Rui, Zhang; Yan, Zheng

A Survey on Biometric Authentication

Published in:
IEEE Access

DOI:
10.1109/ACCESS.2018.2889996

Published: 01/01/2019

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Rui, Z., & Yan, Z. (2019). A Survey on Biometric Authentication. *IEEE Access*, *7*, 5994 - 6009. Article 8590812. https://doi.org/10.1109/ACCESS.2018.2889996

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 26, 2018, accepted December 19, 2018, date of publication December 27, 2018,
date of current version January 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2889996

A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification

ZHANG RUI[1] AND ZHENG YAN[1,2], (Senior Member, IEEE)
[1]State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China
[2]Department of Communications and Networking, Aalto University, 02150 Espoo, Finland

Corresponding author: Zheng Yan (zyan@xidian.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61672410, Grant 61802293, and Grant U1536202, in part by the Academy of Finland under Grant 308087, in part by the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2016ZDJC-06, in part by the National Key Research and Development Program of China under Grant 2016YFB0800704, in part by the Key Lab of Information Network Security, Ministry of Public Security, under Grant C18614, and in part by the China 111 Project under Grant B16037 and Grant B08038.

ABSTRACT In order to overcome the difficulty of password management and improve the usability of authentication systems, biometric authentication has been widely studied and has attracted special attention in both academia and industry. Many biometric authentication systems have been researched and developed, especially for mobile devices. However, the existing biometric authentication systems still have defects. Some biological features have not been deeply investigated. The existing systems could be vulnerable to attacks, such as replay attack and suffer from user privacy intrusion, which seriously hinder their wide acceptance by end users. The literature still lacks a thorough review on the recent advances of biometric authentication for the purpose of secure and privacy-preserving identification. In this paper, we classify and thoroughly review the existing biometric authentication systems by focusing on the security and privacy solutions. We analyze the threats of biometric authentication and propose a number of criteria with regard to secure and privacy-preserving authentication. We further review the existing works of biometric authentication by analyzing their differences and summarizing the advantages and disadvantages of each based on the proposed criteria. In particular, we discuss the problems of aliveness detection and privacy protection in biometric authentication. Based on our survey, we figure out a number of open research issues and further specify a number of significant research directions that are worth special efforts in future research.

INDEX TERMS Aliveness detection, biometric authentication, password management, privacy protection.

I. INTRODUCTION

With the rapid development of the Internet and mobile devices, authentication systems have been widely used in the Internet service access and mobile device access for protecting user devices, contents, and accounts. When users hold more and more accounts, password management is becoming truly difficult in practice since it is normally hard to remember various passwords for different system accesses, especially those with high security levels. In order to solve this problem, biometrics were studied and applied in individual authentication due to their unique characteristics.

Researchers have conducted extensive and in-depth research on biometric authentication in recent years [1]–[4]. Some researchers focused on specific algorithms or frameworks used in biometric-based authentication. Kannavara and Bourbakis [1] summarized a series of biometric recognition methods based on neural networks by using voice, iris, fingerprint, palm-print and face and pointed out potential ways to improve these methods. Shunmugam and Selvakumar [2] believed that unimodal biometric methods are limited. Multimodal biometric methods are much more reliable for building up a safer authentication system. They discussed such multimodal methods as multiple sensors, multiple algorithms, multiple instances, multiple samples and hybrid models.

We note that there already exist a number of surveys on biometric authentication. However, some surveys mainly focus on one particular application environment. Borra *et al.* [5] focused on fingerprint recognition technologies. They discussed different types of fingerprint structures and studied different fingerprint recognition approaches including pattern recognition, wavelet and wave atom.

Challenges and problems in fingerprint recognition were reviewed. Fingerprint image improvement technologies were also discussed. Sreeja and Misbahuddin [6] discussed deoxyribonucleic acid (DNA) based cryptography methods. A couple of surveys [7], [8] focused on keystroke dynamics. Padma and Srinivasan [9] reviewed the existing biometric authentication mechanisms in a cloud computing environment. In this paper, biometric authentication was classified into two categories: physical based biometric authentication and behavioral based authentication. The authors gave an overview on these methods and analyzed their advantages and disadvantages. Meng *et al.* [3] surveyed 11 types of biometric authentication methods on mobile phones. Similarly, Blasco *et al.* [4] focused on sensors in wearable devices and classified the biological signals that can be collected by wearable devices. They discussed the difference between biometric authentication methods and traditional ones and analyzed the computational cost of different signal processing techniques. According to the evaluation and experiments on these biometric authentication methods for wearable devices, they proposed some future research directions.

Obviously, potential risks exist in the biometric system, such as the possibility of replay attacks and privacy disclosure of the biometric itself. These attacks make a particular system expose to danger. User information and interests are threatened as a result. The biometric information used in the authentication system is part of user privacy, which deserves special protection. If such private information is leaked, attackers can use it to behave maliciously, which may threat user information security in other systems and bring huge losses to users. Meng *et al.* [3] pointed out a series of potential attacks in a generic biometric authentication system. Obviously, security and privacy of biometric authentication are critically important. However, this issue has not been fully considered in many existing biometric systems. According to our investigation, many researchers did not take potential attacks into account when designing their systems. The literature still lacks a thorough review on the recent advance of biometric authentication for the purpose of secure and privacy-preserving identification. This motivates us to perform a thorough survey to summarize the current state-of-the-art of security and privacy solutions in biometric authentication. It is also significant to figure out open research issues and propose future research directions on the basis of a general review in this field.

In this survey, we classify and thoroughly review existing biometric authentication systems, mainly focusing on security and privacy issues. We analyze the threats of biometric authentication and propose a number of criteria for secure and privacy-preserving authentication. We thoroughly review the existing works of biometric authentication by analyzing their differences and summarizing the advantages and disadvantages of each based on the proposed criteria. In particular, we discuss the problems of aliveness detection and privacy protection in biometric authentication. Based on our survey, we further figure out a number of open research issues and

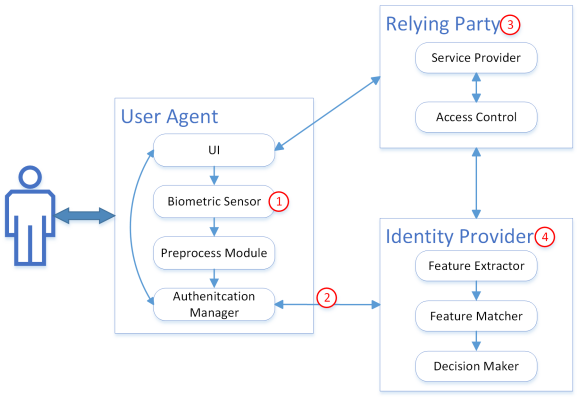


FIGURE 1. An example system structure.

specify a number of significant research directions that are worth special efforts in future research. Specifically, the contributions of this paper can be summarized as below:

- We seriously analyze the security and privacy threats of biometric authentication and propose a number of criteria for achieving secure and privacy-preserving authentication.
- We thoroughly review the existing works of biometric authentication by classifying them into two categories: authentication with static features and authentication with dynamic features. In our review, we pay attention to security and privacy solutions by employing the proposed criteria as a measure to comment the pros and cons of each existing work.
- We point out a number of open issues and suggest future research directions in the field of secure and privacy-preserving biometric authentication.

The rest of the paper is organized as follows. Section 2 gives a brief overview of biometric authentication systems, analyzes its potential security and privacy threats, and proposes a number of criteria towards secure and privacy-preserving authentication. In Section 3, we thoroughly review existing biometric authentication systems in recent decade by employing the proposed criteria as a measure to comment their performance. Section 4 discusses open research issues and proposes future research directions. Finally, a summary of the whole paper is provided in the last section.

II. BIOMETRIC AUTHENTICATION SYSTEMS

A. BIOMETRIC AUTHENTICATION SYSTEM OVERVIEW

Figure 1 illustrates a typical structure of a biometric authentication system [1], [3], [10]. The biometric authentication system generally includes three modules: User Agent (UA) that requests for an eligible identity and gets access to the Internet services or other devices; Identity Provider (IdP) that can verify user identity (i.e., authenticate a user) according to received data from UA and its stored database; Relying Party (RP) that can enforce access control according to the IdP's decision.

When a user raises a request of authentication via a UI, an authentication manager will send an authentication request to IdP through a secure channel. After the IdP receives the authentication request, it will send a challenge to UA. Then the UA can collect biometric signals through a biometric sensor, and preprocess (such as noise reduction and coding) the collected data. After that, the UA responses the authentication challenge. The UA should send the response to IdP through a secure channel in the network. When receiving the challenge response, IdP extracts features of the biometric signals and matches the features with the records in the database. Based on the match result, IdP can decide whether the person participating in the authentication is a legitimate user or not. Yet when receiving the user's access request, RP can determine the access control policy of the current user according to the authentication decision provided by IdP.

It is noteworthy that there are three existing forms of RP and IdP. One is that RP and IdP co-exist in local terminals, and the entire authentication process is completed in the terminal. The other is that RP and IdP co-exist in the cloud as part of the server, and the terminal needs to communicate with the server through the network to complete the authentication process. The third one is as shown in Figure 1, where RP and IdP are separated and owned by different parties. This distinction also brings different weaknesses to the biometric authentication system, which we will discuss in more detail in the following text.

