# Novelty Detection for Risk-based User Authentication on Mobile 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 Zachos
*Instituto de Telecomunicações*
Aveiro, Portugal
*Faculty of Engineering and Science, University of Greenwich*
Chatham Maritime, UK
g.zachos@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

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 acts as the first line of defense verifying the identity of a mobile user, often as a prerequisite to allow access to resources in a mobile device. For several decades, user authentication was based on the ‘‘something the user knows’’, known also as knowledge-based user authentication. Recent studies state 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. 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 mobile authentication security without sacrificing usability. In this context, we, firstly, present an overview of user authentication on mobile devices and discuss risk-based user authentication for mobile devices as a suitable approach to deal with the security vs. usability challenge. Afterwards, a set of novelty detection algorithms for risk estimation is tested and evaluated to identify the most appropriate ones for risk-based user authentication on mobile devices.**

***Keywords— novelty detection, risk-based user authentication, behavioral biometric-based user authentication, mobile devices***

## I. INTRODUCTION

Authentication acts as the first line of defense verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. In mobile devices such as smartphone devices, user authentication is essential to protect smartphone users’ data privacy [1]–[6]. For several decades, user authentication was based on the “something the user knows” paradigm, known also as knowledge-based user authentication including standard passwords, Personal Identification Numbers (PINs), graphical patterns etc. [7], [8]. According to Gupta et al. [9], knowledge-based user authentication schemes are generally used as one-shot authentication in which the user authentication happens only at the beginning of a session and remains valid until the user closes the session or signs off. Therefore, the once authenticated user has unlimited access to the device during the whole session. Nevertheless, recent studies [9]–[11] state that although knowledge-based user authentication has been the most popular for authenticating an individual, nowadays it is no more considered secure and convinient for the mobile user. First of all, these conventional techniques are not able to distinguish the legitimate users, rather they authenticate every person holding the valid credentials. Regardless of this, users are required to memorize their credentials to be able to unlock the device when needed. Zhang at al. [12] describe the users´ difficulties in memorizing and correctly recalling the several passwords for their different accounts. As a result, users select easy to remember passwords making the mobile devices vulnerable and exposing them to numerous attacks such as. dictionary, key-logger-based, shoulder-surfing, and guessing attacks. In addition, in the case of Android mobile devices, users tend to set simple to memorize graphical patterns for device unlocking, which an attacker could easily guess or observe. For instance, in [13], researchers collected 215 unique graphical patterns from different users, and within just five attempts they managed to crack the 95% of those ‘‘unique’’ patterns.

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 that the user is” paradigm has caught the attention [11]. This category includes methods which make use of human physical characteristics (also referred to as physiological biometrics) such as fingerprints, facial and retinal patterns, hand geometries, or involuntary actions (also referred to as behavioral biometrics), such as dynamic keyboarding characteristics, and gait recognition [8], [9]. Considering a smartphone device, the authors in [14] highlight that special hardware and/or software equipment is required to capture physiological biometrics only for authentication purposes. On the other hand, the behavioral biometrics can be effortlessly collected all by the sensors of the mobile device, namely, gyroscope, accelerometer, microphone and touch screen [14]–[17]. 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

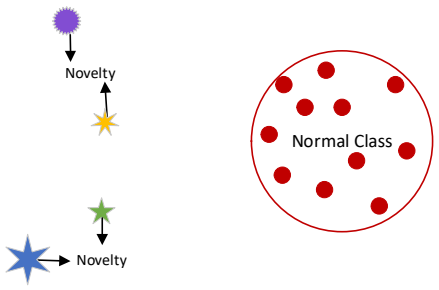


Fig. 1. Visualisation of Novelty Detection.

