Received July 7, 2019, accepted July 18, 2019, date of publication August 1, 2019, date of current version August 27, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2932400

Recent Trends in User Authentication - A Survey

SYED W. SHAH AND SALIL S. KANHERE (Senior Member, IEEE)
School of Computer Science and Engineering, The University of New South Wales, Sydney, NSW 2052, Australia
Corresponding author: Syed W. Shah (syedwajidali.shah@student.unsw.edu.au)

ABSTRACT Recent advancements in technology have led to profusion of personal computing devices, such as smart phone, tablet, watch, glasses, and many more. This has contributed to the realization of a digital world where important daily tasks can be performed over the Internet from any place and at any time and using any device. At the same time, advances in pervasive computing technologies have brought to fruition the concept of smart spaces that target the automated provision of customized services to the inhabitants effortlessly. User authentication, i.e., a procedure to verify the identity of the user, is essential in the digital world so as to protect the user's personal data stored online (e.g., online bank accounts) and on personal devices (e.g., smart phones) and to also enable customized services in smart spaces (e.g., adjusting room temperature and so on). Recently, traditional authentication mechanisms (e.g., passwords or fingerprints) have been repeatedly shown to be vulnerable to subversion. Researchers thus have proposed numerous new mechanisms to authenticate the users in the aforementioned scenarios. This paper presents an overview of these novel systems, so as to guide the future research efforts in these domains.

INDEX TERMS User authentication, identification, personal devices, online services, smart spaces.

I. INTRODUCTION

User authentication is a process that verifies the identity of the user of a computing device (e.g., mobile phone) or an online service (e.g., email). An unerring user authentication mechanism is imperative to thwart an illicit access to personal computing devices (e.g., smart phones, watches, and glasses, etc) and online accounts (e.g., ebanking, emails, etc). Since both personal devices and online accounts carry important private data, unauthorized access can have serious repercussions like loss of money (e.g., online bank accounts) and privacy (e.g., personal pictures stored on mobile phones) [1], [2]. In addition, the wide proliferation of Internet of Things (IoT) have transformed our homes, offices and public spaces into smart spaces, which knit together many sensors and actuators to make our lives easier, simpler, and safer by the seamless provision of customized services. A smart space may adjust the temperature or light settings as per the liking of an individual currently using the space (e.g., smart home), or restrict the access to risky home appliances (e.g., oven) for the children or elderly people. It may also restrict the access to a designated place only to a few individuals (e.g., record rooms in a smart office) [3]. To enable the seamless provision of such services, it is a prerequisite to establish the identity of the person currently using the space. This illustrates that there are three broad scenarios that require mechanism(s) to authenticate the users: personal devices, online services, and smart spaces, as depicted in Figure 1.

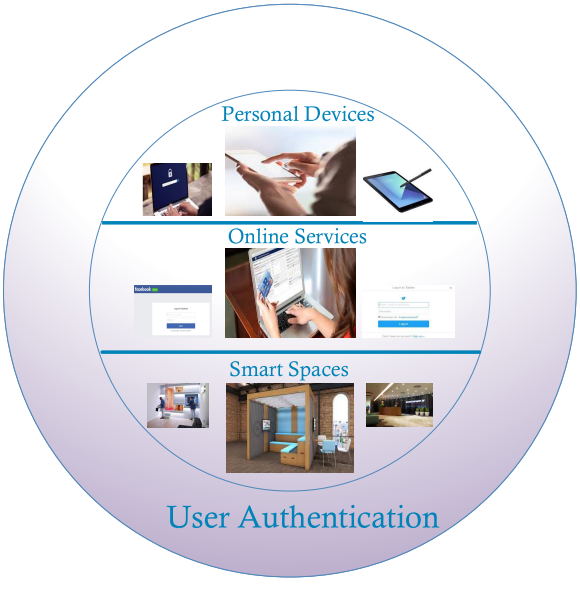

FIGURE 1. User authentication - Possible use cases.

Over the past few decades, several mechanisms have been proposed targeting the aforementioned use cases.

The associate editor coordinating the review of this manuscript and approving it for publication was Junggab Son.

These mechanisms are categorized into three main categories based upon the underlying factors of authentication - i.e., i) *Knowledge-Factor (something you know)*, ii) *Inherence-Factor (something you are)*, and iii) *Possession-Factor (something you have)*. The first category of authentication - i.e., *knowledge-factor*, requires the user to answer some question(s), assuming that only the valid user knows the correct answer. The most widely used instantiation of this authentication factor is the use of passwords and Personal Identification Numbers (PINs). However, this widely used mechanism is known to have several associated vulnerabilities. For example, users tend to use very simple passwords like ''12345''or ''abc123'', and hence are easy to guess [4], [5]. There are several lists published online that compile the most widely used passwords which can be exploited by the hackers to facilitate the popular brute force attack. The brute force scripts have shown success with both encrypted and decrypted passwords [6]. The success rate of brute force attack has lately declined to 10% due to the usage of strong passwords. However, well crafted passwords are also prone to hacking through a number of well know techniques like social engineering, key-logging, remote-administrative tools, malware (Trojan Horses), and packet sniffing, etc [7]. In addition, the authors in [8] demonstrated that the channel frequency response of WiFi signals can be used to infer the passwords of sensitive online services (e.g., Alipay - the world's largest mobile payment platform). Likewise, [9] showed that the keystroke acoustics can also be exploited for cracking passwords. Password databases are also known to be leaked frequently. For example, [10] found that a major breach leaked more than 21 million passwords. Furthermore, the recent statistics show that a single user can has up to 130 online accounts [11], making it difficult to have a strong and unique password for every account. Although the password managers such as OneLogin and LastPass, seem to have resolved this issue, they (i.e., password managers) themselves can get compromised [12]. Moreover, the users tend to replicate the same password across a number of different accounts [11]. A single comprised account thus makes all others susceptible as well. It is conspicuous that, some of the aforementioned problems are tied to the user's bad habits (e.g., password replication and use of simple passwords), and a number of studies also point that many users often consider authentication to be an onerous process [13]–[16]. Secret pattern for authenticating the users on mobile phones is also an instantiation of knowledge-factor, since it is assumed that only the valid user know the authentication pattern (like password or PIN). Studies show that the secret patterns are also not safe, as they leave an oily smudge on the screen, making it possible for an adversary to retrieve the pattern by using a high resolution imagery [17]. Additionally, the authors in [18] demonstrated that the unlock-patterns can be snooped by transforming the mobile phone into an active sonar. The second category of authentication - i.e., *Inherence-Factor*, generally relies upon physical or behavioral biometrics. The physical biometrics are based upon the physical traits of the person (e.g., fingerprint), while the behavioral biometrics aim to establish the subject's identity by identifying unique patterns (or features) that are manifested in an individual's activities. (e.g., gait-pattern, i.e., the way in which a person walks). These mechanisms do not suffer from weaknesses associated with the use of passwords (e.g., they can't be guessed like a weak password). The inherence-factor based authentication generally requires an enrollment procedure, in which the user provides the multiple samples of his physical (e.g., fingerprint) or behavioral (e.g., gait-pattern) trait. Once these samples are collected, the authentication algorithm extracts and stores some features from them for making an authentication decision. During the authentication phase, the user provides a sample of same inherence trait (e.g., fingerprint), from which the same features are extracted (as in enrollment), and compared with the features captured a priori during the enrollment. The most widely used physical biometrics include fingerprint and face-recognition. The fingerprint based mechanisms work by capturing the user's fingerprint using a sensor and then establishes the user's identity by extracting some scrupulous features from the captured fingerprint. The extracted features are compared with the features captured a priori during the enrollment, where person is required to provide the multiple samples of his fingerprint. Recently, face-recognition is also being used extensively. These mechanism utilize a camera to capture the person's face photograph, and then the user-specific facial features are extracted to perform the authentication by comparing these features with ones collected during the enrollment, where user provides multiple images of his face to enable the facial-image based authentication. The problem with these mechanisms is that, they are also not difficult to circumvent. For example, fingerprint based mechanisms can be subverted by simply collecting the victim's fingerprint from any service that he may have touched [19]. Likewise, facial-recognition can be fooled by using the victim's photograph which can be found over the Internet by a simple social media search [20]. Behavioral biometrics (e.g., gait-patterns) is a relatively new concept, which has lately been realized through the availability of numerous sensors on personal smart devices (e.g., motion sensors on smart phones and watches). We present a detailed description of such mechanisms in Section III. A widely anticipated problem with inherence-factor is that, unlike passwords (or knowledge-factor), these mechanisms have no recourse if compromised. For example, if an attacker crafts a dummy finger of the victim by collecting his fingerprint from any surface he may have touched, then these fingerprints may be perilous to use in future for any purpose. The third category of user authentication - i.e., *possession-factor* relies on some form of hardware to be possessed by the legitimate user. The authentication is successful only if user through certain mechanism confirms the possession of that physical hardware. A widely used instantiation is RFID swipe cards used to restrict entry to secure places. Another example is the security token, which is a hardware device to gain access to an online service (e.g., online bank account).

These security token generate a dynamic One Time Password (OTP), which is only valid for a single login session (or for a certain period of time, e.g., 2 mins) and expires afterwards. However, the need to carry a specific device not only makes it burdensome for the user but also incurs an extra cost for the service provider. Since, nowadays, users carry mobile phones all time, the dedicated hardware used for generating OTP is being replaced by the mobile phones, which either receives an OTP thorough SMS or has an application installed which generates the OTP. OTP sent through SMS can be intercepted [21], while the OTP generation through an app requires user interaction to copy the OTP (or user confirmation for login) which is one of the constraints in wider adoption of this approach [22].

