EURASIP Journal on
Information Security

RESEARCH Open Access

Behavior-based user authentication on mobile devices in various usage contexts

Dmytro Progonov[1,2*], Valentyna Cherniakova[1], Pavlo Kolesnichenko[1] and Andriy Oliynyk[1,3]

Abstract

Reliable and non-intrusive user identification and authentication on mobile devices, such as smartphones, are topical tasks today. The majority of state-of-the-art solutions in this domain are based on "device unlock" scenario—checking of information (authentication factors) provided by the user for unlocking a smartphone. As such factors, we may use either single strong authentication factor, for example, password or PIN, or several "weaker" factors, such as tokens, biometrics, or geolocation data. However, these solutions require additional actions from a user, for example, password typing or taking a fingerprint, that may be inappropriate for on-the-fly authentication. In addition, biometric-based user authentication systems tend to be prone to presentation attack (spoofing) and typically perform well in fixed positions only, such as still standing or sitting.

We propose BehaviorID solution that is passwordless (transparent) user-adaptive context-dependent authentication method. The feature of BehaviorID is usage of new "device lock" scenario—smartphone is stayed unlocked and can be fast locked if non-owner's actions are detected. This is achieved by tracking of user's behavior with embedded sensors after triggering events, such as actions in banking apps, e-mails, and social services. The advanced adaptive recurrent neural network (A-RNN) is used for accurate estimation and adaptation of behavioral patterns to a new usage context. Thus, proposed BehaviorID solution allows reliable user authentication in various usage contexts by preserving low battery consumption.

Performance evaluation of both state-of-the-art and proposed solutions in various usage contexts proved the effectiveness of BehaviorID in real situations. Proposed solution allows reducing error levels up to three times in comparison with modern Abuhamad's solutions (Abuhamad et al., IEEE Internet Things J 7(6):5008–5020, 2020) (about 0.3% false acceptance rate (FAR) and 1.3% false rejection rate (FRR)) by preserving high robustness to spoofing attack (2.5% spoof acceptance rate (SAR)). In addition, BehaviorID showed low drift of error level in case of long-term usage in contrast to modern solutions. This makes the proposed BehaviorID solution an attractive candidate for next-generation behavior-based user authentication systems on mobile devices.

Keywords: Authentication, Behavior analysis, Recurrent neural networks, Mobile devices

Mathematics subject classification: Primary, 94A62, Secondary 94A12

1 Introduction

Mobile devices become pervasive in business processes, including corporate systems, e-mails, social networks, and banking. It results in wealth of on-device stored sensitive information such as user's credentials, payments, geolocation data, and device usage history. Important part of this information protection is usage of effective access control system (ACS), namely for identification and authentication of a user [1].

*Correspondence: d.progonov@samsung.com

[2] Institute of Physics and Technology, Igor Sikorsky Kyiv Polytechnic Institute, 37, Prospect Peremohy, 03056 Kyiv, Ukraine
Full list of author information is available at the end of the article

© The Author(s) 2022. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Modern ACS is based on checking of something that a user knows (a password or a passphrase), possesses (a token), or is (biometrics and behavioral templates) [2, 3]. The first and second factors provide strong authentication at the cost of usability, namely necessity of a password typing or carrying an additional equipment (token) with a smartphone. On the other hand, biometric-based authentication solutions allows improving usability by preserving low error rate. Nevertheless, these solutions are vulnerable to presentation attack, namely spoofing of biometric data attackers [3, 4].

Promising approach is provided by modern behavior-based authentication technologies. Typically, they are based on biometric data capturing and extracting user-specific behavioral patterns needed for the analysis of several modalities during user interactions with mobile devices [5–7]. However, the performance of these systems significantly depends on the context, namely user's activity (motionless, walking, running) and application in use [8]. Thus, spoofing-proof transparent user-friendly methods for user authentication are needed.

The contribution of the paper is summarized as follows:

- We propose the BehaviorID method for transparent context-dependent behavior-based user authentication on mobile devices. BehaviorID is based on tracking and updating user behavioral templates for various context using device's embedded sensors. Also, the proposed method allows for fast adaptation of behavioral templates to work with new (previously unseen) usage contexts.
- The BehaviorID method has been benchmarked with keystroke dynamics modality in three cases: typing fixed text in fixed context, typing arbitrary text in fixed context, and typing arbitrary text in varying context. According to the obtained results, the proposed method preserves low error rate for all considered use cases (about 0.3% FAR, 1.3% FRR, and 2.5% SAR).
- It was shown that the proposed method outperformed the modern Abuhamad et al. method [9] in the most difficult case of long-term tracking of behavioral pattern (about 2.1% FAR and 3.9% FRR). The obtained results proved that BehaviorID solution is suitable for on-device sensitive data processing (class 3, strong biometric tier) for Android tiered authentication model (ATAM) (about 5% for fixed usage context).
- The fast detection of non-owner usage of a mobile device (within $0.5 - 1.0$ s for Samsung Galaxy S21 smartphone) with low error level makes the proposed method an attractive candidate for transparent user authentication on next-generation smartphones

The rest of this paper is organized as follows. Notations are presented in Section 2. Section 3 gives an overview of the modern ACS systems for mobile devices. In Section 4, we introduce a user-adaptive multimodal context-dependent behavior-based authentication method and compare it with the state-of-the-art solutions. The results of performance and accuracy evaluation are in Section 5. Section 6 concludes the paper.

2 Preliminaries

High-dimensional arrays, matrices, and vectors are denoted in boldface. Their individual elements are denoted by the corresponding lower-case letters in italic. The calligraphic font is reserved for sets. If nothing additionally specified, we suppose that an element x from a set $\mathcal{X}$ is sampled according to a uniform distribution.

3 Related works

Modern ACS provide wide range of authentication options, while revealing a number of risks for users and infrastructure providers. The most important risks are identity theft and eavesdropping, phishing, inadequate device's resource usage, personal and corporate data blending, vulnerability of biometric-based ACS to spoofing, and usage context shift [1, 10].

Modern multifactor authentication and access control solutions, such as RSA SecurID [11], NuData Security [12], Touch ID and Face ID [13], and SecureAuth [14], address these challenges. The diagram of used authentication factors for these solutions is presented in Fig. 1.

