IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 15, 2022, accepted March 29, 2022, date of publication April 1, 2022, date of current version April 15, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3164245

Toward a Secure and Usable User Authentication Mechanism for Mobile Passenger ID Devices for Land/Sea Border Control

MARIA PAPAIOANNOU[1,2], (Student Member, IEEE), GEORGIOS ZACHOS[1,2], (Student Member, IEEE), ISMAEL ESSOP[2], GEORGIOS MANTAS[1,2], (Member, IEEE), AND JONATHAN RODRIGUEZ[1,3], (Senior Member, IEEE)

[1]Instituto de Telecomunicações, 3810-193 Aveiro, Portugal
[2]Faculty of Engineering and Science, University of Greenwich, Chatham Maritime ME4 4TB, U.K.
[3]Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd CF37 1DL, U.K.

Corresponding author: Maria Papaioannou (m.papaioannou@av.it.pt)

This work was supported by the European Union's Horizon 2020 Research and Innovation Programme under Agreement H2020-MSCA-RISE-2019-eBORDER-872878.

ABSTRACT Nowadays the critical sector of transport becomes progressively more dependent on digital technologies to perform essential activities and develop novel efficient transport services and infrastructure to empower economic and social cohesion exploiting the economic strengths of the European Union (EU). However, although the continuously increasing number of visitors, entering the EU through land-border crossing points or seaports, brings immense economic value, novel border control solutions, such as mobile devices for passenger identification for land/sea border control, are essential to precisely identify passengers ''on the fly'' ensuring their comfort. Nevertheless, these devices are expected to handle highly confidential personal data and thus, it is very likely to become an attractive target to malicious actors. Therefore, to ensure high level of device security without interrupting border control activities, strong secure and usable user authentication mechanisms are required. Towards this direction, we, firstly, discuss risk-based and adaptive authentication for mobile devices as a suitable approach to deal with the security vs. usability challenge and a novel risk-based adaptive user authentication mechanism is proposed to address this challenge. Afterwards, a set of popular Machine Learning (ML) classification algorithms for risk-based authentication was tested and evaluated on the HuMIdb (Human Mobile Interaction database) dataset to identify the most appropriate ones for the proposed mechanism. The evaluation results demonstrated impact of overfitting (i.e., accuracy: 1,0000) and therefore, we considered novelty detection algorithms to overcome this challenge and demonstrate high performance. To the best of our knowledge, this is the first time that novelty detection algorithms have been considered for risk-based adaptive user authentication showing promising results (OneClassSVM 0,9536, LOF 0,9740, KNN_average 0,9998).

INDEX TERMS Adaptive user authentication, border control security, mobile passenger ID devices, risk-based user authentication.

I. INTRODUCTION

Innovative services and products are progressively becoming integral parts of our day-to-day lives in a wide spectrum of applications. Nevertheless, with every advancement towards the connectivity of people, things, and processes, our dependence on technology rises, and so too does our exposure to risks from cyber, underlining the importance of cybersecurity in our daily lives [1], [2]. Specifically, in modern organizations, the exponential increase of interconnected devices combined with the extensive deployment of artificial intelligence in organizational processes expands the organizations' open surface to cyberattacks [1]–[4]. Consequently, it is of outmost importance to understand that although

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

digitalization creates enormous economic benefits and opportunities providing solutions for the challenges that Europe is currently facing, at the same time it exposes the society and economy to security threats. Critical sectors such as transport become progressively more dependent on digital technologies to perform their essential activities and develop novel efficient transport services and infrastructure to empower economic and social cohesion, and to exploit the economic strengths of the EU [5], [6]. For instance, although the continuously increasing number of visitors entering the EU through land-border crossing points and/or seaports brings immense economic value, novel border control solutions, such as mobile devices for passenger identification for land and sea border control, are essential to precisely identify passengers ''on the fly'' ensuring their comfort and safety [6], [7].

However, these devices are expected to handle highly sensitive and confidential personal data and thus, it is very likely to become an attractive target to malicious actors in terms of data misuse, data loss and data theft [6], [8]. In particular, the authors in [9] highlighted that the main aim of attackers is to gain access to sensitive and confidential personal data by surpassing the authentication process using the user's identity information (e.g., brutal-force, observation, guessing, impersonation attacks [9]) or refer to other techniques (e.g., hacking the database in the remote server or intercepting data transmission) and use those data in a malicious manner conducting non-permitted actions. Therefore, to ensure high level of device security and protect sensitive data handled by this type of devices, strong user authentication mechanisms are required to establish confidence in the claimed identity of the user verifying their identity, as a prerequisite to allowing access to the device's resources [10]–[14]. Since this type of mobile devices falls into the category of public safety devices, we explored public safety mobile authentication approaches. NIST Special Publication 8080 [15] acknowledged that most of the current authentication methods are infeasible for public safety use in the field as they are practically not convenient for the first responders such as the land and sea border control officers. Consequently, it is of utmost importance to research, design and implement novel secure and usable user authentication mechanisms that will increase the level of device security of the passenger identification mobile devices while ensuring that border control officers at land and sea borders will be able to complete their missions in an efficient and effective manner [6].

Nevertheless, security and usability are often thought of as being contradictive [6]. Risk-based and adaptive user authentication types have been extensively proposed in the literature to deal with this security vs. usability challenge [6], [7], [14]. In particular, these two types of user authentication in combination have been shown to enhance the reliability of the whole authentication process without interrupting the user's normal activity [16], dynamically authenticating a legitimate user throughout their entire interaction with the mobile device. Towards this direction, we, firstly, provide a review of related work on user authentication solutions for mobile devices, discuss the security vs. usability challenge, and then present background concepts on risk-based and adaptive authentication. Our objective is to provide a foundation for organizing research efforts towards the design and development of effective and efficient risk-based adaptive user authentication mechanisms for mobile passenger identification devices used by border control officers at land and sea borders. Besides that, a novel risk-based adaptive user authentication mechanism is proposed. Afterwards, we focus on the investigation of the performance of a set of the most popular classification algorithms for risk-based authentication, namely k-Nearest Neighbor (k-NN), Decision Tree (DT), Support Vector Machine (SVM), and Naïve Bayes (NB). We train and test these classification algorithms over the same data of the HuMIdb dataset, which, to the best of our knowledge, is the most recent and publicly available dataset for behavioral user authentication [17], [18]. The performance of the classification algorithms is evaluated by the evaluation metrics of accuracy, precision, recall, and F1-score. However, the evaluation results demonstrate impact of overfitting and therefore, we consider the following novelty detection algorithms to overcome the challenge of overfitting: one-class Support Vector Machine (OneClassSVM), Local Outlier Factor (LOF), and KNN_average (i.e., KNN configured properly for novelty detection). All of them demonstrate a high performance. To the best of our knowledge, this is the first time that novelty detection algorithms have been considered for risk-based adaptive user authentication.

Following the Introduction, the rest of the paper is organized as follows. Section II presents: (i) a 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, (iv) the concept of the adaptive user authentication, (v) the HuMIdb dataset, as well as (vi) classification algorithms for risk-based authentication. In Section III, a proposed risk-based adaptive user authentication mechanism is provided, while Section IV presents the performance evaluation of a set of four popular ML classification algorithms for risk-based adaptive user authentication and of a set of three novelty detection algorithms. Finally, the paper is concluded in Section V.

II. RELATED WORK

This section discusses related work on user authentication for public safety and smartphone devices, presents the security vs. usability challenge and, finally, provides related work on risk-based user authentication and adaptive user authentication as an efficient solution to balance security and usability in mobile user authentication for public safety applications.

A. USER AUTHENTICATION FOR PUBLIC SAFETY AND SMARTPHONE DEVICES

User authentication is a fundamental security objective for the security of the next generation mobile passenger

IDentification (ID) devices. However, as these devices comprise a novel solution, no specific user authentication mechanisms for this kind of devices have been developed so far. Nevertheless, it is anticipated that the land and sea border passenger identification mobile devices will be devices with similar capabilities to those of Public Safety mobile devices and smartphone devices.

Previous works on Public Safety mobile devices and smartphone devices have investigated the challenges of user authentication relying on knowledge-based schemes (e.g., standard passwords, Personal Identification Numbers (PINs) and graphical patterns) [15], [16], [19]. However, according to the recent studies, these conventional user authentication techniques are no more considered secure and convenient for the user [16]. Firstly, these techniques are not able to distinguish the users, rather they authenticate everyone with the valid credentials. Zhang *et al.* [20] describe the user's difficulties in memorizing and correctly recalling the several passwords. Consequently, the users set easy or simple passwords to remember making the mobile devices vulnerable to numerous attacks, e.g., guessing and dictionary attacks. On the other hand, Android users tend to set graphical patterns for device unlocking. Nevertheless, this approach, similarly to the passwords, requires users to memorize the graphical patterns. Therefore, users set simple patterns, that a malicious actor could possibly guess or observe them. This illustrates the generally acknowledged conception that knowledge-based schemes are problematic [15], [16], [20].

Apart from knowledge-based schemes, authentication schemes based on biometrics are widely used as well [15], [16], [21]. Although the physiological biometrics are considered secure since they are unique, they have shown to be vulnerable to different types of attacks such an impersonation. More specifically, nowadays, user's fingerprint could be, easily, extracted from the gestures on some photos (e.g., the gesture of "peace"), while the face of a user, could be found on social media websites. Recent researchers have shown that these physiological biometric schemes can be hacked effortlessly with a cheap equipment and not very sophisticated algorithms. For instance, researchers unlocked the Samsung S8 while with a simple photo of the legitimate owner [22], while iPhone X Face ID was hacked with a 150 dollars 3D printed mask of its owner face [23]. Similarly, the German Chaos Computer Club hacked the iPhone 5S fingerprint scanner by photographing the glass surface with the user's fingerprint, and then creating a thin film with a fake one within two days after Apple launched iPhone 5S worldwide [24]. This is a proof that there is a need for novel solutions and more sophisticated algorithms to exploit the advantages of uniqueness of the physiological biometrics.

Last but not least, *u*ser authentication based on behavioral biometrics is considered as the future of user authentication for sensitive applications performed with mobile devices [25]. For instance, for the next generation mobile passenger ID devices for land and sea border control, behavioral biometric-based solutions are very promising. Although the behavioral biometrics are not considered unique enough for ensuring user identification, they have proved efficient for user authentication. Additionally, combining two or more modalities can improve the accuracy and enhance the security. These schemes can work as an additional transparent authentication layer, that enhance the existing authentication mechanisms without affecting the usage of the device [8], [19], [25], [26]. Research efforts have been already started in gait recognition, keystroke or touch dynamics and voice recognition behavioral biometric modalities [8], [19]. For the next generation mobile passenger ID devices for land and sea border control, the *gait-based solution* with a wearable device is not so convenient, considering that the officer may move long distances, and also regarding the large number of the officers working (e.g., cost of many sensors). On the other hand, a gait-based solution implemented by some in-built sensors, such as the accelerometer or the gyroscope, could possible fit better in the land and sea border control application. *Keystroke or touch dynamics* [16], [27] potentially could be integrated for the user authentication for the next generation mobile passenger ID devices for land and sea border control as an additional authentication level when for instance the face recognition fails, and the system asks for the passcode. Finally, *voice recognition* modality [28] could potentially enhance the performance of the traditional biometric systems and broaden the landscape of the continuous user authentication.

