Hindawi
Mobile Information Systems
Volume 2018, Article ID 2649598, 16 pages
https://doi.org/10.1155/2018/2649598

Review Article

Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access

Sandeep Gupta, Attaullah Buriro, and Bruno Crispo

Department of Information Engineering and Computer Science, University of Trento, Trento, Italy

Correspondence should be addressed to Sandeep Gupta; sandeep.gupta@unitn.it

Received 22 August 2017; Revised 11 December 2017; Accepted 9 January 2018; Published 11 March 2018

Academic Editor: Fabio Gasparetti

Smartphones are the most popular and widespread personal devices. Apart from their conventional use, that is, calling and texting, they have also been used to perform multiple security sensitive activities, such as online banking and shopping, social networking, taking pictures, and e-mailing. On a positive side, smartphones have improved the quality of life by providing multiple services that users desire, for example, anytime-anywhere computing. However, on the other side, they also pose security and privacy threats to the users' stored data. User authentication is the first line of defense to prevent unauthorized access to the smartphone. Several authentication schemes have been proposed over the years; however, their presentation might be perplexing to the new researchers to this domain, under the shade of several buzzwords, for example, active, continuous, implicit, static, and transparent, being introduced in academic papers without comprehensive description. Moreover, most of the reported authentication solutions were evaluated mainly in terms of accuracy, overlooking a very important aspect—the usability. This paper surveys various types and ways of authentication, designed and developed primarily to secure the access to smartphones and attempts to clarify correlated buzzwords, with the motivation to assist new researchers in understanding the gist behind those concepts. We also present the assessment of existing user authentication schemes exhibiting their security and usability issues.

1. Introduction

The birth of smartphones can be traced back to 1973, when Motorola launched their first phone—the Dynatac 8000X [1]. In the last 40 years, mobile device manufacturers have invested heavily in the innovation of mobile phones, transforming a device invented merely for calling and short text messaging into the personal, portable and powerful device of nowadays, equipped with many advanced software and hardware features.

Smartphones, undoubtedly, bring rich digital experiences to the users by offering personalized services, for example, chatting, e-mailing, GPS-navigation, net banking, online shopping, social networking, and video conferencing. Most of these services collect and store a large amount of the user's personal data on the device; thus, any unauthorized access to the user's data could have unfavorable consequences. Hence, it becomes extremely important to prevent any unauthorized access to the smartphone. Typically, access to modern smartphones is secured by enabling different authentication solutions, such as PINs/passwords, face recognition, and fingerprint.

By and large multiple terminologies in the field of authentication are being used by researchers not always with clear definitions, which is obviously disconcerting for students and new researchers. Triandopoulos et al. [2] described one-time authentication as "one-time passcodes" or "one-time password" (OTP) as the second authentication factor, although OTP is a more widely accepted term. Crouse et al. [3] described continuous authentication as a periodical composition of one-shot authentication. However, Feng et al. [4] mentioned periodic authentication as equivalent to automatic logouts due to user's inactivity. Patel et al. [5] considered continuous authentication and active authentication systems as the same. Similarly, Dutt et al. [6] suggested the use of transparent modalities in conjunction with explicit authentication methods, such as passwords, PINs, or secret patterns for authenticating users, whereas the study by De Luca et al. [7] considered the use of a transparent modality with or without other schemes and termed it *implicit authentication*. That modality could be used as standalone or to complement the explicit authentication schemes to enhance

their usability [8, 9]. More specifically the concept of *transparent authentication* is explained as implicitly fingerprinting the user's device interaction logs to authenticate the user [10].

Causey [11] considered *risk-based authentication* similar to an *adaptive authentication* scheme. Traore et al. [12] described *risk-based authentication* on the basis of contextual and historical information, extracted from their activities, to build users' risk profiles, for making later the authentication and authorization decisions. Ayed [13] patented the idea for *adaptive authentication* in mobile phones by specifying that *adaptive authentication* uses different authentication methods and different data protection methods depending on the user's location, availability of the network, and the importance of the data. It is pretty much evident from the above discussion that these definitions are correlated, but there is need to relate them to each other by trying to provide consistent definitions for all these terms.

We start this paper by explaining the prevalent ways to authenticate humans along with different types of authentication mechanisms, in the context of smartphones. Then, we try to homogenize different terminologies used in the context of user authentication with the vision that it will benefit the new researchers in understanding existing approaches. Our contribution can help new researchers to get acquainted with different user authentication concepts along with the assessment of their solutions on the basis of modalities, usability, and security.

The rest of work is organized as follows: Section 2 presents the different ways and types of authentication mechanisms. Ways refer to the common factors used to authenticate humans, while types refer to different authentication mechanisms, for example, one-shot, multifactor, continuous, and multimodal, utilizing these factors. Also, we discuss design goals for usable authentication systems and usability evaluation methods. Section 3 surveys the different state-of-the-art solutions proposed over the years for user authentication on smartphones. The related work on the ways and types of user authentication concepts available for smartphones is evaluated on the basis of their usability and security. Finally, Section 4 concludes the paper.

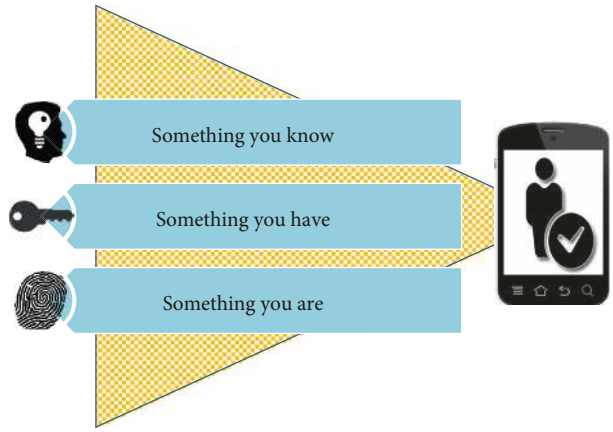

Figure 1: Ways to authenticate humans.

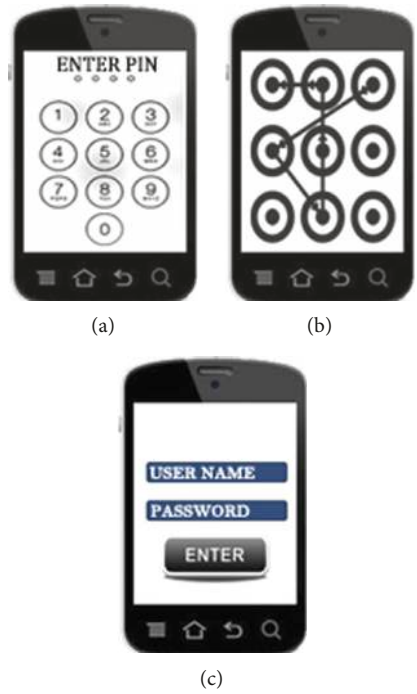

Figure 2: (a) PIN, (b) graphical pattern, and (c) password.

2. Comprehensive Study

In this section, we explain the ways to authenticate the users and the types of authentication mechanisms developed using them, in the context of smartphones.

2.1. Ways to Authenticate Users. The ways in which humans can be authenticated are broadly categorized in three categories [14], that is, "Something you know," "Something you have," and "Something you are," as depicted in Figure 1.

2.1.1. Something You Know. Knowledge-based authentication (KBA) schemes, that is, PINs (Figure 2(a)), graphical passwords (Figure 2(b)), and password (Figure 2(c)), are the most widely used schemes on the smartphones. KBA is based on some sort of a secret knowledge that user sets up earlier during the enrollment and needs to remember as long as he or she continues using the scheme.

2.1.2. Something You Have. This mechanism is also referred as token-based authentication. Many service providers and financial institutions are offering sensitive services, such as net banking, e-wallet, and e-commerce, adopting 2-factor authentication, that is, one-time passcodes (OTPs) along with usual username/password for authentication purpose. Service providers usually supply a small security device to each of their users for generating the one-time passcodes.

OTP schemes can be easily implemented on smartphones (Figure 3(a)) which could be sent either via SMS on the registered number or user could generate this OTP offline (Figure 3(b)) on the mobile apps provided by service

Figure 3: (a) One-time passcode (OTP) via SMS, (b) offline OTP using app, and (c) paired devices.

providers. Additionally, wearable devices (Figure 3(c)) could be used for receiving the OTPs via SMS.

2.1.3. Something You Are. This authentication mechanism relies on the measurement of biometric characteristics of users and is further classified as physiological and behavioral biometrics. Figure 4 illustrates the commonly available authentication ways for smartphone users under this category.

On smartphones, physical traits, that is, ear and face, can be collected using the built-in hardware, that is, camera; however, fingerprint and iris recognition require additional dedicated hardware. Similarly, behavioral biometric modalities, such as gait, grip, swipe, pickup, touch, and voice, can be profiled unobtrusively, using various built-in sensors [15], namely, accelerometer, gyroscope, magnetometer, proximity sensor, touch screens, and microphone. Touch-based solutions authenticate users based on their unique interactions with the device, while they perform a specific task. Additionally, behavioral biometric-based authentication is cost-effective; they generally do not require any special hardware and are considered lightweight in implementation [8].

2.2. Types of Authentication Mechanisms. Researchers have been investigating the utilization of different ways, that is, PIN, passwords, OTP, face, touch, and so on, to design and develop the different types of authentication solutions. These types are briefly explained below:

2.2.1. One-Shot Authentication. One-shot authentication is a type of authentication mechanism in which users' credentials are verified at the beginning of the session [16–18]. This is simply a process where a user claims his or her identity by providing the correct credentials or fulfilling the challenges in order to gain the access to a device. For example, PINs, passwords, graphical patterns, fingerprints, face, and iris are some of the commonly used modalities on the smartphones, for authenticating users. If the verification is successful (e.g., right password is entered), the access is granted; otherwise, the access is denied. Session remains valid until the user signs off or closes the session.

