

Behavioral Biometrics for Continuous User Authentication in Mobile Devices

Amar Sri A¹, Dr. Sandesh Gupta²

¹Research Scholar, Department of Computer Science and Engineering, Chhatrapati Shahu Ji Maharaj University, Kanpur (Formerly Kanpur University) ORCID ID: 0009-0000-6185-2221, Email ID: sriamar2016@gmail.com

²Head, Department of Computer Science and Engineering, Chhatrapati Shahu Ji Maharaj University, Kanpur (Formerly Kanpur University), Email ID: sandeshgupta@csjmu.ac.in

Abstract

The increasing reliance on smartphones for financial, healthcare, professional, and personal services has intensified the need for secure and unobtrusive user authentication beyond initial login. Behavioral biometrics offer a promising basis for continuous authentication by exploiting distinctive interaction patterns such as touch dynamics, keystroke behavior, gait, device motion, sensor responses, application usage, and contextual information. This comprehensive review critically examines recent developments in behavioral biometric authentication for mobile devices, with emphasis on machine-learning and deep-learning techniques, multimodal fusion, adaptive verification, and practical deployment considerations. The reviewed literature demonstrates that conventional machine-learning approaches remain effective for structured behavioral features, while deep-learning models provide stronger capabilities for learning complex temporal and multimodal representations. Multimodal systems can improve robustness by integrating complementary behavioral signals, although their practical adoption is constrained by computational cost, battery consumption, privacy risks, sensor variability, and behavioral drift. The review also highlights persistent challenges involving non-standardized datasets, small user populations, inconsistent evaluation protocols, cross-session and cross-device generalization, spoofing, adversarial attacks, and limited real-world validation. Future research should prioritize privacy-preserving federated learning, lightweight and explainable models, adaptive behavioral profiling, edge intelligence, context-aware authentication, and robust multimodal systems to support trustworthy and scalable continuous mobile authentication.

Keywords: Behavioral Biometrics, Continuous Authentication, Mobile Security, Machine Learning, Multimodal Authentication.

Introduction

Smartphones and mobile devices have made users of these devices much more mobile and capable in their interaction with services of personal, financial, professional, healthcare and communications nature. With the growing volume of sensitive data being stored and processed on mobile platforms, ensuring the security of digital identities and devices has become paramount, and reliable user authentication is a key component of this. Most traditional authentication systems such as passwords, personal identification numbers (PINs), graphical patterns and one-time biometric verification only verify the user at the point of access. After successful authentication, the device typically behaves as if the authenticated user is still controlling the device. This assumption places a security risk on the user's device in case it gets lost, shared, unattended or someone logs into it without permission. For this reason, continuous authentication has become a key component of user authentication in an ongoing session, which does not require frequent explicit user authentication actions [1].

Behavioral biometrics offer a more promising base for continuous authentication as they take advantage of unique patterns that tend to occur in interactions with mobile devices. Behavioral biometrics are based on a person's actions in normal activities, unlike physiological biometrics, which are mostly based on relatively stable physical characteristics. This may therefore be achieved by touch gestures, keystroke dynamics, behavior of the movement of the device, accelerometer and gyroscope data, context by application usage, and other behaviors. This information can be gathered without active involvement from the device, so that authentication can take place as the device is being used, and in a way that minimally disrupts the user. However, there must be a balance between the security and usability, privacy, computation requirements, and security of the sensitive information regarding the behavioral aspects in the continuous behavioral authentication system [2].

With the recent research, the passive mobile authentication has been explored in which behavioral patterns are analyzed without repeatedly asking for a password and explicit biometric sample. With the current trend of multiple sensors in smartphones, it is now possible to build behavioral profiles using multiple signals and to differentiate the users from potentially unauthorized users, based on the behavior. Machine-learning and deep-learning methods have come to play a key role in this process as they are able to detect more complex relationships in behavioral data and help with dynamic identity verification. Passive authentication systems can then be used in conjunction with traditional security systems to offer added authentication during device operation [3].

While significant strides have been made, the literature is wide-ranging in regards to the biometric modalities, data sets, representations of features, learning algorithms, measures of performance, security assumptions, and deployment environments. Other research has also noted ongoing issues with behavioral variability, template protection, privacy, computational complexity, multimodal integration and long-term adaptability. The latest extensive research on continuous biometric authentication highlights the need to combine user profiling, intelligent authentication methods and security factors in the design of practical systems [4]. Thus, this detailed overview survey discusses the behavior-based modalities, machine learning and deep learning methods, multimodal authentication, comparative performance, security and privacy issues, practical constraints, and future research avenues of behavioral biometrics for continuous user authentication in mobile devices.

2. Review Approach and Literature Organization

In this article, the authors take a comprehensive narrative and critical review approach to look at the current status and future prospects of behavioural biometrics for continuous authentication in mobile devices. The review will be a broad thematic review, not necessarily systematic literature review or a meta-analysis protocol. The learning outcomes focus on the understanding of the behavioral biometric features acquired via smartphones, and the use of machine-learning and deep-learning techniques for identity verification, as well as on challenges in authentication performance, usability, privacy, security, computational costs, and practical deployment. We can see from the recent reviews literature that behavioral biometrics has been studied in various contexts of authentication, and their usefulness has not only been found in recognition performance, but also in the type of the biometrics, user characteristics, data collection conditions and implementation environment [5].

The studies reviewed in this literature review are mostly published between 2021 and July 2026 and some earlier studies are included if they provide key conceptual or technological background. The publications are retrieved from a variety of major scholarly platforms and publishers such as IEEE Xplore, ScienceDirect, SpringerLink, MDPI and other reputable academic sources, where applicable with additional identification via a scholarly search service. Research focused on continuous or passive authentication based on the behavior that is produced during mobile-device interaction is preferred. Special focus is placed on the touch dynamics, keystroke patterns, gait, accelerometer and gyroscope signals, device motion, application usage, contextual behavior, and multimodal combinations of these attributes. To this end, studies on machine learning, deep learning, sensor fusion, privacy-preserving mechanisms, and adaptive authentication are also included since they are important technological directions in the current research in behavioral authentication.

In coherent synthesis, the literature reviewed is arranged thematically, not chronologically. Firstly, the theoretical foundations of user authentication and behavioral biometrics are set in place and then each of the behavioral modalities are discussed and characterized. A review of machine-learning and deep-learning methods follows, with their respective applications in behavioural profiling, classification, anomaly detection and continuous verification. Multimodal authentication is treated separately to assess the robustness of using multiple behavioral signals as well as the possibility of lessening reliance on a single biometric source. Previously reported criteria are compared relatively such as behavioral modality, user population/dataset, extracted features, learning algorithm, accuracy,

precision, recall, F1-score, false acceptance rate, false rejection rate, equal error rate, latency, computational requirements, energy consumption, strengths, and limitations. Finally, according to recent review studies, continuous authentication together with intelligent agents, adaptive mechanisms and sophisticated mobile security architectures is becoming a trend, so both the technical performance and practical integration aspects should be discussed [6]. Such a thematic organization thus facilitates a thorough critical synthesis as well as the identification of remaining deficiencies, gaps in research and potential avenues for future research.

3. Background and Theoretical Foundation

3.1 User Authentication

User authentication – the verification of the identity of the person who is attempting to log on to a device, an application or a service. In a mobile environment, authentication is crucial as the smartphone is becoming a repository of personal, financial, professional, communication and other highly sensitive information. There are many different authentication mechanisms that are based on knowledge, possession, physiological biometrics, or behavioural features. Their goal is to keep out unauthorized users and keep users who have legitimate access to the system using the system at an acceptable level of usability.

