Behavioral Biometrics for Mobile User Authentication: Benefits and Limitations

Maria Papaioannou
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
m.papaioannou@av.it.pt

Georgios Mantas
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
gimantas@av.it.pt

Emmanouil (Manos) Panaousis
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
e.panaousis@greenwich.ac.uk

Aliyah Essop
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
a.b.essop@greenwich.ac.uk

Jonathan Rodriguez
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Computing, Engineering and Science, University of South Wales
Pontypridd, UK
jonathan@av.it.pt

Victor Sucasas
Technology Innovation Institute
Abu Dhabi, UAE
victor.sucasas@tii.ae

***Abstract*—User authentication serves as the primary defense, also referred to as first line of defense, by verifying the identity of a mobile user, often as a requirement for accessing resources on a mobile device. For many years, user authentication relied on "something that the user knows," also known as knowledge-based user authentication. However, recent research indicates that knowledge-based user authentication is no longer considered secure or convenient for mobile users because it imposes several limitations. These limitations highlight the need for more secure and user-friendly user authentication methods. One promising solution is user authentication based on "something that the user is," which includes authentication methods that use physical characteristics of the mobile user (i.e., physiological biometrics) or their involuntary actions (i.e., behavioral biometrics). Although physiological biometrics have been successfully deployed for mobile user authentication over the last years, recent studies suggest that they show several weaknesses (e.g., vulnerable to various attacks such as impersonation). Consequently, experts in the security field are now focusing more on user authentication based on behavioral biometrics. Therefore, the aim of this work is to investigate the benefits, as well as the limitations of behavioral biometrics for mobile user authentication in order to provide a foundation for organizing research efforts toward the design and development of proper user authentication solutions based on behavioral biometrics for mobile devices.**

Keywords—mobile user authentication, benefits of behavioral biometrics, limitations of behavioral biometrics

I. INTRODUCTION

Authentication acts as the first line of defense verifying the identity of a user, process, or device, often as a prerequisite to permit access to resources in an information system. In mobile or smartphone devices, user authentication is crucial to safeguard the data privacy of mobile users [1]–[6]. For several decades, user authentication relied on the "something that the user knows" paradigm, including Personal Identification Numbers (PINs), standard passwords, and graphical patterns [7]. These methods are typically used as one-shot authentication at the beginning of a session and remain valid throughout the session [8]. Therefore, the once authenticated user has unlimited access to the device during the whole session. However, recent studies [8]–[10] suggest that knowledge-based user authentication is no longer secure and convenient for mobile users. First of all, these traditional user authentication techniques are not able to distinguish legitimate users, instead authenticate anyone with valid credentials. Regardless of this, mobile users are required to memorize their credentials to unlock their devices. As users tend to select easily remembered passwords, their mobile devices are becoming vulnerable to numerous attacks such as. dictionary, key-logger-based, shoulder-surfing, and guessing attacks, [11]. In addition, in the case of Android mobile devices, mobile users often set simple graphical patterns for device unlocking, which can be easily guessed or observed by attackers. Researchers have shown that it is possible to crack a significant percentage of "unique" Android patterns in just a few attempts [12], exposing devices to attacks such as shoulder-surfing, and guessing attacks.

Moreover, to enhance security in sensitive applications such as e-banking, two-factor authentication methods often are deployed. In particular, traditional username and password user authentication schemes are combined with one-time passcodes (OTPs) (also refered to as "something that the user has" paradigm). Service providers may provide a security device for generating passcodes or send the code via SMS to mobile user's smartphone. Nevertheless, these methods might be vulnerable to Man-In-The-Middle (MITM) attacks and Man-in-the-PC/Phone (MITPC/P) attacks, compromising the confidentiality of the generated passcodes [13]. In fact, the Verizon Data Breach Investigations Report [13] recommends against two-factor authentication via SMS due to the risk of malicious code capturing the second factor delivered by SMS. Furthermore, OTP solutions appear to be inconvenient and more costly for users as they require additional hardware only for authentication purposes, and are generally slower. Typing errors can also lead to issues with OTP-based authentication.