B. POTENTIAL RISKS IN BIOMETRIC AUTENTICATION

Herein, we further identify and characterize several potential attack points (or vulnerable points) with numbers in a biometric authentication system [3], as shown in Figure 1:

- *Faking the sensor (attack point 1).* This type of attacks is able to replace the real biometric feature with a reproduced one, such as a fake finger, a photo, a voice record, etc. Unlike normal network systems, biometric authentication systems are more vulnerable to this kind of attacks. The ability of attacking the network is even unnecessary for attackers. They can achieve the goal by replacing the real biological features with the forged one. This is a serious weakness existing in UA terminals.
- *Resubmitting biometric signals (attack point 2).* This type of attacks is able to bypass the sensor and replay a previously recorded signal to the system. In the process of uploading registration/authentication information, the biometric information may be stolen by the attacker through network eavesdropping. Then, the attacker can re-upload the biometric information in the next authentication to complete a replay attack.
- *Common network attacks on servers (attack points 3 and 4).* When RP and IdP exist in a server, attackers can gain access through a series of common attacks, such as hijacking, lifting power and SQL injection. After that, attackers can obtain more information that only legitimate users can know or access. In the biometric authentication system, if the attacker obtains the biometric information of the legitimate user, they will be able to use this information to behave harmfully.

In practice, focusing on different types of biological characteristics, there are different forms of attacks:

- *Attacks on face recognition:* Face images and videos are very easy to obtain. There is even no need to steal a photo from the users. Attackers can easily get the data they want from the Internet, especially via social networks. Using those images and videos, it could be simple to cheat a face recognition system.
- *Attacks on iris recognition:* With the development of high-resolution camera, stealing an iris image and attack an iris-based recognition system is possible today. However, a high-end optical design always implies a high price. In other words, the cost of this kind of attacks is relatively high.
- *Attacks on fingerprint and palm-print:* Many types of materials can be used to make a fake finger, such as Silica gel, latex, gelatin, etc. Fingerprint can be collected from the surface that the users have touched.
- *Attacks on electrocardiographic (ECG) signals:* Since the ECG signals must be collected by corresponding electrodes or infrared sensors, this kind of attacks is easy to be detected and prevented.
- *Attacks on voice:* Voice is also a kind of biological signal that can be easily collected, since sound travels in all directions in an open environment. If an attacker records user voice and replays it during user authentication, the voice-based authentication system is very likely to be deceived.
- *Attacks on keystroke and touch dynamics:* It is difficult to imitate other people's behaviors. However, this kind of authentication system based on keystroke and touch dynamics is vulnerable to statistic attacks.

For overcoming the above risks, countermeasures were proposed. Common defense strategies for these attacks include: multimodal biometric system, using cryptography techniques, storing sensitive information in a safe place such as a trusted third party. But these methods cannot protect against all attacks. For example, some open biological features, such as voice, can be collected in a relatively large range. The attacker can completely use stolen voice to avoid defense methods.

C. EVALUATION CRITERIA

In this section, we set up a list of criteria for discussing and comparing the performance of the biometric authentication systems.

Researchers have proposed a number of criteria to evaluate the performance of biometric authentication. In [1], researchers focused on the authentication techniques based on neural networks and make a comparative evaluation on those techniques. The evaluation criteria proposed in [1] includes method complexity, invasive, commercialization, training time and computational requirements. Meng *et al.* [3] reviewed 11 types of biometric and made an empirical

TABLE 1. Definitions of quality levels.

Criteria	Levels		
	High	Medium	Low
FAR, FRR, or EER	The experimental results of FAR, FRR or EER is less than 3%	The experimental results of FAR, FRR or EER is between 3% and 10%	The experimental results of FAR, FRR or EER is more than 10%
Efficiency	The time cost is less than 1 second. Or it is mentioned that the algorithm only costs a very little time, which implies that the method's computational cost is low, so that it is suitable to be implemented in a mobile device.	The time cost is between 1 and 3 seconds. Or the method needs a process of training and learning, but his method's computational requirement is medium, thus may be possible but not very suitable to be implemented in a mobile device.	The time cost is more than 3 seconds. Or the method is usually implemented in a capable system, and needs a process of training and learning, which implies that the computational cost of this method is high, thus not suitable to be implemented in a mobile device.
Universality	Everyone has the underlying biometric feature, which is not affected by disability, disease, and accident.	There is a small probability that the biometric feature might be affected by some accidents, e.g., the mute cannot use voiceprint authentication systems.	A large proportion of users do not have this feature.
Uniqueness	All human beings behave differently on the feature (i.e., the feature can uniquely represent every user's identity and be used in authentication).	The underlying feature is different in a large scale (e.g., the probability of two people having the same feature is less than 0.001%).	The feature is only different in a small scale (e.g., the probability of two people having the same feature is less than 0.1%).
Permanence	The biometric feature does not change in a user's whole lifetime.	The feature does not change distinctly in several years.	The feature may change significantly in a short period.
Acceptability	According to the result of searching in the Internet and our own experiences, the underlying biometric feature has been widely used in authentication in industry and business.	A biometric authentication has already been implemented, but it has not been widely used (i.e., the number of searching results is less than a million).	There are few examples of practical applications.
Security	A security solution has been proposed with sound proof.	The biometric feature itself has a security characteristic that it is relatively difficult to attack. Or the proposal has briefly discussed security issue.	There are few studies on the security issue. Or the biometric feature itself is not secure.
MSR	The percentage of $MSR \geqslant 90\%$	$50\% \leqslant The percentage of MSR < 90\%$	$The percentage of MSR < 50\%$

evaluation based on 7 characteristics, including universally, uniqueness, permanence, collectability, performance acceptability and circumvention.

In our opinion, a good biometric authentication system should be not only ''precise and useful'', but also secure. The system should have a certain ability to resist attacks and prevent user privacy disclosure. We believe that the assessment on a biometric authentication system should take its performance into account in terms of accuracy, efficiency, usability, security, and privacy.

1) ACCURACY

In order to evaluate the accuracy of a biometric authentication system, several commonly used metrics are introduced as below:

- *False Acceptance Rate (FAR):* the possibility of identifying an impostor as a legitimate user.
- *False Rejection Rate (FRR):* the possibility of identifying a legitimate user as an impostor.
- *Equal Error Rate (EER):* EER refers to the rate when the proportion of false acceptance is equal to the proportion of false rejection. Generally, the lower the equal error rate, the higher the accuracy of a biometric system is.
- *Authentication Accuracy:* It indicates the possibility of correctly identifying an individual (including both impostors and legitimate users).

For easy comparison of the accuracy of existing work, we mark the quality levels of FAR, FRR and EER by converting percentages into one of three scores. Since the authentication accuracy always corresponds to EER, and the sum of authentication accuracy and EER equals to 100%, herein we take EER into account, while skipping authentication accuracy. Concretely, we only consider FAR, FRR and EER in performance evaluation. Table 1 shows the mapped scores of different percentage rates.

Since FAR and FRR can indicate the ability to resist forgery attacks to a certain extent and security is relatively important in an authentication system, we give the same weight to FAR, FRR, and accuracy. Based on Table 1, we can get the score of a single item and the total score of each existing work. Then, we divide authentication performance into three levels according to the total score. The score corresponding to the three levels are listed in Table 2.

2) EFFICIENCY

It indicates the time required for a system to perform one authentication, mainly including the time spent for data collection, data processing, and feature extraction, as well as authentication decision. When the same method is used in different practical environments, the computational requirements are usually different. In this paper, we only list the testing results of efficiency for reference. In order to evaluate and compare the efficiency of existing work, three quality levels of efficiency are marked as one of three scores and listed in Table 1.

TABLE 2. Range of total score for each level of criteria.

Criteria	Total Score (ts)		
	H	M	L
Accuracy	ts=9	$6 \leqslant ts \leqslant 8$	$1 \leqslant ts \leqslant 5$
Efficiency	ts=3	ts=2	ts=1
Usability	$13 \leqslant ts \leqslant 15$	$8 \leqslant ts \leqslant 12$	$1 \leqslant ts \leqslant 7$
Security	ts=3	ts=2	ts=1
Privacy	$4 \leqslant ts \leqslant 6$	$2 \leqslant ts \leqslant 3$	ts=1

H: High level; M: Medium level; L: Low level.

3) USABILITY

For usability, it is essential to evaluate the authentication systems with the following criteria:

- *Universality (UV):* This means that the underlying method is applicable for all users. Every person should have the underlying biometrics. Therefore, all users can use this method for authentication.
- *Uniqueness (UQ):* It means that the particular biological characteristics of any two people are different. Therefore, the collected features can represent each individual user, making every user's identity differentiated and located.
- *Permanence (PM):* It means that the biometric should not change with time. If the user uses a characteristic that changes over time to register the identity (e.g., the user's weight), then after a period of time when the characteristic changes (e.g., the user loses weight), the user will not be able to prove that he is the exactly registered person.
- *Acceptability (AC):* Users should widely accept the designed biometric authentication system, including accepting the way of biological data collection.
- *Extra Equipment (EE):* This indicates if special extra equipment is needed for collecting biometric signals. Extra equipment might not be embedded in a computer or a mobile phone, such as an ECG sensor.

Similar to the method used above, the quality levels of these five criteria are defined and convert into one of three scores in Table 1. In order to evaluate existing work's overall usability, we calculate the total score of UV, UQ, PM, AC and EE. Then, we divide usability into three levels according to the total score as shown in Table 2.

