AI-Driven Optimisation for Mobile Behavioural Biometrics Continuous Authentication

Mustafa AL SAMARA[a], Ismail BENNIS[a], Marc GILG[a],
Bouziane BRIK[b], Abdelhafid ABOUAISSA[a]
[a]IRIMAS, University of Haute-Alsace, France
[b]Computer Science department, University of Sharjah, UAE
{mustafa.al-samara, marc.gilg, abdelhafid.abouaissa, ismail.bennis}@uha.fr, bbrik@sharjah.ac.ae

***Abstract*—Mobile behavioural biometrics, leveraging touchscreen and background sensor data, have emerged as a promising solution for Continuous Authentication (CA) on mobile devices, enabling secure user authentication. In this paper, we introduce an enhanced CA framework named AI-MBBCA, that integrates a Genetic Algorithm (GA) for optimal training hyper-parameter selection and an Isolation Forest (IF) as a secondary layer for impostor attack detection. A hybrid Long Short-Term Memory (LSTM) network, trained using a triplet loss function and augmented with a regularisation method, effectively captures spatial and temporal patterns in user behaviour. Experimental evaluations on the BehavePassDB dataset demonstrate that AI-MBBCA significantly improves authentication accuracy and reduces error rates across multiple tasks, with notable improvements in the Area Under the Curve (AUC) compared to two other approaches from the literature. Integrating AI-Driven optimisation, including GA and IF-based anomaly detection, paves the way for more resilient and adaptive Behavioural Biometrics Continuous Authentication (BBCA) systems, addressing the challenges posed by sophisticated forgery scenarios in dynamic mobile environments.**

***Index Terms*—Behavioural Biometrics Continuous Authentication (BBCA), Genetic Algorithm (GA), Isolation Forest (IF), Long Short-Term Memory (LSTM).**

I. Introduction

Mobile biometric authentication has traditionally relied on physiological traits, such as fingerprints or facial recognition [1], which, despite their widespread use, are vulnerable to spoofing attacks and digital tampering [2]. Moreover, these one-time authentication methods are inappropriate for Continuous Authentication (CA), a security paradigm that continuously verifies a user's identity throughout an active session without interrupting normal activities. CA systems use unobtrusive, real-time monitoring of behavioural traits, captured via background sensor data (e.g., Accelerometer, Gyroscope, Linear Accelerometer, Gravity and Magnetometer), to verify the authenticated user's continued legitimacy.

In contrast to physiological modalities, behavioural biometrics facilitate a seamless CA experience by continuously processing data that reflects natural user interactions, such as app usage patterns and movement dynamics [3], [4]. However, challenges remain in distinguishing genuine user behaviour from impostor activity, particularly in scenarios where attackers mimic the legitimate user's patterns on the same device.

Behavioural Biometrics for Continuous Authentication (BBCA) has emerged as a promising field, serving both as a robust primary security method and as a complementary second-factor Authentication (2FA) mechanism [5], [6]. Data acquisition strategies in BBCA range from leveraging users' mobile devices, which allows for large-scale, flexible data collection yet may introduce device-specific biases, to employing dedicated acquisition hardware that, while reducing bias, may not fully capture real-world variability [7].

This paper presents an Artificial Intelligence framework for Mobile Behavioural Biometrics Continuous Authentication called AI-MBBCA, which incorporates two significant advancements. First, a Genetic Algorithm (GA) optimises the hyper-parameters of the Long Short-Term Memory (LSTM) network, which is trained with triplet loss and a regularisation method to better capture spatiotemporal user behaviour. Second, an Isolation Forest (IF) acts as a supplementary defense layer, detecting impersonation attacks by identifying impostors in feature embeddings.

Experimental evaluations on benchmark behavioural biometric BehavePassDB dataset [8] for CA demonstrate that AI-MBBCA achieves significant improvements in authentication accuracy and robustness, as compared to two other existing approaches from the literature. The main contributions of this paper can be summarised as follows:

- We propose AI-MBBCA, an advanced CA framework that integrates GA-driven optimisation for training hyper-parameters selection and an IF-based impostor detection layer.
- We implement a hybrid LSTM model trained with a triplet loss function and enhanced with a regularisation method to capture complex spatiotemporal features from the touchscreen and several background sensors' behavioural data.
- We demonstrate, through extensive experiments on

979-8-3503-9281-4/25/$31.00 ©2025 IEEE

the BehavePassDB [8] dataset, that our enhanced approach significantly outperforms existing methods in both random and skilled impostor attack scenarios.

