve point multiplication; $TE_{enc/dec}$: time complexity of symmetric key encryption/decryption; T_e: time of executing a bilinear pairing operation; RV: accuracy ratio of entity verification; SA: segmentation accuracy.

Table 5: Threat models and countermeasures.

Scheme	Biofeature	Threat model	Data attacked	Countermeasure
Khamis et al. [67]	Gaze gestures	(i) Iterative attacks (ii) Side attacks	(i) Observe the user several times from different viewpoints	(i) Multimodal authentication based on combining gaze and touch
Khamis et al. [68]	Gaze gestures	(i) Shoulder surfing (ii) Thermal attacks (iii) Smudge attacks	(i) Uncover a user's password	(i) Multimodal authentication based on combining gaze and touch
Arteaga-Falconi et al. [70]	Electrocardiogram	(i) Adversarial machine learning	(i) Attacking ECG data sensors	(i) ECG authentication algorithm
Kang et al. [71]	Electrocardiogram	(i) Adversarial machine learning	(i) Attacking ECG data sensors	(i) Cross-correlation of the templates extracted
Chen et al. [72]	Voice recognition	(i) Random-guessing attack	(i) Malicious bystanders try to observe the password of the legitimate user	(i) Rhythm-based two-factor authentication
Shahzad et al. [23]	Signature recognition	(i) Shoulder surfing attack (ii) Smudge attack	(i) Malicious bystanders try to observe the password of the legitimate user	(i) Behavior-based user authentication using gestures and signatures
Sitova et al. [32]	Behavior profiling	(i) Population attacks	(i) Guess the user's feature vector	(i) Using the notion of guessing distance
Shahzad et al. [23]	Behavior profiling	(i) Shoulder surfing attack (ii) Smudge attack	(i) Spying on the owner when he performs an action	(i) Authentication scheme based on the gesture and signature behavior
Khamis et al. [69]	Touch dynamics	(i) Side attack model (ii) Iterative attack model	(i) Spying on the owner when he performs an action	(i) Multimodal authentication
Ferdowsi and Saad [39]	N/A	(i) Eavesdropping attacks	(i) Extract the watermarked information	(i) Deep learning algorithm with long short-term memory
Khan et al. [79]	Fingerprint	(i) Replay attacks, forgery attack and impersonation attack, server spoofing attack	(i) Replaying of an old login message	(i) Chaotic hash-based authentication

mobile IoT devices. Specifically, the authors considered five factors, namely, the number of electrodes, quality of mobile ECG sensors, time required to gain access to the phone, FAR, and TAR. Before applying the ECG authentication algorithm, the preprocessing stages for the ECG signal pass by the fiducial point detection. The ECG authentication algorithms are based on two aspects: (1) employing feature-specific percentage of tolerance and (2) employing a hierarchical validation framework. The results reveal that the algorithm [70] has 1.41% FAR and 81.82% TAR with 4*s* of signal acquisition. Note that ECG signals from mobile IoT devices may be affected by noise due to the type of motion and signal acquisition, as discussed by Kang et al. [71]. However, the advantage of using ECG authentication is concealing the biometric features during authentication, but it is a serious problem if privacy-preservation is not considered.

6. Future Directions

Several challenges still remain which open interesting research opportunities for future work, including Doppler radar, vocal resonance, mobile malware threats, and adversarial machine learning.

6.1. Doppler Radar. A team of researchers at Buffalo University, led by Wenyao Xu, developed a system that exploits a Doppler radar capable of "reading" the human heart! It works roughly like any other radar, emitting microwaves and analyzing the return signal in order to detect changes in motion [115]. As scientists say, the process of identifying a person through the method takes about eight seconds, and radar power is just 5 milliwatts, which means that radiation is not dangerous to the body. This method can be a basis for future biometric systems that can be fast and efficient and recognize unique characteristics of the human body.

6.2. Vocal Resonance. In [116], the authors proposed using vocal resonance, that is, the sound of the person's voice, as it travels through the person's body. Vocal resonance can be used as a passive biometric, and it achieves high accuracy in terms of identification and verification problems. It is a method that is suitable for devices worn on the chest or neck or initially but could also be used in the near future for recognizing any device that a user possesses.