considered to be lightweight in the implementation [7]. For instance, the touch-based solution such as swipe or keystroke, manage to authenticate the users unobtrusively based on their interactions with the device. Furthermore, the authentication mechanisms based on behavioral biometrics are considered secure and accurate since they are unique and they cannot be shared, copied, lost or stolen [9]. On top of that, they can be combined with another authentication means (e.g., knowledge-based schemes) for establishing multifactor authentication in order to improve the accuracy and enhance the overall security of the mobile device. In other words, the behavioral biometric-based schemes can work as an additional transparent authentication layer, that enhance the existing authentication mechanisms without affecting the usage of the device [18]–[20]. Research efforts have been already started in gait recognition, keystroke or touch dynamics and voice recognition behavioral biometric modalities. As such, security experts are focusing on developing such mechanisms as they seem that they will restructure the authentication landscape in the following years [9], [21].

In particular, risk-based user authentication based on behavioral biometrics appears to have the potential to increase mobile authentication security without sacrificing usability [22], [23]. Risk-based type of user authentication mechanisms has been proposed to dynamically authenticate a legitimate mobile user throughout their entire interaction with the mobile device, based on a risk score computed in real-time, enhancing the reliability of whole authentication process without interrupting the user's normal activity [9]. In our previous publications [24]–[27], 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, which, to the best of our knowledge, is the most recent and publicly available dataset for behavioral user authentication [28], [29]. In our more recent work [27], we have provided a thorough work on the design of a risk-based adaptive user authentication mechanism that comprises a novel secure and usable user authentication solution ensuring continuous user authentication behind-the-scenes and invisible to the user. Particularly, its main objective is to automatically adapt the authentication requirements and 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 user´s location, date, time, device´s ID, and device´s connection, ii) the user's behavioral patterns, and iii) device contextual information such as the device's IP address. The combination of all those traits for estimating the risk score aims to improve the accuracy and enhance the security of the mobile device given the benefits of biometrics in user authentication discussed previously.

On top of that, in [27], we also modified adequately the ''HuMIdb'' dataset files, and we trained and tested the following most popular classification algorithms for risk-based authentication: K-NN, DT, SVM, and NB over the ''HuMIdb'' dataset using ten-fold cross validation. However, the evaluation results demonstrated impact of overfitting and therefore, we considered the concept of novelty detection to overcome this challenge. Thus, we tested and evaluated the following novelty detection algorithms: one-class Support Vector Machine (OneClassSVM), Local Outlier Factor (LOF), and KNN_average (i.e., KNN configured properly for novelty detection). All of them demonstrated a high performance for the same part of the ''HuMIdb'' dataset that was also used for the evaluation of the classification algorithms, when applied to distinguish between a known legitimate user and an unknown malicious user. To the best of our knowledge, this was the first time that novelty detection algorithms have been considered for risk-based adaptive user authentication demonstrating promising results. In the current paper, our aim is to investigate further the concept of novelty detection for risk-based user authentication and thus, we target to test more novelty detection algorithms found in the literature and evaluate to identify the most appropriate ones that can also be applied to the proposed mechanism in [27].

Following the Introduction, the rest of the paper is organized as follows. Section II presents related work of the most popular novelty detection algorithms for behavioral biometric-based user authentication, while Section III presents the performance evaluation of those novelty detection algorithms. Finally, the paper is concluded in Section V.

## II. Novelty Detection Algorithms For Risk-Based User Authentication

Many applications including user authentication for mobile devices require being able to decide whether a new observation is an inlier which means that it belongs to the same distribution as existing observations or should be considered as an outlier (i.e., different from the existing observations) [30]. According to [30], in novelty detection, the training data is not polluted by outliers, and we are interested in detecting whether a new observation is an outlier (i.e., a novelty). Novelty detection is also known as semi-supervised anomaly detection.