The rest of the paper is organised as follows: Section II reviews related work in BBCA systems. Section III details the architecture of the proposed AI-MBBCA framework. Experimental setups and results are presented in Section IV, and Section V concludes the paper.

II. Related Works

Behavioural biometrics have long been explored for CA on mobile devices, with the rapid advancement of deep learning techniques driving significant innovation in this area. Early studies, such as [9], introduced multimodal systems that integrated data from up to eight different sensors, which included a touchscreen, keystroke dynamics, and various motion sensors, to verify user identity passively. Their Siamese RNN LSTM architecture with contrastive loss achieved a high true acceptance rate of 96.47% at a false acceptance rate of 0.1% over 3-second intervals. However, limitations such as a low sampling rate (1Hz), and the dataset consists of only 37 subjects, which may affect the generalisability of the results to more diverse and real-world conditions.

In [10], researchers focused on background sensor data like Accelerometers, Gyroscopes, and Magnetometers within a deep learning-based behavioural biometric system. They employed RNN LSTM architectures trained with triplet loss and achieved an impressive Equal Error Rate (EER) of 0.41% over 1-second intervals using data from 84 participants. However, a key limitation of their approach is the continuous, unrestricted collection of sensor data. This lack of constraints increases the risk that the system may learn device-specific artifacts and noise instead of capturing the truly unique behavioural characteristics of the genuine user, potentially compromising the system's generalizability and reliability in real-world scenarios.

Touchscreen-based approaches have also been explored. For example, [11] analyzed swiping gestures using the HuMIdb public database and a Siamese RNN, yielding an EER of 19%. As evaluated on the Aalto database, additional experiments on keystroke dynamics from free-text inputs demonstrated a 9.2% EER for touchscreen typing. When RNNs with triplet loss were applied separately to different modalities and later fused at the score level, the resulting EERs ranged between 4% and 9% over 3-second intervals. These results underscore a key limitation: effectively combining diverse biometric cues remains challenging. Each modality introduces its noise and variability, and the fusion process can struggle to balance these differences potentially compromising the overall robustness and consistency of the authentication system.

In [6], the authors introduced BehavePassDB [8], a public database designed for benchmarking mobile BBCA. The dataset captures natural human-mobile interactions through eight tasks, using touchscreen and background sensor data (Accelerometer, Gravity, Gyroscope, and Magnetometer). They implemented an authentication system based on an RNN LSTM with a triplet loss function to learn user embeddings. The study evaluates the system's performance under two impostor scenarios: random impostor forgeries, where data from different devices are compared, and skilled impostor forgeries, where the same device is used by a different user attempting to mimic the genuine user's behaviour.

In [12], the authors propose a novel framework for privacy-preserving CA of mobile devices that leverages homomorphic encryption and machine learning. The method preprocesses raw behavioural data on the client side using LSTM-based neural networks to extract compact behaviour vectors. These are then encrypted with the Cheon-Kim-Kim-Song (CKKS) scheme and transmitted to a server for coherence analysis. Their approach significantly reduces network traffic and authentication latency, achieving reductions of approximately 32% and 68%, respectively, while maintaining competitive accuracy under diverse attack scenarios.

Various techniques for BBCA systems on mobile devices have been proposed in the literature. However, some of these approaches still exhibit limitations and potential drawbacks, necessitating careful consideration and addressing in future research. One of the primary limitations observed in current works, such as those discussed in the multimodal approach [9], is experiencing high accuracy under controlled conditions; constraints such as low sampling rates and limited subject diversity hinder the generalisability of their results. Similarly, methods leveraging RNN LSTM architectures with triplet loss for background sensor data have shown strong performance [10], [11] but often suffer from minimal data restrictions. This can lead to models capturing device-specific artifacts rather than the genuine behavioural traits of users. Touchscreen-based CA systems also display variable success across different modalities, highlighting the persistent challenge of effectively integrating heterogeneous behavioural cues [11].

