Risk Estimation for a Secure & Usable User Authentication Mechanism for Mobile Passenger ID Devices

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

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

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

Najwa Aaraj
Technology Innovation Institute
Abu Dhabi, UAE
Okinawa Institute of Science and Technology
Okinawa, Japan
najwa.aaraj@tii.ae

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

***Abstract*— User Authentication in mobile devices acts as a first line of defense verifying the user´s identity to allow access to the resources of a device and typically was based on ‘‘something the user knows’’, known also as knowledge-based user authentication for several decades. However, recent studies point out that although knowledge-based user authentication has been the most popular for authenticating an individual, nowadays it is no more considered secure and convenient for the mobile user as it is imposing several limitations in terms of security and usability. These limitations stress the need for the development and implementation of more secure and usable user authentication methods. Toward this direction, user authentication based on the ‘‘something the user is’’ has caught the attention. This category includes authentication methods which make use of human physical characteristics (also referred to as physiological biometrics), or involuntary actions (also referred to as behavioral biometrics). In particular, risk-based user authentication based on behavioral biometrics appears to have the potential to increase the reliability of authentication without sacrificing usability. In this context, we focus on the estimation of the risk score, in a continuous mode, of the risk-based user authentication mechanism that we have proposed in our previous work for mobile passenger identification (ID) devices for land/sea border control.**

Keywords*— *risk-based user authentication, risk score estimation, behavioral biometrics-based user authentication, mobile devices

I. INTRODUCTION

Although security and usability in mobile user authentication are often thought of as being contradictory, Risk-Based user Authentication (RBA) method has been extensively proposed in the literature to address this security vs. usability challenge enhancing security without sacrificing usability [1]–[5]. In particular, Risk-Based user Authentication (RBA) method based on behavioral biometrics appears to have the capacity to enhance the whole authentication process´s reliability without interrupting the user’s normal activity by dynamically authenticating a genuine mobile user throughout their entire interaction with the mobile device, based on a risk score computed in real-time [6]–[8]. In our previous publications [1]–[3], [9], we have given: (i) a thorough review of user authentication solutions used in public safety and mobile devices, (ii) the security vs. usability challenge, (iii) the risk-based user authentication concept, as well as (iv) the HuMIdb dataset, which comprises the most recent and publicly available dataset for behavioral user authentication [10], [11].

In our most recent work [1], we have provided a comprehensive work on the design of a risk-based adaptive user authentication mechanism for mobile passenger identification (ID) devices for land/sea border control. The proposed mechanism comprises a secure and usable user authentication solution ensuring continuous user (i.e., officer) authentication behind-the-scenes and invisible to the user (i.e., officer). Specifically, its main objective is to automatically adapt the suitable type of authentication to the specific situation based on a real-time risk score depending on the combination of: i) the user´s contextual information such as device´s ID, and device´s connection, user´s location, date, time, , ii) the user’s behavioral patterns, and iii) the device´s contextual information such as the device’s IP address. The combination of all those traits for estimating the risk score, in a continuous mode, aims to improve the security and usability of our proposed mechanism in [1] given the benefits of behavioral biometrics in user authentication as also discussed in Section II. Therefore, in this paper, our aim is to focus on

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.

the estimation of the risk score, in a continuous mode, within the risk estimation module of Risk Estimation Agent (REA) component of the authentication mechanism that we proposed in [1] and an overview of its architecture is as depicted in Fig. 1.

Following the Introduction, the rest of the paper is organized as follows. Section II provides related work on the three basic types which may serve as a basis for verifying a mobile user's identity: something the user knows, something the user has, and something the user is, presenting their main advantages and disadvantages. Section III focuses on the estimation of the risk score, in a continuous mode, for the proposed authentication mechanism in [1], while Section IV concludes the paper and provides directions for future work.