The RSA SecurID and Amazon GuardDuty [15] are comprehensive solutions that rely on knowledge and possession-based authentication factors (Fig. 1). The SecureAuth system includes biometric-based factors for improving robustness of ACS to password leakages. Full biometric-based ACS solutions for mobile devices are TouchID and FaceID of Apple Inc. Unfortunately, these solutions are vulnerable to spoofing attacks that limits their usage for sensitive information processing. In addition, TouchID and FaceID solutions need additional actions from users, such as fingerprint check during launching of banking application, that may negatively impact user experience.

A variety of behavior-based authentication systems were proposed for smartphones in the last years, such as MasterCard NuData [12], TwoSense.AI [16], BioSig-ID [17], OneSpan [18], and Zighra [19]. These solutions can be compared by the types of used behavioral features, abilities of tracking/update person's behavioral profile, and engaged device sensors (Table 1).

The all-in-one ACS solutions, such as MasterCard NuData, TwoSense.AI, and OpenSpan, use location-based features for counteracting spoofing attack based

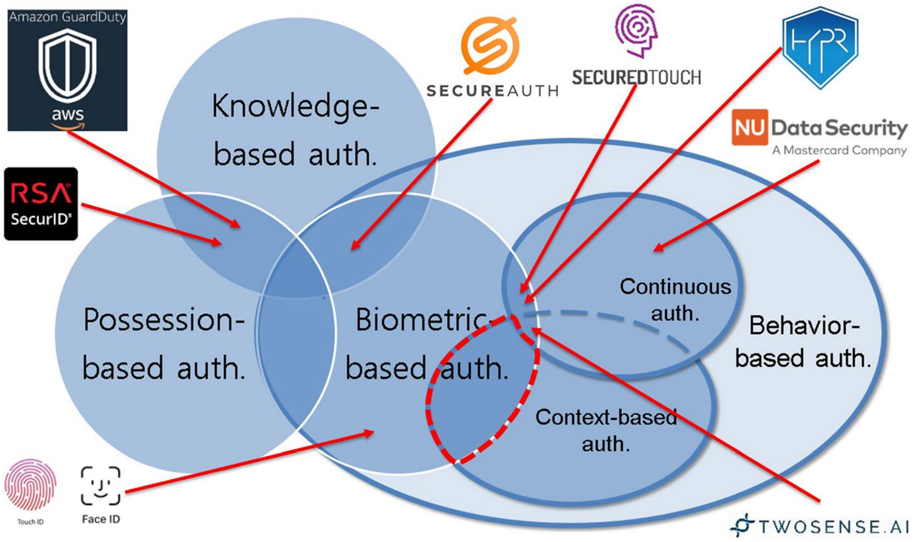

Fig. 1 Landscape of authentication solutions for mobile devices. Despite high usability, the domain of context-dependent behavior-based authentication (marked with dashed red line) does not attract much attention yet

Table 1 Comparison of state-of-the-art commercial solutions in the domain of behavior-based user authentication on mobile devices

Solution	MasterCard NuData	TwoSense.AI	BioSig–ID	OneSpan	Zighra
Authentication method	Behavior-based	Continuous and multi-factor	Multifactor	Multifactor	Continuous and multi-factor
Used sensors	Motion sensor, touch-screen, GPS, wireless adapters	Motion sensor, touch-screen, front-facing camera, GPS	Touchscreen	Motion sensor, touchscreen, front-facing camera	Motion sensor, touch-screen
On-device solution	No	No	No	Yes	Yes
Behavioral profile's update	No	No	No	No	No
Used modalities	Apps usage, geolocation, keystroke dynamics, device tilts, wireless connections	Touchscreen, apps usage, keystroke dynamics, geolocation, gaits	PIN or password, gestures on touchscreen	Apps usage, keystroke dynamics, wireless connections	Apps usage, keystroke dynamics, wireless connections
Transparent (password-less) authentication	Yes	Yes	No	Yes	Yes
Context-adaptive	No	No	No	Yes	No

on user device cloning (Table 1). Nevertheless, analysis of the user's location may raise privacy concerns. Also, these solutions require connection to external databases with user profiles that may be inappropriate for offline use cases.

The modern solutions for continuous multifactor user authentication, such as OneSpan and Zighra (Table 1), rely on detection of unusual usage patterns. However, these solutions provide limited opportunities to track behavioral profile's alterations caused by the user's habit changes. Thus, users may be required for regular update of their profiles that may be inconvenient.

The promising way to improve the accuracy of ACS system is analysis of the contextual information, namely applications usage and user's physical activity [20] (Fig. 1). The data retrieved from context-aware sources is more difficult for the attacker to manipulate which decreases the effectiveness of spoofing attack. Examples of context-aware ACS solutions are SecuredTouch (acquired by Ping Identity [21]), Samsung HYPR [22], NuData Security, and TwoSense.AI [16] (Fig. 1). These systems are continuously tracking both behavior-related features and contextual information, such as user location during use of banking apps. Despite the high authentication accuracy and robustness to spoofing, these solutions may be inappropriate for private users due to privacy violation concerns and high consumption of computation and battery resources [23, 24].

Therefore, a transparent on-device privacy-preserving user authentication solution is needed. This paper is devoted to fill this gap by development of a user-adaptive multimodal context-dependent behavior-based authentication method.

4 Proposed technology

To provide on-device context-dependent behavior-based authentication, we propose the BehaviorID solution. The flowchart of the user's features processing with proposed method is presented in Fig. 2.

The user authentication with the BehaviorID method starts from a triggering event, such as launch a predefined application (Fig. 2). Then, signals from the device's embedded sensors are being gathered until finalization trigger event, for instance, start typing in a launched application. The collected signals are preprocessed with dynamic time warping (DTW) algorithm to compensate the time shift between them [25].

At the second step, context recognition is performed using preprocessed signals. The recognition model is based on convolutional neural network (CNN) for feature extraction from inputted signals. Also, the prepared signals are combined into modalities to be processed. For instance, touchscreen keyboard timing and touch locations are transformed into type patterns.

At the third step, each modality is processed with advanced A-RNN model [26]. The feature of the network is usage of mixture layer to improve performance in case of processing sequences with multiple patterns, e.g., mixture of output signals from embedded sensors. The output of context recognition model is used as an external parameter for mixture layers of A-RNN to compensate possible alterations of of user behavioral profile.

Finally, the outputs of each A-RNN related to individual modality are processed with decision-making module (Fig. 2). In case of positive decision (user is authenticated), the user is notified about the success authentication, and the extracted features are used to update the A-RNN parameters. Otherwise, negative decision is reported (user is not recognized).