3.2 Traditional Mobile Authentication

The most common traditional methods of mobile authentication include passwords, personal identification numbers (PINs), graphical patterns, security tokens, fingerprints and facial recognition. The simplicity of having to remember passwords and PINs makes them a common choice but they can be guessed, stolen, observed, and reused in other services. Pattern locks are also vulnerable to observation attacks and smudge attacks. The physiological biometrics like fingerprints and facial features have higher degree of identity binding, but are typically used only at the time of authentication and not continuously during a session. This means that once users are successfully authenticated, it does not necessarily mean they have the control of the device.

3.3 Continuous User Authentication

Continuous user authentication: It is a process that continually evaluates the validity of the current device operator, as opposed to just at the initial login. Continuous mechanisms are used during a live session to monitor information that is relevant and can start further verification when suspicious information is detected. Passive authentication involves less explicit user input than active authentication, which requires an input like a password or biometric sample. Risk-driven approaches involve initial authentication that is followed by periodic behavioral analysis and may lead to higher levels of verification if the perceived risk level rises [7].

3.4 Behavioral Biometrics

Behavioral biometrics are based on the unique way that users interact with devices. There are factors to consider such as touch behaviour, typing rhythm, gait, device movements, gestures, and repetitive usage patterns. These features are especially well suited for continuous authentication, as they can often be gathered naturally from a normal usage of the mobile device without interrupting the user.

3.5 Physiological vs. Behavioral Biometrics

Physiological biometrics are derived from relatively stable physical features like fingerprints, facial characteristics and iris patterns. Behavioral biometrics, however, refer to learned or habit actions such as touch dynamics, keystroke pattern, gait, motion and application-interaction behavior. Physiological biometrics are good for strong verification at specific access points, while behavioral characteristics allow for repeated or passive assessment throughout the ongoing interaction with the device. However, there can be contextual variability in behavioral patterns, depending on context, activity, physical state and use of the device, etc., which is an important consideration for authentication design [8].

3.6 Behavioral Biometrics in Smartphones

There are several sources for smartphones to offer behavioral authentication. Touchscreens can record the

direction, pressure, length and trajectory of a swipe and a virtual keyboard can record the timing and rhythm of typing. The movement and orientation are captured by accelerometers and gyroscopes, while the magnetometers give more information about the movement and GPS can characterize the behavior related to the location. Application interaction and overall movement of the device can also help to build up behavioral profile. These sources can also be combined to give richer representations of user behaviour than a single characteristic.

3.7 Machine Learning in Behavioral Authentication

Machine learning algorithms can be used to detect patterns in behavioral data, and distinguish between authorized and unauthorized users. Popular techniques include support vector machines, random forests, nearest-neighbor methods, ensemble techniques, and anomaly detection. These techniques can convert a set of heterogeneous behavioral measurements to a decision as to who is authenticated or a value of confidence.

3.8 Deep Learning-Based Authentication

Deep-learning methods are used to enhance behavioral authentication by learning complex representations from temporal and sensor data automatically. Convolutional, recurrent neural networks, LSTM and GRU models are architectures of interest for sequential behaviors. With users connecting to a growing number of devices, all of which are intertwined with each other, authentication is also shifting from verifying the identity of one device to continuous authentication across multiple environments. The multi-device continuous authentication, however, is an important extension of behavioral biometric systems, and can only be supported with models that are able to model the variation in sensors, interaction characteristics, and the behavioral differences between the different devices.

4. Behavioral Biometric Modalities for Continuous Mobile Authentication

4.1 Touch-Based Behavioral Authentication

Another important reason why the touch modality is one of the most studied behavioral biometric types for smart phones is simply because people interact with their smart phones naturally whenever they are using them. Authentication systems can recognize user by touch duration, touch pressure, swipe speed, swipe direction, gesture trajectory and the human touch pattern. These features can create unique behavioral patterns without having to perform extra authentication actions. In mobile banking, for example, behavioral interaction could be used as an extra layer of security after the initial login [10]. In addition to using touch only authentication, continuous mobile authentication has been extended to using motion sensor data, explicitly considering privacy preservation, proving that smartphone behavioral verification can combine multiple sources of unobtrusive sensing [11]. We recently see some efforts where touch events are combined with human activities – it is another great example of the potential of interaction patterns for persistent authentication of a smartphone [12]. Omnidirectional touch analysis has also investigated whether touch behavior can be informative in varying directions of touch and under varying interaction contexts, dealing with the variability in real-world mobile use [13].

4.2 Keystroke Dynamics

Keystroke dynamics are used to recognize a user based on their regular typing patterns, instead of on the words that they enter. These features include dwell time (the time measured between the pressing of keys and their release), flight time (the time between the release of a key and the pressing of another key), typing speed (the speed at which the keys are pressed), inter-key latency (the time taken between the release of one key and the pressing of another key), and the overall typing rhythm. These features are especially significant in the case of smartphones since the virtual keyboard is often used to send and receive messages, search for information, enter credentials, and engage with applications. The information from the keystrokes can also be integrated with motion sensor information to give a more complete picture of user activity. Combined behavioral information of soft-keyboard typing patterns and smartphone motion information shows the potential value of the combined

information for continuous authentication by machine learning [14]. Research on behavioral authentication has also expanded to include implicit characteristics like the user's posture, indicating that behavioral authentication models can be extended beyond patterns of direct input to include the context of physical interaction [15]. More recent clientside methods have focused on lightweight keystroke authentication and cross-session evaluation, which are significant considerations when considering authentication effectiveness when typing style changes from session to session [16].

4.3 Gait-Based Authentication

Gait-based authentication is used for a characteristic of a person's gait. On-board motion sensors within smartphones can get information about walking, such as step characteristics, gait cycles, acceleration, and periodicity of movements, which can be analyzed. The gait method is not an explicit authentication method, which could be monitored while the user is wearing the device naturally. But gait parameters can change when walking, depending on the gait speed, type of shoes, placement of the device, walking surface, and physical activity. In order to perform the gait authentication practically, there is a need to accommodate natural variation in behavior while maintaining authentication capabilities between legitimate users and impostors.

4.4 Motion and Accelerometer-Based Authentication

The accelerometers continuously gather data from devices as they move on several axes, hence offering valuable data on how the user carries, holds, rotates and interacts with the smartphone. Behavioral features might involve hand movement, incline of a device, how fast a device is moved, and frequent holding patterns. The signals are good for passive authentication because the data can be gathered when the device is being used normally. Motion can also be used in conjunction with touch or keystroke data, especially if it is not possible to interact with the touch screen directly. However, there is significant variability in motion-based behavioral profiles depending on the location and orientation of the sensor as well as the activity of the user and the environment.

4.5 Gyroscope and Other Sensor-Based Authentication

In addition to providing angular velocity information, gyroscopes are used to help characterize angular orientation changes and rotation of the device, and the magnetometer and other orientation sensors add more information regarding movement. Multiple sensing sources can have a more complete picture of user-device interaction than a single sensing source. Combinations of sensors can then be more robust since they register complementary behavioral aspects, but at the same time consume more processing resources, raise new privacy and energy issues.