II. Related Work

User authentication in mobile devices such as the smartphone devices acts as a first line of defense verifying the identity of a user in order to allow access to the device´s resources [6]–[8], [12]–[14]. For several decades, user authentication techniques were employed based on the "something the user knows" paradigm, known also as Knowledge-Based user Authentication (KBA). These techniques include the standard passwords, Android graphical patterns, Personal Identification Numbers (PINs), "shared secrets" or "shared secret questions". [15], [16]. Gupta et al. [4] presented the commonly used ways to authenticate a mobile user and classified numerous types of authentication mechanisms to achieve authentication in smartphones. According to their review article [4], KBA schemes are generally used for one-shot and periodic authentication. More precisely, in one-shot authentication, the user authentication happens only at the beginning of a session and remains valid until the user closes the session or signs off. Consequently, the previously authenticated user has unrestricted access to the mobile device during the whole session. On the other hand, periodic authentication is basically the variant of one-shot authentication with the addition of a default timeout duration. After this timeout duration, the mobile user will be automatically singed out and they will have to re-authenticate themselves to continue having access to the device´s resources. Nonetheless, there are several recent studies [4], [17] in the literature that they have stated that although KBA has been the most popular approach for authenticating an individual, nowadays it is no more considered secure and convenient for the mobile user.

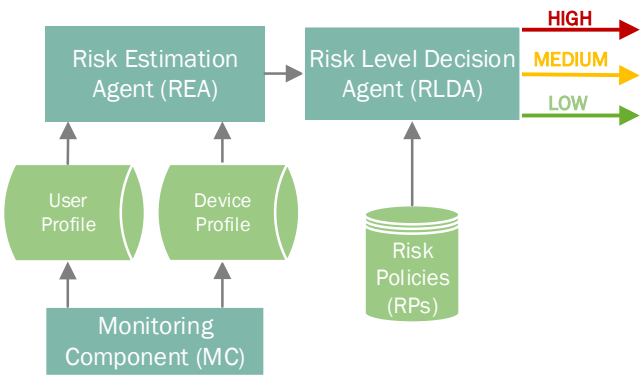

Fig. 1. Overview of the Secure and Usable User Authentication Mechanism Proposed in [1].

First of all, the KBA techniques are not capable of differentiating the legitimate users, instead they authenticate every person (legitimate or not) that holds the valid credentials. On top of this, KBA schemes require mobile users to memorize their credentials in order to unlock their device when needed. Zhang at al. [18] pointed out the difficulties of the users in memorizing and properly recalling their several PINs, passwords or answers to their "shared secret questions" for their different accounts, and stated that as a consequence users choose easy to remember passwords (i.e., the same password for several accounts, or a password composed with their name and date of birth). Therefore, the mobile devices are getting vulnerable and exposed to numerous attacks such as guessing, dictionary, key-logger-based, shoulder-surfing attacks. Additionally, Android users are likely to set easy to memorize graphical patterns for device unlocking, which an attacker could simply observe or guess. For instance, in [19], researchers collected 215 unique graphical patterns from different users, and within just five attempts they managed to crack the 95% of those ''unique'' patterns.

Another popular approach for verifying the identity of a user is user authentication based on the "something the user has" paradigm, known also as Token-Based user Authentication (TBA). This technique typically includes a physical accessory such as smart cards or chipcards, hand-held customized calculators (also known as password generators), magnetic-striped cards, which deliver time-variant passwords and tokens for user authentication purposes. For instance, smartphone applications that handle sensitive user information such as e-banking and e-wallet typically enable two-factor authentication techniques that along with the usual username and password authentication include also one-time passcodes (OTPs) derived from hand-held customized calculators. For such purposes, each user is often supplied with a small security device by the service providers, otherwise the passcode could be sent on the user´s smartphone via SMS [4]. OTP scheme could be easily employed on mobile devices. Furthermore, the user is capable to generate even offline the passcode by using the mobile app offered by the service provider, or with the secure device pairing with another (often wearable) trusted Bluetooth device, such as smartwatches or smartglasses [4]. Nevertheless, OTP schemes are vulnerable to Man-In-The-Middle attacks and Man-In-The-PC/Phone attacks and thus, they do not guarantee the confidentiality of the generated passcodes. As per the Verizon Data Breach Investigations Report [20], the National Institute of Standards and Technology (NIST) does not recommend anymore the two-factor user authentication with OTPs and especially for passcodes sent via SMS [21], as malicious code infesting mobile endpoints could secretly capture second factors (i.e., passcodes) delivered by SMS or offline OTP generated using apps. On top of that, thorough security and usability studies [22], [23] stated that OTP schemes cause more cost to the mobile user and are relatively slower, as they require an additional hardware for the only purpose of authentication. Regarding those security and usability studies, users themselves do not consider the OTP-based authentication a convenient solution. In particular, the analysis in [24] showed that the users were facing various difficulties due to mistyped passcodes for instance.