The introduction of the BehavePassDB dataset [6], [8] represents a significant step forward, offering a comprehensive benchmark for evaluating BBCA systems across diverse conditions and attack scenarios. Nonetheless, the fusion of multiple modalities and consistent performance across real-world variability remains an open challenge. Moreover, while the privacy-preserving framework introduced in [12] effectively reduces network traffic and authentication latency, its reliance on client-side LSTM preprocessing may impose non-trivial computational and energy overheads on mobile devices with limited re-

sources. To further validate the effectiveness of our approach, we compare AI-MBBCA against these two advanced frameworks [6], [12], and demonstrate its superior performance across key performance evaluation metrics. To address these challenges, we propose AI-MBBCA. This enhanced BBCA framework combines a hybrid LSTM RNN architecture with an optimised regularisation technique, a GA technique for optimal parameter selection, and an IF method for improved impostor detection. Unlike previous systems constrained by low sampling rates and limited subject diversity, AI-MBBCA is evaluated on a diverse dataset, ensuring stronger generalisability. To mitigate the risk of learning device-specific artefacts, the hybrid architecture and regularisation enhance the extraction of robust behavioural patterns across users and sessions. The framework also handles the complexity of multimodal data fusion via score-level integration, optimised through GA-based tuning, which boosts adaptability across tasks. Finally, the integration of IF method strengthens the system's resilience against both random and skilled impostor attacks. Our experimental results demonstrate that AI-MBBCA outperforms existing methods, including those in [6], [12], paving the way for more robust and adaptive mobile authentication systems.

III. The AI-MBBCA: Architecture

Fig. 1 illustrates the layered and modular architecture of the AI-MBBCA framework, which is designed to provide robust CA using mobile behavioural biometrics. The process begins with acquiring raw data from two primary sources: behavioural biometrics and input from background sensors. This raw data is then subjected to preprocessing and normalization to remove noise and standardize the signals, ensuring high-quality inputs for subsequent analysis. The preprocessed data feeds into the central CA system, which acts as the orchestrator by integrating multiple subsystems. A hybrid LSTM network, trained with a triplet loss function and enhanced by a regularisation method, captures the complex spatiotemporal patterns in the user's behaviour. To optimize this model, a GA is employed; it iteratively refines hyper-parameters such as learning rate, batch size, dropout rate, and the number of LSTM units, thus enhancing the model's performance and generalisation method. Simultaneously, the system establishes a compact feature embedding space where genuine and impostor behavioural patterns are distinctly clustered. An IF method is then used as a secondary layer to detect anomalies in these embeddings by generating anomaly scores. These scores are fused with distance-based metrics using a weighted sum, leading to a final authentication decision. To ensure robust BBCA system, our framework consists of several interconnected components, we detail each component below. The green-highlighted components in Fig. 1 represent the novel contributions introduced in this paper.

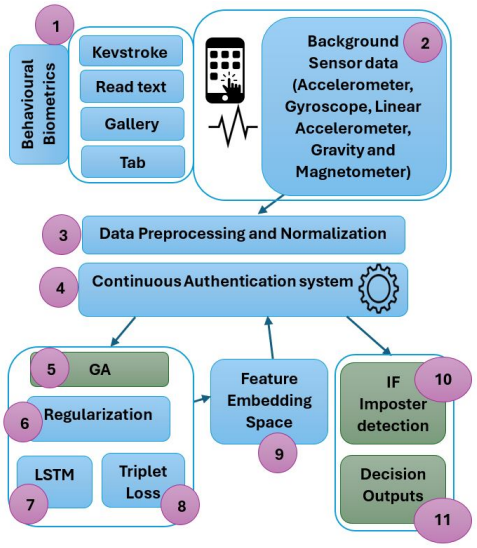

Fig. 1. AI-MBBCA approach.