The limitations of current authentication methods highlight the necessity of developing more secure and user-friendly solutions. Toward this direction, user authentication based on the "something that the user is" paradigm has caught the attention [10]. This category includes methods which utilize human physical characteristics (i.e., physiological biometrics), such as fingerprints, hand geometries, retinal and

ISBN 978-3-903176-57-7

facial patterns, or involuntary actions (i.e., behavioral biometrics), such as gait and dynamic keyboarding characteristics [8]. Considering a smartphone device, the authors in [14] highlight that the physiological biometrics, require special hardware equipment and/or software to be captured only for authentication purposes, while behavioral biometrics can be effortlessly collected by the sensors of mobile devices, namely, gyroscope, accelerometer, microphone and touch screen [14]–[16]. Thus, behavioral biometrics are considered cost-effective as they do not need any additional hardware equipment for their deployment. Furthermore, behavioral biometrics are considered to be lightweight in the implementation [7], and highly secure, as they are unique and cannot be copied, shared, lost, or stolen [8]. On top of that, they can even be combined with other authentication means, such as knowledge-based schemes, to establish multifactor authentication and enhance security without disrupting device usage [8]. Research efforts are already underway to develop behavioral biometric modalities, such as gait, keystroke or touch dynamics, and voice, for user authentication. As such, experts in the security field are focusing on creating user authenication mechanisms based on behavioral biometrics, as they could revolutionize the authentication landscape in the coming years [8], [17]. Toward this direction, the aim of this work is to investigate the benefits, as well as the limitations of behavioral biometrics for mobile user authentication in order to provide a foundation for organizing research efforts toward the design and development of proper user authentication solutions based on behavioral biometrics for mobile devices.

Following the Introduction, the rest of the paper is organized as follows. Section II presents related work on mobile user authentication. Section III presents the benefits of behavioral biometrics used for mobile user authentication, while Section IV discusses their limitations. Finally, the paper is concluded in Section V.

II. Related Work on Mobile User Authentication

Mobile user authentication is the process of verifying the identity of a user who is attempting to access resources or services on a mobile device acting as a first line of defense. This typically involves the user providing some form of authentication factor, such as a password, PIN, fingerprint, facial recognition, or other biometric data, to prove that they are the legitimate owner or authorized user of the device. In particular, user authentication techniques may be divided into three main categories, depending on which of the following they are based on: (i) something the user knows, (ii) something the user has, and (iii) something the user is [18]. In the following of Section II, we provide more details about each category.

A. Something the User Knows

The "something the user knows" category includes standard passwords, PINs, graphical patterns, and secret or private keys used in challenge-response protocols [18]. Gupta et al. [8] have categorized the commonly used methods for achieving authentication in smartphones. According to their study, knowledge-based schemes are generally used as one-shot, periodic, and single sign-on (SSO). More specifically, one-shot authentication involves user authentication only at the beginning of the session, after which the user has unrestricted access to the device until they sign off or close

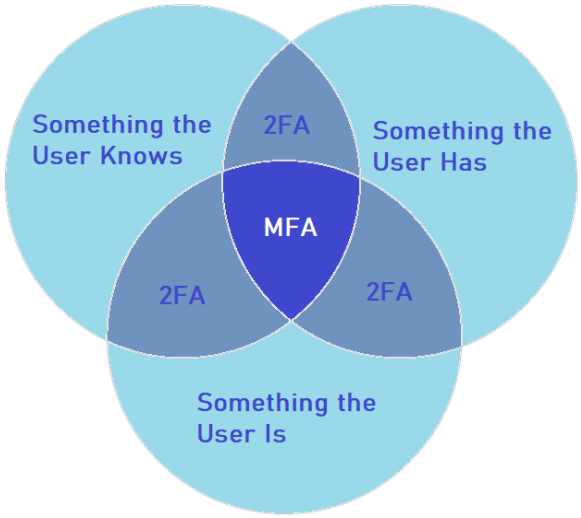

Fig. 1. Vizualization of the three types of user authentication, and their combinations leading to 2-Factor Authentication (2FA) and Multi-Factor Authentication MFA.

the session. On the other hand, periodic authentication is a variant of one-shot authentication, but with a default timeout period after which the user must re-authenticate himself. Finally, SSO authentication allows the mobile user to remain signed in with valid login credentials until the session is terminated or revoked, but abnormal system activity may trigger re-authentication [8]. For example, Google provides SSO mechanisms for G Suite apps on Android devices, which can be accomplished by pairing smartphones with wearable devices like smartwatches [19].