To sum up, considering a smartphone device, the face physiological biometric can be collected by using the camera of the device, while the fingerprint and iris recognition need special equipment. On the other hand, the behavioral biometrics, such as gait, touch, swipe and voice can be collected all by the sensors of the mobile device, namely, accelerometer, gyroscope, touch screen and microphone [29]. The behavioral biometrics are starting to get attention as they are cost-effective; they do not need any additional hardware equipment, and they are lightweight in the implementation [27]. For instance, the touch-based solution e.g. swipe or keystroke, manage to authenticate the users unobtrusively based on their interactions with the device. Additionally, both physiological and behavioral biometrics authentication mechanisms are considered secure and accurate as they are unique and they cannot be shared, copied, lost or stolen [16]. Furthermore, they can be combined with another authentication means (e.g., username and password) for establishing multifactor authentication in order to enhance the security of the mobile device. As such, security experts are focusing on developing such mechanisms as they seem that they will restructure the authentication landscape in the following years [16], [30].

On the other hand, security requirements should not compromise the ability of first responders (i.e., the land and sea border control officers) to complete their missions in an efficient and effective manner [15]. Therefore, it is critical to ensure the usability of user authentication, since poor usability often results in user circumvention, which can ultimately degrade the intended security control [15], [31].

TABLE 1. Usability analysis summary of public safety mobile authentication methods.

Authentication Method	Feasible	Challenging	Impractical
No authentication	👮		
Knowledge-based authentication			👮
Password			👮
PIN		👮	
Gesture		👮	
OTP device		👮	
Embedded cryptographic token	👮		
Removable hardware cryptographic token		👮	
Smartcard with external reader			👮
NFC-enabled smartcard		👮	
Proximity token	👮		
Fingerprints	👮		
Facial recognition		👮	
Iris recognition		👮	
Speaker recognition			👮
Keystroke dynamics			👮
On-body detection	👮		
Location-based awareness	👮		

For instance, several usability issues are emerged when looking across conventional authentication methods: issues with memorizing information (i.e., knowledge-based schemes), issues with users who are wearing gloves (e.g., fingerprints-based authentication), masks (e.g., face recognition) and/or protective eyewear (e.g., iris recognition), the difficulty of text entry (e.g., passwords, PINs, keystroke dynamics authentication) on mobile devices, the necessity of having access to the biometric samples of a user, and the environmental issues that could negatively affect sensitive electronics (e.g., speaker recognition) [15].

Therefore, it is of utmost importance the design and implementation of novel secure and usable user authentication mechanisms that will increase the level of security of the mobile passenger identification devices and will ensure that border control officers at land and sea borders are able to successfully complete their missions.

B. SECURITY VS. USABILITY CHALLENGE

Security and usability are often thought of as being contradictive. In this section, we explore the possibility of incorporating both security and usability in user authentication for mobile passenger identification devices for land and sea border control. In order to meet the objectives for secure and usable user authentication for land and sea border passenger identification mobile devices, it is of utmost importance to conduct research to understand the land and sea border control officers' needs, key characteristics, tasks, and environments [6], [15]. Due to the fact that this kind of mobile devices falls into the category of public safety [6], [15], we began our work with qualitative research, which focuses on the information provided by NIST about public safety mobile authentication. According to NIST Special Publication 8080 [15], most of the current authentication methods are not feasible for public safety use in the field as they are practically not convenient for the first responders (e.g., the land and sea border control officers). In Table 1, conventional authentication methods are rated as feasible, challenging, or impractical from a usability perspective based on NIST Special Publication 8080 [15], highlighting the need for novel more sophisticated user authentication mechanisms for public safety applications.

According to NIST Special Publication 8080 [15], the aim is that authentication should not interrupt actively responding first responders, nor should it overburden them in any stage of response. For instance, if authentication can be implemented such that first responders authenticate at the beginning of a shift, and stay authenticated throughout the shift, then many of the existing and commonly implemented authentication methods (e.g., knowledge-based authentication schemes or biometrics) would then become more feasible. To support such a scenario, more sophisticated mechanisms must be implemented to enhance the reliability of whole authentication process without interrupting the land and sea border control officer's normal activity on the field. To deal with this security vs. usability challenge, adaptive and risk-based authentication mechanisms have been proposed to constantly authenticate a legitimate user throughout the entire session [16], [32]. In the rest of this section, we are going to further elaborate the aforementioned types of user authentication.

C. RISK-BASED USER AUTHENTICATION

Nowadays, risk-based authentication schemes 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." [33]) while enhancing security and promoting user's comfort [16], [21], [34]–[36]. For instance, in [16], the authors describe risk-based authentication as the continuous decision on user authentication acceptance or rejection based on the user's behavior and the risk of their action. In particular, this decision depends on the comparison of a risk score, computed in real time, with the stored scores in the risk profile of the user, and, when required, the system challenges the user for re-authentication, accordingly, as it is illustrated in Fig. 1. There is no doubt that the ***risk estimation*** component constitutes a key part of the risk-based user authentication mechanisms as it is the responsible element for processing

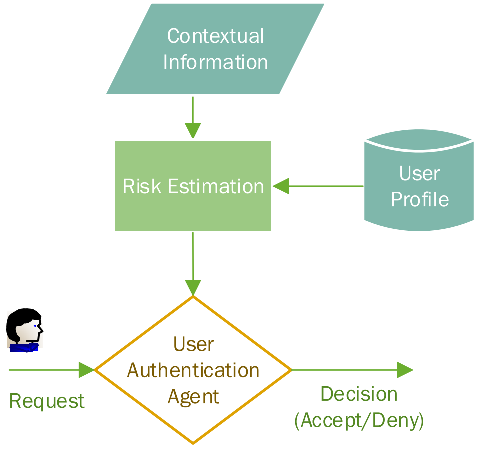

FIGURE 1. Risk-based user authentication overview.

available information from user's environment (e.g., contextual information), user's profile (e.g., user risk history reflecting previous user's [16], [37]–[39] action or event [40]. Typically, in qualitative Risk Assessment (RA), which is a well-established approach within information security for ensuring a commensurate level of security is provided given the risks [41], the risk score is estimated by a function of (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence ([42] under Risk CNSSI 4009), and the most common mathematical formula to represent it is the following:

$$Risk\ Score = Likelihood \times Impact$$

where likelihood represents the probability of an incident to happen, and impact represents the estimation of the value of the damage regarding that incident ([42] under Risk CNSSI 4009). Then, based on the results of the risk estimation process, the estimated risk scores are transformed into a "human readable" format.

For example, the authors in [41] developed a Mobile Device Risk Assessment (MDRA) based on the qualitative RA. Their risk calculation scheme consists of the six steps as shown in Table 2. The authors considered as assets the installed applications and services in the mobile device such as e-mail, e-banking, e-health, stored sensitive documents, and they assigned an asset value (from 1 to 8) in each asset based on the applications sensitivity. In addition, they considered threat levels from 1 (less severe) to 5 (harmful), and they constructed a Risk Matrix based on Threat Level and Asset Value. Their main goal was to evaluate the risks associated with various actions and applications in a mobile device in a user-friendly manner.

Actions or events with both high likelihood and high impact would be considered "high risk", while those with low likelihood and low impact would be in the opposite considered "low risk" events. The main idea is that the higher the score, the more important something is and the sooner you should address it. However, despite the fact that existing qualitative approaches sound reasonable, they involve a lot of expert intuition, and thus the risks are always rated subjectively, making this approach unsuitable for real-world cybersecurity solutions [43], [44]. Thus, there is the tendency to move in the direction of more quantitative risk estimation methods [43]. Towards this direction, in the context of risk-based user authentication, efforts should be placed on developing and implementing novel and efficient quantitative security risk estimation algorithms. In the literature, various classification algorithms such as decision trees [37], [38], Naïve Bayes [37], [46] and logistic regression [38] as well as other approaches, such as fuzzy logic [37], and Monte Carlo simulation [45], [51] have been proposed for quantitative risk estimation for risk-based user authentication. The efficiency and effectiveness of these approaches are evaluated based on their performance to reliably calculate a risk score of an action or an event, requiring comprehensive datasets. However, one of the major research challenges in this field is the lack of proper datasets including user's contextual information such as user's location, date, time, device's ID, and device's connection, as well as other information related to the device attributes, the user history, the user's behavioral patterns, etc. To the best of our knowledge, HuMIdb dataset, described in section II.E, is one of the few publicly available datasets including proper information for user authentication.

TABLE 2. Mobile device risk assessment (MDRA).

MDRA Step	Description
1	Evaluation of asset value categories
2	Calculation of a single asset value
3	Evaluation of threats
4	Calculation of a single threat value
5	Answer vulnerability questions
6	Calculation of risk level

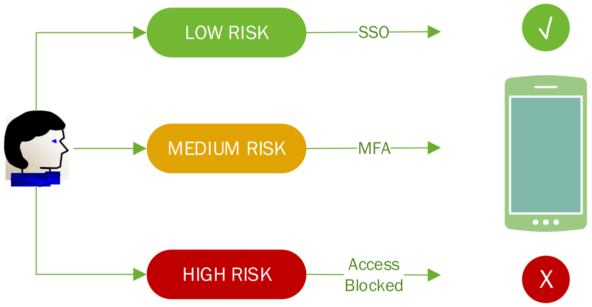

FIGURE 2. Adaptive user authentication block diagram. (Source: https://www.onelogin.com/learn/what-why-adaptive-authentication).

D. ADAPTIVE USER AUTHENTICATION

Adaptive authentication is a way that two-factor authentication or multifactor authentication can be efficiently configured and deployed (see Fig. 2). In particular, it is a method for selecting the proper authentication factors based on:

a.) user's risk profile, and b.) user's tendencies - for adapting the suitable type of authentication to the specific situation [16]. According to [16], there are three ways that adaptive authentication can be deployed:

1. The system admin can define fixed risk levels based on static policies for different factors, such as user's location, authentication's request time of day, day of week, user role, or resource importance.
2. The system can observe the user's typical day-to-day activities on his/her habits and tendencies over time and generate proper dynamic policies. This learning process of adaptive authentication is similar to behavioral correlation [16].
3. A combination of both 1 and 2 ways utilizing static and dynamic policies.

Regardless of how the risk levels are defined for certain application, the main idea is that adaptive authentication adapts to that risk level, enabling the appropriate level of authentication for the given level of risk [16], [52]. For instance, when a land and sea border control officer is using the mobile passenger ID device in their usual shift (i.e., the date and time of the day that they are supposed to be working), re-authentication should not be required (e.g., the risk level is low). While in case of device usage at any other time (e.g., high risk level), the service may lock, and its unlocking may be only possible by IT staff. Or, when an officer is located in a nonverified location during their shift (e.g., medium risk level), the system should require additional evidence that this person is who claims to be by asking re-authentication.

