Computers & Security 128 (2023) 103184

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Stationary mobile behavioral biometrics: A survey

Aratrika Ray-Dowling*, Daqing Hou, Stephanie Schuckers

Department of Electrical and Computer Engineering, Clarkson University, 8 Clarkson Avenue, Potsdam, 13699, New York, USA

ARTICLE INFO

Article history:
Received 29 November 2022
Revised 25 February 2023
Accepted 12 March 2023
Available online 15 March 2023

Keywords:
Mobile device security
Continuous authentication
Stationary behavioral biometrics
Motion sensor
Cognitive psychology
Natural behavior
Designed behavior

ABSTRACT

Current security mechanisms in mobile devices such as PINs, passwords, patterned passwords, and biometrics are one-time entry-point authentication and vulnerable to attacks. Furthermore, advanced mechanisms like Multi-Factor Authentication (MFA) introduce friction in the user experience. In contrast, behavioral biometrics rely on user interaction with computing devices to authenticate a user and thus, can be continuous, non-intrusive, and cost-effective, representing a promising direction that complements existing authentication techniques. This survey focuses on stationary/non-walking (sitting, standing) mobile behavioral biometrics through motion events like acceleration, gyroscope, magnetometer, and orientation (rotation) with the optional support of other non-motion, sporadic modalities such as swipes and keystrokes. The focus on stationary behaviors can be justified because such behaviors represent the major way a user interacts with mobile devices. To help readers understand the broad landscape of user activities/behaviors, we categorize the state of the art into *natural* and *designed* behaviors and describe the underpinning of behavioral biometrics in cognitive psychology. Furthermore, we categorize the surveyed studies into three groups based on the fusion of motion modalities and characterize each study along dimensions such as task, datasets, modality, algorithms, and performance. Based on our survey, we identify several future directions of research.

1. Introduction

Mobile devices are widely used for daily activities such as transmission of sensitive information, messaging, online banking, fitness tracking, and online shopping, among others. Confidential user data is often protected through one-time entry-point security mechanisms like PINs, passwords, patterned passwords, and biometrics (face, iris, fingerprint). Such security mechanisms are either knowledge-based static passwords (PINs, passwords, patterned passwords) (Aravindhan and Karthiga, 2013) or static biometrics (iris, fingerprint, face) (Behavioral biometrics vs static biometrics: Dynamic fraud detection explained, 2022; Li et al., 2020a; Ryu et al., 2021), both of which are vulnerable to attacks. On the other hand, the more advanced Multi-Factor Authentication (MFA) requires the user to provide additional factors such as one-time passwords (OTP) and thus introduces friction to the user experience.

Behavioral biometrics in addition to being dynamic (Behavioral biometrics vs static biometrics: Dynamic fraud detection explained, 2022; Fantana et al., 2015) is also frictionless as it passively authenticates users to secure their mobile devices. There are multiple in-built mobile sensors (touch, keypress, motion, light, camera, proximity, temperature, and elevation) that log the user's behavioral biometrics data which can be used to authenticate the legitimate user of the device. This cost-effective security mechanism can continuously authenticate users if the data is non-sporadic in nature. Among the phone sensors, touch event (swipe, tap, pinch, zoom), keypress, and proximity log sporadic data which if unavailable at an instant cannot be utilized for authentication. However, the motion sensors (accelerometer, gyroscope, magnetometer, and rotation/orientation) can log data whenever the phone is in operation and are therefore non-sporadic in nature which will support continuous authentication even when the sporadic modalities (keypress, swipes) are unavailable.

In this survey, we explore the strengths and challenges of motion events (accelerometer, gyroscope, magnetometer, orientation) based continuous authentication on mobile devices. We focus on studies where the users' motion is captured in their stationary/non-walking (sitting/standing) states. This focus on stationary behaviors can be justified because such behaviors represent the major way a user interacts with mobile devices. Additionally, stationary behaviors are important because modern knowledge workers spend a significant amount of time working with mobile devices in stationary states (Barkley and Lepp, 2016; Zagalaz-Sánchez et al., 2019). Barkley and Lepp (2016) (Barkley and Lepp, 2016) show that 87% users in their study are seated while

[*] Corresponding author.
E-mail address: ray@clarkson.edu (A. Ray-Dowling).

https://doi.org/10.1016/j.cose.2023.103184
0167-4048/© 2023 Elsevier Ltd. All rights reserved.

interacting with their phones and that only 5.9% of the users who use their phones frequently interact with their cell phones in non-stationary states. Zagalaz-Sánchez et al. (2019) review studies that show how excessive mobile phone usage in modern days is leading to reduced physical activity. These studies show the preference of users to maintain stationary states over non-stationary while interacting with mobiles. Furthermore, in many cases, the magnitudes of the sensor events and their variations with time are lower compared to when users are walking/moving which affects the performance (Alobaidi et al., 2022; Ehatisham-ul Haq et al., 2018) therefore making the stationary scenario more challenging. Thus the stationary scenario deserves further attention. Through our survey of the studies involving stationary behaviors, we observe that even with minimal motion during sitting and standing the users can be authenticated with comparable high performances to that of walking-based postures. The study by Ray et al. (2021) has observed gyroscope data of lower magnitudes ($<$ 0.05 radian/second) produce worse results for which they consider gyroscope data beyond 0.05 radian/second. In the dataset papers (Ehatisham-ul Haq et al., 2018; Kumar et al., 2018; Sitová et al., 2015) where the same experimental setup is maintained between stationary and non-stationary data we observe a drop in performance in the case of stationary data. These studies overcome this challenge by several techniques which include fine-tuning the normalization technique of the data (Kumar et al., 2018), performing experiments with many algorithms (Ehatisham-ul Haq et al., 2018; Kumar et al., 2018), performing fusion of modalities (Ray et al., 2021; Sitová et al., 2015), and choosing deep network algorithms over traditional machine learning when the latter underperforms (Amini et al., 2018). However, we believe that in the future more research needs to be performed focusing on better overcoming this challenge.

We identify the following unique characteristics of stationary user behavior:

1. Behaviors/Tasks performed when users are either sitting or standing (including relaxed and non-relaxed postures).
2. Stationary behaviors broadly include fore limb movements ranging from hand micro-movements during moving phones, tapping, typing, and swiping to wide angular motion of arms during hand waving, sweeping, and moving arms around elbow holding phones.
3. A stationary posture must involve minimal hip muscle movements.
4. Stationary user postures must not include flexing of hind limb muscles due to walking and running. Flexing of hind limb muscles during stationary behaviors must be limited to fidgeting/twitching and/or flexing during a change of posture (e.g. changing of posture to cross-legged sitting or the other way).

In the case of stationary behaviors, users are either sitting or standing and interacting with the mobile device during which even the smallest magnitude of hand micro-movements can be logged by the motion sensors. Users interacting with mobile devices in hand tend to achieve stability and precision. As a result, the users develop a postural preference. Additionally, the user's hand size, grip strength, and age constitute the physiological traits. Both postural preference and physiological traits are believed to contribute to the uniqueness of user behaviors (Ray et al., 2021; Ray-Dowling et al., 2022; Sitová et al., 2015). Thus the highly available motion sensor data can be analyzed for continuous authentication to secure mobile devices. Stationary behavior on mobiles through motion event-based biometric systems complements the existing security mechanisms in mobile devices and provides additional protection post the entry-point security checking.

As shown in Fig. 5, in this survey we have categorized the behaviors/activities of stationary users across the studies into *natural* (e.g., routine usage, postures with phones, novel behavior, and context limited) and *designed* (e.g., in-air signatures, pattern tracing, and tapping in predefined screen locations, among others). The natural behaviors are non-intrusive, more available than designed, and thus have the advantage of enabling more frequent authentications. Furthermore, the categorization provides a quick overview of all the relevant application scenarios to future researchers. This categorization is also useful since user behavior affects the authentication performance in a biometric system (Eglitis et al., 2020; Sitová et al., 2015).

In our survey, we identify studies (for example Belman et al., 2019; Ehatisham-ul Haq et al., 2018; Kumar et al., 2018; Sitová et al., 2015) which present datasets with both stationary and non-stationary behaviors. For the completeness of their survey and to explain the entire user activities we acknowledge the presence of the non-stationary behaviors and group them under the postures with phones context of the natural behaviors category. All such dataset papers have non-stationary behaviors along with substantial stationary behaviors. However, none of the surveyed studies consists of purely walking-gait-based behaviors.

In this survey, we observe the underpinning of behavioral biometrics by cognitive psychology since the features derived from behavioral biometrics are sequences of motor actions. Irrespective of the skill level that a user possesses (novice, intermediate, and expert), they perform a wide range of behaviors on mobile devices. Such user behaviors are influenced by the general psychology or willingness of the users which in turn affects performances. We explore the stability that a user tends to achieve over time to get accustomed to the mobile interface which is believed to have an effect on authentication performance.

Recent surveys (Abuhamad et al., 2020b; Alsaadi, 2021; Alzubaidi and Kalita, 2016; Eglitis et al., 2020; Mahfouz et al., 2017; Stylios et al., 2021; Stylios et al., 2016; Teh et al., 2016) on behavioral biometrics group studies by the wide variety of modalities involved (keypress, touch, gait, and others). In contrast, our survey focuses on stationary behaviors on mobile devices through motion events. Given that stationary postures are the major way a user interacts with a mobile phone, it is important to focus on stationary user behaviors on mobiles. Moreover, unlike other surveys, we highlight only stationary behaviors through motion events because the motion sensor readings are non-sporadic and become the only means of user authentication when no other sporadic modalities (keypress, swipes, taps) are available.

The state of the art on motion event-based authentication system often fuses the motion data with other sporadic modalities like keypress, swipe, tap, and elevation. Fusing motion events with other modalities when available can improve the performance of the authentication (Abuhamad et al., 2020b; Roy et al., 2015; Shen et al., 2017; Stylios et al., 2021; Teh et al., 2016). In many cases, only the motion sensors (accelerometer, gyroscope, magnetometer, and orientation) are fused to enhance the overall authentication performance (Shen et al., 2017; Sitová et al., 2015). Given the above, we have categorized the reviewed state of the art into three categories by focusing on motion events, as follows:

(i) stationary behavior on mobiles through only motion sensors (presence of at least two motion sensors)
(ii) stationary behavior on mobiles through at least two motion events fused with non-motion sporadic modalities
(iii) stationary behavior on mobiles through only one motion event which may or may not be fused with non-motion sporadic modalities

Across the three categories above, our survey further highlights each reviewed study along the following dimensions - the datasets used, number of data providers, user behavior, duration of device usage, modalities, sampling rate of motion events, algorithms

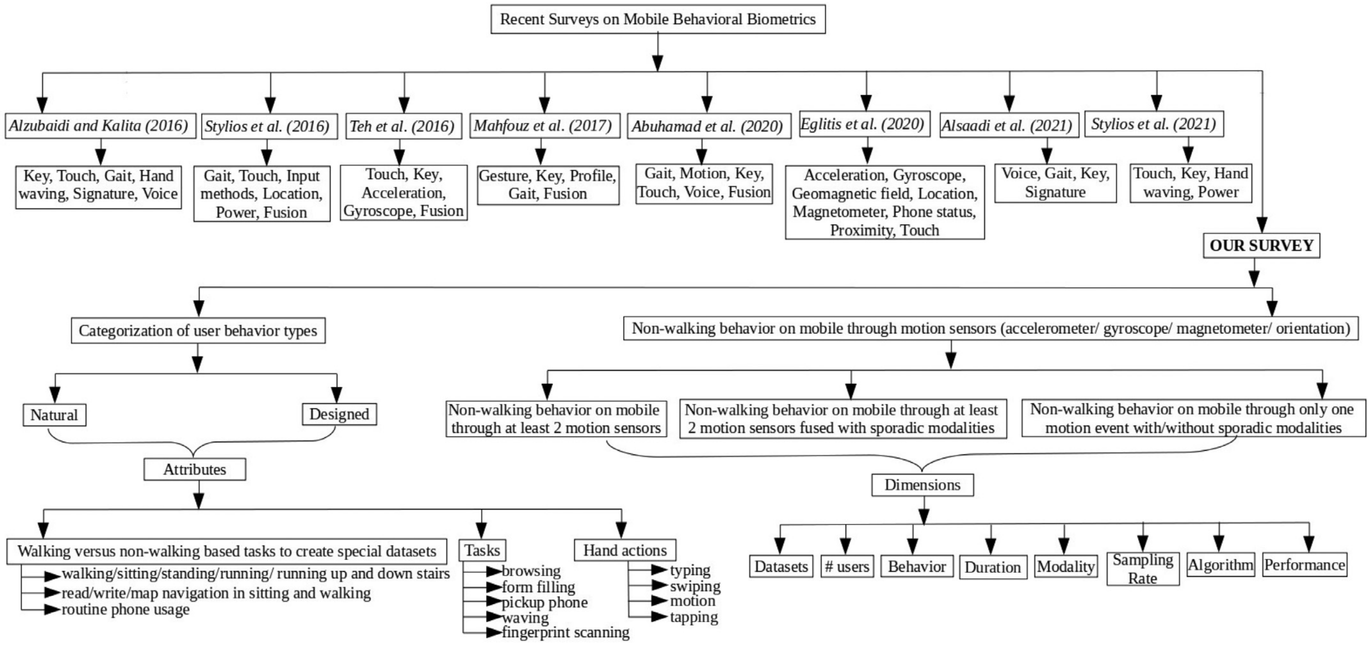

Recent Surveys on Mobile Behavioral Biometrics
Alzubaidi and Kalita (2016)
Stylios et al. (2016)
Teh et al. (2016)
Mahfouz et al. (2017)
Abuhamad et al. (2020)
Eglitis et al. (2020)
Alsaadi et al. (2021)
Stylios et al. (2021)
Key, Touch, Gait, Hand waving, Signature, Voice
Gait, Touch, Input methods, Location, Power, Fusion
Touch, Key, Acceleration, Gyroscope, Fusion
Gesture, Key, Profile, Gait, Fusion
Gait, Motion, Key, Touch, Voice, Fusion
Acceleration, Gyroscope, Geomagnetic field, Location, Magnetometer, Phone status, Proximity, Touch
Voice, Gait, Key, Signature
Touch, Key, Hand waving, Power
OUR SURVEY
Categorization of user behavior types
Non-walking behavior on mobile through motion sensors (accelerometer/ gyroscope/ magnetometer/ orientation)
Natural
Designed
Attributes
Non-walking behavior on mobile through at least 2 motion sensors
Non-walking behavior on mobile through at least 2 motion sensors fused with sporadic modalities
Non-walking behavior on mobile through only one motion event with/without sporadic modalities
Dimensions
Walking versus non-walking based tasks to create special datasets
walking/sitting/standing/running/ running up and down stairs
read/write/map navigation in sitting and walking
routine phone usage
Tasks
browsing
form filling
pickup phone
waving
fingerprint scanning
Hand actions
typing
swiping
motion
tapping
Datasets
# users
Behavior
Duration
Modality
Sampling Rate
Algorithm
Performance

Fig. 1. Comparison of the recent surveys and ours.

evaluated, fusion type, and performance measurement. We further project the behavior dimension of each study to the following attributes/aspects, namely, walking versus non-walking-based tasks to create special datasets, tasks, and hand actions. See Fig. 1 and Section 5. We also elaborately discuss notable feature extraction methods performed by certain studies.

Therefore, this survey has made the following contributions:

1. Focuses on stationary mobile behavioral biometrics where the motion events may also optionally be fused with other non-motion modalities. No prior survey has focused on only stationary behavior on mobiles through motion events which need attention given that stationary behaviors represent the major way of user interaction with mobile devices. See Section 2.
2. User behavior categorization across the state of the art studies into natural and designed behaviors. No prior survey has categorized user behaviors. The natural behaviors which are the most common behavioral type among users (compared to designed) are further divided into four levels of contexts, namely, postures and phone locations, routine usage, context limited, and novel behaviors. See Sections 4.1 and 4.2.
3. Observing the effects of behavioral types on performance to analyze the usability in real-life implementation of behavioral biometrics-based mobile authentication. See Section 4.3.
4. Describing the underpinning of behavioral biometrics in cognitive psychology and the possible effects of general human psychology on the performance of an authentication system. See Section 4.
5. Grouping the state of the art on stationary user behaviors into three categories based on the usage of the motion modalities and others for authentication. See Section 5.
6. Reviewing each study from the three categories along dimensions such as tasks, number of users, datasets, modality, sampling rate, algorithms, and performance along with additional behavioral attributes (walking versus non-walking behaviors, tasks, and hand actions). See Sections 2, 4.4, and 5.