Recent studies [9] suggest that conventional user authentication techniques are no longer considered secure or convenient for mobile users. First of all, these techniques authenticate anyone with valid credentials, without distinguishing between legitimate and malicious users. Despite this, they also require mobile users to memorize their passwords to unlock the device each time it is needed. Zhang et al. [11] describe the difficulties users face in remembering and correctly recalling multiple passwords, leading to the use of simple and easily guessed passwords, making mobile devices vulnerable to various attacks such as guessing or dictionary attacks. Alternatively, Android users tend to use graphical patterns to unlock their devices. However, this method also requires mobile users to memorize their pattern, resulting in the use of simple and easily guessed patterns. Researchers were able to crack 95% of the unique graphical patterns collected from 215 users within just five attempts [12].

B. Something the User Has

This is typically a physical accessory, resembling a passport in function. Examples include chip cards, magnetic-striped cards, customized calculators (password generators) that provide time-variant passwords, and tokens [18]. For instance, smartphone applications that handle sensitive information, such as e-banking and e-wallets, employ two-factor authentication techniques, such as one-time passcodes (OTPs), in conjunction with the usual username and password authentication. Service providers usually offer a small security device to users for generating passcodes, or the

passcode could be sent via SMS to the user's smartphone [8]. OTP schemes can also be implemented on mobile devices. Furthermore, users can even generate passcodes offline using the mobile app provided by the service provider or by pairing with another device, such as smartwatches or smart glasses [8]. However, OTP solutions appear to be vulnerable to attacks, including Man-in-the-Middle (MITM) and Man-in-the-PC/Phone (MITPC/P) attacks, which compromise the confidentiality of the generated passcodes. In fact, the Verizon Data Breach Investigations Report [13] has stopped recommending two-factor user authentication via SMS due to the risk of malicious code capturing the second factors delivered by SMS or offline OTPs generated using apps. Additionally, studies have shown that OTP schemes are inconvenient and more costly for users, as they require additional hardware only for the purpose of authentication and are comparatively slower. Furthermore, users may make mistakes when typing passcodes [20], [21], which can cause problems with OTP-based authentication.

C. *Something the User Is*

This category includes authentication methods which make use of either mobile user's physiological biometrics, or their behavioral biometrics [8], [18]. Physiological biometrics include physical and anatomical characteristics of an individual, such as fingerprints, facial images, iris or retina scans, or hand geometry [8], [18], while behavioral biometrics refer to unique patterns of human behavior, such as keystroke dynamics, voice, and gait [8], [18].

a) Physiological Biometrics: Regarding the physiological biometrics (e.g., face, fingerprint, and iris recognition), the mobile device manufacturers have begun embedding the corresponding sensors to capture them and employ them for accurate and convenient mobile user authentication. For instance, Apple, Huawei, Samsung, and Nokia have already incorporated iris and fingerprint scanners in their latest smartphones. Although these biometric schemes are considered secure because of their uniqueness, they appear to be vulnerable to various attacks, such as impersonation. Nowadays, the user's face can easily be found on social media pages, and their fingerprints can simply be extracted from photos. Researchers have shown that physiological biometrics can be hacked with inexpensive equipment and simple algorithms. For instance, the iPhone X Face ID was hacked using a 3D printed mask of the owner's face that cost around $150 [22], while a simple photo of the owner unlocked the Samsung S8 [23]. The German Chaos Computer Club also hacked the iPhone 5S fingerprint scanner by photographing the glass surface with the user's fingerprint and creating a fake thin film within two days of Apple launching the iPhone 5S worldwide [24]. Additionally, a researcher from Japan's National Institute of Informatics showed that fake fingerprints can be easily created from a simple photo taken from three meters away with the peace sign, and they can unlock the device without any sophisticated process [25]. Therefore, there is a need for more sophisticated algorithms and novel solutions to leverage the advantages of the uniqueness of physiological biometrics.

b) Behavioral Biometrics: Behavioral biometric-based user authentication appears as a promising solution for securing sensitive applications performed on mobile devices [10], [26]. Behavioral biometrics can be combined with other authentication methods as an additional layer of authentication without disrupting device usage, improving the overall accuracy and device security [8], [10], [26]. Research has already begun on various behavioral biometric modalities, such as gait, keystroke or touch dynamics, and voice [8]:

- Gait recognition is a technique that utilizes the walking style of an individual in order to authenticate them [8]. Recently, smartphones and wearable devices have started incorporating gait recognition schemes for user authentication [27]–[29]. Many researchers have developed gait-based solutions that are used in conjunction with wearable sensors, and initial results have been promising, though further testing is necessary to ensure resistance against impersonation attacks [27]–[29]. Nevertheless, using a gait-based solution with a wearable device may be costly for the user and not that practical, as they require additional hardware only for the purpose of authentication. Instead, a gait-based solution that utilizes built-in sensors like accelerometers or gyroscopes may be more suitable and convenient for mobile users.
- Keystroke or touch dynamics refer to the characteristics of how a user types or interacts with the touch screen of a mobile device, such as the timing and pressure of keystrokes or swipes. These characteristics are unique to each user and can be used efficiently for user authentication [8], [7], [30], [31]. In particular, by analyzing the user's unique keystroke or touch dynamics, the system can verify the user's identity and provide an additional layer of security [8], [7], [30], [31]. For example, when a user enters their login credentials on a mobile banking app, the system can analyze their keystroke or touch dynamics to verify their identity as an additional authentication layer to their credential verification (that might have been compromised or stolen by a malicious actor). These methods do not require special hardware and have been extensively evaluated [8], [7], [30], [31].
- Research efforts have been focused on voice recognition by testing it on publicly available databases [32]. The mobile user's voice is digitized, and the Mel Frequency Cepstral Coefficients (MFCCs) and Euclidean distance are calculated. These findings could potentially improve the accuracy of traditional biometric systems and expand the possibilities for continuous user authentication [33].

Overall, for a smartphone device, the face physiological biometric can be collected by using the camera of the device, while the fingerprint and iris recognition require specialized equipment (i.e., fingerprint and iris scanners). On the other hand, the behavioral biometrics can be collected all by the sensors integrated already on mobile devices [14]. As such, behavioral biometrics are starting to get attention as they appear to be cost-effective; they do not require any additional hardware and/or software equipment, and they are lightweight in their implementation [7]. On top of that, they can also be combined with other authentication methods such as username and password for multifactor authentication to improve mobile device security. Security experts are focusing on developing such mechanisms as they are expected to reshape the authentication landscape in the coming years [8], [17], [34].

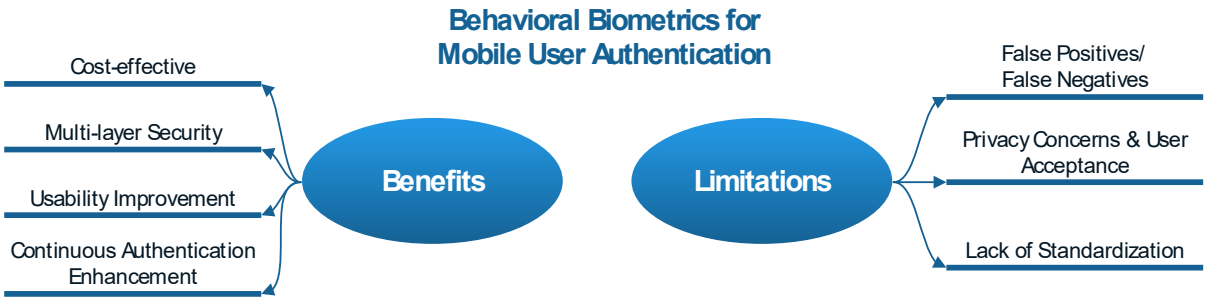

Fig. 2. Benefits and limitations of behavioral biometrics used in mobile user authentication.

III. Benefits of Behavioral Biometrics in Mobile User Authentication

There is no doubt that behavioral biometrics have caught not only researchers' attention, but also the industry's as they appear to be a promising user authentication solution for mobile devices ensuring data privacy, while addressing major limitations that conventional user authentication techniques impose. In the following of this section, we will discuss the main benefits of behavioral biometrics when they are used in mobile user authentication.

A. Cost-effective

As we have already discussed in Section II, one of the major advantages of behavioral biometrics is that they can be cost-effective compared to other authentication methods that they require hardware tokens or biometric scanners [8], [35], [36]. Since behavioral biometrics rely on software analysis of the mobile user's behavior (e.g., mobile user's walking style, their way to type or interact with the touch screen of their mobile device, such as the timing and pressure of keystrokes or swipes, or characteristics of their voice), they can be captured and implemented on existing mobile devices without requiring additional hardware. In particular, behavioral biometrics can be captured using the mobile integrated sensors, namely gyroscope, magnetometer, gravity, orientation, proximity accelerometer, linear accelerometer, touchscreen, keystroke, GPS, light, Bluetooth, microphone, and WiFi during natural human-mobile interaction [8], [35], [36].