2.2.2. Periodic Authentication. Periodic authentication is simply the variant of "one-shot authentication" in which idle timeout duration is set, for closing the session, automatically [4, 19]. If a user remains inactive for more than the idle timeout duration, the device locks itself.

2.2.3. Single Sign-On (SSO) Authentication. Single sign-on (SSO) is a long-term or persistent authentication type in which a user remains signed on till the time he or she revokes or terminates the session. In case, if the system observes any discrepancy with respect to fix set of attributes, for example, change in location, network connection, and anomaly in usage pattern, the session is terminated or the user is asked for reauthentication [20–22]. VMware identity manager provides APIs to implement mobile sign-on authentication for airwatch-managed Android devices [23]. Similarly, Google offers G Suite apps for single sign-on for Android devices which can be done by pairing smartphones with smartwatches [24].

2.2.4. Multifactor Authentication. Multifactor authentication utilizes the concept of combining 2 or more authentication ways, that is, e-mail verification, OTP via SMS, phone call to the predefined numbers, push notification to the paired device, smart tokens, and so on, along with the usual method of authentication [25–27]. A very common practice is registering ones mobile number with service providers, and whenever the corresponding user accesses that service for sensitive operation, for example, online banking, service provider sends the one-time passcodes (OTPs) via SMS, getting assured that a legitimate user has requested access to that service.

2.2.5. Static and Dynamic Authentication. The static authentication mechanism presents the fixed set of challenges to the users, whereas dynamic authentication mechanism capitalizes the concept in which diverse set of prestored challenges are presented every time users unlock their smartphones [28, 29].

2.2.6. Continuous Authentication. As the name implies, continuous authentication mechanisms are developed to authenticate a legitimate owner throughout their entire session. If any anomaly is detected by the device, the access to the device is stopped, immediately, and the device asks for explicit reauthentication [4, 29, 30]. In other words, the users are passively and periodically monitored throughout their interactive session with any device or system [5]. This concept

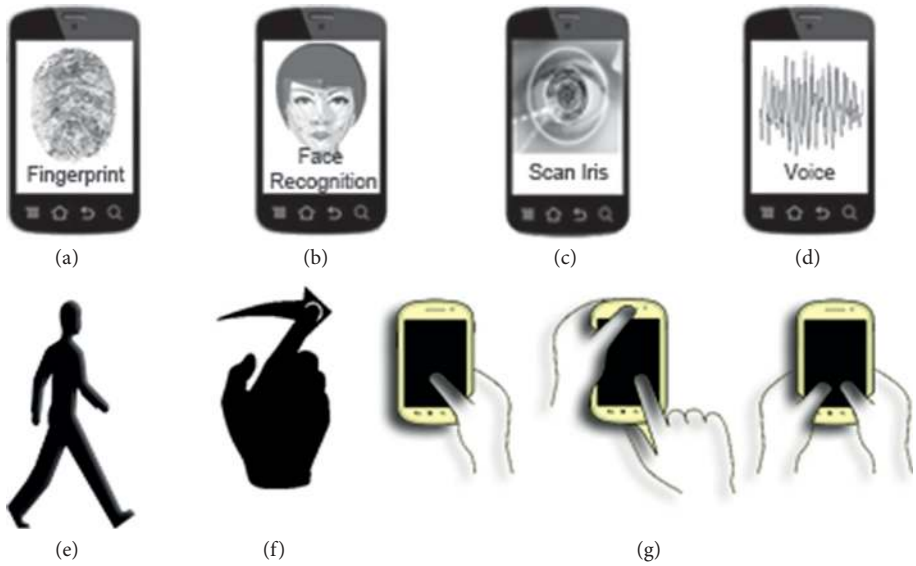

Figure 4: (a) Fingerprint, (b) face, (c) iris, (d) voice, (e) gait, (f) swipe, and (g) touch.

seems to promise higher security as compared to the other authentication mechanisms, such as *one-shot* authentication, *one-time* authentication, and *periodic* authentication, but at the same time much more complex to implement. Additionally, it is desirable that a *continuous* authentication system should not interrupt the user's normal activity and be lightweight, that is, on battery consumption.

2.2.7. Transparent Authentication. This concept stresses more on the procedure of collecting and analyzing user authentication identifiers [4, 10]. More specifically, if the system performs authentication steps in background (without requiring explicitly user cooperation) [10, 31], they are termed as *implicit, transparent, or unobtrusive* authentication systems. However, various authentication types (one-shot, risk-based, or continuous) could collect input transparently.

2.2.8. Risk-Based Authentication. Risk-based authentication schemes are mostly based on nonstatic authentication decision engine, where the decision to accept or reject authentication is based on a risk score computed in real-time, which is compared with the stored risk profiles of the users, and then the system challenges the users for authentication [32], accordingly. For instance, if a user is checking a bank account balance from a verified secure location (home or workplace), verification of identity should not be required. While in case of nonverified location, for example, the service requires additional evidence about the identity of the user thus asking for the authentication credentials. Nowadays, risk-based authentication schemes tend to offer frictionless authentication providing user experience, that could be tailored as per threats observed by the service providers [11, 12, 33, 34].

2.2.9. Adaptive Authentication. Adaptive user authentication boasts the concept having ability to change and to prepare for different conditions and situations, while securing any unauthorized access [13, 35, 36]. It entails for multifactor user authentication mechanisms which should be readily configurable and deployable.

2.2.10. Unimodal and Multimodal Authentication. This term is typically used for biometric authentication schemes. The literal meaning of modality (https://dictionary.cambridge.org/dictionary/english/modality) is a particular way of doing or experiencing something. This concept is based on the number of modalities or traits being used in the authentication systems [37–39]. Unimodal authentication systems leverage only a single biometric modality or trait, whereas multimodal systems are developed by combining two or more modalities. Multimodal authentication systems demonstrate several advantages, such as higher recognition rate, accuracy, and universality [39].

2.3. Usable Authentication System Design Goals. Usability along with security plays a pivotal role in evaluating user authentication schemes. This leads to an important question—how to trade-off between security and usability [40]? We present the guidelines described by Yee for usable security designs [41]. Yee's work focused on addressing valid and nontrivial concerns specific to usable security. We explain below the design goals from usability perspective as suggested in [41]:

(i) *Appropriate boundaries*: this goal is based on *the principle of boundaries* [42]. In order to distinguish among objects and actions along the boundaries, which are relevant to users, system should expose the boundaries and must acknowledge the users. For example, in the context of mobile devices, popular Operating Systems (OS), such as Android (Ver. 6 onwards) and iOS, allow users to grant permissions to the applications and services accessing resources while installing them. Here,

the object could be assumed as the apps or services for the devices and actions could be defined as the indicators that the apps or services demand from users to serve them and to use the system's resources. However, boundaries are the thin line that defines the users' decisions affecting the security of system due to human factors.

(ii) *Path of least resistance*: choosing the most natural method in granting the authority is the most secure way.

(iii) *Explicit authorization*: any authorization to other actors must only be granted in accordance with user actions which should be well understood by a user while acknowledging the consent.

(iv) *Visibility*: a user should be aware of others' active authority affecting any security-relevant decisions.

(v) *Revocability*: a user should be able to revoke others' authority to access the system.

(vi) *Self-awareness*: maintain accurate awareness of the user's own authority to control the system.

(vii) *Trusted path*: protect the user's channels to any entity that manipulate authority on the user's behalf.

(viii) *Identifiability*: any specific objects and specific actions must be clearly identifiable and apparent to the user.

(ix) *Expressiveness*: enable the user to express safe security policies in terms that fit the user's goals.

(x) *Clarity*: notify the consequences of any security-relevant decisions precisely that the user is most likely to perform.

2.4. Usability Evaluation. System usability scale (SUS) questionnaire [43] is utilized to gather subjective assessments about the usability of the proposed systems [8]. The questionnaire consists of 10 questions or statements. The response to each question/statement is measured on a 5-point scale ranging from "strongly disagree" to "strongly agree." The final SUS score ranges between 0 and 100, where a higher value indicates a more usable system. The system usability scale (SUS) template for questionnaire and scoring is available online [44].

3. Literature Review and Analysis

In this section, we review the recent literature emphasizing on the types of authentication mechanisms and the ways on which they are developed and analyze them from security and usability point of view. More specifically, we present the assessment of commonly used user authentication mechanisms on smartphones, focusing on the security and usability issues.

3.1. Ways of Authentication. The usability of authentication mechanisms is one of the dominant attributes that influence users' acceptance of a particular authentication scheme [45]. The ISO standard:13407 defines usability as "*the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction, in a specified context of use*" [46]. Further, the study [47] suggests that the usability can be done on the basis of three criteria: task performance, user satisfaction, and user cost.

Conventional authentication schemes, that is, PIN, passwords, and graphical patterns, are no more considered secure and convenient [48] because they are not able to distinguish between the users, rather they authorize everyone (regardless of whether that person is the legitimate owner of the device or not) who enter the correct credentials. Physiological biometric-based solutions are considered more secure because it is assumed that human body traits cannot be shared, copied, lost or stolen. Moreover, they genuinely authenticate their users by forcing them to present themselves physically to the system. However, they are less preferable on smartphones due to their inherent usability issues [49]. As such, security experts are focusing on developing the usable authentication systems because they believe that behavioral biometrics will restructure the authentication landscape in the next 5–8 years [50].