1) **Behavioural biometrics:** These attributes capture user-specific interaction patterns:
   - **Keystroke:** Typing patterns (e.g., dwell times, flight times) that reveal unique rhythmic signatures.
   - **Readtext:** Scrolling or reading behaviours (e.g., speed, pauses, and revisit frequency).
   - **Gallery:** Navigation patterns through image galleries (e.g., swipe speed, dwell time on images).
   - **Tab:** Touch and swipe interactions, including gesture speed, direction, and pressure.
2) **Input Background Sensors:** capture device motion and orientation.
   - **Accelerometer** and **Linear Accelerometer** measure changes in velocity.
   - **Gyroscope** detects changes in rotation/orientation.
   - **Gravity** provides data on the gravitational force relative to the device.
   - **Magnetometer** measures the Earth's magnetic field for orientation adjustments.

   These raw signals form the foundational layer, continuously supplying behavioural data.
3) **Data Preprocessing and Normalisation:** Sensor data is preprocessed to remove noise and normalised for consistency, ensuring high-quality and reliable input for effective feature extraction.
4) **CA System:** Acts as the central orchestrator that manages data ingestion and feature extraction. It integrates multiple subsystems (e.g., LSTM, GA, IF) to analyze behavioural patterns and makes real-time authentication decisions.

5) **GA :** Utilised for hyperparameter optimisation in the training phase. Key details include:
   - **Population of Solutions:** Each individual encodes a unique set of hyper-parameters, such as margin(0,1 to 1.0), learning rate(0.001 to 0.05), batch size(128, 256, 512), dropout rate(0.4 to 0.8), the number of LSTM units (64, 128, 256), regularisation method (Ridge, Lasso, ElasticNet, Bayesian), and the triplet Strategy which defines how triplets (anchor, positive, negative) are selected (random, semi-hard, hard).
   - **Fitness Function:** The performance of each individual is evaluated based on model metrics. One common approach is described in Equation (1):

$$\textbf{Fitness} = \max(\text{AUC}) - \min(\text{Loss}) \quad (1)$$

     This function simultaneously rewards high AUC and penalises high loss, ensuring a balanced optimisation.
   - **Evolutionary Operators:**
     - **Selection:** Employing NSGA-II method, individuals with superior fitness are retained for the next generation.
     - **Crossover:** hyper-parameters from two-parent individuals are recombined (with a 50% swap probability per parameter) to create offspring.
     - **Mutation:** Random perturbations (e.g., adding Gaussian noise to numeric values) are introduced to maintain diversity and explore new solutions.
   - **Outcome:** The GA iteratively refines the hyper-parameters, culminating in an optimal configuration that enhances the LSTM model's performance and generalisation in CA.
6) **Regularisation:** Adding penalty terms to the loss function prevents overfitting in machine learning models. This technique enhances generalisation by discouraging overfitting and promoting simpler models.
7) **LSTM:** Processes sequential sensor data, capturing temporal dependencies in user behaviour. This allows the system to model dynamic interaction patterns over time effectively.
8) **Triplet Loss Function:** Ensures that the feature embeddings maintain a desirable structure:
   - Positive Pairs (same user) are forced to be close.
   - Negative Pairs (different users) are pushed apart by a predefined margin.
   - The margin parameter is optimised via GA, and different triplet mining strategies (random, semi-hard, hard) can be applied to select informative sample triplets.
9) **Feature Embedding Space:** The output from the LSTM model is a compact, discriminative feature space:
   - Genuine user embeddings cluster together.
   - Impostor embeddings are distanced to enable clear differentiation.
10) **IF Imposter Detection:** An unsupervised method for anomaly detection [13], particularly suitable for identifying deviations in user behaviour:
    - **Training:** IF is trained on the feature embeddings from enrollment and verification samples.
    - **Anomaly Scoring:** The anomaly score for a sample x is given by the Equation (2):

$$s(x, n) = 2^{-\frac{E(h(x))}{c(n)}} \quad (2)$$

      Here, $E(h(x))$ represents the average path length required to isolate x within a forest of decision trees, and $c(n)$ is a normalisation factor related to the number of samples n (typically, the average path length of unsuccessful searches in a binary search tree). A lower $s(x, n)$ indicates a higher likelihood of the sample being anomalous.
    - **Integration:** The IF anomaly scores are combined with distance-based metrics to provide a robust final decision. This dual approach enhances detection accuracy by leveraging global similarity and local anomaly information.
11) **Decision Outputs:** The CA system combines two key metrics to decide on authentication:
    - **Distance-based Metrics:** Such as the Euclidean distance between enrollment and verification embeddings.
    - **Anomaly Scores:** Derived from the IF, indicating the likelihood of an authentication attempt being anomalous.
      These are typically fused via a weighted sum as shown in Equation (3):