4) SECURITY

As mentioned in Section 2, the biometric authentication systems are vulnerable to a series of attacks, especially replay/faking attack. Therefore, the system should have a certain ability to resist cyber-attacks (i.e., the biometrics should be difficult to deceive and fool). The quality levels of existing work's security are defined and marked as one of three scores in Table 1.

5) PRIVACY

When the system is subjected to replay attacks, it is often accompanied by the leakage of user biological information, which is also a kind of privacy disclosure. In biometric authentication systems, there are two possible ways of revealing private information. We describe them as below:

Privacy disclosure in a practical environment: People may disclose their biological information at any time in real life, such as the fingerprints left after touching some objects, the signature left when paying with a credit card, the face information and even iris information contained in high definition photos, the voice recorded in public areas, and so on.

Privacy disclosure in a network environment: Biometric information might be stolen, tampered with, or used during storage and transmission.

In order to provide a reference for the research of biometric privacy protection, we propose a number of evaluation criteria on privacy protection as below:

- *Mission Success Rate (MSR):* the possibility of successfully resisting attacks and protecting the privacy of biometric data.
- *Noninvertibility (NI):* In order to protect private data, some algorithms might do some transformation on biometric information. These transformations must be irreversible, so that we can ensure that when a biometric storage database is attacked, attackers cannot recover the user's true private biometric information through the data stored in the database.
- *Revocability (RV):* When biometric information currently used is stolen, the user has to be able to withdraw previously uploaded authentication information and re-register and certify his account using new or altered biological information.
- *Unlinkability (UL):* It is good to make a user's true biological information not connected to the outside world. It is also good if a system only uses changed or indirectly generated information for authentication. Because the real information is not connected to computer networks, the chance of being hacked by corresponding attacks raised from the network will be greatly reduced.

Similar to the method we used for the evaluation of accuracy and usability, we try to evaluate each criterion of privacy and totally divide it into three levels. First, the MSR will be marked in one of three scores as shown in Table 1. Then, regarding NI, RV and UL, if the reviewed method supports a criterion, its score on the corresponding criterion will be mark as 1. Otherwise the score will be marked as 0. Then, we divide privacy into three levels according to the total score as shown in Table 2.

It is worth noting that the specification in Table 1 could be a little bit subjective and only for reference. Since users are subjective on which level of the criteria can be satisfied during the usage of the authentication system. For example, some users can tolerate one or two failures of authentication and a few seconds of response speed, while some users require almost 100 percent success rate and very high response efficiency. At present, there is no clear standard in the literature to stipulate a certain degree of accuracy and authentication speed that an authentication system should achieve a certain level in accuracy, efficiency, etc. In our survey, we specify

TABLE 3. Summary of existing biometric authentication systems with static features.

References	Methods	Accuracy			Efficiency	Usability					Security	Privacy			
		FAR	FRR	EER		UV	UQ	PM	AC	EE		MSR	NI	RV	UL
[11]	Point distribution model	1	1	1	-	3	1	1	3	3	1	-	×	×	-
[12]	Surface Interpenetration Measure	3	2	2	2	3	1	1	3	2	3	-	-	-	-
[13]	Multiobjective evolution	1	1	1	-	3	1	1	3	3	1	-	-	-	-
[14]	iProov	2	2	2	3	3	1	1	3	3	3	-	-	-	✓
[15]	Random projections	3	3	3	-	2	3	3	1	1	2	-	✓	-	-
[17]	Visible sensing	3	3	3	-	2	3	3	1	1	2	-	-	-	-
[16]	-	3	3	3	-	2	3	3	1	1	2	-	-	-	-
[18]	Pupil dynamics	3	3	3	-	2	3	3	1	1	3	-	-	-	-
[19]	Biometric smart card	3	3	3	1	2	3	3	1	1	2	-	-	✓	-
[20]	Eye movement tracking	2	2	2	-	2	3	3	1	1	2	-	-	-	-
[21]	The variation in pupil size	3	3	3	2	2	3	3	1	1	2	-	-	-	-
[34]	Delaunay quadrangle	-	-	-	-	2	3	3	3	3	2	-	-	-	-
[25]	Shift and rotation invariant feature extraction	3	3	3	3	2	3	3	3	3	-	-	-	-	-
[24]	-	3	3	3	3	2	3	3	3	3	-	-	-	-	-
[26]	Thermal images	3	3	3	-	2	3	3	3	1	3	-	-	-	-
[27]	Spectroscopic approach	-	-	-	-	2	3	3	3	1	3	-	-	-	-
[28]	Finger vein biometric	3	2	2	2	2	3	3	3	1	3	-	-	-	-
[29]	Finger odor	2	2	2	-	2	3	3	3	1	3	-	-	-	-
[30]	Hyperspectral imagery	2	2	2	-	2	3	3	3	1	3	-	-	-	-
[32]	Data hiding	3	3	3	-	2	3	3	3	3	1	-	×	✓	×
[33]	Template synthesis	3	3	3	-	2	3	3	3	3	1	1	✓	✓	✓

✓:The scheme in this article supports this criterion;
×:The scheme in this article does not support this criterion.

the quality level of accuracy, efficiency, usability, security and privacy based on the information collected from the following three major sources:

- *Literature:* we collect the experiment and evaluation results from the existing literature.
- *The Internet:* we search with several search engines using the keywords mentioned in the literature, and then statistically analyze the search result.
- *Our own experiences:* based on the collected information above, we then discuss and decide the final results based on our own experience.

According to the information collected from the sources listed above, we integrate the views in the literature with feedback from some users on the network. We attempt to make specific definitions for each level of the criteria. Table 1 shows the mapped scores of each criteria specified above in terms of different performance.

In the existing survey, there is no discussion on how to classify the works into different levels by a numerical method. For easy comparison of different works, we try to provide quantified evaluation. We calculate the total scores of criteria specified above with regard to each aspect of performance evaluation. Then, we divide them into three levels i.e., high, medium and low according to the total score. For accuracy, usability and privacy, the conditions to reach a high-level are the most stringent. In contrast, conditions of reaching medium-level or low-level are correspondingly loose. For efficiency and security, since there is only one criterion belongs to them, their quantified evaluation scores correspond to the level of their criterion. Table 2 shows the range of total score for each level of accuracy, efficiency, usability, security and privacy.

III. LITERATURE REVIEW

In this survey, we review the works published in recent ten years by searching articles from IEEE Xplore Digital Library, ACM Digital Library, Elsevier and Springer. The keywords we used in the search include biometric authentication, face, iris, fingerprint, electrocardiographic, voice, keystroke, recognition, aliveness detection, privacy protection, template protection, and so on. We divide biometric authentication systems into two categories. One is based on static features, that is, physical characteristics, such as face, iris, fingerprint, and so on. Researchers usually collect this kind of biological signals in a spatial frequency domain. The other is based on dynamic features, i.e., behavioral characteristics, such as electrocardiographic (ECG) signal, voice, keystroke, and so on. Researchers usually collect this kind of biological signals in a time-frequency domain. In Table 3 and Table 4, we respectively summarize the reviewed existing works about biometric authentication with static features and dynamic features by summarizing proposed methods/algorithms, their scores on each of the criteria proposed above. We also marked the quality level of accuracy, efficiency, usability, security and privacy in Table 5 based on the criteria specified in Section 1 and Table 1. In order to simplify the table, we use some abbreviations and symbols in the table. In what follows, we review the literature by firstly introducing each paper work, then commenting its pros and cons in terms of accuracy, efficiency, usability, security and privacy.

A. BIOMETRIC AUTHENTICATION WITH STATIC FEATURES

Static features are the physical characteristics of a user. They usually do not change with time. Their sampling results are mostly expressed as images.

TABLE 4. Summary of existing biometric authentication systems with dynamic features.

References	Methods	Accuracy			Efficiency	Usability					Security	Privacy			
		FAR	FRR	EER		UV	UQ	PM	AC	EE		MSR	NI	RV	UL
[35]	-	-	-	-	-	3	1	1	3	2	3	-	-	-	-
[36]	-	2	2	2	-	3	1	1	3	2	3	-	-	-	-
[37]	Fiducial point dependent method, Fiducial points independent method	3	3	3	-	3	1	1	3	2	3	-	-	-	-
[38]	HMM	3	1	1	-	3	3	2	3	3	3	-	-	-	-
[39]	HMM-GMM	2	2	2	-	3	3	2	3	3	1	-	-	-	-
[10]	-	3	1	1	-	3	3	2	3	3	3	-	-	-	-
[40]	PNN analytical method	3	3	3	-	2	1	1	1	1	2	-	-	-	-
[41]	-	2	2	2	-	2	1	1	1	1	2	-	-	-	-
[42]	Nearest neighbor, Neural network, Support vector machine, Random forest	2	2	2	-	2	1	1	1	1	2	-	-	-	-

TABLE 5. Summary of existing biometric authentication systems.