In each subsections, we have included tables presenting the synopsis of each authentication ways being used as different authentication types along with the references that either indicating usability pros and cons or reporting security solutions and concerns.

3.1.1. Something You Know. As per the web report [51], average smartphone users get themselves engaged in 76 separate phone sessions, while heavy users (the top 10%) peaked to 132 sessions per day. PIN/passwords, and graphical patterns, require users to memorize their text, they had set earlier, to unlock their devices, every time they need to initiate the session (76 times a day). The capacity of the human brain to process the information varies from person to person [52]. Zhang et al. [53] found that users faced problems in remembering their passwords and more especially, to memorize and correctly recall numerous passwords. This encouraged users going for an easy or simple password which is quick to remember [54], but this opens plenty of opportunities for attackers to guess or crack their passwords, easily [55]. When the system enforces stringent password policies, users due to memorability issues [56], allow their browsers or password managers to save their username/password information to make future logins easier. However, users trusting their browsers or password managers are more likely to be a victim of a wide variety of attacks [57, 58]. Overall, 82% of end users are frustrated with managing passwords [59]. Clearly, this indicates the lack of usability, and a result, nearly, 75 million smartphones users in the US do not use any of PIN, pattern, or passwords because they consider them annoying and an obstacle in quick access to their smartphones [60].

From security perspective, PINs and passwords are vulnerable to various attacks, for example, guessing [61], because users choose date of births [57], easier digits (1111, 2222, etc.,) [62] to set up their PIN. Alternatively, Android

Table 1: Synopsis of knowledge-based schemes.

Modalities	Authentication types	Usability pros and cons indicated	Security solutions or concerns reported
PIN [57, 60, 62]; password [53, 60]; pattern [60, 64]	One-shot; static; periodic; single sign-on; unimodal	[48, 52–57, 60, 62, 71, 72]	[58, 61–70]

Table 2: Synopsis of token-based schemes.

Modalities	Authentication types	Usability pros and cons indicated	Security solutions or concerns reported
OTP [75]; device pairing [77, 79]	Multifactor; adaptive; dynamic; risk-based	[40, 79, 80–82]	[73–78]

users (40% of them) prefer graphical patterns for device unlocking. But this approach too requires users to remember them; hence users choose simple and less secure patterns, that is, if a user connects at least four dots without repeating any of them in their patterns, the maximum number of combinations are 389,112 which could be easily cracked by brute force [63]. Ye at al. [64] managed to crack 95% of 120 unique patterns collected from 215 independent users within just five attempts by recording their smartphone screen, remotely, while they were unlocking their devices. In addition, these schemes are more vulnerable to shoulder surfing than textual passwords [65].

Knowledge-based authentication schemes are generally used as one-shot, static, or unimodal authentication types (refer Table 1) due to usability issues they are prone to several attacks, such as smudge attacks [66], shoulder surfing or observation attacks [61, 67], dictionary-based attacks, or rainbow table password attacks [68]. Recently, Mehrnezhad et al. [69] demonstrated the recovery of entered PIN or password from the sensory data collected, while the users were entering their secrets. They installed PINlogger.js—a JavaScript-based side-channel attack, capable of recording motion and orientation sensor streams without requiring any user permission from the user. The attack resulted in 94% accuracy in recovering the correct PIN number in just three rounds of tries. Similarly, Sarkisyan et al. [70] demonstrated an approach to exploit smartwatch motion sensors to recover the entered PINs. They infested smartwatches with malware to get access to the smartwatch motion sensors and inferred user activities and PINs. In a controlled scenario, authors obtained PIN numbers within 5 guesses with an accuracy of at least 41% using random forest classifier over a dataset of 21 users.

3.1.2. Something You Have. As defined in Section 2.1.2, smartphones are being utilized for authentication purposes in several sensitive operations by the means of OTP via SMS, offline OTP using Apps, or pairing the wearable devices, for example, smartwatches, smartglasses, and smartcards. However, this idea of enhancing security with multifactor authentication, that is, topping *knowledge-based authentication* with *token-based authentication* (one-time passcode), eventually perishes too due to side-channel attacks, for example, MITM (man-in-the-middle) and MITPC/Phone (man-in-the-PC/phone) [73]. Software-based OTP solutions also do not guarantee the confidentiality of the generated passwords or the seeds as the mobile OS could be compromised, at the same time, could also suffer from denial-of-service attacks on the account of mobile OS crashes [74].

The adversaries by the means of real-time phishing or intercept attacks could reveal the users' secret information and valid OTP by breaking into their smartphones [75]. As per the Verizon Data Breach Investigations Report [76], NIST stopped recommending the users for two-factor authentication via SMS, as malicious code infesting mobile endpoints could surreptitiously capture second factors delivered by SMS or offline OTP generated using apps. Secure device pairing schemes allow access to the smartphones by pairing it with a trusted Bluetooth device like a smartwatch and use the same to unlock the phone. This concept from the usability point of view is a very elegant solution but not safe from insider attacks or sniffing attacks [77, 78].

Token-based authentication (TBA) schemes are used in multifactor, adaptive, dynamic, and risk-based authentication types (Table 2). Unfortunately, they could not add too much to the usability because the users are required to manage always an additional hardware for the sole purpose of authentication. As a result, Braz and Robert [40] gave usability rating 3 (out of 5) to one-time generator acquisition devices. Additionally, Belk mentioned that token-based authentication mechanism incurred more cost to users and are comparatively slower [79]. According to a study by Zink and Waldvogel [82], 83.3% users considered that SMS-based transaction authentication number is not a usable solution. Another in-depth usability study by Krol et al. [81] evaluated 2-factor authentication on 21 online banking customers (16 among 21 were having multiple accounts with more than one bank). Total 90 separate login sessions of all the participants were collected meticulously, over the period of 11 days. Their analysis showed approximately 13.3% faced problems due to mistyped credentials, misplaced token, forgotten credentials and so on.

3.1.3. Something You Have: Insertable Biometrics. Insertable biometrics [83–85] (Table 3) including implantable medical devices (IMDs) [86] and emerging technologies such as Bespoke devices [87, 88], neodymium magnets [89], NFC or RFID chips [90, 91], smart piercings [92, 93], and smart tattoos [93] are the newer addition to biometrics that

Table 3: Synopsis of insertable biometrics.

Modalities	Authentication types	Usability pros and cons indicated	Security solutions or concerns reported
Bespoke devices [87, 88]; neodymium magnets [89]; NFC or RFID chips [90, 91]; smart piercings [92, 93]; smart tattoos [93]	Continuous; multimodal; transparent	[94]	Data not available

Table 4: Synopsis of physiological biometrics.

Modalities	Authentication types	Usability pros and cons indicated	Security solutions or concerns reported
Face [99, 100]; eyes [10, 101]; iris [102]; fingerprint [103, 104]	One-shot; multifactor; multimodal	[49, 105–109]	[17, 95–97, 99, 100, 102–104, 110]

potentially can be used to provide increased usability over the existing solutions [94]. Researches are exploring the further possibilities of insertable biometrics as go-to solution for improving digital security and usability in smartphones.

3.1.4. Something You Are: Physiological Biometrics. Mobile device manufacturers have started embedding biometric sensors in their flagship smartphones for reliable and convenient user authentication with the intuition that biometric approaches are better than their conventional authentication schemes. For example, Apple, Huawei, Lenovo (Motorola), Microsoft (Nokia), Samsung, and many other leading manufacturers have integrated fingerprint sensors, iris scanners, and face recognition algorithms, in some of their high-end devices. These advancements are akin to replacing a hay castle with a glass house to ward off attacks from sophisticated cyber pirates.

Physiological biometrics, for example, face, fingerprint, iris, and eyes, are commonly used as one-shot or multifactor/multimodel (combining with other modalities) authentication schemes for smartphones (Table 4). Unexpectedly, biometric systems have shown to be exposed to different types of attacks, for example, impersonation, replay, spoofing, and hill climbing [95], exposing their security loopholes. These schemes suffer from their data leakage; that is, a user's face can be easily found on social media websites, or his or her fingerprints can be extracted from the photos from their gestures, to mount a presentation attack [96] against them. Additionally, these solutions also suffer from lack of secrecy [97] and vulnerability to various spoofing attacks [98].

Recent research has shown that these schemes can be hacked very easily with almost negligible investment and efforts. For example, iPhone X face ID was hacked with 3D-printed mask costing just $150 approximately [100], while Samsung S8 facial recognition technology [99] was simply fooled with a photo of the owner. Similarly, German Chaos Computer Club cracked the Samsung Galaxy S8 iris scanner [102] with a dummy eye made from pictures of the iris, taken by a digital camera in a night mode, and covered it with a contact lens to match the curvature of the eye, within a month of S8 launch. The same club earlier cracked the iPhone 5S fingerprint sensor protection within two days after the device went on sale worldwide [103]. Their hacking team photographed the glass surface containing the fingerprint of a user and created a "fake fingerprint" using a thin film to unlock the phone. Japan's National Institute of Informatics (NII) researcher Isao Echizen [104] demonstrated that fingerprints can easily be recreated from photos, taken just from three meters distance, without the use of any sophisticated process and warned casually making a peace sign in front of a camera, which could lead to fingerprint theft.