4.6 App Usage and Interaction Patterns

Behavioral authentication can be based on user interaction with mobile apps as well. Key applications include how often users are using them, common app sequences, session duration, navigation behavior and interaction frequency. These can create longer-term behavioural patterns as people can establish a regular pattern of accessing specific services. Application behaviour, however, can change dramatically over time, and authentication systems must be able to cope with such legitimate changes.

4.7 Location and Contextual Behavior

Contextual authentication builds on the use of behavioral attributes, adding other factors like location, time of day, network context, device state, and environmental conditions. Direct behavioral evidence is enhanced by contextual information to support authentication decisions. But location and contextual information is a private sensitive data and must be handled with care, securely stored and used proportionately.

4.8 Multimodal Behavioral Biometrics

Multimodal behavioral authentication uses complementary signals like touch and keystroke dynamics, touch and motion, accelerometer and gyroscope data, gait and movement of the device, or interaction and interaction pattern with contextual data. The fusion can be done at the feature level with extracted features, and the score level with the confidence value of the authentication, and the decision level with the output of more than one of the classifiers. The use of multimodal solutions can decrease the level of reliance on a single behavioral signal and give a more comprehensive picture of user-behaviour. However, their applicability relies on the availability of

sensors, synchronization, computational burden, protection of privacy, and processing of missing/inconsistent modalities.

5. Machine Learning and Deep Learning Approaches

5.1 Traditional Machine-Learning Approaches

Even though deep learning is gaining popularity in behavioral biometric authentication, traditional machine-learning techniques are still crucial and can be used to effectively process engineered features derived from touch, keystroke, motion, gait, and sensor signals. Logistic Regression, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Decision Trees, Random Forest, Gradient Boosting and XGBoost are often used as classifiers. Most of these methods involve some pre-processing and feature extraction before classification. Additionally, they have relatively low computing demands and thus may be viable to be used on a cell phone, especially if authentication is required on the spot. But the effectiveness of their application is heavily reliant on the quality and stability of the behavioral features and on their capacity to encode differences in user behavior across sessions and contexts.

5.2 One-Class and Anomaly Detection Approaches

An alternate formulation of the continuous authentication problem is as an anomaly detection problem where the system's main learning task is to learn the normal behavior of the legitimate user. One-class approaches do not need representative samples for all of the possible impostors, but instead assess the similarity of the new behaviour to the behaviour that has been enrolled. This formulation is useful in the context of real-world authentication as it is hard to get complete unauthorized user data. However, factors such as threshold selection, behavioral drift and legitimate usage pattern changes can increase the rate of false reject and/or false accept. One-class and anomaly detection methods are not explored as the main focus of the present reference set, and should be interpreted with caution.

5.3 Artificial Neural Networks

Due to these reasons, Artificial Neural Networks (ANNs) have high flexibility in modelling compared to many other traditional classifiers, as they are able to model the non-linear relationships between behavioural features and authentication results. Their use is especially applicable in scenarios with multiple correlated measurements from the smartphone's sensors. Deep-learning methods using mobile sensing have shown the feasibility of learning the patterns of the activities that may be used to establish authentication, paving the way for the wider use of neural architectures for continual user authentication [17].

5.4 Convolutional Neural Networks

Structured behavioral/sensor data can provide localized and hierarchical representation to Convolutional Neural Networks (CNNs). Continuous authentication can employ CNN models to recognize discriminatory patterns in motion sequences or sensor windows or transformed behavioral signals. They are useful when the authentication features that are relevant are spread over complex multidimensional inputs, in situations where they can also help to lessen the need for manually engineered features.

5.5 Recurrent Neural Networks

Recurrent Neural Networks (RNNs) are especially of particular interest for behavioral biometrics, since behavioral biometrics often require a sequence of signals. The keystroke timing, touch sequence, gait cycle and sensor trajectory evolves over time, not as standalone measurements. RNNs have the ability to learn temporal relationships that traditional static classifiers can't necessarily learn from previous observations, since they can hold information from past observations.

5.6 LSTM and GRU Networks

The Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) variants of the recurrent model are extensions that address some of the challenges of long-term dependencies. These models can be used for

continuous authentication, as normal behaviours might require to be captured over longer stretches of interactions. Comparative analysis of deep-learning models to perform continuous authentication has pointed out the importance of neural network architectures for learning behavioral biometric patterns and determining their applications for persistent user verification [18].

5.7 Autoencoders and Representation Learning

High-dimensional behavioral observations can be represented concisely using autoencoders and other representation learning techniques. These methods can be helpful in the case of two or more sensor channels or advanced behavioral factors in the authentication of a smartphone. They may be used for dimensionality reduction, feature learning, and even for anomaly-based authentication. The references assigned to this section, however, do not contain direct evidence of mobile authentication specifically for autoencoder-based continuous authentication, and thus the approach is considered as a general avenue of research in representation learning.

5.8 Hybrid and Advanced Deep-Learning Models

In recent years, complementary learning techniques are more and more becoming used together to enhance behavioral authentication robustness. Variability in the information from smartphone sensors is also an area of interest that has been explored using generative methods. For enhanced robustness in behavioral verification, a continuous authentication system using Wasserstein generative adversarial networks and sensors on the smartphone is introduced [19]. Multicriteria decision mechanisms like TOPSIS have also been used in the combination of machine-learning models with hybrid decision frameworks in the smartphone behavioral authentication [20]. More recent hybrid deep-learning architectures have harnessed multiple neural components to tackle continuous authentication based on smartphone sensor data, as well as demonstrating a shift towards more broadly capable architectures that can leverage the different behavioral signals that are temporally and heterogeneously available [21].

5.9 Emerging Temporal and Transformer-Based Approaches

Temporal modeling is also an important direction as it is important for these systems to be able to detect pattern changes in user behavior for continuous authentication, along with short-term behavioral patterns. Attention mechanisms that can capture long-range relationships might provide benefits for transformer-based architectures. The references cited for this section, however, do not explicitly assess the continuous mobile authentication with transformers. Currently, therefore, the transformer-oriented behavioral modeling should be considered as a new line of research in this particular application field, that needs more empirical evidence.

5.10 Comparative Assessment of ML and DL Approaches

Continuous behavioural authentication requires the use of traditional machine-learning and deep-learning approaches, each with its own set of benefits. The conventional ML methods are typically more reliant on manually designed features, but have lower computational complexity, simpler interpretation and may be more appropriate for resource-limited devices. The models themselves are deep-learning algorithms, which can learn complex spatial and temporal representations, require more data and resources, and generally require more careful optimization. Hybrid approaches seek to exploit these benefits by mixing complementary models, representations of the sensors, or decision mechanisms. Thus, the decision of whether to use ML or DL should not solely come from the accuracy of authentication, but also take into account data availability, computational cost, latency, data interpretability, adaptability, privacy and the requirement of smartphone deployment. A model, then, for continual mobile authentication is thus context-dependent and must take into account practical considerations such as continuous operation on the device.

6. Comparative Analysis of Existing Studies

There is significant diversity in behavioral modalities, datasets, learning strategies, evaluation protocols, and performance reported for previous studies on continuous-authentication. Therefore, it is important to take the

broader perspective when comparing the figures directly. The chosen studies cover various stages of the evolution of behavioral authentication starting from few-shot anomaly detection, unsupervised modeling of combined smartphone signals, and adaptive verification based on smartphone and smartwatch sensing, up to recent multimodal deep-learning ensembles. Table 1 displays their main characteristics.