Methods	References	Accuracy	Efficiency	Usability	Security	Privacy
Face recognition	[11]	L	-	M	L	-
	[12]	M	M	M	H	-
	[13]	L	-	M	-	-
	[14]	M	H	M	H	L
Iris recognition	[15]	H	-	M	M	L
	[17]	H	-	M	M	-
	[16]	H	-	M	M	-
	[30]	H	-	M	H	-
	[31]	H	L	M	M	L
	[32]	M	-	M	M	-
	[33]	H	M	M	M	-
Fingerprint/palm-print recognition	[34]	-	-	H	M	-
	[25]	H	H	H	-	-
	[24]	H	H	H	-	-
	[26]	H	-	M	H	-
	[27]	-	-	M	H	-
	[28]	M	M	M	H	-
	[29]	M	-	M	H	-
	[30]	M	-	M	H	-
	[32]	H	-	H	L	L
	[33]	H	-	H	L	M
Electrocardiographic (ECG) signals	[35]	-	-	M	H	-
	[36]	M	-	M	H	-
	[37]	H	-	M	H	-
Voice reccognition	[38]	L	-	H	H	-
	[39]	M	-	H	L	-
	[10]	L	-	H	H	-
Keystroke and touch dynamics	[40]	H	-	L	M	-
	[41]	M	-	L	M	-
	[42]	M	-	M	M	-

1) FACE RECOGNITION

Human beings always distinguish and identify other people by observing and comparing faces in the daily life. This recognition method is very common. However, there is little difference between different individuals, and the structures of all faces are similar, even the structures and shapes of facial organs are similar. Such characteristics are not good enough to distinguish human beings from human faces. In addition, the shape of the face is very unstable. Expression, observation angle, age and illumination are all influencing factors. In conclusion, face recognition has a very high UV with a low UQ and PM.

Face recognition has a lot of in-depth excellent research results. González-Jiménez and Alba-Castro [11] proposed a point distribution model to deal with the pose variation in 2-D face recognition. They used pose eigenvectors and pose parameters to synthesize pose corrected images based on thin plate splines-based warping. In the evaluation, the proposed methods achieved state-of-the-art results, outperforming a 3-D morphable model and other approaches in a set of rotation angles ranging from $-45°$ to $45°$. This face recognition's accuracy is not high, only about 30%. The proposed system is able to recognize users in offset gesture, which provides a great convenience for users and improves AC. However, it also means that attackers do not need to look for a positive photo of the user, and they may just need to find a photo of any pose – which is easy to do in today's social network. Since the author did not consider a corresponding solution, the possibility of the system being subjected to replay attacks has greatly increased. In addition, based on

the proposed point distribution model and pose parameters, it can be seen that even if the user profile changes, user face specific information still exists. It cannot satisfy the criteria of NI and RV, which also increase the possibility of user private information disclosure. Thus, this method has a low accuracy level with medium-level usability, low security and no privacy. Efficiency was not mentioned in this paper.

Soon afterwards, in 2010, Queirolo *et al.* [12] presented an automatic framework based on Simulated Annealing-based approach and Surface Interpenetration Measure to perform 3-D face recognition. An authentication score can be obtained by combining four different face regions. They also proposed a modified algorithm to better handle facial expression. Compared with all works tested using the FRGC v2 database, this work achieves the highest verification accuracy, over 96% at 0.1 percent FAR. The time it takes to complete the recognition process is less than 3.1 seconds but more than 1.5 seconds. At the same time, the 3-D face scanning also avoids the possibility that an attacker could fool the system with a photo. This means that the proposed system has a certain ability of detecting aliveness. However, 3-D scanning may not be available in our mobile terminals. In addition, the high dimensional data obtained by the system contain rich user facial information, which may result in serious privacy disclosure. Therefore, this method achieves medium-level accuracy, medium-level efficiency, medium-level usability, and high security, but privacy is not considered.

Recently, plastic surgery is becoming more and more popular, which deeply affects facial recognition and causes special attention in academia. The non-linear changes the surgery makes are difficult to model using existing systems. Bhatt *et al.* [13] proposed a multi-objective evolutionary particle algorithm to generate non-detached facial data at multiple granularity levels, while using multi-objective genetic algorithms to optimize particle information to match facial images before and after surgery. The results show a higher degree of accuracy than an existing algorithm was achieved based on the test of a plastic surgery facial database. But the accuracy is still less than 90%. So this method only achieves low-level accuracy and medium-level usability. However, efficiency, security and privacy are not mentioned in this paper.

Apple launched FaceID in 2017, which gives stimulus to the market of facial authentication [14]. FaceID uses machine learning to continually improve its recognition accuracy. It usually takes very little time to unlock a phone when a user picks it up. This method is applied to iPhoneX and is highly accepted by users. Apple has taken aliveness detection into account and use a scheme called iProov to solve this problem. Many people worried that a person could be authenticated to a device without their knowledge or consent. In fact, you can only unlock the device when you are looking at the lens, which means the authentication process requires user permission. In addition, Apple takes privacy issue into consideration and supports the requirement of unlinkability. In general, FaceID has medium-level accuracy, high-level efficiency, medium-level usability, high security and low privacy.

2) IRIS RECOGNITION

Non-contact biometric features such as face and iris are of additional benefit than contact-based biometrics such as fingerprint and hand geometry. In contrast, the UV of iris recognition is slightly lower than that of face recognition, as a small number of users may have visual impairment. But the UQ and PM of iris recognition are very high. However, three main challenges still remain in non-contact biometric authentication systems: ability to handle unconstrained acquisition, robust and accurate matching and privacy enhancement without compromising security. For iris recognition, low resolution and image distortion will have a negative impact on recognition results, so a good hardware for iris data collection is necessary. In fact, iris recognition is rarely used in mobile devices. The AC of iris recognition is low. But on the other hand, iris data is difficult to be duplicated without user consent, which reduces the possibility of replay attack (spoofing attack) and has correspondingly higher security than other types of recognition.

Pillai *et al.* [15] proposed a unified framework based on random projections and sparse representations. Its algorithm can deal with common distortion in iris image collection. Thus, this iris recognition method can achieve very high accuracy, over 99%. System operating efficiency is not mentioned in this paper. At the same time, random projections and random permutations are used in the proposed framework, thus their proposed algorithm is irreversible. Attackers cannot obtain user information through simple reverse engineering methods (i.e., this method can support NI). In other words, the proposed method can prevent the disclosure of sensitive user biological information to some extent. So this method has high-level accuracy, medium-level usability, medium security and low privacy.

With the popularity of mobile devices like mobile phones, the application of non-contact biometric authentication on mobile devices has also received researchers' attention. Thavalengal *et al.* [16] analyzed the feasibility of iris recognition applied to non-contact handheld devices. They argued that pixel resolution still limits the application of iris recognition, while existing optical design and smartphone volume cannot allow the embedment of this system. Thavalengal *et al.* [17] focused on critical factors for system implementation such as iris size, image quality and acquisition wavelength. They discussed system requirements for unconstrained acquisition in smartphones. Based on these analyses, they presented several design strategies. Both of the two works have reached high accuracy, over 98%. Besides, both of them have medium-level usability and security. The efficiency and privacy of them are not mentioned.

Some researchers noticed that replay attack should be prevented in the iris recognition system. Pacut and Czajka [18] surveyed possible types of eye forgery. They introduced three solutions of eye aliveness detection based on the analysis

of image frequency spectrum, controlled light reflection from eye cornea, and pupil dynamics. Their solutions were embedded into the Polish Research and Academic Computer Network (NASK) iris recognition system and resulted in a zero FAR and a FRR of 2.8%, while the FAR of two other popular iris cameras without embedding the proposed aliveness detection solutions is 73% and 15%, respectively. The first aliveness detection solution they proposed is frequency spectrum analysis. It does not require additional hardware, the same image used in iris recognition is used for aliveness analysis. But this method has a serious drawback according to Shannon's theory: the method fails once the resolution of the counterfeit iris image is more than twice of the resolution of the analysis camera. The second aliveness detection solution is controlled light reflection analysis. This method needs additional diodes for reflections, and a horizontal and relatively far (20 cm) positioning of the diodes is suggested. The third aliveness detection method they proposed for iris detection is pupil dynamics analysis since the pupil can response to light changes. This method also requires additional hardware, but there is no much requirement on the location of the hardware. Generally speaking, this work has high-level accuracy, medium-level usability and high security. System operating efficiency and privacy protection are not mentioned in the paper.

Czajka *et al.* [19] presented a biometric smart card that can support multi-factor verification. The experimental results show that the method achieves 100% accuracy, and the average time consuming to complete the recognition process is 8.465 seconds. This scheme uses an iris coder based on Zak-Gabor transform and includes an eye aliveness detection. An iris template is securely stored in a smart card, thus unlinkability can be supported with privacy preservation to some extent. System evaluation showed very favorable results. In a word, this method has high-level accuracy, low-level efficiency, medium-level usability, medium security and low privacy.

Rigas and Komogortsev [20] applied the difference between a paper-printed iris and a natural eye iris to propose a method based on the utilization of eye movement to deal with the iris fake attack. Due to the similarities between eye tracking and iris capturing systems, the method they proposed can be used in the existing iris authentication systems with a minimal cost. The evaluation based on a database including 200 subjects showed that the system can achieve an average classification rate (ACR, that is the average percentage of correctly classified test feature vectors) of 96.5% with 3.4% FAR and 3.5% FRR. The advantage of this method is that it can be embedded into an existing iris authentication system without introducing too much burden, so as to provide liveliness detection capability to prevent printing attacks. However, we did not see the protection of iris information in this method, which implies that this system may suffer from privacy leakage. So this method can achieve a medium-level accuracy, medium-level usability, and medium security. The issue of efficiency and privacy is not discussed in this article.