6.3. Mobile Malware Threats against Biometric Reference Template. In 2016 [117, 118], an Android malware succeeded in bypassing the two-factor authentication scheme of many banking mobile applications that are installed on the user's mobile device. The malware can intercept two-factor authentication code (i.e., verification code sent through SMS) and forward it to the attacker. In case of biometric-based authentication, this threat can be evolved to access the biometric reference template, which is stored at the mobile device, and send it to the attacker. One research direction to prevent this kind of attacks is to employ policy-enforcement access control mechanisms that are appropriate for resource-constrained mobile devices.

6.4. Adversarial Machine Learning against Biometric-Based Authentication Schemes. Some biometric-based authentication mechanisms, and especially behavioral-based ones, use machine learning techniques for extracting features and building a classifier to verify the user's identity. Adversarial machine learning aims to manipulate the input data to exploit specific vulnerabilities of the learning algorithms. An adversary using adversarial machine learning methods tries to compromise biometric-based authentication schemes and gain illegal access to the system or the mobile device. The future research efforts should focus on dealing with this kind of threats.

6.5. Machine Learning and Blockchain-Based Authentication. The blockchain technology is being used in different application domains beyond the cryptocurrencies, for example, SDN, Internet of Things, and fog computing [119]. To develop a machine learning and blockchain-based solution for authenticating mobile IoT devices, we have to take in mind the specific requirements of the blockchain, for example, (1) when IoT data needed to be checked by the IoT entities without any central authority and (2) the ledger copies required to be synchronized across all of the IoT entities. In addition, the vulnerabilities of the peer-to-peer blockchain networks during the authentication need to be considered, including private key leakage, double spending, transaction privacy leakage, 51% vulnerability, and selfish and reputation-based behaviors. Hence, the machine learning-based authentication schemes using the blockchain technology should be investigated in the future.

6.6. Developing a Novel Authentication Scheme. For developing a novel authentication scheme for mobile IoT devices using biofeatures, we propose the following six-step process:

(1) Definition of IoT network components (cloud computing, fog computing, and IoT devices).

(2) Choose the threat models (e.g., iterative attacks, shoulder surfing attacks, thermal attacks, smudge attacks, and eavesdropping attacks).

(3) Choose the biofeatures (e.g., face, eyes, fingerprints-palm, electrocardiogram, signature, voice, gait, and keystroke).

(4) Choose the machine learning and data mining methods (unsupervised, semisupervised, or supervised).

(5) Proposition of the main steps (e.g., enrollment steps, classifier building step, and user authentication step).

(6) Evaluating the scheme's performance using classification metrics, including TAR, FAR, FPR, and EER.

7. Discussion

There is a big discussion regarding the use of biometric characteristics of the users from new systems or technologies. Biometric technology can be used to protect privacy, since only a minimum amount of information is required to determine whether someone is authorized, for example, to enter a specific area. On the other hand, since biometrics

can reveal sensitive information about a person, controlling the usage of information may be tricky, especially now that the technology has reached the stage of being applied in mobile devices which can be easily lost or stolen [120]. Those who are against the use of such features raise concerns about how these data are going to be used. These concerns could be mitigated by making it clear to people that their data is only stored for a limited time and explaining who will process this data and for what purposes [121]. To that sense, the General Data Protection Regulation (GDPR) for European Member States addresses biometric data storage and processes in terms of data protection and privacy. EU countries are affected, including the UK and all companies that store or process data of EU citizens. On the other hand, in the United States, there is no single comprehensive federal law regulating the collection and processing of biometric data. Only three states, Washington, Texas, and Illinois, have a biometric privacy law despite the fact that US regulators are also increasingly focusing on the protection of biometric data. Moreover, in August 2017, India's supreme court decision about a landmark case that named privacy a "fundamental right" showcased that biometric data protection is top on regulators' agenda.

Except from data use issues, general terms such as *computer fear* and *technophobia* also provide established accounts of individuals' resistance to using new and unfamiliar information technologies, especially for elder people [122]. Moving one step further, companies that produce applications or methods that use biometric characteristics must comply with a code of ethics or a consistent legal framework governing this kind of data collection, which is still absent. For that reason, IEEE P7000 is the first standard IEEE ever going to publish on ethical issues in system design in the next couple of years [123].