The rest of the paper is arranged as follows - Section 2 introduces our proposed conceptual framework and explains the selection criteria of the reviewed studies and the methodology based on the conceptual framework to search the state of the art. It also compares and contrasts our survey with existing ones. Section 3 describes the background of the surveyed mobile security system with involved motion event sensors and the authentication pipeline utilized across the studies. The section also establishes stationary mobile behavioral biometrics as an authentication modality. Section 4 is a detailed elaboration of our conceptual framework and description of the categorization of user behaviors under natural and designed types and linking each behavior across the studies under such category. It also describes the attributes or properties exhibited by each study. Section 5 contains the survey of the state of the art and links each with the proposed framework described in the sections before. Section 6 discusses the future directions of this research domain towards its application in real-life as a mobile security system. Lastly, Section 7 concludes our survey.

2. Conceptual framework, survey methodology, and existing surveys

This section describes the core conceptual framework of our survey in brief based on which and other factors we list the criteria for choosing studies that we review for our survey in stationary mobile behavioral biometrics through motion events. It also discusses the methodology of searching state of the art to frame our survey following the criteria. Thereafter, in this section, we compare and contrast the existing surveys with ours and demonstrate that no other surveys have proposed similar ideas to ours.

2.1. Proposed conceptual framework

In Fig. 1, we present the taxonomy of the surveys on behavioral biometrics and highlight our uniqueness from others. Our survey focuses on an in-depth review of stationary behaviors on mobiles through motion events/sensors, unlike other surveys which perform a wide review of studies under different modalities. We observe that user behaviors/activities affect authentication performance for which we categorize user behaviors across the studies into natural and designed to analyze the effects of the type on performance. The core concept of our survey lies in the categorization of stationary behaviors in mobiles where we define natural behaviors as routine/daily activities on phones and designed behaviors as the type which are defined by an experimenter for special research purposes (Fig. 5). So far, no other surveys have categorized user behaviors. Furthermore, as shown in Fig. 1, natural and designed behaviors are assigned to the attributes of walking versus non-walking tasks to create special datasets, tasks, and hand actions. Depending on the usage of motion event modalities and their fusion with other sporadic modalities, we categorize the reviewed studies into three groups (see Fig. 1) and analyze each based on dataset, modalities, number of users, duration of phone usage, algorithms, and performance. The above concept is elaborately explained by applying it to each of the surveyed studies in Sections 4 and 5.

2.2. Survey methodology

Based on the core conceptual framework we set the criteria for the selection of the state of the art as follows:

1. The state of the art must be about mobile behavioral biometrics.
2. The state of the art must involve stationary (sitting and standing) user behaviors. Some studies may involve both stationary and non-stationary (gait-based) user behaviors but they must have substantial stationary user behaviors.
3. The stationary user behaviors must be measured utilizing embedded motion event sensors (acceleration, gyroscope, magnetometer, and orientation) to capture a user's stationary hand micro-movements. However, we encourage the fusion of other simultaneously available non-motion modalities with the motion events.
4. We review the novel state of the art works that are published in the following publication venues, namely, Elsevier, IEEE, ACM, and Springer. We have also identified a few notable studies from arXiv. We also review studies that show the potential to include a variety in the range of stationary user behaviors.
5. The existing surveys mostly cover the state of the art on mobile behavioral biometrics up to till 2015. Hence, we decide to review the more recent works (2015 to present) involving stationary behaviors. However, we also include a few studies from the timeline ranging from 2006 to the present to observe the shift of using natural behaviors over designed with time.

Our methodology of surveying the state of the art includes two methods. First, we search Google Scholar and Research Gate with the following four phrases "*continuous authentication on mobile behavioral biometrics*"; "*motion events based continuous authentication*"; "*acceleration based continuous authentication*"; and "*gyroscope based continuous authentication*". Among the four, the first phrase is the most effective. Second, we utilize the "*snowballing*" method to identify more state of the art from the list of references of a study that we have already reviewed.

Depending on the usage of modalities, we identify and review 59 relevant papers by grouping them under three categories. Additionally, we also review the 8 most recent surveys on mobile behavioral biometrics to support our understanding of the state of the art. Given that we categorize the user behaviors/activities across the 59 studies, we study the effect of users' cognitive psychology to interact with the interface for which we analyze 6 studies related to cognitive psychology.

2.3. Other surveys of mobile behavioral biometrics

In this section, we compare other surveys on mobile behavioral biometrics with ours.

The survey by Alzubaidi and Kalita (2016), has grouped studies under seven mobile behavioral biometric modalities (keypress, touch, gait, hand waving, signature, voice, and general profiling). The motivation of this survey is to review the state of the art that can provide additional security mechanisms to overcome active attacks like shoulder surfing. The authors survey papers based on the following key points, namely, the amount of data used in authentication, the types of classifiers utilized, and the authentication performances.

In the survey by Stylios et al. (2016), the authors have grouped continuous authentication studies on mobile devices under walking gait, touch gestures, input methods, location familiarity, power modalities, and their fusion. The key points of surveying each study are the context of the problem, methods/algorithms, number of participants, and citation count.

Reviewing touch and keypress dynamics-based behavioral biometrics studies, Teh et al. (2016) point out the characteristics of an ideal authentication platform based on customizability, flexibility, cost, and market share factors. It explains the degree of control that can be adapted during the data acquisition and device selection process. Additionally, it discusses the type of input string that is ideal for touch-based authentication (free, fixed, semi-fixed, or any touch gestures). The survey discusses the scenario of cross-session-based data acquisition methods which should focus on behavioral adaptation due to cognitive factors, psychological factors, physiological factors, and environmental factors that may affect the authentication performance over time. It also surveys studies that perform fusion of touch-based modalities with motion sensors (acceleration and gyroscope) logged simultaneously.

Mahfouz et al. (2017), group the reviewed state of the art based on gesture, keypress, general profiling, gait, and fusion-based authentication. The authors classify two types of attack scenarios that commonly challenge the traditional security mechanisms of mobile devices, namely insider attacks (from close circles like family and friends) and stranger attacks (from unknown impostors). The main characteristics that a continuous authentication system must possess are continuity- where a smartphone is verifying the user in a continuous manner; periodic re-authentication mechanism- re-authenticating the genuine users; and transparency- unobtrusive continuous authentication. The state of the art are reviewed based on data collection, feature extraction, classification models, and performance. The survey points out the limitations of an authentication system, which are, noisy data, non-universality, intra-class variations, and lack of uniqueness.

A recent survey by Abuhamad et al. (2020b) groups around 140 studies under gait, motion, keystroke, touch, voice modalities, and combination (fusion) of modalities. It classifies the enrollment phase of an authentication system into template and model-based. In template-based, users submit multiple samples to establish templates for the future. Physiological biometrics mostly follow template-based enrollment methods. On the other hand, model-based enrollment trains a Machine Learning model for user authentication where the model decides whether the data belongs to the genuine user. Behavioral biometric-based authentication mostly relies on model-based enrollments where the quality of the features plays an important role. The studies are reviewed under the following key points: user activities, modalities, classifiers used, number of users, performance, authentication time, and the mobile device used.

Eglitis et al. (2020), in their survey discuss the effect of discrete adaptive learning on authentication and therefore relate learning to the overall psychology of the users while getting adapted to the data acquisition interface. They review around 40 works under accelerometer, gyroscope, geomagnetic field, location, magnetometer, phone status, proximity sensor, and touch sensor modalities. The review dimensions for each study are citation count, device operating system, data and software availability, modalities used, data collection conditions, user activities during data collection, sessions, the time between sessions, use of multiple datasets, and attack scenarios.

In a recent short survey, Alsaadi (2021) review studies under voice, gait, keystroke dynamics, and signature modalities. The dimensions of reviewing each study are general problem description, advantages, disadvantages, and applications.

Stylios et al. (2021), is an updated survey on mobile behavioral biometrics that groups reviewed works under touch gestures, keystroke dynamics, hand waving, and power consumption modalities. The survey states the advantages of behavioral biometrics-based continuous authentication as cost-effective, improving systems and the socio-political pressure, and user-friendly. The survey includes the following dimensions to review each study, analysis of data collection methodologies, different feature extraction methods, possible attack vectors of behavioral biometrics, challenges, and future trends. The survey categorizes different attack mechanisms (passive attack and active attack) and points out the kind of attack that is common per reviewed modality.

In our survey, the reviewed state of the art capture user's hand micro-movements while they are in their stationary states and interacting with a mobile device. The state of the art therefore must utilize motion sensors (accelerometer, gyroscope, magnetometer, and orientation) to log the micro-movements exhibited by the user. It is hypothesized that the user's hand micro-movements during stationary behaviors along with their other physiological traits (arm sweep, muscular flexing, grip strength, and hand size) are unique among individuals and can be utilized to authenticate the legitimate user of the mobile device. Additionally, the hand micro-movements are impacted by the user's task/activity/behavior, for which we categorize user behaviors into natural and designed (Section 4).

3. Background

As background, this section aims to present stationary mobile behavioral biometrics through motion events as an acceptable and usable authentication modality. It describes the three major motion sensors that measure the hand micro-movements of static users, the building blocks of a typical authentication pipeline based on authenticating stationary users through micro-movements, and the characteristics and application-scenarios of non-walking mobile behavioral biometrics.

3.1. Motion sensors in smartphones

A biometric system measures one or more physical (face, iris, hand geometry, fingerprint, and others) or behavioral characteristics (micro-movements, typing, swiping, gait, and others) information of an individual to determine or verify their identity. These characteristics are referred to by different terms such as *traits, indicators, identifiers,* or *modalities* (Jain et al., 2011). This section describes the three most commonly used motion sensor modalities for user authentication on mobile devices, namely, accelerometer, gyroscope, and magnetometer. The reviewed state of the art studies have measured stationary/non-walking behaviors in mobile utilizing these three most common motion sensors. Other motion sensors on Android devices like step counters and step detectors are out of the scope of our discussion. Figure 2 shows the graphical readings of acceleration, gyroscope, and magnetometer (geomagnetic field) sensors from the Sensors app (from the Google Play store) on a Samsung Galaxy S22 Android phone. The Sensors app runs in the background when a subject is sitting and typing. The app displays the readings of the phone's sensors on the application interface. The magnitudes of each sensor are low since the subject is in a sitting state.

3.1.1. Accelerometer

Acceleration is the change of speed of an object in three dimensions. An accelerometer is designed to measure static and dynamic accelerations (Carlson et al., 2015). Static acceleration is the constant force acting on a body, like gravity (acceleration due to gravity is constant at 9.8 m/s). Dynamic acceleration forces are non-uniform and caused by vibration or shock. In smartphones, an accelerometer is used to measure the vibration or acceleration of motion of the device. The force caused by vibration or acceleration triggers the sensor material to produce an electrical charge which is proportional to the force exerted on it. The device mass is constant. The charge is also proportional to the acceleration produced due to exerted force and so we have $force = acceleration * device\_mass$ (How to measure acceleration, 2022; Liu, 2013).

3.1.2. Gyroscope

Gyroscope is used to measure orientation, based on angular momentum which is the rotational analog of linear momentum ($linear\_momentum = mass * velocity$). The gyroscope returns the value of angular velocity which indicates how fast the device rotates around its axes (Liu, 2013).

Applications of a phone's gyroscope include motion sensing GUI (Graphical User Interface) which enables users to hover, shake, select, and perform other interactions; answer phone by shaking the device; stabilizing image quality by preventing trembling; GPS navigation; and other motion sensing gaming activities (How does a gyroscope sensor work in your smartphone, 2022).

3.1.3. Magnetometer

A magnetometer measures the strength and direction of the magnetic field. It requires an absolute direction (the direction that obeys the earth's coordinate system). For acquiring error-free magnetometer readings, we need to get rid of the offsets from each axis.

$X\_offset = [\max(Mx) + \min(Mx)]/2$

$Y\_offset = [\max(My) + \min(My)]/2$

$Z\_offset = [\max(Mz) + \min(Mz)]/2$ where Mx, My, and Mz are magnetometer readings along the x, y, and z axes respectively.

$Mx' = Mx - X\_offset$

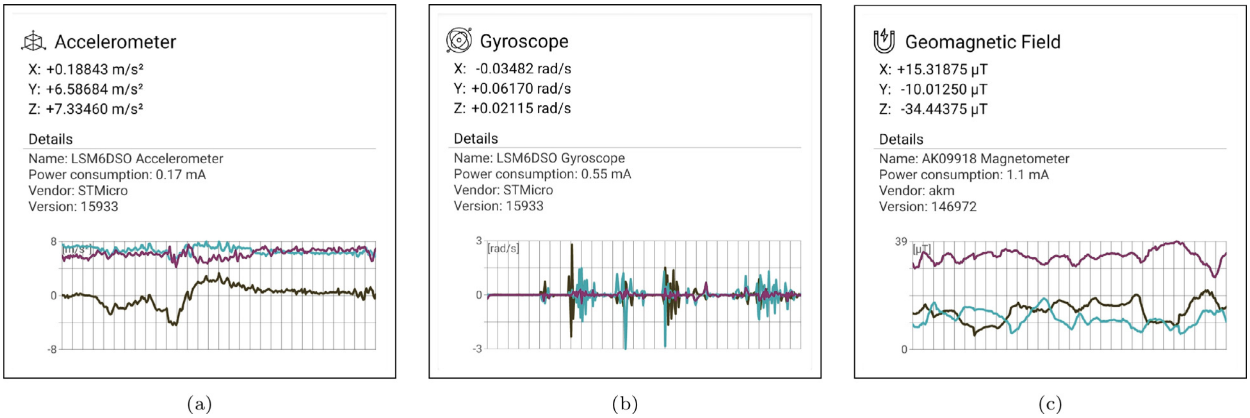
$My' = My - Y\_offset$

$Mz' = Mz - Z\_offset$ where Mx', My', and Mz' are the new magnetometer readings along the x, y, and z axes respectively after subtracting the offsets (Liu, 2013).

Magnetometers in smartphones are used as an e-compass that measures the magnetic fields generally greater than 1 nT (nanoTesla). The magnetometer sensor in smartphones creates a miniature Hall-effect that detects the Earth's magnetic field along the three axes x, y, and z. It works on the principle that a voltage can be detected across a thin metallic element when placed in a strong magnetic field perpendicular to the element's plane (surface) as shown in Fig. 3. The detected voltage is called Hall voltage (V_hall). The Hall voltage is directly proportional to the strength and polarity of the magnetic field perpendicular to the surface. The sensed voltage is converted to a digital signal representing the magnetic field intensity. The output Hall voltage is:

$V\_hall = R_h * [(I/t) * B]$ where R_h is the Hall Effect co-efficient, I is the current flow through the surface in Ampere (amp), t is the surface thickness in millimeter (mm), and B is the magnetic field in Tesla (Cai et al., 2012; hall-effect, 2022; What is magnetometer sensor, 2022).

In addition to accelerometer, gyroscope, and magnetometer there are other position sensors in modern smartphones, namely,



Accelerometer

X: +0.18843 m/s²
Y: +6.58684 m/s²
Z: +7.33460 m/s²

Details

Name: LSM6DSO Accelerometer
Power consumption: 0.17 mA
Vendor: STMicro
Version: 15933

(a)

Gyroscope

X: -0.03482 rad/s
Y: +0.06170 rad/s
Z: +0.02115 rad/s

Details

Name: LSM6DSO Gyroscope
Power consumption: 0.55 mA
Vendor: STMicro
Version: 15933

(b)

Geomagnetic Field

X: +15.31875 μT
Y: -10.01250 μT
Z: -34.44375 μT

Details

Name: AK09918 Magnetometer
Power consumption: 1.1 mA
Vendor: akm
Version: 146972

(c)

Fig. 2. (a) Acceleration, (b) Gyroscope, and (c) Magnetometer sensor readings from the Sensors app on a Samsung Galaxy S22 Android phone while the user is sitting and typing.

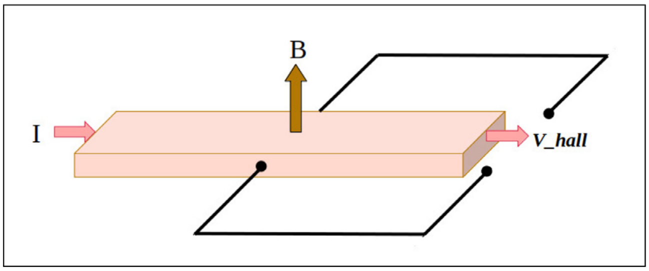


Fig. 3. The Hall Effect principle works by detecting a voltage across a metallic surface (the Hall voltage) in response to a magnetic field that's perpendicular to the metallic surface (Cai et al., 2012).

rotation or orientation sensors which can additionally complement user authentication.