Adaptive authentication enables significant benefits for user authentication for the mobile passenger identification devices used by border control officers at land and sea borders. In particular, adaptive authentication can ensure that certain attributes about the land and sea border control officer will be monitored and changes on these attributes will enable different authentication methods. In this way, officer's activities will not be interrupted for inessential reasons, while additional authentication will be required only when the risk level has reached a particular value. It is worthwhile to highlight that proper attributes, also refer to as fraud indicators [53], [37], about the land and sea border control officer should be considered in order to design and develop effective and efficient adaptive authentication. In Section III, the design of the proposed mechanism is presented in detail.

E. HuMIdb DATASET FOR BEHAVIORAL USER AUTHENTICATION

The HuMIdb dataset (Human Mobile Interaction database) includes data captured by 14 sensors (i.e., accelerometer, linear accelerometer, gyroscope, magnetometer, orientation, proximity, gravity, light, touchscreen, keystroke, GPS, WiFi, Bluetooth, and microphone), during natural human-mobile interaction performed by more than 600 smartphone users [17], [18]. For the data acquisition, the authors developed an Android application that gathers sensor signals when users perform eight simple tasks with their own devices and without any supervision (i.e., the users could be walking, sitting standing, at daytime or night, being indoors or outdoors, etc.). In particular, the designed tasks included: a) keystroking, b) swiping up, c) swiping down, d) tapping and double tapping, e) circle hand gesturing, f) cross hand gesturing, g) voice recording, and h) finger handwriting. The acquisition protocol comprised 5 sessions with at least 1 day gap among them (i.e., the minimum time between one user finishes a session and the next time the app allows to have the next session). At the beginning of each task, the app shows a brief pop-up message explaining the procedure to complete each task. The application also captured the orientation (e.g., landscape/portrait) of the smartphone, the screen size, resolution, the model of the device, and the date when the session was captured. The developed app was advertised in the authors' research web site and was launched on Google Play Store. Afterwards, participants were self-selected worldwidely, producing a diverse network of people compared to previous state-of-the-art mobile databases. The authors in [17] and [18] highlight that all captured data have been stored in private servers and anonymized with previous participant consent according to the GDPR (General Data Protection Regulation). The structure of HuMIdb is as follows:

$$\boxed{\text{User}} \rightarrow \boxed{\text{Sessions}} \rightarrow \boxed{\text{Tasks}} \rightarrow \boxed{\text{Sensors}}$$

where the data are stored in nested folders with the ID number to identify each user's folder. Inside the user's folder, there are five "session" sub-folders corresponding to the five different sessions the user has completed. Each "session" sub-folder contains a set of "task" sub-folders (e.g., keystroking, swiping up and down, tapping and double tapping) and three CSV files with the Bluetooth, WiFi and GPS data signals acquired during the given session. Besides that, each "task" sub-folder includes a "sensors" sub-folder including data from the various sensors required for the particular task.

F. CLASSIFICATION ALGORITHMS FOR RISK-BASED AUTHENTICATION

The classification algorithms can be further classified into parametric and non-parametric. The first ones are based upon the assumptions of normally distributed population and estimate the parameters of the distributions to solve the classification problem, while the second ones make no assumptions about the specific distributions involved.

1) k-NN CLASSIFIER

The k-Nearest Neighbor (k-NN) classifier serves as an illustration of a non-parametric statistical approach and does not require any initial parameter for its proper working. The main idea of k-NN classifier is that it predicts the label of a new unclassified instance after observing the labels of the k closest training instances to this new instance (i.e., the k-nearest neighbors), and the majority class of the k closest training instances is assigned to the new instance. To achieve this, it determines the k closest training instances using a distance metric, and selects the dominant class label among them as the relevant class [54]. Generally, the standard Euclidean distance is used, while other options include Chebyshev, Manhattan, and Minkowski distances [54].

It is noteworthy that the choice of k - which defines the number of closest training instances (i.e., nearest neighbors) required to accurately classify the new instance - constitutes an important parameter that affects the overall performance of the classifier [54]. Nevertheless, the k can be determined experimentally, i.e., starting with k=1, we estimate the accuracy of the classifier, and the process is repeated increasing the number of the k-nearest neighbors used to predict the label of the new unclassified instance. Then, the k-value that achieves the higher accuracy may be selected. In general, the larger the number of training instances is, the larger the value of k will be.

In Fig. 3, we can observe an example of K-NN classifier in the context of risk-based authentication. The orange rhombuses depict the instances of the high risk class, the yellow squares depict the instances of the medium risk class, and the green triangles depict the instances of the low risk class, while the new unclassified instance is represented by a dark red x. This new unclassified instance will be classified under a known class (i.e., high, medium, or low risk) based on the majority class of the k closest training instances. As we cited previously, k is the number of nearest neighbors used for the classification of the new instance and it is worthwhile to highlight that the classification might be different depending on the chosen value of k [54].

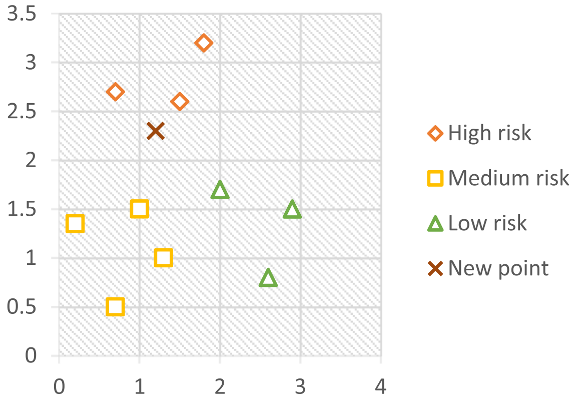

FIGURE 3. k-NN classifier.

Furthermore, in [46], the authors proposed a location-aware authentication model, in which they calculated a risk score based on changes in user's location, and then, classified this risk score using the k-NN classifier to accept or deny the authentication. According to their findings, the k-NN classifier presents a significant advantage in terms of its simplicity. On top of that, it is noise-tolerant, and it has relatively low update cost [46]. Finally, they applied the "Brute Force k-NN", "K-D Tree" and "Ball Tree" algorithms from the Scikit-learn library for the Python programming language in order to build their prediction model and compare the performance results. Furthermore, in [55], the authors presented a comprehensive survey on machine learning techniques and user authentication approaches for credit card fraud detection where they presented a comparative study that was initially presented in [56]. In particular, the authors in [56] compared the predictive performance of several data mining methods including k-NN, Artificial Neural Network (ANN), Decision Trees (DT), and Naïve Bayes (NB) classifiers, as well as Logistic Regression (LR). Based on their findings, although the k-NN classifier does not perform better than the NB classifier, ANN, and DT, it achieved the lowest error rate.

2) DECISION TREES-BASED RISK ESTIMATION

Decision Trees (DTs) are a non-parametric supervised machine learning algorithm used for classification [54]. The main target of DTs classifier is to create a model that predicts the value (e.g., low, medium, high) of a target variable (e.g., risk) by learning simple decision rules inferred from the data features [45], [46]. In particular, it extracts features of the training dataset and organize an ordered tree based on the value of these features [54]. To do this, it considers a feature of the training dataset as a root node of a tree and all its possible values as the branches of this root node. This splits up the training dataset into subsets, one for every value of the selected feature. Afterwards, the process might be repeated recursively for each branch, using only those training instances that actually reach the branch (i.e., they have the feature value of the particular branch). If at any time all training instances at a node have the same classification, then the development of that part of the tree is stopped, and this class is considered the terminal node. The main challenge is how to determine which feature to split on in order to create the ordered tree [54]. Various metrics, such as Gini Index, Entropy and Information Gain, are utilized for i) identification of the feature that will be considered the root node, which will optimally divide the training dataset [45], [46], and ii) identification of which feature to split on. An example of a DT classifier is illustrated in Fig. 4.

The main advantage of DTs is that they work well even with insufficient data if proper set of rules is determined. In addition, DTs are considered valuable models for classification and easy to understand and to interpret as they can be visualized [45], [47]. Furthermore, DTs require little data preparation compared to other classifiers requiring, for instance, data normalization, or removal of the blank values. However, when the DTs become significant in terms of size, it becomes more difficult to understand them and, on top of that, more data are needed for identifying and validating the set of rules [45], [47], [48]. Finally, DTs can be unstable as a slight change in certain value of a feature could lead to a totally different conclusion because of the discreteness of the partition, resulting in a completely different generated tree. This problem can be mitigated by training multiple trees in a majority voting ensemble learner, where the features are randomly sampled with replacement, or by using DTs within an ensemble of other classifiers. Ensemble learning is a

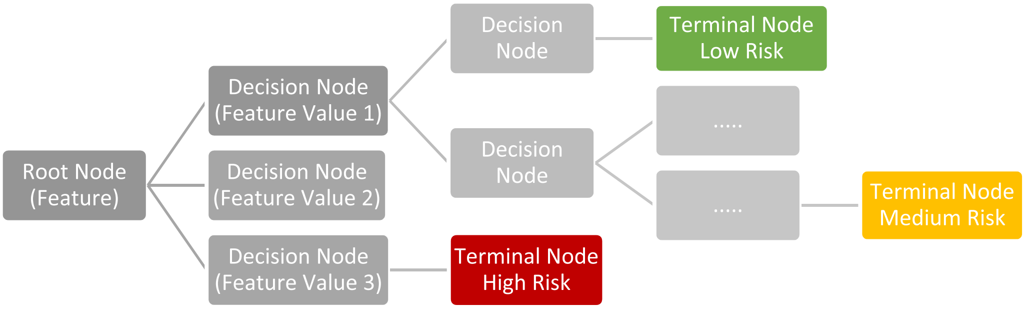

FIGURE 4. DT classifier.

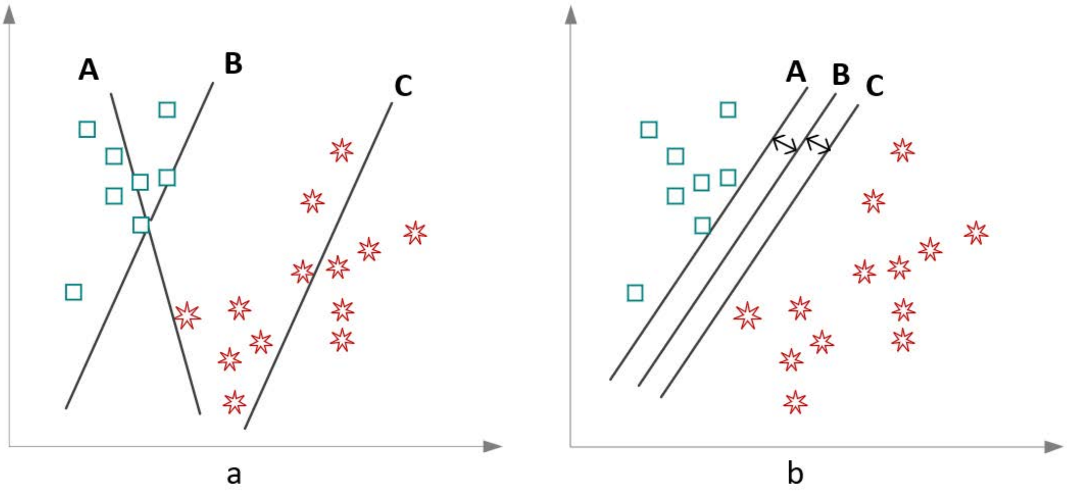

FIGURE 5. SVM classifier.

well-known strategy for obtaining accurate classifiers [54] and has been utilized in risk-based authentication mechanisms such as in (46).