8. Conclusion

In this article, we have presented a comprehensive literature review, focusing on authentication and authorization for mobile IoT devices using biofeatures, which were published between 2007 and 2018. We presented the machine learning and data mining algorithms used by authentication and authorization schemes for mobile IoT devices, including unsupervised, semisupervised, and supervised approaches. We reviewed all the biofeatures used by authentication and authorization schemes for mobile IoT devices. We presented the pitfalls and limitations of the existing authentication and authorization schemes for mobile IoT devices. Several challenging research areas (e.g., Doppler radar, vocal resonance, mobile malware threats, adversarial machine learning, machine learning, and blockchain-based authentication) will open doors for possible future research directions for mobile IoT devices.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] L. A. Maglaras, K.-H. Kim, H. Janicke et al., "Cyber security of critical infrastructures," *ICT Express*, vol. 4, no. 1, pp. 42–45, 2018.

[2] J. Sanchez del Rio, D. Moctezuma, C. Conde, I. Martin de Diego, and E. Cabello, "Automated border control e-gates and facial recognition systems," *Computers & Security*, vol. 62, pp. 49–72, 2016.

[3] P. Vinkel and R. Krimmer, "The how and why to internet voting an attempt to explain e-stonia," in *Proceedings of the International Joint Conference on Electronic Voting*, vol. 10141, pp. 178–191, Springer.

[4] D. Springall, T. Finkenauer, Z. Durumeric et al., "Security analysis of the estonian internet voting system," in *Proceedings of the 21st ACM Conference on Computer and Communications Security, CCS 2014*, pp. 703–715, ACM, 2014.

[5] R. Sen and S. Borle, "Estimating the contextual risk of data breach: an empirical approach," *Journal of Management Information Systems*, vol. 32, no. 2, pp. 314–341, 2015.

[6] "United biometrics," http://unitedbiometrics.com/, [accessed: 2018-30-11].

[7] M. A. Ferrag, L. Maglaras, A. Derhab, and A. A. Korba, "Taxonomy of biometric-based authentication schemes for mobile computing devices," in *Proceedings of the 2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, pp. 1–8, IEEE, 2018.

[8] D. Gafurov, "A survey of biometric gait recognition: Approaches, security and challenges," in *Proceedings of the Annual Norwegian computer science conference*, pp. 19–21, 2007.

[9] K. Revett, H. Jahankhani, S. T. de Magalhães, and H. M. Santos, "A survey of user authentication based on mouse dynamics," in *Global E-Security*, vol. 12, pp. 210–219, Springer, 2008.

[10] R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: a survey and classification," *International Journal of Biometrics*, vol. 1, no. 1, pp. 81–113, 2008.

[11] D. Shanmugapriya and G. Padmavathi, *A survey of biometric keystroke dynamics: Approaches, security and challenges*, 2009, https://arxiv.org/abs/0910.0817.

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

[13] S. P. Banerjee and D. Woodard, "Biometric authentication and identification using keystroke dynamics: a survey," *Journal of Pattern Recognition Research*, vol. 7, no. 1, pp. 116–139, 2012.

[14] P. S. Teh, A. B. J. Teoh, and S. Yue, "A survey of keystroke dynamics biometrics," *The Scientific World Journal*, vol. 2013, Article ID 408280, 24 pages, 2013.

[15] S. Bhatt and T. Santhanam, "Keystroke dynamics for biometric authentication-a survey," in *Proceedings of the International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME)*, pp. 17–23, IEEE, 2013.

[16] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1268–1293, 2015.

[17] P. S. Teh, N. Zhang, A. B. J. Teoh, and K. Chen, "A survey on touch dynamics authentication in mobile devices," *Computers & Security*, vol. 59, pp. 210–235, 2016.

[18] A. Mahfouz, T. M. Mahmoud, and A. S. Eldin, "A survey on behavioral biometric authentication on smartphones," *Journal of Information Security and Applications*, vol. 37, pp. 28–37, 2017.

[19] N. A. Mahadi, M. A. Mohamed, A. I. Mohamad, M. Makhtar, M. F. A. Kadir, and M. Mamat, "A survey of machine learning techniques for behavioral-based biometric user authentication," in *Recent Advances in Cryptography and Network Security*, IntechOpen, 2018.

[20] K. Sundararajan and D. L. Woodard, "Deep learning for biometrics: a survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 3, p. 65, 2018.

[21] A. Rattani and R. Derakhshani, "A survey of mobile face biometrics," *Computers and Electrical Engineering*, vol. 72, pp. 39–52, 2018.