3.2. Building blocks of behavioral biometrics-based authentication system

This section presents the general building blocks of the authentication pipeline of the reviewed studies on stationary mobile behavioral biometrics. A behavioral biometrics-based authentication system generally has the following *subsystems*, namely, collection, transmission, storage, processing, classifier, and decision. Each subsystem comprises *processes*. A behavioral biometric-based authentication system has enrollment and authentication phases in both of which the processing and classifier subsystems are present. See Fig. 4. The reviewed state of the art studies include such building blocks or its subset. The subsystems together with their processes are described as follows:

- *Collection* - is the data collection subsystem in which a biometric pattern is presented to a sensor. The processes of the collection subsystem include biometric pattern, presentation, and sensor (Jain et al., 1999).
- *Transmission* - is the subsystem that is generally present following the collection subsystem. Here, the biometric pattern/signal can be compressed for storage purposes. The signal can be expanded for further processing of the data in the next stages. The processes of this subsystem include compression, transmission, and expansion (Jain et al., 1999).
- *Storage* - is the subsystem to store raw signals from the transmission phase (Jain et al., 1999).
- *Processing* - this subsystem is present in both enrollment and authentication phases to process the raw signals to be used as training and testing samples respectively. The testing samples are future examples that are validated through the pre-trained model. The subsystem includes processes like data cleaning (pre-processing and quality control), feature extraction, and feature selection (optional).
- *Classifier* - The classifier subsystem is present in the enrollment phase for training the model/classifier with the training samples. It is also used in the authentication phase to verify the test samples against the pre-trained model.
- *Decision* - is the last subsystem of the authentication system. Here a decision over the test sample is made of whether or not the sample is accepted as a genuine or rejected as an impostor.

3.3. Characteristics and application-scenarios of stationary mobile behavioral biometrics

In this section, we explore stationary mobile behavioral biometrics through motion events as a biometric modality for user authentication.

Any physiological or behavioral biometrics should possess the following desirable characteristics: *i) universality* - every user possessing the measurable trait; *ii) uniqueness* - the trait must be unique in every individual; *iii) permanence* - the trait should be invariant with time; *iv) collectibility* - the trait can be measured quantitatively; *v) performance* - the trait should achieve an acceptable identification accuracy; *vi) acceptability* - user acceptance of the biometric system based on the trait; *vii) circumvention* - how easily the biometric system based on the trait can be compromised (Jain et al., 1999; 2011; Ross et al., 2006). Several state of the art on stationary behavior on mobiles show that the modality has universality, uniqueness, collectibility, performance, acceptability, and endurance against spoof attacks (cannot be circumvented). However, no single biometrics is expected to possess all the characteristics.

Any biometric system design is application dependent. The applications of stationary behavior-based authentication systems on mobiles can be classified based on the following issues:

i) Cooperative versus non-cooperative users: this issue refers to the user behavior while interacting with the biometric system. The motive of a non-cooperative user generally lies in attempting to hide their identity (Jain et al., 1999; 2011). Stationary behavior on mobiles through motion events-based authentication system does not have this issue as there is passive data logging. Genuine users will allow the sensors to log their data in their own interest in securing their devices. On the other hand, any non-legitimate user will be locked out of the device by the authentication system. For recognition systems that are based on face, fingerprint, and hand geometry, a lot depends on the cooperation of the user.

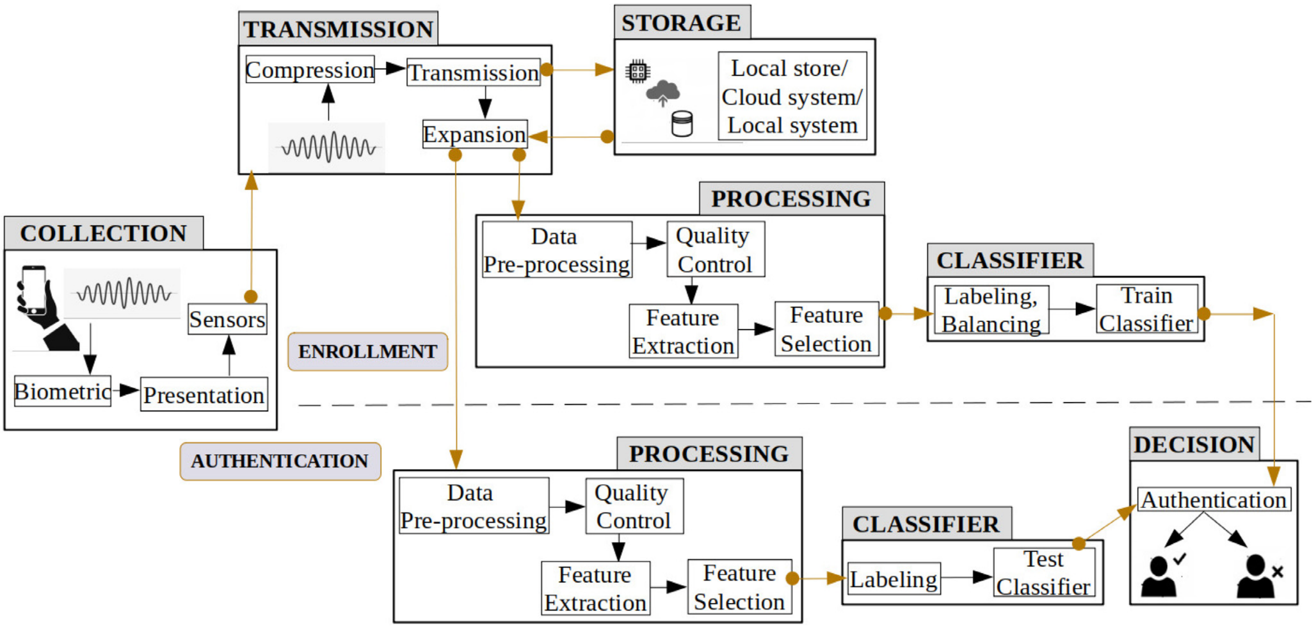


Fig. 4. General Building blocks of behavioral biometrics-based authentication system utilized by the reviewed studies (Abuhamad et al., 2020b; Jain et al., 1999).

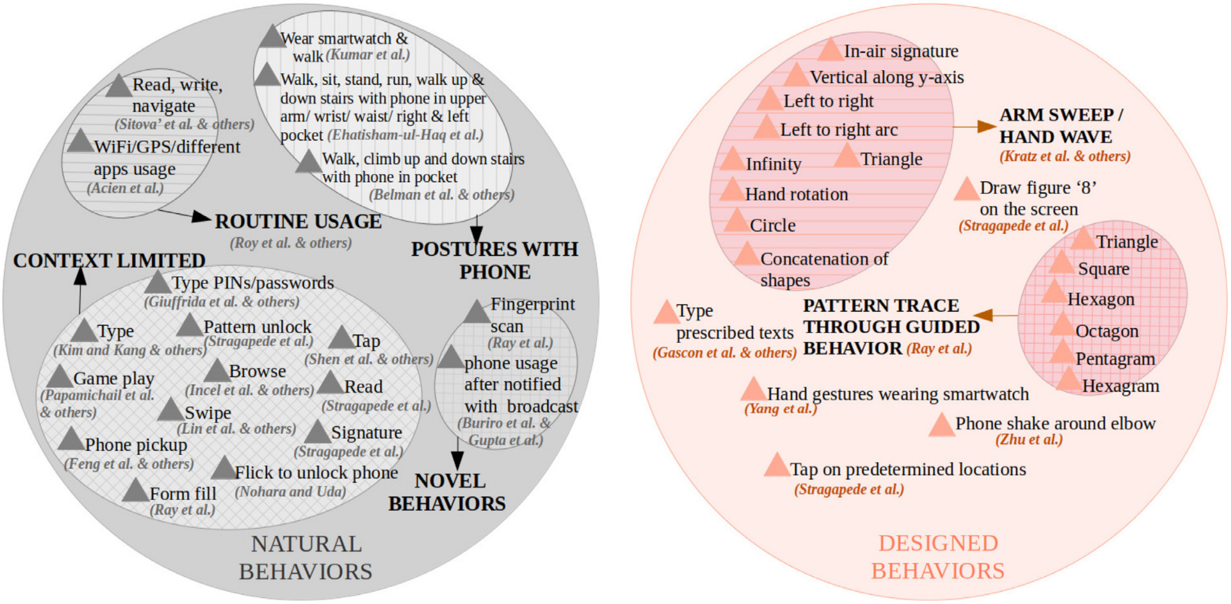

Wear smartwatch & walk (Kumar et al.)
Walk, sit, stand, run, walk up & down stairs with phone in upper arm/ wrist/ waist/ right & left pocket (Ehatisham-ul-Haq et al.)
Walk, climb up and down stairs with phone in pocket (Belman et al. & others)
Read, write, navigate (Sitova' et al. & others)
WiFi/GPS/different apps usage (Acien et al.)
ROUTINE USAGE (Roy et al. & others)
POSTURES WITH PHONE
CONTEXT LIMITED
Type PINs/passwords (Giuffrida et al. & others)
Type (Kim and Kang & others)
Pattern unlock (Stragapede et al.)
Tap (Shen et al. & others)
Game play (Papamichail et al. & others)
Browse (Incel et al. & others)
Read (Stragapede et al.)
Swipe (Lin et al. & others)
Signature (Stragapede et al.)
Phone pickup (Feng et al. & others)
Flick to unlock phone (Nohara and Uda)
Form fill (Ray et al.)
Fingerprint scan (Ray et al.)
phone usage after notified with broadcast (Buriro et al. & Gupta et al.)
NOVEL BEHAVIORS
NATURAL BEHAVIORS
In-air signature
Vertical along y-axis
Left to right
Left to right arc
Infinity
Triangle
Hand rotation
Circle
Concatenation of shapes
ARM SWEEP / HAND WAVE (Kratz et al. & others)
Draw figure '8' on the screen (Stragapede et al.)
Triangle
Square
Hexagon
Octagon
Pentagram
Hexagram
Type prescribed texts (Gascon et al. & others)
PATTERN TRACE THROUGH GUIDED BEHAVIOR (Ray et al.)
Hand gestures wearing smartwatch (Yang et al.)
Phone shake around elbow (Zhu et al.)
Tap on predetermined locations (Stragapede et al.)
DESIGNED BEHAVIORS

Fig. 5. Subcategories of different user behaviors within natural and designed behavior sets.

ii) Overt versus covert deployments: indicate whether the users are aware that they are being authenticated (overt) or otherwise (covert) (Jain et al., 1999; 2011). Motion through a stationary mobile behavior-based authentication system is covert as the users do not have to perform any additional task to authenticate themselves and therefore the data logging is passive. An example of an overt biometric system is fingerprint-based recognition in general.

iii) Habituated versus non-habituated users: Habituated users are those who are accustomed to the biometric system due to frequent interaction. Non-habituated users on the other hand are new to the system (Jain et al., 1999; 2011). Stationary behavior-based authentication systems on mobiles are expected to remain unaffected with users having various skill levels since the motion data gets passively logged while users are interacting on their devices. Additionally, the familiarity of users with the system positively affects the recognition/authentication accuracy (Jain et al., 2011). More insight into this is provided in Section 4.

iv) Attended versus unattended operations: Attended operation refers to observed, guided, or supervised data acquisition (Jain et al., 1999; 2011). An example of an attended operation is a face and fingerprint-based biometric system used to issue identity documents. On the other hand, passive data logging through mobile sensors is unattended.

v) Controlled versus uncontrolled operations: Under controlled operation, environmental conditions like temperature, crowd, lighting, and others can be moderated. On the other hand, data acquisition in outdoor environments is classified as uncontrolled (Jain et al., 1999; 2011). Stationary behavior on mobiles through motion events can be logged in both controlled and uncontrolled environments.

vii) Open versus closed systems: When a user's biometric template can be used as an authenticator in multiple applications it is known as open system. For example, a user's fingerprint may be used for entering a secured building, logging into a workstation, banking, and others (Jain et al., 1999; 2011). On the other hand, the dynamic time-dependent data of motion events-based authentication system cannot be used as an authenticator across several applications or devices and is therefore a closed system. Open systems can be more prone to spoof attacks.

4. Categorizing user behaviors

An authentication system can expect users with different skill levels of interacting with the authentication interface, which are - novice, intermediate, and expert (Haasnoot et al., 2018). Irrespective of the skill level, users perform a wide range of activities/behaviors while interacting with an authentication interface installed to secure a mobile device. Such user activities or behaviors can be categorized as natural and designed behaviors.

Natural User Behavior - It is a type of common behavior when a passive authentication is performed to authenticate the user as a legitimate owner of the device where a user is not constrained to perform any active/designed special tasks. Behaviors like routine phone usage, browsing, typing, form filling, and swiping fall under this category. Therefore, no user training is required before the data acquisition process. The only factor that can affect the authentication is the experience/skill level of the user to interact with a mobile device.

Designed User Behavior - It is the type of user behavior where an active (a designed) special task is required to be performed to log data that will be used for authentication. In many cases, when an authentication dataset is built, researchers may require user behavioral patterns for a certain task (Carroll and Rosson, 1987) for which they include designed behaviors. Examples of designed user behavior are hand waving/arm sweeping, pattern tracing through guided behavior, phone shaking around the elbow, typing prescribed texts, and others. Many data acquisition processes require users to perform an active attack scenario. Here, a user acts as an impostor and tries to mimic a genuine user by watching them perform a designed task in a video. This too falls under the designed user behavior category to test the robustness of the authentication system through the collected data. The designed user behavior requires training/practice for users to get accustomed to the process.

Through our research, we observe that behavioral biometrics involve user tasks/ behaviors that are either performed as per the user's own will without any training or performed when a dataset is collected by an experimenter who is providing special instructions/training. Thus we broadly classify behaviors/tasks into natural and designed.

The concept of cognitive psychology lies in the mental processing of attention, language use, memory, perception, problem solving, creativity, and reasoning as a sequence of information (Cognitive psychology, 2022). On the other hand, the features derived from behavioral biometrics (behaviorism in individuals) are sequences of motor actions. Thus, behavioral biometrics is underpinned by the founding idea of cognitive psychology. Hence, understanding the behavior of users and their adaptability to an interface through a learning process is important.

For both natural and designed behaviors performed, the key factor is the general psychology or degree of willingness of the user. Irrespective of the level of skill and perception, a user tends to develop a learning or an adaptability curve to interact with the authentication interface. The perception of using an embedded biometric system varies across users. Cooperative users have the general psychology to follow the process of authentication and develop individually unique behaviors that are difficult for imposters to emulate. In many cases, an impostor can exhibit haphazard psychology and has the motive to bypass the security mechanism. However, there are enough cooperative and stable users available to utilize the advantages of an authentication system. Therefore, a user's cognitive psychology and adaptability affect their interactive behavior which in turn affects the authentication performance. We observe the effects of natural and designed behaviors in authentication performance to further refine our justification of behavior categorization (Section 4.3). We explore whether both types exhibit acceptable authentication performance given in the real-life implementation both of them can be utilized for user authentication. Additionally, we expect natural behaviors to show good performance since that is exhibited the most by the users during device interactions.

There is an effect of practice (to get accustomed to the task) on the authentication performance (Anderson, 1982; Ericsson et al., 1993; Haasnoot et al., 2018). In Psychology, the Power Law of Practice states that learning does not occur at a constant rate. When learning a new task, the speed of performance improvement in an individual declines. See Fig. 6(b). In behavioral biometrics, the adaptability (the steady state in the curve in Fig. 6(b)) to perform tasks like typing, and swiping while holding devices is believed to reach faster compared to learning any other skillful tasks (e.g. a designed behavior). The natural behaviors are non-intrusive and users are more accustomed to them than designed behaviors. Cognitive Science recognizes that users tend to develop consistency while performing natural behaviors faster than designed (Carroll and Rosson, 1987). Figure 6(a) shows the Speed Accuracy Trade-off (SATF) curves for novice, intermediate, and expert users. The SATF shows a complex relationship between the speed of learning and the accuracy of a system's performance. It shows that a fast learner does not necessarily produce high authentication accuracy and a slow learner does not necessarily show low authentication accuracy. In motor skill learning (like in behavioral biometrics), skill improvements are defined as the changes in the location and shape of a Speed-Accuracy Trade-off Function. See Fig. 6(a). Such variations in performance can affect authentication in a biometric system.

4.1. Natural behaviors across the state of the art

In the case of passive/natural tasks, it requires an individual to process a sequence of motor events. Sequences of motor events can be classified into - (i) *motor adaptation* which is a form of re-learning with gradual improvements in performance and (ii) *motor sequence learning* that involves the acquisition of skill to produce a sequence of movements with limited effort (Anderson, 1982). In Fig. 5, the set of natural behaviors shows the identified user behaviors from the reviewed studies that fall in this group.