$$\textbf{Combined Score} = \alpha \times \text{Euclidean Distance} + (1 - \alpha) \times \text{IF Score} \quad (3)$$

      where α (e.g., 0.2) balances the contribution from both sources.

IV. Experiments results analysis

In this section, we present our simulation results conducted with Python. We use a client-server model, and all experiments are conducted using Tensorflow $V2.10.1$, Scikit-learn $V1.4.2$, and Numpy $V2.0.1$ on

a Debian 12 Server environment, which is Intel Core i7-10700 CPU, 32GB RAM. We conducted a series of experiments using the BehavePassDB dataset [8], which is a public database designed to facilitate research in mobile BBCA. It captures data from 81 users across four acquisition sessions, each separated by at least 24 hours to account for intra-subject variability. The dataset comprises three subsets: a training set (51 users), a validation set (10 users), and an evaluation set (20 users). Data was collected via a dedicated Android application on participants' smartphones, simulating natural Human-Computer Interaction (HCI). The sessions included eight tasks representing typical mobile interactions, such as pattern unlocking, texting, text reading, gallery swiping, and tapping. The dataset integrates multimodal data sources, including touchscreen interaction and background sensor data, sampled at 200 Hz.

The BehavePassDB [8] dataset supports two impostor scenarios: random impostor forgeries, where genuine and impostor data come from different devices, and skilled impostor forgeries, where impostors attempt to mimic genuine users on the same device. This design allows for rigorous evaluation of CA systems under both real-world and challenging scenarios. The training set in the BehavePassDB dataset contains data only from random impostor scenarios, while the validation and evaluation sets include both random and skilled impostor data. This hybrid approach ensures scalability and robustness while addressing device bias and user variability in behavioural biometric systems. The dataset has been used as a benchmark in the MobileB2C competition at IJCB 2022 [14].

Regarding the hyper-parameters used during training, we use the optimal set resulting from the GA as follows: margin(0,2, learning rate (0.001), batch size (512), dropout rate (0,55), the number of LSTM units (64), regularisation method (ElasticNet), and the triplet Strategy (random).

The first experiment evaluated the AI-MBBCA approach, employing GA-optimised hyper-parameters and using the AUC metric for the best fusion of different background sensors in the Keystroke task under random and skilled attacks. AUC, a robust measure of classification performance in biometric systems, quantifies the ability to distinguish genuine users from impostors, with higher values indicating better performance. We compared AI-MBBCA performance against the two approaches [12] and [6] from the literature. As Fig. 2 demonstrates, AI-MBBCA achieved an AUC of 93.50% for random impostors, 71.98% for skilled impostors, and 82.74% for mixed impostors (which is the average of both random and skilled impostors rates) significantly exceeding the other studied works.

The second experiment evaluated the AI-MBBCA approach, employing GA-optimised hyper-parameters, using the AUC metric for the best fusion of different

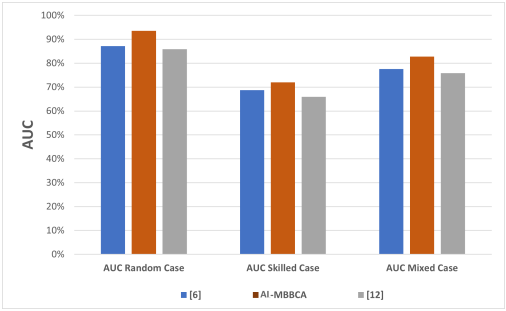

Fig. 2. AUC Performance for the best fusion of different background sensors in the Keystroke Task.

background sensors in the Readtext task under random and skilled attacks. We compared AI-MBBCA's AUC performance against the two approaches [12] and [6]. Fig. 3 shows that the AI-MBBCA significantly outperformed the studied works in both attack scenarios and also in the mixed case.