B. Multi-layer Security

Behavioral biometrics can provide an additional layer of security to traditional authentication methods such as passwords and PINs. By analyzing patterns in the user's behavior, such as the way they type, swipe, or hold their mobile device, behavioral biometrics can efficiently identify fraudulent users who may have stolen a legitimate user's credentials [8], [35], [36]. One of the primary benefits of behavioral biometrics is that it is extremely difficult for an unauthorized person to replicate another person's unique behavior patterns. For instance, while an attacker may be able to guess a password or compromise it through a phishing attack, it would be much harder for them to mimic the exact way a person types on a keyboard or interacts with their smartphone. This makes it a powerful tool for preventing account takeovers and other types of fraud. Behavioral biometrics can also be used to detect anomalies in user behavior that could indicate suspicious activity [8], [33], [35], [36]. For instance, if a user typically logs in from a specific device and suddenly begins logging in from a different location or using a different typing pattern, this could be a red flag for potential fraud or hacking attempts. Overall, behavioral biometrics are considered secure and accurate for mobile user authentication as they are unique and cannot be shared, copied, lost, or stolen [8], [33], [35], [36].

C. Usability Improvement

Behavioral biometrics are able to make the authentication process more convenient and user-friendly [8], [33], [35]–[39]. Since it is based on the user's natural behavior, there is no need to remember or enter a password or PIN, or even carry a particular hardware only for their authentication which can be a hassle for mobile users. On the contrary, it is suggested that behavioral biometrics manage to authenticate the users unobtrusively based on their interactions with the device. In this way, they have been attractive among the researchers in the field of user authentication, offering frictionless user authentication (i.e., "the ability to verify authenticity of a user (to a device or service) without the user needing to respond to an explicit authentication request", enhancing the existing authentication mechanisms without affecting the usage of the device [35].

D. Continuous Authentication Enhancement

Unlike traditional authentication methods, which are typically performed only at the beginning of the session (i.e., one-shot authentication) and, afterwards, any future changes and/or abnormalities in user identity/behavior remain undetected, increasing the risk of sensitive information leakage and user's privacy violation, behavioral biometrics can enhance continuous authentication throughout the user's session [37], [38]. In other words, if a user's behavior changes, the system can detect this and prompt re-authentication. This allows to overcome the limitations of the conventional one-shot authentication [8], [10], [40], [41]. Nowadays, continuous user authentication, relying on behavioral biometrics, has been shown to have the potential to further improve mobile authentication security without sacrificing usability (i.e., security and usability are often thought of as being contradictory) [8], [26], [41]–[44].

IV. Limitations of Behavioral Biometrics in Mobile User Authentication

While behavioral biometrics offer numerous benefits when used for user authentication, there are also limitations and potential risks that need to be taken into account in order

to gain the trust of all involved stakeholders, as well as the potential mobile users and reach their full potential toward their adoption in mobile user authentication.

A. False Positives/False Negatives

According to [10], [26], behavioral biometrics are subject to false positives/false negatives. This is because behavioral biometrics rely on analyzing patterns in the user's behavior to authenticate legitimate users, such as mouse movement patterns or keystroke dynamics. However, these patterns can change over time (e.g., device orientation or user fatigue) or might be affected by external factors such as ambient noise or environmental conditions (e.g., foggy weather), leading to false positives where legitimate users are identified as fraudulent, and thus, they are denied access [10], [26]. Similarly, behavioral biometrics can also result in false negatives, whereby unauthorized users are mistakenly identified are legitimate users, and thus they are granted access. This can occur if an attacker is able to successfully mimic the user's behavior and fool the system [10], [26]. Nevertheless, this is extremely difficult to happen compared to other authentication means that are easily compromised or stolen such as passwords or fingerprints according to [10], [26]. Moreover, behavioral biometrics can also suffer from inconsistencies. The authors in [10], [26] state that it is essential to maximize the accuracy of the deployed algorithms in order to overcome this limitation of false positives/false negatives. They additionally argue that given that the behavior and habits of a mobile user might change over time, authentication systems should also be capable of adapting to these changes [10], [26].