Each study involving different natural behaviors has been identified under the appropriate subcategories or levels of context. Looking at the wide range of user behaviors performed naturally we coin four levels of context. However, with fewer designed behaviors such sub-categorization is not meaningful. There are four major frames of reference within natural behavior. The broadest frame of reference is when a user is in different postures (e.g., sitting, standing, walking, running, climbing stairs) and keeps the phone in different body locations (e.g., pockets, waist, hands, upper arms). Under this context, users can perform a wide range of natural behaviors. The next frame of reference is routine usage followed by context limited natural behaviors (typing, swiping, browsing, and others). Routine usage is daily activities on the device whereas context limited focuses on a specific natural task. The narrowest frame of reference is performing novel behaviors for a small interval of time. See Fig. 7. Among the levels of context, novel behaviors, routine usage, and context limited include station-

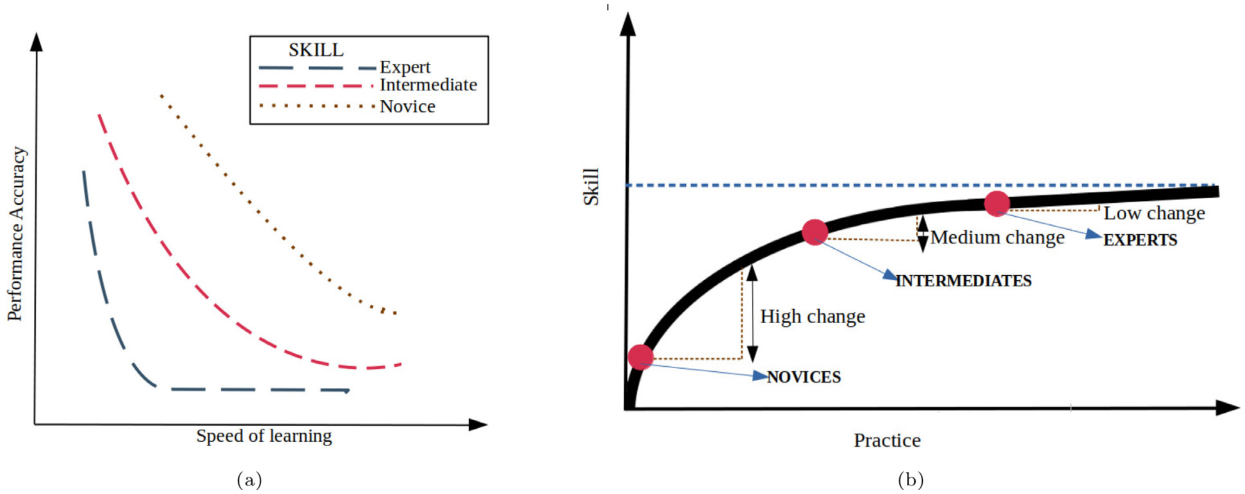


Fig. 6. (a) Speed-Accuracy Trade-off (SATFs) for novice, intermediate, and expert individuals. For each level, there is a change in the shape and location, (b) An example of a Power Law of Practice. The rate of skill change becomes lower for those with higher initial skill/more accumulated practice (Haasnoot et al., 2018).

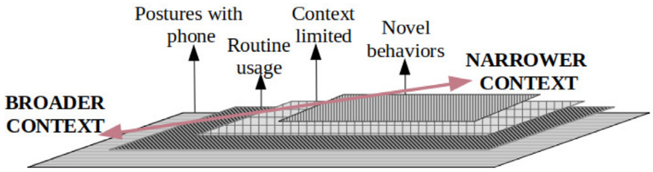


Fig. 7. Four levels of context under natural behaviors. The contexts of novel behaviors, routine usage, and context limited include stationary behavior whereas postures with phone include both stationary and walking behaviors.

ary behaviors. On the other hand, the broadest context, postures with phone, consists of identified studies that include walking behaviors (in addition to stationary behaviors). However, our focus is mainly on studies that involve stationary behaviors.

Postures with phone: Studies that include different postures and phone locations beyond stationary user postures fall under this broadest frame of reference. In the study by Belman et al. (2019) the users walk and climb up and down the stairs with the phone in their pocket. The study by Ehatisham-ul Haq et al. (2018) authenticates users when they are walking, sitting, standing, running, walking up and down stairs with the phone in one of the five different body locations (upper arm/wrist/waist/right pocket/left pocket). User authentication has been performed taking every combination of the user's posture and phone location. In the study by Kumar et al. (2018), the users are walking while wearing a smartwatch and while having a phone in their pocket, through which the movements are measured using motion events. Apart from these, there is the study by Sitová et al. (2015) which involves walking posture in addition to sitting. Figure 5 shows the different natural behaviors under the level/subset of postures with phones exhibited across the above studies.

Routine usage: The studies under routine usage (Abuhamad et al., 2020a; Centeno et al., 2017; Deb et al., 2019; Lee and Lee, 2015; Neverova et al., 2016; Roy et al., 2015; Shen et al., 2017; 2022) have asked users to use the device for a long time span ranging from hours to weeks and perform daily activities. The main purpose of these studies has been collecting large samples of data when users are performing daily tasks. The routine usage behavior in the study by Roy et al. (2015) includes activities like reading Wikipedia articles and answering Qualtrix questions. In Abuhamad et al. (2020a), the users perform a wide range of activities which include screen touch and taps, web browsing, document and email reading, making calls, chatting, and browsing pictures among others. In a different study by Acien et al. (2019) users use GPS, WiFi, and different phone applications like Whatsapp, Facebook, YouTube, and others. Here, users are profiled utilizing information from keystrokes, touch, acceleration, gyroscope, app usage, WiFi, and GPS usage. In Lee and Lee (2017), users perform four routine behaviors which are- using a smartphone while standing, sitting, or moving; when stationary on the table; and in a moving vehicle. The user behavior of read/write/map navigation belongs to routine usage. However, all of these natural activities together are the data collection format of HMOG data by Sitová et al. (2015). Thereafter, other studies (Bhattarai and Siraj, 2018; Centeno et al., 2017; Li et al., 2018; Li et al., 2020a; Li et al., 2021; Li et al., 2020b; Shen et al., 2022; Volaka et al., 2019) have either utilized HMOG or followed the same data collection method to create a special dataset. Motion events are logged while users perform the above routine phone usage. Figure 5 shows the different natural behaviors under the level/subset of routine usage exhibited across the above studies.

Context limited: Other natural behaviors like typing, typing passwords, browsing, swiping, game playing, and phone pick-up fall within the context limited frame of reference. There are studies (Belman et al., 2019; Centeno et al., 2017; Crawford and Ahmadzadeh, 2017; Kim and Kang, 2020; Kumar et al., 2018; Li et al., 2020a; Ray et al., 2021; Ray-Dowling et al., 2022; Sitová et al., 2015; Volaka et al., 2019) that involve the specific task of typing. Out of these works, the study by Kim and Kang (2020) involves typing in both Korean and English languages. In the study by Stragapede et al. (2022a), users answer questions and type free texts through which keypress and other sensor data are logged. Works by Owusu et al. (2012), Giuffrida et al. (2014), Cai and Chen (2012), Stanciu et al. (2016), and Buriro et al. (2021) involve authentication through motion events when users are typing PINs/passwords. Studies by Jain and Kanhangad (2015), Belman et al. (2019), Sitová et al. (2015), Stragapede et al. (2022a), Stragapede et al. (2022b), and Ray et al. (2021) have logged substantial swipes along with motion event data. In the study by Belman et al. (2019) there is a large number of horizontal and vertical swipes. The study by Sitová et al. (2015) logs swipes during the reading and writing activities that users perform across sessions. In Ray et al. (2021) swipes during the form filling process are logged in addition to other modalities. In Jain and Kanhangad (2015) the data includes left to right, right to left, and up and down swipes. In one among 8 different tasks in Stragapede et al. (2022a), users read a document that involves logging vertical swipes along with motion events. It also includes gallery swiping which has logged horizontal swipes and simultaneous motion events. Lin et al. (2012) include up-down flicks/swipes and left-right flicks on the phone's screen. There are wide ranges of applications that are browsed across the studies. The users in Amini et al. (2018) browse the Target shopping app. Users in Incel et al. (2021), Basar et al. (2019), and Stragapede et al. (2022a) browse a banking app and perform standard online banking activities. In the study by Murmuria et al. (2015) users browse Chrome and Facebook. In Kumar et al. (2016b) users sit and perform web browsing. Other context limited behaviors include game playing as performed by the users in Li et al. (2020a) and Papamichail et al. (2019). One of the most common context limited tasks is phone pickup. Studies by Feng et al. (2013), Carlson et al. (2015), Kunnathu (2015), Stragapede et al. (2022a), and Buriro et al. (2015) have authenticated users through the phone pickup trajectory. The behavior of flicking to unlock phones by users in Nohara and Uda (2016) is another example of a specific task for user authentication. On the other hand, Stragapede et al. (2022a) perform unlocking of devices using patterned passwords. Stragapede et al. (2022a) also include signature tasks on the device's screen as a context limited natural behavior. Shen et al. (2016) involve inputting taps on the phone's screen. Another such context limited user behavior is form filling for registration purposes as performed by users in Ray et al. (2021). During all the above tasks the studies capture motion events. Figure 5 shows the different natural behaviors under the level/subset of context limited exhibited across the above studies.

Novel behaviors: We have identified two novel natural behaviors performed by three studies. The studies by Buriro et al. (2017) and Gupta et al. (2022) have authenticated users through motion events for *n* seconds after being notified with a broadcast event that gets triggered when suspicious activity is detected. In the study by Ray et al. (2021) users are authenticated through motion events during a few seconds of using the fingerprint hardware. This is to prevent sensitive applications like online banking that are sometimes locked through the user's fingerprint which can be spoofed easily once an impostor manages to bypass the entry-point authentication. Figure 5 shows the different natural behaviors under the level/subset of novel behaviors exhibited across the above studies.

4.2. *Designed behaviors across the state of the art*

For designed behaviors, training leads to the acquisition of cognitive skills which has two phases - (i) *declarative stage* in which information about the skill domain is interpreted and (ii) *procedural stage* in which domain knowledge is applied for performing the skill (Abrahamse et al., 2013). Figure 5 shows the user activities/behaviors grouped under the set of designed behavior.

In the study by Ray et al. (2021) users trace basic shapes like triangle, square, hexagon, octagon, pentagram, and hexagram. Users trace the patterns through a guided outline and are authenticated through the strokes obtained from the tracing. In Stragapede et al. (2022b), users draw the figure '8' on screen.

Although typing in general is a natural behavior, typing prescribed texts is designed. In the study by Ray et al. (2021), users have to type a declaration statement which is *"I declare that everything I type is truthful"*. One of the tasks in the study of Belman et al. (2019) includes typing two static texts which are *"this is a test to see if the words that i type are unique to me. there are two sentences in this data sample"* and *"second session will have different set of lines. carefully selected not to overlap with the first collection phase"*. Similarly, in the study by Gascon et al. (2014) users type the pangram *"The quick brown fox jumps over the lazy dog"*. Owusu et al. (2012) also involves typing of prescribed pangrams. Users in Stragapede et al. (2022b) perform the tasks of typing a prescribed text in Spanish, which is, *"En un lugar de la Mancha, de cuyo nombre no quiero acordarme"*. In all these studies, motion events are captured while users type the prescribed texts.

In the study by Stragapede et al. (2022a), one of the user behaviors includes a designed behavior of tapping on predetermined locations of the device's screen as fast as possible. Although tapping behavior itself is a natural behavior, the factor of predetermined locations makes the behavior designed.

The study by Yang et al. (2015) has collected motion event data for authentication while users are performing the designed behavior of hand gestures wearing a smartwatch.

Multiple studies have collected motion event data through the designed behavior of hand waving/arm sweeping. The study by Kratz et al. (2013) has trained users to perform six different hand waving gestures as shown in Fig. 9. Similarly, Okumura et al. (2006) have collected user's hand waving data while users have swept their hands vertically along the y-axis. In-air signatures are performed by users in the studies of Casanova et al. (2010) and Laghari et al. (2016). Additionally, Casanova et al. (2010) also performs drawing of concatenated shapes by holding phones in the air. Other similar studies that perform hand waving/arm sweeping are Hong et al. (2015), Yang et al. (2014), and Fantana et al. (2015).

There is a designed behavior performed by Zhu et al. (2017) where users shake the handheld phone utilizing their elbow as the fulcrum as shown in Fig. 10. Hand waving is different from phone shaking around the elbow since in the former case the elbow is not always used as the fulcrum. However, here their elbows are fixed. Additionally, there are only four gestures that users perform under this behavior by always making sure that the shaking happens about the elbow.

We can therefore understand that for most natural behaviors the stability in learning skills to get accustomed to the interface will reach faster (see Fig. 6(b) where the curve plateaus for expert users) than most designed behaviors. To deploy stationary mobile behavioral biometric systems in real life, our research community has performed their studies with mostly natural behaviors. In Fig. 8 we can see a gradual shift toward research using natural user behavior over time. After 2015 the utilization of designed behaviors to authenticate users based on motion events has narrowed down. However, in the studies like Belman et al. (2019), Stragapede et al. (2022a), Stragapede et al. (2022b), and Ray et al. (2021) there is the utilization of both natural and designed behaviors where the number of designed behaviors are less. On the other hand, towards the middle of the timeline (around 2015), there are several studies that started exploring natural behaviors. The plot in Fig. 8 shows a preference for natural behaviors over designed ones since the utilization of natural behaviors can estimate the robustness of the authentication system when deployed in real life. Additionally, natural behaviors are to be expected more in a real-life scenario, than designed. Therefore, the gradual shift in the usage of natural behaviors is justified.

4.3. *Effects of behavior type on authentication*

In case of the natural behaviors, users are free to follow accustomed strategies. On the other hand, while performing designed behaviors users are constrained to perform artificial tasks. Cognitive Science recognizes that users tend to develop consistency in performing natural behaviors which is not the same in the case of designed or artificial tasks (Carroll and Rosson, 1987).

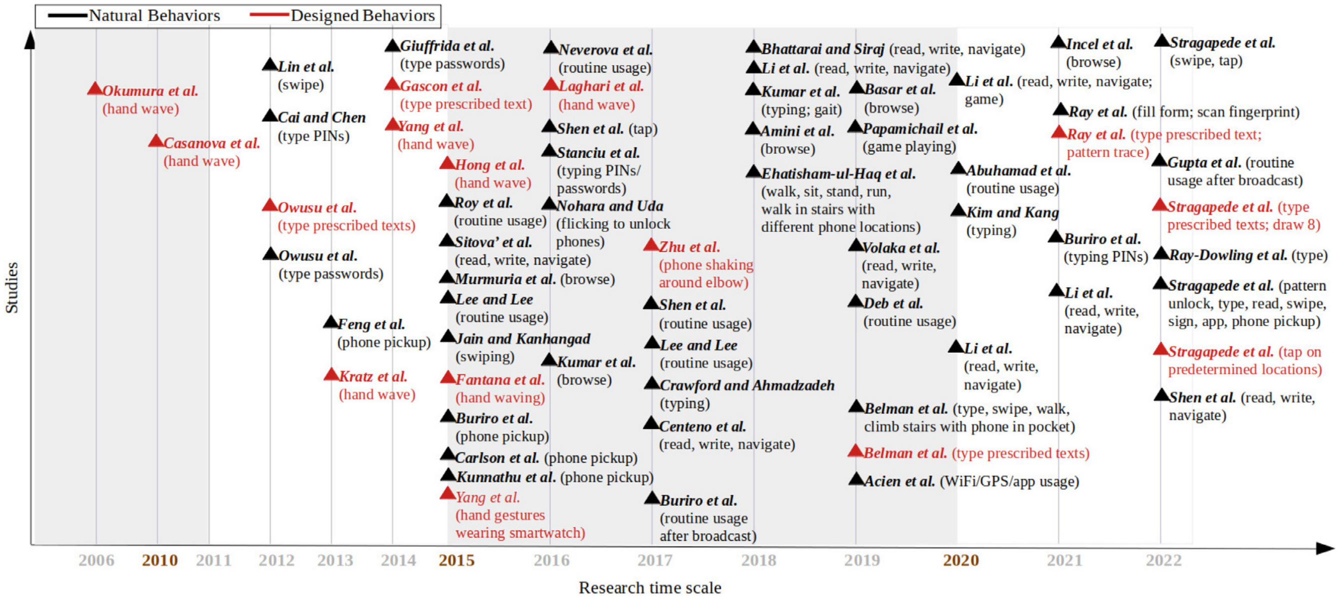


Fig. 8. Research timeline to show a gradual shift toward natural behaviors.

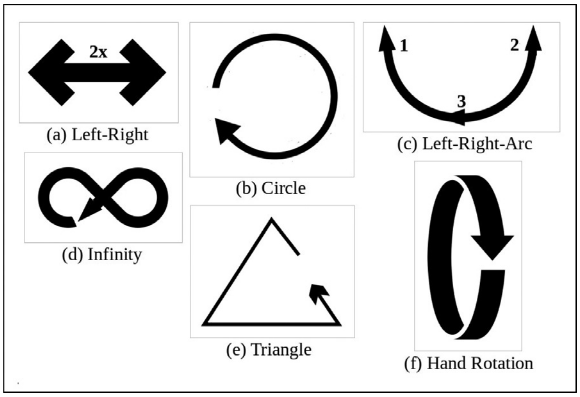


Fig. 9. Hand waving or arm sweeping in Kratz et al. (2013).