In light of the aforementioned vulnerabilities of almost all of the traditional authentication mechanisms (e.g., passwords, fingerprints, and hardware tokens), researchers have proposed numerous new ways to authenticate the user. In this paper, we present a succinct overview of the new research in this area and discuss their applicability across different use cases (i.e., personal devices, online accounts, and smart spaces). We group these methods as per the authentication factor employed, namely, *knowledge, inherence,* and *possession* factor.

Multi-Factor Authentication (MFA) - i.e., the combination of two or more authentication-factors, is being increasingly advocated by the experts for securing online services. Merging multiple factors into an authentication mechanism makes it more resilient to attacks, as if one of the factors is compromised, other(s) is still in place to thwart an attacker. The typical instantiation of MFA is referred to as Two-Factor Authentication (2FA), which combines any two from the knowledge, inherence, and possession factors. All of the mechanisms discussed so far authenticate the user only at one instance - i.e., when the access is required. However, once an access is granted, there is generally no mechanism in place that ascertains whether the actual user is still in control of the device or not [23]. For example, if a victim's mobile phone is stolen, and an adversary somehow succeeds in guessing the PIN, the important private content stored on such a device will be exposed, which potentially can lead to severe consequences. In order to protect the user's private data under such circumstances, an approach that is widely advocated is referred to as *continuous authentication*, which attempts to authenticate the user periodically after the log-in [23]. Most of the continuous authentication mechanisms generally rely on the behavioral inherence-factor, and we thus present this approach under the inherence-factor (see Section III). Note that the terms continuous, active, transparent, and implicit authentication are used interchangeably in the literature.

The rest of the paper is organized as follows. Section II presents the newly proposed authentication mechanisms based upon the Knowledge-Factor (i.e., something you know). Section III expands on the mechanisms based upon the Inherence-Factor (i.e., something you are). Authentication mechanisms based upon the Possession-Factor (i.e., something you have) are discussed in Section IV. Section V presents the commercial MFA systems. Comparison of different approaches across all the usage scenarios is done in Section VI, a concluding discussion appears in Section VII.

II. AUTHENTICATION MECHANISM BASED UPON THE KNOWLEDGE-FACTOR

Recall from Section I that the traditional knowledge-factor based authentication mechanisms like passwords, PINs, and secret patterns have been repeatedly shown to be vulnerable to circumvention. In view of this, researchers have proposed a number of other mechanisms that rely on the knowledge-factor (i.e., something you know). Table 1 presents the summary of such mechanisms. Authors in [24] presented an alternative mechanism which focuses on the episodic memories with a spatio-temporal context to generate the location-based authentication questions. This work requires the user to select some pre-defined locations during the enrollment and, for authentication he is required to select the corresponding (i.e., asked) location on the map (not entered as a text or selected from multiple options). Any location within the 30m of the actual answer is considered correct. Evaluations reveal that the users have a good recall rate for these questions as the maps (for answering the questions) can be conducive to recall the answers. In addition, this approach shows a reasonable resilience against both close adversaries (i.e., partners, friends) and strangers. As expected, this approach has a high authentication time (up to 232s in some cases), which may be strenuous for the users. Likewise, authors in [25] also proposed a similar approach, where the user selects a location as a password and, during authentication, he is required to select the corresponding location on the map. Authors in [26] used the questions based upon the digital memories of the user for authentication (e.g., which year given picture was taken?). Whenever the user requests access to the online service, the Service Provider (SP) prompts Digital Memory Authentication Service (DMAS) to generate a challenge to authenticate the user. The challenge question is based upon the user's digital memories, e.g., *which year given picture was taken?* If the user provides the correct answer, DMAS informs SP to provide access to the user. Otherwise, access is denied. However, we anticipate that this information (i.e., digital memories) may not be difficult to obtain from a simple social media search as the people often share this information over the social networks. Many works have proposed to monitor the user's activities on the mobile phone (e.g., calls, SMS, locations, etc) and make a questionnaire from this data to use for the authentication (e.g., whom did you make the first call today? or, where you have been to?). Since the user's activity on the mobile phone is dynamic (i.e., call/SMS logs and location information change with the time), the authentication questions change over the time, making it harder for an adversary to accurately answer the ever-changing questions. Leveraging this idea, researchers

TABLE 1. Summary of knowledge-factor-based authentication mechanisms.

Reference	For	Attributes Used	Performance
A. Hang et al., [24]	Online Accounts	Pre-defined Location Questions	Accuracy = 91%
J. Thrope et al., [25]	Online Accounts	Location Questions	Accuracy = 97%
N. Shone et al., [26]	Online Accounts	Digital Memories	Attack Resilience
Y. Albayram et al., [27]	Online Accounts	Location information using smart phones	Accuracy = 83%
P. Gupta et al., [28]	Mobile Phones	Calls, SMS, Email, Calender and Applications usage data	FPR and FNR = 15%
S. Das et al., [29]	Mobile Phones	Calls, SMS, Browsing and App usage data	User Memorability= 64%, Accuracy improves with Bayesian Modeling
S. K. Dandapat et al., [30]	Mobile Phones	Calls, SMS, Web,Facebook and Audio data	Recall Rate = 86% Guessabiity = 14%
H. Sun et al., [31]	Mobile Phones	Apps installed on the phone	Accuracy = 95%
A. Hang et al., [32]	Mobile Phones	Calls, SMS, App, Photo and Music data	Accuracy = 95.5%

have presented numerous authentication mechanisms. For example, authors in [27] used the questions regarding the location of the user (i.e., where the user has been to?). To achieve this, the user's mobile phone periodically records the beacons of WiFi APs and uploads them to the authentication server (when the connection is available). MAC address of each AP is used to map the WiFi fingerprint to a specific location using the Geo Maps Geo-location API. Using the location information, questions are generated by splitting the entire day into different windows of 15 minutes. A Bayesian Classifier is used to account for the recall capabilities of the user and make the authentication decision by requiring the user to not answer all questions correctly but consistently. As this mechanism relies upon a series of questions, a high authentication time may limit its usability. Authors in [28] proposed to create a memorable fingerprint by using the raw cell phone data (i.e., SMS, calls, emails, calendar, and app usage). They crafted questions from the collected data and analyzed whether the close relatives (e.g., partners) and acquaintances (e.g., friends) can answer these questions. Analysis revealed that, out of four possible types of questions - i.e., *who* (who do you call the most?), *what* (what app do you use in morning?), *when*(when do you call Bob?), and *where* (where do you usually charge your phone?), intimates (e.g., partners) can easily answer the *'when'* and *'where'* questions with high accuracy. Evaluations show a high False Negative Rate (FNR, 15%) which may not be suitable for scenarios where frequent authentication is required, e.g., unlocking the mobile phone. In addition, this mechanism also suffers from the power drainage issue and has a high authentication time (around 9 secs for a single question). Thus, this approach may also suffer from the usability issues, since the users often consider the authentication to be onerous (see Section I for this discussion). Similarly, the authors in [29] also used the autobiographical data captured by the cell phone (i.e., calls, SMS, browsing and app usage data) for authentication purpose. This work found that, as the mobile phones capture a lot of data, users make high systematic errors in answering questions regarding their activity on the cell phones ($\approx$ 36% *errors*). However, the analysis against different types of adversaries (e.g., naive, observing and empirical adversaries, etc) reveals that, by using the Bayesian modeling on response errors for a series of questions, a confidence rating can be computed to decide whether the attempting user is legitimate or an adversary. Although a series of five questions improves the performance, this approach requires around two minutes to complete the authentication process, which is approximately 10$\times$ greater than a standard PIN-based authentication. Likewise, authors in [30] also used a similar approach to authenticate the users and found that, recent non-frequent activities (i.e., calls, SMS, web, audio and Facebook data of past 3 days) have a better recall rate for the actual user and a low guessability for an adversary (i.e., partners, close friends). They further found that a single question is not sufficient for the authentication and, a reliable system requires at least three questions. The analysis also revealed that the binary questions (*yes/no*) are easy to guess (by an adversary), while the text-based questions without any hint (e.g., who did you call at 12 pm?, with no options) are difficult to recall for the valid user. Authors in [31] generated the authentication questions regarding the *apps* installed on the mobile phone. For successful authentication, the user must select the 4 apps installed on his device from a selection panel of 16 apps, out of which only 4 are installed on the user's phone. Rest of the 12 apps are selected from the app store with a similar rating and category to that of the apps installed on the user's device (i.e., game, social networking, etc). Evaluations show a reasonable accuracy (95%) and resilience to guessing and shoulder surfing attacks with a log-in time of around 7 secs (comparable to password-based authentication). Likewise, authors in [32] used the questions generated from the calls, SMS, app usage/installation, photo, and music data. This study also shows that app usage and installation data offers a reasonable trade-off between the usability and security. Analysis reveals that app-based questions related to the recent past (e.g., past one week) are more confidently answered by the user. Furthermore, in the usability study of this work, users raised the privacy concerns about the photo-based questions and expressed the memorability issues about the music-based questions.