Bodade and Talbar [21] proposed a method to detect the inner boundary of iris based on pupil size variation. Since pupil size changes with different light levels, its variation can be used to detect the aliveness of iris. 384 images of both eyes of 64 subjects were used in experimental tests. The accuracy of iris localization from eye images was 99.48%, which shows a great result in aliveness detection. In the experiment, the iris recognition process costs 1.43s on average. However, we did not see any measures for protecting user iris information in this method, either. Thus, this method has high-level accuracy, medium-level efficiency, medium-level usability, and medium accuracy. The issue of privacy is not explored in this paper.

3) FINGERPRINT RECOGNITION

In recent years, fingerprint-based authentication systems have been widely accepted in both academia and industry. As a kind of biological feature commonly owned by human beings (except for a few persons with hand disabilities), fingerprints have enough inter-user differences and individual stability. Because the operation of fingerprint authentication is very simple, its user acceptance is very high. The fingerprint sensor has been widely developed and applied. It is a kind of authentication method with medium universality, high uniqueness, permanence and acceptance. An extra fingerprint sensor does not introduce much cost to the application of fingerprint recognition. Overall, the usability of fingerprint recognition is very good. Nowadays, the fingerprint recognition system has been embedded into the vast majority of smart phones.

a: FINGERPRINT RECOGNITION WITHOUT SECURITY AND PRIVACY PROTECTION

Delaunay Triangle-Based Structure was well applied in many fingerprint authentication systems and demonstrated excellent results [22], [23]. But there still remain some flaws in this structure. For example, most of these systems have no template protection, the feature sets and similarity measures used in these systems are even not suitable for existing template protection methods. In addition, nonlinear distortion causes local structural changes in these systems. Yang et al. proposed a Delaunay quadrangle-based fingerprint authentication system in [b15]. Delaunay quadrangles can be used to deal with the nonlinear distortion-induced local structural change that the Delaunay triangle-based structure suffers. The experimental results show that the Delaunay quadrangle-based fingerprint authentication system can achieve a better performance. It is more discriminative than the Delaunay triangle-based system. Furthermore, they proposed to construct a unique topology code based on each Delaunay quadrangle, thus the system can enhance the security of template data. But there is no experimental result provided in this paper to allow us know its accuracy and complexity. The issue of privacy is not mentioned in this paper.

In addition to the authentication systems based on fingerprint, there are also some authentication systems based

on other hand features. Kumar and Ravikanth [25] presented a new approach for personal authentication by using finger-back surface imaging. This paper introduced a peg-free imaging technology. The finger-back surface images of each user are normalized to minimize their scale, translation, and rotational variations in knuckle images. Experimental tests achieved promising results, an EER of 1.39%. The authentication process costs about 530 milliseconds Prasad *et al.* [24] improved a palm-print recognition system based on Discrete Wavelet Transformation (DWT). They proposed the technique for shift and rotation invariant feature extraction by employing DWT extension and extracted modal palm lines and energy characteristics from the same wavelet decomposition of palm-print. As a result, recognition ability and recognition accuracy were improved and their test achieved an accuracy of 98.63%. Moreover, the feature extraction process of this method spends only 6 22 milliseconds. The above works make full use of the texture features of human hands and realize the function of identity authentication. However, except authentication, security and privacy were not considered in the above works. Attackers could make a fake fingerprint and spoof the authentication systems. In addition, the information collected and stored in the system faces the risk of leakage. These systems do not provide any basic protection on sensitive private information. Therefore, both of the two methods have high-level accuracy, high-level efficiency, high-level usability, but no assurance on security and privacy.

b: FINGERPRINT RECOGNITION WITH ALIVENESS DETECTION

Fingerprint authentication is the most widely used biometric authentication method in mobile applications. In order to ensure its security and preserve user privacy, some fingerprint authentication systems provide aliveness detection.

Pavešić *et al.* [26] developed a multimodal biometric verification system based on palm surface. The system includes an aliveness detection module based on thermal images of hand dorsa. The experiment with a database of 29 live thermal images and 56 artificial thermal images resulted in a 0% error rate. Clearly, the design of the system takes the user experience into account. A user only needs to reach out their hands, a camera below collects the palm print image, while a thermal camera above will collect thermal image for aliveness detection. This system requests a dedicated hardware device to support, which cannot be satisfied by most of mobile devices. In addition, this system does not consider how to protect palm print images although they are sensitive private information. So this method has high-level accuracy, medium-level usability, high security but no concern on privacy.

Pishva [27] proposed the use of spectroscopic approach to prevent spoofing attacks. The melanin, hemoglobin, arterial, venous blood and so on are unique features of human beings, which are difficult to forge into a fake finger/hand. Those features can represent unique spectral signatures so that they can be used to detect the aliveness of users. The author even considered an extreme example that the proposed system is presented with a severed finger of an authentic person. The features that only exist in an alive person like oxy-hemoglobin can be used to detect whether the signal comes from an alive person. It may be difficult to use this method as an independent identification scheme. But this method can be integrated with a primary biometric feature, not only fingerprint, but also iris and so on to ensure that those biometric signatures used in authentication come from a living person. Similar to the systems described above, this approach does not pay attention to privacy preservation problems. Thus, this method has medium-level usability and high security. However, its accuracy, efficiency and privacy are not discussed.

Jadhav and Nerkar [28] argued that a finger vein biometric authentication system is better than other biometric systems since it has a lower forgery rate. They introduced an image processing algorithm, and implemented Field Programmable Gate Array (FPGA) to deal with template matching. Test results showed that its accuracy can reach 97% with 3% FRR. Since the finger vein is difficult to forge, their experiment did not take forgery finger vein into account and there was no FAR result provided. The authentication process of this method costs about 2 seconds. Thus, this method achieves a medium level of accuracy, efficiency and usability. Its security is high, but privacy is not considered.

Franco and Maltoni [29] focused on reverse-engineering and addressed the topic of fake fingerprint detection. They thought that attackers might use reverse-engineering to forge a fingerprint. Thus, the attackers can fake the authentication system. They argued that an odor-based method is effective to detect a fake fingerprint. The experiment used fake fingerprints with different compounds including bicomponent silicone, natural latex, and gelatin for alimentary use. The EER of this method was 7.48%. So, it is a fingerprint recognition method with medium-level accuracy, medium-level usability and high security. The efficiency and privacy of this method are not discussed in this paper.

Ferrer *et al.* [30] proposed an approach based on Short Wavelength Infrared (SWIR) hyperspectral hand biometrics. In this system, a common camera used in the hand-based authentication system was replaced by a SWIR camera in conjunction with an optical spectrograph. Their experiments showed that local spectral properties of human tissue are effective for discriminate users of a large population and perform better than other hand features. The test based on a database of 154 subjects gave an EER of 3.29%. It is a method with medium-level accuracy, medium-level usability and high security. The efficiency and privacy of this method is not investigated in this paper.

All the works in [26]–[30] provide aliveness detection in fingerprint authentication. Some methods can even be applied to other biometric authentication systems, such as face recognition and iris recognition. But the problem of these systems

is they require extra data, such as spectra, odors, thermal images, etc., which normally requests additional hardware (e.g., sensors) support. In addition, these systems do not consider the problem of sensitive private information protection. That means there is a risk of privacy disclosure in these systems.

c: FINGERPRINT RECOGNITION WITH PRIVACY PROTECTION

Some researchers considered privacy protection in fingerprint authentication. Their proposed methods can protect user fingerprint information from being compromised. The vast majority of users have ten fingerprints. This characteristic is different from other types of biological features. Based on this characteristic, the researchers proposed a number of interesting methods.

Li and Kot [32] proposed a fingerprint authentication system, which uses data hiding and data embedding technology to embed private user data into a fingerprint template. A novel data hiding scheme was proposed in this paper. In the stage of system registration, a user's identity is hidden into his fingerprint template. The template with hidden identity is stored in a database for subsequent authentication. Since fingerprint information is usually sparse binary images, this method does not cause visible changes and is not perceived by the vision of the user or attackers. Therefore, during the process of registration, data embedding does not cause obvious anomalies. During the phase of authentication, query fingerprint is used to match the template stored in an online database. Then, the query identity is compared to the identity hidden in the template for the purpose of authenticating an authorized person. Due to the proposed data hiding scheme, attackers will not be able to obtain the identity and original fingerprint of the stolen templates. However, the security of this scheme was not proved. We suspect its support on both noninvertibility and unlinkability. This system achieved a very high accuracy with high-level usability. The EER showed in testing is 0%. But the efficiency of this fingerprint recognition system is not provided. Although it supports a low level of privacy, it does not satisfy the criterion of security.

Li and Kot proposed another fingerprint authentication system in [33]. General fingerprint authentication systems, only need one fingerprint. But in this system, two fingerprint images are collected. The directional features of one fingerprint are combined with the minutiae of another fingerprint to form a composite fingerprint template. Thus, when the template saved in a server database is stolen, a single true fingerprint cannot be exposed, and the user can replace the fingerprint to generate a new composite template. That is perfectly consistent with the criteria of noninvertibility and revocability. The experimental results show that the system is excellent in terms of accuracy and achieves an EER of 0.4%. System efficiency is not mentioned in this paper. Besides, this system has a high level of usability, a low level of security and a high level of privacy.

B. BIOMETRIC AUTHENTICATION WITH DYNAMIC FEATURES

Dynamic characteristics are mainly about behavioral characteristics of a user. They usually show continuity in the time domain. Feature extraction is a key step of authentication in terms of collected behavioral data processing.