6.1 Study-Level Comparative Analysis

Table 1. Comparative analysis of representative continuous behavioral authentication studies

Ref.	Year	Behavioral Modality	Dataset/Users	Main Features	Algorithm/Approach	Reported Performance	Key Finding	Main Limitation
[22]	2021	Touch/position + accelerometer	Android-based data from multiple users	Touch position, acceleration, timestamps	Unsupervised Hidden Markov Model	AUC up to 100%; EER 1.34%	Combining position and accelerometer information substantially strengthened continuous verification	Best performance required aggregation of 25 gestures and gestures with at least 50 data points
[23]	2022	Touch + accelerometer + gyroscope	HMOG: 100 users; BBMAS: 117 users	Raw touch and motion-sensor signals	Few-shot anomaly detection with LFP-TCN	EER 10.95% on HMOG and 12.85% on BBMAS with multimodal sensor input	Few-shot learning improved authentication when complete impostor information was unavailable	Performance varied considerably according to sensor combination and evaluation dataset
[24]	2022	Motion-based smartphone and smartwatch behavior	WISDM: 51 users performing 18 activities	Accelerometer and gyroscope signals	ML-based two-step adaptive verification with confidence threshold	Best-case accuracy included 98.8% for drinking and 96.4% for eating a sandwich	Motion behavior can complement MFA and confidence scores can assist rejection of adversarial inputs	Authentication performance and thresholds depend on activity and sensor context

[25]	2026	Touch + sliding + inertial sensor data	35,519 samples from 15 users	Touch, geometric trajectory, IMU kinematics	CNN + LSTM + GRU with optimized weighted voting	Accuracy 99.23%; precision 100%; F1-score 82.14%; EER 0.16%	Optimized multimodal fusion produced high authentication performance, with sensor kinematics contributing strongly	Small participant cohort limits broader generalizability
------	------	--	------------------------------	---	---	---	--	--

[22] showed that in the earlier combined-biometric approach, both touch-position and accelerometer signals can be complementary to each other in providing authentication evidence. When predictions from various gestures were combined, its HMM implementation resulted in an AUC of up to 100% and an EER of 1.34%. Note, however, that it is only after 25 consecutive gestures that aggregation is required, which represents an important trade-off in continuous authentication: The more behavioral evidence that can be used to provide more confidence in authentication, the longer the time interval between gestures for authentication.

Wagata and Teoh [23] adopted a few-shot anomaly detection problem for mobile authentication, and tested their technique on HMOG and BBMAS. When touch, accelerometer, and gyroscope signals were all taken into account, their LFP-TCN actually produced multimodal errors of 10.95% and 12.85%. The study is significant because practical systems generally do not have full representations of potential impostors, and few-shot and weakly supervised strategies are appealing.

Verma et al. [24] explored motion based behavioral verification using the WISDM database which has 51 subjects and 18 daily activities recorded from the smartphone and smartwatch accelerometer and gyroscope. They concluded that the authentication ability varies with the different physical activities, and the best case of 98.8% was obtained in the case of drinking and eating a sandwich, while the case of eating a sandwich yielded 96.4%. It has also been shown that adversarial manipulation can significantly impact a traditional classifier, leading to the adoption of confidence-based thresholds under adaptive authentication.

More recent work [25] is a step towards multi-modal heterogeneous deep learning. It was a hybrid of CNN sensor modeling, sliding-pattern analysis based on LSTM, and touch modeling based on GRU, which are integrated by an optimized weighted-voting method. The peak accuracy score for the optimized configuration was 99.23%, with a precision of 100%, an F1 score of 82.14% and an EER of 0.16% over 35,519 samples obtained from 15 subjects. The relatively small number of participants is considered an important limitation for the population level generalization, although the reported performance is good.

6.2 Performance Across Behavioral Modalities

The comparative evidence suggests that the behavioral modalities vary with respect to the level of discriminative information that they provide. The attraction of touch behavior is that it is a natural occurrence in normal use and relies on appropriate gestures, application context and duration of interactions. In [22] the integration of touch-position information with accelerometer data demonstrates how motion information can be used in conjunction with touchscreen behaviour. Likewise, [23] demonstrated that multi-modal authentication using touch, accelerometer and gyroscope signals obtained better EER results than the few sensor-based combinations.

Another important source of behavioural information is the motion oriented authentication. In [24] the evaluation of the smartphone-smartwatch analysis suggests that discrimination ability is highly dependent on the activity to be performed. Some hand-oriented activities gave more information about the user than some of the traditional gait oriented activities. In addition, the kinematics of inertial sensors offer additional biometric information, which can be especially useful in conjunction with direct interaction characteristics like touch and sliding actions, as

indicated by more recent multimodal evidence [25]. So, it is not possible to find a single modality that is universally most effective; this would depend on the data available, context, temporal stability, sensor quality and the authentication scenario.

6.3 Comparison of Machine-Learning Approaches

In the context of comparatively low computational requirements, and explicit feature modeling, the advantages of traditional and probabilistic machine-learning techniques are apparent. For instance, HMM-based methods in [22] showed that the performance of an unsupervised probabilistic model is high, when its appropriate touch and motion features are integrated. The adaptive verification strategy described in [24] is another example of conventional classifiers being useful in combination with confidence based decision logic.

The performance of conventional ML, on the other hand, can be drastically different depending on the method of preprocessing, the choice of features, the threshold, and the behavioral representation. The same authors in [24] also point out that high accuracy of benign-data is not always a sign of a strong authentication as accuracy can be greatly reduced if the observations of the sensors are distorted. Therefore, the robustness and decision confidence should be taken into account when assessing the classical ML systems, besides their classical accuracy.

6.4 Comparison of Deep-Learning Approaches

Deep-learning methods are more capable of extracting discriminative representations automatically from raw or minimally-processed behavioral signals. In [23] the few-shot temporal architecture shows the potential of temporal convolutional modeling for authentication in the case of few impostor data. The results also indicate that using multiple sensing modalities can afford more discriminating information than only motion sensing modalities. The concept is further extended in the heterogeneous architecture reported in [25] where the neural architectures are assigned to different modalities: CNNs for inertial sensor information, LSTMs for sliding trajectories and GRUs for discrete touch events. This modality-specific processing is based on the knowledge that each behavioral signal has its own temporal and structural properties. However, as the architecture becomes more complex, so do computational needs, tuning and reliance on representative training data.

6.5 Unimodal vs. Multimodal Authentication

Overall, the studies reviewed in this paper support multimodal authentication in the presence of complementary behavioral information. Situation change (temporary change in user behavior, sensor position, interaction context or environmental conditions) can render a single modality ineffective. Multiple touchscreen and motion channels [23] or smartphone and smartwatch sensing [24] or touch, sliding and inertial information [25] can lessen the need to rely on any one of these signals.

But multimodality does not necessarily translate to better in all circumstances. Crowding sensors together makes acquisition more complex, requires more synchronization, leads to higher battery usage, more dimensionality and privacy exposure. The goal of the practice problem is then to find such combinations that yield complementary biometric evidence, with acceptable latency and computational cost.