[22] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: recent progress and remaining challenges," *IEEE Signal Processing Magazine*, vol. 33, no. 4, pp. 49–61, 2016.

[23] M. Shahzad, A. X. Liu, and A. Samuel, "Behavior based human authentication on touch screen devices using gestures and signatures," *IEEE Transactions on Mobile Computing*, vol. 16, no. 10, pp. 2726–2741, 2017.

[24] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 136–148, 2013.

[25] D.-J. Kim and K.-S. Hong, "Multimodal biometric authentication using teeth image and voice in mobile environment," *IEEE Transactions on Consumer Electronics*, vol. 54, no. 4, pp. 1790–1797, 2008.

[26] C. Lin, C. Chang, and D. Liang, "A new non-intrusive authentication approach for data protection based on mouse dynamics," in *Proceedings of the 2012 International Symposium on Biometrics and Security Technologies (ISBAST)*, pp. 9–14, IEEE, 2012.

[27] C. Shen, Z. Cai, and X. Guan, "Continuous authentication for mouse dynamics: A pattern-growth approach," in *Proceedings of the Dependable Systems and Networks (DSN), 2012 42nd Annual IEEE/IFIP International Conference on*, pp. 1–12, IEEE, 2012.

[28] H. Jagadeesan and M. S. Hsiao, "A novel approach to design of user re-authentication systems," in *Proceedings of the 2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems (BTAS)*, pp. 1–6, IEEE, 2009.

[29] A. Buriro, B. Crispo, and M. Conti, "AnswerAuth: A bimodal behavioral biometric-based user authentication scheme for smartphones," *Journal of Information Security and Applications*, vol. 44, pp. 89–103, 2019.

[30] J. V. Monaco, N. Bakelman, S.-H. Cha, and C. C. Tappert, "Recent advances in the development of a long-text-input keystroke biometric authentication system for arbitrary text input," in *Proceedings of the 2013 4th European Intelligence and Security Informatics Conference, EISIC 2013*, pp. 60–66, 2013.

[31] J. C. Stewart, J. V. Monaco, S. Cha, and C. C. Tappert, "An investigation of keystroke and stylometry traits for authenticating online test takers," in *Proceedings of the 2011 IEEE International Joint Conference on Biometrics (IJCB)*, pp. 1–7, 2011.

[32] Z. Sitova, J. Sedenka, Q. Yang et al., "HMOG: new behavioral biometric features for continuous authentication of smartphone users," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 877–892, 2016.

[33] S. Sarkar, V. M. Patel, and R. Chellappa, "Deep feature-based face detection on mobile devices," in *Proceedings of the 2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, pp. 1–8, IEEE, 2016.

[34] H. Gunasinghe and E. Bertino, "PrivBioMTAuth: privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 1042–1057, 2018.

[35] K. O. Bailey, J. S. Okolica, and G. L. Peterson, "User identification and authentication using multi-modal behavioral biometrics," *Computers & Security*, vol. 43, pp. 77–89, 2014.

[36] L. Fridman, A. Stolerman, S. Acharya et al., "Multi-modal decision fusion for continuous authentication," *Computers and Electrical Engineering*, vol. 41, no. C, pp. 142–156, 2015.

[37] N. Zheng, A. Paloski, and H. Wang, "An efficient user verification system via mouse movements," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, pp. 139–150, ACM, 2011.

[38] C.-J. Tasia, T.-Y. Chang, P.-C. Cheng, and J.-H. Lin, "Two novel biometric features in keystroke dynamics authentication systems for touch screen devices," *Security and Communication Networks*, vol. 7, no. 4, pp. 750–758, 2014.

[39] A. Ferdowsi and W. Saad, "Deep learning-based dynamic watermarking for secure signal authentication in the internet of things," in *Proceedings of the 2018 IEEE International Conference on Communications (ICC 2018)*, pp. 1–6, IEEE, 2018.

[40] R. Das, A. Gadre, S. Zhang, S. Kumar, and J. M. Moura, "A deep learning approach to iot authentication," in *Proceedings of the 2018 IEEE International Conference on Communications (ICC 2018)*, pp. 1–6, IEEE, 2018.

[41] S. Bazrafkan and P. Corcoran, "Enhancing iris authentication on handheld devices using deep learning derived segmentation techniques," in *Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1-2, IEEE, 2018.