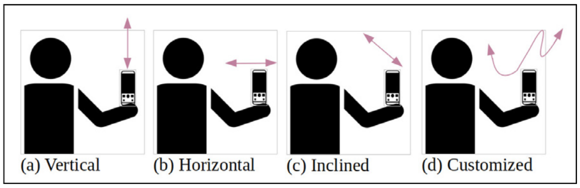


Fig. 10. Phone shaking around the elbow in Zhu et al. (2017).

Figure 11 shows the performances across the reviewed studies which utilize natural behaviors for user authentication. We plot bar graphs for each performance metric. The performance metrics utilized by the studies are EER (Fig. 11(a)), Accuracy (Fig. 11(b)), TAR (Fig. 11(c)), AUC (Fig. 11(d)), and HTER (Fig. 11(e)). We observe from each bar graph that the user authentication performance utilizing natural behaviors for most studies is more than acceptable.

On the other hand, Fig. 12 shows the performances across the reviewed studies which utilize designed behaviors for user authentication. We present bar graphs for each performance metric utilized by the studies which are EER (Fig. 12(a)) and FPR (Fig. 12(b)). However, there are lesser samples of designed behavior performances compared to natural which explains the shift in utilizing natural behaviors more than designed as the research timeline has progressed (Fig. 8). Even among the few identified designed behaviors, the user authentication performances are acceptable.

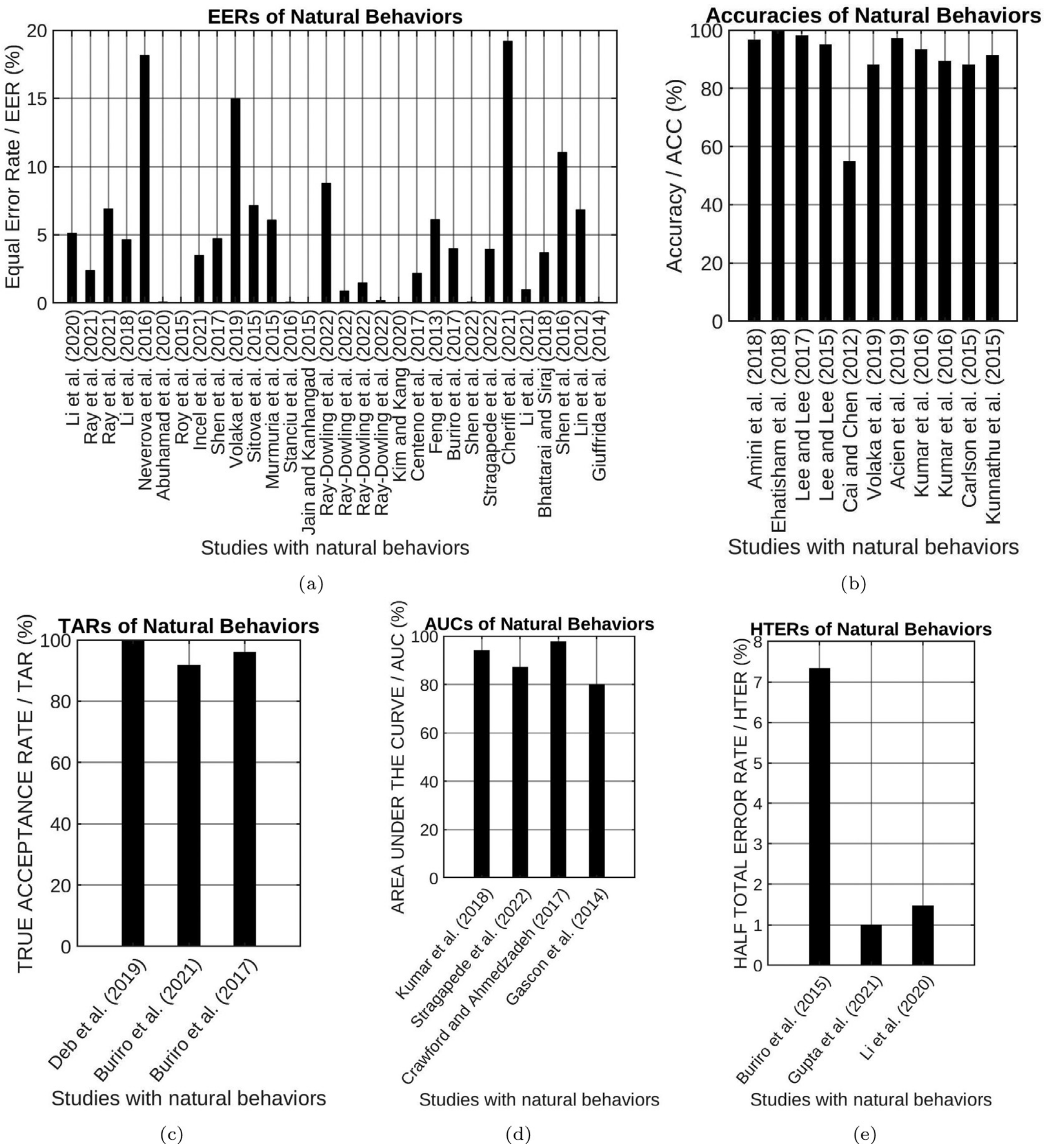
In real-life experience, user authentication should primarily depend on natural behaviors since those are easily available through user inputs. However, as a security mechanism, there can be designed behaviors incorporated in the real-life implementation of user authentication on mobiles, e.g. pattern tracing of geometrical shapes for unlocking interfaces. The authentication performances across studies utilizing natural and designed behaviors are observed to be acceptable. However, the difference between the natural and designed behaviors strongly exists due to their variations in nature and the reaching of user stability (Carroll and Rosson, 1987) as explained by cognitive psychology. From a classifier's capability, for either natural or designed, the training and testing samples belong to the same group (either natural or designed), which makes the performances more than acceptable in both cases. Attaining faster stability among users while performing natural than designed behaviors hypothesizes better authentication performance of natural behaviors. But the classifiers are observed to overcome the noise or haphazardness due to unfamiliarity among users to perform designed behaviors which explains the comparable performances of both natural and designed.

Therefore, we need to acknowledge the difference in nature between natural and designed behaviors and the differences as explained by cognitive science which will be helpful before real-life deployment of user authentication utilizing any behavior type. Alongside, we need to understand a classifier's capability to overcome haphazard traits in designed behaviors and therefore perform equivalent to natural. This further ensures that the future real-life implementation of user authentication can depend both on natural and designed behaviors. However, it is expected to rely more on natural, as is the trend, due to its large availability and usage familiarity among mobile consumers.

4.4. Additional attributes/aspects of behaviors

In addition to the user behavior categorization, we also characterize each behavior from the reviewed studies under the following attributes/aspects:

- *Attribute 1:* walking versus non-walking
- *Attribute 2:* tasks



(a)

(b)

(c)

(d)

(e)

Fig. 11. Performances across studies utilizing natural behaviors: (a) Equal Error Rate (EER); (b) Accuracy; (c) True Acceptance Rate (TAR); (d) Area Under the Curve (AUC); and (e) Half Total Error Rate (HTER).

- *Attribute 3:* hand actions

There are studies (Belman et al., 2019; Ehatisham-ul Haq et al., 2018; Kumar et al., 2018; Sitová et al., 2015) that involve a wide range of postures with the handheld phone to create special datasets with multiple modalities. In other cases, researchers hand over the data collection device/phone to volunteers for several days to log multi-modality data while users perform routine activities. Such behaviors hold the first attribute of walking versus non-walking-based tasks to create special datasets. On the other hand, there are studies (Okumura et al., 2006; Ray et al., 2021; Stragapede et al., 2022a) that collect data through assigning tasks to users, such as browsing, form filling, waving, and phone pickup, among others. Therefore, they are assigned to the second attribute. Lastly, typing, swiping, tapping, and hand motion, among others (Frank et al., 2012; Gupta et al., 2022; Ray et al., 2021; Stragapede et al., 2022a) are fine-grained characteristics of the tasks attribute and form the third attribute of hand actions. The taxonomy of surveys in Fig. 1 lists the attributes projected in addition to the behavior categorization into natural versus designed. These attributes will be assigned to the behaviors of each reviewed study in Section 5.

5. Survey of stationary mobile behavioral biometrics

Our survey groups studies in stationary mobile behavioral biometrics into three categories. We highlight each reviewed study along the following dimensions - the datasets used, number of data providers, user behavior, duration of device usage, modalities, sampling rate of motion events, algorithms evaluated, fusion type, and performance measurement.

Our survey focuses on studies that involve motion events. Based on the number of motion event modalities and whether fusion is involved, three categories of stationary mobile behavior are defined as follows:

1. presence of at least two motion sensors but without fusion with non-motion sporadic modalities
2. at least two motion events fused with non-motion sporadic modalities

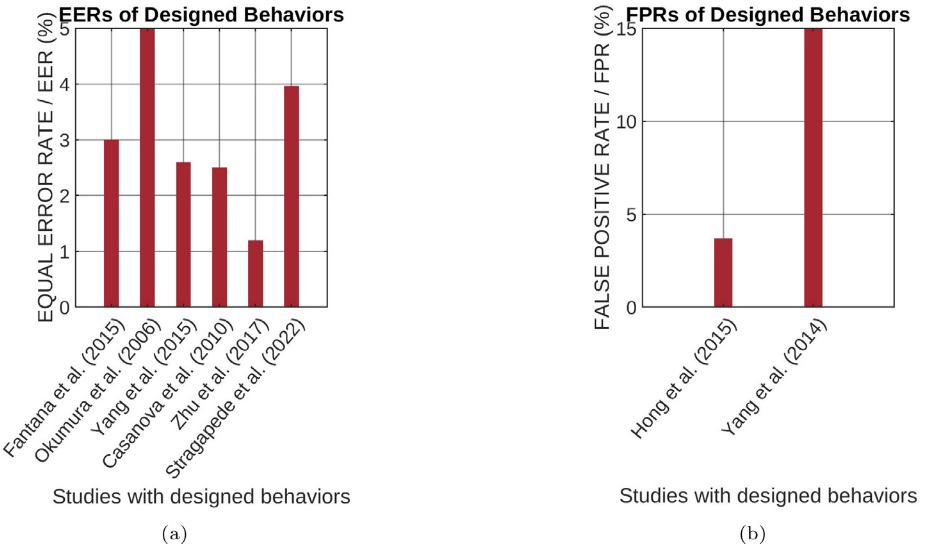


Fig. 12. Performances across studies utilizing designed behaviors: (a) Equal Error Rate (EER) and (b) False Positive Rate (FPR).

3. only one motion event which may or may not be fused non-motion sporadic modalities

The above grouping is motivated by observed advantages and disadvantages unique to each of the studies. We list them along with the performance trend of each group which will help readers to observe each category as a whole and understand their distinctiveness from one another.

The first group of works includes studies that involve measuring motion through two or more motion sensor modalities (acceleration, gyroscope, magnetometer, and rotation) only. No other non-motion modalities data are included. These studies focus solely on the measurement of phone's motion about the reference frame of inertia due to the user's behavior/activity on the device. The other sporadic modalities (keypress, touch, location, and gravity) are considered stronger compared to the motion sensor modalities. Thus, excluding them makes the first group of studies more challenging than the others. However, there are studies that involve activities like typing, swiping, and touch events but these sporadic sensor data are not utilized for authentication under this category. In these cases, users are authenticated through the motion events logged while a user is performing such activities of typing, swiping, and others.

Advantages:

- Systems falling under this group do not have to depend on the occasional presence of sporadic modalities.
- The motion events are always available whenever the phone is in use which serves the core purpose of continuous authentication.

Disadvantages:

- System's authentication depends on at least two motion events where each may have a very high sampling rate (Buriro et al., 2015; Zhu et al., 2017). This has the potential to challenge the mobile's battery consumption.
- Systems processing such highly sampled data may pose challenges to the computational cost.

Performance and Overall Trends:

- In this study we identify the use of two algorithms in most cases which are SVM and neural networks (Table 1) which justifies handling the higher sampled data or the same with more feature dimensions.
- We find a few studies with high performances even with smaller sampling rates (Feng et al., 2013; Ehatisham-ul Haq et al., 2018; Kumar et al., 2018; Ray et al., 2021). However, our research community is encouraged to perform benchmarking for further assurance.

The second group of studies includes works that involve experiments with two or more motion sensor modalities fused or combined with other sporadic non-motion sensor modalities. The sporadic modalities usually log the user behaviors like typing, swiping, zooming in/out, and others in an input format. These are sporadic because their logging depends on human behavior. One cannot expect the behavior of typing or swiping to occur constantly. These are comparatively stronger modalities than the motion sensor modalities. The fusion/combination of these sporadic modalities (when available) with motion sensor modalities strengthens the authentication performance.

Advantages:

- Motion events occur simultaneously with stronger sporadic events which enhance performances as demonstrated in Sitová et al. (2015), Deb et al. (2019), Incel et al. (2021).
- Due to occasional occurrences the sampling rates of the motion events will be under control to not challenge the battery consumption and computational cost.

Disadvantages:

- System's performance depending on the sporadic modalities fails to serve the purpose of continuous authentication.
- Cases, where the system's algorithm is not competent enough, will fail to produce satisfactory performance with multiple modalities.

Performance and Overall Trends:

- We observe the usage of a wide range of algorithms.
- Here we observe a range of performances with low satisfactory results as in Cherifi et al. (2021), Gascon et al. (2014) to high performances as in Abuhamad et al. (2020a), Roy et al. (2015), Incel et al. (2021) among others. Further benchmarking will ensure the performance range of fusion of motion events with other sporadic modalities.

The third group of studies involves works that measure user behavior through only one motion event (Kim and Kang, 2020; Kumar et al., 2016b; Yang et al., 2014). The single motion event may

Table 1
Comparative literature review: Fusion of at least two motion events for measuring stationary behaviors on mobile. Abbreviations - ACC: Accuracy, AB: AdaBoost, AUC:Area Under the Curve, BN:Bayes Network, DT: Decision Trees, DTW: Dynamic Time Warping, EE: Elliptic Envelope, EER: Equal Error Rate, FAR: False Acceptance Rate, FRR: False Rejection Rate, GCU: Glasgow Caledonian University dataset, GBC: Gradient Boosting Classifier, HTER: Half Total Error Rate, HMOG:Hand Movement, Orientation, and Grasp, IF: Isolation Forest, kNN: k Nearest Neighbor, KRR: Kernel Ridge Regression, LDA: Linear Discriminant Analysis, LinReg: Linear Regression, LOF: Local Outliers Factor, LReg: Logistic Regression, LSTM: Long Short-Term Memory, MLP: Multilayer Perceptron, NB: Naive Bayes, PABG: Phone Acceleration-based Gait Biometric, RF: Random Forest, RNN: Recurrent Neural Network, StatM: Statistic Method, SVDD: Support Vector Data Description, SVM: Support Vector Machine, SPMP: Swiping and Phone Movement Patterns, TRM: Trajectory Reconstruction Method, WABG: (Smart)watch Acceleration-based Gait, WRBG: (Smart)watch Rotation-based Gait.