B. Privacy Concerns & User Acceptance

Another concern is user's privacy and how this concern might affect user's acceptance. Behavioral biometric data is highly personal and can reveal sensitive information about the user, such as their physical condition or emotional state [10], [26]. As a result, mobile users may be hesitant to adopt behavioral biometrics for authentication, as they may feel uncomfortable with the collection, storage, and use of their behavioral data for authentication purposes, especially in the context of data breaches or unauthorized access. In particular, there are potential security risks associated with the collection and storage of behavioral biometric data, as these data may be susceptible to misuse or hacking. Consequently, it is crucial to weight the benefits and risks of behavioral biometric authentication and safeguard proper security measures are in place to protect them as the success of behavioral biometrics relies on user acceptance and adoption and mobile users may be skeptical and prefer traditional authentication methods that are familiar and trusted. However, behavioral biometrics (e.g., gait, keystroke dynamics) remain less sensitive than physiological biometrics (e.g., fingerprints, iris) [10], [26].

C. Lack of Standardization

Given the fact that behavioral biometrics have emerged as a new tendency in mobile user authentication, there is currently no specific standardization for behavioral biometric data [45]–[48], rather than the General Data Protection Regulation (GDPR). On top of that, there are no specific guidelines for behavioral biometric data processing and storage which means that different providers may use different metrics and algorithms. This can make it difficult to compare or combine data across different systems. It is worthwhile to mention that although NIST supports the timely development of biometric standards [49], there has not been such effort in the EU. Last but not least, the International Organization for Standardization (ISO) has developed several standards related to physiological biometric authentication, but not yet for behavioral biometric authentication. Hence, it is important to highlight the necessity of standardization efforts for the behavioral biometrics used in mobile user authentication in order to ensure interoperability and reliability of behavioral biometric technologies, as well as to facilitate broader adoption of these technologies in various industries [45]–[48].

In summary, while behavioral biometrics offer numerous benefits for mobile user authentication, it also imposes limitations that need to be carefully considered and addressed in order to ensure its effectiveness and user acceptance.

V. Conclusions

User authentication serves as a first line of defense, verifying the identity of a mobile user, often as a prerequisite for accessing resources on a mobile device. For many years, user authentication relied on "something that the user knows," also known as knowledge-based user authentication. However, recent research indicates that knowledge-based user authentication is no longer considered secure or convenient for mobile users because it imposes several limitations. Therefore, user authentication for sensitive applications often deploys 2FA combining "something that the user knows," and "something that the user has," paradigms. Nevertheless, this has appeared to be costly for the users and comparatively slower. These limitations highlight the need for more secure and user-friendly user authentication methods. One promising solution is user authentication based on "something that the user is," which includes authentication methods that use (i) the physiological biometrics, or (ii) the behavioral biometrics of the mobile user. The aim of this work was to investigate the benefits, as well as the limitations of behavioral biometrics for mobile user authentication in order to provide a foundation for organizing research efforts toward the design and development of proper user authentication solutions based on behavioral biometrics for mobile devices.

Acknowledgment

The research work leading to this publication has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement H2020-MSCA-RISE-2019-eBORDER-872878. This research work was also supported by the Fundação para a Ciência e Tecnologia (FCT-Portugal) under Grant 2022.11452.BD.

References

[1] C. Liang, C. Yu, and X. Wei, "Auth+track: Enabling authentication free interaction on smartphone by continuous user tracking," *Conf. Hum. Factors Comput. Syst. - Proc.*, 2021.

[2] V. Sucasas, G. Mantas, M. Papaioannou, and J. Rodriguez, "Attribute-based pseudonymity for privacy-preserving authentication in cloud services," *IEEE Trans. Cloud Comput.*, vol. 7161, no. c, 2021.

[3] M. Papaioannou *et al.*, "A survey on security threats and countermeasures in Internet of Medical Things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, no. May, pp. 1–15, 2020.

[4] M. Papaioannou, J. C. Ribeiro, V. Monteiro, V. Sucasas, G. Mantas, and J. Rodriguez, "A privacy-preserving user authentication mechanism for smart

city mobile apps," in *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (IEEE CAMAD)*, 2021, pp. 1–5.

[5] I. Essop, J. C. Ribeiro, M. Papaioannou, J. Rodriguez, G. Zachos, and G. Mantas, "Generating datasets for anomaly-based intrusion detection systems in IoT and industrial IoT networks," *Sensors*, vol. 21, no. 4, pp. 1–31, 2021.

[6] F. Pelekoudas-Oikonomou *et al.*, "Blockchain-Based Security Mechanisms for IoMT Edge Networks in IoMT-Based Healthcare Monitoring Systems," *Sensors*, vol. 22, no. 7, 2022.