6.6 Authentication Performance Measures

The current studies use different performance metrics, of which EER is particularly important when applying the authentication system to biometric systems since it denotes the operating point at which FAR and FRR are equal. The lower the EER, the better the balance between legitimate users and imposters. For instance, in [22] the EER was found as 1.34% and in [23] EERs of 10.95% and 12.85% on HMOG and BBMAS, respectively, were reported. These values are not to be understood as a direct ranking since there are significant differences between the datasets, the participants, the authentication protocols, the behavioral inputs and the learning strategies. In terms of performance metrics for authentication, accuracy, precision, recall, F1score, FAR, FRR, ROC-AUC and EER are complementary metrics. Falsely inferring accuracy is problematic when classes are imbalanced, especially in the presence of large numbers of samples containing no legitimate users. The precision and recall thus offer further insight into acceptance decisions, and the F1-score combines them. It is security-critical to have FAR because it concerns non-authorised users who were accepted by the system, whereas FRR is related to the legitimate users

who have been rejected and is related strongly to the usability. ROC-AUC is a measure of discrimination over operating thresholds and EER is a compact biometric comparison point. Several of these metrics were used in the recent multimodal system presented in [25] which achieved 99.23% peak accuracy, 100% precision, 82.14% F1-score and 0.16% EER, showing that considering several metrics simultaneously is more appropriate than focusing solely on peak accuracy.

Overall the comparative literature showcases a trend towards individually engineered behavioral features and probabilistic classifiers to adaptive, few-shot, and multimodal deep-learning systems. Concurrently, the differences between datasets, participant groups, sensor combinations, authentication windows and evaluation methods make direct numerical comparisons hard. The accuracy should therefore be considered in the context of the experiments in which it was measured, and should not be viewed as the best possible result for any single method.

7. Literature-Derived Conceptual Behavioral Authentication Framework

7.1 Framework Overview

Based on the approaches discussed in the literature reviewed, the continuous BA can be considered as the sequence of interconnected tasks of sensing, representation of the behavior, intelligent analysis, risk assessment, and decision making for authentication. The concept of the conceptual framework is to be used not for the introduction of the new authentication system but to be used to combine the main functional components that were repeatedly observed in the research of mobile behavioural authentication. The framework continuously gathers behavioral evidence whilst the smartphone is used for everyday tasks and translates the collected evidence into representative behavioral characteristics, which are then matched with a stored user profile, and generate an authentication or confidence assessment. Previous work has integrated sensor-related information, statistical information, and user-related information into AI-based continuous smartphone authentication, and this work demonstrates the possibility of combining diverse sources of behavioral evidence in a single authentication architecture.

7.2 System Architecture

The conceptual architecture is composed of several logical layers: behavioral data acquisition, behavioral data preprocessing, feature representation, behavioral profiling, intelligent authentication, risk/confidence estimation, authentication decision making and ongoing monitoring. These components do not depend on the one login, but rather work in an iterative manner that allows the determination of the legitimacy of the current device user to be reassessed over the course of a session. This kind of architecture also enables the possibility to add different behavioral modalities, depending on the kind of sensors and interaction means that are available in a specific mobile device.

7.3 Behavioral Data Acquisition Layer

The first layer is capturing behaviour and sensor data as a result of normal interactions with the device. Sources may be touch screen events, keystroke timing, acceleration or gyroscope readings, device motion, gait features, use of application, and context. The frequency at which these signals occur, the number of dimensions, and their meaningfulness in behavior vary. The framework thus allows for unimodal and/or multimodal acquisition as needed for authentication. The collection should be done with minimum disruption so as the explicit interaction will not be the major benefit of the behavioral authentication.

7.4 Data Preprocessing Layer

Raw smartphone behavior data can include sensor noise, gaps in the data, non-uniform sampling rates, missing data and data that varies based on context. Preprocessing is thus used to make the signals collected appropriate for further analysis of the authentication. Depending on the modality, operations performed may include noise reduction, normalization, segmentation, temporal alignment, missing values, and discarding of inappropriate observations. Synchronization is a critical issue in a multimodal environment as the signals from various sensors

could be of varying temporal resolution.

7.5 Feature Extraction and Representation

Behavioral observations are then used to extract characteristics that are relevant to the authentication. Touch interactions can be modeled using duration, velocity, pressure, direction or trajectory features, while keystroke behaviour can include dwell and flight times. Motion signals can be described using statistical, temporal, frequency domain or learned properties. With the advent of modern deep-learning systems, it is possible to further decrease the reliance on manually engineered features by learning representations directly from the sequences of sensors. The representation stage should capture identity-related behaviors, and should reduce extraneous variance due to context and device changes.

7.6 User Behavioral Profile

The legitimate user's behavior is represented by a behavioral profile created from the extracted characteristics. Behavioral biometric templates, unlike physiological ones, are not always stable as they can change with time due to varying interactions. Therefore, a practical solution should allow for some degree of profile adaptation, but also be able to filter out unwanted actions from the profile. Depending on the authentication technique, profile construction can be based on reference distributions, learned embeddings or statistical models, or classifier-specific representations.

7.7 ML/DL Authentication Engine

The authentication engine compares the behavior that it observes to the legitimate-user representation. This layer can host conventional machine learning classifiers, anomaly detection techniques, ensemble classifiers, deep neural architectures and more. An integrated continuous authentication system combining multiple sensors from the smartphone and statistical data shows the way to use heterogeneous behavioral inputs to facilitate continuous user authentication [26]. The learning method should be chosen based on the modality, the size of the training data, the available computational resources, the required latency, and adaptation.

7.8 Continuous Authentication Process

The framework doesn't make one authentication decision, but rather continually revisits certain behavioral evidence throughout the use of the device. Observations are processed in temporal windows and on the basis of interactions and passed on to the authentication engine continuously. That way, the security profile of the device can dynamically shift as its current behavior seems increasingly to be counter to the authorized profile. Where continuous assessment is to be used, however, it should be done with minimal "interruptions" since such interruptions may make the concept less usable in the real world.

7.9 Authentication Decision Mechanism

The authentication result of the authentication engine may be mapped to more than just a binary legitimate/impostor determination. Normally, if the behaviour is sufficiently consistent, then access remains normal; if it deviates moderately, access may be monitored more closely; if it deviates a great deal, it may be explicitly verified or access may be restricted. When using implicit evidence from sensors is not enough or not certain, human-centered bimodal fallback authentication shows the relevance of keeping alternative authentication mechanisms [27].

7.10 Risk and Confidence Score

A confidence or risk score can be maintained continuously and is used to make authentication decisions flexibly. A high confidence means that the behavior is consistent with the legitimate profile and a low confidence means it becomes more and more likely that it is not consistent with the legitimate profile. Based on thresholds, normal traffic flows can continue, more behavioral information can be gathered, or more authentication is needed. It is especially useful for multimodal systems as it allows information from multiple behavioral channels to be fused prior to taking a security action.

7.11 Re-Authentication and Adaptive Response

Access should not be automatically terminated if the behavior is not within an acceptable level of confidence. A

staged response might need a PIN or password, fingerprint, face verification or other authentication factor. In addition, supplementary authentication can be used without unnecessarily restrictive reactions to unknown implicit authentication, as shown by sensor-based bimodal fallback mechanisms [27]. Depending on the risk estimated, other actions can be taken such as access restriction to sensitive applications, higher monitoring frequency, temporary lock of services or full re-authentication of the device.

7.12 Privacy and Security Layer

It is important for privacy and security to be part of the entire framework and not the last step. Raw data, extracted features, behavioral templates, authentication scores and trained model parameters are sensitive and need to be appropriately protected as they provide behavioral information. Excessive exposure can be minimized by data minimization and secure storage, encrypted transmission, restricted access and on-device processing. The conceptual framework thus goes beyond considering privacy protection as a separate condition and equates it with authentication accuracy, computational efficiency, usability, and adaptability.