Applying of mixture layer for A-RNN allows tracking multiple patterns by preserving fixed computation complexity that is important for on-device usage [26]. In addition, update of A-RNN parameters taking into account the usage context allows compensating user behavioral profile alterations caused by user's habits changes. Let us describe this part of the proposed solution in more details. Description of A-RNN features is presented in Section 4.1. Modalities that were used are described in Section 4.2.

4.1 Adaptive recurrent neural network

Today, one of the most popular approach for solving sequence modeling tasks is based on usage of long short-term memory (LSTM) and gated recurrent unit (GRU) networks [27]. The LSTM network is based on

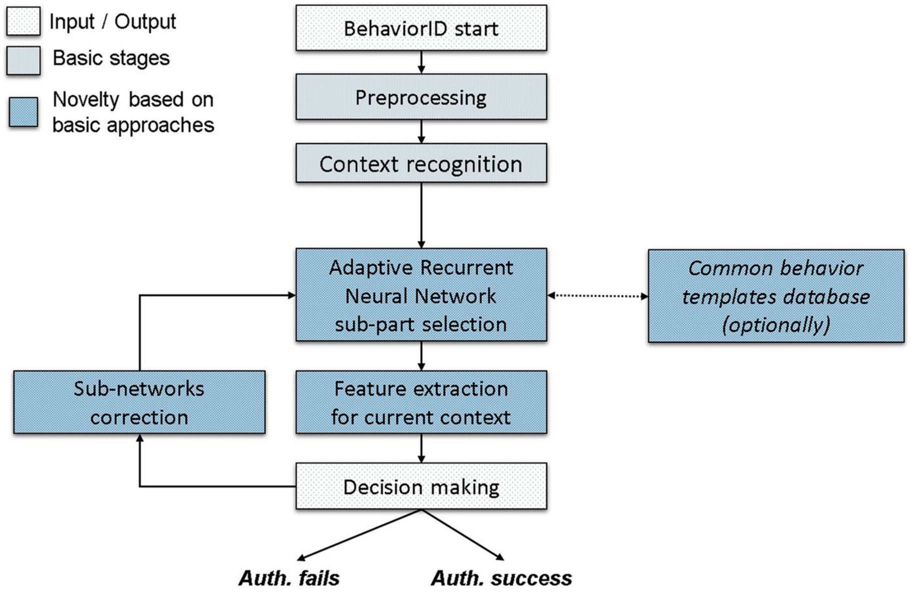
Input / Output
Basic stages
Novelty based on basic approaches
BehaviorID start
Preprocessing
Context recognition
Adaptive Recurrent Neural Network sub-part selection
Common behavior templates database (optionally)
Sub-networks correction
Feature extraction for current context
Decision making
Auth. fails
Auth. success

Fig. 2 User authentication procedure with proposed BehaviorID method

utilizing memory cells and a gating mechanism to control information flow. The GRU networks use simplified memory cells with a single update gate that controls forgetting and updating factors simultaneously.

Some advanced mechanisms appeared during the last years to extend LSTM and GRU functionality [27]. The first one is attention mechanism based on the estimation of the similarity between encoded source sentence and output words. The mechanism is particularly useful in machine translation, image captioning, and rating prediction tasks. Another mechanism is memory-augmented networks that use an external memory for each sequence. These networks aim to memorize the recent useful samples and compare them with the current ones within the input sequence. This approach is frequently used in meta and one-shot learning tasks. Nevertheless, these mechanisms are aimed at tracking a single template in inputted sequence [27]. This limits the usage of such methods in applications related to behavior analysis, where several patterns may present in gathered data at the same time.

Recently, the A-RNN was proposed by Zhao et al. [26] for modeling and memorizing multiple patterns in training sequences. This is achieved by applying a mixture layer to improve the performance of a single recurrent neural networks (RNN). Therefore, the mixture layer makes possible storage for the set of patterns in contrast to mixture of expert models, where the output is controlled by a sparse gating function [26]. The structure of mixture layer augmented A-RNN is illustrated in Fig. 3 [26].

The mixture layer is based on the usage of a matrix $\mathbf{M} \in \mathbb{R}^{m \times n}$ that contains n prototypes (patterns) from the training sequences, while each pattern has m elements (samples). Then, the hidden state $\mathbf{h}_{t-1}$ for RNN is able to represent the sub-sequence $(\mathbf{x}_1, \ldots, \mathbf{x}_{t-1})$ from an input sequence $(\mathbf{x}_1, \mathbf{x}_2, \ldots)$, $\mathbf{x}_i \in \mathbf{R}^m$ (Fig. 3).

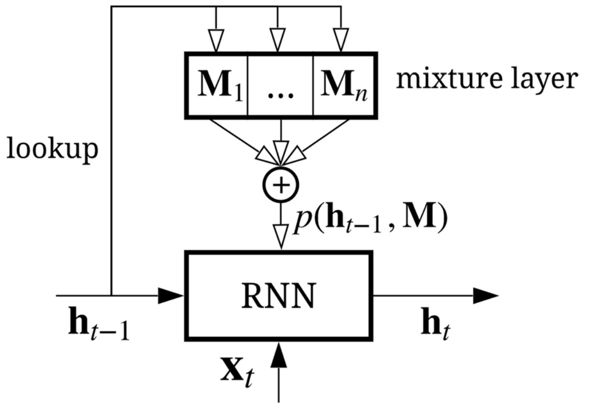

Fig. 3 Architecture of mixture layer in adaptive recurrent neural network. Here, $\mathbf{M}_1, \ldots, \mathbf{M}_n$ denote the patterns extracted from the training sequences

The similarity s_i between $\mathbf{h}_{t-1}$ and extracted patterns (columns of the matrix $\mathbf{M}_i, i \in [1; n]$) is used to produce a weight vector $\mathbf{w} = (w_1, \ldots, w_n)$ for scaling (amplifying or attenuating) each pattern [26]:

$$w_i = \frac{\exp(s_i)}{\sum_j \exp(s_j)}, i \in [1; n].$$

Consequently, the task of estimation probability of current state $p(\mathbf{h}_{t-1}, \mathbf{M})$ can be formulated as [26]:

$$p(\mathbf{h}_{t-1}, \mathbf{M}) = \sum_i w_i \mathbf{M}_i. \tag{1}$$

Therefore, the hidden states in A-RNN are updated in the following way [26]:

$$\mathbf{h}_t = g(\mathbf{h}_{t-1}, \mathbf{x}_t, p(\mathbf{h}_{t-1}, \mathbf{M})), \tag{2}$$

where $\mathbf{h}_t, \mathbf{h}_{t-1}$ are the hidden states of current cell on t and $(t-1)$ time steps correspondingly, $\mathbf{x}_t$ is the input vector on t time step, and $g(\cdot)$ is the activation function for RNN cell.