In [46], the authors applied the ID3, C4.5 and CART in order to build their prediction model and compare the performance results. These algorithms employ "Entropy" and 'Gini Index' as splitting criteria [46]. According to their findings, CART classification algorithm performs better for systems like theirs where the desired output was the binary decision: to *Accept* or to *Deny* authentication. They also constructed a dataset on Matlab, based on the state-of-the-art research to develop their data-driven model (i.e., classifier). In conformity with their conclusions, CART shows benefits over the other two algorithms in terms of reducing over-fitting and the ability of handling incomplete data [46]. On top of that, the authors presented an optimized version of CART implemented in Scikit-learn library for the Python programming language.

3) SUPPORT VECTOR MACHINE (SVM)

Support Vector Machine (SVM) is a supervised ML algorithm used for binary classification problems and is considered one of the most robust and widely used binary classifiers [46], [54]. Given a set of labeled data (i.e., training data), the main objective of SVM is to generate an optimal hyperplane in the feature space which accurately demarks the two different classes. Optimal hyperplane is considered the separating hyperplane which maximizes the distance between the nearest training instances (i.e., from both classes, meaning from both sides of the hyperplane) and the hyperplane [46]. This distance is called 'Margin'. A margin is considered to be good if the separation is larger for both classes, and points belonging to one class should not cross to another class. In the beginning, the algorithm starts with randomly plotting of x hyperplanes along with the training data, as for instance it is shown in Fig. 5a where hyperplanes "A", "B" and "C" have been considered. Afterwards, it attempts to adjust the orientation of the hyperplanes in such a way that it homogeneously divides the given classes. In Fig. 5b, we can observe that all three hyperplanes ("A", "B" and "C") segregate the two classes (i.e., green squares and red 7-point stars) well, but a rather pertinent question is about which is the most appropriate hyperplane for the particular training instances. Selecting the hyperplane with the higher margin from the nearest training instances, SVM achieves higher degree of robustness as the chance of misclassification is lower. In the example in Fig. 5b, "B" is considered the optimal hyperplane as the margin for hyperplane "B" is comparatively higher than both "A" and "C". Therefore, we consider hyperplane 'B' as the optimal hyperplane.

In [46], the authors designed and developed a risk-based authentication system. They considered the following attributes for each authentication request: (i) time of the request; (ii) location of the request; and (iii) credentials provided by the user to calculate the corresponding risk value associated with this request, also referred to as uncertainty value. The risk values (i.e., uncertainty values) for each of these attributes were represented by probability distribution functions (PDFs) since, in real word scenarios, these attributes derived from stochastic processes. Each attribute was studied separately to determine the PDF that reflects the uncertainty in authentication by presenting the likelihood of the incident occurrence for the selected attribute. The outcome was an uncertainty matrix consisting of the calculated uncertainty values for these three attributes. Having calculated the risk values (i.e., uncertainty values) for every attribute separately, they designed a risk engine to compute the overall risk score (i.e., uncertainty value) per user request. Afterwards, they performed risk (i.e., uncertainty) binary classification (i.e., accept or reject authentication) using ML algorithms and demonstrated that logistic regression and SVM classifiers showed better performance in terms of model accuracy in comparison with DTs. In particular, SVM and logistic regression showed similar results in terms of accuracy, precision, recall and F1. The authors discussed that this was expected due to the optimization method that these two algorithms are employing. Both classifiers are considered probabilistic models which are optimized by minimizing some cost associated with misclassification based on the likelihood ratio [46].

Furthermore, the authors in [57] designed and implemented a risk-based authentication system using ML techniques. They built the User Profile collecting the following information referred to as user parameters: IP address, geolocation, time zone, login time, OS version, browser version, device type and number of failure attempts. In addition, they set different weights to every user parameter depending on their importance. Then, the risk engine calculated the risk score as follows:

$$Risk\ score = \sum_{i=1}^{n} user\_parameter\_value_i \times user\_parameter\_weight_i$$

Their proposed risk-based authentication system used three machine learning algorithms, namely SVM, one-class SVM and Naïve Bayesian for risk classification. As mentioned in [57], one-class SVM is an unsupervised machine learning algorithm. Hence, genuine user behavior patterns are sufficient to train the model. On the other hand, for the development of SVM and Bayesian models, both genuine and fraudulent user behavior patterns are required to train the models. The authors simulate several tests changing one or more user parameters at a time. According to their results, the risk score computed by one-class SVM was more relevant to the given test scenarios. In particular, Bayesian probability values showed extreme results for almost all the test cases. For instance, a change in the time zone would outcome a very low risk level, while a slight change in geolocation would outcome a very high risk level.

4) NAÏVE BAYES

Naive Bayes (NB) classifier is a supervised ML algorithm based on applying Bayes' theorem with the "naïve" assumption of conditional independence between every pair of features given the value of the class variable in order to simplify the process of modelling [54]. Regardless this controversial assumption, it is anticipated that Naïve Bayes is a fast classifier and has a great performance in practice for many domains such as risk-based authentication [46]. Given events Y and X with $P(X) \neq 0$, Bayes' theorem states the following:

$$P(Y \mid X) = \frac{P(Y)\,P(X \mid Y)}{P(X)}$$

where,

$P(Y \mid X)$ represents the conditional probability of Y occurring given that X is true,

$P(X \mid Y)$ represents the conditional probability of X occurring given that Y is true,

$P(Y)$ represents the probability of Y occurring without any condition,

and $P(X)$ represents the probability of X occurring without any condition.

However, in a real case classification problem, there can be multiple X variables depending on the features of the training data. Hence, in the situation in which features are independent or under this assumption, Bayes Theorem is extended to Naïve Bayes classifier:

$$P(Y \mid X_1, \cdots, X_n) = \frac{P(Y)\,P(X_1, \cdots, X_n \mid Y)}{P(X_1, \cdots, X_n)} \tag{1}$$

Based on the "naive" assumption of class-conditional independence, the features are conditionally independent of one another given the class, thus:

$$\begin{aligned} P(X_1, \cdots, X_n \mid Y) &= P(X_1 \mid Y) \cdots P(X_n \mid Y) \\ &= \prod\nolimits_{i=1}^{n} P(X_i \mid Y) \end{aligned} \tag{2}$$

Based on (1) and (2), we have:

$$P(Y \mid X_1, \cdots, X_n) = \frac{P(Y)\prod_{i=1}^{n} P(X_i \mid Y)}{P(X_1, \cdots, X_n)} \tag{3}$$

Since $P(X_1, \cdots, X_n)$ is constant given the input, we can use the following classification rule:

$$P(Y \mid X_1, \cdots, X_n) \propto P(Y)\prod_{i=1}^{n} P(X_i \mid Y)$$

$$\hat{Y} = arg \max_{Y} P(Y)\prod_{i=1}^{n} P(X_i \mid Y)$$

and we can use Maximum A Posteriori (MAP) estimation to estimate $P(Y)$ and $P(X_i \mid Y)$; the former is then the relative frequency of class Y in the training set.

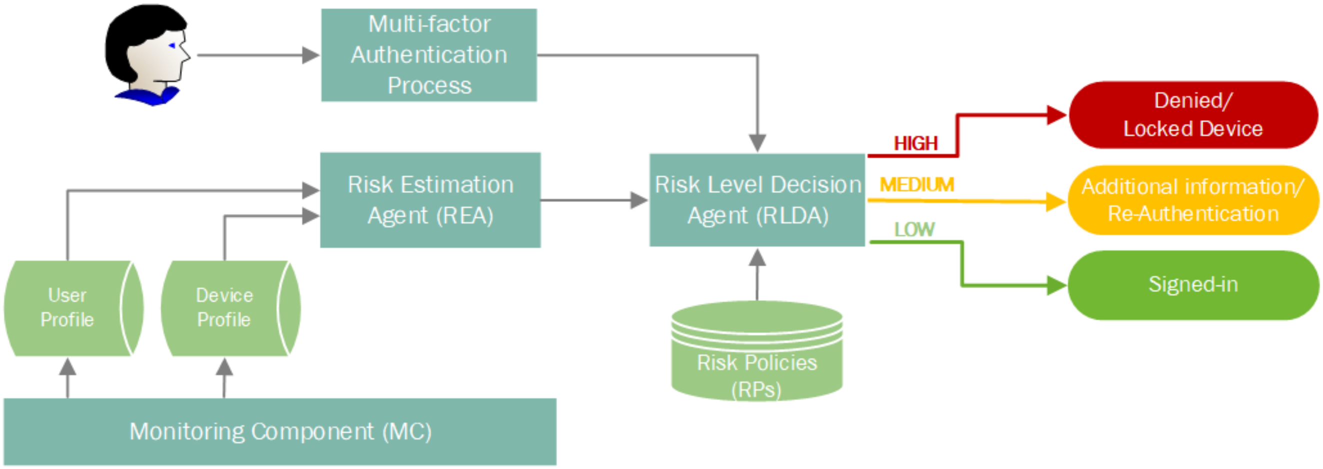
Multi-factor Authentication Process
Risk Estimation Agent (REA)
Risk Level Decision Agent (RLDA)
HIGH
MEDIUM
LOW
Denied/ Locked Device
Additional information/ Re-Authentication
Signed-in
User Profile
Device Profile
Risk Policies (RPs)
Monitoring Component (MC)

FIGURE 6. The generic flow of the proposed risk-based adaptive user authentication mechanism.

The different NB classifiers differ mainly by the assumptions they make regarding the distribution of $P(X_i \mid Y)$. Depending on the application (e.g., text classification, binary classification, large scale classification etc.) and the type of the data (e.g., multinomially distributed data, categorical data etc.), NB classifier makes different assumptions to define the likelihood of the features. For instance, it implements Bernoulli NB for data that are distributed based on multivariate Bernoulli distributions; i.e., there may be multiple features on a given training dataset, however each one is assumed to be a binary-valued (i.e., Bernoulli, Boolean) variable.

Despite their apparently over-simplified assumptions, NB classifiers have outperformed other more sophisticated classifiers in many real-world applications [54], mainly in document classification and spam filtering. Their main advantage is that they rely on a small amount of training data to estimate the necessary parameters for their proper running. On top of that, NB classifiers can be extremely fast compared to more sophisticated methods. The decoupling of the class conditional feature distributions means that each distribution can be independently estimated as a one-dimensional distribution. This in turn helps to alleviate problems stemming from the dimensionality issue.