Overall, the literature-derived framework can be represented as:

Mobile Device/User → Behavioral and Sensor Data Acquisition → Data Preprocessing → Feature Extraction and Representation → User Behavioral Profile → ML/DL Authentication Engine → Authentication/Risk Score → Authentication Decision → Continuous Monitoring → Re-Authentication or Adaptive Response

This framework consolidates the major functional stages identified in existing behavioral-authentication research and provides a conceptual basis for interpreting how sensing, intelligent analysis, confidence assessment, and fallback authentication can operate together within a continuous mobile security environment.

8. Discussion

8.1 Interpretation of Review Findings and Effectiveness of Behavioral Biometrics

From the literature reviewed, it is clear that behavioral biometrics are a viable complementary authentication mechanism for ongoing mobile authentication since they make it possible to verify identity after the initial login. Behavioral authentication can continually review device activity and usage through touch, keystroke, movement, gait, sensor and contextual data, unlike passwords or PINs, or one-time physiological biometric authentication. The value of those systems, however, is very much subject to the stability and discriminative properties of the chosen behavioural features. Patterns generated by touching and typing provide direct interaction, while signatures from the accelerometer, gyroscope and motion signals may be used to help authenticate in more passive ways. Systems that incorporate more than one source of evidence can be more resilient, with multiple behavioural signals removed from the requirements. Meanwhile, inconsistent authentication may result from the variations of behavior when using the device, which include the context of use, posture, activity, device position, environment, fatigue, or use. So, continuous behavioural authentication should be considered not as a static biometric verification but as a continuous verification process.

8.2 Security Threats and Attack Surface

While behavioral biometrics can enhance security after login, they also create attack surface distinct from traditional authentication methods. Spoofing and impersonation are significant issues as the impersonator may be trying to mimic or replicate valid interaction patterns. For example, keystroke based systems could be compromised if typing behavior can be deduced from observed information. Synthetic typing patterns based on screen-recorded video have been used to attack the keystroke-dynamics authentication system as shown by Siahaan and Chowanda [28] where they showed that it is necessary to test behavioral systems against imitation and observation-based attacks.

There will need to be more coordinated attack scenarios for continuous authentication systems. Collusion attacks can be made by multiple malicious parties, or by a manipulation of the interaction between the two parties that goes beyond what regular impostor testing can detect. Several studies on continuous authentication against collusion attacks have demonstrated that the robustness evaluation should be done with more than just the

genuine-user vs. single-impostor scenario [29]. As a result, future behavioral authentication systems must take into account a variety of threats and not just security in terms of traditional recognition accuracy, such as spoofing, replay, manipulation of the sensor, mimicry, collusion, and adversarial interference.

8.3 Privacy, Behavioral Data Protection, and Ethical Considerations

Behavioral authentication is based on long-term observation of users' actions, and thus raises significant privacy concerns. Patterns of touch, typing speed, motion, use of applications, where the person is and what he or she is doing can tell more than just who he or she is. These data can reveal routines, patterns of movement, physical activity or interaction patterns. Thus, privacy protection should be taken into account for all phases of the authentication pipeline such as acquisition, feature extraction, template construction, model training, model storage, transmission and decision-making.

Therefore, privacy preserving continuous authentication has been emerging as an important research direction. Baig et al. [30] specifically looked at a privacy-preserving behavioral biometric authentication, highlighting the importance of minimizing the disclosure of potentially sensitive behavioral information while still retaining the ability to do authentication. Here are some of the relevant protections that can be adopted: data minimization, secure storage, encrypted communication, limited access to templates, local or on-device processing, and privacy-conscious model design. Ethical issues are also significant as continuous monitoring should be made clear to the users and they should be informed. Users should be aware of the information about the behavior that is being collected, the purpose for the collection, how long it's being stored, whether or not it's being processed outside their control, and so on. To ensure bias and fairness, the issue of behavioral patterns and sensor availability should be taken into account since these may vary from person to person, from device to device, with physical measures, by age and in the environment where the sensors are used.

8.4 Multimodal Authentication, ML/DL, and the Security–Usability Trade-Off

Multimodal behavioral authentication, which uses complementary signals, is suggested to be more robust option, according to the review. One modality may be decreased while another is increased; for instance, if less touchscreen interaction is available, some other modality might be increased to compensate. But there are extra complexities with multimodal systems, such as sensor synchronization, missing data, feature fusion, computation, and privacy. Thus, more modalities does not necessarily lead to a more successful practical authentication system. Machine-learning and deep-learning technologies are at the heart of making authentication decisions based on behavioral observations. While conventional ML approaches can provide lower complexity and higher interpretability, deep-learning models can gain automatic knowledge of the temporal and nonlinear representation from heterogeneous sensor data. However, their actual utility needs to be carefully evaluated in terms of resource usage, data needs, latency, and flexibility. The important thing to remember is that continuous authentication should not create false rejections over and over which disrupt the legitimate authentication process. The emphasis in human-centred work on behavioural biometric interfaces has been the adaption and co-adaptation of the authentication method and the users: security enhancements need to be integrated with the usability of the interaction process [31]. Therefore, the best system isn't necessarily the one with the highest classification accuracy, but rather, the one that meets a desired balance of security, usability, privacy and operational cost.

8.5 Computational, Energy, and Practical Deployment Challenges

As mobile deployments become more practical, behavioral authentication systems must comply with a few hard requirements. Frequent sensing, feature extraction, and retraining of the model may lead to higher power consumption, memory usage, and battery consumption in a processor. Monitoring behavior frequently can enhance the availability of behavioral evidence, but can be very energy consuming. On the other hand, the lower sampling rate or authentication frequency will save resources and delay the time of detecting unauthorized control.

These challenges are especially important for multimodal and deep-learning systems, where multiple streams of

data from multiple sensors may be required to be processed at the same time. The use of lightweight models, selective sensing, adaptive sampling, and event-triggered authentication may help to lower the amount of computations. On-device processing can also enhance privacy by reducing the amount of raw behavioural data transmitted, but it will need models that can be used on smartphones with limited resources. The practical systems should also be designed to consider the variance in the hardware, operating systems, sensor characteristics, device models, and the variations in the ways the devices are used. A method that works well in a controlled environment may thus be less effective when deployed in a more diverse mobile environment.

8.6 Implications for Real-World Mobile Authentication

All the evidence indicates that behavioral biometrics is best viewed as a complementary continuous security measure, not a replacement for other forms of authentication. Conventional credentials and physiological biometrics are still valuable for explicit identity confirmation, with the help of behavioral monitoring to look for suspicious changes after the initial access. A risk-adaptive design can thus continue to grant normal access when there is an ample amount of confidence in behavior, prompt more monitoring when the confidence is not high enough, and explicitly ask for re-authentication when the estimated risk is too high to be accepted.

These are just some scenarios where such an architecture can come in handy, such as mobile banking, enterprise applications, healthcare systems, digital payments and others where it can be crucial to prevent misuse after login, which can have far-reaching implications. But, apart from the recognition performance, some other factors like authentication latency, false rejection, energy consumption, privacy exposure, model adaptability, and sensitivity of the protected application should be taken into account for deployment decision. In most continuous-authentication situations, it is better to have a context-dependent threshold and multiple authentications than to have a binary decision for authentication.