As an example of A-RNN, we used LSTM network augmented by mixture layer. Since the retrieved result of looking up matrix in mixture layer (1) is added to all gates and cells of LSTM, the forget gate $\mathbf{f}_t$ and the input gate $\mathbf{i}_t$ can be represented as [26]:

$$\begin{aligned} \mathbf{f}_t &= \sigma(\mathbf{W}_f[\mathbf{h}_{t-1}, \mathbf{x}, p(\mathbf{h}_{t-1}, \mathbf{M})] + \mathbf{b}_f), \\ \mathbf{i}_t &= \sigma(\mathbf{W}_i[\mathbf{h}_{t-1}, \mathbf{x}, p(\mathbf{h}_{t-1}, \mathbf{M})] + \mathbf{b}_i), \end{aligned}$$

where $\sigma(\cdot)$ is the sigmoid function, and $\mathbf{W}, \mathbf{b}$ are the weighting matrix and bias vector, respectively, for forget $(\mathbf{W}_f, \mathbf{b}_f)$, input $(\mathbf{W}_i, \mathbf{b}_i)$, and output $(\mathbf{W}_o, \mathbf{b}_o)$ gates. In the same way, the weighting matrix and bias vector for memory cell are defined as $\mathbf{W}_c$ and $\mathbf{b}_c$, respectively. Then, the memory cell $\mathbf{c}_t$ can be updated as [26]:

$$\begin{aligned} \tilde{\mathbf{c}}_t &= \tanh(\mathbf{W}_c[\mathbf{h}_{t-1}, \mathbf{x}, p(\mathbf{h}_{t-1}, \mathbf{M})] + \mathbf{b}_c), \\ \mathbf{c}_t &= \mathbf{f}_t \circ \mathbf{c}_{t-1} + \mathbf{i}_t \circ \tilde{\mathbf{c}}_t. \end{aligned}$$

where $\circ$ is the concatenation operator for multidimensional vectors, and $\tilde{\mathbf{c}}_t$ is the updated state of memory cell. Consequently, the output gate $\mathbf{o}_t$ and the cell's hidden state $\mathbf{h}_t$ (2) become:

$$\begin{aligned} \mathbf{o}_t &= \sigma(\mathbf{W}_o[\mathbf{h}_{t-1}, \mathbf{x}, p(\mathbf{h}_{t-1}, \mathbf{M})] + \mathbf{b}_o), \\ \mathbf{h}_t &= \mathbf{o}_t \circ \tanh(\mathbf{c}_t). \end{aligned}$$

Correction of extracted patterns (columns of matrix $\mathbf{M}$) is done after decision-making (Fig. 2). Note that A-RNN for proposed solution consists of several augmented LSTM networks pretrained for different usage contexts.

4.2 Modalities for user authentication

Ensuring low error rate for ACS requires combining several modalities, such as PIN input, pick-up [28], gripping [29], and touchscreen utilization [30]. However, modern authentication solutions are based on taking these modalities in predefined usage contexts, only for example during typing, that requires usage of ensemble models for data processing. The A-RNN provides ability to tracking of several behavioral patterns at the same time. Thus, we propose to combine the following modalities during user authentication with BehaviorID method to provide flexible trade-off between authentication accuracy and usability:

1 *Type pattern* based on touchscreen keyboard timing and touches locations:

   1. Keyboard hit-map
   2. Distance between touches and buttons centers

2 *Swipe pattern* on touchscreen

3 *Device small motions* estimated with motion sensor:

   1. Tilt of device
   2. Small motions during text typing or swiping on touchscreen

4 *Behavioral profiling* based on app usage patterns

5 *Eyes tracking* during app usage estimated by using device's front-facing camera

6 *Mobile grip pattern* detected by utilizing touchscreen and gyroscope

Effective countermeasures against spoofing attack during user authentication requires using additional factors [3]. BehaviorID allows "strengthening" of widespread authentication methods by the usage of several modalities, for example:

1 *Password-based authentication*—user's behavior parameters are analyzed during typing, namely keystroke dynamics, device small motion, and keyboard hit map. If user behavior differs from saved profile, the device will remain locked regardless of the correctness of the entered password.

2 *Secure keyboard*—the proposed method can be used for touchscreen keyboard strengthening while working in messengers, social networks, etc. In case of failure of the BehaviorID authentication, a message will not be sent and the system will ask for additional authentication.

3 *Strengthening of biometric-based authentication*—BehaviorID can be used for increasing the robustness of biometric-based authentication to spoofing. This is achieved by analyzing the device's small motions during authentication. Thus, a device remains locked even for spoofed biometric authentication, for example, facial recognition, if motion patterns differ from a known one or even absent.

4 *Users transparent authentication*—the method checks of user authenticity at the background (without making of authentication request) after launching of predefined applications, for example, banking app. If the difference between gathered behavioral data, such as swipe patterns, touchscreen hit map, user's sight tracking, and a reference profile, is above a threshold, the device is locked in short time.

Rich functionality of the proposed BehaviorID method makes it an attractive solution for transparent multifactor on-device user authentication. However, performance evaluation of BehaviorID in real cases requires additional investigation. Therefore, of special interest is the performance evaluation of modern and proposed methods.

5 Experiments

Performance evaluation of the state-of-the-art and proposed BehaviorID solutions was performed for both single modal and multimodal user authentication. The following use cases were considered:

1 Estimation of SAR is performed to check the conformity of BehaviorID performance with requirements of ATAM [3] for processing sensitive data on mobile and wearable devices.

2 Keystroke dynamics-based authentication in various context corresponds to the case of "strengthening" of user authentication by single modality (e.g., password-based authentication) in several usage contexts.

3 Multimodal authentication by changing usage context allows evaluating the solution robustness to changes of person's behavioral templates, for example, start walking after still standing.

4 Long-term tracking of behavioral pattern alterations corresponds to the case of changing of user's behavior over long-term usage of ACS system.