These limitations stress the need for the design and implementation of more secure and usable user

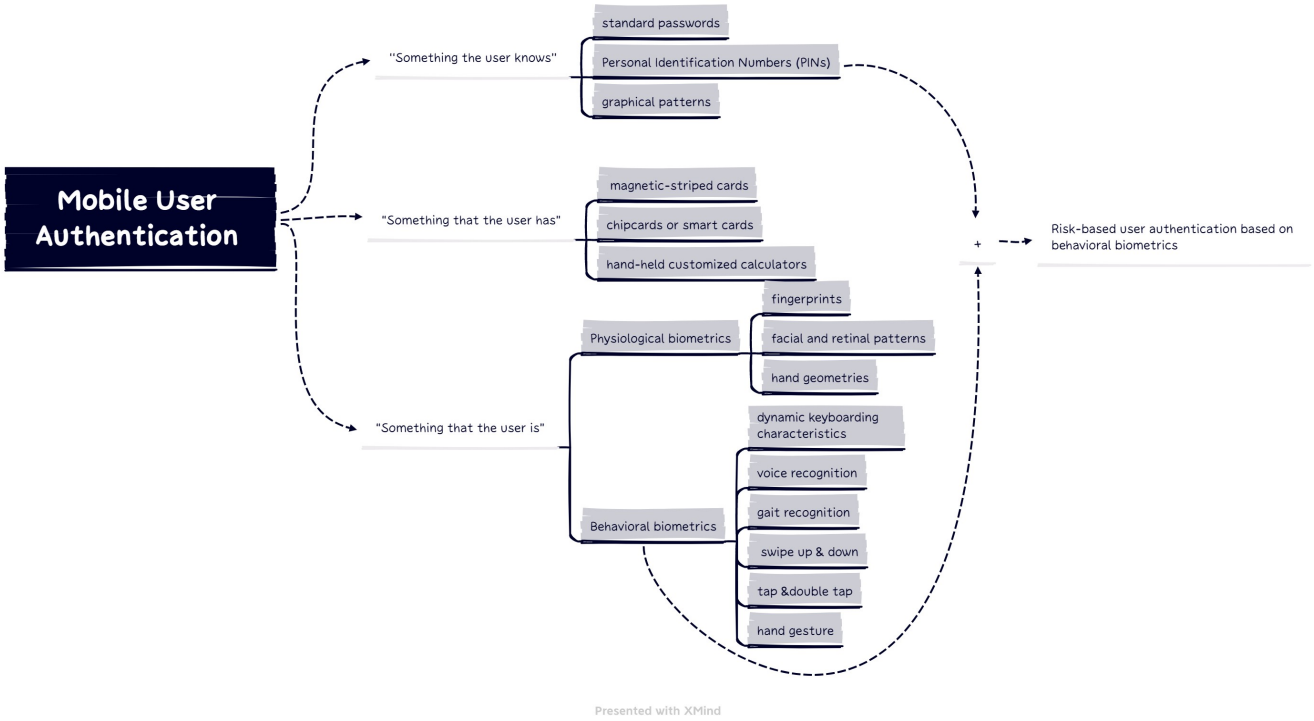

Fig. 2. Visualisation of the Three Basic Types of User Authentication and the Risk-based User Authentication Method.

authentication schemes. Toward this direction, user authentication based on the "something that the user is" paradigm, known also as Biometric-Based user Authentication (BBA), has caught the attention [17]. This category can be further classified as physiological and behavioral biometrics. User authentication mechanisms based on physiological biometrics make use of human physical characteristics such as fingerprints, facial and retinal patterns, as well as hand geometries. The major mobile device manufacturers have already started embedding the corresponding biosensors and developed adequate software to capture these human physical characteristics and utilize them for accurate and convenient user authentication. For instance, Apple, Samsung, Huawei, Nokia, Xiaomi have already developed fingerprint sensors and iris scanners in the majority of their launched smartphones. However, although the physiological biometrics are considered secure as they are unique, they have appeared to be susceptible to several types of attacks including impersonation. More precisely, nowadays, the face of a user could be effortlessly found on various social media websites, while the fingerprint could be easily obtained from specific gestures on photos posted on social media website. As such, researchers have proved that the aforementioned physiological biometric schemes can be hacked effortlessly with not very sophisticated algorithms, as well as with a cheap equipment. For instance, the researcher Isao Echizen from Japan´s National Institute of Informatics (NII) proved that fake fingerprints can be simply extracted from a photo with the peace sign taken just from three meters away, and they can be used to unlock the mobile device impersonating the legitimate user without any sophisticated process [25]. Additionally, the Samsung S8 was unlocked with a simple photo of the legitimate owner [26], while researches hacked the iPhone X Face ID with a 3D printed mask costing around 150 dollars of its owner face [27]. Similarly, the iPhone 5S fingerprint scanner was hacked by the German Chaos Computer Club hacked within two days after Apple launched iPhone 5S worldwide by simply photographing the glass surface with the user´s fingerprint, and afterwards creating fake one in a thin film [28].