The case of risk-based user authentication based on behavioral biometrics typically involves single-user mobile devices where there is need for distinction between a known legitimate user and an unknown malicious user. Toward this direction and based on the literature [15], [31], [32], novelty detection algorithms, which also referred to as one-class classifiers [15], [31], [32], have caught the researcher´s attention showing significant advantages for user

authentication based on behavioral biometrics. In particular, in [32], the authors stated that one-class classifiers and especially the one-class SVM has been applied to solve a variety of authentication problems, including face recognition, touch and mouse dynamics typist recognition, smart-stroke. Antal et al. [33] used four one-class classifiers, namely Parzen density estimator, kNN_average (i.e., kNN configured properly for novelty detection), Gaussian mixtures method and Support Vector Data Description method to build their authentication model based on swipe gestures. Moreover, the swipe gestures and micro-movements of the device were collected in a constrained environment under a very specific scenario – while responding to psychological questionnaire. The kNN_average and Parzen density estimator achieved mean Equal Error Rate (EER) as low as 0.024, and 0.023 after combining the decisions from successive swipe gestures.

Antal et al. [34] also compared one-class classifiers and multi-class classifiers for keystroke-based user authentication on mobile devices and demonstrated that multi-class classifiers outperformed one-class classifiers with 4% of error rate difference. Gupta et al. [15], after studying the state-of-the-art and an exploratory data analysis of their collected dataset, selected the following one-class classifiers to train their IDeAuth system: Isolation Forest (IF), Support Vector Method (SVM), Local Outlier Factor (LOF), and Minimum Covariance Determinant (MCD). Their selection criteria included the diversity of the classifier's learning paradigm, classification efficiency for platforms with limited computing power, nominal memory space consumption, and proven ability to deal with similar sensory data. Their proposed scheme IDeAuth achieved an HTER of $\approx$ 4% using a decision level fusion, with an improvement of $\approx$ 1% on the MCD that yields the best individual performance. The HTERs for the MCD, LOF, IF, and SVM classifiers, trained with 20 Singular Value Decomposition (SVD) components, are 5.25%, 6.89%, 7.28%, and 9.06%, respectively. Shen et al. [35] applied SVM-, Neural Network-, and KNN-based one-class classifiers on the mouse-usage patterns. They report the Half Total Error Rates (HTER) of $\sim$ 8%, $\sim$ 15%, and $\sim$ 15% respectively on a dataset of 5550 mouse-operation samples collected from 37 subjects. Also, they strongly argued that one-class classifiers are more suitable for user authentication in real-world applications.

In fact, the main advantage of one-class novelty detection algorithms is that they do not require samples from the impostors' class, and thus only genuine samples are required to the models. Thus, the general lack of available data for behavioral biometrics, combined with the fast evolution of the data acquisition quality of mobile computing devices makes novelty detection, a semi-supervised method, a suitable modelling strategy for risk-based user authentication based on behavioral biometrics. Supervised models are challenging to utilize in a real-world user authentication application as negatively labelled samples are not available in sufficient quantities per-user. Based on our recent work [27], we also found out that novelty detection algorithms considered for risk-based adaptive user authentication demonstrated promising results and outperformed popular Machine Learning (ML) classification algorithms for risk-based authentication, namely k-Nearest Neighbor (k-NN), Decision Tree (DT), Support Vector Machine (SVM), and Naïve Bayes (NB), which demonstrated impact of overfitting (i.e., accuracy: 1,0000).

## III. Performance Evaluation of Novelty Detection Algorithms for Risk-Based User Authentication

Further to our recent work [27], we evaluated the performance of more novelty detection algorithms as this type of ML algorithms could be more suitable to be run on the risk estimation component of the proposed mechanism in [27]. The algorithms that we evaluated in this work, along with their respective used Python libraries, are the following: (i) Deep One-Class Classification (DeepSVDD), (ii) Gaussian Kernel Density Estimation (G_KDE), (iii) Parzen window Kernel Density Estimation (PW_KDE), and (iv) Bayesian Gaussian Mixture Model (B_GMM). These algorithms are the most popular novelty detection algorithms for behavioral biometric-based user authentication in the literature [15], [31]–[35].