Performance analysis of the BehaviorID method was done using PC- and Android-based prototypes. The PC-based prototype includes the implementation of A-RNN module with the TensorFlow package and its tuning of predefined datasets. Then, pretrained model was transferred to Samsung Galaxy S21 smartphone with TensorFlow Lite converter. The smartphone operated under Android 11 OS.

Usage context recognition for Android demo was performed with usage of human activity recognition (HAR) module. The module allows detecting the following physical activities—users are laying down, sitting, still standing, and walking. The HAR module uses CNN proposed by Gholamrezaii et al. [31] for feature extraction from signals gathered by motion sensor, namely accelerometer and gyroscope. The network was trained on standard UCI HAR dataset [32] and fine tuned on modern HARTH [33] and KU-HAR [34] datasets.

BehaviorID performance evaluation was done using a set of public and in-house datasets of behavioral patterns for mentioned modalities (Section 4.2) in various usage contexts. The following datasets were used:

- *The ExtraSensory dataset* [35] includes measurements of several sensors for 60 persons on smartphones and tablets made "in the wild." The data was captured by motion sensor, geolocation, and magnetometer for 15 smartphone models (Android and iOS).
- *The MotionSense dataset* [36] includes time series generated by motion sensor of iPhone 6s smartphone. The device was kept in the participant's front pocket. The dataset includes the estimation for 24 participants performing 6 physical activities (15 trials-per-activity in average).
- *The SherLock dataset* [37] is a huge dataset of long-term tracking of smartphone sensors with a high temporal resolution. The dataset offers explicit labels that capture the activity of applications running on the device. It contains about 10 billion data records from 30 users collected over a period of 2 years and an additional 20 users for 10 months (totally 50 users).
- *The H-MOG dataset* [38] includes the results of large-scale user study to collect a wide range of behavioral patterns related to touch dynamics, gesture, and movement and orientation of the phone. The data of 100 volunteers was collected during sitting and walking.
- *The UMDAA-02 dataset* [39] consists of 141.14 GB of smartphone sensor signals collected from 48 volunteers on Nexus 5 devices over 2 months. The data was gathered by frontal-facing camera, touchscreen, motion sensor, magnetometer, light sensor, GPS, Bluetooth, WiFi, proximity sensor, temperature sensor, and pressure sensor. The data collection application also stored the timing of the screen lock and unlock events, start and end timestamps of calls, foreground application, etc.
- *The BB-MAS dataset* [40] is collected by the international research teams for the analysis of the behavioral biometrics, obtained from multiple devices. Data from 117 subjects was collected for typing fixed and free text, walking, and touchscreen utilization on desktops, tablets, and smartphones.
- *Fixed-context dataset* was collected by our team during analysis of behavior-based authentication systems. The signals were gathered for 30 users (at least 5 authentication probes per user) during still standing. The users were requested to enter a 10-character passwords by left, right, or both hands.

Usage of several datasets during performance analysis is caused by the absence of a single "universal" dataset for the evaluation of behavior-based authentication systems for both short- and long-term changes of users behavioral patterns. Thus, we divided the considered datasets into two groups, namely with short-time (ExtraSensory, MotionSense, and in-house databases) and long-term (SherLock, H-MOG, and UMDAA-02 datasets) estimations.

For comparison, we considered the following state-of-the-art solutions for behavior-based user authentication on smartphones:

- Abuhamad et al. method [9]—based on the utilization of deep RNN, namely LSTM, for modeling temporary dependencies between samples of behavioral templates
- Reichinger et al. [41]—based on unsupervised learning approach for gathered behavioral features with usage of hidden Markov model
- MMAuth method [42]—integrates the heterogeneous information of user identity from multiple modalities with usage of developed time-extended behavioral feature set and a deep learning based one-class classifier

The performance analysis of modern and proposed methods was done in several stages. At the first step, we evaluate the conformity of the proposed BehaviorID to the requirements of ATAM [3], namely FAR, FRR, and SAR values. The SAR was estimated as the probability of false acceptance of non-target user [3]. Analysis was performed with standard ExtraSensory, MotionSense, and in-house datasets. Both single and multifactor authentication cases were considered with the usage of motion sensor (accelerometer and gyroscope) as well as inter-touch duration (ITD). The estimated values of FAR, FRR, and SAR are presented in Table 2.

Note that the Abuhamad et al. method allows negligibly decreasing the error level for the single modal case, while preserving similar or even higher error values for

Table 2 Estimated FAR, FRR, and SAR for single and multifactor authentication cases for fixed usage context (users are still sitting) using state-of-the-art and proposed methods. The "Acc" and "Gyr" stand for accelerometer and gyroscope

		In-house dataset				**Motion-Sense dataset**	**ExtraSensory dataset**	
		Acc	**Gyr**	**Acc, Gyr**	**Acc, Gyr, and ITD**	**Acc, Gyr**	**Acc, Gyr**	**Acc, Gyr, and ITD**
Abuhamad et al.	FAR	18.3%	34.1%	15.6%	4.0%	4.7%	3.2%	3.1%
	FRR	14.1%	24.6%	13.8%	8.1%	9.5%	6.6%	4.2%
	SAR	20.6%	45.8%	15.4%	5.1%	6.0%	3.2%	3.0%
Reichinger et al.	FAR	17.5%	36.8%	15.6%	13.1%	4.9%	3.4%	2.9%
	FRR	12.4%	26.7%	12.3%	8.2%	9.1%	5.3%	4.0%
	SAR	18.3%	41.5%	16.8%	5.7%	6.8%	3.1%	2.8%
MMAuth	FAR	19.4%	38.1%	15.0%	7.5%	5.0%	4.1%	3.0%
	FRR	13.7%	25.1%	14.3%	7.6%	8.6%	5.5%	4.1%
	SAR	17.1%	37.9%	16.1%	7.8%	5.3%	4.2%	2.9%
BehaviorID	FAR	16.0%	37.2%	13.1%	12.5%	3.5%	3.5%	2.5%
	FRR	11.2%	24.8%	10.4%	6.9%	7.7%	4.4%	3.8%
	SAR	15.6%	37.2%	12.5%	3.5%	4.8%	2.9%	2.5%

multimodal case in comparison with modern Reichinger et al. and MMAuth methods (Table 2). This can be explained by better accuracy of modeling cross-samples dependencies for gathered signals by usage of deep LSTM model in comparison with the hidden Markov model for advanced methods.