While the idea of creating questions from the user's activity on mobile phone is interesting and has shown promise in some cases, it is discernible that asking a series of questions may not be feasible for the situations where frequent authentication is required. For example, it may be infeasible to unlock the mobile phone which is done approximately 80 times/day by an average iPhone user [33]. However, this approach may be utilized as a fallback authentication for online services, i.e., where the user forgets his password and may need a secondary mechanism to confirm his identity. The fallback authentication is generally not required frequently, and the traditional mechanisms ask some pre-defined questions, like, pet or best-friend name, which are easy to find over the Internet. Sometimes, if a user forgets his password of an online service and wants to reset the password, a reset link is directly sent to his email. A potential adversary who has already got access to the victim's email (e.g., through leaked password) can thus sneak into several other online services with no difficulty. The questions generated from the user's activity on the mobile phone might be helpful in the aforementioned scenario. For this purpose, the collected data (i.e., calls, SMS, location, etc) needs to be uploaded to the authentication server (as done in [27]), and upon a request to reset the password (e.g., if the user forgets his password), questions from the uploaded data can be used to verify the legitimacy of the user. However, an anticipated problem with this approach, which could be precarious, is that it requires a continuous monitoring of user's activity on the mobile phone which may lead to battery drainage problems.

Knowledge-factor is also used for authenticating the user attempting to access the IoT devices in a smart environment. In practice, the user establishes his identity by providing a password or a PIN through an application installed on his mobile phone for accessing the IoT devices used for enabling the smart home operations (e.g., turning lights on or off remotely). For example, [34], [35] proposed mechanisms that utilize password for authenticating the user attempting to access the devices connected in a smart space. However, the problems associated with the passwords are well documented in the literature (as discussed in Section I). Similarly, the knowledge-factor is also used for restricting entry to the designated areas in a smart space. For example, [36], [37] are the smart locks that can be unlocked by a PIN and offer the convenience of key-less entry to a secure place.

III. AUTHENTICATION MECHANISM BASED UPON THE INHERENCE-FACTOR

Recall from Section I that the traditional physical biometrics (i.e., fingerprint and face-recognition) are known to be vulnerable to subversion. In view of the problems described in Section I, researchers have not only sought to address the vulnerabilities of traditional mechanisms, but have also proposed numerous other physical and behavioral biometrics to authenticate the user. Table 2 presents the summary of such mechanisms. For example, a number of works have attempted to perform the liveness detection for fingerprints - i.e., a procedure that ascertains whether the finger is live or an artificial replica. The approaches for liveness detection can be divided into two categories, namely, hardware and software solutions. The hardware solutions require an additional sensor to detect some characteristics like arterial oxygen saturation of hemoglobin [38] or skin conductivity [39], to identify a fake finger. These (hardware) solutions are not only expensive, but they may also be spoofed. For example, the oximeter based technique may be deceived by using a translucent dummy finger, and the conductivity based approach may be fooled by using saliva on the silicon artificial fingerprint [40]. In software-based solutions, some features are extracted from the fingerprint which helps in discriminating a live finger from an artificial dummy. For example, [41] used the Laplacian operator to obtain the image gradient values and demonstrated its feasibility for liveness detection using the back-propagation neural network. Likewise, authors in [42] presented a local descriptor referred to as Weber local binary descriptor, which leverages the intensity-variance and orientation features to distinguish a live finger from the artificial replicas. However, the performance of software-based solutions often lacks consistency across the fingerprints captured with different hardware (sensors) [41], which may be a deterrent in real-world deployment. We refer readers to [43] for a detailed discussion of the liveness detection and related issues. As described earlier, the facial-recognition may also be spoofed by using the victim's facial-photograph, which can easily be found over the social media. The recently introduced facial-recognition leverages the 3D camera technology which computes the distance of different parts of face from the camera view-point (e.g., on LG G7 and iPhone X [44]). This approach is resilient to image-based spoofing. However, [45], [46] have demonstrated that this approach can also be deceived by using a 3D-printed head of the victim. A number of works have explored some other physical traits and demonstrated their feasibility for user authentication. For example, [47] proposed an iris-based authentication mechanism (for Samsung Galaxy S8), where the unique features are extracted from the iris of the person's eye by exploiting an iris scanner. However, this mechanism can also be deceived by using the victim's image superimposed with a contact lens [48]. Hackers in [48] have demonstrated that it is possible to even capture the victim's image furtively from a distance of 5m, and use it to circumvent the iris scan. Since the iris-scan works through the infrared illumination on eyes from a short distance ($\approx$ 30cm), numerous users have reported eye's discomfort while using them [49], which might lead to more severe eye-health issues. Authors in [50] proposed to use the depth sensor (which is increasingly appearing on the smart phones) to extract vein patterns from the person's hand dorsum and use them for authentication. The vein patterns are user-specific and do not change appreciably unless subjected to a major surgery [50]. In addition, veins offer numerous benefits over the other counterparts like fingerprint and face-recognition. For example, the veins are located underneath the skin, they are unlikely to leave

TABLE 2. Summary of inherence-factor-based authentication mechanisms.

Reference	For	Attributes Used	Performance
T. V. Puttee et al., [39]	Mobile Phone / Access Control	Fingerprint - Liveness detection (Using Skin Conductance)	Vulnerable to Spoofing
M.SandstrÃĎom [38]	Mobile Phone / Access Control	Fingerprint - Liveness detection (Using oximeter)	Vulnerable to Spoofing
C. Yuan et al., [41]	Mobile Phone / Access Control	Fingerprint - Liveness Detection (Software Solution)	True Ratio = 98%
X. Zia et al., [42]	Mobile Phone / Access Control	Fingerprint - Liveness Detection (Software Solution)	ACE = 4 - 25%
M. Staff et al., [44]	Mobile Phone	3D Facial Data	Vulnerable to Spoofing
Samsung [47]	Mobile Phone	Iris	Vulnerable to Spoofing
H. Zhong et al., [50]	Mobile Phone	Vein Patterns	Precision = 98%
J. Chauhan et al., [52]	Mobile Phone	Breathing Sound	Accuracy = 94%
NEC [53]	Mobile Devices with Earphone Connectivity	Ear Canal Shape	NA
A. Fahimi et al., [54] [53]	Mobile Devices (in call interaction)	Ear Shape and Texture	Accuracy = 92.5%
X. Zhang et al., [55]	NA	EEG Signal	Accuracy = 98%
I. Martinovic et al., [56]	NA	Body Pulse-Response	Accuracy = 88%
Y. Chen et al., [58]	Mobile Phones	Taps/Slides	TPR= 99% for tap gesture, 96% for slide gesture
N. Zheng et al., [57]	Mobile Phone	Taps while entering the PIN	EER = 7.3% for 4 digit PIN, 4.5% for 8 digit PIN
J. Sun et al., [59]	Mobile Phones	Arbitrary curve any where on screen	TPR = 99%
T. Feng et al., [60]	Mobile Phone (Continuous Authentication)	Touch, Motion and Speech data	Unauthorized Access detection = 90%
C. Bo et al., [61]	Mobile Phone (Continuous Authentication)	Tap, Fling, Scroll and Motion data	FAR= 1%
N. Neverova et al., [62]	Mobile Phone (Continuous Authentication)	Motion Data	EER=8.8%
L. Fridman et al., [63]	Mobile Phone	Text, App, Browsing and Location data	EER=0.01%
K. Kumar et al., [64]	Smartwatch/Phone	Arm motion pattern	Accuracy=85%
Y. Yang et al., [65]	Smartwatch/Phone	Arm rotation and movement	EER=3.8%
S. Davidson et al., [30]	Smartwatch/Phone	Walk, open a door, type, lift a cup and check wrist watch	TP=99%
S. Li et al., [66]	Smart Glasses	Head movement	FAR=15.8%
T. Alpcan et al., [67]	Online Accounts	Touch-pad data in response to Signature-gesture	NA
S. W. Shah et al., [68]	Online Accounts	WiFi perturbations in response to Signature-gesture	Accuracy= 79%
S. W. Shah et al., [69]	Online Accounts	WiFi perturbations due to typing	Accuracy= 92%
L. Middelton et al., [70]	Smart Space	Gait-data captured using floor-sensors	Success Rate = 80%
J. Cheng et al., [71]	Smart Space	Foot-size and Pressure exerted on floor-sensors	Accuracy=88%
H. Kim et al., [72]	Smart Space	Foot-shape and Pressure data (using floor-sensors)	Accuracy = 99%
A S Guinea et al., [73]	Smart Space	Hand and Arm motion data	Accuracy = 88%
X. Wang et al., [74]	Smart Space	Hand Gestures recorded using Kinect	Accuracy = 99%
J. Zhang et al., [75]	Smart Space	Gait-Pattern manifested in WiFi Signals	Accuracy = 77%
W. Wang et al., [76]	Smart Space	Gait-Pattern manifested in WiFi Signals	Accuracy = 79%
Y. Zeng et al., [77]	Smart Space	Gait-Pattern manifested in WiFi Signals	Accuracy = 80 %
C. Shi et al., [3]	Smart Space	Gait-Pattern manifested in WiFi signals	Accuracy = 91%

any imprint on a surface that a victim may have touched (unlike fingerprints). Likewise, they are generally not available over the social media (unlike facial photographs). However, the hackers in [51] have demonstrated that it is possible to craft a replica of vein patterns by leveraging the modified SLR camera with the infrared filter removed to record the vein pattern and relaying it on a wax mock-up. In [52], authors proposed to use the breathing sound of the person for authentication. This mechanism requires user to perform a breathing gesture (i.e., sniff and deep breath) by placing the mobile phone very close to the nose. Microphone available on the mobile phone is used to record the sound and audio features are extracted to form a user-specific audio signature which can be used for the authentication. However, an anticipated deterrent in wider adoption of this approach could be the sound gesture which may be awkward to do in some situations (e.g., in presence of other individuals like friends, etc). Reference [53] presented a mechanism that authenticates the user by exploiting the person's ear canal shape. This mechanism requires the user to wear an earphone with microphone, and sends a sound signal in the ear canal and record the reflected sound (sound in both audible and inaudible range can be used). Since each user has a distinctive shape of the ear canal, the reflected sound shows