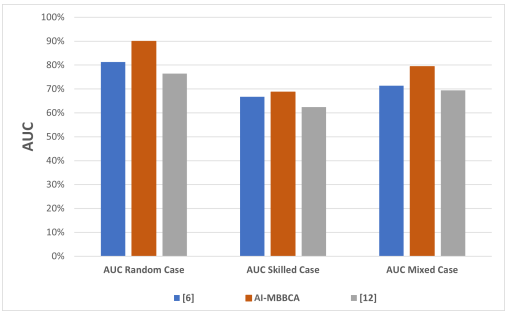

Fig. 3. AUC Performance for the best fusion of different background sensors in the Readtext Task.

In the third experiment, we assessed the AUC performance of our AI-MBBCA approach, employing GA-optimised hyper-parameters, using the AUC metric for the best fusion of different background sensors in the Gallery task under both random and skilled attacks. We compared AI-MBBCA's AUC performance against the two approaches [12] and [6]. Fig. 4 shows that the AI-MBBCA significantly outperformed the studied works in both attack scenarios and also in the mixed case.

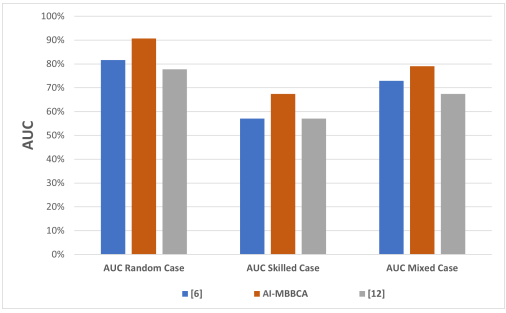

Fig. 4. AUC Performance for the best fusion of different background sensors in the Gallery Task.

In the fourth experiment, we evaluated the AUC performance of our AI-MBBCA approach, employing GA-optimised hyper-parameters, using the AUC metric for the best fusion of different background sensors in the Tap task under random and skilled attacks. The results, shown in Fig. 5, reveal that the AI-MBBCA significantly outperformed the studied works [6], [12] in all cases.

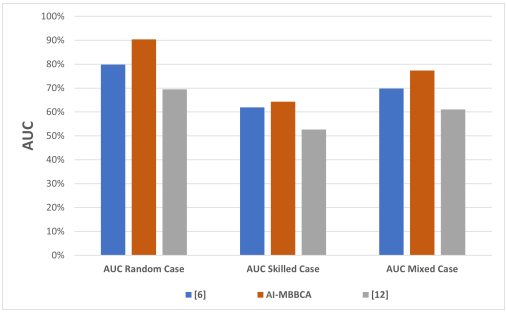

Fig. 5. AUC Performance for the best fusion of different background sensors in the Tap Task.

In summary, our enhanced AI-MBBCA approach outperformed the other compared approaches [6], [12] across all tasks under random, skilled, and mixed impostor attack scenarios. Specifically, it achieved an average AUC improvement of +13.26% over [12] and +8.16% over [6] under random impostor attacks, +9.0% over [12] and +5.0% over [6] under skilled impostor attacks, and +11.19% over [12] and +7.0% over [6] under mixed impostor conditions. The combination of GA-optimized hyperparameters with the IF fusion strategy markedly improved the system's ability to distinguish between genuine and impostor inputs, particularly under the more challenging skilled attack conditions. This substantial performance boost, especially in handling subtle behavioural variations such as keystroke dynamics, demonstrates the robustness and accuracy of our method across all attack types.

V. Conclusion

In this paper, we presented AI-MBBCA, an enhanced CA framework that harnesses GA-driven optimisation for hyperparameter tuning and incorporates an IF layer for sophisticated impostor detection. Our method strikes an effective balance between model complexity and generalisation, preventing overfitting while capturing detailed spatiotemporal behavioural patterns from mobile sensor data. Tests on the BehavePassDB dataset reveal that AI-MBBCA surpasses two state-of-the-art approaches, achieving the highest AUC scores under random and skilled impostor scenarios. Despite these advancements, challenges such as, device-specific biases and the complexities of highly skilled forgery attacks, persist. Future research should explore additional attack types, including data extraction and poisoning, and evaluate the framework using other datasets, calculating runtime and energy consumption and paving the way for more secure and adaptive mobile authentication systems.