Study & Dataset	#User	Behavior	Duration	Modality	Sampling (Hz)	Algorithm	Fusion	Best performance
Li et al. (2020a), own, Brain-Run (Papamichail et al., 2019)	100, 82	read, write, navigate; game playing	24 Sess. (~60 hr), -	Accel, Gyro	100, 10	SVM	sensor (data)	5.14%, EER
Kumar et al. (2018), PABG (Kumar et al., 2015), WABG (Kumar et al., 2016a), WRBG (Kumar et al., 2016a), SPMP (Kumar et al., 2016b)	18, 40, 28	typing in sitting, gait	-	Accel, Gyro	46, 25, -	SVM, LOF, IF, EE, AB, NB, kNN, LDA, LReg, MLP, RF	score, decision	94.22%, AUC
Ray et al. (2021), own	49	Form filling in siting, typing prescribed texts, motion during fingerprint scanning, pattern tracing through guided behavior	2 Sess. (intra, inter)	Accel, Gyro	2	SVM	score (weighted, LR)	2.4%, EER (intra); 6.9%, EER (inter)
Li et al. (2018), own	100	read, write, navigate	6 hr	Accel,Gyro	100	SVM	feature	4.66%,EER
Amini et al. (2018), own	47	browsing shopping app in sitting	10-13 min	Accel, Gyro	100	LSTM, SVM, RF, LReg, GBC	sensor	96.7%, ACC
Ehatisham-ul Haq et al. (2018), own	10	walking, sitting, standing, running, walking up and down stairs placing phone in different locations of user's body	90 min	Accel, Gyro, Magneto	50	SVM, DT, kNN	feature	100%, ACC
Lee and Lee (2017), own	35	routine usage	2 weeks	Accel, Gyro	50	KRR, SVM, LinReg, NB	feature	98.1%, ACC
Fantana et al. (2015), own	-	hand waving/arm sweeping holding phone	5 Sess.	Accel, Gyro	200	DTW	-	0.02% FAR, 10% FRR, 3% EER
Lee and Lee (2015), own, GCU (Kayacik et al., 2014)	4, 4	routine usage	5 days, 3 weeks	Accel, Rotate, Magneto	5, -	SVM	sensor	95%, ACC
Zhu et al. (2017), own	20	phone shaking around elbow in sitting and standing	2 Sess.	Accel, Gyro	200	SVM	sensor	1.2%, EER
Feng et al. (2013), own	31	phone pick up	3 Sess.	Accel, Gyro, Magneto	25	StatM, TRM	feature	6.13%, EER
Neverova et al. (2016), own	1500	routine usage	several days	Accel, Gyro	-	RNN	feature	18.17%, EER
Carlson et al. (2015), own	10	phone pickup	1 Sess.	Accel, Gyro	68.7	MLP	feature	88%, ACC
Buriro et al. (2015), own	26	phone pickup	1 Sess.	Accel, Gyro, Rotate	150, 190, -	BN, RF, SVM	score	7.33%, HTER
Kunnathu (2015), own	7	phone pickup	1 Sess.	Accel, Gyro	25	MLP	feature	91.43%, ACC
Kratz et al. (2013), own	15	hand waving/arm sweeping holding phone	1 Sess.	Accel, Gyro	80	Protractor3D, DTW, LReg	feature	95%, F1 score
Yang et al. (2015), own	30	hand gestures wearing smartwatch	2 Sess.	Accel, Gyro	100	DTW, histogram	feature	2.6%, EER
Li et al. (2020b), own	50	read, write, navigate	24 Sess	Accel, Gyro, Magneto	100	SVDD	feature	1.47%, HTER
Li et al. (2021), own	100	read, write, navigate	24 Sess.	Accel, Gyro	100	SVM (OCC)	feature	1%, EER
Bhattarai and Siraj (2018), HMOG (Sitová et al., 2015)	100	read, write, navigate	24 Sess.	Accel, Gyro	100	SVM (OCC), fuzzy SVM (OCC)	feature	3.7%, EER

or may not be fused with other sporadic modalities. For example, the study by Kumar et al. (2016b) has acceleration as the only motion sensor modality and two sporadic modalities - keypress and swipe. This work is based on authenticating users while they perform the two most common activities which are typing and swiping during which the phone motion gets captured through acceleration. The common single motion sensor modality is acceleration which is used by most of the studies under this group. Among all the motion sensors, acceleration is considered to be the most useful modality as it includes inertial force (force which is caused due to the momentum of the mass/phone). The only reason for which the phone's mass is subjected to momentum is the user activity on the device and therefore it becomes an important motion sensor modality. However, considering only one motion sensor modality for authentication can be challenging.

Advantages:

- Due to the presence of only one motion modality the battery consumption and computational cost are not potential concerns.

Disadvantages:

- Due to the presence of only one single modality system reliability can be challenging.

Performance and Overall Trends:

- We observe the utilization of a wide variety of algorithms even in this small group of studies.
- In most cases the performances are satisfactory (Centeno et al., 2017; Crawford and Ahmadzadeh, 2017; Kim and Kang, 2020; Kumar et al., 2016b; Laghari et al., 2016). Future benchmarking is required to be conclusive.

5.1. *Fusion of two or more motion modalities*

Table 1 lists the state of the art under this category.

In the study by Li et al. (2020a) two motion events (acceleration and gyroscope) are logged with the goal of capturing arm movement and fine-grained motion. Two datasets are utilized in this study, of which their own collected dataset consists of 100 users who perform reading, writing, and map navigation activities over 24 sessions. There is the use of the BrainRun (Papamichail et al., 2019) public dataset as the second dataset from which 82 random users' data is utilized for evaluation. The users in the public dataset perform a game-playing activity that can be classified under the natural behavioral trait. The user activities from their own and public datasets belong to the subset of routine phone usage and context limited respectively under natural behaviors. Based on such categorization, the user behavior of routine usage and gaming possess the attribute of walking versus non-walking-based tasks to create special datasets and tasks respectively (See Fig. 1). The platform, Scanet, evaluates the logged data which consists of two-stream CNN (Convolutional Neural Network) as feature extractors so that both time and frequency domain features are learned. Thereafter, PCA (Principal Component Analysis) is utilized to select the top 25 features with high discriminability after which classification is performed utilizing a one-class SVM (Support Vector Machine). During training the SVM, they perform 10-fold cross-validation. Investigating the combination of acceleration and gyroscope using one-class SVM, they achieve an average EER (Equal Error Rate) of 5.14% on their own and the BrainRun dataset.

Kumar et al. (2018) compare the performances of several one-class classifiers (OCC) with binary classifiers (BC) utilizing four small datasets (number of users in each set < 50). However, the user activity of the four datasets involves both non-gait and gait-based activities under natural behavior (web browsing, typing, swiping, walking, and walking while wearing a wristwatch as a wearable sensor device). The user behaviors of the four datasets include walking back and forth for 200 m with a phone in trouser pocket (PABG dataset Kumar et al., 2015), wearing a smartwatch and walking (WABG and WRBG datasets Kumar et al., 2016a), and browsing (SPMP dataset Kumar et al., 2016b). These are natural behaviors where the first two possess the attribute of walking versus non-walking-based tasks to create special datasets and the third behavior of browsing possesses the attribute of tasks. Acceleration and/or gyroscope are the motion events that are utilized across all four datasets to log user behaviors. Among experiments performed on individual OCC, BC, and fusion of multiple OCCs, the kNN (k-Nearest Neighbor) BC produces the best result of 94.22% Area Under the Curve (AUC).

In Ray et al. (2021), utilizing acceleration and gyroscope, continuous authentication is performed on mobile devices collecting a dataset of 49 seated users. The user behavior includes an Android registration form filling which is categorized under natural behavior type given it is a real-life scenario or a common practice of mobile users to sit and fill out online registration forms to open an account or a portal for utilizing banking, e-commerce, and other online services. The form filling in sitting behavior is projected into tasks attribute. The data collection also includes typing a prescribed text (a designed behavior with the attribute of hand actions), followed by capturing motion events when users are using the phone's fingerprint scanner (a natural behavior with the tasks attribute), and then tracing geometrical patterns through guided outline (a designed behavior projected into tasks attribute). Fusing the two modalities at weighted score level and likelihood ratio-based score level, the best EERs of 2.4% and 6.9% are achieved for intra- and inter-session experiments respectively. Between the two score fusion techniques, the likelihood ratio-based score fusion performs the best in both intra-session and inter-session (with the effect of concept drift) experiments.

Another study by Li et al. (2018) with 100 users' data utilizes only acceleration and gyroscope to capture the fine-grained motion of users' hand movements. Users perform routine phone usage as a natural behavior for around 6 h. The routine usage behavior possesses the attribute of walking versus non-walking-based tasks to create special datasets. The authentication platform, SensorAuth, consists of a feature extraction module that extracts both the time domain (mean, median, standard deviation, maximum, minimum, range, kurtosis, skewness, 25%, 50%, and 75% quantiles) and frequency domain (energy, entropy, peak1, peak2f, and peak2) features. The raw data in this study undergo data augmentation to prevent overfitting and improve the classifier's generalizability. Utilizing the SVM classifier, they obtain the best EER of 4.66%.

In the study by Amini et al. (2018) a Deep Learning-based re-authentication platform, DeepAuth, is utilized through RNN (LSTM) models. The data is collected from 47 volunteers using accelerometer and gyroscope sensors. The user behavior includes sitting and browsing the Target shopping app for 10–13 min while another app logs the sensor data running in the background. It is a context limited natural behavior as in real-life scenarios it is a common task for mobile users. The user behavior of browsing is projected into tasks attribute as shown in Fig. 1. The platform architecture is to re-authenticate genuine users but lock out impostors unless they can pass other security mechanisms like providing passwords. The data is first pre-processed by downsampling from 100 Hz to 50 Hz. Then it is windowed or segmented with window sizes of 20, 40, 100, 200, and 500. It is observed that the window size of 100 performs the best. The time domain features of the sensors are converted to the frequency domain using Fast Fourier Transform. Data is split into training-validation-testing sets in percentages of 70%-15%-15%. In the next stage, the data is passed to the LSTM (Long Short-Term Memory) network which outputs a series of feature vectors. The very last output is fed to a fully connected output layer and then to a sigmoid activation function from which the positive/negative result is obtained. The LSTM produces the best result of 96.7% accuracy based on 20 s of data.

Ehatisham-ul Haq et al. (2018) perform six user behaviors, namely walking, sitting, standing, running, walking upstairs, and walking downstairs for a duration of 90 min when the sensor device is kept in 5 locations of a user's body (left, right jeans pocket, waist, upper arm, and wrist). These user behaviors are natural behaviors under the subset of postures with phone. The user behaviors are projected into the attribute of walking versus non-walking-based tasks to create special datasets. The classifiers utilized for the user authentication are SVM, Decision Trees, and kNN (k-Nearest Neighbors) of which SVM performs the best. They authenticate users through acceleration, gyroscope, and magnetometer sensors achieving 100% accuracy from walking and running behaviors.

The work by Lee and Lee (2017) focuses on unobtrusive user authentication. The authentication system SmarterYou combines users' information recorded in the smartphone and wearable device. The work also includes the calculation of energy consumption of the device as the system needs to be continuously retrained. The authors assume that each smartwatch is associated with one owner who does not share their smartphone or smartwatch and that the communication between the two devices is secure. The smartwatch monitors the user's raw sensor data and sends this information to the smartphone via Bluetooth. The sampling rate for collecting the data from both devices is 50 Hz. The authors choose accelerometer and gyroscope sensor data because the accelerometer records motion patterns and the gyroscope records fine-grained motions of users such as how one holds a smartphone. They have segmented the raw data into sliding windows. The features derived from the two modalities are mean, variance, maximum, minimum, range, peak, peakf, peak2, and peak2f of the sensor stream. Accelerometer and gyroscope data from both devices are fused at the feature level. It is observed that the data from the smartwatch fused with the phone's data enhances the performance. Users perform four routine behaviors- using smartphone while standing or sitting, while moving, while it is stationary on the table, and in a moving vehicle. All of these are of the natural behavior type. These routine phone usage behaviors possess the attribute of walking versus non-walking-based tasks to create special datasets. They have classified the data using Kernel Ridge Regression (KRR), SVM, Linear Regression, and Naive Bayes. Out of these, KRR performs the best with an accuracy of 98.1%.

The study by Lee and Lee (2015) involves their own dataset and the GCU (Glasgow Caladonian University) dataset (Kayacik et al., 2014). The users in their dataset perform routine phone usage (natural behavior) for several days, which is captured using three motion sensors - accelerometer, magnetometer, and rotation (orientation). The user behavior is projected into the attribute of walking versus non-walking-based tasks to create special datasets. They utilize 10-fold cross-validation during classification. Fusing the data at sensor level and utilizing SVM as the classifier they obtain the best result of 95% accuracy.

The study by Neverova et al. (2016) is performed on a large dataset of 1500 users. Users perform routine phone usage for several months which is a natural behavior. The user behavior is projected into the attribute of walking versus non-walking-based tasks to create special datasets. Both acceleration and gyroscope data are used for authentication. RNN-based deep neural network is used in this study. They propose a Dense Convolutional Clockwork RNN model. They pre-process the data by normalizing and making a 14-tuple data vector (accel x, accel y, accel z, accel magnitude, gyro x, gyro y, gyro z, gyro magnitude, angles made by accel and gyro in the phone's coordinate system per axis). They perform authentication experiments with their proposed RNN-based network and other neural networks. Data from all 1500 users is collected using 587 phones. Data from 150 phones are used for validation and another 150 phones are used for testing. An EER of 18.17% is obtained as the best.

In the study by Fantana et al. (2015), a designed behavior of hand waving holding a phone is performed across five sessions. The user behavior possesses the tasks attribute as shown in Fig. 1. Two modalities namely, acceleration and gyroscope are utilized to log the user behavior. Each movement/gesture is recorded for 3 s and is referred to as a snippet. To test the reliability of the authentication method they perform another designed behavioral task to create an attack scenario. They utilize genuine user's video-recorded attempts to reproduce the movement by skilled forgers. The recorded video is shown to the forgers and they are asked to repeat the movement to the best of their ability. Both zero-effort and skilled forgeries are performed. In the data processing stage, the 3-second data per movement is reduced to 500 ms data where the actual gesture is present. Several experiments are performed to evaluate authentication performance utilizing DTW (Dynamic Time Warping) classifier. The best performance obtained in this study is an EER of 3%.

The study by Carlson et al. (2015) involves a special behavior of taking out a phone from pocket to ear, holding it to ear, and putting it back to the pocket. This is a natural behavior because in real life this activity is common in practice. The behavior falls under the attribute of tasks as shown in Fig. 1. The number of participants involved in this study is 10 from different age groups. Each user repeats the behavioral pattern for 5 times. Both accelerometer and gyroscope motion events are utilized to log users' hand movements. Utilizing MLP (Multi-Layer Perceptron) as the classifier, they observe the best performance of 88% accuracy.

A similar study by Kunnathu (2015) utilizes their own dataset of 7 users. Here also the same natural behavioral patterns (falling under the attribute of tasks) of taking out a phone from pocket to ear, holding it to ear, and putting it back in pocket are performed during data collection. Both accelerometer and gyroscope motion events are utilized to log users' hand movements. Utilizing MLP as the classifier, they obtain a CCI (Correctly Classified Instances or Accuracy) of 91.43%.

In another similar study by Buriro et al. (2015) users perform the behavior of slide swiping while unlocking a phone, then put the phone to ear, and speak over the phone while sitting and walking. It is classified under natural behavior with the attribute of tasks. Acceleration, gyroscope, and rotation are logged when users put the phone to their ears after unlocking. They achieve a Half Total Error Rate (HTER) of 7.33% as the best using Bayesian Network among other classifiers.

Feng et al. (2013) is a similar work that involves the natural behavior of phone pick-up through accelerometer, gyroscope, and magnetometer modalities. This work achieves an EER of 6.13% as the best performance.

The work by Kratz et al. (2013) involves the user behavior of arm sweep action holding the device in hand. The sweep actions or gestures include left to right, circular, left to right arc, infinity, triangle, and rotation which are designed behaviors. The user behavior also possesses the tasks attribute. The modalities that log the user's arm sweeps are acceleration and gyroscope. The classifiers used in this study are Protractor3D, DTW and Logistic Regression. They observe the best performance of 95% F1 score.

The work by Yang et al. (2015) involves the behavior of hand waving while wearing a smartwatch. This is a designed behavior since the wave motions are random. It has the attribute of tasks. The gesture is logged through acceleration and gyroscope motion event modalities. They achieve an EER of 2.6% as their best performance.

The work by Zhu et al. (2017) involves a designed user behavior of phone shaking around the elbow in sitting and standing. Such designed user behavior is projected into the attribute of tasks. Shake refers to a to-and-fro movement with one hand holding a smartphone and swinging the x- and y-axis coordinate plane of the phone around the elbow in the air. The authors divide continuous shakes into segments and extract two behavioral patterns of motion velocity and angular speed and one physiological pattern of shaking radius based on shaking segments. The user's phone shaking gesture is logged using accelerometer and gyroscope. Utilizing SVM as the classifier they achieve the best performance of 1.2% EER.

The study by Li et al. (2020b) implements a sensor-based continuous mobile authentication system, FusionAuth where acceleration, gyroscope, and magnetometer motion sensors are utilized. They utilize data from 50 users who participated in 24 sessions performing the natural behavior of read, write, and map navigate. Such behavior possesses the attribute of walking versus non-walking-based tasks to create special datasets. The raw sensor data is segmented into time windows from which statistical and frequency features are extracted. The work extracts 11 statistical features (mean, median, maximum, minimum, standard deviation, range, 25%, 50%, and 75% quartiles, kurtosis, and skewness) and 5 frequency features (energy, entropy, HP1, FHP2, and HP2). HP1 is the amplitude of the first highest peak in one-axis reading in a time window, FHP2 is the frequency of the second highest peak, and HP2 is the amplitude of the second highest peak. Therefore, 144 features (3 sensors*3 axes*16 features) are extracted. They perform both serial and parallel feature level fusion where the feature dimension of a sample is 144 and 48 respectively. They utilize the Conditional Mutual Information Maximization (CMIM) method for feature selection per user. Utilizing one-class Support Vector Domain Description (SVDD) classifiers, they obtain the mean HTERs of 1.47% and 1.79% with serial and parallel feature fusion respectively.