On the other hand, BBA might be employed based on user´s involuntary actions, also referred to as behavioral biometrics. This category might include dynamic keyboarding characteristics, voice recognition, swipe up and down and gait recognition [16], [4]. The authors in [29] emphasize that the behavioral biometrics can be effortlessly collected all by the typical sensors of the mobile device, namely, gyroscope, accelerometer, microphone and touch screen [29]–[32], on the contrary to the physiological biometrics that require special hardware and/or software equipment to capture physiological biometrics only for authentication purposes. Therefore, the behavioral biometrics are starting to get attention as they appear to be cost-effective; they do not need any additional hardware equipment, as well as they are considered to be lightweight in the implementation [15]. For instance, the touch-based solutions such as keystroke or swipe, are able to authenticate the users unobtrusively based on their interactions with the mobile device. Moreover, the behavioral biometrics are considered secure and precise given the fact that they are unique and they cannot be copied, shared, stolen or lost [4]. On top of that, they can be combined with another authentication means (e.g., KBA schemes) for establishing multifactor authentication to enhance the overall security of the mobile device [33]. In other words, the behavioral biometrics-based mechanisms can enhance the existing authentication mechanisms

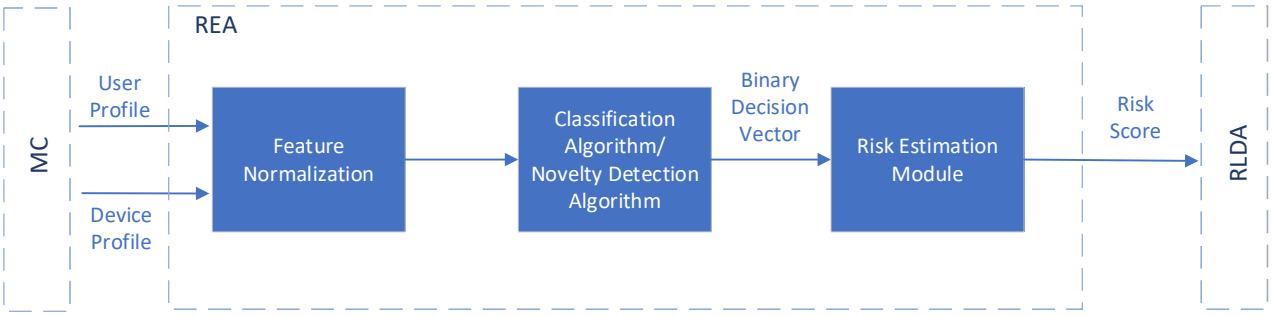

Fig. 3. An Overview of the Risk Score Estimation for the Proposed Secure and Usable User Authentication Mechanism for Mobile Passenger ID Devices for Land/Sea Border Control in [1].

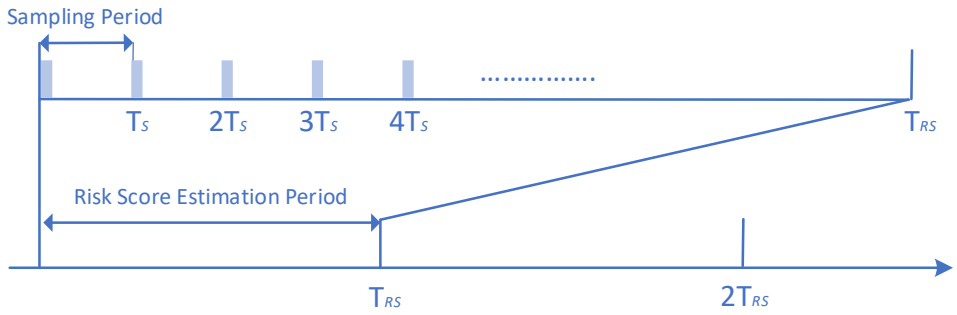

Fig. 4. Illustration of the Sampling Period *Ts* the Risk Score (RS) Estimation Period T_{RS}.