The authors in [46] applied Gaussian Naïve Bayes classifier, implemented in the scikit-learn library, for their proposed novel prediction model for risk-based authentication with binary decision: *Accept* or *Deny* authentication. According to their findings, although the Naïve Bayes model showed lower performance with respect to true positive and false positive rates than the other used prediction models (i.e., DTs, Logistic Regression and SVM), the Naïve Bayes model was extremely fast in classification and achieved an acceptable accuracy rate slightly lower than the other classifiers. Furthermore, the RSA Risk Engine (RE) in [37] is used to analyze a wide range of indicators associated with an activity in a mobile device to determine the probability that the activity is fraudulent [37]. In particular, the RE combines Bayesian methods with sophisticated device identification and recognition and user behavior analysis to enable intelligent decision-making that significantly reduces fraud in risk-based authentication. According to their results, given the particular features that have been selected for classification, NB performs fast classification achieving high accuracy results.

III. PROPOSED RISK-BASED ADAPTIVE USER AUTHENTICATION MECHANISM

A. MECHANISM ARCHITECTURE

The proposed Risk-Based Adaptive Authentication mechanism comprises a novel secure and usable authentication solution ensuring continuous authentication behind-the-scenes and invisible to the user-officer. Particularly, its main objectives are:

- To provide Multifactor Authentication at the beginning of Officer's shift requiring two pieces of evidence: (i) something you know (i.e., the personal identification number (PIN)); and (ii) something you have (i.e., the proximity token).
- 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 context.
- To, behind-the-scenes and without interrupting Officer's normal activities and missions, continuously monitor: a) the officer's contextual information (i.e., the officer's geographical, location, time, and information about the closeness to the user's proximity token); b) the officer's activity (i.e., behavioural patterns); and c) the device's contextual information (i.e., IP addresses and network reputations), in order to verify their identity throughout their interaction with the mobile device.

B. MECHANISM COMPONENTS

The key components of the proposed Risk-Based Adaptive Authentication mechanism are the following:

1) MULTI-FACTOR AUTHENTICATOR

During the first-time authentication, the Officer is being authenticated through a two-level authentication process. At the first level, the Officer is being authenticated through a multi-factor authentication process based on a PIN and a proximity token. In case that the validity of the claimed identity of the Officer requesting access to the device is verified, the first-level authentication is considered as successful and then, the Multi-factor Authenticator sends a second-level authentication request to RLDA which is responsible for the second-level authentication based on the overall real-time risk score calculated by REA. Otherwise, the authentication request is denied, and the authentication process stops.

2) RISK ESTIMATION AGENT (REA)

REA makes use of the User Profile and the Device Profile to estimate the overall real-time risk score the first time that the Officer attempts to get authenticated and sign in (i.e., Officer's first-time authentication) as well as every time that the user profile and/or the device profile are updated from the MA component (i.e., Officer's continuous authentication). Afterwards, REA forwards the calculated risk score to RLDA to indicate the level of the risk, namely low, medium or high risk.

3) RISK LEVEL DECISION AGENT (RLDA)

RLDA receives the estimated overall real-time risk score calculated by REA and compares it with the risk level thresholds to decide whether the estimated risk score is low, medium, or high. Afterwards, RLDA forwards the Risk Level to ADH.

4) MONITORING AGENT (MA)

As soon as the Officer requested the first-time authentication, MA has started collecting profile information and created the User Profile and Device Profile, which sends to REA, after the corresponding request. Afterwards, once Officer's first-time authentication is successful and throughout their login session, MA, behind-the-scenes and without interrupting Officer's normal activities and missions, continuously monitors the User's and Device's attributes. In particular, MA continuously monitors: a) the officer's contextual information (i.e., the officer's geographical, location, time, and information about the closeness to the user's proximity token); b) the officer's activity (i.e., behavioural patterns); and c) the device's contextual information (i.e., IP addresses and network reputations). If MA detects any changes regarding the User's and/or Device's attributes, then it updates the User Profile and/or Device Profile accordingly and forwards the updated profile(s) to REA.

5) AUTHENTICATION DECISION HANDLER (ADH)

ADH is responsible for handling the authentication decision and adapting to suitable authentication type given the risk level provided by RLDA component. Depending on the risk level decision taken by RLDA the Officer may be: (i) allowed to sign-in (during the Officer's first-time authentication) or remain signed-in (during the Officer's continuous authentication) when the risk level is low; (ii) required to provide additional authentication information about the identity of the user when the risk level is medium in order ADH to perform re-authentication based on iris-based user authentication; or (iii) denied to sign-in when the risk level is high and the mobile device may be locked (e.g., in case of physical theft).

C. OFFICER'S FIRST-TIME AUTHENTICATION

Figure 7 shows the sequence diagram which presents the interactions between the components of the Risk-Based Adaptive Authentication mechanism during the officer's first-time authentication. The interactions between the Risk-Based Adaptive Authentication mechanism components consist of a number of exchanged messages, which are grouped into the following steps:

Step 1: At the first level, the Officer requests authentication from the Multi-factor Authenticator (Message 1). In case that the validity of the claimed identity of the officer requesting access to the device is verified, the first-level authentication is considered as successful, and the officer is signed in (Message 2).

Step 2: After the successful first-level authentication, the Multi-factor Authenticator sends a *second-level authentication request* to RLDA which is responsible for the second-level authentication based on the overall real-time risk score calculated by REA. (Messages 3)

Step 3: RLDA sends a *risk score request* to REA. (Messages 4)

Step 4: For the risk estimation, REA requests profile information (i.e., User Profile and Device Profile information) from MA (Messages 5). MA has started collecting profile information and created the User Profile and Device Profile (Messages 6 & 7), as soon as the Officer requested the first level authentication. Once REA has received the requested profile information from MA (Message 8), REA computes the risk score (Messages 9) and provides the risk score to RLDA (Messages 10).

Step 5: RLDA compares the risk score with the risk level thresholds to decide whether the estimated risk score is low, medium, or high (Messages 11). Afterwards, RLDA forwards the risk level decision to ADH (Messages 12).

Step 6: When the risk level is low, the Officer is allowed to sign-in (Messages 13), and ADH forwards a "Successful Authentication" message to the Officer (Messages 14).

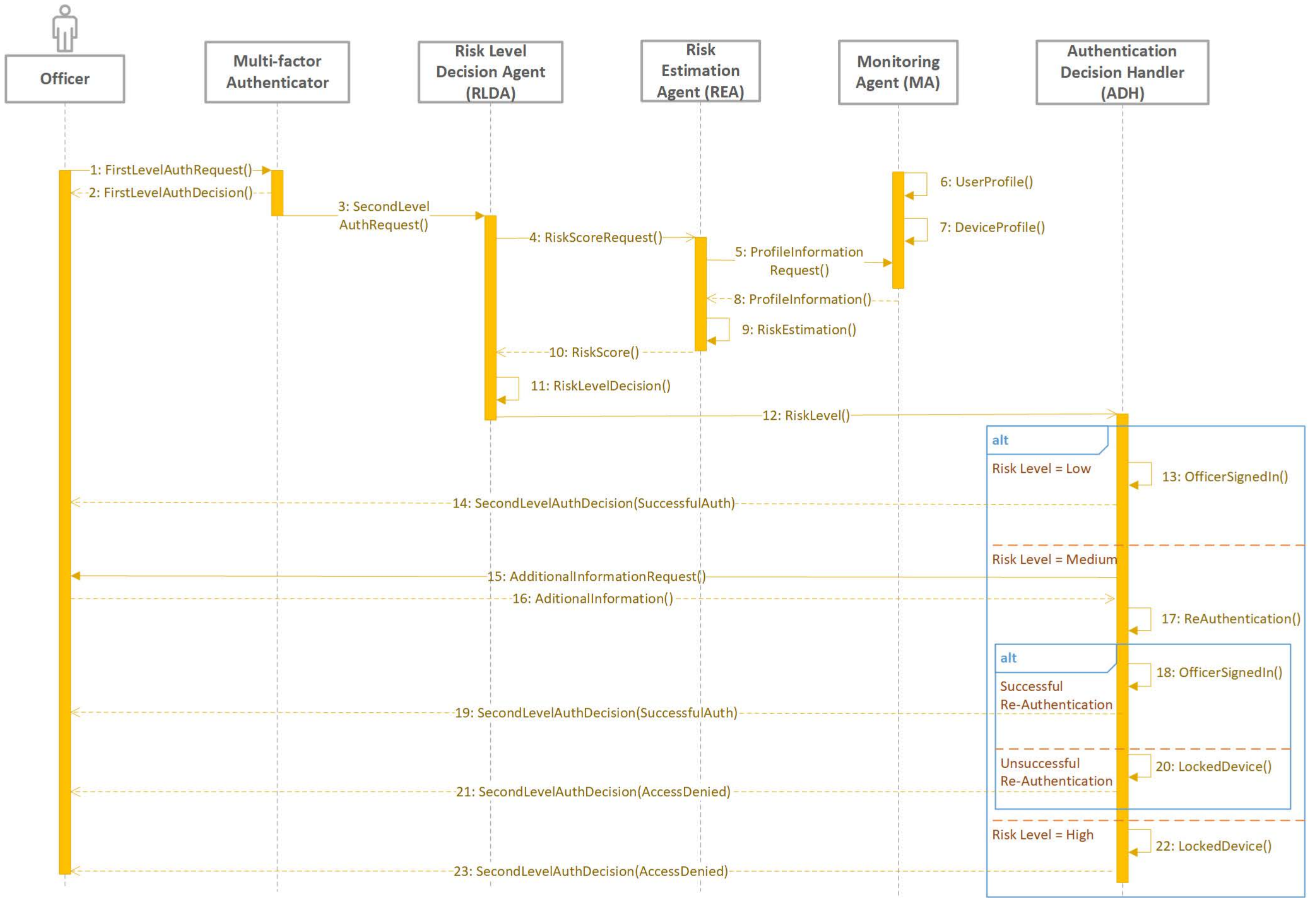
Officer
Multi-factor Authenticator
Risk Level Decision Agent (RLDA)
Risk Estimation Agent (REA)
Monitoring Agent (MA)
Authentication Decision Handler (ADH)
1: FirstLevelAuthRequest()
2: FirstLevelAuthDecision()
3: SecondLevel AuthRequest()
4: RiskScoreRequest()
5: ProfileInformation Request()
6: UserProfile()
7: DeviceProfile()
8: ProfileInformation()
9: RiskEstimation()
10: RiskScore()
11: RiskLevelDecision()
12: RiskLevel()
alt
Risk Level = Low
13: OfficerSignedIn()
14: SecondLevelAuthDecision(SuccessfulAuth)
Risk Level = Medium
15: AdditionalInformationRequest()
16: AditionalInformation()
17: ReAuthentication()
alt
Successful Re-Authentication
18: OfficerSignedIn()
19: SecondLevelAuthDecision(SuccessfulAuth)
Unsuccessful Re-Authentication
20: LockedDevice()
21: SecondLevelAuthDecision(AccessDenied)
Risk Level = High
22: LockedDevice()
23: SecondLevelAuthDecision(AccessDenied)

FIGURE 7. The sequence diagram of officer's first-time authentication.

Step 7: When the risk level is medium, the Officer is requested by ADH to provide additional authentication information (i.e., iris-based authentication) (Message 15). As soon as the Officer provides the requested additional information to ADH (Message 16), ADH performs re-authentication based on iris-based user authentication (Message 17). If the re-authentication is successful, the Officer is allowed to sign-in (Message 18) and ADH forwards a ''Successful Authentication'' message to the Officer (Message 19). If the re-authentication is unsuccessful, the device is locked (Message 20), and ADH forwards an ''Access Denied'' message to the Officer (Message 21).