8.7 Limitations of Existing Literature and the Present Review

However, there are limitations in the literature that impact on the interpretation of reported performance in behavioral-authentication. Often, studies have different numbers of participants, different setups for sensors, different sets of behavioral tasks, different session lengths, different data sets, different representations of features, different model architectures, and different evaluation protocols. As a result, the accuracy, FAR, FRR, EER and other metrics from different studies are not necessarily directly comparable. Some findings are limited in generalizability due to the limited use of cross-session evaluation, the controlled data-collection environment, and the small number of participants involved and limited cross-device testing. Another real-world behavioral drift is problematic, as the way users use the software can change over days, months, devices, or across different application contexts.

The present article is not a systematic literature review or meta-analysis, but a comprehensive narrative and critical review. It therefore does not attempt to cover exhaustively all publications in the field but rather to put together representative recent publications and important research lines. The review focuses mostly on the latest literature published since 2021, and provides a thematic organization of the evidence along behavioral modalities, ML/DL techniques, multimodal authentication, security, privacy and deployment aspects. While these are all limitations, the evidence that was reviewed does provide a coherent basis to conclude on the key strengths, unaddressed challenges, and future needs of behavioral biometrics for continual authentication over mobile devices.

9. Research Gaps

Although significant advances have been made, there are still a number of issues that need to be addressed with regard to continuous behavioral authentication for mobile devices. The lack of a standardized benchmark data set and common evaluation methods is one of the major drawbacks, limiting the possibility of comparing studies directly. A number of the databases studied exist with small populations of users (or homogeneous populations)

and do not provide generalizability for users in larger populations or for a variety of usage conditions. The authentication is further complicated by behavioral drift and cross-session variations, as the legitimate behavior may vary between sessions as a result of context, device placement, user behavior or environmental factors. The generalization across devices is also limited; the characteristics and interaction of sensors with the phone may differ across models and platforms. Recently, research on behavioral biometric adaptability has demonstrated that the problem of ensuring reliable authentication even though user behavior changes from session to session and across operational contexts remains challenging [32]. However, there are limited long-term evaluations and real-world applications, along with privacy-performance balance problems, computational burden and battery usage. Multimodal systems add more fusion/synchronization challenges, and the degree of robustness to spoofing, adversarial manipulation and behavioral imitation is not sufficiently explored. Lastly, lack of explainability may lead to decreased user trust, especially if authentication actions lead to access control restrictions for no clear reason.

10. Future Research Directions

Future work for continuous behavioral authentication should aim to be more adaptive, private, light- and deployment-ready systems. The use of advanced multimodal authentication that incorporates additional complementary behavioral cues, such as touch, keystroke, motion, gait, and contextual information, can enhance robustness, yet there is a need for efficient fusion strategies to manage computational and energy requirements. However, federated learning is also very promising as it allows for the training of behavioral authentication models across decentralised devices without the need for the collection of raw user data by a central entity, which facilitates privacy-preserving and decentralised learning [33]. Future systems must also include explainable AI in order to provide meaning to the authentication decision and the confidence scores and re-authentication requests for the user and/or the system administrator. The distributed learning approach for scalable authentication without compromising user-specific behavioral information across devices has also been investigated in mobile crowdsourcing systems [34]. To minimize data exposure and communication costs, privacy-preserving machine learning should thus be leveraged to work in tandem with lightweight deep-learning architectures, edge processing, and on-device inference. The recent work on privacy-aware federated biometric authentication also shows the promise of combining federated deep learning with privacy-based continuous verification [35]. Some directions of importance are adaptive behavioral profiles that undergo legitimate behavioral drift, continual and online learning, better cross-device generalization, context-aware authentication, and risk-adaptive decision mechanisms. A future system should also be tested for more complex attacks of the spoofing, mimicry, adversarial, and sensor-manipulation types to be sure that any improvements in authentication performance actually result in strong, real-world security.

12. Conclusion

However, to overcome the password, PIN and one time authentication limitations of mobile users, behavioral biometrics have become a significant method of improving continuous user authentication. The literature surveyed indicates that the dynamics of interacting with the touch, the dynamics of pressing keys, gait, motion signals, sensor patterns, application usage and contextual information can provide useful evidence of behavior for persistent identity verification. The ability of these systems has been greatly enhanced by machine-learning and deep-learning techniques that allow them to better model behavior, detect anomalies and adapt their authentication methods. Multimodal approaches are especially promising in that they utilize complementary signals and do not rely on a single behavioral characteristic, but are also faced with increased computational, energy and privacy requirements. Direct comparisons of performance are challenging due to differences among the studies, the data sets, the participants, the sensors and evaluation procedures, and the metrics reported. However, a good indication of the potential exists when comparisons are made across studies. This is also a

security threat, spoofing, behavioural mimicry, privacy issues and robustness of the model are still critical. There are several major research gaps such as small number of user populations, behavioral drift, insufficient longterm real-world validation, limited benchmark datasets and cross-session and cross-device variability. What is recommended for the future is to focus on privacy-preserving federated learning, lightweight models, explainable AI, adaptive profiles, edge intelligence, multimodal fusion, and advanced attacks' robustness.

Refereneces

1. M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, "Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 65–84, 2021, doi: 10.1109/JIOT.2020.3020076.
2. A. F. Baig and S. Eskeland, "Security, privacy, and usability in continuous authentication: A survey," *Sensors*, vol. 21, no. 17, Art. no. 5967, 2021, doi: 10.3390/s21175967.
3. P. M. A. B. Estrela, R. O. Albuquerque, D. M. Amaral, W. F. Giozza, and R. T. de Sousa Júnior, "A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications," *Sensors*, vol. 21, no. 12, Art. no. 4212, 2021, doi: 10.3390/s21124212.
4. J. M. Espín López, A. Huertas Celdrán, J. G. Marín-Blázquez, F. Esquembre, and G. Martínez Pérez, "S3: An AI-enabled user continuous authentication for smartphones based on sensors, statistics and speaker information," *Sensors*, vol. 21, no. 11, Art. no. 3765, 2021, doi: 10.3390/s21113765.
5. S. Mekruksavanich and A. Jitpattanakul, "Deep learning approaches for continuous authentication based on activity patterns using mobile sensing," *Sensors*, vol. 21, no. 22, Art. no. 7519, 2021, doi: 10.3390/s21227519.
6. D. Reichinger, E. Sonnleitner, and M. Kurz, "Continuous mobile user authentication using combined biometric traits," *Appl. Sci.*, vol. 11, no. 24, Art. no. 11756, 2021, doi: 10.3390/app112411756.
7. L. Hernández-Álvarez, J. M. de Fuentes, L. González-Manzano, and L. Hernández Encinas, "SmartCAMPP—Smartphone-based continuous authentication leveraging motion sensors with privacy preservation," *Pattern Recognit. Lett.*, vol. 147, pp. 189–196, 2021, doi: 10.1016/j.patrec.2021.04.013.
8. A. Buriro, S. Gupta, A. Yautsiukhin, and B. Crispo, "Risk-driven behavioral biometric-based one-shot-cum-continuous user authentication scheme," *J. Signal Process. Syst.*, vol. 93, pp. 989–1006, 2021, doi: 10.1007/s11265-021-01654-2.
9. D. Progonov, V. Cherniakova, P. Kolesnichenko, and A. Oliynyk, "Behavior-based user authentication on mobile devices in various usage contexts," *EURASIP J. Inf. Secur.*, vol. 2022, Art. no. 6, 2022, doi: 10.1186/s13635-022-00132-x.
10. G. Stragapede, R. Vera-Rodriguez, R. Tolosana, A. Morales, A. Acien, and G. Le Lan, "Mobile behavioral biometrics for passive authentication," *Pattern Recognit. Lett.*, vol. 157, pp. 35–41, 2022, doi: 10.1016/j.patrec.2022.03.014.
11. K. Wagata and A. B. J. Teoh, "Few-shot continuous authentication for mobile-based biometrics," *Appl. Sci.*, vol. 12, no. 20, Art. no. 10365, 2022, doi: 10.3390/app122010365.
12. A. Verma, V. Moghaddam, and A. Anwar, "Data-driven behavioural biometrics for continuous and adaptive user verification using smartphone and smartwatch," *Sustainability*, vol. 14, no. 12, Art. no. 7362, 2022, doi: 10.3390/su14127362.
13. A. Jairam, T. Halevi, and T. Raphan, "Improving mobile device security by embodying and co-adapting a behavioral biometric interface," *Front. Comput. Sci.*, vol. 4, Art. no. 754716, 2022, doi: 10.3389/fcomp.2022.754716.
14. C. R. P. Siahaan and A. Chowanda, "Spoofing keystroke dynamics authentication through synthetic typing pattern extracted from screen-recorded video," *J. Big Data*, vol. 9, Art. no. 111, 2022, doi: 10.1186/s40537-022-00662-8.
15. P. Lyu, W. Cai, and Y. Wang, "Continuous authentication against collusion attacks," *Sensors*, vol. 22, no. 13,