without affecting the usage of the device, working as an additional transparent authentication layer [34]–[36]. Research efforts have been already started in behavioral biometric modalities such as voice and gait recognition, keystroke or touch dynamics. It is expected that such mechanisms will restructure the authentication landscape in the following years and thus, security experts have already focused on developing and implementing such mechanisms [4], [37], [38]. A visualisation of the three basic types of user authentication and the risk-based user authentication method is given in Fig. 2.

III. Risk Score Estimation

The Risk Estimation Agent (REA) component, as depicted in Fig. 3, of the proposed secure and usable user authentication mechanism in [1], firstly, performs data normalization to the input data (i.e., user profile and device profile) to make sure that features with substantially large values do not outweigh features with smaller values. According to [1], the Monitoring Component (MC), as depicted in Fig. 3, updates the user profile and the device profile (i.e., input data), and forwards them to REA every sampling period *Ts*, where te data normalization process (i.e., Feature Normalization) takes place Afterward, the REA component employs classification algorithms and/or novelty detection algorithms on the normalized input data to classify each entry of the normalized data as legitimate or malicious. More precisely, for each entry, the algorithm outputs either 0 (i.e., legitimate user) or 1 (i.e., malicious user). Hence, the output is a binary vector, the length of which, is equal to the number of the normalized entries. This vector is then fed to the risk estimation module, as depicted in Fig. 3, that calculates the risk score, in a continuous mode, for a given period of time T_{RS} (i.e., an illustration of the introduced periods *Ts* and T_{RS} is given in Fig. 4). Denoting the output (binary) vector of the classification and/or novelty detection algorithms as $y \epsilon R^{m\,x\,1}$, the risk score (i.e, $P_0(k) \epsilon [0,1]$) in a period k (e.g., T_{RS}, $2T_{RS}$) can be calculated as follows [34], [35], [39]:

$$P_0(k) = \frac{\sum_{i=1}^{m} y_i}{\mathrm{m}} A \tag{1}$$

Here, A denotes the accuracy of the classification algorithms and/or novelty detection algorithms, which is defined as follows:

$$A = \frac{TP + TN}{TP + TN + FP + FN} \tag{2}$$

where:

- True Positive (TP) is the number of malicious users (i.e., positive entries) that are correctly classified.
- True Negative (TN) is the number of legitimate users (i.e., negative entries) that are correctly classified.
- False Positive (FP) is the number of legitimate users (i.e., negative entries) that are wrongly classified as malicious users (i.e., positive entries).
- False Negative (FN) is the number of of malicious users (i.e., positive entries) that are wrongly classified as legitimate users (i.e., negative entries).

Afterwards, the risk score is forwarded to Risk Level Decision Agent (RLDA) component, as depicted in Fig. 3,

that compares the received risk score with the risk level thresholds stored in RLDA to decide whether the estimated risk score is low, medium, or high.

IV. Conclusions and Future Work

User Authentication in mobile devices such as the smartphone devices acts as a first line of defense verifying the identity of a user in order to allow access to the device´s resources and was based on the ‘‘something the user knows’’ paradigm for several decades. However, recent studies showed that although knowledge-based user authentication has been the most popular for authenticating an individual, nowadays it is no more considered secure and convenient for the mobile user as it is imposing several limitations in terms of security and usability, and thus, there is a need for the development and implementation of more secure and usable user authentication methods. Toward this direction, user authentication based on the ‘‘something the user is’’ has caught the attention. This category includes the physiological biometrics and the behavioral biometrics. In particular, risk-based user authentication based on behavioral biometrics appears to have the potential to increase the reliability of mobile authentication without sacrificing usability.