From the usability perspective, smartphone users have not shown optimistic inclination to physiological biometric-based authentication schemes. For example, De Luca et al. [49] determined smartphone users felt like as if they are taking selfies all day to authenticate themselves. Additionally, the performance of these schemes is affected by several exogenous factors, such as accessories, camera movement, capturing distance, clothing, illumination, interoperability of the sensors, noise, occlusion, operators, postures, and training, which makes the authentication process more challenging and less usable to the user [106–109].

3.1.5. Something You Are: Behavioral Biometrics. Behavioral biometrics [111] is described as the future of user authentication. Thus, the focus of the research has been shifted to develop newer behavioral biometric-based solutions. For example, applications like e-wallet, m-commerce, and mobile banking are some of the sensitive domains, where behavioral biometric-based solutions have shown to be handy in authenticating the customers on their smartphones.

Although the behavioral modalities are not considered to be unique enough for identification purposes, they have proved to be sufficiently unique for user authentication [112, 113]. One or more modalities can be combined to increase their accuracy and enhance their usability. These schemes could be stitched to the existing user authentication mechanisms as an additional transparent authentication layer [8, 9, 114] enhancing the reliability of whole authentication process without affecting the usability. Behavioral biometric techniques could be deployed as adaptive, continuous, multimodal, risk-based, transparent authentication (Table 5).

Gait recognition is a process of identifying or verifying individuals on the basis of their walking style. In clinical applications, human gait was already getting utilized for the studies related to the health of a person, and nearly 25 key patterns from gait were detected using different techniques like

Table 5: Synopsis of behavioral biometrics.

Modalities	Authentication types	Usability pros and cons indicated	Security solutions or concerns reported
Touch [9, 113]; keystroke [115]; hold [8]; gait [116–118]; behavior profiling [119]	Adaptive; continuous; multimodal; risk-based; transparent	[3, 5, 10, 113, 119–121]	[8, 12, 29, 112, 113, 115–117, 122–127]

image processing, floor sensors, and sensors placed on the body [118]. Recently, smartphones and wearable devices have also started utilizing it for authentication purposes [128]. As users are not required to perform any explicit interaction with their devices, gait modality can be collected unobtrusively, and this leads to making it convenient for a user-friendly access system [116]. Muaaz and Mayrhofer [116] evaluated the security strength of a smartphone-based gait recognition system against zero-effort and live-minimal-effort impersonation attacks under realistic scenarios and achieved an equal error rate (EER) of 13% on a dataset of 35 participants. However, more testing is required to check the robustness against impersonation attacks. Hestbek et al. [117] introduced a method using wearable sensors and noncyclic feature extraction and achieved 18.92% half total error rate (HTER) on a dataset of 36 users. Similarly, the grip is another natural way to authenticate users. It is robust too as the finger movements and pressure applied while gripping the mobile device are visibly unseen and difficult to be replicated or imitated by the impostor. Murao et al. [124] proposed a grip-based authentication solution, which profiles grip gestures using pressure sensors mounted on the lateral and back sides of a smartphone and achieved a 2% ERR, which is equivalent to face recognition-based authentication.

Keystroke or touch dynamics refers to the typing characteristics (due to the timing differences) of individuals to fingerprint their identity. Researchers have proved its effectiveness in both fixed text and text independent scenarios. Since designing such systems does not require any additional dedicated hardware and data can be collected, unobtrusively, they have been widely tested and evaluated [9, 114]. Zheng et al. [115] proposed authentication mechanism based on tapping; they collected tapping data from over 80 users; and their system achieved high accuracy with averaged 3.65% EER. Another bimodal authentication scheme developed using client-server architecture for online financial environments achieved 96% true acceptance rate (TAR) and 0.01% false acceptance rate (FAR) using 15 training samples on a dataset of 95 users [9]. This scheme used motion-based touch-types biometrics, that is, touch typing and phone movements by users and collected data, transparently, while users entering their credentials to sign in to their banking apps using 8-digit PIN/password [9], while the "touchstroke" scheme used 4-digit PIN/password [114]. Buriro et al. [8], proposed, implemented, and evaluated the "Hold and Sign" scheme on commercially available smartphones and achieved 95% TAR on a dataset of 30 volunteers. This was a bimodal behavioral biometric based on user's smartphone holding style, by examining the hand and finger micromovements of users, while the users were signing on device's touchscreen. In an another approach, Buriro et al. [113] proposed multimodal behavioral biometrics (swipe, pickup movement, and voice) for user authentication on smartphones and reported 7.57% HTER in an experiment involving 26 participants.

Brunet et al. [123] experimented on voice modality for user authentication on a public database (Sphinx Database of the Carnegie Mellon University [129]). They digitized the user's voice and extracted Mel Frequency Cepstral Coefficients (MFCCs) features and computed the Euclidean distance to authenticate the user and reported an EER of 4.52%. Behavior profiling techniques were based on the applications, and the services utilized in past for generating a user profile and compared it against the current activity of a user in real-time [5]. If any significant variation is observed, the system could take action for a possible intrusion. Sultana et al. [119] combined social behavioral information of individuals that was extracted from the online social networks to fuse with traditional face and ear biometrics, to enhance the performance of the traditional biometric systems.

Studies suggest that no single biometric trait can ideally fit all the scenarios; however, by trying multimodal biometric approaches, most of the limitation of unimodal systems can be addressed [121, 122, 125]. The selection of proper modalities and combining them, systematically, most of the times increase the accuracy, usability, and security. In a study conducted by Saevanee et al. [126], the unimodal systems, namely, behavior profiling, keystroke dynamics, and linguistic profiling, were proved less accurate; they yielded an EER of 20%, 20%, and 22%, respectively. However, by applying matching-level fusion, the error rate was decreased, significantly (EER 8%). Additionally, the use of users' transparent characteristics for data collection and classification also increases the usability of the system. Thus, in order to furnish users with an adequate security, a better usability is also required to design the authentication solutions for smartphones.

3.2. Authentication Types

3.2.1. One-Shot Authentication. *One-shot authentication* schemes are designed to authenticate a user at the initiation of a session (subject's identity is verified only once, just before allowing access to the resources) [16, 18]. Roth et al. [18] also discussed the limitations of one-shot authentication, such as short sensing time, inability to rectify decisions, and enabling the access for potentially unlimited periods of time. Meng et al. [17] introduced the term one-off authentication for one-shot authentication. They also concluded that authenticating just once leaves the possibilities for impostors to gain the access to the current session and retrieve sensitive information from mobile phones.

3.2.2. Periodic Authentication. Bertino et al. [19] defined *periodic authorization* with a mathematical expression "{[begin,

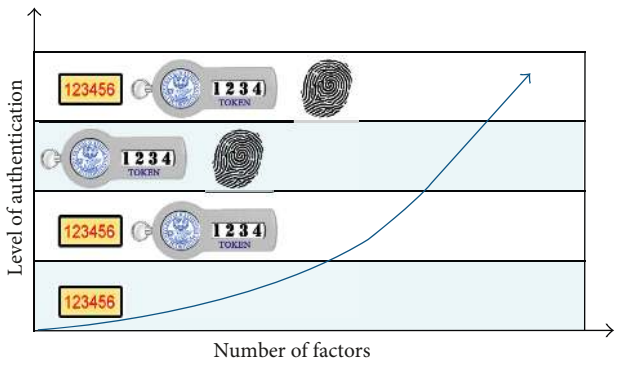

Figure 5: Factors of authentication [27].

end], P, auth}" holding of 3 prime attributes, where "begin" is authorization start date, "end" is either the constant ∞, or a deauthorization date after the start date, "P" is the duration of a session, and "auth" is an authorization function. Feng et al. [4] determined that periodic authentication or automatic logouts are more detrimental while one-shot authentication solutions are prone to a wide variety of attacks. Typing an error-free username and/or password on smartphone's keyboard is really a tedious task, especially when an average user initiates 76 phone sessions a day [51]. *Single sign-on* (SSO) has been seen as the solution to the problem.

3.2.3. Single Sign-On. *Single sign-on* (SSO) enables users to sign in to an app using a single or federated identity, for example, Facebook, Twitter, and Google+. But this concept is severely risky for mobile devices as they are more likely to be misplaced or could be inadvertently shared with someone. In an SSO system, the user is authenticated to a single identity provider (IDP) which acts as a trusted party between the user and multiple service providers (SPs), and on the demand of the user, IDP generates an authentication token for a specific SP asserting the users' identity; in turn, SP allows the user to access the services [20]. Users can access different applications using SSO, once they are authenticated to the system. SSO is further divided into two categories, that is, Enterprise Single Sign-ON (ESSO) and Reduced Sign-ON (RSSO) [21]. ESSO enables a user to enter the same id and password to sign into multiple applications within an enterprise domain. The system is considered the least secure because there could be potential curious adversary which can try to spoof and consequently resulting in an identity theft. Therefore, it is also known as RSSO.

3.2.4. Multifactor Authentication. Security experts also suggest the use of *multifactor authentication* by processing multiple factors, simultaneously, for the verification purposes [27]. In multifactor authentication, generally, a PIN or password is the baseline authentication standard, while more factors can be augmented from a wide variety of available sources to verify users (Figure 5). It could be observed in Figure 5 that as the number of factors increases, the level of authentication also increases. For an instance, if only PIN is used, the authentication level is minimum, but when other factors like tokens and fingerprints are added, the authentication level tends to increase proportionally.

Figure 6: Static authentication process [29].

The most common authentication mechanism is the secondary code that can be delivered either via SMS to the registered mobile number or can be obtained directly from a secure authenticator mobile app. Other forms of multifactor authentication involve the use of a smart card or smart token entitled to the user, biometrics like the face or fingerprint scans, or a dedicated code generator linked to user's account [25]. This concept is mainly influenced by the notions that not all the authentication factors could be hacked at the same time. Stanislav [26] in his paper explained various technical methods by which two-factor authentication can be implemented.