Using ten-fold cross validation, we trained the novelty detection algorithms over the first user (i.e., user000) of the HuMIdb dataset, while we tested the novelty detection algorithms over the first user (i.e., user000) and second user (i.e., user001) of the HuMIdb dataset [28], [29]. It is worthwhile mentioning that the first user (i.e., user000) and the second user (i.e., user001) were considered as a benign and malicious user, respectively. In addition, the ``HuMIdb" dataset was modified by removing all features related to bluetooth, gps, wifi, micro, humidity, proximity, temperature, and light in the "HuMIdb" dataset files. This was because these features: (i) suffered from lack of values, (ii) contained alphanumeric values that did not allow further processing, or (iii) were closely related to specific device characteristics (e.g., MAC address) whose values were always fixed. In the rest of this section, we will refer to this part of the dataset as "HuMIdb" dataset. The performance of the novelty detection algorithms was evaluated by the evaluation metrics of accuracy, precision, recall, and F1-score. Among the four novelty detection algorithms, three of them demonstrated an extremely high performance for the "HuMIdb" dataset.

### *A. Dataset pre-processing and normalization*

Technically, it is required to properly prepare the available datasets before they are employed to train and test novelty detection algorithms. In principle, data preparation involves two processes: a) data pre-processing; and b) data normalization. During pre-processing, the removal of unnecessary features and the conversion of the nominal values of the categorical features to numeric values take place. Nevertheless, in our situation, there were no redundant features which were required to be removed, as well as the values of all features were already numeric. Therefore, the data pre-processing process was omitted for the "HuMIdb" dataset that was chosen for training and testing the novelty detection algorithms. Alternatively, the data normalization process was performed to the numeric values of each feature. Generally, when the values of a feature are significantly

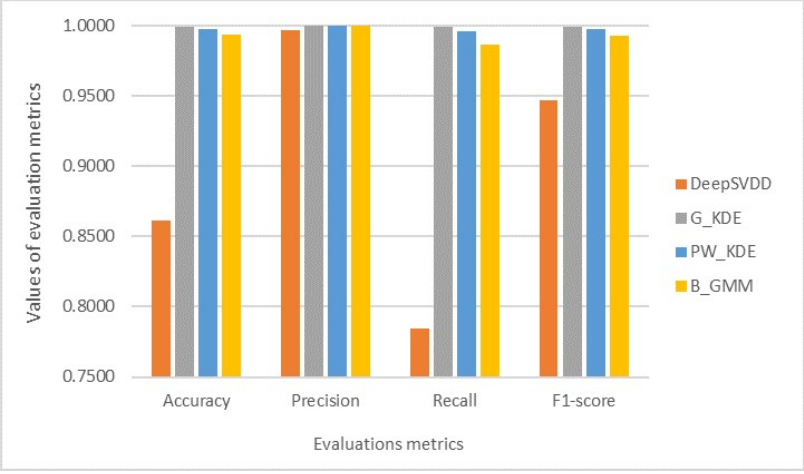


Fig. 2. Evaluation metrics for novelty detection for the ``HuMIdb'' dataset.

TABLE I. SUMMARY OF THE HYPERPARAMETERS OF EACH NOVELTY DETECTION ALGORITHM.

| Algorithm | Hyperparameters |
|---|---|
| DeepSVDD | The value of the "contamination" parameter was set to 0.00001. |
| G_KDE | 1) The value of the "bandwidth" parameter was set to 0.2.<br>2) The value of the "kernel" parameter was set to "gaussian". |
| PW_KDE | 1) The value of the "bandwidth" parameter was set to 0.5.<br>2) The value of the "kernel" parameter was set to "tophat". |
| B_GMM | The value of the "n_components" parameter was set to 1. |

larger compared to the values of other features, the results of the algorithms might be inaccurate. Consequently, data normalization is necessary in order to make sure that features with smaller values will not be outweighed by features with significantly large values. To achieve this, we performed a min-max normalization process on each feature in order to ensure that all of the features' values are scaled within the range of [0.0, 1.0]. This normalization process is described by the following equation:

$$z = (x - x_{min}) / (x_{max} - x_{min}) \quad (1)$$

where z is the normalized value (i.e., after scaling), x is the value before scaling, and $x_{max}$ and $x_{min}$ are the maximum and minimum values of the feature, respectively.