The study by Li et al. (2021) proposes DeFFusion (Deep Feature Fusion) CNN-based continuous authentication system. They collect a dataset of 100 users who perform read, write, and map navigation for 24 sessions which is a natural behavior under the subset of routine usage. It possesses the attribute of walking versus non-walking-based tasks to create special datasets. The motion event modalities utilized are acceleration and gyroscope that are fused at feature level. From each acceleration and gyroscope, they process time and frequency domain data and feed it to CNN to extract CNN-based features. Then feature selection happens using factor analysis. These resultant fused feature vectors are input to the one-class SVM classifier for authentication. The CNN architecture utilizes multi-stream feature extraction and spatial downsampling followed by two fully connected layers. The best result of 1% median EER is obtained with a time window size of 5 s. To observe the effectiveness of CNN-based features they compare the performance of the DeFFusion architecture to statistical features extracted from the data (mean, standard deviation, maximum, minimum, range, kurtosis, skewness, 25%, 50%, 75% quartiles, energy, entropy, P1 (amplitude of the first highest peak of one-axis readings), P2F (frequency of the second highest peak of one-axis readings), and P2 (amplitude of the second highest peak of one-axis readings)) and input to traditional machine learning algorithms, namely, one-class SVM, kNN, random forest, and decision trees. In such comparison also DeFfusion performed the best with an EER of 1%.

Bhattarai and Siraj (2018) utilize the acceleration and gyroscope data from HMOG dataset (Sitová et al., 2015). They extract HMOG resistance features on acceleration and gyroscope and perform feature selections utilizing filter-based and wrapper-based methods. The data is fused at feature level. They split the data into training and testing in the ratio of 80:20. They utilize both one-class SVM and one-class fuzzy SVM (membership values between 0 and 1 are assigned to each sample to denote the degree of belongingness to the class). The best EER of 3.7% is obtained utilizing fuzzy OCC-SVM utilizing the HMOG sitting data.

5.2. Fusion of two or more motion event modalities with other sporadic modalities

Table 2 lists the state of the art under this category.

Abuhamad et al. (2020a) evaluate their authentication platform AUToSen on their own dataset of 84 volunteers. The data is logged through motion sensors accelerometer, gyroscope, and magnetometer which are fused with the elevation sensor which is a non-motion sensor modality. They also log other sporadic modalities like touch and tap data from the touch sensor. Users perform routine phone usage for five days which is a natural behavior. Such user behavior can be projected into the attribute of walking versus non-walking-based tasks to create special datasets. They utilize LSTM models for classification. They perform four groups of experiments, namely, 5-sensor data (touch, acceleration, gyroscope, magnetometer, and elevation); 4-sensor data (acceleration, gyroscope, magnetometer, and elevation); 3-sensor data (acceleration, gyroscope, and magnetometer); and 2-sensor data (acceleration and gyroscope). Combining the modalities at sensor (data) level, they achieve the best performance of 0.09% EER with the 3-sensor modality set up.

Roy et al. (2015) implement an HMM (Hidden Markov Model)-based multi-sensor system, which is evaluated on their own dataset of 42 volunteers. The user activities include routine usage of reading Wikipedia articles and filling out a questionnaire which are natural behaviors. The user behaviors possess the attribute of walking versus non-walking tasks to create special datasets. Through these user tasks, they log modalities like swipe, tap, acceleration, and gyroscope. Here acceleration and gyroscope are the motion event modalities whereas swipe and tap are the sporadic touch modalities. Utilizing a single swipe observation and its corresponding motion events, they achieve an EER of 13.29% which improves to 0% when 19 consecutive swipes (and the simultaneous motion events) are combined. A similar pattern is observed in the case of taps where the EER improves from 16.55% to 1% when 17 consecutive taps are consolidated.

Incel et al. (2021) investigate authentication performance over 15 sessions when 45 users interact with smartphones in hand (browsing banking apps) while sitting and standing and in sitting when the device is on the table. Such user behavior is a natural behavior under context limited subset. The behavior of browsing during data collection projects itself into the tasks attribute as shown in Fig. 1. They utilize acceleration, gyroscope, and magnetometer as motion event modalities and scroll event as a sporadic non-motion modality. Utilizing binary classifier they achieve the best performance of 3.5% EER.

The work by Shen et al. (2017) involves their own dataset collected from 102 users. The motion events used to authenticate a user are acceleration, rotation/orientation, gyroscope, and magnetometer. The volunteers in this study have input touch gestures on the smartphone during which the motion sensor data are collected. The authors observe that more than 98% of touch interaction comprises touch-tapping and single-touch sliding actions and hypothesize that different users would generate different levels of posture and motion which exhibits uniqueness among users. The users in this study have undergone three behavioral scenarios for contributing data which are- hand-hold (holding smartphones and performing touch actions while sitting and standing), table-hold (smartphones are placed on a desktop and subjects perform touch actions using a single hand), and hand-hold walk (subjects hold

Table 2

Comparative literature review: Fusion of at least two motion events with other sporadic modalities captured during stationary behaviors on mobiles. Abbreviations - ACC: Accuracy, AUC: Area Under the Curve, BN:Bayes Network, BB-MAS:Behavioural Biometrics Multi-device and multi-Activity data from Same users, DT: Decision Trees, DeSVDD: Deep Support Vector Data Description, DTW: Dynamic Time Warping, EL: Ensemble Learning, EER: Equal Error Rate, ED: Euclidean Distance, END: Euclidean Normed Distance, FAR: False Acceptance Rate, HTER: Half Total Error Rate, HMOG:Hand Movement, Orientation, and Grasp, HMM: Hidden Markov Model, HuMIdb: Human Mobile Interaction database, IF: Isolation Forest, kNN: k Nearest Neighbor, LOF: Local Outliers Factor, LSTM: Long Short-Term Memory, ManD: Manhattan Distance, ManSD: Manhattan Scaled Distance, MCD: Minimum Covariance Determinant, MHD: Modified Hausdorff Distance, MLP: Multilayer Perceptron, NB: Naive Bayes, NN: Neural Network, RF: Random Forest, SE: Scaled Euclidean, SM: Scaled Manhattan, SOM: Self Organizing Maps, SVM: Support Vector Machine, TCM: Transductive Classification Machine, TAR: True Acceptance Rate, UMDAA-02: University of Maryland Active Authentication Dataset 02.

Study & Dataset	#User	Behavior	Duration	Modality	Sampling (Hz)	Algorithm	Fusion	Best performance
Abuhamad et al. (2020a), own	84	routine usage	5 days	Accel, Gyro, Magneto, Elevation, Touch	64	LSTM	sensor (data)	0.09%,EER
Roy et al. (2015), own	42	routine usage	1 Sess.	Accel, Gyro, Swipe, Tap	-	HMM	feature	0%, EER
Shen et al. (2017), own	102	routine usage	3 rounds	Accel, Gyro, Magneto, Rotate, Touch	-	HMM, SVM, NN	feature	4.74%, EER
Incel et al. (2021), own	45	browsing banking app in sitting and standing	15 Sess. (22.5 min)	Accel, Gyro, Magneto, Scroll	100	SVM, kNN, MLP, DT, RF, NB, EL	Feature	3.5%, EER
Deb et al. (2019), own	37	routine usage	15 days	Accel, Linear Accel, Gyro, Magneto, Rotate, Key, GPS, Gravity	1	LSTM	score	99.98%, TAR at 0.1% FAR
Stragapede et al. (2022a), BehavePassDB (own)	81	pattern unlock, texting, reading, gallery swiping, signature, critical app, phone pickup, tapping in predetermined locations	4 Sess.	Accel, Linear Accel, Gyro, Magneto, Gravity, Key, Tap, Swipe, GPS, temp, proximity, light, humidity, pressure, WiFi, BT, battery	200	LSTM	score	87.2% AUC
Gascon et al. (2014), own	315	typing prescribed texts	1 Sess.	Accel, Gyro, Rotate, Key	-	SVM	feature	80%, AUC
Cai and Chen (2012), own	21	typing PINs	-	Accel, Gyro, Key	-	SVM, DTW	-	55%, ACC
Papamichail et al. (2019), BrainRun (own)	2218	game playing	-	Accel, Gyro, Magneto, Swipe, Tap	10	-	-	-
Volaka et al. (2019), HMOG (Sitová et al., 2015)	100	read, write, navigate	24 Sess. (~60 hr)	Accel, Gyro, Swipe	100	LSTM	Feature	15%, EER
Belman et al. (2019), BB-MAS (own)	117	multiple activities	1 Sess. (1.8 hr)	Accel, Gyro, Swipe, Key, Mouse	100	-	-	-
Sitová et al. (2015), HMOG (own)	100	read, write, navigate	24 Sess. (~60 hr)	Accel, Gyro, Magneto, Swipe, Tap, Key, Pinch	100	SM, SE, SVM	score	7.16%, EER
Murmuria et al. (2015), own	73	browsing Google chrome and Facebook	2 Sess. (each 45 min)	Accel, Gyro, Touch, Key, Zoom, Pinch, Power	-	TCM	feature	6.1%, EER
Stanciu et al. (2016), own	20	typing passwords	1 Sess.	Accel, Gyro, Key	17	kNN, ED, ManD	feature	0.08%, EER
Nohara and Uda (2016), own	-	flicking to unlock phone	1 Sess.	Accel, Gyro, Flick	-	SOM	feature	-
Jain and Kanhangad (2015), own, own	104, 30	swiping	1 Sess.	Accel, Rotate, Swipe, Tap, Zoom	-	DTW, MHD	score	0.03%, EER
Acien et al. (2019), UMDAA-02 (Mahbub et al., 2016)	48	WiFi, GPS, and app usages	10 days	Accel, Gyro, Touch, Key, Wifi, GPS, app use	-	SVM	score	97.1%, ACC
Buriro et al. (2017), own	31	micro-hand movements through routine usage for 10 sec when notified with broadcast event	1 Sess.	Accel, Gyro, Magneto, Gravity, HPF, LPF	5	BN, MLP, NN, RF	feature	4% EER, 96% TAR
Gupta et al. (2022), own	41	micro-hand movements through routine usage for 5 sec when notified with broadcast event	1 Sess.	Accel, Gyro, Magneto, Gravity, HPF, LPF	1000	IF, SVM, LOF, MCD	decision, feature	1%, HTER
Buriro et al. (2021), own	95	typing passwords in sitting, standing, and walking	3 Sess.	Accel, Gyro, Rotate, Magneto, Gravity, Key	-	NB, NN, RF	feature	91.79% TAR, 0.04% FAR
Ray-Dowling et al. (2022), HMOG (Sitová et al., 2015), BB-MAS (Belman et al., 2019)	100, 115	typing in sitting	4 Sess., 25 min	Accel, Gyro, Swipe	100, 100	SVM (OCC, BC)	score (LR Nandakumar et al. (2007))	0.2%, EER
Basar et al. (2019), own	15	browsing banking app	multiple days	Accel, Gyro, Magneto, Touch	5, 25, 100	-	-	-
Stragapede et al. (2022b), HuMIdb (Acien et al., 2020)	600	typing prescribed text, swipe, drawing the number 8, tap	5 Sess.	Accel, Gyro, Magneto, Touch	50	LSTM-RNN	score	3.96%, EER

(*continued on next page*)

Table 2 (*continued*)

Study & Dataset	#User	Behavior	Duration	Modality	Sampling (Hz)	Algorithm	Fusion	Best performance
Shen et al. (2022), own, HMOG (Sitová et al., 2015)	100, 100	routine phone usage; read, write, navigate	63 days, 24 Sess.	Accel, Gyro, Magneto, Rotate, Touch	-, 100	DeSVDD	decision	0.088%, EER
Cherifi et al. (2021), own	7	reaching, grasping, and manipulating objects	-	Accel, Gyro, Gravity	50	HMM	feature	19.2%, EER
Shen et al. (2016), own	50	touch/tapping	2 weeks	Accel, Gyro, Gravity, Tap	-	SVM (OCC), kNN (OCC)	feature	11.05%, EER
Giuffrida et al. (2014), own	20	typing passwords	1 Sess.	Accel, Gyro, Key	17	ED, END, ManD, ManSD	feature	0.08%, EER

the smartphone and perform touch actions while walking). All of these are natural user behavior types under routine phone usage. The user behaviors possess the attribute of walking versus non-walking-based tasks to create special datasets. For each touch action that the user inputs, four sensor data are logged each of which has 3 components along the x, y, and z axes. The authors propose a statistical feature set with 16 features per sensor which are- energy, entropy, mean, minimum, maximum, range, variance, kurtosis, quantiles (from 30% to 80% with a step of 10%), cross mean rate, and skewness. Therefore, there are 3*4*16 = 192 features per touch input. The informativeness of the features is calculated for each sensor behavior to determine how users' identities differ with respect to features. The authors applied Hidden Markov Model (HMM) as the one-class classifier, SVM, and Neural Network (NN) to classify the data. They combine multiple motion events (acceleration, gyroscope, magnetometer, and orientation) and a subset of the four sensor events. However, the combination of all four motion sensor modalities produces the best EER of 4.74%.

In the study by Deb et al. (2019) multi-modal data from smartphone sensors is collected from 37 users. A passive authentication of the users (unobtrusive monitoring of the user's interaction with the device) is performed. In total, 30 smartphone sensor modalities are collected but for experiments, only 8 (keystroke dynamics, GPS location, accelerometer, gyroscope, magnetometer, linear accelerometer, gravity, and rotation) are used. Each user has contributed data for over 15 days during which they perform routine phone usage (natural behavior type). This behavior possesses the attribute of walking versus non-walking-based tasks to create special datasets. Out of the 8 modalities, accelerometer, gyroscope, magnetometer, linear accelerometer, and rotation are motion events and the others are non-motion events. For each modality, they train a Siamese LSTM network to learn deep temporal features. To remove the irregularity in data samples across sensors, they segment the data by moving a window of fixed size. The original data is in the time domain. So they transform the data to the frequency domain using Fast Fourier Transform. Following this, the pre-processed data is passed to the Siamese LSTM network. They perform 5-fold cross-validation where each fold has 29 user data for training and 8 user data for testing. Experiments are performed on individual modalities but it is observed that the performance is not satisfactory. Therefore, the fusion of 2, 3, 4, 5, 6, 7, and 8 modalities is performed at score level. They achieve the best TAR (True Acceptance Rate) of 99.98% at FAR (False Acceptance Rate) of 0.1%.

In the recent study by Stragapede et al. (2022a), data from 15 phone sensors are logged while users perform 8 different tasks of pattern unlock, typing, reading, gallery swiping, tapping on predetermined locations, signing, using a banking app, and performing phone pickup trajectory. Out of these 8 behaviors, only tapping on predetermined locations is a designed behavior and the rest are natural behaviors. The behaviors of reading, using a banking app, and performing phone pickup trajectory possess the attribute of tasks, and the other behaviors of phone unlocking, typing, gallery swiping, tapping on predetermined locations, and signing possess the attribute of hand actions (see Fig. 1). The study collects a novel dataset, named BehavePassDB from 81 users across 4 sessions where each session is parted by a day. For pre-processing the sensor data, they retain the readings along the x, y, and z-axis and calculate and add their Fast Fourier Transforms (FFTs), first-order derivatives, and second-order derivatives. For pre-processing the touch event data, they retain the x and y coordinates of each touch event and add their FFTs, first-order derivatives, and second-order derivatives. They utilize LSTM RNN Deep Neural Networks to perform authentication using a single modality and fusion of modalities. The fusion of the modalities at score level improves system performance. They have fused 6 modalities where any one of the touch events (keypress/swipe/tap) is fused with sensor events (acceleration, linear acceleration, gyroscope, magnetometer, and gravity). Hence, from all the tasks, they perform a total of 63 different fusion experiments. They have performed two attack scenarios, namely, skilled and random which involve the estimation of system performance when different users' data is logged from their own devices and when different users log data on the same device, respectively. Fusing keystrokes with sensor events they achieve the best Area Under the Curve (AUC) of 87.2%.

The study by Gascon et al. (2014) involves 315 users who type short prescribed sentences of 160 characters each. This is a designed behavior as the texts are prescribed. The user behavior is projected into the hand actions attribute as shown in Fig. 1. The motion event modalities utilized in this study are accelerometer, gyroscope, and rotation. The non-motion sporadic modality used is keypress. The motion events corresponding to the keypress or occurring during the keypress are included in the experiments while the others are eliminated. The data is then normalized from which 88 features are extracted. Hence, there are 3*9*88 = 2376 features in total. The classifier used in this study is Support Vector Machine. The best performance achieved is an AUC of 80%.

Another similar study by Cai and Chen (2012) includes motion events of accelerometer and gyroscope in combination with the non-motion sporadic event, keypress. Here, 21 users need to type random strings/PINs which is a natural behavior under the context limited subset. The user behavior possesses the hand actions attribute. The best performance obtained in this study is accuracy of 55%.

The public dataset BrainRun by Papamichail et al. (2019) includes 2218 volunteers who perform a natural behavior of game playing. The motion events logged from the users are accelerometer, gyroscope, and magnetometer and the non-motion event modalities obtained are swipe and tap. No authentication experiments are performed in this study.