3.2.5. Static versus Dynamic Authentication. *Static authentication* process, like other authentication types, mainly consists of three steps: enrollment, presentation, and evaluation as illustrated in Figure 6, and the outcome of the evaluation is a binary decision [29]. In the enrollment step, system generates a feature template by processing the information gathered from the user, profiles the feature vectors with the label of the user, and saves it for the evaluation or matching. During the presentation step, system asks the user to confirm his or her credentials. In the final step, that is, evaluation, information given by the user is compared with the stored templates of the claimed identity. Conclusively, the access is granted or denied as per the match result.

Static authentication verifies the individual's identity only at the start of a session like one-shot authentication does, whereas in *dynamic authentication* the user is presented with a varying set of challenges to enable the dynamic scaling of access controls. Ren and Wu [28] explained dynamic authentication as a scheme that utilizes one-time password derived from the user's password, the authenticating time, and a unique attribute only known to the user.

3.2.6. Continuous Authentication. *Continuous authentication* is a mechanism to repeatedly verify the identity of a user for the entire duration of an authorized session as illustrated in Figure 7 [29]. More specifically a continuous authentication is an approach that constantly verifies a user's identity and locks the system once the change in users' identity is observed [29]. Continuous authentication process dynamically iterates in between the three steps involved (Figure 6) throughout the session. However, these iterations can be event-based or can be adjusted at fix intervals (periodically) or randomly [29]. A continuous authentication is an approach that constantly verifies a user's identity and locks the system once the change in user identity is observed. Thus, overcoming the limitations of one-shot authentication, where authentication happens only at the time of login, and any future changes in user identity go undetected [130]. Behavioral biometric-based

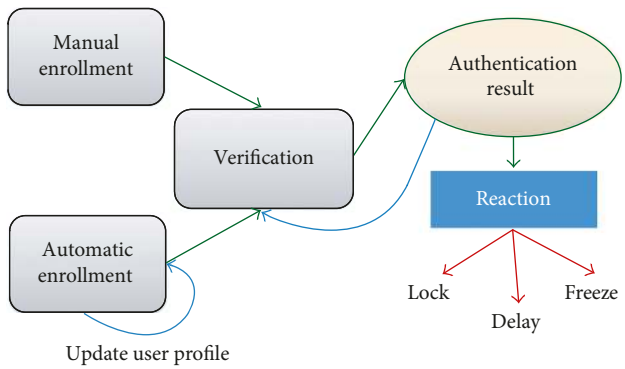

Figure 7: Continuous authentication process [29].

continuous authentication solutions have shown to be more attractive to the researchers of the domain because these behavioral modalities can be collected and utilized, unobtrusively, for authentication purposes [30].

However, continuous authentication, active authentication, implicit authentication, and transparent authentication have been interchangeably used in many papers [10, 120, 131, 132]. Patel et al. [5] considered continuous authentication and active authentication systems as similar and explained it as continuous monitoring of the user activities after the initial access to the mobile device. Active authentication, as defined by Stolerman et al. [132], is the process of continuously verifying users based on their on-going interaction with the device. The Defense Advanced Research Projects Agency (DARPA) started Active Authentication program [133] in order to seek solutions by shifting the focus during authentication from the password to people themselves. The first phase of their Active Authentication program focused on the behavioral traits, that is, cognitive fingerprint, which could be processed without the need for additional sensors.

According to Fridman et al. [134], active authentication is the problem of continuously verifying the identity of an individual. They conducted an experiment using Android mobile devices and collected several biometric modalities, namely, text entered via soft keyboard, applications used, websites visited, physical location of the device as determined from GPS (when outdoors) or WiFi (when indoors), and stylometry, of 200 volunteers approximately for a period of at least 30 days. Their authentication system achieved an ERR of 0.05 (5%) after 1 minute of user interaction with the device, and an EER of 0.01 (1%) after 30 minutes in identifying a legitimate user. In another stylometric-based continuous authentication, an EER of 12.42% for message blocks of 500 characters is achieved using support vector machine (SVM) for classification [135]. However, stylometry-based authentication schemes must improve the accuracy, delays, and forgery.

Khan et al. [120] mentioned that *implicit authentication* employs behavioral biometrics in a continuous and transparent manner to recognize and validate smartphone users' identity and conducted a field study on implicit authentication usability and security perceptions with 37 participants. Their experiment indicated that 91% of participants found implicit authentication to be convenient and 81% perceived defined the protection level to be satisfactory.

3.2.7. Transparent Authentication. *Transparent authentication* [10] was suggested as an alternative authentication mechanism with minimal or no noticeable involvement of users. Transparent authentication implicitly authenticates the users on the basis of their unique interactions with the device and creates a logic for authentication decisions. Feng et al. [4] utilized the term transparent and continuous for their Finger-gestures Authentication System using Touchscreen (FAST) to protect the mobile system. The approach transparently captures the touch data without intervening to user's normal user-device interactions. After the user's login, FAST continues to authenticate the mobile user in the background using intercepted touch data from their normal user-smartphone interactions.

3.2.8. Risk-Based Authentication. ClearLogin [136] defines *risk-based user authentication* as a method which adapts authentication levels based on the apparent risks, to mitigate the potential intrusion, before they happen. Existing *risk-based user authentication* schemes generate a risk profile to determine the complexity of challenge to authenticate a user during a session, that is, higher-risk profiles lead to stronger authentication, whereas usual authentication scheme should be sufficient in normal scenarios [137]. Identity Automation [138] considers *risk-based user authentication* similar to *adaptive authentication* because they adapt to the stringency of authentication processes based on the likelihood that access to a given system could result in its compromise.

Earlier risk-based user authentication mechanisms were mainly based on contextual or historical user information or both [139]. Furthermore, these systems use ad hoc or simplistic risk management models based on some rule-based techniques, which are proved to be ineffective due to human factors [140]. However, nowadays as NuData Security [34] mentioned risk-based authentication schemes are getting fueled by behavior piercing technology that gives maximum security with minimal interruption to the user experience. Risk-based user authentication can be applied from two different perspectives: proactive or re-active [12]. When applied proactively, risk-based authentication actively anticipates the genesis of potential attacks, failures, or any kind of security issues and takes prompt action. In contrast, re-active risk-based authentication accepts some of the risks until the risk score goes beyond the permissible threshold level, and consequently, reauthentication is required.

3.2.9. Adaptive Authentication. *Adaptive authentication* [141] is a way by which two- or multifactor authentication can be configured and deployed by doing risk assessment. Thus, it is a method for selecting the appropriate authentication factors accustomed to the situation accordingly to the user risk profile and tendencies. It can be deployed as follows:

(i) By setting static policies based on risk levels for different factors, such as user role, resource importance, location, time of day, or day of the week

(ii) By learning day-to-day activities of users based on their habits to generate dynamic policies

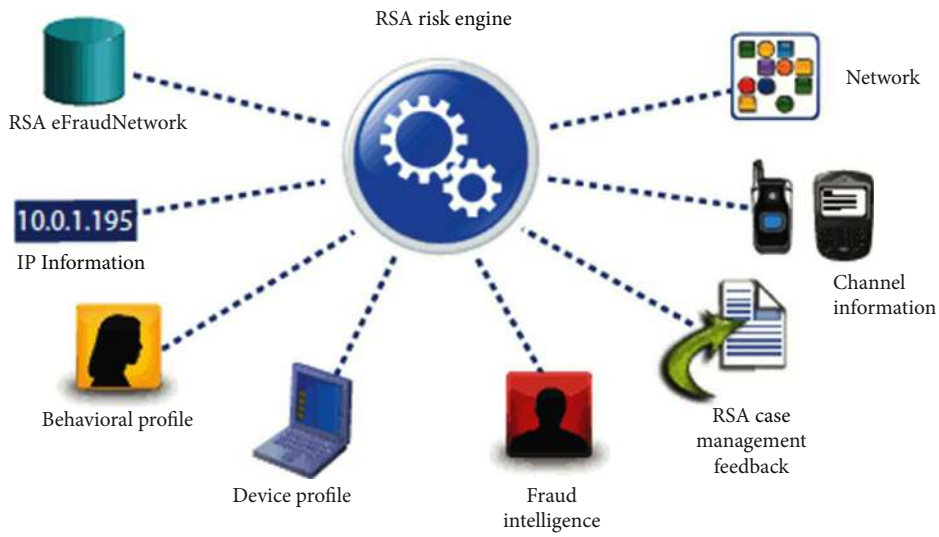

Figure 8: RSA adaptive authentication [36]. The RSA Risk Engine measures over one hundred indicators and assigns a unique risk score to each activity.

(iii) Lastly, by combing of both static and dynamic policies

Hulsebosch et al. [35] exploited the ability to sense and use context information to augment or replace the traditional static security measures by making them more adaptable to a given context and thereby less intrusive to derive context sensitive adaptive authentication. RSA Risk Engine [36] used self-learning risk model and adapts itself on the basis of received feedback. The feedback loop includes case resolution and genuine or failed authentication results as well as chargeback files for *adaptive authentication* for e-commerce (Figure 8).

3.2.10. Unimodal and Multimodal Authentication Systems. *Unimodal authentication systems* use single modality for establishing user identity, whereas *multimodal authentication systems* include multiple modalities (sources of information) [39]. Unimodal and multimodal terms are more associated with biometric systems where person recognition is based on distinctive personal traits or characteristics [37]. Unimodal physiological biometric based on face, fingerprint, and iris are already deployed on the smartphones; however, multimodal systems are yet to be deployed. Behavioral biometric-based solutions based on touch-stroke dynamics, voice, gait, and so on have been widely tested and evaluated by researchers; however, their deployment to the smartphones is still awaited.