Step 8: When the risk level is high, the device is locked (Message 22), and ADH forwards an ''Access Denied'' message to the Officer (Message 23).

D. OFFICER'S CONTINUOUS AUTHENTICATION

Figure 8 shows the sequence diagram which presents the interactions between the components of the Risk-Based Adaptive Authentication mechanism during the officer's continuous authentication. The interactions between the Risk-Based Adaptive Authentication mechanism components consist of a number of exchanged messages, which are grouped into the following steps:

Step 1: Once Officer's first-time authentication is successful and throughout their login session, MA, behind-the-scenes and without interrupting Officer's normal activities and missions, continuously monitors the User's and Device's attributes as described in Section III.B.4. If MA detects any changes regarding the User's and Device's attributes, then it updates the *User Profile* and *Device Profile accordingly*, (Message 1) and forwards the updated profiles to REA (Message 2). If MA detects any changes regarding only the User's *attributes*, it updates only the *User Profile* (Message 3), and forwards the updated profile to REA (Message 4). Similarly, if MA detects any changes regarding only the *Device's attributes*, then it updates only the Device profile (Message 5) and forwards the updated profile to REA (Message 6).

Step 2: As soon as REA receives the updated *User Profile and/or Device Profile*, it computes the risk score (Message 7) and forwards it to RLDA (Message 8).

Step 3: RLDA compares the risk score with the risk level thresholds to decide whether the estimated risk

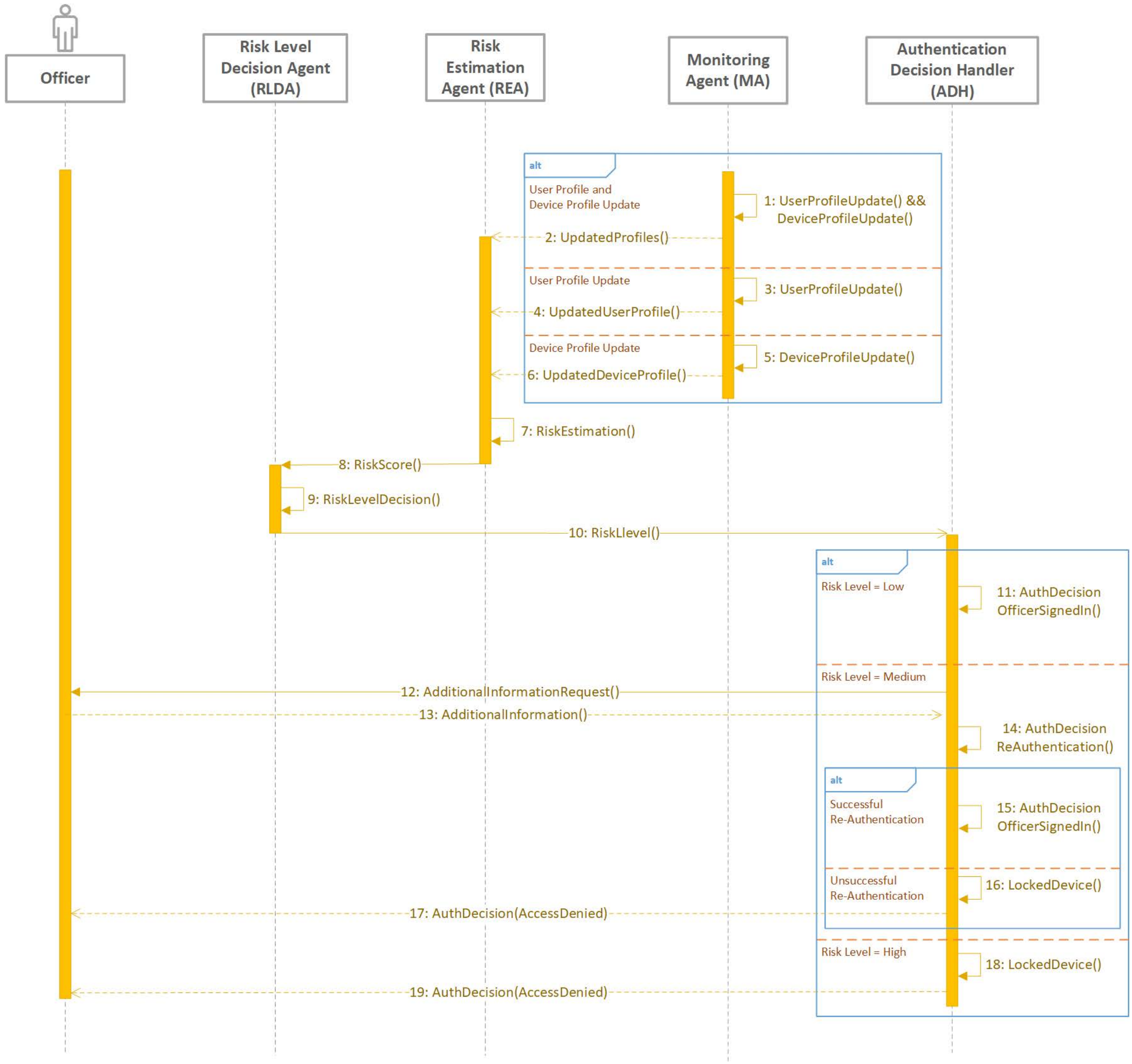
Officer
Risk Level Decision Agent (RLDA)
Risk Estimation Agent (REA)
Monitoring Agent (MA)
Authentication Decision Handler (ADH)
alt
User Profile and Device Profile Update
1: UserProfileUpdate() && DeviceProfileUpdate()
2: UpdatedProfiles()
User Profile Update
3: UserProfileUpdate()
4: UpdatedUserProfile()
Device Profile Update
5: DeviceProfileUpdate()
6: UpdatedDeviceProfile()
7: RiskEstimation()
8: RiskScore()
9: RiskLevelDecision()
10: RiskLlevel()
alt
Risk Level = Low
11: AuthDecision OfficerSignedIn()
Risk Level = Medium
12: AdditionalInformationRequest()
13: AdditionalInformation()
14: AuthDecision ReAuthentication()
alt
Successful Re-Authentication
15: AuthDecision OfficerSignedIn()
Unsuccessful Re-Authentication
16: LockedDevice()
17: AuthDecision(AccessDenied)
Risk Level = High
18: LockedDevice()
19: AuthDecision(AccessDenied)

FIGURE 8. The sequence diagram of officer's continuous authentication.

score is low, medium, or high (Message 9). Afterwards, RLDA forwards the Risk Level to ADH (Message 10).

Step 4: When the risk level is low, the Officer remains signed-in (Message 11).

Step 5: When the risk level is medium, the Officer is requested by ADH to provide additional authentication information (i.e., iris-based authentication) (Message 12). As soon as the Officer provides the requested additional information to ADH (Message 13), ADH performs re-authentication based on iris-based user authentication (Message 14). If the re-authentication is successful, the Officer is allowed to remain signed-in (Message 15). If the re-authentication is unsuccessful, the device is locked (Message 16) and ADH forwards an "Access Denied" message to the Officer (Message 17).

Step 6: When the risk level is high, the device is locked (Message 18) and ADH forwards an "Access Denied" message to the Officer (Message 19).

IV. PERFORMANCE EVALUATION OF MACHINE LEARNING ALGORITHMS FOR RISK-BASED ADAPTIVE USER AUTHENTICATION

Initially, we focused on the investigation of the performance of the following most popular classification algorithms for risk-based authentication, relying on user's contextual information and user's activity: K-NN, DT, SVM, and NB.

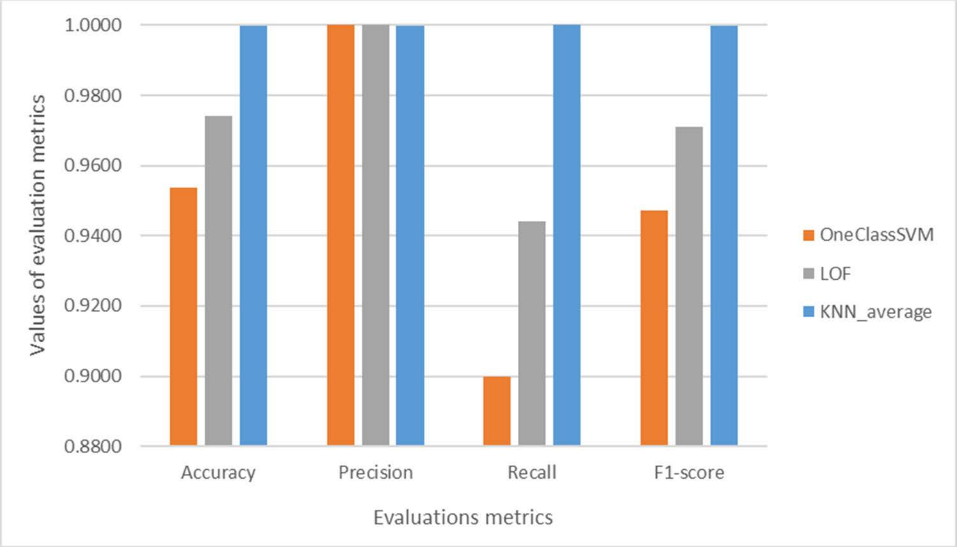

FIGURE 9. Evaluation metrics for novelty detection for the "HuMIdb" dataset.

These algorithms are considered to run on REA and the output of these algorithms will be input in the risk estimation module in REA. Using ten-fold cross validation, we trained and tested these classification algorithms over the same data of the HuMIdb dataset [17], [18]: the data related to the first user (i.e., user000), who was considered as the normal one, and the data related to the second user (i.e., user001) who was considered as the malicious one. In addition, the "HuMldb" dataset was modified by removing all features related to bluetooth, gps, wifi, micro, humidity, proximity, temperature, and light in the "HuMldb" 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 classification algorithms was evaluated by the evaluation metrics of accuracy, precision, recall, and F1-score.

However, the evaluation results demonstrated impact of overfitting and therefore, we considered the following novelty detection algorithms to overcome the challenge of overfitting: 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. To the best of our knowledge, this is the first time that novelty detection algorithms have been considered for risk-based adaptive user authentication. Similar to the classification algorithms, these novelty detection algorithms are considered to run on REA and the output of these algorithms will be input in the risk estimation module in REA.

A. DATASET PRE-PROCESSING AND NORMALIZATION

In principle, it is necessary to prepare the datasets before they are utilized to train and test ML algorithms. The preparation of the data includes: a) data pre-processing; and b) data normalization. The pre-processing step involves the removal of unnecessary features and the conversion of the nominal values of the categorical features to numeric values. However, in our case, there were no unnecessary features which were required to be removed and the values of all features were already numeric. Thus, the data pre-processing step was omitted for the of the HuMIdb dataset that was selected for training and testing the classification algorithms and the novelty detection algorithms.

TABLE 3. Summary of the hyperparameters of each classification algorithm.