[42] B. Bayar and M. C. Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," in *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*, pp. 5–10, ACM, 2016.

[43] M. Alhussein and G. Muhammad, "Voice pathology detection using deep learning on mobile healthcare framework," *IEEE Access*, vol. 6, pp. 41034–41041, 2018.

[44] A. F. Abate, M. Nappi, and S. Ricciardi, "I-Am: implicitly authenticate me person authentication on mobile devices through ear shape and arm gesture," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–13, 2017.

[45] Z. Yan and S. Zhao, "A usable authentication system based on personal voice challenge," in *Proceedings of the 2016 International Conference on Advanced Cloud and Big Data (CBD)*, pp. 194–199, IEEE, 2016.

[46] V. Yano, A. Zimmer, and L. L. Ling, "Extraction and application of dynamic pupillometry features for biometric authentication," *Measurement*, vol. 63, pp. 41–48, 2015.

[47] K. Annapurani, M. A. K. Sadiq, and C. Malathy, "Fusion of shape of the ear and tragus - A unique feature extraction method for ear authentication system," *Expert Systems with Applications*, vol. 42, no. 1, pp. 649–656, 2015.

[48] Y. Liu, J. Ling, Z. Liu, J. Shen, and C. Gao, "Finger vein secure biometric template generation based on deep learning," *Soft Computing*, vol. 22, no. 7, pp. 2257–2265, 2018.

[49] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: closing the gap to human-level performance in face verification," in *Proceedings of the 27th IEEE Conference on Computer Vision and Pattern Recognition (CVPR '14)*, 2014.

[50] Y. Sun, X. Wang, and X. Tang, "Deeply learned face representations are sparse, selective, and robust," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR '15)*, 2015.

[51] A. Rattani, N. Reddy, and R. Derakhshani, "Multi-biometric convolutional neural networks for mobile user authentication," in *Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, pp. 1–6, IEEE, 2018.

[52] A. B. Khalifa, S. Gazzah, and N. E. B. Amara, *Multimodal biometric authentication using choquet integral and genetic algorithm*, arXiv, 1804.00528, 2018, https://arxiv.org/abs/1804.00528.

[53] A. A. Ahmed and I. Traore, "Biometric recognition based on free-text keystroke dynamics," *IEEE Transactions on Cybernetics*, vol. 44, no. 4, pp. 458–472, 2014.

[54] A. A. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 3, pp. 165–179, 2007.

[55] O. Alpar, "Frequency spectrograms for biometric keystroke authentication using neural network based classifier," *Knowledge-Based Systems*, vol. 116, pp. 163–171, 2017.

[56] C. Ntantogian, S. Malliaros, and C. Xenakis, "Gaithashing: a two-factor authentication scheme based on gait features," *Computers & Security*, vol. 52, pp. 17–32, 2015.

[57] H. Gamboa, A. L. N. Fred, and A. K. Jain, "Webbiometrics: User verification via web interaction," in *Proceedings of the 2007 Biometrics Symposium, BSYM*, pp. 1–6, 2007.

[58] Y. Cai, H. Jiang, D. Chen, and M. Huang, "Online learning classifier based behavioral biometrie authentication," in *Proceedings of the 2018 IEEE 15th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, pp. 62–65, IEEE, 2018.

[59] C. Feher, Y. Elovici, R. Moskovitch, L. Rokach, and A. Schclar, "User identity verification via mouse dynamics," *Information Sciences*, vol. 201, pp. 19–36, 2012.

[60] S. M. Furnell, J. P. Morrissey, P. W. Sanders, and C. T. Stockel, *Applications of Keystroke Analysis for Improved Login Security and Continuous User Authentication*, Springer, Boston, MA, USA, 1996.

[61] Y. Sheng, V. V. Phoha, and S. M. Rovnyak, "A parallel decision tree-based method for user authentication based on keystroke patterns," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 35, no. 4, pp. 826–833, 2005.

[62] A. Kumar, M. Hanmandlu, and H. M. Gupta, "Fuzzy binary decision tree for biometric based personal authentication," *Neurocomputing*, vol. 99, pp. 87–97, 2013.

[63] Y. Nakkabi, I. Traore, and A. A. E. Ahmed, "Improving mouse dynamics biometric performance using variance reduction via extractors with separate features," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 40, no. 6, pp. 1345–1353, 2010.