[7] A. Buriro, B. Crispo, F. DelFrari, and K. Wrona, "Hold and Sign: A novel behavioral biometrics for smartphone user authentication," in *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016*, 2016, pp. 276–285.

[8] S. Gupta, A. Buriro, and B. Crispo, "Demystifying authentication concepts in smartphones: Ways and types to secure access," *Hindawi Mob. Inf. Syst.*, vol. 2018, 2018.

[9] 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," *SOUPS '14 Proc. Tenth Symp. Usable Priv. Secur.*, pp. 213–230, 2016.

[10] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, "Behavioral biometrics & continuous user authentication on mobile devices: A survey," *Inf. Fusion*, vol. 66, no. February 2020, pp. 76–99, 2021.

[11] J. Zhang, X. Luo, S. Akkaladevi, and J. Ziegelmayer, "Improving multiple-password recall: An empirical study," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 165–176, 2009.

[12] G. Ye *et al.*, "Cracking Android Pattern Lock in Five Attempts," 2017.

[13] Verizon, "'How long since you took a hard look at your cybersecurity?,'" 2017.

[14] N. Forsblom, "Were you aware of all these sensors in your smartphone?," 2015. [Online]. Available: https://blog.adtile.me/2015/11/12/wereyou-%0Aaware-of-all-these-sensors-in-your-smartphone/.

[15] A. Buriro, B. Crispo, M. Eskandri, S. Gupta, A. Mahboob, and R. V. and Acker, "Snap auth: a gesture-based unobtrusive smartwatch user authentication scheme," in *International Workshop on Emerging Technologies for Authorization and Authentication*, pp. 30–37.

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

[17] T. Sloane, "'Behavioral biometrics: the restructuring of the authentication landscape,'" 2017. .

[18] B. Schneier, *Applied Cryptography*, vol. 1, no. 32. 1996.

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

[20] C. Braz and J. M. Robert, "Security and usability: The case of the user authentication methods," *ACM Int. Conf. Proceeding Ser.*, vol. 133, pp. 199–203, 2006.

[21] S. G. Belk M., Germanakos P., Fidas C., "A Personalization Method Based on Human Factors for Improving Usability of User Authentication Tasks," *Springer, Cham*, vol. 8538, no. User Modeling, Adaptation, and Personalization. UMAP 2014. Lecture Notes in Computer Science, 2014.

[22] J. Titcomb, "Hackers claim to beat iPhone X's face id in one week with 115 mask," 2017. [Online]. Available: http://www.telegraph.co.uk/technology/2017/11/13/hackers-beat-iphone-xs-face-oneweek-115-mask/. [Accessed: 07-Jan-2023].

[23] S. Kovach, "Business insider-Samsung's Galaxy S8 facial recognition feature can be fooled with a photo," 2017. [Online]. Available: http://www.businessinsider.com/samsung-galaxy-s8-facial-recognitiontricked-with-a-photo-2017-3?IR=T. [Accessed: 07-Jan-2023].

[24] A. Charles, "The guardian-iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club," 2013. [Online]. Available: https://www.theguardian.com/technology/2013/sep/22/apple-iphonefingerprint-scanner-hacked. [Accessed: 10-Jan-2023].

[25] D. McGoogan, C., & Demetriou, "Peace sign selfies could let hackers copy your fingerprints," 2017. [Online]. Available: http://www.telegraph.co.uk/technology/2017/01/12/peace-signselfies-could-let-hackers-copy-fingerprints. [Accessed: 10-Jan-2023].

[26] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, "Key factors driving the adoption of behavioral biometrics and continuous authentication technology: an empirical research," *Inf. Comput. Secur.*, vol. 30, no. 4, pp. 562–582, 2022.

[27] M. Muaaz and R. Mayrhofer, "Smartphone-Based Gait Recognition: From Authentication to Imitation," *IEEE Trans. Mob. Comput.*, vol. 16, no. 11, pp. 3209–3221, 2017.

[28] M. R. Hestbek, C. Nickel, and C. Busch, "Biometric gait recognition for mobile devices using wavelet transform and support vector machines," *2012 19th Int. Conf. Syst. Signals Image Process. IWSSIP 2012*, no. April, pp. 205–210, 2012.

[29] T. Murao, K., Tobise, H., Terada, T., Iso, T., Tsukamoto, M. and Horikoshi, "'Mobile phone user authentication with grip gestures using pressure sensors,'" *Int. J. Pervasive Comput. Commun.*, vol. 11, no. 3, pp. 288–301, 2015.