### B. *Training process of novelty detection algorithms*

The novelty detection algorithms were trained and tested over the HuMIdb dataset. Initially, the dataset was divided into two parts: (i) the train part which was consisted of 80% of the dataset and (ii) the test part which was consisted of 20% of the dataset. The train part was utilized to train and evaluate the novelty detection algorithms, while, on the other hand, the test part was held back for further evaluation of the models with unseen data. The percentage split of 80% train data-20% test data was defined according to [36], where the author suggested it as the best ratio to avoid the overfitting problem. Afterwards, the training process of each novelty detection algorithm over each dataset was performed using the ten-fold cross validation method. According to this method, the training dataset is split into ten subsets of equal size and the records of each subset are randomly chosen. The training process is repeated ten times. Each time, nine of the ten subsets are utilized for the training of the novelty detection algorithms and the remaining subset is used for validation.

TABLE II. EVALUATION METRICS FOR NOVELTY DETECTION FOR THE ``HUMIDB'' DATASET.

| Algorithm | Accuracy | Precision | Recall | F1-Score |
|---|---|---|---|---|
| DeepSVDD | 0.86 | 0.99 | 0.78 | 0.95 |
| G_KDE | 0.99 | 1.00 | 0.99 | 0.99 |
| PW_KDE | 0.99 | 1.00 | 0.99 | 0.99 |
| B_GMM | 0.99 | 1.00 | 0.99 | 0.99 |

In our tests, we used the Python language version 3.9.7, along with the Scikit-Learn [37] library and the PyOD [38] library. We used specific functions of the Scikit-Learn library and the PyOD library, and a Python script was developed utilizing these functions in order to perform the training and testing of the four selected novelty detection algorithms. Additionally, it is worthwhile to mention that three of the four novelty detection algorithms (i.e., G_KDE, PW_KDE, B_GMM) are implemented in Scikit in a way so that for a new sample, the trained novelty detection algorithm is capable of computing the log-likelihood of the new sample. The log-likelihood is a number in the range of $(-\infty, +\infty)$ with higher values signifying that the new sample is more similar to the samples that were used for training the algorithm. In our experiment, our python script set zero as the threshold point, meaning that when the computed log-likelihood of a new sample is equal or higher than zero, the new sample was classified as a normal sample. Otherwise, when the computed log-likelihood of a new sample is lower than zero, the new sample was classified as a malicious sample.

### C. Performance evaluation results

The performance results of the novelty detection algorithms were produced by averaging the results of the ten folds [36]. Table I presents the summary of the hyperparameters of each novelty detection algorithm. The numerical results of the evaluation metrics for the selected novelty detection algorithms, when applied to the "HuMIdb" dataset, are shown in Table II and Figure 2.

It can be easily observed that among the four novelty detection algorithms, three of them (i.e., G_KDE, PW_KDE, B_GMM) demonstrate an extremely high performance for the "HuMIdb" dataset. These three novelty detection algorithms are accurate almost in all cases (i.e., 0,99), followed by the DeepSVDD methods (i.e., 0,86). As far as the rest of the evaluation metrics (i.e., precision, recall, and F1-score), the same three algorithms (i.e., G_KDE, PW_KDE, B_GMM) continue to demonstrate better performance compared to the DeepSVDD algorithm.

## IV. Conclusions and Future Work

User authentication acts as the first line of defense verifying the identity of a mobile user, often as a prerequisite to allow access to resources in a mobile device and typically was based on the ''something the user knows'', known also as knowledge-based user authentication 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, 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 mobile authentication security without sacrificing usability.