[64] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, and I. Lai, "Combining mouse and keystroke dynamics biometrics for risk-based authentication in web environments," in *Proceedings of the 4th International Conference on Digital Home, ICDH 2012*, pp. 138–145, IEEE, 2012.

[65] S. H. Khan, M. Ali Akbar, F. Shahzad, M. Farooq, and Z. Khan, "Secure biometric template generation for multi-factor authentication," *Pattern Recognition*, vol. 48, no. 2, pp. 458–472, 2015.

[66] W. Louis, M. Komeili, and D. Hatzinakos, "Continuous authentication using One-Dimensional Multi-Resolution Local Binary Patterns (1DMRLBP) in ECG biometrics," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2818–2832, 2016.

[67] M. Khamis, F. Alt, M. Hassib, E. von Zezschwitz, R. Hasholzner, and A. Bulling, "GazeTouchPass," in *Proceedings of the 2016 CHI Conference Extended Abstracts*, pp. 2156–2164, ACM Press, New York, NY, USA, 2016.

[68] M. Khamis, R. Hasholzner, A. Bulling, and F. Alt, "GTmoPass," in *Proceedings of the the 6th ACM International Symposium*, pp. 1–9, ACM Press, New York, NY, USA, 2017.

[69] M. Khamis, M. Hassib, E. Von Zezschwitz, A. Bulling, and F. Alt, "GazeTouchPIN: Protecting sensitive data on mobile devices using secure multimodal authentication," in *Proceedings of the 19th ACM International Conference on Multimodal Interaction, ICMI 2017*, pp. 446–450, ACM Press, New York, NY, USA, 2017.

[70] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "ECG authentication for mobile devices," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 3, pp. 591–600, 2016.

[71] S. J. Kang, S. Y. Lee, H. I. Cho, and H. Park, "ECG authentication system design based on signal analysis in mobile and wearable devices," *IEEE Signal Processing Letters*, vol. 23, no. 6, pp. 805–808, 2016.

[72] Y. Chen, J. Sun, R. Zhang, and Y. Zhang, "Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices," in *Proceedings of the IEEE INFOCOM 2015 - IEEE Conference on Computer Communications*, pp. 2686–2694, IEEE, 2015.

[73] Z. Ali, M. S. Hossain, G. Muhammad, I. Ullah, H. Abachi, and A. Alamri, "Edge-centric multimodal authentication system using encrypted biometric templates," *Future Generation Computer Systems*, vol. 85, pp. 76–87, 2018.

[74] T. Hoang, D. Choi, and T. Nguyen, "Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme," *International Journal of Information Security*, vol. 14, no. 6, pp. 549–560, 2015.

[75] Y. Yang and J. Sun, "Energy-efficient W-layer for behavior-based implicit authentication on mobile devices," in *Proceedings of the IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, Atlanta, GA, USA, 2017.

[76] E. Maiorana, P. Campisi, N. González-Carballo, and A. Neri, "Keystroke dynamics authentication for mobile phones," in *Proceedings of the 2011 ACM Symp. Appl. Comput. - SAC '11*, p. 21, ACM Press, New York, NY, USA, 2011.

[77] S.-S. Hwang, S. Cho, and S. Park, "Keystroke dynamics-based authentication for mobile devices," *Computers & Security*, vol. 28, no. 1-2, pp. 85–93, 2009.

[78] S. Mondal and P. Bours, "A study on continuous authentication using a combination of keystroke and mouse biometrics," *Neurocomputing*, vol. 230, pp. 1–22, 2017.

[79] M. K. Khan, J. Zhang, and X. Wang, "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices," *Chaos, Solitons & Fractals*, vol. 35, no. 3, pp. 519–524, 2008.

[80] K. Xi, T. Ahmad, F. Han, and J. Hu, "A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment," *Security and Communication Networks*, vol. 4, no. 5, pp. 487–499, 2011.

[81] C.-L. Chen, C.-C. Lee, and C.-Y. Hsu, "Mobile device integration of a fingerprint biometric remote authentication scheme," *International Journal of Communication Systems*, vol. 25, no. 5, pp. 585–597, 2012.

[82] M. K. Khan, S. Kumari, and M. K. Gupta, "More efficient key-hash based fingerprint remote authentication scheme using mobile device," *Computing: Archives for Scientific Computing*, vol. 96, no. 9, pp. 793–816, 2014.