a discriminating frequency response for various users. However, the use of earphone for authentication may be onerous for the users. Likewise, authors in [54] proposed a mechanism for implicit user authentication on mobile phones by exploiting the shape of the person's ear. They leverage the shape and texture information of the ear to perform the authentication by taking an implicit ear image during a call interaction. This approach only seems suitable for the mentioned usage scenario (i.e., authentication during call interaction), and may be difficult to adapt under the typical authentication setting (i.e., to unlock a mobile device). In [55], authors presented an EEG (Electroencephalography)-based human identification system. This mechanism leverages the person's brainwave signals for authentication, and thus is difficult to spoof unlike fingerprints or face-recognition. However, this approach requires an assembly of electrodes to be placed on the user's head for capturing the EEG signals, making it infeasible for our usage scenarios - i.e., personal device, online services, and smart spaces. Authors in [56] presented a biometrics solution that authenticates the user by measuring the body response to an electric square pulse. Analysis show that human body shows a unique response to the pulse applied at the palm of one hand and measured on the other. However, we anticipate that passing an electric pulse from the human body may be agonizing for the users if they have any deep lacerations on the body. In light of the problems associated with the physical biometrics, researchers have explored behavioral biometrics as a potential alternate, which attempts to measure the user's unique behavioral characteristics while performing different activities to authenticate the user (e.g., how a person taps on the mobile phone? or, how a person walks?). For example, the authors in [57] proposed a mechanism that attempts to verify whether the correct password is being typed by the actual user or not. Since the users generally have a unique behavioral pattern to tap on the screen of a mobile phone, this mechanism exploits the touch and motion sensors available on the smart phone to seamlessly collect the touch pressure, time, size and motion data while the user is typing his PIN (4 or 8 digit). Once the data is collected, this mechanism extracts the features and compares them with the enrolled data of the user. Evaluations show a good accuracy for this approach. Similarly, authors in [58] proposed a system which requires user to select a familiar melody as a password and then inputs its rhythm by taping or sliding on the screen of mobile phone. In response to tap or slide gesture, finger pressure, touch size, touch coordinates, finger ID and time of touch is recorded by exploiting the available sensors. Since different users perform the tap/slide gestures differently, the extracted features from the collected data proves helpful in making an authentication decision by leveraging the machine-learning based classifier. Evaluations show that the tap gesture have a better performance than the slide gesture, while both the gestures show resilience against different type of attackers (i.e., those attackers who don't know about the rhythm/gesture and, those who have observed the user while performing the tap/slide gestures, etc). Likewise, the authors in [59] presented a system that requires the user to draw an arbitrary curve with a finger any where on the screen of mobile phone. In response to this gestures, different features are extracted by leveraging the data recorded using the sensors available on the mobile phone (i.e., touch pressure, size, velocity, etc). For making an authentication decision, dynamic time wrapping is used to compare the drawn curve with the enrolled curve. Evaluation show a high True Positive Rate (TPR) for this approach. As this approach allows users to draw the curve anywhere on the screen, it may be helpful for visually impaired people.

As the aforementioned mechanisms leverage the behavioral-biometrics to authenticate the user at only one instance - i.e., when access in required (e.g., for unlocking the mobile phone), a number of works have attempted to utilize the behavioral biometrics to enable the continuous authentication on mobile phones - i.e., confirming the user's identity periodically after the log-in. This can be helpful in securing the mobile phones against the opportunistic access where an adversary somehow succeeds in gaining access to an unlocked phone or steals the victim's phones and correctly guess the PIN and gain access to the private content stored on the mobile phone. For example, the authors in [60] leveraged the touch and motion sensors to decide whether the mobile phone has left the user's hand or not (i.e., the touch and motion sensor data changes if the actual user transfers device to the other hand or device is picked by an adversary). Once such an event is identified, this approach further computes the user-specific features from the touch (i.e., taps on screen) and speech (e.g., voice dialer, personal voice assistant) data to decide whether the mobile phone is being used by the actual user or by an adversary. Likewise, [61] also used the motion and touch sensors to capture the data corresponding to user's walking and tapping (on screen) behavior to enable the non-intrusive active authentication. Authors in [62] used deep-learning to extract the temporal features from the motion data (i.e., walking and arm motion) captured by exploiting the on-device accelerometer and gyroscope and subsequently used the computed features to enable the continuous authentication. Authors in [63] showed that users typing behavior (e.g., misspelling), app usage (e.g., number of times an app is used), web visits (e.g., number of times a particular url is visited) and location information (based upon GPS or WiFi) can be utilized to enable the active authentication. We refer readers to [23] for a more thorough discussion of continuous authentication on mobile devices.

Since users nowadays carry a number of other personal devices like smartwatches and glasses, a few works have exploited the sensors available on these devices to capture the user's unique arm or head motion data to perform the authentication. For example, the authors in [64] exploited the accelerometer available on the smartwatch to capture the arm motion data and extracted different features for implicit authentication. Evaluation show that the arm motion data (i.e., extracted features) is user-specific and results in an accurate authentication. Similarly, the authors in [65] showed

that the accelerometer and gyroscope on a smartwatch can be exploited to record the data corresponding to specific arm gestures and authenticate the user (i.e., rotating arm, moving arm upward/downward and making a circle with arm in air). Likewise, the authors in [78] showed that the accelerometer on smartwatch can be used to collect the data corresponding to user's daily activities like walking, opening a door, typing a pre-defined statement, lifting a cup, and checking the time on the wrist watch, which can then be used to authenticate the user. Evaluations show that the time and frequency domain features extracted form the accelerometer data can yield high accuracy. Authors in [66] presented a mechanism for authenticating the users of the head-worn devices (i.e., smart glasses). This mechanism records the user's unique head motion data in response to a specific audio stimulus by leveraging the accelerometer available on the smart glasses. The features are extracted from the accelerometer data and compared against those computed during the enrollment. Evaluations show the feasibility of this approach for authenticating the users of head-worn devices.

As the personal devices (smart-phones, watches, and glasses) are equipped with plenty of sensors, this has resulted in numerous authentication mechanisms for personal devices in recent years. A typical problem associated with the most sought after mode - i.e., continuous authentication is that, the user's behavioral data occasionally change under different circumstances (e.g., data may have different distributions during enrollment and testing). More research efforts are needed to have an in-depth analysis of behavioral biometrics in regard to this issue.

The physical biometrics is not a preferred choice for securing online services. Reason being that, they offer no recourse if compromised. As described above in Section I, users credentials stored online are frequently leaked. This makes it precarious to store the sensitive data like physical biometrics (e.g., fingerprint) in an online database, as a breach in this case will make the physical biometrics (e.g., fingerprint) unusable for any purpose in future. In addition, as online services can be accessed from a variety of devices, authentication mechanisms for such services thus can not simply rely upon sensors that may not be available on some devices. This limits the usability of behavioral biometrics for securing online services. For example, accelerometer and gyroscopes are extensively used to collect the user's behavioral data for authentication on mobile phones. However, these sensors (i.e., accelerometer and gyroscope, etc) are not available on some devices (e.g., laptop). An authentication mechanism for an online service that relies on these sensors will then not be feasible to access the online account from the devices which do not have these sensors. This is a deterrent in the wider utilization of behavioral-inherence-factor for user authentication for online services. However, a few works have utilized the behavioral biometrics for crafting the authentication mechanisms for the online accounts. For example, authors in [67] presented a mechanism which requires user to perform his signature with the finger on the touch-pad of the log-in device. As the way in which user moves his finger while performing his signature is highly user-specific, the corresponding data can thus be used for establishing the identity of the user. Different features (e.g., speed, velocity, shape etc) are extracted from the touch-pad data collected in response to the signature gesture and compared against the enrolled data. However, it is imaginable that, this mechanism will only work if the device from which the online account is being accessed has a touch pad. A number of devices from which online accounts are frequently accessed has no touch pad (e.g., mobile phone and tablets etc), which thus limits the wider usability of this mechanism. Likewise, the authors in [68] proposed to utilize the perturbations in WiFi signals in response to the user signature performed on a designated place (e.g., on touch pad) with a bare finger (without instrumenting with any sensors) and use these for user authentication for online services. Since user places and moves his hand in a specific manner while performing the signature gesture, this results in user-specific perturbations in the ubiquitous WiFi signals. Time and frequency domain features are extracted from the WiFi perturbations and compared against the enrolled features to make an authentication decision. Similarly, [69] proposed to use the WiFi perturbations due to the fingers and hand movements while typing the password for authenticating the user. As the users move his fingers in a specific formation while typing the password, this also results in user-specific variations in CSI of the received WiFi signals and thus can be used to authenticate the user. However, the radio signals based mechanisms are only suitable for accessing the online service from a fixed location. The reason is that, changing the position of the WiFi receiver (or AP) changes the multipath, which affects the performance of the authentication mechanism.