Moving from single factor to multifactor authentication allows for decreasing SAR values from 37.2 to 2.9% by preserving low FAR (about 2.5%) and FRR (near 8%) values for the proposed method (Table 2). The obtained results are close to state of the art in the domain of behavior-based authentication [1, 20, 43]. Note that the obtained SAR values for multifactor authentication ($SAR < 7\%$) corresponds to class 3 (strong) tier of ATAM [3]. This makes the proposed solution an attractive candidate for use in security-sensitive scenarios.

On the second stage of performance analysis, evaluation of error level in both fixed and various usage contexts was done. The obtained metrics values are represented in Tables 3 and 4.

Note that there is a relatively high level of SAR and FRR values in case of usage of a single sensor (Table 3)—up to 22.1% SAR and 13.4% FRR for all sensors. The usage of output signals for accelerometer and gyroscope allows reducing up to two times SAR by preserving the similar FRR values (Table 3). Merging of signals for all considered sensors leads to considerable decrease of error rates—up to 0.35% for SAR and 6.9% for FRR.

The password-based authentication "in-the-wild" by varying usage contexts and the password's length was considered on BB-MAS dataset (Table 4). The noticeable decreasing of SAR and FRR values was obtained—up to 9% reducing of SAR and up to two times in comparison with the fixed-context dataset. This can be explained by huge size of BB-MAS dataset [40] in comparison with in-house dataset—3.5 million keystroke events, 57.1 million data points for motion sensor, and 1.7 million data points for swipes. The usage of much bigger amount of samples for BB-MAS dataset allows considerably improving the detection accuracy of both HAR module and A-RNN networks.

The next stage of performance analysis is aimed at the evaluation of considered solutions for the case of multimodal authentication in several usage contexts. The H-MOG and UMDAA-02 datasets were used for the estimation of FAR and FRR in this case. The keystroke dynamics, device fine motions, swipe patterns, applications profiling, and gaze tracking were used as authentication factors. The estimated values of FAR and FRR metrics for the state-of-the-art and proposed solutions for case of changing usage context (from still sitting to walking) are presented in Table 5.

State-of-the-art solutions and the proposed BehaviorID methods achieve similar values of FAR and FRR by multifactor authentication during usage contexts changes (UMDAA-02 dataset, Table 5). However, BehaviorID allows for achieving smaller error rates (up to three times in comparison with Abuhamad's solutions) on H-MOG dataset. In both cases, values of FAR and FRR are close to the state-of-the-art results [1, 43] that prove the effectiveness of the proposed solution in this case.

Table 3 Estimated values of FAR, FRR, and SAR for password-based password's length (fixed-context in-house dataset) with modern and proposed methods

Modalities	**Single sensor**			**Two sensors**	**Multisensors**
Sensors	**Accelerometer**	**Gyroscope**	**Touchscreen**	**Accelerometer and gyroscope**	**Motion sensor and touchscreen**
Abuhamad et al. method					
FAR	17.2%	32.8%	20.3%	15.8%	4.6%
FRR	12.4%	25.5%	15.1%	10.8%	7.6%
SAR	13.8%	38.2%	13.6%	13.2%	2.6%
Reichinger et al. method					
FAR	18.1%	37.1%	19.8%	13.9%	12.4%
FRR	13.8%	27.9%	15.6%	12.1%	8.4%
SAR	16.8%	39.1%	14.2%	13.9%	3.4%
MMAuth method					
FAR	19.1%	34.0%	17.6%	14.8%	7.7%
FRR	13.0%	26.3%	15.3%	11.4%	7.2%
SAR	16.4%	39.5%	14.9%	12.8%	1.5%
BehaviorID method					
FAR	14.5%	32.1%	17.2%	12.7%	11.9%
FRR	11.2%	24.8%	14.2%	10.4%	6.9%
SAR	15.9%	37.2%	13.1%	12.5%	0.4%

Table 4 Estimated values of FAR, FRR, and SAR during user authentication during free-text typing in various contexts (BB-MAS dataset) with modern and proposed methods

Modalities	**Single sensor**			**Two sensors**	**Multisensors**
Sensors	**Accelerometer**	**Gyroscope**	**Touchscreen**	**Accelerometer and gyroscope**	**Motion sensor and touchscreen**
Abuhamad et al. method					
FAR	14.2%	24.1%	10.8%	7.7%	3.4%
FRR	9.8%	18.1%	8.4%	6.0%	3.2%
SAR	11.9%	27.1%	9.1%	9.5%	2.6%
Reichinger et al. method					
FAR	12.4%	23.2%	11.1%	8.2%	3.0%
FRR	9.4%	17.5%	8.2%	7.6%	2.8%
SAR	12.8%	26.0%	9.9%	9.1%	3.3%
MMAuth method					
FAR	13.8%	24.5%	11.7%	8.0%	2.2%
FRR	10.1%	18.9%	8.7%	7.9%	3.0%
SAR	12.0%	27.5%	9.2%	9.4%	3.1%
BehaviorID method					
FAR	10.6%	22.8%	8.9%	5.4%	1.7%
FRR	7.2%	15.3%	6.8%	5.8%	2.1%
SAR	13.4%	25.7%	9.4%	9.6%	0.7%

At the last stage, the most difficult case of long-term tracking of behavioral template was considered. The performance analysis was done on SherLock dataset using three modalities, namely keystroke dynamics, application usage logs, and device's fine motions. The estimated values of FAR and FRR metrics for modern and proposed

Table 5 Estimated values of FAR and FRR during multifactor authentication in various usage contexts

Metric	Abuhamad et al. method	Reichniger et al. method	MMAuth method	BehaviorID method
H-MOG dataset				
FAR	1.8%	0.9%	1.3%	0.3%
FRR	3.0%	1.5%	1.9%	1.3%
UMDAA-02 dataset				
FAR	7.4%	6.8%	7.9%	7.0%
FRR	5.4%	4.1%	5.0%	3.5%

Table 6 Estimated values of FAR and FRR during multifactor authentication for the case of long-term usage of a smartphone (SherLock dataset)

Metric	Abuhamad et al. method	Reichniger et al. method	MMAuth method	BehaviorID method
FAR	9.4%	2.8%	6.6%	2.1%
FRR	12.7%	4.2%	11.9%	3.9%

solutions for the 3-week usage period are presented in Table 6.