[83] S. Ghosh, A. Majumder, J. Goswami, A. Kumar, S. P. Mohanty, and B. K. Bhattacharyya, "Swing-pay: one card meets all user payment and identity needs: a digital card module using nfc and biometric authentication for peer-to-peer payment," *IEEE Consumer Electronics Magazine*, vol. 6, no. 1, pp. 82–93, 2017.

[84] X. Li, J. Niu, S. Kumari, F. Wu, and K.-K. R. Choo, "A robust biometrics based three-factor authentication scheme for Global Mobility Networks in smart city," *Future Generation Computer Systems*, vol. 83, pp. 607–618, 2018.

[85] C.-T. Li and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1–5, 2010.

[86] D.-J. He, M.-D. Ma, Y. Zhang, C. Chen, and J.-J. Bu, "A strong user authentication scheme with smart cards for wireless communications," *Computer Communications*, vol. 34, no. 3, pp. 367–374, 2011.

[87] Q. Feng, D. He, S. Zeadally, and H. Wang, "Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment," *Future Generation Computer Systems*, vol. 84, pp. 239–251, 2018.

[88] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures," in *Proceedings of the 2012 ACM Annu. Conf. Hum. Factors Comput. Syst. - CHI '12*, p. 977, ACM Press, New York, NY, USA, 2012.

[89] J. Sun, R. Zhang, J. Zhang, and Y. Zhang, "TouchIn: Sightless two-factor authentication on multi-touch mobile devices," in *Proceedings of the 2014 IEEE Conference on Communications and Network Security (CNS)*, pp. 436–444, IEEE, 2014.

[90] T.-Y. Chang, C.-J. Tsai, and J.-H. Lin, "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices," *The Journal of Systems and Software*, vol. 85, no. 5, pp. 1157–1165, 2012.

[91] M. De Marsico, C. Galdi, M. Nappi, and D. Riccio, "FIRME: Face and iris recognition for mobile engagement," *Image and Vision Computing*, vol. 32, no. 12, pp. 1161–1172, 2014.

[92] U. Mahbub, V. M. Patel, D. Chandra, B. Barbello, and R. Chellappa, "Partial face detection for continuous authentication," in *Proceedings of the 2016 IEEE International Conference on Image Processing (ICIP)*, pp. 2991–2995, IEEE, 2016.

[93] E. Vazquez-Fernandez and D. Gonzalez-Jimenez, "Face recognition for authentication on mobile devices," *Image and Vision Computing*, vol. 55, pp. 31–33, 2016.

[94] D. Gragnaniello, C. Sansone, and L. Verdoliva, "Iris liveness detection for mobile devices based on local descriptors," *Pattern Recognition Letters*, vol. 57, pp. 81–87, 2015.

[95] C. Galdi, M. Nappi, and J.-L. Dugelay, "Multimodal authentication on smartphones: combining iris and sensor recognition for a double check of user identity," *Pattern Recognition Letters*, vol. 82, pp. 144–153, 2016.

[96] C. Holz, S. Buthpitiya, and M. Knaust, "Bodyprint: Biometric user identification on mobile devices using the capacitive touchscreen to scan body part," in *Proceedings of the Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst. - CHI '15*, pp. 3011–3014, ACM Press, New York, NY, USA, 2015.

[97] K.-H. Yeh, C. Su, W. Chiu, and L. Zhou, "I walk, therefore i am: continuous user authentication with plantar biometrics," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 150–157, 2018.

[98] P. Gupta and P. Gupta, "Multibiometric authentication system using slap fingerprints, palm dorsal vein, and hand geometry," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 12, pp. 9777–9784, 2018.

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

[100] N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis," *International Journal of Information Security*, vol. 6, no. 1, pp. 1–14, 2007.

[101] D. Mishra, S. Kumari, M. Khan, and S. Mukhopadhyay, "An anonymous biometric-based remote user-authenticated key agreement scheme for multimedia systems," *International Journal of Communication Systems*, vol. 30, no. 1, Article ID e2946, 2017.

[102] X. Li, J. Niu, M. K. Khan, J. Liao, and X. Zhao, "Robust three-factor remote user authentication scheme with key agreement for multimedia systems," *Security and Communication Networks*, vol. 9, no. 13, pp. 1916–1927, 2016.