Acknowledgment

This research is part of the European AURA.AI project, funded by the European Interreg Upper Rhine program no. 2021-2027. The authors would like to thank all project partners for their collaboration and support.

References

[1] Wang, C., Wang, Y., Chen, Y., Liu, H. and Liu, J., 2020. User authentication on mobile devices: Approaches, threats and trends. Computer Networks, 170, p.107118.

[2] Marcel, S., Nixon, M.S., Fierrez, J. and Evans, N. eds., 2019. Handbook of biometric anti-spoofing: Presentation attack detection (Vol. 2). Cham, Switzerland: Springer.

[3] Stragapede, G., Vera-Rodriguez, R., Tolosana, R., Morales, A., Acien, A. and Le Lan, G., 2022. Mobile behavioral biometrics for passive authentication. Pattern Recognition Letters, 157, pp.35-41.

[4] Delgado-Santos, P., Stragapede, G., Tolosana, R., Guest, R., Deravi, F. and Vera-Rodriguez, R., 2022. A survey of privacy vulnerabilities of mobile device sensors. ACM Computing Surveys (CSUR), 54(11s), pp.1-30.

[5] Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices: Recent progress and remaining challenges. IEEE Signal Processing Magazine, 33(4), 49-61.

[6] Stragapede, G., Vera-Rodriguez, R., Tolosana, R. and Morales, A., 2023. BehavePassDB: public database for mobile behavioral biometrics and benchmark evaluation. Pattern Recognition, 134, p.109089

[7] Acien, A., Morales, A., Fierrez, J., Vera-Rodriguez, R., & Delgado-Mohatar, O. (2021). BeCAPTCHA: Behavioral bot detection using touchscreen and mobile sensors benchmarked on HuMIdb. Engineering Applications of Artificial Intelligence, 98, 104058.

[8] G. Stragapede, R. Vera-Rodriguez, R. Tolosana, and A. Morales, "BehavePassDB: Public Database for Mobile Behavioral Biometrics and Benchmark Evaluation," GitHub repository, 2022. [Online]. Available: https://github.com/BiDAlab/MobileB2C_BehavePassDB/

[9] Deb, D., Ross, A., Jain, A.K., Prakah-Asante, K. and Prasad, K.V., 2019, June. Actions speak louder than (pass) words: Passive authentication of smartphone users via deep temporal features. In 2019 international conference on biometrics (ICB) (pp. 1-8). IEEE.

[10] Abuhamad, M., Abuhmed, T., Mohaisen, D. and Nyang, D., 2020. AUToSen: Deep-learning-based implicit continuous authentication using smartphone sensors. IEEE Internet of Things Journal, 7(6), pp.5008-5020.

[11] Acien, A., Morales, A., Vera-Rodriguez, R. and Fierrez, J., 2020, July. Smartphone sensors for modeling human-computer interaction: General outlook and research datasets for user authentication. In 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1273-1278). IEEE.

[12] Monschein, D., Waldhorst, O.P. (2025). Optimizing Privacy-Preserving Continuous Authentication of Mobile Devices. In: Song, H.H., Di Pietro, R., Alrabaee, S., Tubishat, M., Al-kfairy, M., Alfandi, O. (eds) Network and System Security. NSS 2024. Lecture Notes in Computer Science, vol 15564. Springer, Singapore. https://doi.org/10.1007/978-981-96-3531-3_4

[13] Liu, F.T., Ting, K.M. and Zhou, Z.H., 2008, December. Isolation forest. In 2008 eighth ieee international conference on data mining (pp. 413-422). IEEE.

[14] G. Stragapede et al., "IJCB 2022 Mobile Behavioral Biometrics Competition (MobileB2C)," 2022 IEEE International Joint Conference on Biometrics (IJCB), Abu Dhabi, United Arab Emirates, 2022, pp. 1-7, doi: 10.1109/IJCB54206.2022.10007985.