The state-of-the-art Abuhamad et al. solution has shown a decreasing authentication accuracy up to 13% for the considered case, while the proposed method preserves low performance degradation (only about 4%, Table 6). Thus, BehaviorID provides the same or even better performance for short-term tracking of behavioral templates and performs much better in long-term usage scenarios.

6 Conclusion

Many solutions for biometric- and behavior-based authentication and liveness detection on mobile devices are presented on the market. Despite the widespread integration, they tend to be vulnerable to presentation attack (spoofing of biometric data). In addition, majority of the modern solution are typically designed to operate in fixed usage context, such as still positions, that negatively impacts the user experience.

Major contribution of this paper is the proposed context-dependent behavior-based BehaviorID method that allows for accurate on-the-fly user authentication in various usage contexts. The BehaviorID is based on applying advanced A-RNN model for simultaneously tracking several behavioral templates in signals gathered from built-in sensors. This makes possible fast adaptation of behavioral templates to alterations caused by alterations of user habits as well as changes in person's physical state, for example, injuries. Also, the A-RNN allows tracking of behavioral features by preserving low computation overhead that makes it attractive for usage on resource-constrained mobile devices.

Performance analysis of the proposed methods showed that BehaviorID allows outperforming the state-of-the-art multifactor behavior-based authentication methods even in the most difficult case of long-term tracking of behavioral patterns (about 2.1% FAR and 3.9% FRR). Also, the proposed method provides low error rate in various usage context (about 0.5% FAR and 1.3% FRR) by preserving fast detection of non-owner user (within $0.5 - 1.0$ s for Samsung Galaxy S21 smartphone). This makes the proposed BehaviorID method a promising candidate for the next-generation user authentication systems on mobile and wearable devices.

Our future work will be devoted to investigating the accuracy of behavioral template tracking for long-term evaluation in real environment. Moreover, we will focus on the adaptation of the proposed method for wearable devices, such as smartwatches, by reducing the computational overhead of behavioral template tracking procedure.

Abbreviations

ACS: Access control system; ATAM: Android tiered authentication model; A-RNN: Adaptive recurrent neural network; CNN: Convolutional neural network; DTW: Dynamic time warping; FAR: False acceptance rate; FRR: False rejection rate; GRU: Gated recurrent unit; HAR: Human activity recognition; ITD: Inter-touch duration; LSTM: Long short-term memory; RNN: Recurrent neural networks; SAR: Spoof acceptance rate.

Acknowledgements

Not applicable.

Authors' contributions

DP performed the initial set of experiments with the proposed neural network architecture that showed its applicability. VC and PK prepared the demo for on-device usage and performed the experiments for checking the applicability of the proposed solution. AO drafted the first version of the manuscript. DP updated the manuscript to the final version. All authors read and approved the final manuscript.

Funding

Research was conducted on funds of Samsung R &D Institute Ukraine, Kyiv.

Availability of data and materials

Model evaluation was performed on open datasets, namely UCI HAR [32], ExtraSensory [35], MotionSense [36], SherLock [37], H-MOG [38], UMDAA-02 [39], and BB-MAS [40]. The considered state-of-the-art Abuhamad et al. [9], Reichinger et al.[41], and MMAuth [42] methods are available from the corresponding author on reasonable request. We compared the obtained results with the requirements of ATAM [3].

Declarations

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Security Team, Samsung R &D Institute Ukraine, 57, Lva Tolstogo Street, 01032 Kyiv, Ukraine. [2]Institute of Physics and Technology, Igor Sikorsky Kyiv

Polytechnic Institute, 37, Prospect Peremohy, 03056 Kyiv, Ukraine. [3]Faculty of Mechanics and Mathematics, Taras Shevchenko National University of Kyiv, 64/13, Volodymyrska Street, 01601 Kyiv, Ukraine.

Received: 15 September 2021 Accepted: 17 August 2022
Published online: 16 September 2022