[103] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baaaharun, and K. Sakurai, "Authentication in mobile cloud computing: A survey," *Journal of Network and Computer Applications*, vol. 61, pp. 59–80, 2016.

[104] M. U. Aslam, A. Derhab, K. Saleem et al., "A survey of authentication schemes in telecare medicine information systems," *Journal of Medical Systems*, vol. 41, no. 1, p. 14, 2017.

[105] D. Kunda and M. Chishimba, "A survey of android mobile phone authentication schemes," *Mobile Networks and Applications*, pp. 1–9, 2018.

[106] Y.-P. Liao and C.-M. Hsiao, "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients," *Future Generation Computer Systems*, vol. 29, no. 3, pp. 886–900, 2013.

[107] R. Ranjan, S. Sankaranarayanan, A. Bansal et al., "Deep learning for understanding faces: machines may be just as good, or better, than humans," *IEEE Signal Processing Magazine*, vol. 35, no. 1, pp. 66–83, 2018.

[108] H. J. Patel, M. A. Temple, and R. O. Baldwin, "Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting," *IEEE Transactions on Reliability*, vol. 64, no. 1, pp. 221–233, 2015.

[109] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck, "Continuous authentication on mobile devices by analysis of typing motion behavior," *Sicherheit 2014–Sicherheit, Schutz und Zuverlässigkeit*, 2014.

[110] L. Wolf and N. Levy, "The SVM-minus similarity score for video face recognition," in *Proceedings of the 26th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2013*, pp. 3523–3530, USA, June 2013.

[111] H. Li, G. Hua, Z. Lin, J. Brandt, and J. Yang, "Probabilistic elastic matching for pose variant face verification," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2013.

[112] H.-A. Park, J. W. Hong, J. H. Park, J. Zhan, and D. H. Lee, "Combined authentication-based multilevel access control in mobile application for dailylifeservice," *IEEE Transactions on Mobile Computing*, vol. 9, no. 6, pp. 824–837, 2010.

[113] Y. Meng, D. S. Wong, R. Schlegel, and L. Kwok, "Touch gestures based biometric authentication scheme for touchscreen mobile phones," in *Proceedings of the Int. Conf. Inf. Secur. Cryptol*, vol. 7763, pp. 331–350, Springer, Berlin, Heidelberg, Germany, 2013.

[114] T. Feng, Z. Liu, K. Kwon et al., "Continuous mobile authentication using touchscreen gestures," in *Proceedings of the 2012 IEEE International Conference on Technologies for Homeland Security (HST)*, pp. 451–456, IEEE, 2012.

[115] F. Lin, C. Song, Y. Zhuang, W. Xu, C. Li, and K. Ren, "Cardiac scan: A non-contact and continuous heart-based user authentication system," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, pp. 315–328, ACM, 2017.

[116] R. Liu, C. Cornelius, R. Rawassizadeh, R. Peterson, and D. Kotz, "Vocal resonance: Using internal body voice for wearable authentication," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 1, p. 1, 2018.

[117] "Android malware defeats two-factor authentication," https://www.welivesecurity.com/2016/03/09/android-trojan-targets-online-banking-users/.

[118] "Android banking trojan masquerades as flash player and bypasses 2fa," https://thestack.com/security/2016/01/18/android-malware-defeats-two-factor-authentication/.

[119] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: research issues and challenges," *IEEE Internet of Things Journal*, 2018.

[120] L. Royakkers, J. Timmer, L. Kool, and R. van Est, "Societal and ethical issues of digitization," *Ethics and Information Technology*, vol. 20, no. 2, pp. 127–142, 2018.

[121] A.-M. Oostveen, "Non-use of automated border control systems: Identifying reasons and solutions," in *Proceedings of the 28th International BCS Human Computer Interaction Conference: Sand, Sea and Sky - Holiday HCI, HCI 2014*, pp. 228–233, UK, September 2014.

[122] N. Selwyn, "Apart from technology: Understanding people's non-use of information and communication technologies in everyday life," *Technology in Society*, vol. 25, no. 1, pp. 99–116, 2003.

[123] S. Spiekermann, "IEEE P7000—the first global standard process for addressing ethical concerns in system design," *Multidisciplinary Digital Publishing Institute Proceedings*, vol. 1, no. 3, p. 159, 2017.