Jain et al. [38] showed that multimodal biometric systems driven by multiple biometric sources perform, generally, better recognition performance as compared to unimodal systems. As per the type of multiple modalities being used, multimodal biometric systems can be further divided into three categories: (1) multiphysiological, (2) multibehavioral, and (3) hybrid multimodal systems [142]. The multiphysiological category includes multimodal biometric systems, where only physiological traits, such as face, fingerprint, and iris, are fused at different levels, whereas the multibehavioral system combines data from keyboard, mouse, and graphical user interface interactions. Hybrid multimodal system [143] fused face, ear, and signature with social network analysis at the decision level to enhance the biometric recognition performance.

Researchers have been actively working on combining different modalities to develop multimodal solutions; however, these systems have yet to appear on the real products.

4. Conclusion

In this paper, we presented the gist of ways and types of user authentication concepts in the context of smartphones. We surveyed the different state-of-the-art solutions proposed over the years and attempted to homogenize correlated buzzwords used in this field, with the motivation to assist new researchers in understanding these concepts. Then, we evaluated the related work on the ways and types of user authentication mechanisms available for smartphones, on the basis of their usability and security. Also, we discussed design goals for usable authentication systems and usability evaluation methods.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement no. 675320.

References

[1] Motorola, "Timely achievements," 2017, https://www.motorola.com/us/about/motorola-history-milestones.

[2] N. Triandopoulos, A. Juels, R. L. Rivest, and J. Brainard, "Multi-server one-time passcode verification on respective high order and low order passcode portions," US Patent 9,454,654, 2016.

[3] D. Crouse, H. Han, D. Chandra, B. Barbello, and A. K. Jain, "Continuous authentication of mobile user: fusion of face image and inertial measurement unit data," in *Proceedings of the International Conference on Biometrics (ICB)*, pp. 135–142, IEEE, Phuket, Thailand, May 2015.

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

[5] 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.

[6] D. C. Dutt, A. B. Somayaji, and M. J. K. Bingham, "System and method for behavioural biometric authentication using program modelling," US Patent App. 15/059,692, 2016.

[7] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and i know it's you!: implicit authentication based on touch screen patterns," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 987–996, ACM, New York, NY, USA, 2012.

[8] A. Buriro, B. Crispo, F. Del Frari, and K. Wrona, "Hold and sign: a novel behavioral biometrics for smartphone user authentication," in *Proceedings of the 2016 IEEE Security and Privacy Workshops (SPW)*, pp. 276–285, IEEE, San Jose, CA, USA, May 2016.

[9] A. Buriro, S. Gupta, and B. Crispo, "Evaluation of motion-based touch-typing biometrics in online financial environments," in *Proceedings of the 16th International Conference of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, September 2017.

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

[11] B. Causey, "Adaptive authentication: an introduction to risk-based authentication," 2013, http://searchsecurity.techtarget.com/tip/Adaptive-authentication-An-introduction-to-risk-based-authentication.

[12] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, and I. Lai, "Online risk-based authentication using behavioral biometrics," *Multimedia tools and applications*, vol. 71, no. 2, pp. 575–605, 2014.

[13] M. B. Ayed, "Method for adaptive authentication using a mobile device," US Patent 8,646,060, 2014.

[14] F. B. Schneider, "Something you know, have, or are," 2005, https://www.cs.cornell.edu/courses/cs513/2005fa/NNLauthPeople.html.

[15] N. Forsblom, "Were you aware of all these sensors in your smartphone?," 2015, https://blog.adtile.me/2015/11/12/were-you-aware-of-all-these-sensors-in-your-smartphone/.

[16] A. Buriro, "Behavioral biometrics for smartphone user authentication," Ph.D. thesis, University of Trento, Trento, Italy, 2017.

[17] 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.

[18] J. Roth, X. Liu, A. Ross, and D. Metaxas, "Biometric authentication via keystroke sound," in *Proceedings of the International Conference on Biometrics (ICB)*, pp. 1–8, IEEE, Madrid, Spain, June 2013.

[19] E. Bertino, C. Bettini, E. Ferrari, and P. Samarati, "An access control model supporting periodicity constraints and temporal reasoning," *ACM Transactions on Database Systems*, vol. 23, no. 3, pp. 231–285, 1998.

[20] F. Feldmann, *Binding Credentials: Securing (SSO) Authentication*, Ruhr University Bochum, Bochum, Germany, 2016.

[21] HuntingtonVentures, "Single sign on: the business of authentication," 2006, https://archive.is/20140315095827/.

[22] A. Salazar, "SSO vs. centralized authentication," 2014, https://stormpath.com/blog/sso-vs-centralized-auth.

[23] VMware, "VMware identity manager documentation center," 2017, https://pubs.vmware.com/vidm/index.jsp?topic=%2Fcom.vmware.wsair-administration%2FGUID-1E5128A5-1394-4A50-8098-947780E38166.html.

[24] Google, "G suite: single sign-on on an android device," 2016, https://support.google.com/a/users/answer/2758865?hl=en.

[25] R. Ritchie, D. Rubino, K. Michaluk, and P. Nickinson, "The future of authentication: Biometrics, multi-factor, and co-dependency," 2013, https://www.androidcentral.com/talk-mobile/future-authentication-biometrics-multi-factor-and-co-dependency-talk-mobile.

[26] M. Stanislav, *Two-Factor Authentication*, IT Governance Ltd., Ely, UK, 2015.

[27] D. G. Warnock and C. C. Peck, "A roadmap for biomarker qualification," *Nature biotechnology*, vol. 28, no. 5, pp. 444-445, 2010.

[28] X. Ren and X.-W. Wu, "A novel dynamic user authentication scheme," in *Proceedings of the International Symposium on Communications and Information Technologies (ISCIT)*, pp. 713–717, IEEE, Gold Coast, QLD, Australia, October 2012.

[29] I. Traoré and A. A. E. Ahmed, *Introduction to Continuous Authentication, in Continuous Authentication Using Biometrics: Data, Models, and Metrics: Data, Models, and Metrics*, University of Victoria, Victoria, BC Canada, 2011.

[30] 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.

[31] A. Buriro, B. Crispo, and Y. Zhauniarovich, "Please hold on: unobtrusive user authentication using smartphone's built-in sensors," in *Proceedings of the IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, pp. 1–8, IEEE, New Delhi, India, February 2017.

[32] Wikipedia, "Risk-based authentication," 2017, https://en.wikipedia.org/wiki/Risk-based_authentication.

[33] A. J. Harris and D. C. Yen, "Biometric authentication: assuring access to information," *Information Management & Computer Security*, vol. 10, no. 1, pp. 12–19, 2002.

[34] NuData Security, "What is risk based authentication?," 2017, https://nudatasecurity.com/blog/ecommerce/what-is-risk-based-authentication/.

[35] R. Hulsebosch, M. S. Bargh, G. Lenzini, P. Ebben, and S. M. Iacob, "Context sensitive adaptive authentication," in *Proceedings of the European Conference on Smart Sensing and Context*, pp. 93–109, Springer, Kendal, UK, October 2007.

[36] RSA, "RSA adaptive authentication system," 2017, https://www.rsa.com/content/dam/rsa/PDF/h9096-rsa-risk-engine-sb-11-2.pdf.

[37] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross, "Biometrics: a grand challenge," in *Proceedings of the 17th International Conference on Pattern Recognition (ICPR)*, vol. 2, pp. 935–942, IEEE, Cambridge, UK, August 2004.

[38] A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognition*, vol. 38, no. 12, pp. 2270–2285, 2005.

[39] A. Ross and A. Jain, "Information fusion in biometrics," *Pattern recognition letters*, vol. 24, no. 13, pp. 2115–2125, 2003.

[40] C. Braz and J.-M. Robert, "Security and usability: the case of the user authentication methods," in *Proceedings of the 18th Conference on l'Interaction Homme-Machine*, pp. 199–203, ACM, New York, NY, USA, 2006.

[41] K.-P. Yee, "User interaction design for secure systems," in *Proceedings of the 4th International Conference on Information and Communications Security*, pp. 278–290, Singapore, December 2002.

[42] Microsoft, "Key principles of software architecture," 2018, https://msdn.microsoft.com/en-us/library/ee658124.aspx.

[43] J. Brooke, *SUS-A Quick and Dirty Usability Scale: Usability Evaluation in Industry*, Taylor and Francis, Oxford, UK, 1996.

[44] Usability, "System usability scale (sus)," 2017, https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html.

[45] M. F. Theofanos, R. J. Micheals, and B. C. Stanton, "Biometrics systems include users," *IEEE Systems Journal*, vol. 3, no. 4, pp. 461–468, 2009.

[46] ISO, *Human-Centred Design Processes for Interactive Systems*, International Organization for Standardization, Geneva, Switzerland, 1999.

[47] M. A. Sasse, "Red-eye blink, bendy shuffle, and the yuck factor: a user experience of biometric airport systems," *IEEE Security & Privacy*, vol. 5, no. 3, pp. 78–81, 2007.

[48] M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It's a hard lock life: a field study of smartphone (un) locking behavior and risk perception," in *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pp. 9–11, Menlo Park, CA, USA, July 2014.

[49] A. De Luca, A. Hang, E. Von Zezschwitz, and H. Hussmann, "I feel like I'm taking selfies all day!: towards understanding biometric authentication on smartphones," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 1411–1414, ACM, New York, NY, USA, 2015.