1) ELECTROCARDIOGRAPHIC (ECG) SIGNALS

Biomedical signals such as electrocardiography waveforms can help solve the problem of long-standing aliveness detection and continuous recognition in a biometric system [35]. However, their uniqueness (inter-subject variability) and permanence over time (intra-subject variability) still remain open questions. In other words, this method has high UV, low UQ and low PM.

Carreiras *et al.* [36] did a preliminary study focusing on the uniqueness question. They investigated an ECG based method through a database with 618 subjects and achieved an EER of 9.01%. Its accuracy is medium. The result of experiment showed that the information extracted from ECG signals is sufficient to distinguish a large population. They also demonstrated that the error rate does not increase with an increasing number of subjects. That is, the ECG signal is a viable trait for biometric authentication applications.

Keshishzadeh and Rashidi [37] proposed two different feature extraction methods for ECG signals. They selected reference beats and then generated four artificial features for every extracted feature. Then the artificial features were classified using five different classifiers. In experimental tests, a high accuracy over $99.38 \pm 0.04\%$ was achieved.

With the development of technology, the prices of various sensors are quickly reduced. These ECG-based systems can be embedded into mobile devices such as bracelets, as a module for multimode authentication or as a means of continuous authentication for the purpose of aliveness detection. Therefore, in general, such methods have low usability and high security. However, the issue of privacy protection is normally not considered [35]–[37].

2) VOICE RECOGNITION

As a kind of biological feature commonly owned by human beings (except for a few persons with voice disabilities), voice have enough inter-user differences and individual stability. Moreover, this identification method is simple to operate, and the microphone required for voice data collection is available in almost all mobile devices. In other words, UV, UQ, AC and EE in terms of voice recognition is high. So it is a recognition method with high level of usability.

Jayamaha *et al.* [38] proposed a voice authentication system based on Hidden Markov Model (HMM)l. Previously, HMM has been used in speech recognition for a long time, but this system is different from previous HMM based systems. It uses HMM for voice authentication. The authentication system is text-independent, only relying on the voice of

a speaker. They used HMM to extract some certain features from voice waveform. Experimental test showed that the accuracy of this method is not high, only about 86%. Its efficiency is not investigated. But the result clearly showed that when there were impostors, out of the 150 test cases considered, only 2 instances allowed an impostor to gain access. So this method can resist replay attack (spoofing attack) to a certain extent and thus has high security. The problem of privacy is not discussed in this paper.

Galka *et al.* [39] presented access control based on voice. They introduced an embedded solution of voice biometric access system. This solution uses a Hidden Markov Model - Gaussian Mixture Model (HMM-GMM) method and achieves an EER of 3.4%. The accuracy of this method is close to a high level. However, all the criteria except accuracy are not considered in this paper.

Yan and Zhao [10] proposed a voice authentication framework. This framework consists of three main modules: UA, RP and IdP. It is flexible to support user authentication for different services. System registration and voice-based authentication are based on auto-challenge, and the codes used in challenge change every time. Thus, it is hard to steal the codes and act a forgery attack. The experiment based on 15 participants showed that this system can achieve an average recognition rate of 80.6%. The accuracy of this method is not high, but it has high security. The efficiency and privacy issue are not discussed.

3) KEYSTROKE AND TOUCH DYNAMICS

Saevanee and Bhattarakosol [40] pointed out that finger pressure gives more discriminative information than keystroke dynamics does. There must be a press sensor in the screen to collect the pressure signals. The keystroke dynamic authentication usually uses a two-class classifier. The classifier is trained by both positive samples and negative ones. Then an authentic person can be distinguished. In order to improve the accuracy of authentication system based on keystroke, Antal and Szabó [41] implemented an authentication test-framework that is capable of working with both one-class and two-class classification algorithms. When collecting negative samples is not possible and the two-class classifier cannot work, this framework can use a one-class classification algorithm to distinguish a valid user.

In recent years, because the smart phones are no longer using pressure sensitive screen, researchers began to do some investigation on touch dynamics [42]. Serwadda et al. studied the problem of high error rate in authentication systems based on behavioral characteristics. They pointed out that temporal information associated with the occurrence of errors might help solve this problem.

When smart phones have just been developed, such methods based on keystroke and touch dynamics emerge with the advent of touch screens. However, with the development and application of various fingerprint sensors, this kind of methods have been rapidly replaced by fingerprint authentication. The reason is the level of usability of these methods is very low. Moreover, in the three articles above, the issue of security and privacy protection was not considered.

C. COMPARISON, ANALYSIS AND SUMMARY

In order to evaluate the existing works in terms of accuracy, efficiency, usability, security and privacy, we firstly calculate the score of these articles in these five aspects according to Table 3 and Table 4. Then we rank the level of these works on the five aspects according to Table 2. The evaluation results are shown in Table 5.

We observe from Table 5 that Iris recognition normally achieves high recognition accuracy with low error rate. But this kind of methods requests extra equipment support, which could have a high cost. Fingerprint-based authentication methods generally have good identification accuracy and are widely used nowadays. Other biometric authentication methods seem immature, which requests additional investigation.

With the popularity of mobile communications and mobile devices, most biometric systems can be implemented in mobile devices. However, several limits exist in the mobile phone in terms of hardware limitation, computational capability and electricity power. In the choice of authentication methods, we should pay attention to corresponding resource costs. In addition, due to the openness of mobile communication signals, mobile devices are more likely to be attacked, so the security of the biometric authentication system should be seriously considered.

From Table 5, we can see that the overall performance of the authentication systems based on static features is relatively high, especially the fingerprint authentication systems. It achieves not only a high accuracy, but also high efficiency with a time-cost of millisecond level. Fingerprint identification and authentication systems have been applied almost everywhere in our daily life. It is clear that fingerprint methods not only have been thoroughly studied by researchers, but also have been widely used in practice. In contrast, the overall performance of the authentication systems based on dynamic features is relatively low in terms of either accuracy or acceptance, with the need of additional equipment.

In this survey, we pay more attention to the security and privacy of authentication systems. As we mentioned above, the difference between common network systems and biometric authentication systems is that researchers should pay more attention to the aliveness detection and privacy protection issue in biometric authentication systems. In our evaluation, some systems can achieve a high level of security, such as the authentication systems based on iris, fingerprint, ECG signals and voice. But they all have their own defects. Since iris is a precise image that should be collected in a very short distance in order to achieve an effective resolution, the iris images are hard to be stolen and fake by attackers. Dynamic detection can further enhance its security. However, the usability of iris recognition is not good enough. The fingerprint authentication, by contrast, has sound usability with relatively low security because people often touch the surfaces of many things in their everyday life, which

provides convenience for attackers to steal fingerprint images. Some methods [26]–[31] were proposed to detect aliveness for achieving high security. But without exception, they all impact usability to some extent. The drawback of applying ECG signals is that the usability of designed system is not high. Moreover, the drawback of voice recognition is that its authentication accuracy is low. Besides, there are also some biometric authentication systems with low security, such as the authentication systems based on face. Attackers can easily gain users' face images because the information of these biometric features are widely spread in real life or through a networking environment.

As we summarized in Section 2, faking sensors to perform replay attacks is the most typical type of attacks in biometric authentication systems. The attackers do not even need to have professional programming skills, but only need to steal a copy of the user's biological signal, e.g., the fingerprint remained on a touched surface, facial photos, voice recording, etc. The weakness of biometric authentication system is often caused by user carelessness in the process of authentication. Aliveness detection checks if an entity submitting a challenge response sample is a living organism. Therefore, aliveness detection becomes critically important to effectively prevent fake attacks.

For the authentication systems based on static features, aliveness detection methods can be divided into two categories. One is to increase the difficulty of biological data collection [35]. The shortcoming of this approach is it normally requests additional equipment. Although this method impedes attackers, it also increases user cost and influence usability. The other kind of aliveness detection methods is applying dynamic monitoring [35]. In this method, a user's knowledge/consent becomes an element of authentication. If continuous monitoring is not allowed by the user, or the answer given by the user is not based on what he knows, the user cannot pass the authentication. Its shortcoming is the complexity of user operations and data processing increases. As a result, the usability of the system is still a problem.

In addition, due to the uniqueness of individual biological characteristics (''uniqueness'' means a user only has a limited number of biometric features, e.g., a person only has 10 fingerprints and 2 iris image), the biometric authentication system usually establishes a relatively fixed template for each user. This is the equivalent of setting up a target for attackers and results in high risk of privacy disclosure and authentication system attack. Therefore, there are two possible issues of privacy protection. One is that the network data may be stolen by attackers and obtain user biometric information. Second, users may unintentionally cause privacy disclosure in their daily life (e.g., the photos, audio and video posted in social networking sites may cause the information disclosure of face, iris and voiceprint). Based on our survey, almost all the existing biometric authentication systems are used to control access and protect user interests and data privacy [43]–[59]. Herein, user private data typically include demographic information (e.g., age, gender and occupation), Internet usage information (e.g., browsing history and purchasing records), context information (e.g., location and time) and so on [43]. However, few existing systems actually protect user biometric information. Some articles [14], [15], [19], [32], [33] mentioned this problem and proposed a solution. However, the proposed schemes were designed for the authentication based on specific static biometric features. They may not be suitable for applying into other types of biometric authentication systems.

Security and privacy could bring serious risks to the biometric authentication systems. Since the biometric authentication based on a dynamic feature can obtain high usability while achieving high security, there is no doubt that it has a promising potential since such kind of authentication systems easily gain user acceptance.