ML algorithm	Hyperparameters
Decision Tree	1) The Gini index was used to select tree nodes. 2) Minimum samples per leaf node set to 10.
Naïve Bayes	The Gaussian variant of the NB algorithm was used.
Logistic Regression	-
Support Vector Machine	The Gaussian radial basis function (RBF) was set as the kernel function.
K-Nearest Neighbor	1) The value of K was set to 5. 2) The Euclidean distance was set as the distance metric.

On the other hand, the data normalization step was performed to the numeric values of each feature. If the values

TABLE 4. Evaluation metrics for novelty detection for the "HuMIdb" dataset.

ML algorithm	Accuracy	Precision	Recall	F1-Score
DT	1,0000	1,0000	1,0000	1,0000
NB	1,0000	1,0000	1,0000	1,0000
LR	1,0000	1,0000	1,0000	1,0000
SVM	1,0000	1,0000	1,0000	1,0000
KNN	1,0000	1,0000	1,0000	1,0000

TABLE 5. Summary of the hyperparameters of each novelty detection algorithm.

ML algorithm	Hyperparameters
One-Class SVM	1) The Gaussian radial basis function (RBF) was set as the kernel function. 2) The number (i.e., nu parameter) representing both an upper bound on the fraction of training errors and a lower bound o the fraction of support vectors was set to 0,1. 3) The kernel coefficient (i.e., gamma parameter) for the RBF kernel was set to 0,1.
Local Outlier Factor	The number of neighbors to be used for queries was set to 20.
KNN	1) The number of neighbors to be used was set to 5. 2) The contamination parameter representing the percentage of abnormal samples in the dataset was set to a very small value (i.e., 0,0001). 3) The average distance to k nearest neighbors was used in order to measure the legitimacy of the sample.

of a feature are significantly larger compared to the values of other features, this may lead to inaccurate results. Thus, data normalization helps to ensure that features with significantly large values do not outweigh features with smaller values. To achieve this, all of the features' values are scaled within the range of [0.0, 1.0] by performing a min–max normalization process on each feature. This normalization process is described by the following equation:

$$z = (x - x_{\min})/(x_{\max} - x_{\min}) \tag{4}$$

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 MACHINE LEARNING ALGORITHMS

Both the classification algorithms and the novelty detection algorithms were trained and tested over the same data of the HuMIdb dataset. Initially, the dataset was split into two parts: the train part and the test part. The train part consisted of 80% of the dataset and the ML algorithms were trained and evaluated with this part. On the other hand, the test part consisted of 20% of the dataset and was held back for further evaluation of the models with unseen data. The percentage split of 80% train–20% test was determined according to [58] as the best ratio to avoid the overfitting problem. After that, the training process of each ML algorithm over each dataset was performed using the ten-fold cross validation method. According to this method, the training dataset is divided into ten subsets of equal size and the records of each subset are randomly selected. The training process is repeated ten times. Each time, nine of the ten subsets are utilized for the training of the ML algorithms and the remaining subset is used for validation.

TABLE 6. Evaluation metrics for novelty detection for the "HuMIdb" dataset.

ML algorithm	Accuracy	Precision	Recall	F1-Score
OneClassSVM	0,9536	1,0000	0,8998	0,9471
LOF	0,9740	1,0000	0,9440	0,9711
KNN_average	0,9998	0,9997	1,0000	0,9998

In our experiments, the Python language version 3.9.7 was used, along with the Scikit-Learn [59] library and the PyOD [60] library. We utilized specific functions of the Scikit-Learn library and the PyOD library, and a Python script was created utilizing these functions in order to perform the training and testing of the four classification algorithms and the thee novelty detection algorithms.

C. PERFORMANCE EVALUATION RESULTS–CLASSIFICATION ALGORITHMS

The performance results were produced by averaging the results of the ten folds [58]. Table 3 presents a summary of the hyperparameters of each ML algorithm. The numerical results of the evaluation metrics for the selected ML algorithms, when applied to the "HuMIdb" dataset, are shown in Table 4.

Through the training process, it was noticed that the generated models used to become very closely related to training data with specific training features (e.g., pressure) and thus, perfect scores in terms of accuracy, precision, recall and F1 score were achieved by the models. However, these scores cannot be considered as reliable since they are derived from overfitted models which are strongly reliant and biased towards specific features of the training data. Therefore, the classification algorithms tested in this work were not selected as proper algorithms for REA component of the proposed user authentication mechanism.

D. PERFORMANCE EVALUATION RESULTS–NOVELTY DETECTION ALGORITHMS

The performance results were produced by averaging the results of the ten folds [58]. Table 5 presents a summary of the hyperparameters of each algorithm. The numerical results of the evaluation metrics for the selected ML algorithms, when applied to the ''HuMIdb'' dataset, are shown in Table 6 and Figure 9.

It can be easily observed that all ML algorithms demonstrate a high performance for the ''HuMIdb'' dataset. The KNN algorithm is accurate almost in all cases (i.e., 0,99), followed by the LOF and OneClassSVM methods (i.e., 0,97 and 0,95). As far as the rest of the evaluation metrics (i.e., precision, recall, and F1-score), the KNN algorithm continues to demonstrate slightly better performance compared to the LOF and OneClassSVM algorithms.

V. CONCLUSION AND FUTURE WORK

As innovative services and products take off, digitalization becomes integral part of our daily lives in a wide spectrum of applications. For instance, critical sectors such as transport become progressively more dependent on digital technologies to perform their core activities and develop novel efficient transport services and infrastructure to exploit the economic strengths of the EU. Although the continuously increasing number of visitors entering the EU through land-border crossing points and/or seaports brings immense economic value, novel border control solutions, such as mobile devices for passenger identification for land and sea border control, are essential to precisely identify passengers ''on the fly'' ensuring their comfort. Therefore, novel secure and usable user authentication mechanisms are required to increase the level of security of new mobile devices for passenger identification used by border control officers at land and sea borders, without interrupting border control activities.

Towards this direction, we provide a review of related work on user authentication solutions for mobile devices, discuss the security vs. usability challenge, and then present background concepts on risk-based and adaptive authentication. Our objective is to provide a foundation for organizing research efforts towards the design and development of effective and efficient risk-based adaptive user authentication mechanisms for mobile passenger identification devices used by border control officers at land and sea borders. Besides that, a novel risk-based adaptive user authentication mechanism is proposed providing the mechanism architecture, the mechanism components, the sequence diagram of officer's first-time authentication and the sequence diagram of officer's continuous authentication.

On top of that, we 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. These algorithms are considered to run on REA and the output of these algorithms will be input in the risk estimation module in REA. However, the evaluation results demonstrated impact of overfitting and therefore, we considered the following novelty detection algorithms to overcome the challenge of overfitting: 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 they are applied in order to distinguish between a known legitimate user and an unknown malicious user. To the best of our knowledge, this is the first time that novelty detection algorithms have been considered for risk-based adaptive user authentication demonstrating promising results.

Our next steps include evaluation of other classification algorithms, as well as novelty detection algorithms for risk-based adaptive authentication, relying not only on user's contextual information and behavior, but also on device's contextual information and behavior. Afterwards, the next step will be focused on the risk estimation module within the REA component of the proposed authentication mechanism. It is intended the risk estimation module to take as input the output of the classification or novelty detection algorithms (i.e., a binary vector, the length of which, is equal to the number of entries in the ''on-the-fly'' dataset) and output the value of the overall ''on-the-fly'' risk score which then will be forwarded to RLDA component to decide whether the estimated risk score is low, medium, or high. Finally, we are planning to implement and evaluate the performance of the proposed risk-based adaptive user authentication mechanism on the mobile devices for passenger identification at land and sea borders. In particular, we will investigate the incurred overhead when the proposed mechanism runs on the mobile device. As a mobile device for this implementation, a Raspberry pi 4 with Android OS will be considered.

REFERENCES

[1] B. Jakobsen, B. T. Muguruza, D. C. de Magalhaes, A. Ballester, and M. Sweerts, ''Challenges to effective EU cybersecurity policy—Briefing paper,'' *Eur. Court Audit.*, pp. 1–74, Mar. 2019.

[2] *The Global Risks Report 2021*, 16th ed., World Econ. Forum, Cologny, Switzerland, 2021.

[3] V. Sucasas, G. Mantas, M. Papaioannou, and J. Rodriguez, ''Attribute-based pseudonymity for privacy-preserving authentication in cloud services,'' *IEEE Trans. Cloud Comput.*, early access, May 27, 2021, doi: 10.1109/TCC.2021.3084538.

[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 *Proc. IEEE 26th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Oct. 2021, pp. 1–5.

[5] *Transport in the European Union: Current Trends and Issues*, Mobility Transp., Eur. Commission, Brussels, Belgium, Apr. 2018, p. 144.

[6] 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 *Proc. 12th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, Jul. 2020, pp. 8–13.

[7] 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 *Proc. IEEE 26th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Oct. 2021, pp. 1–6.

[8] 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," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 164–172, Feb. 2020.

[9] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats and trends," *Comput. Netw.*, vol. 170, Apr. 2020, Art. no. 107118.

[10] G. Mantas, N. Komninos, J. Rodriguez, E. Logota, and H. Marques, "Security for 5G communications," in *Fundamentals of 5G Mobile Networks*, J. L. Rodriguez, Eds. Chichester, U.K.: Wiley, 2015, pp. 207–220.

[11] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "A survey on security threats and countermeasures in internet of medical things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, pp. 1–15, Jul. 2020.

[12] 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.

[13] F. P. Oikonomou, J. Ribeiro, G. Mantas, J. M. C. S. Bastos, and J. Rodriguez, "A hyperledger fabric-based blockchain architecture to secure IoT-based health monitoring systems," in *Proc. IEEE Int. Medit. Conf. Commun. Netw. (MeditCom)*, Sep. 2021, pp. 186–190.

[14] M. Papaioannou, G. Mantas, and J. Rodriguez, "Risk-based user authentication for mobile passenger ID devices for land and sea border control," in *Proc. IEEE Int. Medit. Conf. Commun. Netw. (MeditCom)*, Sep. 2021, pp. 180–185.

[15] Y.-Y. Choong, J. M. Franklin, and K. K. Greene, "Usability and security considerations for public safety mobile authentication," U.S. Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Interagency Rep. 8080, Jul. 2016, vol. 8080, doi: 10.6028/NIST.IR.8080.

[16] S. Gupta, A. Buriro, and B. Crispo, "Demystifying authentication concepts in smartphones: Ways and types to secure access," *Mobile Inf. Syst.*, vol. 2018, pp. 1–16, Mar. 2018.

[17] 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," May 2020, *arXiv:2005.13655*.

[18] A. Acien, A. Morales, J. Fierrez, R. Vera-Rodriguez, and I. Bartolome, "BeCAPTCHA: Detecting human behavior in smartphone interaction using multiple inbuilt sensors," 2020, *arXiv:2002.00918*.

[19] B. Schneier, *Applied Cryptography*, vol. 1, no. 32. Hoboken, NJ, USA: Wiley, 1996.

[20] 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.

[21] A. J. Harris and D. C. Yen, "Biometric authentication: Assuring access to information," *Inf. Manage. Comput. Secur.*, vol. 10, no. 1, pp. 12–19, Mar. 2002.