Inherence-factor is also being widely used for authenticating the users of the third use case - i.e., smart spaces. Since smart spaces aim at seamless provision of customized services to its inhabitant, establishing the identity of the person currently using the space is essentially required in an effortless manner. To achieve this, a number of researchers have proposed to embed sensors in the smart space (e.g., in floor) to collect the user's biometrics data (e.g., how a person walks), and use it for identification. For example, the authors in [70] proposed to integrate a grid of simple resistive sensors in the floor to capture the user's gait-pattern. They extracted three features from the sensor's data, i.e., stride length, gait-period and heel-toe ratio and demonstrated their feasibility for the user recognition. In [71] authors demonstrated that a matrix of low precision pressure sensors embedded in the floor can be used to identify the person by computing the person's foot size and pressure exerted on the sensors while performing the daily activities like opening/closing doors. Likewise, the authors in [72] proposed a network of specially designed sensor mats that may be used in a smart space to record the foot-size and exerted pressure to recognize the user. In [74], the authors leveraged the Kinect to record different hand gestures of the user (e.g., move up, down,

make circle an draw letters etc) and used this data to perform the user recognition by utilizing the dynamic time wrapping to compute similarity with the enrolled data. Since all of the aforementioned systems rely on the special sensors integrated in the smart environment, cost of their deployment can be a deterrent in their wider adoption. In [73], the authors proposed to use smartwatch (which is being increasingly possessed by the occupants of smart spaces) to capture the arm motion data by leveraging the on-device Inertial Measurement Unit (IMU). This work shows that the IMU data can be used to continuously identify an individual from the daily activities without requiring to undertake a specific gesture. In addition, the smartwatches can be interfaced with a smart environment to provide the person's identity information for enabling different operations in a smart space (e.g., temperature adjustments). Many researchers have leveraged the ubiquitous WiFi signals for the seamless human identification in smart environments [3], [75]–[77]. Researchers have demonstrated that the fine grained Channel State Information CSI) of the pervasive WiFi signals can capture the impact of different activities of people (e.g., walking [75]–[77] or stationary activities like opening refrigerator etc [3]) and a scrupulous extraction of appropriate features can help in human identification. Since most of the devices in smart spaces are WiFi enabled by default (e.g., smart TV or refrigerator), they can be utilized to deploy the approaches in [3], [75]–[77] by a simple software extension, without requiring any specialized sensors as in [70]–[72]. However, these mechanisms suffer from a limitation, i.e., they work in a controlled environment where only the authenticating individual is present in the vicinity of WiFi transmitter and receiver. Further research is needed to expand these works so that they can identify a person in the presence of other people and activities in smart space.

IV. AUTHENTICATION MECHANISM BASED UPON THE POSSESSION-FACTOR

As discussed in Section I, these mechanisms require the user to possess (and produce) some form of hardware for successful authentication. RFID cards and key fobs used to control access to a restricted area are the widely used instantiations of this authentication-factor. In addition, this approach is often used to secure online services. As described above, there are relatively less options available to craft authentication mechanisms for online services (i.e, less options to exploit inherence-factor and, recent trends in knowledge-factor has a high authentication time and they may be answered by the family members and friends). In addition, online services are more prone to hacking (i.e., as they can be accessed over the Internet) than the personal devices (i.e., they are generally in possession of the user), and a malicious access can result in severe consequences like loss of money (e.g., in case of an online bank account). In order to have a secure authentication mechanism for online services, the research community is increasingly advocating the Two-Factor Authentication (*2FA*), that generally combines any two from *something you know, something you are,* and *something you have*. In most of the 2FA mechanisms the first- factor is password (i.e., something you know), as it is widespread and having an alternative is difficult. The *second-factor* in most cases is based upon the *possession* of a certain hardware device (i.e., something you have). The possession-factor based mechanisms (as a second authentication-factor) generally rely on either hardware or software tokens that generate (or receive) the One Time Password (OTP). For example, [84] and [85] are the hardware token based solutions, which require the user to possess a specific hardware associated to his online account, that produce an OTP for a successful authentication. However, as described above in Section I, the problem associated with this mechanism is that, it incurs an extra cost for the service provider, and also requires users to carry a dedicated hardware at all the times, which may be arduous for the users. Software tokens generally rely on the pervasiveness of the user's mobile phone to receive the OTP sent by the service provider (e.g., OTPs for Gmail accounts). As the users already carry their mobile phones all the time, this approach eliminates the need of an additional hardware for generation of security token (e.g., as in [85]). However, this approach is susceptible to interception [21]. An alternative method is to have the 2FA application installed on the mobile phone that can generate the security token (e.g., Google Authenticator app). Although this approach curtails the problem of SMS interception, it still requires user to interact with the mobile phones to copy the generated OTP (or to confirm the login). Authors in [22] found that the additional user interaction required for establishing the possession of secondary device is a serious deterrent in wider adoption of 2FA mechanisms. There are a number of other approaches that rely on the user's mobile phones and extract some form of information for establishing the possession-factor which subsequently helps in user authentication. For example, authors in [79] proposed a mechanism that utilizes the GPS available on the user's pre-registered mobile phone to access the location information. Whenever user wants to access the online service, the user's pre-registered mobile phone is triggered to access the location and send to the authentication server. The location information is compared against the range of locations pre-registered by the user during the registration phase. Authentication is unsuccessful if the user does not possess his pre-registered mobile phone or is not present at a registered place. Likewise, authors in [80] also leveraged the user's pre-registered mobile phone to access the location information for enabling the 2FA. For authentication, the service provides requests a security token from the user, which is generated by performing the hash function of the location, time-stamp, and a pre-shared number. Once the server has obtained the token, it compares it (token) against the locally generated token which is computed by performing the hash on the same pre-shared number and location/ time-stamp obtained from the GPS server, to which the user's registered mobile-phone also sends the location and time information. Authentication is successful only if both the tokens are same, helping to

TABLE 3. Summary of possession-factor-based authentication mechanisms.

Reference	For	Attributes Used	Performance
F. Zhang et al., [79]	Online Accounts	Location-information accessed Using Smartphone	NA
U. A. Abdurrahman et al., [80]	Online Accounts	Security-Token generated using Location, Time-stamp and a pre-shared number	NA
N. Karapanos et al., [81]	Online Accounts	Ambient Sound (for establishing possession-factor)	FRR = 0.3%
J. Zhang et al., [82]	Online Accounts	Ambient Sound (for establishing possession-factor)	Success Rate = 99%
Syed W. Shah et al., [83]	Online Accounts	Channe State Information (CSI) - for establishing possession-factor	Accuracy= 94%

thwart the Man-in-the-middle attack. It is conspicuous that the access to online service is only possible if the user is in possession of his pre-registered phone. Authors in [81] also proposed a 2FA mechanism that requires the user's pre-registered mobile phone to be placed in close proximity of the device from which user is attempting log-in. Both the mobile phone and the log-in device record the ambient sound and authentication is successful only if the both the devices record a similar sound. A similar sound recorded by both the devices confirms that the user attempting to login to the online account is in possession of the pre-registered mobile phone and hence is deemed to be the legitimate user. Likewise, authors in [82] proposed a similar 2FA mechanism that computes the similarity between ambient sound recorded by the login device and user's pre-registered mobile phone. In addition, it also authenticate the user's mobile phone by using a Physical Unclonable Function (PUF). An anticipated problem with this (i.e., ambient sound) approach is that, an attacker in close vicinity of the victim can by-pass this mode of authentication. Authors in [83] proposed to use the Channel State Information (CSI) recorded by two devices in close vicinity (i.e., user's pre-registered mobile phone and log-in device) for establishing the possession of user's pre-registered mobile as 2FA. Because the CSI (of WiFi) recorded by two nearby devices is similar, it can be used to check if two devices are in vicinity of each other or not, which thus can be used to determine whether the account is being assessed by the legitimate user who is in the possession of his pre-registered mobile phone or by a potential adversary.

Possession-factor is also being utilized for restricting entry to a designated area or accessing IoT devices in a smart environment. For example, [86], [87] are the smart locks that operate by detecting the user's paired mobile phone (over Bluetooth) in the close vicinity and offers the convenience of automated lock/unlock operations. In addition, they ([86]) also offer key fobs for their operations rather than relying on user's mobile phone. However, [88] demonstrated a possible way to hack such locks. Similarly, the user's personal mobile phone is also used for accessing the devices connected in a smart space (e.g., Hue Philips), assuming that a request to access a device using the user's mobile phone establishes the identity of the actual user.

Possession-factor is also recently utilized for unlocking the personal devices. For example, [89] allows user to automatically unlock his laptop when he is wearing his paired smart watch. However, it requires both Bluetooth and WiFi to sense the watch and compute the proximity from the laptop, respectively, which may be onerous in certain situations (e.g., when no WiFi is available). In addition, [90] conducted a successful Man-in-the-Middle attack on this protocol.

V. COMMERCIAL MULTI-FACTOR-AUTHENTICATION SYSTEMS

In this Section, we briefly present a discussion of different MFA solutions present in the market. For example, [84] is a hardware token that generates a unique 6 digit OTP every sixty seconds. For successful authentication, user needs to provide this code as a part of 2FA, which confirms that user is in possession of 2FA device linked to his account. Likewise, [85] is also a hardware solution that does not require user to copy the OTP as in [84]. Instead, for a successful authentication, user is required to connect the hardware device to the USB port of the primary device (i.e., the device from which login attempt is being made) as a part of 2FA, and by pressing the capacitive button provided on the hardware, a character string which implements OTP is emitted by the device. Similarly, [91] is also a hardware-token which is presented in form of a ring to be worn on the finger. As a part of 2FA, the user performs a specific gesture with the hand (upon which 2FA ring is worn) in front of the primary device, which (i.e., gesture's data) is then used as a second-factor of authentication. All of these solutions not only require user to carry a dedicated device all the time, but they also require an extra manufacturing cost. As a result, they are not widely used. Alternative cheaper options that leverage software tokens include Duo Push [92], Encap Security [93] and Google's two-step verification, wherein the OTP is sent to the user's registered mobile device following a successful login attempt. The dependence of these solutions on a secondary-device (i.e., mobile phone) can potentially lead to severe repercussions. For example, sharing of personal mobile phone number with numerous service providers can potentially allow spam. Similarly, one cannot access his account if the mobile phone (i.e., secondary device) is lost, stolen, or discharged. There are a few 2FA systems that are

TABLE 4. Comparison of authentication mechanisms for personal devices.