In our previous publications [1]–[3], [9], we have presented: (i) a comprehensive review of related work on user authentication solutions for public safety and mobile devices, (ii) the security vs. usability challenge, (iii) the concept of the risk-based user authentication, as well as (iv) the HuMIdb dataset. In our most recent work [1], we have provided a thorough work on the design of a risk-based adaptive user authentication mechanism that comprises a secure and usable user authentication mechanism for mobile passenger identification (ID) devices for land/sea border control ensuring continuous user (i.e., officer) authentication behind-the-scenes and invisible to the user (i.e., officer). In this paper, our focus was on the estimation of the risk score, in a continuous mode, within the REA component of the our proposed authentication mechanism in [1].

Our next steps, first of all, include evaluation of other classification algorithms, as well as novelty detection algorithms for risk-based adaptive authentication to identify the most appropriate ones in terms of accuracy for our proposed authentication mechanism in [1]. Afterwards, the next step will be focused on the risk estimation module within the REA component of the proposed authentication mechanism. It is intended to implement and evaluate not only the risk estimation algorithm proposed in this paper, but also to investigate more risk estimation algorithms proposed in the literature for risk-based adaptive authentication in order to identify the most efficient ones for the REA component of our proposed authentication mechanism in [1]. Lastly, we are aiming to implement the proposed risk-based adaptive user authentication mechanism and evaluate its performance on the mobile devices for passenger identification at land and sea borders. As a mobile device for this implementation, we will cosider a Raspberry pi 4 with Android OS.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] A. Acien, A. Morales, J. Fierrez, R. Vera-Rodriguez, and I. Bartolome, “BeCAPTCHA: Detecting human behavior in smartphone interaction using multiple inbuilt sensors,” *arXiv Prepr. arXiv2002.00918*, 2020.

[11] A. Acien, A. Morales, J. Fierrez, R. Vera-Rodriguez, and O. Delgado-Mohatar, “BeCAPTCHA: Bot detection in smartphone interaction using touchscreen biometrics and mobile sensors,” *arXiv Prepr. arXiv2005.13655*, no. May, 2020.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

[18] 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.

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

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

[21] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "NIST 800-63-3: Digital Identity Guidelines," *NIST Spec. Publ.*, p. 68, 2017.

[22] 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.

[23] T. Zink and M. Waldvogel, "X.509 user certificate-based two-factor authentication for web applications," *Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform.*, vol. 271, 2017.

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

[25] D. McGoogan, C., & Demetriou, "Peace sign selfies could let hackers copy your fingerprints," 2017. .

[26] S. Kovach, "Business insider-Samsung's Galaxy S8 facial recognition feature can be fooled with a photo," 2017.

[27] J. Titcomb, "Hackers claim to beat iPhone X's face id in one week with 115 mask," 2017.

[28] A. Charles, "'The guardian-iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club,'" 2013. .

[29] 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/.

[30] S. Gupta, R. Kumar, M. Kacimi, and B. Crispo, "IDeAuth: A novel behavioral biometric-based implicit deauthentication scheme for smartphones," *Pattern Recognit. Lett.*, vol. 157, no. March, pp. 8–15, 2022.

[31] 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.

[32] 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.

[33] G. Mantas, N. Komninos, J. Rodriguez, E. Logota, and H. Marques, "Security for 5G Communications," in *Fundamentals of 5G Mobile Networks, J. Rodriguez*, L. Eds., John Wiley & Sons, Ed. Chichester, UK, 2015, pp. 207–220.

[34] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, and R. A. Abd-Alhameed, "HIDROID: Prototyping a behavioral host-based intrusion detection and prevention system for android," *IEEE Access*, vol. 8, pp. 23154 – 23168, 2020.

[35] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, S. J. Shepherd, and R. A. Abd-Alhameed, "An Autonomous Host-Based Intrusion Detection System for Android Mobile Devices," *Mob. Networks Appl.*, vol. 25, no. 1, pp. 164–172, 2020.

[36] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, S. J. Shepherd, and R. A. Abd-Alhameed, "Towards an autonomous host-based intrusion detection system for android mobile devices," in *9th EAI International Conference on Broadband Communications, Networks, and Systems (BROADNETS2018)*, 2018, pp. 139–148.

[37] 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.

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

[39] P. Borges *et al.*, "Towards a Hybrid Intrusion Detection System for Android-based PPDR Terminals," in *Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM): Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2017)*, 2017, pp. 1034–1039.