Art. no. 4711, 2022, doi: 10.3390/s22134711.

16. U. Uslu, Ö. D. Incel, and G. I. Alptekin, "Evaluation of deep learning models for continuous authentication using behavioral biometrics," *Procedia Comput. Sci.*, vol. 225, pp. 1272–1281, 2023, doi: 10.1016/j.procs.2023.10.115.
17. V. Gattulli, D. Impedovo, G. Pirlo, and F. Volpe, "Touch events and human activities for continuous authentication via smartphone," *Sci. Rep.*, vol. 13, Art. no. 10515, 2023, doi: 10.1038/s41598-023-36780-3.
18. A. F. Baig, S. Eskeland, and B. Yang, "Privacy-preserving continuous authentication using behavioral biometrics," *Int. J. Inf. Secur.*, vol. 22, pp. 1833–1847, 2023, doi: 10.1007/s10207-023-00721-y.
19. P. Aaby, M. V. Giuffrida, W. J. Buchanan, and Z. Tan, "An omnidirectional approach to touch-based continuous authentication," *Comput. Secur.*, vol. 128, Art. no. 103146, 2023, doi: 10.1016/j.cose.2023.103146.
20. S. Zou, H. Sun, G. Xu, et al., "A robust continuous authentication system using smartphone sensors and Wasserstein generative adversarial networks," *Secur. Commun. Netw.*, vol. 2023, Art. no. 3673113, 2023, doi: 10.1155/2023/3673113.
21. Y. Wang, X. Zhang, and H. Hu, "Continuous user authentication on multiple smart devices," *Information*, vol. 14, no. 5, Art. no. 274, 2023, doi: 10.3390/info14050274.
22. R. Veiga, C. B. Both, I. Medeiros, D. Rosário, and E. Cerqueira, "A federated learning approach for authentication and user identification based on behavioral biometrics," in *Proc. Brazilian Symp. Comput. Netw. Distrib. Syst. (SBRC)*, 2023, pp. 15–28, doi: 10.5753/sbrc.2023.536.
23. E. A. Sağbaş and S. Ballı, "Machine learning-based novel continuous authentication system using soft keyboard typing behavior and motion sensor data," *Neural Comput. Appl.*, vol. 36, pp. 5433–5445, 2024, doi: 10.1007/s00521-023-09360-9.
24. O. L. Finnegan, J. W. White III, B. Armstrong, et al., "The utility of behavioral biometrics in user authentication and demographic characteristic detection: A scoping review," *Syst. Rev.*, vol. 13, Art. no. 61, 2024, doi: 10.1186/s13643-024-02451-1.
25. S. Ayeswarya and J. K. Singh, "A comprehensive review on secure biometric-based continuous authentication and user profiling," *IEEE Access*, vol. 12, pp. 82996–83021, 2024, doi: 10.1109/ACCESS.2024.3411783.
26. M. Wazzeah, H. Ould-Slimane, C. Talhi, A. Mourad, and M. Guizani, "A continuous authentication approach for mobile crowdsourcing based on federated learning," *IEEE Access*, vol. 12, pp. 178237–178250, 2024, doi: 10.1109/ACCESS.2024.3507695.
27. A. A. Farhan, A. Basharat, N. Allheeb, and S. Kanwal, "Enhancing smartphone security with human centric bimodal fallback authentication leveraging sensors," *Sci. Rep.*, vol. 14, Art. no. 24730, 2024, doi: 10.1038/s41598-024-74473-7.
28. B. Hu, S. Tang, F. Huang, G. Yin, and J. Cai, "Implicit identity authentication method based on user posture perception," *Electronics*, vol. 14, no. 5, Art. no. 835, 2025, doi: 10.3390/electronics14050835.
29. M. L. Shuwandy, Q. Alasad, M. M. Hammood, et al., "A robust behavioral biometrics framework for smartphone authentication via hybrid machine learning and TOPSIS," *J. Cybersecurity Privacy*, vol. 5, no. 2, Art. no. 20, 2025, doi: 10.3390/jcp5020020.
30. B. Alotaibi and M. Alotaibi, "Hybrid deep learning framework for continuous user authentication based on smartphone sensors," *Sensors*, vol. 25, no. 9, Art. no. 2817, 2025, doi: 10.3390/s25092817.
31. C.-S. Cheng, K.-C. Chang, H.-C. Chen, and C.-L. Chou, "Continuous smartphone authentication via multimodal biometrics and optimized ensemble learning," *Mathematics*, vol. 14, no. 2, Art. no. 311, 2026, doi: 10.3390/math14020311.
32. A. Subash, I. Song, I. Lee, and K. Lee, "Adaptability of current keystroke and mouse behavioral biometric systems: A survey," *Comput. Secur.*, vol. 160, Art. no. 104731, 2026, doi: 10.1016/j.cose.2025.104731.
33. Z. Zhang, M. Papaioannou, G. Choudhary, and N. Dragoni, "Client-side continuous authentication using keystroke dynamics: A lightweight pipeline and cross-session evaluation," *Electronics*, vol. 15, no. 11, Art. no.

2325, 2026, doi: 10.3390/electronics15112325.

34. A. Al Abdulwahid, "Privacy-aware continuous federated biometric authentication (PACFBA) using federated deep learning: A novel usable security framework," *Sci. Rep.*, vol. 16, Art. no. 24856, 2026, doi: 10.1038/s41598-026-55046-2.
35. M. Gali, A. Kassenkhan, Y. Chinibayev, A. Abshukirova, and V. Serbin, "Behavioral biometric continuous authentication for mobile devices with an intelligent personal agent: A systematic review," *Technologies*, vol. 14, no. 7, Art. no. 451, 2026, doi: 10.3390/technologies14070451.