In our previous publications [24]–[27], 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 more recent work [27], we have provided a thorough work on the design of a risk-based adaptive user authentication mechanism that comprises a novel secure and usable user authentication solution ensuring continuous user authentication behind-the-scenes and invisible to the user. On top of that, we also modified adequately the ''HuMIdb'' dataset files, and we trained and tested the following most popular classification algorithms for risk-based authentication: K-NN, DT, SVM, and NB over the ''HuMIdb'' dataset using ten-fold cross validation. However, the evaluation results demonstrated impact of overfitting and therefore, we considered the concept of novelty detection to overcome this challenge. Thus, we tested and evaluated the following novelty detection algorithms: one-class Support Vector Machine (OneClassSVM), Local Outlier Factor (LOF), and KNN_average (i.e., KNN configured properly for novelty detection). All of them demonstrated a high performance for the same part of the ''HuMIdb'' dataset that was also used for the evaluation of the classification algorithms, when applied to distinguish between a known legitimate user and an unknown malicious user. To the best of our knowledge, this was the first time that novelty detection algorithms have been considered for risk-based adaptive user authentication demonstrating promising results. In the current paper, our aim was to investigate further the concept of novelty detection for risk-based user authentication and thus, we target to test more novelty detection algorithms found in the literature and evaluate them to identify the most appropriate ones that can also be applied to our proposed mechanism.

Therefore, we trained and tested four more novelty detection algorithms over the "HuMIdb" dataset to identify the most appropriate ones for risk-based user authentication on mobile devices. It is worthwhile to highlight that three of the four novelty detection algorithms showed an almost perfect performance. Our next step is to continue training and test novelty detection algorithms over the training part of the "HuMIdb" dataset (i.e., 80% part) using 10-fold cross validation along with different combination of hyperparameters for each novelty detection algorithm in order to determine the best hyperparameters for each algorithm. After the best hyperparameters have been identified for each novelty detection algorithm, we will perform one final performance evaluation over the withheld part of the "HuMIdb" dataset (i.e., 20% part) in order to acquire more realistic performance metrics over unseen data.

## 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.

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] G. Ye *et al.*, “Cracking Android Pattern Lock in Five Attempts,” 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] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] T. Sloane, “‘Behavioral biometrics: the restructuring of the authentication landscape,’” 2017. .

[22] 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.

[23] 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*.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] scikit-learn developers, “Novelty and Outlier Detection.” [Online]. Available: https://scikit-learn.org/stable/modules/outlier_detection.html.

[31] J. Kim, H. Kim, and P. Kang, “Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection,” *Appl. Soft Comput. J.*, vol. 62, pp. 1077–1087, 2018.

[32] R. Kumar, P. P. Kundu, and V. V. Phoha, “Continuous authentication using one-class classifiers and their fusion,” *2018 IEEE 4th Int. Conf. Identity, Secur. Behav. Anal. ISBA 2018*, vol. 2018-Janua, pp. 1–8, 2018.

[33] M. Antal and L. Z. Szabó, “Biometric Authentication Based on Touchscreen Swipe Patterns,” *Procedia Technol.*, vol. 22, no. October 2015, pp. 862–869, 2016.

[34] M. Antal and L. Z. Szabo, “An evaluation of one-class and two-class classification algorithms for keystroke dynamics authentication on mobile devices,” *Proc. - 2015 20th Int. Conf. Control Syst. Comput. Sci. CSCS 2015*, pp. 343–350, 2015.

[35] C. Shen, Z. Cai, X. Guan, Y. Du, and R. A. Maxion, “User authentication through mouse dynamics,” *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 1, pp. 16–30, 2013.

[36] A. Géron, *Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow: Concepts, tools, and techniques to build intelligent systems.* O’Reilly Media, 2019.

[37] F. Pedregosa *et al.*, “Scikit-learn: Machine learning in python,” *J. Mach. Learn. Res.*, vol. 12, no. 85, pp. 2825–2830, 2011.

[38] Y. Zhao, Z. Nasrullah, and Z. Li, “PyOD: A python toolbox for scalable outlier detection,” *J. Mach. Learn. Res.*, vol. 20, no. 96, pp. 1–7, 2019.