Factor	TPR	Attack Resilience	Usability	Know Issues	Ref
Knowledge	High	Vulnerable to subversion by partners, friends	Difficult	Long authentication time and power drainage	[28]- [32]
Inherence (Physical)	High	Shown to be vulnerable to subversion	Easy	No recourse if compromised	[44] [47] [50]
Inherence (Behavioral)	Moderate	Yes	Easy	Behavioral data changes in different circumstances	[57]- [65]
Possession	High	Vulnerable to MiTM attack	Easy	Needs both WiFi and Bluetooth Connection	[89]

TABLE 5. Comparison of authentication mechanisms for online services.

Factor	TPR	Attack Resilience	Usability	Know Issues	Ref
Knowledge	High	Moderate - May be deceived by partners, friends, etc.,	Difficult	Suitable only for fallback authentication	[24] - [27]
Inherence (Physical)	-	-	-	Not preferred for online services	-
Inherence (Behavioral)	Moderate	Yes	Easy	Works only in controlled settings	[67]- [69]
Possession	High	Yes	Difficult	Depends upon a secondary device	[79]- [83]

not dependent upon any secondary device like mobile phone. For example, [94] presents a solution that performs 2FA by recording the user's voice using the login device. A close adversary can surreptitiously record the victim's voice and launch a playback attack. Similarly, [95] is also not dependent upon any secondary device. However, this solution requires user to have two passwords for successful authentication (one as a first factor and other as a second factor). The second password (of 4 characters) needs to be drawn using the mouse as a part of 2FA. The user's behavioral characteristics while drawing the second password are extracted and used as 2FA (characteristics like length, height, width, speed, direction, angle and number of strokes while drawing second password are extracted). The requirement of a second password for 2FA can be onerous for the users.

VI. COMPARISON OF DIFFERENT AUTHENTICATION APPROACHES

In this Section, we compare the authentication mechanisms proposed across different usage scenarios. Table 4 presents the comparison of different approaches for personal devices. For personal devices, physical biometrics is the most popular solution since they are highly accurate and easy to use. However, most of the physical biometrics (e.g., fingerprint, facial-images, iris, and vein patterns) are shown to be vulnerable to subversion and offer no recourse once compromised. Table 5 shows the comparison of different approaches for online services. For online services, possession-factor (e.g., mobile phone for OTP reception) is increasingly used to confirm the identity of the user attempting to access an account. However, the dependence of this approach upon a secondary-device (i.e., mobile phone) can potentially lead to severe repercussions (e.g., online account can not be accessed if mobile phone is lost, stolen, or discharged). Table 5 present the comparisons of different approaches proposed to establish the identity of an individual currently using the smart space so as to enable different operations in the smart environment (e.g., seamless adjustments of temperature/light). The behavioral biometrics is the most preferred option for user-identification in smart spaces as this approach is non-intrusive and generally does not demand any explicit participation from the user (e.g., the user can be identified from his gait-pattern). However, the need to have specialized sensors (e.g., floor sensors) or the availability of a controlled setting (e.g., whereby only a single user is present near the radio transceivers) are the deterrents in wider adoption of such approaches.

VII. DISCUSSION AND CONCLUSION

This paper presents an overview of recent advances in user authentication for different usage scenarios - i.e., personal devices, online services, and smart spaces. We anticipate that this survey will help readers to obtain a comprehensive overview of the extensive literature to narrow down the future research directions. Since the inclusion of all the available literature is difficult, we present a representative subset of the available mechanisms for all the use cases. Although, the research community have adopted numerous ways to achieve secure authentication, the area still is active in view of many shortcomings of the available systems. We conclude this discussion by pointing out the possible future directions across different usage scenarios.

- *Knowledge-Factor:* As pointed out in Section II, the users typically make high systematic errors in answering the questions generated from the user's daily activity on the mobile phone (e.g., calls, SMS logs, etc). This is because the mobile phones collect a lot of data, which makes it difficult for the users to remember each activity. One of the possible alternatives could be to generate questions from the user's activities in the smart

TABLE 6. Comparison of authentication mechanisms for smart spaces.

Factor	TPR	Attack Resilience	Usability	Know Issues	Ref
Knowledge	High	Moderate - Passwords/PINs can be hacked	Easy	Known issues of Passwords/PINs	[34]- [37]
Inherence (Physical)	High	NA	Easy	Need specialized sensors integrated in the space	[71] [72]
Inherence (Behavioral)	Moderate	NA	Easy	Works for small smarts spaces only	[75]- [77]
Possession	High	Shown to be vulnerable to hacking ([88])	Easy	Depends upon a secondary device	[86], [87]

spaces *(e.g., when did you use the oven this morning?)*. Since the smart spaces also gather the user-specific data by default, this may be an appropriate option for authenticating the user. For example, Bluetooth Low-Energy beacons are often integrated in smart spaces that can be used to perform the precise indoor positioning of an individual (using the person's smartphone). The questions can be generated based on the person's indoor position. This data is likely to be much smaller than the activities on mobile phone (i.e., calls, SMS, location, social media, etc), which would be easy to remember. In addition, one can think of generating some context-aware questions that may be difficult to answer by close adversaries (such as partners and friends). This is a frailty in knowledge-based mechanisms that are presented in Section II - i.e., they are vulnerable to subversion by close adversaries. At home, for example, questions from the office-activities can be used that may be difficult for the partner to answer. Similarly, in an office environment, questions from the home-activities can be used that would be difficult for friends to answer.

- *Inherence-Factor:* The behavioral biometrics used for continuous authentication on mobile devices are largely dependent on simple, manually-engineered features extracted from the data captured by on-device sensors (e.g., accelerometers, gyroscopes, touch and pressure sensors, etc.) Since the behavioral biometrics collected at the time of enrollment may have different characteristics than the authentication data, such features may not perform optimally where enrollment and authentication takes place under significantly different conditions. This problem is often referred to as domain adaptation [96]. One approach that may be helpful under such circumstances is deep-learning. Since the users typically use their personal devices (e.g., mobile phones) continuously, the sensors can be implicitly used to perform non-invasive data collection, and then a deep-learning approach can be used for automatic extraction of features that may be a representative of user's overall behavioral pattern to achieve the authentication under different conditions and times.

  Some of the inherence-factor-based mechanisms proposed for smart spaces have limitations that restrict their wider usability. For example, the use of radio signals to seamlessly identify the people in smart space allows only a single person near WiFi transceivers. Further research is required to segregate the perturbations related to the authenticating user from the others that may be present nearby. One solution could be the use of Blind Source Separation (BSS) techniques, which can help isolate the WiFi perturbations of different users, and then identify multiple occupants occupying a space. Another approach that might be helpful is the use of 60 GHz WiFi to capture the human gait-patterns. 60GHz WiFi is becoming available for commercial use. Unlike prior works which have used 2.4GHz or 5GHz bands (e.g., [3], [77]), 60Hz WiFi has a wavelength in order of *mms*. We anticipate that these mmWaves may be able to capture the impact of different body parts while walking at much finer granularity (than 2.4GHz or 5GHz). This can be helpful in discriminating the perturbations that belong to the different users. Such enhancements may allow the wider use of radio signals to seamlessly identify the occupants of smart spaces.
- *Possession-Factor:* The possession-factor is increasingly used to secure the online services. However, most possession-factor solutions require a non-trivial user interaction (e.g., copying the OTP), which discourages broader adoption of these mechanisms. To improve the adoption rate of possession-factor mechanisms, it may be advantageous to have a mechanism that requires minimum participation on the user's part to confirm the possession of the secondary hardware device (e.g., mobile phone). One of the potential alternatives could be to use smartwatch as a possession-factor (instead of a mobile phone). Smartwatches are increasingly owned by the users and are equipped with numerous sensors that are not available on smartphones. For example, they are equipped with GSR sensors (Galvanic Skin Resistance) which can be used to determine whether the watch is on the wrist. Whenever the user wants access to an online service, the primary-device (i.e., the device from which a login attempt is being made) can connect to the user's paired smartwatch via Bluetooth as a part of 2FA (i.e., establishment of possession-factor). Once the connection is made, an algorithm on the watch can use the GSR sensor to confirm that the watch is

on the wrist (which generally is expected to be on the wrist). If not, user may be prompted to wear his paired smartwatch to access the online service. After confirmation, the distance between the watch and primary-device can be calculated using the Bluetooth RSSI, which is likely to be very less. Access may only be allowed if two devices (i.e., primary-device and smartwatch) are in close proximity to each other. This may also help thwart the close adversaries present in the immediate vicinity of the victim. The entire process can potentially be transparent to the user, and thus may help in curtailing the user's participation required for establishing the possession-factor in traditional mechanisms (e.g., copying OTP).

REFERENCES

[1] (2018). *Importance of User Authentication in Network Security—Seqrite*. [Online]. Available: https://blogs.seqrite.com/

[2] Craig Mathias. (2014). *Why Mobile User Authentication is More Important than Ever*. [Online]. Available: https://searchmobilecomputing.techtarget.com/

[3] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT," in *Proc. MobiHoc*, 2017, Art. no. 5.