[50] T. Sloane, "Behavioral biometrics: the restructuring of the authentication landscape," 2017, https://www.mercatoradvisorygroup.com/Webinars/Behavioral_Biometrics__The_Restructuring_of_the_Authentication_Landscape/.

[51] M. Winnick, "Putting a finger on our phone obsession," 2016, https://blog.dscout.com/mobile-touches.

[52] N. Cowan, C. C. Morey, Z. Chen, A. L. Gilchrist, and J. S. Saults, "Theory and measurement of working memory capacity limits," *Psychology of Learning and Motivation*, vol. 49, pp. 49–104, 2008.

[53] J. Zhang, X. Luo, S. Akkaladevi, and J. Ziegelmayer, "Improving multiple-password recall: an empirical study," *European Journal of Information Systems*, vol. 18, no. 2, pp. 165–176, 2009.

[54] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[55] M. Awad, Z. Al-Qudah, S. Idwan, and A. H. Jallad, "Password security: password behavior analysis at a small university," in *Proceedings of the 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA)*, pp. 1–4, IEEE, Ras Al Khaimah, UAE, December 2016.

[56] S. Komanduri, R. Shay, P. G. Kelley et al., "Of passwords and people: measuring the effect of password-composition policies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2595–2604, ACM, New York, NY, USA, 2011.

[57] J. Bonneau, S. Preibusch, and R. J. Anderson, "A birthday present every eleven wallets? The security of customer-chosen banking pins," in *Proceedings of the 16th International Conference Financial Cryptography and Data Security*, vol. 7397, pp. 25–40, Springer, Kralendijk, Bonaire, February-March 2012.

[58] D. Silver, S. Jana, D. Boneh, E. Y. Chen, and C. Jackson, "Password managers: attacks and defenses," in *Proceedings of the 23rd USENIX Security Symposium*, pp. 449–464, San Diego, CA, USA, August 2014.

[59] T. Bhattasali, K. Saeed, N. Chaki, and R. Chaki, "A survey of security and privacy issues for biometrics based remote authentication in cloud," in *Proceedings of the IFIP International Conference on Computer Information Systems and Industrial Management*, pp. 112–121, Springer, Ho Chi Minh City, Vietnam, November 2014.

[60] PandaSecurities, "No password? You're asking to be hacked," 2016, https://www.pandasecurity.com/mediacenter/tips/smartphone-risk-dont-use-password.

[61] C. Katsini, M. Belk, C. Fidas, N. Avouris, and G. Samaras, "Security and usability in knowledge-based user authentication: a review," in *Proceedings of the 20th Pan-Hellenic Conference on Informatics*, p. 63, ACM, Patras, Greece, November 2016.

[62] J. K. Thorpe, *On the Predictability and Security of User Choice in Passwords*, Carleton University, Ottawa, ON, Canada, 2008.

[63] Secure Group, "Lock pattern, pin, or password: What is the most reliable way to lock a phone," 2017, https://blog.securegroup.com/lock-pattern-pin-or-password-what-is-the-most-reliable-way-to-lock-a-phone.

[64] G. Ye, Z. Tang, D. Fang et al., "Cracking android pattern lock in five attempts," in *Proceedings of the Network and Distributed System Security Symposium*, San Diego, CA, USA, February-March 2017.

[65] F. Tari, A. Ozok, and S. H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in *Proceedings of the Second Symposium on Usable Privacy and Security*, pp. 56–66, ACM, Pittsburgh, PA, USA, July 2006.

[66] A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith, *Smudge Attacks on Smartphone Touch Screens*, Vol. 10, Woot, Carrollton, TX, USA, 2010.

[67] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: a survey," in *Proceedings of the 21st Annual Computer Security Applications Conference*, p. 10, IEEE, Tucson, AZ, USA, December 2005.

[68] CAPEC-Release1.6, "Common attack pattern enumeration and classification," 2016, http://capec.mitre.org.

[69] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao, "Stealing pins via mobile sensors: actual risk versus user perception," *International Journal of Information Security*, pp. 1–23, 2016.

[70] A. Sarkisyan, R. Debbiny, and A. Nahapetian, "Wristsnoop: smartphone pins prediction using smartwatch motion sensors," in *IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 1–6, IEEE, Abu Dhabi, UAE, December 2015.

[71] F. Breitinger and C. Nickel, "User survey on phone security and usage," in *Proceedings of the Biometrics and Electronic Signatures (BIOSIG)*, pp. 139–144, Darmstadt, Germany, September 2010.

[72] M. Meeker and L. Wu, "Kleiner Perkins Caufield and Byers (KPCB): internet trends," 2017, http://www.kpcb.com/internet-trends.

[73] H. Choi, H. Kwon, and J. Hur, "A secure OTP algorithm using a smartphone application," in *Proceedings of the Seventh International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 476–481, IEEE, Sapporo, Japan, July 2015.

[74] H. Sun, K. Sun, Y. Wang, and J. Jing, "TrustOTP: transforming smartphones into secure one-time password tokens," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 976–988, ACM, Denver, CO, USA, October 2015.

[75] B. Cha, N. Kim, and J. Kim, "Prototype analysis of OTP key-generation based on mobile device using voice characteristics," in *Proceedings of the International Conference on Information Science and Applications (ICISA)*, pp. 1–5, IEEE, Jeju, Korea, April 2011.

[76] Verizon, "How long since you took a hard look at your cybersecurity?," 2017, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017.

[77] I. Agadakos, C.-Y. Chen, M. Campanelli et al., *Jumping the Air Gap: Modeling Cyber-Physical a Ack Paths in the Internet-of-Things*, ACM, New York, NY, USA, 2017.

[78] M. Fomichev, F. Alvarez, D. Steinmetzer, P. Gardner-Stephen, and M. Hollick, "Survey and systematization of secure device pairing," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 517–550, 2018.

[79] M. Belk, P. Germanakos, C. Fidas, and G. Samaras, "A personalization method based on human factors for improving usability of user authentication tasks," in *Proceedings of International Conference on User Modeling, Adaptation, and Personalization*, pp. 13–24, Springer, Aalborg, Denmark, July 2014.

[80] M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1411–1418, 2014.

[81] K. Krol, E. Philippou, E. De Cristofaro, and M. A. Sasse, ""They brought in the horrible key ring thing!" Analysing the usability of two-factor authentication in UK online banking," arXiv preprint arXiv:1501.04434, 2015.

[82] T. Zink and M. Waldvogel, "X. 509 user certificate-based two-factor authentication for web applications," in *Proceedings of the 10. DFN-Forum Kommunikationstechnologien*, pp. 51–61, Berlin, Germany, May 2017.

[83] K. J. Heffernan, F. Vetere, L. M. Britton, B. Semaan, and T. Schiphorst, "Insertable digital devices: voluntarily under the skin," in *Proceedings of the 2016 ACM Conference Companion Publication on Designing Interactive Systems*, pp. 85–88, ACM, Brisbane, QLD, Australia, June 2016.

[84] P. Strohmeier, C. Honnet, and S. Von Cyborg, "Developing an ecosystem for interactive electronic implants," in *Proceedings of the Conference on Biomimetic and Biohybrid Systems*, pp. 518–525, Springer, Edinburgh, UK, July 2016.

[85] M. Janiak, C. Schaub, D. Lynam, B. Howe, G. Wachter, and G. Krueger, "Biometric authentication device for use with a personal digital assistant," US Patent App. 09/854,078, 2001.

[86] K. J. Heffernan, "Insertables workshop," 2016, https://insertables.wordpress.com/.

[87] TechTarget, "Bespoke," 2017, http://whatis.techtarget.com/definition/bespoke.

[88] M. Gupta, C. Holloway, B. M. Heravi, and S. Hailes, "A comparison between smartphone sensors and bespoke sensor devices for wheelchair accessibility studies," in *Proceedings of the IEEE 10th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, pp. 1–6, IEEE, Singapore, April 2015.

[89] First4magnets, "Use of neodymium magnets," 2016, https://www.first4magnets.com/tech-centre-i61/information-and-articles-i70/neodymium-magnet-information-i82/common-applications-of-neodymium-magnets-i88.

[90] P. Urien and S. Piramuthu, "Framework and authentication protocols for smartphone, NFC, and RFID in retail transactions," in *Proceedings of the IEEE 8th International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pp. 77–82, IEEE, Melbourne, VIC, Australia, April 2013.

[91] I. J. Forster and A. N. Farr, "Method for preventing unauthorized diversion of nfc tags," US Patent App. 15/659,941, 2017.

[92] H. Hassan, S. Wacquant, and H. B. Seifert, "Vehicle driver monitoring system," US Patent App. 15/463,293, 2017.

[93] M. Cuff, "Smart digital tattoos," 2014, http://www.stylus.com/scckpj.

[94] K. J. Heffernan, F. Vetere, and S. Chang, "Towards insertables: devices inside the human body," *First Monday*, vol. 22, no. 3, 2017.

[95] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, *Guide To Biometrics*, Springer Science & Business Media, Berlin, Germany, 2013.

[96] R. Ramachandra and C. Busch, "Presentation attack detection methods for face recognition systems: a comprehensive survey," *ACM Computing Surveys*, vol. 50, no. 1, pp. 1–37, 2017.

[97] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, vol. 79, pp. 80–105, 2016.

[98] A. Hadid, N. Evans, S. Marcel, and J. Fierrez, "Biometrics systems under spoofing attack: an evaluation methodology and lessons learned," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 20–30, 2015.