[30] B. Attaullah, S. Gupta, and B. Crispo, "Evaluation of Motion-based Touch-typing Biometrics in Online Financial Environments," pp. 219–226, 2017.

[31] A. Buriro, S. Gupta, and B. Crispo, "Evaluation of Motion-Based Touch-Typing Biometrics for Online Banking," *Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform.*, 2017.

[32] Y. Obuchi, "Pda speech database," 2006. [Online]. Available: http://www.speech.cs.cmu.edu/databases/pda/index.html.

[33] M. Papaioannou, G. Mantas, D. Lymberopoulos, and J. Rodriguez, "User authentication and authorization for next generation mobile passenger ID devices for land and sea border control," in *12th International Symposium on Communication Systems, Networks and Digital Signal Processing, CSNDSP 2020*, 2020, pp. 8–13.

[34] 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," *Conf. Hum. Factors Comput. Syst. - Proc.*, vol. 2015-April, pp. 1411–1414, 2015.

[35] M. Papaioannou, G. Zachos, I. Essop, G. Mantas, and J. Rodriguez, "Towards a Secure and Usable User Authentication for Mobile Passenger ID Devices for Land/Sea Border Control," *IEEE Access*, vol. 10, pp. 38832–38849, 2022.

[36] A. Acien, A. Morales, R. Vera-Rodriguez, J. Fierrez, and J. V. Monaco, "TypeNet: Scaling up keystroke biometrics," *IJCB 2020 - IEEE/IAPR Int. Jt. Conf. Biometrics*, 2020.

[37] M. Papaioannou, G. Zachos, G. Mantas, and J. Rodriguez, "Novelty Detection for Risk-based User Authentication on Mobile Devices," in *IEEE Global Communications Conference*, 2022, p. Accepted to be published.

[38] M. Papaioannou, G. Mantas, and J. Rodriguez, "Risk-based user authentication for mobile passenger ID devices for land and sea border control," in *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, 2021, pp. 180–185.

[39] M. Papaioannou, G. Mantas, A. Essop, P. Cox, I. E. Otung, and J. Rodriguez, "Risk-based adaptive user authentication for mobile passenger ID devices for land/sea border control," in *IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2021, pp. 1–6.

[40] M. Abuhamad, A. Abusnaina, G. S. Member, D. Nyang, D. Mohaisen, and S. Member, "Sensor-Based Continuous Authentication of Smartphones ' Users Using Behavioral Biometrics : A Contemporary Survey," vol. 8, no. 1, pp. 65–84, 2021.

[41] V. M. 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, 2016.

[42] S. Wiefling, M. Dürmuth, and L. Lo Iacono, "Verify It's You: How Users Perceive Risk-Based Authentication," *IEEE Secur. Priv.*, vol. 19, n, no. December, pp. 47–57, 2021.

[43] S. Wiefling, L. Lo Iacono, and M. and Dürmuth, "Is this really you? An empirical study on risk-based authentication applied in the wild.," in *In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 134-148). Springer, Cham*.

[44] M. Papaioannou, F. Pelekoudas-oikonomou, G. Mantas, E. Serrelis, J. Rodriguez, and M. Fengou, "A Survey on Quantitative Risk Estimation Approaches for Secure and Usable User Authentication on Smartphones," *Sensors 2023*, vol. 23, 2979, 2023.

[45] S. Khan, "Mouse Dynamics Behavioral Biometrics : A Survey," 2022.

[46] S. Ulupinar, S. Dogan, E. Akbal, and T. Tuncer, "The importance of standardization in biometric data for digital forensics," in *2nd International Conference on Computer Science and Engineering*, 2017.

[47] G. Pahuja and T. N. Nagabhushan, "Biometric authentication & identification through behavioral biometrics: A survey," *Proc. - 2015 Int. Conf. Cogn. Comput. Inf. Process. CCIP 2015*, 2015.

[48] S. P. Banerjee and D. Woodard, "Biometric Authentication and Identification Using Keystroke Dynamics: A Survey," *J. Pattern Recognit. Res.*, vol. 7, no. 1, pp. 116–139, 2012.

[49] NIST - National Institute of Standards and Technology, "Standards for Biometric Technologies," 2013. [Online]. Available: https://www.nist.gov/speech-testimony/standards-biometric-technologies. [Accessed: 03-Mar-2023].