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

[5] A. Vance. (2010). *If Your Password is 12345, Just Make it HackMe*. [Online]. Available: http://www.nytimes.com/

[6] H. League. (2018). *What is Brute Force Attack?* [Online]. Available: https://medium.com/

[7] Mahesh. (2019). *How Hackers Hack Your Accounts and Passwords and Ways to Avoid Being Compromised*. [Online]. Available: https://www.shoutmeloud.com/

[8] M. Li, Y. Meng, J. Liu, H. Zhu, X. Liang, Y. Liu, and N. Ruan, "When CSI meets public WiFi: Inferring your mobile phone password via WiFi signals," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2016, pp. 1068–1079. [Online]. Available: http://doi.acm.org/10.1145/2976749.2978397

[9] A. Kelly, "Cracking passwords using keyboard acoustics and language modeling," M.S. thesis, School Inform., Univ. Edinburgh, Edinburgh, U.K., 2010.

[10] A. Ng. (2019). *Massive Breach Leaks 773 Million Email Addresses, 21 Million Passwords*. [Online]. Available: https://www.cnet.com/

[11] N. Lord. (2018). *Uncovering Password Habits: Are Users' Password Security Habits Improving? Infographic*. [Online]. Available: https://digitalguardian.com/

[12] M. Tullock. (2018). *Do Password Managers Keep You Secure—Or Give You a False Sense of Security?* [Online]. Available: http://techgenix.com/

[13] D. Tapellini. (2014). *Smart Phone Thefts Rose to 3.1 Million in 2013: Industry Solution Falls Short, While Legislative Efforts to Curb Theft Continue*. [Online]. Available: http://www.consumerreports.org

[14] H. Khan, U. Hengartner, and D. Vogel, "Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying," in *Proc. SOUPS*, 2015, pp. 225–239.

[15] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner, "Are you ready to lock?" in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2014, pp. 750–761.

[16] 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 *Proc. Symp. Usable Privacy Secur. (SOUPS)*, 2014, pp. 213–230.

[17] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proc. 4th USENIX Conf.*, 2010, pp. 1–10.

[18] P. Cheng, I. E. Bagci, U. Roedig, and J. Yan, "SonarSnoop: Active acoustic side-channel attacks," 2018, *arXiv:1808.10250*. [Online]. Available: https://arxiv.org/abs/1808.10250

[19] *Fingerprints are Not Fit for Secure Device Locking*, Secur. Res. Labs, Berlin, Germany, 2019. [Online]. Available: https://srlabs.de/bites/spoofing-fingerprints/

[20] L. H. Newman. (2016). *Hackers Trick Facial-Recognition Logins with Photos From Facebook What Else?* [Online]. Available: https://www.wired.com/2016/08/

[21] R. Brandom. (2017). *Two-Factor Authentication is a Mess*. [Online]. Available: https://www.theverge.com/

[22] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Comput. Secur.*, vol. 30, no. 4, pp. 208–220, Jun. 2011.

[23] V. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," *IEEE Signal Process. Mag.*, vol. 33, no. 4, pp. 49–61, Jul. 2016.

[24] A. Hang, A. De Luca, M. Smith, M. Richter, and H. Hussman, "Where have you been? Using location-based security questions for fallback authentication," in *Proc. Symp. Usable Privacy Secur. (SOUPS)*, 2015, pp. 169–183.

[25] J. Thorpe, B. MacRae, and A. Salehi-Abari, "Usability and security evaluation of GeoPass: A geographic location-password scheme," in *Proc. Symp. Usable Privacy Secur. (SOUPS)*, 2013, Art. no. 14.

[26] N. Shone, C. Dobbins, W. Hurst, and Q. Shi, "Digital memories based mobile user authentication for IoT," in *Proc. IEEE Int. Conf. Comput. Inf. Technol.; Ubiquitous Comput. Commun.; Dependable, Autonomic Secure Comput.; Pervasive Intell. Comput.*, Oct. 2015, pp. 1796–1802.

[27] Y. Albayram, M. M. H. Khan, A. Bamis, S. Kentros, N. Nguyen, and R. Jiang, "A location-based authentication system leveraging smartphones," in *Proc. IEEE 15th Int. Conf. Mobile Data Manage.*, Jun. 2014, pp. 83–88.

[28] P. Gupta, T. K. Wee, N. Ramasubbu, D. Lo, D. Gao, and R. K. Balan, "HuMan: Creating memorable fingerprints of mobile users," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Mar. 2012, pp. 479–482.

[29] S. Das, E. Hayashi, and J. I. Hong, "Exploring capturable everyday memory for autobiographical authentication," in *Proc. UbiComp*, 2013, pp. 211–220.

[30] S. K. Dandapat, S. Pradhan, B. Mitra, R. R. Choudhury, and N. Ganguly, "ActivPass: Your daily activity is your password," in *Proc. ACM Conf. Hum. Factors Comput.*, 2015, pp. 2325–2334.

[31] H. Sun, K. Wang, X. Li, N. Qin, and Z. Chen, "PassApp: My app is my password!" in *Proc. 17th Int. Conf. Hum.-Comput. Interact. Mobile Devices Services (MobileHCI)*, Copenhagen, Denmark, no. 10, 2015, pp. 306–315. doi: 10.1145/2785830.2785880.

[32] H. Hang, A. De Luca, and H. Hussmann, "I know what you did last week! Do You?: Dynamic security questions for fallback authentication on smartphones," in *Proc. CHI*, 2015, pp. 1383–1392.

[33] J. Naftulin. (2016). *Research Shows We Touch Our Cell Phones 2,617 Times Per Day*. [Online]. Available: https://www.businessinsider.com.au/

[34] M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci, and C. Gransart, "Token-based lightweight authentication to secure IoT networks," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2018, pp. 1–4.

[35] J. Liu, Y. Xiao, and C. L. P. Chen, "Authentication and access control in the Internet of Things," in *Proc. 32nd Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2012, pp. 588–592.

[36] Kwikset. (2019). *No More Keys*. [Online]. Available: https://www.kwikset.com/electronics/homeowners/keylessentry.aspx

[37] Yale. (2019). *Yale Assure Lock*. [Online]. Available: https://www.yalelock.com.au/en/yale/yale-au/yale-products/secure-connect/yale-assure-digital-lock/

[38] M. Sandström, "Liveness detection in fingerprint recognition systems," M.S. thesis, Dept. Syst. Eng., Linköpings Univ., Linköping, Sweden, 2004.

[39] T. van der Putte and J. Keuning, "Biometrical fingerprint recognition: Don't get your fingers burned," in *Proc. 4th Working Conf. Smart Card Res. Adv. Appl. Smart Card Res. Adv. Appl.*, Sep. 2000, pp. 289–303.

[40] M. Sepasian, C. Mares, and W. Balachandran, "Liveness and spoofing in fingerprint identification: Issues and challenges," in *Proc. Int. Conf. Comput. Eng. Appl.*, 2010, pp. 150–158.

[41] C. Yuan, X. Sun, and Q. M. J. Wu, "Difference co-occurrence matrix using BP neural network for fingerprint liveness detection," *Soft Comput.*, vol. 23, no. 13, pp. 5157–5169, Jul. 2019.