[22] 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-recognition-tricked-with-a-photo-2017-3?IR=T

[23] 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-one-week-115-mask/

[24] A. Charles, "The guardian-iPhone 5S fingerprint sensor hacked by Germany's chaos computer club," 2013. [Online]. Available: https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security

[25] 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.

[26] 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 *Proc. 9th EAI Int. Conf. Broadband Commun., Netw., Syst. (BROADNETS)*, 2018, pp. 139–148.

[27] A. Buriro, B. Crispo, F. Delfrari, and K. Wrona, "Hold and sign: A novel behavioral biometrics for smartphone user authentication," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2016, pp. 276–285.

[28] Y. Obuchi. (2006). *PDA Speech Database*. [Online]. Available: http://www.speech.cs.cmu.edu/databases/pda/index.html

[29] N. Forsblom. (2015). *Were You Aware of All These Sensors in Your Smartphone?* [Online]. Available: https://blog.adtile.me/2015/11/12/wereyou-%0Aaware-of-all-these-sensors-in-your-smartphone/

[30] A. De Luca, A. Hang, E. Von Zezschwitz, and H. Hussmann, "I feel like I'm taking selfies all day! Towards understanding biometric authentication on smartphones," in *Proc. Conf. Hum. Factors Comput. Syst.*, Apr. 2015, pp. 1411–1414.

[31] J. M. Franklin, G. Howell, S. Ledgerwood, and J. L. Griffith, "Draft NISTIR 8196, Security analysis of first responder mobile and wearable devices," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Interagency Rep. 8196, 2020, doi: 10.6028/NIST.IR.8196.

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

[33] N. Clarke, "Frictionless user authentication," in *Encyclopedia of Cryptography, Security and Privacy*, S. Jajodia, P. Samarati, and M. Yung, Eds. Berlin, Germany: Springer, 2019, pp. 1–5.

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

[35] A. Buriro, B. Crispo, M. Eskandri, S. Gupta, A. Mahboob, and R. V. Acker, "Snap auth: A gesture-based unobtrusive smartwatch user authentication scheme," in *Proc. Int. Workshop Emerg. Technol. Authorization Authentication*, 2018, pp. 30–37.

[36] T. Van Hamme, V. Rimmer, D. Preuveneers, W. Joosen, M. A. Mustafa, A. Abidin, and E. A. Rúa, "Frictionless authentication systems: Emerging trends, research challenges and opportunities," 2018, *arXiv:1802.07233*.

[37] EMC Corporation. (2015). *The RSA Risk Engine*. [Online]. Available: https://dl.icdst.org/pdfs/files1/850b0425c53be7709124a59491062a16.pdf

[38] J. Spooren, D. Preuveneers, and W. Joosen, "Mobile device fingerprinting considered harmful for risk-based authentication," in *Proc. 8th Eur. Workshop Syst. Secur.*, Apr. 2015, pp. 1–6.

[39] M. T. Gebrie and H. Abie, "Risk-based adaptive authentication for Internet of Things in smart home eHealth," in *Proc. 11th Eur. Conf. Softw. Archit., Companion*, Sep. 2017, pp. 102–108.

[40] W. A. Jansen, T. Winograd, and K. Scarfone. (2008). Guidelines on active content and mobile code. Recommendations of the National Institute of Standards and Technology. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-28ver2.pdf

[41] T. Lederm and N. L. Clarke, "Risk assessment for mobile devices," in *Proc. Int. Conf. Trust, Privacy Secur. Digit. Bus.*, 2011, pp. 210–221.

[42] R. M. Blank and P. D. Gallagher, "Guide for conducting risk assessments," U.S. Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Special Publication 800–30 Revision, Interagency Rep. 800-30, 2012, vol. 1. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[43] D. W. Hubbard and R. Seiersen, *How to Measure Anything in Cybersecurity Risk*. Hoboken, NJ, USA: Wiley, 2016.

[44] M. Ghazouani, S. Faris, H. Medromi, and A. Sayouti, "Information security risk assessment a practical approach with a mathematical formulation of risk," *Int. J. Comput. Appl.*, vol. 103, no. 8, pp. 36–42, Oct. 2014.

[45] H. F. Atlam, A. Alenezi, R. J. Walters, and G. B. Wills, "An overview of risk estimation techniques in risk-based access control for the Internet of Things," in *Proc. 2nd Int. Conf. Internet Things, Big Data Secur. (IoTBDS)*, 2017, pp. 254–260.

[46] M. Heydari, A. Mylonas, V. Katos, E. Balaguer-Ballester, V. H. F. Tafreshi, and E. Benkhelifa, "Uncertainty-aware authentication model for fog computing in IoT," in *Proc. 4th Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Jun. 2019, pp. 52–59.

[47] K. Shang and Z. Hossen. (2013). Applying fuzzy logic to risk assessment and decision-making. Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries. [Online]. Available: https://www.soa.org/globalassets/assets/Files/Research/Projects/research-2013-fuzzy-logic.pdf

[48] S. Wang, C. Fan, C.-H. Hsu, Q. Sun, and F. Yang, "A vertical handoff method via self-selection decision tree for internet of vehicles," *IEEE Syst. J.*, vol. 10, no. 3, pp. 1183–1192, Sep. 2016.

[49] M. Friedman and A. Kandel, "On the design of a fuzzy intelligent differential equation solver," in *Fuzzy Expert Systems*, A. Kandel, Ed. Boca Raton, FL, USA: CRC Press, 1991.

[50] L. A. Zadeh, "On fuzzy algorithms," in *Fuzzy Sets, Fuzzy Logic, and Fuzzy Systems: Selected Papers*. USA: World Scientific, 1996, pp. 127–147.

[51] S. A. V. Goerdin, J. J. Smit, and R. P. Y. Mehairjan, "Monte Carlo simulation applied to support risk-based decision making in electricity distribution networks," in *Proc. IEEE Eindhoven PowerTech*, Jun. 2015, pp. 1–5.

[52] Identity Automation. (2017). *Risk-Based Authentication*. [Online]. Available: https://blog.identityautomation.com/what-is-risk-based-authentication-types-of-authentication-methods

[53] A. Hurkala and J. Hurkala, "Architecture of context-risk-aware authentication system for web environments," in *Proc. ICIEIS*, 2014, pp. 219–228.

[54] I. Witten, E. Frank, and M. Hall, *Data Mining*. Amsterdam, The Netherlands: Elsevier, 2011.

[55] N. Yousefi, M. Alaghband, and I. Garibay, "A comprehensive survey on machine learning techniques and user authentication approaches for credit card fraud detection," 2019, pp. 1–27, *arXiv:1912.02629*.

[56] I.-C. Yeh and C.-H. Lien, "The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients," *Expert Syst. Appl.*, vol. 36, no. 2, pp. 2473–2480, Mar. 2009.

[57] M. Misbahuddin, B. S. Bindhumadhava, and B. Dheeptha, "Design of a risk based authentication system using machine learning techniques," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Aug. 2017, pp. 1–6.

[58] A. Géron, *Hands-On Machine Learning With Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*. Sebastopol, CA, USA: O'Reilly Media, 2019.

[59] F. Pedregosa, S. Varoquaux, A. Gramfort, V. Michel, and B. Thirion, "Scikit-learn: Machine learning in Python," *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, Dec. 2011.

[60] 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, Jan. 2019.

MARIA PAPAIOANNOU (Student Member, IEEE) received the Diploma degree in electrical and computer engineering and the M.Sc. degree in biomedical engineering from the University of Patras, Greece, in 2016 and 2018, respectively. She is currently pursuing the Ph.D. degree in engineering with the University of Greenwich, U.K. Since 2018, she has been a member of the 4TELL Research Group, Instituto de Telecomunicações, Aveiro, Portugal, where she has been involved in research projects, such as POCI-01-0247-FEDER-024539 5G Mobilizador, where her focus was on the deployment of a privacy-preserving user authentication protocol for Smart City applications and H2020-MSCA-RISE-2019-eBORDER-872878, where she is currently working on the design and implementation of secure authentication mechanisms. Her research interests include user authentication and access control, privacy-preserving authentication, and threat modeling.

GEORGIOS ZACHOS (Student Member, IEEE) received the Diploma degree in electrical and computer engineering from the University of Patras, Greece, in 2020. He is currently pursuing the Ph.D. degree in engineering with the University of Greenwich, U.K. Since January 2021, he has been a member of the 4TELL Research Group, Instituto de Telecomunicações, Aveiro, Portugal, and he has been involved in the European research projects H2020-ECSEL-2019-IA-876190–Moore4Medical and H2020-MSCA-RISE-2019-872878-eBORDER, where his focus is on the development of anomaly-based intrusion detection systems for Internet of Medical Things networks and for passenger identification mobile devices at land/sea border, respectively. His research interests include machine learning (ML) algorithms, dataset generation methods, anomaly-based intrusion detection mechanisms, and network and system security.

ISMAEL ESSOP received the B.Sc. degree in computer science in 1997 and the M.Sc. degree in distributed computer systems from the School of Computing and Mathematical Sciences. He is currently pursuing the Ph.D. degree in engineering with the University of Greenwich. He is an experienced academic with over 20 years of experience in higher education. In 2001, he joined the University of Greenwich, as a Lecturer in computer engineering, where he was promoted to a Principal Lecturer, in 2017. Since then, he has led several programmes, both at undergraduate and postgraduate levels. He is also a Partnership Lead for universities in Europe and Middle East. He has been involved in European Research projects, such as the INTERREG Programme.

GEORGIOS MANTAS (Member, IEEE) received the five-year Diploma degree in electrical and computer engineering from the University of Patras, Greece, in 2005, the M.Sc. degree in information networking from Carnegie Mellon University, Pittsburgh, PA, USA, in 2008, and the Ph.D. degree in electrical and computer engineering from the University of Patras, in 2012. In 2014, he became a Postdoctoral Researcher with the Instituto de Telecomunicações, Aveiro, Portugal, where he has been involved in research projects, such as H2020-MSCA-ITN-SECRET, ECSEL-IA-SemI40, CATRENE-MobiTrust, ARTEMIS-ACCUS, and FP7-SEC-SALUS. Since 2020, he has been a Senior Lecturer with the University of Greenwich, U.K.

JONATHAN RODRIGUEZ (Senior Member, IEEE) received the master's degree in electronic and electrical engineering and the Ph.D. degree from the University of Surrey, U.K., in 1998 and 2004, respectively. In 2005, he became a Researcher with the Instituto de Telecomunicações, Portugal, and achieved Senior status, in 2008. He has served as a Project Coordinator for major international research projects, including Eureka LOOP, FP7 C2POWER, and H2020-ITN-SECRET, while serving as the Technical Manager for FP7 COGEU and FP7 SALUS. In 2009, he has been an Invited Assistant Professor with the University of Aveiro, Portugal, and attained Associate Level, in 2015. In 2017, he was appointed as a Professor of mobile communications with the University of South Wales, U.K. He has authored more than 600 scientific works, including ten book editorials. He is a Chartered Engineer (2013) and an IET Fellow (2015).