IV. OPEN RESEARCH ISSUES AND FUTURE RESEARCH DIRECTIONS

A. OPEN ISSUES

Based on our serious survey, we find a number of open research issues in biometric authentication that should be well explored.

First, the performance of biometric authentication systems (e.g., accuracy and computational requirement) still needs to be improved. As can be seen from the evaluation, except for the widely used fingerprint authentication system, the accuracy of other types of systems (e.g., biometric authentication based on voiceprint and face) has a lot of room for improvement. Only by solving this problem can these systems be used more widely. Biometric authentication system based on behavioral characteristics is generally not accurate. How to improve its accuracy and make it more applicable is a big challenge.

Second, how to balance between security, system performance and usability is still an interesting and open topic. Spoofing and replying are the simplest and most possible means of attack. How to detect the activity of current authenticator and prevent such attacks needs to be solved. Aliveness detection may introduce a certain degree of influence on system performance. Different types of solutions have different impacts. The aliveness detection by increasing the difficulty of data collection and verification increases system overhead. On the other hand, the aliveness detection based on dynamic detection also increase the complexity of user operation. As a result, the usability of the system will be negatively impacted. It is challenging to design a biometric authentication system with high security, sound usability and high efficiency.

Third, there still lack sound solutions on privacy protection in biometric authentication, as shown in Table IV. Only few privacy protection schemes for fingerprint authentication were proposed. As part of the privacy information, the disclosure of user biometric information will cause serious problems and brings big loss to users. Especially in today's networked and intelligent era, many rights will be determined by a series of electronic identities held by users. Biometric authentication has gradually become the mainstream of

identity authentication due to its simple and convenience operation. It is not difficult to imagine that the disclosure of biometric features will make many user permissions be exposed to risks, which will cause huge safety hazard to user interests. Thus, privacy protection in biometric authentication is urgently requested. On the other hand, privacy disclosure in a real-life environment and corresponding protection are still an open issue. Privacy disclosure in network transmission can be solved by enhancing the noninvertibility, revocability and unlinkability of data. In order to solve the problem of privacy disclosure in real life, we need to educate the privacy awareness of users.

B. FUTURE DIRECTION

We suggest a number of future research directions intending to focus on the implementation of a usable and secure authentication system with privacy preservation.

First, research on a secure and privacy-preserving biometric authentication system is urgently needed. A number of open issues need to be solved as soon as possible facing such a complex and risky cyberspace. At present, the widely used biometric authentication system based on static characteristics, such as touchID and faceID needs to provide a means of liveliness detection. Notably, the performance of aliveness detection should be well studied in order to achieve low system cost and high efficiency. We found that almost all biometric systems lack privacy protection on user biological information. How to protect user private biometric information is an important research topic worth studying, especially when user biometric templates are stored in a third party that cannot be fully trusted.

Second, usability enhancement and accuracy insurance are worth particular exploration for achieving high level user acceptance and wide adoption. A series of factors could affect the usability of a biometric authentication system, including UI design, user-device interaction design, data collection method, authentication protocol design, and so on. How to design a usable biometric authentication system is a significant topic, especially when security and privacy should be considered. In addition, in order to make the system operate in an efficient and accurate way for wide user acceptance and adoption, developing a proper biometric data processing algorithm plays a crucial role. Advanced algorithms should be further researched to support efficiency, usability accuracy and security and privacy at the same time.

Third, cost of authentication in a source limited mobile device should be considered. Most mobile devices (such as mobile phones and smart bracelets) have limited resources of electricity, computing capability, storage space, and so on. Therefore, it becomes essential to study biometric authentication methods and algorithms that can be implemented in wearable devices or even low-end devices with low computational requirements.

Fourth, the systems based on dynamic features have a potential for further study due to its advantages regarding aliveness detection. After the comprehensive comparison on the existing works, coupled with our discussion, we believe that in the field of biometric authentication, the systems based on dynamic features have a potential. It does not require user distraction to make input data on the screen, nor does it require users to fix their body positions. From the user point of view, they provide more convenience to users than the authentication system based on iris, face and so on, since when collecting iris or face images, users have to look at the camera and hold their position for a while. In addition, the data collection process of dynamic features can only be conducted with user consent and cooperation, which provides a good way for aliveness detection. But this kind of system has not been widely used in practice due to some defects, which attract our further efforts and may be good future research topics. Concrete topics include the optimization of authentication accuracy and the improvement of privacy and security.

V. CONCLUSION

In this paper, we reviewed the recent advances in the field of biometric authentication. We pointed out potential attacks and security risks in biometric authentication and further proposed a series of evaluation criteria for evaluating the performance of existing works. We gave a comparative evaluation on the recent literature by dividing existing biometric authentication systems into two categories by using either static biometric features or dynamic ones. We found that most of the existing systems suffer from security and privacy issues, although the authentication accuracy of some systems based on dynamic biometric features should be further improved. Based on our survey, we found several open issues and forecast future research directions. We believe that improving the security and privacy of biometric authentication should be emphasized in future research.

REFERENCES

[1] R. Kannavara and N. Bourbakis, "A comparative survey on biometric identity authentication techniques based on neural networks," in *Biometrics: Theory, Methods, and Applications*, N. V. Boulgouris, K. N. Plataniotis, and E. Micheli-Tzanakou, Ed. 2009, ch. 3, pp. 47–79.

[2] S. Shunmugam and R. Selvakumar, "Electronic transaction authentication—A survey on multimodal biometrics," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res.*, Dec. 2014., pp. 1–4.

[3] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, p. 1268–1293, 3rd Quart., 2015.

[4] J. Blasco, T. M. Chen, J. Tapiador, and P. Peris-Lopez, "A survey of wearable biometric recognition systems," *ACM Comput. Surv.*, vol. 49, no. 3, p. 43, Dec. 2016.

[5] S. R. Borra, G. J. Reddy, and E. S. Reddy, "A broad survey on fingerprint recognition systems," in *Proc. Int. Conf. Wireless Commun. Signal Process. Netw. (WiSPNET)*, Mar. 2016, pp. 1428–1434.

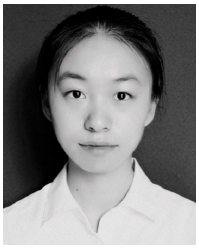
[6] C. S. Sreeja, M. Misbahuddin, and N. P. H. Mohammed, "DNA for information security: A survey on DNA computing and a pseudo DNA method based on central dogma of molecular biology," in *Proc. Int. Conf. Comput. Commun. Technol.*, Dec. 2014, pp. 1–6.

[7] G. Pahuja and T. N. Nagabhushan, "Biometric authentication & identification through behavioral biometrics: A survey," in *Proc. Int. Conf. Cogn. Comput. Inf. Process. (CCIP)*, Mar. 2015, pp. 1–7.