[42] Z. Xia, C. Yuan, R. Lv, X. Sun, N. N. Xiong, and Y.-Q. Shi, "A novel weber local binary descriptor for fingerprint liveness detection," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published.
[43] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry*, vol. 11, no. 2, p. 141, 2019.
[44] M. Staff and G. Fleishman. (2017). *Face ID on the iPhone X: Everything You Need to Know About Apple's Facial Recognition*. [Online]. Available: https://www.macworld.com
[45] T. Brewster. (2018). *We Broke Into a Bunch of Android Phones with a 3D-Printed Head*. [Online]. Available: https://www.forbes.com/
[46] (2017). *Bkav's New Mask Beats Face ID, 'Twin Way': Severity Level Raised, Do Not Use Face ID in Business Transactions*. [Online]. Available: http://www.bkav.com
[47] Samsung. (2016). *Iris Recognition on Galaxy S8*. [Online]. Available: https://www.samsung.com/au/iris/
[48] D. Goodin. (2016). *Breaking the Iris Scanner Locking Samsung's Galaxy S8 is Laughably Easy*. [Online]. Available: https://arstechnica.com/
[49] Stacy. (2017). *Is the Galaxy S8 Hazardous to Your Eyesight? Samsung Users Claim Iris Scanner is Causing Eye Discomfort*. [Online]. Available: https://www.dailymail.co.uk/
[50] H. Zhong, S. S. Kanhere, and C. T. Chou, "VeinDeep: Smartphone unlock using vein patterns," in *Proc. PerCom*, Mar. 2017, pp. 2–10.
[51] J. Cox. (2018). *Hackers Make a Fake Hand to Beat Vein Authentication*. [Online]. Available: https://www.vice.com/
[52] J. Chauhan, Y. Hu, S. Seneviratne, A. Misra, A. Seneviratne, and Y. Lee, "BreathPrint: Breathing acoustics-based user authentication," in *Proc. MobiSys*, 2017, pp. 278–291.
[53] NEC. (2018). *Biometric Authentication Based on the Acoustic Characteristics of the Ears*. [Online]. Available: https://www.nec.com
[54] A. F. P. Negara, E. Kodirov, D.-J. Choi, G.-S. Lee, M. F. A. Abdullah, and S. Sayeed, "Implicit authentication based on ear shape biometrics using smartphone camera during a call," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2012, pp. 2272–2276.
[55] X. Zhang, L. Yao, S. S. Kanhere, Y. Liu, T. Gu, and K. Chen, "MindID: Person identification from brain waves through attention-based recurrent neural network," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 2, no. 3, pp. 149:1–149:23, Sep. 2018. [Online]. Available: http://doi.acm.org/10.1145/3264959
[56] I. Martinovic, K. Rasmussen, M. Roeschlin, and G. Tsudik, "Authentication using pulse-response biometrics," *Commun. ACM*, vol. 60, no. 2, pp. 108–115, Jan. 2017. [Online]. Available: http://doi.acm.org/10.1145/3023359
[57] N. Zheng, K. Bai, H. Huang, and H. Wang, "You are how you touch: User verification on smartphones via tapping behaviors," in *Proc. IEEE 22nd Int. Conf. Netw. Protocols*, Oct. 2014, pp. 211–221.
[58] Y. Chen, J. Sun, R. Zhang, and Y. Zhang, "Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr./May 2015, pp. 2686–2694.
[59] J. Sun, R. Zhang, J. Zhang, and Y. Zhang, "Touchin: Sightless two-factor authentication on multi-touch mobile devices," in *Proc. IEEE Conf. Commun. Netw. Secur.*, Oct. 2014, pp. 436–444.
[60] T. Feng, X. Zhao, N. DeSalvo, Z. Gao, X. Wang, and W. Shi, "Security after login: Identity change detection on smartphones using sensor fusion," in *Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST)*, Apr. 2015, pp. 1–6.
[61] C. Bo, L. Zhang, X.-Y. Li, Q. Huang, and Y. Wang, "Silentsense: Silent user identification via touch and movement behavioral biometrics," in *Proc. MobiCom*, 2013, pp. 187–190.
[62] N. Neverova, C. Wolf, G. Lacey, L. Fridman, D. Chandra, B. Barbello, and G. Taylor, "Learning human identity from motion patterns," Apr. 2016, *arXiv:1511.03908*. [Online]. Available: https://arxiv.org/abs/1511.03908
[63] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, "Active authentication on mobile devices via stylometry, application usage, Web browsing, and GPS location," *IEEE Syst. J.*, vol. 11, no. 2, pp. 513–521, Jun. 2016.
[64] R. Kumar, V. V. Phoha, and R. Raina, "Authenticating users through their arm movement patterns," Mar. 2016, *arXiv:1603.02211*. [Online]. Available: https://arxiv.org/abs/1603.02211
[65] J. Yang, Y. Li, and M. Xie, "MotionAuth: Motion-based authentication for wrist worn smart devices," in *Proc. IEEE PerCom*, Mar. 2015, pp. 550–555.
[66] S. Li, A. Ashok, Y. Zhang, C. Xu, J. Lindqvist, and M. Gruteser, "Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns," in *Proc. IEEE PerCom*, Mar. 2016, pp. 1–9.
[67] T. Alpcan, S. Kesici, D. Bicher, M. K. Mihçak, C. Bauckhage, and S. Çamtepe, "A lightweight biometric signature scheme for user authentication over networks," in *Proc. SecureComm*, 2008, Art. no. 33.
[68] S. W. Shah and S. S. Kanhere, "Wi-sign: Device-free second factor user authentication," in *Proc. MobiQuitous*, 2018, pp. 135–144.
[69] S. W. Shah and S. S. Kanhere, "Wi-access: Second factor user authentication leveraging WiFi signals," in *Proc. PerCom Workshops*, 2018, pp. 330–335.
[70] L. Middleton, A. A. Buss, A. Bazin, and M. S. Nixon, "A floor sensor system for gait recognition," in *Proc. 4th IEEE Workshop Autom. Identificat. Adv. Technol. (AutoID)*, Oct. 2005, pp. 171–176.
[71] J. Cheng, M. Sundholm, B. Zhou, M. Kreil, and P. Lukowicz, "Recognizing subtle user activities and person identity with cheap resistive pressure sensing carpet," in *Proc. Int. Conf. Intell. Environ.*, Jun./Jul. 2014, pp. 148–153.
[72] H. Kim, I. Kim, and J. Kim, "Designing the smart foot mat and its applications: As a user identification sensor for smart home scenarios," *Adv. Sci. Technol. Lett.*, vol. 87, pp. 1–5, Apr. 2015.
[73] A. S. Guinea, A. Boytsov, L. Mouline, and Y. Le Traon, "Continuous identification in smart environments using wrist-worn inertial sensors," in *Proc. MobiQuitous*, 2018, pp. 87–96.
[74] X. Wang, A. M. Bernardos, P. Tarrío, and J. R. Casar, "A gesture-enabled method for natural identification in smart spaces," in *Proc. 16th Int. Conf. Inf. Fusion*, Jul. 2013, pp. 827–834.
[75] J. Zhang, B. Wei, W. Hu, and S. S. Kanhere, "WiFi-ID: Human identification using WiFi signal," in *Proc. Int. Conf. Distrib. Comput. Sensor Syst.*, May 2016, pp. 75–82.
[76] W. Wang, A. X. Liu, and M. Shahzad, "Gait recognition using WiFi signals," in *Proc. UbiComp*, 2016, pp. 363–373.
[77] Y. Zeng, P. H. Pathak, and P. Mohapatra, "WiWho: WiFi-based person identification in smart spaces," in *Proc. ISPN*, 2016, Art. no. 4.
[78] S. Davidson, D. Smith, C. Yang, and S. C. Cheah, "Smartwatch user identification as a mean of authentication," Univ. California San Diego, San Diego, CA, USA, 2016.
[79] F. Zhang, A. Kondor, and S. Muftic, "Location-based authentication and authorization using smart phones," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 1285–1292.
[80] U. A. Abdurrahman, M. Kaiiali, and J. Muhammad, "A new mobile-based multi-factor authentication scheme using pre-shared number, GPS location and time stamp," in *Proc. Int. Conf. Electron., Comput. Comput.*, Nov. 2013, pp. 293–296.
[81] N. Karapanos, C. Marforio, C. Soriente, and S. Čapkun, "Sound-proof: Usable two-factor authentication based on ambient sound," in *Proc. 24th USENIX Secur. Symp.*, 2015, pp. 483–498.
[82] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, "T2FA: Transparent two-factor authentication," *IEEE Access*, vol. 6, pp. 32677–32686, 2018.
[83] S. W. Shah and S. S. Kanhere, "Wi-Auth: WiFi based second factor user authentication," in *Proc. MobiQuitous*, 2017, pp. 393–402.
[84] RSA. (2019). *RSA SecureID*. [Online]. Available: https:www.rsa.com
[85] Yubico. (2019). *YubiKeys*. [Online]. Available: https:www.yubico.com
[86] Kwikset. (2019).*Touch-to-Open Smart Lock*. [Online]. Available: https://www.kwikset.com/kevo/default
[87] (Aug. 2019). *Your Smart Home Starts at the Front Door*. [Online]. Available: https://august.com/
[88] M. Wollerton. (2016). *Here's What Happened when Someone Hacked the August Smart Lock*. [Online]. Available: https://august.com/
[89] B. M. Wolf and L. Gil. (2019). *How to Enable Auto Unlock on Your Mac and Apple Watch*. [Online]. Available: https://www.imore.com/auto-unlock
[90] S. Klee, "Understanding the apple auto unlock protocol," B.S. thesis, Dept. Comput. Sci., Tech. Univ. Darmstadt, Darmstadt, Germany, 2017.
[91] Motiv. (2018). *Motiv Ring Now Provides New, Easy-to-Use Security Features to Protect Your Online Identity.*. [Online]. Available: https://mymotiv.com/online-security/
[92] Duo Security. (2019). *Duo Push*. [Online]. Available: https://duo.com/product/trusted-users/two-factor-authentication/authentication-methods/duo-push
[93] Encap Security. (2019). *Encap Security*. [Online]. Available: https://www.encapsecurity.com/

[94] Auth0. (2017). *Two Factor Authentication Using Biometrics*. [Online]. Available: https://auth0.com/blog/two-factor-authentication-using-biometrics/
[95] Biosig-ID. (2018). *Biometric Multi-Factor Authentication Smart Password*. [Online]. Available: https://www.biosig-id.com
[96] V. M. Patel, R. Gopalan, R. Li, and R. Chellappa, "Visual domain adaptation: A survey of recent advances," *IEEE Signal Process. Mag.*, vol. 32, no. 3, pp. 53–69, May 2015.

SYED W. SHAH received the M.S. degree in electrical and electronics engineering from the University of Bradford, U.K. He is currently pursuing the Ph.D. degree from the University of New South Wales (UNSW), Sydney, Australia. His research interests include pervasive/ubiquitous computing, user authentication/identification, the Internet of Things, and signal processing.

SALIL S. KANHERE received the M.S. and Ph.D. degrees in electrical engineering from Drexel University, Philadelphia, PA, USA. He is currently a Professor with the School of Computer Science and Engineering, UNSW, Sydney, Australia. He is also a Conjoint Researcher with CSIRO Data61. He has published over 200 peer-reviewed articles and delivered over 30 tutorials and keynote talks on these topics. His research has been featured on ABC News Australia, Forbes, the IEEE Spectrum, Wired, ZDNET, Computer World, Medium, MIT Technology Review, and other media outlets. His research interests include the Internet of Things, pervasive computing, blockchain, crowdsourcing, data analytics, privacy, and security. He is a Senior Member of the ACM. He is a recipient of the Alexander von Humboldt Research Fellowship. He regularly serves on the organizing committee of a number of the IEEE and ACM international conferences. He is on the Editorial Board of Elsevier's Pervasive and Mobile Computing and Computer Communications and serves as an ACM Distinguished Speaker.