[99] S. Kovach, "Business insider-Samsung's Galaxy S8 facial recognition feature can be fooled with a photo," 2017, http://www.businessinsider.com/samsung-galaxy-s8-facial-recognition-tricked-with-a-photo-2017-3?IR=T.

[100] J. Titcomb, "Hackers claim to beat iPhone X's face id in one week with 115 mask," 2017, http://www.telegraph.co.uk/technology/2017/11/13/hackers-beat-iphone-xs-face-one-week-115-mask/.

[101] H. Saevanee, N. Clarke, S. Furnell, and V. Biscione, "Continuous user authentication using multi-modal biometrics," *Computers & Security*, vol. 53, pp. 234–246, 2015.

[102] A. Hern, "The guardian-Samsung Galaxy S8 iris scanner fooled by German hackers," 2017, https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security.

[103] A. Charles, "The guardian-iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club," 2013, https://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked.

[104] C. McGoogan and D. Demetriou, "The telegraph-peace sign selfies could let hackers copy your fingerprints," 2017, http://www.telegraph.co.uk/technology/2017/01/12/peace-sign-selfies-could-let-hackers-copy-fingerprints.

[105] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides, "Biometric authentication on iPhone and Android: usability, perceptions, and influences on adoption," in *Proceedings of the Workshop on Usable Security (USEC)*, pp. 1-2, San Diego, CA, USA, January 2015.

[106] A. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*, Vol. 479, Springer Science & Business Media, Berlin, Germany, 2006.

[107] M. Kumar, A. Insan, N. Stoll, K. Thurow, and R. Stoll, "Stochastic fuzzy modeling for ear imaging based child identification," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 9, pp. 1265–1278, 2016.

[108] M. Sultana, M. Gavrilova, and S. Yanushkevich, "Multi-resolution fusion of DTCWT and DCT for shift invariant face recognition," in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (SMC)*, pp. 80–85, IEEE, Hong Kong, China, October 2014.

[109] Y. Xu, X. Fang, X. Li et al., "Data uncertainty in face recognition," *IEEE transactions on cybernetics*, vol. 44, no. 10, pp. 1950–1961, 2014.

[110] C. Song, A. Wang, K. Ren, and W. Xu, "EyeVeri: a secure and usable approach for smartphone user authentication," in *Proceedings of the 35th Annual IEEE International Conference on Computer Communications, IEEE INFOCOM 2016*, pp. 1–9, IEEE, San Francisco, CA, USA, April 2016.

[111] IBIA, "Behavioral biometrics," 2017, https://www.ibia.org/biometrics-and-identity/biometric-technologies/behavioral-biometrics.

[112] L. M. Mayron, "Behavioral biometrics for universal access and authentication," in *Proceedings of the International Conference on Universal Access in Human-Computer Interaction*, pp. 330–339, Springer, Los Angeles, CA, USA, August 2015.

[113] A. Buriro, B. Crispo, F. Del Frari, J. Klardie, and K. Wrona, "ITSME: multi-modal and unobtrusive behavioural user authentication for smartphones," in *Proceedings of the International Conference on Passwords*, pp. 45–61, Springer, Cambridge, UK, December 2015.

[114] A. Buriro, B. Crispo, F. Del Frari, and K. Wrona, "Touchstroke: smartphone user authentication based on touch-typing biometrics," in *Proceedings of the International Conference on Image Analysis and Processing*, pp. 27–34, Springer, Genoa, Italy, September 2015.

[115] N. Zheng, K. Bai, H. Huang, and H. Wang, "You are how you touch: user verification on smartphones via tapping behaviors," in *Proceedings of the IEEE 22nd International Conference on Network Protocols (ICNP)*, pp. 221–232, IEEE, Raleigh, NC, USA, October 2014.

[116] M. Muaaz and R. Mayrhofer, "Smartphone-based gait recognition: from authentication to imitation," *IEEE Transactions on Mobile Computing*, vol. 16, no. 11, pp. 3209–3221, 2017.

[117] M. R. Hestbek, C. Nickel, and C. Busch, "Biometric gait recognition for mobile devices using wavelet transform and support vector machines," in *Proceedings of the 19th International Conference on Systems, Signals and Image Processing (IWSSIP)*, pp. 205–210, IEEE, Vienna, Austria, April 2012.

[118] A. Muro-De-La-Herran, B. Garcia-Zapirain, and A. Mendez-Zorrilla, "Gait analysis methods: an overview of wearable and non-wearable systems, highlighting clinical applications," *Sensors*, vol. 14, no. 12, pp. 3362–3394, 2014.

[119] M. Sultana, P. P. Paul, and M. L. Gavrilova, "Social behavioral information fusion in multimodal biometrics," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2017.

[120] H. Khan, U. Hengartner, and D. Vogel, "Usability and security perceptions of implicit authentication: convenient, secure, sometimes annoying," in *Proceedings of the Symposium on Usable Privacy and Security (SOUPS 2015)*, pp. 225–239, Santa Clara, CA, USA, July 2015.

[121] N. Poh and J. Korczak, "Hybrid biometric person authentication using face and voice features," in *Proceedings of the 3rd International Conference Audio- and Video-Based Biometric Person Authentication (AVBPA)*, vol. 1, pp. 348–353, Springer, Halmstad, Sweden, June 2001.

[122] R. Brunelli and D. Falavigna, "Person identification using multiple cues," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 17, no. 10, pp. 955–966, 1995.

[123] K. Brunet, K. Taam, E. Cherrier, N. Faye, and C. Rosenberger, "Speaker recognition for mobile user authentication: an Android solution," in *8ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR SSI)*, p. 10, Mont-de-Marsan, France, September 2013.

[124] K. Murao, H. Tobise, T. Terada, T. Iso, M. Tsukamoto, and T. Horikoshi, "Mobile phone user authentication with grip gestures using pressure sensors," *International Journal of Pervasive Computing and Communications*, vol. 11, no. 3, pp. 288–301, 2015.

[125] J. Kittler, J. Matas, K. Jonsson, and M. R. Sánchez, "Combining evidence in personal identity verification systems," *Pattern Recognition Letters*, vol. 18, no. 9, pp. 845–852, 1997.

[126] H. Saevanee, N. Clarke, and S. Furnell, "Multi-modal behavioural biometric authentication for mobile devices," in *Information Security and Privacy Research*, pp. 465–474, Springer, Heidelberg, Germany, 2012.

[127] Y. Tang, N. Hidenori, and Y. Urano, "User authentication on smart phones using a data mining method," in *Proceedings of the International Conference on Information Society (i-Society)*, pp. 173–178, IEEE, London, UK, June 2010.

[128] S. M. Welten, *Sensing with Smartphones*, 2013.

[129] Y. Obuchi, "PDA speech database," 2006, http://www.speech.cs.cmu.edu/databases/pda/index.html.

[130] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Evaluating behavioral biometrics for continuous authentication: challenges and metrics," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pp. 386–399, ACM, Abu Dhabi, UAE, April 2017.

[131] U. Mahbub, S. Sarkar, V. M. Patel, and R. Chellappa, "Active user authentication for smartphones: a challenge data set and benchmark results," in *Proceedings of the IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS 2016)*, pp. 1–8, IEEE, Buffalo, NY, USA, September 2016.

[132] A. Stolerman, A. Fridman, R. Greenstadt, P. Brennan, and P. Juola, "Active linguistic authentication revisited: real-time stylometric evaluation towards multi-modal decision fusion," in *Proceedings of the Tenth Annual IFIP WG 11.9 International Conference on Digital Forensics*, vol. 11, pp. 1–11, Vienna, Austria, January 2014.

[133] R. P. Guidorizzi, "Security: active authentication," *IT Professional*, vol. 15, no. 4, pp. 4–7, 2013.

[134] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, "Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location," *IEEE Systems Journal*, vol. 11, no. 2, pp. 513–521, 2017.

[135] M. L. Brocardo, I. Traore, and I. Woungang, "Toward a framework for continuous authentication using stylometry," in *Proceedings of the IEEE 28th International Conference on Advanced Information Networking and Applications (AINA 2014)*, pp. 106–115, IEEE, Victoria, Canada, May 2014.

[136] ClearLogin, "Risk-based authentication," 2017, http://www.clearlogin.com/glossary/risk-based-authentication/.

[137] B. Schneier, "Risk-based authentication," 2013, https://www.schneier.com/blog/archives/2013/11/risk-based_auth.html.

[138] Identity Automation, "Risk-based authentication," 2017, https://www.identityautomation.com/iam-platform/rapididentityidentity-access-management/multi-factor-authentication/risk-based-authentication/.

[139] D. Hintze, E. Koch, S. Scholz, and R. Mayrhofer, "Location-based risk assessment for mobile authentication," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, pp. 85–88, ACM, Heidelberg, Germany, September 2016.

[140] Y. Y. Haimes, *Risk Modeling, Assessment, and Management*, John Wiley & Sons, Hoboken, NJ, USA, 2015.

[141] IdentityAutomation, "What is adaptive authentication?," 2017, http://blog.identityautomation.com/what-is-adaptive-authentication.

[142] A. Jain and A. Kumar, "Biometric recognition: an overview," in *Second Generation Biometrics: The Ethical, Legal and Social Context*, E. Mordini and D. Tzovaras, Eds., pp. 49–79, Springer, Dordrecht, Netherlands, 2012.

[143] P. P. Paul, M. L. Gavrilova, and R. Alhajj, "Decision fusion for multimodal biometrics using social network analysis," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 11, pp. 1522–1533, 2014.