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

[9] P. Padma and S. Srinivasan, "A survey on biometric based authentication in cloud computing," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, vol. 1, Aug. 2016, pp. 1–5.
[10] Z. Yan and S. Zhao, "A usable authentication system based on personal voice challenge," in *Proc. Int. Conf. Adv. Cloud Big Data (CBD)*, Aug. 2016, pp. 194–199.
[11] D. Gonzalez-Jimenez and J. L. Alba-Castro, "Toward pose-invariant 2-D face recognition through point distribution models and facial symmetry," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 413–429, Sep. 2007.
[12] C. C. Queirolo, L. Silva, O. R. P. Bellon, and M. P. Segundo, "3D face recognition using simulated annealing and the surface interpenetration measure," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 2, pp. 206–219, Feb. 2010.
[13] H. S. Bhatt, S. Bharadwaj, R. Singh, and M. Vatsa, "Recognizing surgically altered face images using multiobjective evolutionary algorithm," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 89–100, Jan. 2013.
[14] A. B. Proov, "Facing the future: The impact of Apple FaceID, " *Biometric Technol. Today*, vol. 2018, no. 1, pp. 5–7, Jan. 2018.
[15] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 9, pp. 1877–1893, Sep. 2011.
[16] S. Thavalengal, P. Bigioi, and P. Corcoran, "Iris authentication in handheld devices—Considerations for constraint-free acquisition," *IEEE Trans. Consum. Electron.*, vol. 61, no. 2, pp. 245–253, May 2015.
[17] S. Thavalengal, I. Andorko, A. Drimbarean, P. Bigioi, and P. Corcoran, "Proof-of-concept and evaluation of a dual function visible/NIR camera for iris authentication in smartphones," *IEEE Trans. Consum. Electron.*, vol. 61, no. 2, pp. 137–143, May 2015.
[18] A. Pacut and A. Czajka, "Aliveness detection for IRIS biometrics," in *Proc. 40th Annu. Int. Carnahan Conf. Secur. Technol.*, Oct. 2006, pp. 122–129.
[19] A. Czajka, P. Strzelczyk, M. Chochowski, and A. Pacut, "Iris recognition with match-on-card," in *Proc. 15th Eur. Signal Process. Conf.*, Sep. 2007, pp. 189–192.
[20] I. Rigas and O. V. Komogortsev, "Eye movement-driven defense against iris print-attacks," *Pattern Recognit. Lett.*, vol. 68, pp. 316–326, Dec. 2015.
[21] R. M. Bodade and S. N. Talbar, "Dynamic iris localisation: A novel approach suitable for fake iris detection," in *Proc. Int. Conf. Ultra Mod. Telecommun. Workshops*, Oct. 2009, pp. 1–5.
[22] M. Abellanas, F. Hurtado, and P. A. Ramos, "Structural tolerance and delaunay triangulation," *Inf. Process. Lett.*, vol. 71, nos. 5–6, pp. 221–227, Sep. 1999.
[23] A. Khanban and A. Edalat, "Computing Delaunay triangulation with imprecise input data," in *Proc. 15th Can. Conf. Comput. Geometry*, Aug. 2003, pp. 1–4.
[24] S. M. Prasad, V. K. Govindan, and P. S. Sathidevi, "Palmprint authentication using fusion of wavelet and contourlet features," *Secur. Commun. Netw.*, vol. 4, no. 5, pp. 577–590, May 2011.
[25] A. Kumar and C. Ravikanth, "Personal authentication using finger knuckle surface," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 1, pp. 98–110, Mar. 2009.
[26] N. Pavešić, T. Savič, S. Ribarić, and I. Fratrić, "A multimodal hand-based verification system with an aliveness-detection module," *Ann. Des. Télécommun.*, vol. 62, nos. 1–2, pp. 130–155, Jan. 2007.
[27] D. Pishva, "Spectroscopic approach for aliveness detection in biometrics authentication," in *Proc. 41st Annu. IEEE Int. Carnahan Conf. Secur. Technol.*, Oct. 2007, pp. 133–137.
[28] M. Jadhav and P. M. Nerkar, "Implementation of an embedded hardware of FVRS on FPGA," in *Proc. Int. Conf. Inf. Process. (ICIP)*, Dec. 2015, pp. 48–53.
[29] A. Franco and D. Maltoni, "Fingerprint synthesis and spoof detection," in *Advances in Biometrics*. Berlin, Germany: Springer, 2008, pp. 385–406.
[30] M. A. Ferrer, A. Morales, and A. Díaz, "An approach to SWIR hyperspectral hand biometrics," *Inf. Sci.*, vol. 268, pp. 3–19, Jun. 2014.
[31] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in *Proc. Int. Conf. Biometrics*. Berlin, Germany: Springer, Jan. 2006, pp. 265–272.
[32] S. Li and A. C. Kot, "Privacy protection of fingerprint database," *IEEE Signal Process. Lett.*, vol. 18, no. 2, pp. 115–118, Feb. 2011.
[33] S. Li and A. C. Kot, "Fingerprint combination for privacy protection," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 2, pp. 350–360, Feb. 2013.
[34] W. Yang, J. Hu, and S. Wang, "A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 7, pp. 1179–1192, Jul. 2014.
[35] H. P. da Silva and A. Fred, "Harnessing the power of biosignals," *Computer*, vol. 47, no. 3, pp. 74–77, Mar. 2014.
[36] C. Carreiras, A. Lourenço, A. Fred, and R. Ferreira, "ECG signals for biometric applications—Are we there yet?" in *Proc. 11th Int. Conf. Inform. Control, Automat. Robot. (ICINCO)*, vol. 2, Sep. 2014, pp. 765–772.
[37] S. Keshishzadeh and S. Rashidi, "Single lead electrocardiogram feature extraction for the human verification," in *Proc. 5th Int. Conf. Comput. Knowl. Eng. (ICCKE)*, Oct. 2015, pp. 118–122.
[38] R. G. M. M. Jayamaha, M. R. R. Senadheera, T. N. C. Gamage, K. D. P. B. Weerasekara, G. A. Dissanayaka, and G. N. Kodagoda, "Voizlock—Human voice authentication system using hidden Markov model," in *Proc. 4th Int. Conf. Inf. Automat. Sustainability*, Dec. 2008, pp. 330–335.
[39] J. Galka, M. Masior, and M. Salasa, "Voice authentication embedded solution for secured access control," *IEEE Trans. Consum. Electron.*, vol. 60, no. 4, pp. 653–661, Nov. 2014.
[40] H. Saevanee and P. Bhattarakosol, "Authenticating user using keystroke dynamics and finger pressure," in *Proc. 6th IEEE Consumer Commun. Netw. Conf.*, Jan. 2009, pp. 1–2.
[41] M. Antal and L. Z. Szabó, "An evaluation of one-class and two-class classification algorithms for keystroke dynamics authentication on mobile devices," in *Proc. 20th Int. Conf. Control Syst. Comput. Sci.*, May 2015, pp. 343–350.
[42] 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.
[43] K. Xu and Z. Yan, "Privacy protection in mobile recommender systems: A survey," in *Proc. Int. Conf. Secur. Privacy Anonymity Comput. Commun. Storage*, Nov. 2016, pp. 305–318.
[44] J. Sen, "Security and privacy issues in wireless mesh networks: A survey," in *Wireless Networks and Security*. Berlin, Germany: Springer, 2013, pp. 189–272.
[45] T. Winkler and B. Rinner, "Security and privacy protection in visual sensor networks: A survey," *ACM Comput. Surv.*, vol. 47, no. 1, p. 2, Jul. 2014.
[46] H. Liang, D. Wu, J. Xu, and H. Ma, "Survey on privacy protection of android devices," in *Proc. IEEE 2nd Int. Conf. Cyber Secur. Cloud Comput.*, Nov. 2015, pp. 241–246.
[47] Z.-W. Liang, J. Li, C.-R. Li, and J.-C. Deng, "The survey of location privacy protection," in *Proc. Int. Conf. Wavelet Active Media Technol. Inf. Process. (ICWAMTIP)*, 2012, pp. 227–230.
[48] R. Smith and J. Xu, "A survey of personal privacy protection in public service mashups," in *Proc. IEEE 6th Int. Symp. Service Oriented Syst. (SOSE)*, Dec. 2011, pp. 214–224.
[49] J. Liao, C. Jiang, and C. Guo, "Data privacy protection based on sensitive attributes dynamic update," in *Proc. 4th Int. Conf. Cloud Comput. Intell. Syst. (CCIS)*, Aug. 2016, pp. 377–381.
[50] O. Sarwar, B. Rinner, and A. Cavallaro, "Design space exploration for adaptive privacy protection in airborne images," in *Proc. 13th IEEE Int. Conf. Adv. Video Signal Based Surveill. (AVSS)*, Aug. 2016, pp. 159–165.
[51] J. Yu, B. Zhang, Z. Kuang, D. Lin, and J. Fan, "iPrivacy: Image privacy protection by identifying sensitive objects via deep multi-task learning," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1005–1016, May 2017.
[52] R. Liu and S. Tang, "Negative survey-based privacy protection of cloud data," in *Proc. Int. Conf. Swarm Intell.* Berlin, Germany: Springer, Jun. 2015, pp. 151–159.
[53] K. Fan, Q. Tian, J. Wang, H. Li, and Y. Yang, "Privacy protection based access control scheme in cloud-based services," *China Commun.*, vol. 14, no. 1, pp. 61–71, Jan. 2017.
[54] J. Zhao, J. Liu, Z. Qin, and K. Ren, "Privacy protection scheme based on remote anonymous attestation for trusted smart meters," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3313–3320, Jul. 2018.
[55] L. Zhu, Z. Zhang, Z. Qin, J. Weng, and K. Ren, "Privacy protection using a rechargeable battery for energy consumption in smart grids," *IEEE Netw.*, vol. 31, no. 1, pp. 59–63, Jan./Feb. 2017.
[56] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," vol. 42 no. 4, Jun. 2010, Art. no. 14, doi: 10.1145/1749603.1749605.

[57] S. Donghong, L. Wu, R. Ping, and L. Ke, "Reputation and attribute based dynamic access control framework in cloud computing environment for privacy protection," in *Proc. 12th Int. Conf. Natural Comput. Fuzzy Syst. Knowl. Discovery (ICNC-FSKD)*, Aug. 2016, pp. 1239–1245.
[58] C. Piao, Y. Zuo, and C. Zhang, "Research on hybrid-cloud-based user privacy protection of O2O platform," in *Proc. IEEE 13th Int. Conf. E-Bus. Eng. (ICEBE)*, 2016, pp. 214–219.
[59] T. B. Ionescu and G. Engelbrecht, "The privacy case: Matching privacy-protection goals to human and organizational privacy concerns," in *Proc. Joint Workshop Cyber-Phys. Secur. Resilience Smart Grids (CPSR-SG)*, Apr. 2016, pp. 1–6.



ZHANG RUI received the B.Sc. degree in computer science and technology from the China University of Mining and Technology, Xuzhou, China, in 2016. She is currently pursuing the master's degree in information security with Xidian University, Xi'an, China. Her research interests include information security, authentication, and privacy preserving in social network.

ZHENG YAN (M'06–SM'14) received the D.Sc. degree in technology from the Helsinki University of Technology, Finland. Before joining academia in 2011, she has been a Senior Researcher with the Nokia Research Center, Helsinki, Finland, since 2000. She is currently a Professor with Xidian University, China, and a Visiting Professor and a Finnish Academy Research Fellow with Aalto University, Finland. Her research interests include trust, security, privacy, and security-related data analytics.

She received several awards, including the 2017 Best Journal Paper Award by the IEEE Communication Society Technical Committee on Big Data and the Outstanding Associate Editor of 2017 from the IEEE Access. She served as a General Chair or a Program Chair for a number of international conferences, including the IEEE TrustCom 2015. She is a founding Co-Chair of the Steering Committee of the IEEE Blockchain Conference. She is an Associate Editor of the IEEE Internet of Things Journal, *Information Fusion*, *Information Sciences*, the IEEE Access, and JNCA.