References

1. M. Papadopouli, A. Arnes, J.A. Bombin, E. Boschi, S. Buchegger, R.B. Cortiñas, et al., Mobile identity management. IDM report. Eur. Netw. Inf. Secur. Agency. (2010). https://www.enisa.europa.eu/publications/Mobile20IDM. Accessed 24 June 2020
2. M.A. Ferrag, L. Maglaras, A. Derhab, H. Janicke, Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues. Telecommun. Syst. **73**, 317–348 (2020)
3. Google. Lockscreen and authentication improvements in Android 11. (2020). https://android-developers.googleblog.com/2020/09/lockscreen-and-authentication.html. Accessed 23 May 2022
4. C. Wu, K. He, J. Chen, Z. Zhao, R. Du, Liveness is not enough: enhancing fingerprint authentication with behavioral biometrics to defeat puppet attacks. in 29th USENIX Security Symposium (USENIX Security 20) (2020), p. 2219–2236. https://www.usenix.org/conference/usenixsecurity20/presentation/wu. Accessed 12 July 2021
5. C. Burt, U.S. DISA develops prototype multi-biometric smartphone for "assured identity". (2019). https://www.biometricupdate.com/201908/u-s-disa-develops-prototype-multi-biometric-smartphone-for-assured-identity. Accessed 23 May 2022
6. M. Ehatisham-ul Haq, M.A. Azam, J. Loo, K. Shuang, S. Islam, U. Naeem, et al., Authentication of smartphone users based on activity recognition and mobile sensing. Sensors. 17(9), (2017). https://www.mdpi.com/1424-8220/17/9/2043. Accessed 12 July 2021
7. A. Alzubaidi, J. Kalita, Authentication of smartphone users using behavioral biometrics. IEEE Commun. Surv. Tutor. **18**(3), 1998–2026 (2016)
8. O. Riva, C. Qin, K. Strauss, D. Lymberopoulos, Progressive authentication: deciding when to authenticate on mobile phones. in 21st USENIX Security Symposium (USENIX Security 12) (Bellevue, 2012), p. 301–316. https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/riva. Accessed 12 July 2021
9. M. Abuhamad, T. Abuhmed, D. Mohaisen, D. Nyang, AUToSen: deep-learning-based implicit continuous authentication using smartphone sensors. IEEE Internet Things J. **7**(6), 5008–5020 (2020)
10. A. Cser, M. Merritt, The future of identity and access management. FORRESTER Inc. (2019). https://www.forrester.com/report/The+Future+Of+Identity+And+Access+Management/-/E-RES136522. Accessed 24 Jun 2020
11. RSA SecurID Suite. https://www.rsa.com/en-us/products/rsa-securid-suite. Accessed 24 Jun 2020
12. NuData Security. https://nudatasecurity.com/. Accessed 24 Jun 2020
13. Apple Inc . Touch ID and Face ID technologies description. https://support.apple.com/en-us/HT208108. Accessed 24 Jun 2020
14. SecureAuth Identity Platform. https://www.secureauth.com/products/identity-platform. Accessed 24 Jun 2020
15. Amazon GuardDuty: protect your AWS accounts with intelligent threat detection. https://aws.amazon.com/guardduty/?nc1=h_ls. Accessed 23 May 2022
16. TwoSense.AI: continuous multifactor authentication. https://www.twosense.ai/. Accessed 23 May 2022
17. Biometric signature ID. https://biosig-id.com/. Accessed 23 May 2022
18. OneSpan: do more business with better security & simplified customer experiences. https://www.onespan.com/. Accessed 23 May 2022
19. Zighra: insights and resources. https://zighra.com/. Accessed 23 May 2022
20. Context-aware identity management framework. Alliance Telecommun. Ind. Solutions. (2018). https://access.atis.org/apps/group_public/download.php/43565/ATIS-I-0000070.pdf. Accessed 24 Jun 2020
21. Ping identity announces the acquisition of SecuredTouch to accelerate identity fraud capabilities. https://www.pingidentity.com/en/company/ping-newsroom/press-releases/2021/securedtouch.html. Accessed 23 May 2022
22. E. Koster, Why Samsung NEXT and HYPR believe the future will be passwordless. https://news.samsung.com/us/samsung-next-hypr-believe-future-will-passwordless/. Accessed 23 May 2022
23. H.G. Kayacik, et al. Data Driven Authentication: On the Effectiveness of User Behaviour Modelling with Mobile Device Sensors. Cornell University preprint repository. arXiv:1410.7743 (2014)
24. M.A. Alqarni, S.H. Chauhdary, M.N. Malik, et al., Identifying smartphone users based on how they interact with their phones. Hum. Cent. Comput. Inf. Sci. **10**(7), (2020). https://doi.org/10.1186/s13673-020-0212-7
25. S. Salvador, P. Chan, Toward accurate dynamic time warping in linear time and space. Intell. Data Anal. **11**(5), 561–580 (2007)
26. K. Zhao, Y. Li, C. Zhang, C. Yang, H. Xu, Adaptive recurrent neural network based on mixture layer. (2018). arXiv e-prints. http://arxiv.org/abs/1801.08094
27. I. Goodfellow, Y. Bengio, A. Courville, *Deep learning* (The MIT Press, Cambridge, 2016)
28. W.H. Lee, X. Liu, Y. Shen, H. Jin, R.B. Lee, Secure pick up: implicit authentication when you start using the smartphone. (2017). arXiv e-prints. http://arxiv.org/abs/1708.09366
29. K. Murao, H. Tobise, T. Terada, T. Iso, M. Tsukamoto, T. Horikoshi, Mobile phone user authentication with grip gestures using pressure sensors. Int. J. Pervasive Comput. Commun. **11**(3), 288–301 (2015)
30. S.J. Alghamdi, L.A. Elrefaei, Dynamic authentication of smartphone users based on touchscreen gestures. Arab. J. Sci. Eng. **43**, 789–810 (2018)
31. M. Gholamrezaii, S.M. Taghi Almodarresi, "Human Activity Recognition Using 2D Convolutional Neural Networks," 2019 27th Iranian Conference on Electrical Engineering (ICEE), pp. 1682–1686, (2019) https://doi.org/10.1109/IranianCEE.2019.8786578
32. D. Garcia-Gonzalez, D. Rivero, E. Fernandez-Blanco, M.R. Luaces, A public domain dataset for human activity recognition using smartphones. Sensors. 20(8), (2020)
33. A. Logacjov, K. Bach, A. Kongsvold, H.B. Bårdstu, P.J. Mork. HARTH: a human activity recognition dataset for machine learning. Sensors (Basel). 21(23), (2021)
34. N. Sikder, A.A. Nahid, KU-HAR: an open dataset for heterogeneous human activity recognition. Pattern Recognit. Lett. **146**, 46–54 (2021)
35. Y. Vaizman, K. Ellis, G. Lanckriet, Recognizing detailed human context in the wild from smartphones and smartwatches. IEEE Pervasive Comput. **16**(4), 62–74 (2017)
36. M. Malekzadeh, R.G. Clegg, A. Cavallaro, H. Haddadi, Mobile sensor data anonymization, in *Proceedings of the International Conference on Internet of Things Design and Implementation. IoTDI '19*. (ACM, New York, 2019), pp.49–58
37. Y. Mirsky, A. Shabtai, L. Rokach, B. Shapira, Y. Elovici, "Sherlock vs moriarty: A smartphone dataset for cybersecurity research", Proc. ACM Workshop Artif. Intell. Secur. pp. 1–12, (2016). https://doi.org/10.1145/2996758.2996764
38. Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti et al., HMOG: new behavioral biometric features for continuous authentication of smartphone users. IEEE Trans. Inf. Forensic. Secur. **11**(5), 877–892 (2016)
39. U. Mahbub, S. Sarkar, V.M. Patel, R. Chellappa, "Active user authentication for smartphones: A challenge data set and benchmark results," 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), (2016), pp. 1–8, https://doi.org/10.1109/BTAS.2016.7791155
40. A.K. Belman, L. Wang, S.S. Iyengar, P. Sniatala, R. Wright, R. Dora, et al., Insights from BB-MAS – a large dataset for typing, gait and swipes of the same person on desktop, tablet and phone. (2019), arXiv e-prints. http://arxiv.org/abs/1912.02736
41. D. Reichinger, E. Sonnleitner, M. Kurz, Continuous mobile user authentication using combined biometric traits. Appl. Sci. 11(24), (2021)
42. Z. Shen, S. Li, X. Zhao, J. Zou, MMAuth: a continuous authentication framework on smartphones using multiple modalities. IEEE Trans. Inf. Forensic. Secur. **17**, 1450–1465 (2022)
43. G. Rowe, N. Nikols, D. Simmons, The future of identity management (2018-2023). TechVision Res. (2018). https://techvisionresearch.com/wp-content/uploads/2018/01/The-Future-of-Identity-Management-2018-final.pdf. Accessed 24 Jun 2020

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.