Volaka et al. (2019) utilizes the HMOG public dataset (Sitová et al., 2015) to evaluate their authentication platform. The data involves reading, writing/typing, and map navigation in sitting and walking which are natural behaviors. The behaviors possess the attribute of walking versus non-walking-based tasks to create special datasets (See Fig. 1). The modalities they select from the HMOG data are acceleration, gyroscope (motion events), and swipe (non-motion sporadic event). A three-layer deep neural network is used for binary classification (each user profile is made with all data from the genuine user and randomly selected data from other users as impostors). Data processing involves the application of the min-max normalization technique. One network has 64 nodes in each layer and the other has 128 nodes in each layer. The data is batched as 8192*feature columns and is used as input to the network that ran with 200 epochs. Data is split into training-validation-testing. Four groups of experiments are performed with data from only swipes, swipes combined with acceleration, swipes combined with gyroscope, and a combination of swipe, acceleration, and gyroscope. They obtain an EER of 15% as the best result with only swipes using the 128 nodes per layer setup. Another best result of 88% accuracy is obtained when all the modalities are fused and using 64 nodes per layer.

The public dataset, BB-MAS by Belman et al. (2019), has 117 recruited volunteers who provide data on multiple interfaces (phone, tablet, and desktop), while performing several activities (sitting, walking, walking up and down staircase) which are falling under natural behavior. These user behaviors possess the attribute of walking versus non-walking-based tasks to create special datasets. The user behaviors also include typing prescribed texts which is a designed behavior. This behavior is projected into the attribute of hand actions. See Fig. 1. While sitting and typing, the sequence of activities that the users need to perform are typing two pieces of static texts of approximately 112 characters each, followed by ten questions whose answers must be of at least 50 characters each. The layout of the questions makes users swipe vertically and horizontally in between. Within one visit users need to finish the entire task of logging data on multiple devices which takes around 2 h (110 min) in total. The motion events logged in this dataset are acceleration and gyroscope. The non-motion sporadic modalities logged in this dataset are swipe, keypress, and mouse events. The authors report no experiments for user authentication with BB-MAS.

The HMOG public dataset by Sitová et al. (2015) has recruited 100 participants. The data is collected on Android mobile phones. There are 24 sessions in total involving several activities like reading, writing, and map navigation which are natural behaviors. The user behaviors possess the attribute of walking versus non-walking-based tasks to create special datasets. Out of the 8 typing/writing sessions, the 4 sessions (3, 9, 15, 21) require users to sit and type. In these four sessions, each user is asked to perform three free text typing tasks where each answer is approximately 250 characters. Users visit for multiple days to finish the entire task. The motion event modalities logged in this dataset are acceleration, gyroscope, and magnetometer. The non-motion sporadic modalities are swipe, tap, pinch, and keypress. They utilize SVM, Scaled Euclidean, and Scaled Manhattan classifiers. The best result obtained is an EER of 7.16%.

The study by Murmuria et al. (2015) involves 73 volunteers to evaluate the system which continuously authenticates users on mobile devices. The authors hypothesize that the behavior of users is context specific. This means the user behavior changes from one application under use to another. Thus, they have presented the performance of the system while users browse two applications, namely, Google Chrome and Facebook. They observe differences in authentication performance between the usage of Facebook and Chrome applications by taking five random baseline users and testing users. When both the contexts or data while using both applications are fused an improvement in performance is noticed. These browsing activities are natural behavior projected into tasks attribute. The modalities used in this study are acceleration, gyroscope (motion events), power consumption, touch, keypress, zoom, swipe, and pinch (non-motion events). From the motion event, 14 features are extracted which include mean and standard deviation along each axis and the resultant magnitude of all axes, for both accelerometer and gyroscope readings. From the touch-based modality, five features are extracted which are duration, end-to-end distance, end-to-end direction, average pressure, and average touch area. The classification algorithm used in this study is known as Transduction Classification Machine (TCM). The train-test split from each user data is 60% training and 40% testing. They obtain the best EER of 6.1%.

Stanciu et al. (2016) have recruited 20 volunteers who type passwords as a natural behavior. The behavior possesses the attribute of hand actions. The modalities utilized in this study are acceleration and gyroscope as motion events and keypress as the non-motion sporadic event. The features extracted from acceleration and gyroscope are root mean square, minimum and maximum, the number of local maxima and minima, mean delta, the sum of positive, the sum of negative, mean, mean during keystroke events, and standard deviation. Features extracted from the keypress are hold time and inter-key press time. They utilize kNN, Euclidean distance, and Manhattan distance as classifiers. They obtain the best EER of 0.08%.

The work by Nohara and Uda (2016) requires users to flick and unlock phones which is a natural behavior (under the subset of context limited) through which they log accelerometer and gyroscope as motion events and flick as a non-motion sporadic touch event. Thus this behavior possesses the hand action attribute. The classifier utilized in this study is SOM (Self Organizing Maps) which is a type of Artificial Neural Network. Several features are extracted from the modalities which are - distance from touch to release on X and Y-axes; moving distance per unit time on X and Y-axes; time from touch to release; acceleration at touch on X, Y, and Z axes; acceleration at release on X, Y, and Z axes; angular velocity at touch on X, Y, and Z axes; and angular velocity at release on X, Y, and Z axes.

Jain and Kanhangad (2015) perform a swipe-based study on more than 100 users. Each user performs seven gestures - left to right swipe (L2R), right to left swipe (R2L), scroll up (SU), scroll down (SD), zoom in (ZI), zoom out (ZO), and single tap (ST). These are natural behaviors. This user behavior is projected into the attribute of hand actions as shown in Fig. 1. The motion event modalities logged simultaneously with the touch events (swipe, tap, and zoom) are acceleration and rotation. Features extracted from the data are x, and y coordinates of every touch point, finger area from non-motion events, acceleration along x/y/z axes, rotation along x/y/z axes, point curvature, and swipe curvature. They utilize two classifiers, namely, MHD (Modified Hausdorff Distance) and DTW. MHD consistently outperforms DTW. They obtain the best result of 0.03% EER.

The study by Acien et al. (2019) utilizes the UMDAA-02 (University of Maryland Active Authentication Dataset 02) (Mahbub et al., 2016). In this dataset, users perform routine usage of phones which is a natural behavior. Through this, they log motion event modalities like acceleration, gyroscope, and non-motion events like touch, keypress, WiFi, GPS, and app use (apps used by users are Whatsapp, Navigator, Youtube, and Facebook). The user behaviors are projected into the attribute of walking versus non-walking-based tasks to create special datasets. Features extracted from acceleration and gyroscope include mean, median, maximum, minimum, distance between maximum and minimum, and standard deviation for each array of coordinates. The two other features are 1 and 99 percentiles and the distance between them. Extracted features from keystrokes include hold time, press-press latency, and press-release latency. The data is split into training (60%) and testing (40%). Two scenarios are tested in this study, namely, one-time authentication (involving data from 1 session that is the time between unlocking and locking of the device) and active authentication (involving data from multiple sessions). Utilizing SVM as the classifier they obtain the best performance of 97.1% accuracy.

Buriro et al. (2021) collected data from 95 volunteers, obtaining 11,400 samples in total. Users are recruited using Ubertesters. The study is based on one-shot-cum-continuous authentication mechanism where risk management is a novelty. If the risk score is more than a predefined threshold then a user needs to re-authenticate. User behavior includes entering a random PIN of 8 alphanumeric characters while sitting, standing, and walking. This falls under natural behavior. The duration of data collection is 3 h (1 h per day). The user behavior is projected into the hand action attribute as shown in (Fig. 1). Modalities collected are acceleration, gyroscope, magnetometer, rotation as motion event modalities and gravity and keypress as non-motion modalities. The data is divided into data streams from each of which four features are extracted, namely, mean, standard deviation, skewness, and kurtosis. Finally, 30 keypress samples and 112 hand-movements features are used to create a feature vector of size 142 (therefore they perform a feature-level fusion). Classifiers used in this study are Naive Bayes, Neural Network, and Random Forest. The Random Forest classifier outperforms Neural Network. They achieve a TAR of 91.79% and a corresponding FAR of 0.04% as the best result.

The work by Ray-Dowling et al. (2022) evaluates the performance of user authentication based on acceleration, gyroscope, and swipe data from two public mobile datasets, HMOG (Sitová et al., 2015) and BB-MAS (Belman et al., 2019) extracted with different feature sets to observe the variation in authentication performance. The study only includes data when users are typing in sitting (which is a natural behavior) and also projected into the hand actions attribute. The study evaluates the performances of both individual modalities and their fusion. From the swipe data, Frank et al.'s (2012) Touchalytics (Frank et al., 2012) features are extracted. But the work extracts three different feature sets (median, HMOG Sitová et al., 2015, and Shen et al., 2017's) on the motion event data, among which the Shen's features perform best. Fusion of multiple modalities is performed using Nandakumar's likelihood (Nandakumar et al., 2007) ratio-based score fusion by utilizing both one-class and binary SVMs. The best EERs (Equal Error Rates) of fusing all three modalities when using the one-class SVMs are 8.8% and 0.9% for HMOG and BB-MAS respectively. On the other hand, the best EERs in the case of binary SVMs are 1.5% and 0.2% respectively. Observing the better performances of BB-MAS compared to HMOG in swipe-based experiments, the study examines the difference in swipe trajectory between the two datasets and finds that BB-MAS has longer swipes than HMOG which would explain the performance difference in the experiments.

The study by Buriro et al. (2017) involves the behavior of logging micro-hand movements through phone usage for 10 s after the user is notified of a broadcast event. The broadcast receiver is triggered at the moment the user either enters their credentials or performs the slide-to-unlock gesture to unlock their smartphone. This is natural user behavior and has the hand actions attribute. The authors consider the situation where an attacker is already in possession of a smartphone. An attacker can be an unknown person, e.g., traveling with a real user on a bus or train and getting smartphone access (stranger attacks). Alternatively, an attacker could be the victim's friend, family member, or co-worker attempting to access the smartphone (insider attacks). Simple statistical features are extracted from the data, namely, mean, mean absolute deviation, median, unbiased standard error of the mean, standard deviation, unbiased skewness, and kurtosis. With 10-fold cross-validation, they achieve the best EER of 4%.

A similar study is performed by Gupta et al. (2022) which evaluates their deauthentication platform, named as IDeAuth. The aim is to minimize unauthorized access to security-sensitive applications and services running on users' smartphones when unauthorized access or intrusions are detected. The deauthentication mechanism automatically revokes the usage of the applications when unauthorized access is detected. The scheme acquires the hand movements data for 5 s using four built-in smartphone sensors, i.e., accelerometer, gyroscope, magnetometer, and gravity sensor, and two mathematically derived high-pass and low-pass sensors. This is a natural behavior and is projected into the hand actions attribute as shown in Fig. 1. They have collected their own dataset of 41 users. They consider a scenario in which the impostor is already in possession of the user's smartphone. There can be two possibilities where either the smartphone has no authentication mechanism or the impostor manages to bypass the existing single entry-point authentication mechanism on it. The user's micro-hand movement data will be logged by the motion sensors for 5 s upon receiving a notification for the broadcast events that trigger when the user unlocks, adds, or removes a package on the smartphone. Any unauthorized operation or intrusion detection will trigger the default user account's sign-off, and thus, access to all the applications and services linked with the default user account will be revoked. Four statistical features are extracted from the data, namely, mean, standard deviation, skewness, and kurtosis. They obtain 1% HTER (Half Total Error Rate) as the best performance.

The study by Basar et al. (2019) involves browsing a local banking app by 15 volunteers in sitting while the phone is on the table and standing. Users check their bank account and credit card balance in the process. It is a natural user behavior with the attribute of tasks as shown in Fig. 1. The study mainly focuses on the analysis of resource usage when a behavioral biometrics-based continuous authentication platform runs in the background. It is observed that the power consumption and CPU usages are more during authentication through motion (acceleration, gyroscope, and magnetometer) and touch sensors than during normal scenarios when no authentication is performed. During the collection of each touch gesture the following information is collected, namely, finger pressure, size, and (x, y) coordinates on the screen. The authors select the user behavior of browsing banking app since it is a sensitive application and therefore needs security measures. They also study the effects of sampling rates of the sensors on resource usage. When only the banking app is used the power consumption and CPU usage are 136 mW and 28.6% respectively. When the banking app is integrated with the logger app (with motion and touch logging) to perform authentication the power consumption and CPU usage are 189 mW and 33.86% respectively. The sampling rates of 5 Hz, 20 Hz, and 100 Hz are used per sensor, to see the impact of it on power consumption and CPU usage. The impact of acceleration sampled at 5 Hz, 20 Hz, and 100 Hz on power consumption is 149 mW, 188 mW, and 209 mW respectively. The impact of acceleration sampled at 5 Hz, 20 Hz, and 100 Hz on CPU usage is 30.22%, 32.16%, and 40.12% respectively. The impact of gyroscope sampled at 5 Hz, 20 Hz, and 100 Hz on power consumption is 170 mW, 214 mW, and 231 mW respectively. The impact of gyroscope sampled at 5 Hz, 20 Hz, and 100 Hz on CPU usage is 31.33%, 35.94%, and 42.56% respectively. The impact of magnetometer sampled at 5 Hz, 20 Hz, and 100 Hz on power consumption is 167 mW, 184 mW, and 253 mW respectively. The impact of magnetometer sampled at 5 Hz, 20 Hz, and 100 Hz on CPU usage is 31.72%, 33.85%, and 45.41% respectively.

Stragapede et al. (2022b) utilizes the large dataset of HuMIdb (Human Mobile Interaction database) (Acien et al., 2020) consisting of data from 600 users. The dataset consists of data from the following modalities, namely, touch, accelerometer, gravity sensor, gyroscope, linear accelerometer, and magnetometer. Users perform the tasks of typing a prescribed text in Spanish, *"En un lugar de la Mancha, de cuyo nombre no quiero acordarme"*; scrolling up and down; drawing the number '8' with their finger; and tapping on the screen. Of these behaviors typing the prescribed text and drawing the number '8' with their finger are designed and the rest are natural. All the behaviors possess the attribute of hand actions. The sampling rate per sensor is kept at 50 Hz. Features corresponding to a single timestamp are arranged into a 12-dimensional vector per sensor [x, y, z, x', y', z', x", y", z", fft(x), fft(y), fft(z)]. Utilizing the LSTM-RNN deep learning network both individual modality-based authentication and weighted score level fusion of available modalities in a time window is performed. Scores from modalities occurring at the same time window are fused. They come up with 63 different fusion combinations. The best EER of 12.19% is obtained with individual keypress modality. Fusing keypress, acceleration, and magnetometer the best fusion result of 3.96% EER is obtained.

Shen et al. (2022) propose the MMAuth continuous authentication platform. Utilizing HMOG (Sitová et al., 2015) and their own dataset, they perform authentication utilizing touch and motion sensor data. Users in HMOG perform read, write, and navigation while the users in their own dataset perform routine usage for 63 days. Both are natural behaviors with the attribute of walking versus non-walking-based tasks to create special datasets. They extract a time-extended behavioral feature set from motion events, touch events, and usage context data. To create the TEB feature set, they quantify each touch gesture as a feature vector [fm, ft, fc] of motion sensor-based feature (fm), touch screen sensor-based feature (ft), and usage context-based feature (fc). The features extracted from motion sensors from a time interval of the start and end of a touch gesture are mean, minimum, maximum, variance, complexity, and intensity. The features extracted from touch events are position, length, angle, touch time, speed, area, pressure, and direction. The features extracted from the usage context are application and time. Given only genuine training is possible for the authentication system in a real-life scenario, they utilize a deep one-class SVDD (Support Vector Data Description) classifier. EERs of 0.149% and 0.088% are obtained with their own data and HMOG dataset respectively.

The users in Cherifi et al. (2021) perform prehensile movements of reaching, grasping, and manipulating objects which is a natural behavior under the tasks attribute. The modalities utilized are acceleration, gyroscope, and gravity. From each sensor, the following features are extracted, mean, standard deviation, speed, or angle of motion. They propose a user pattern based on HMM architecture with a mixture of Gaussian outputs. The training: testing split of 60:40 is utilized. They obtain the best EER of 19.2%.

Shen et al. (2016) presents a sensor-based smartphone authentication system utilizing acceleration and gyroscope as motion events, gravity as another sensor event, and touch/tap events. The modalities of acceleration, gyroscope, and gravity (each with three components x, y, and z) are collected during the occurrence of taps. The target is to log users' unique touch habits and rhythms. The touch/tapping data is collected from 50 users across several rounds that span for 2 weeks. This is a natural behavior under context limited subset. It has the hand actions attribute. For each touch event, the touch timestamp (touch-up and down) and touch pressure are logged. From the sensor events occurring within a touch event, the following features are extracted - mean, variance, range, maximum, minimum, median, quartile deviation, kurtosis, and skewness. From the touch event, the features derived are the mean of touch pressure as well as the duration of the touch event. The Kolmogorov-Smirnov test is performed to test whether features are significantly different from one another. They perform one-class classification using SVM and kNN where one-class kNN produces the best EER of 11.05%.

Giuffrida et al. (2014) develop a sensor-enhanced keystroke dynamics-based authentication system where the acceleration and gyroscope motion sensors are utilized. Users need to type two passwords, namely, "satellite" and "internet". This is a natural behavior with the hand actions attribute. They only consider alphanumeric keystrokes and ignore the rest to remove noise. Motion events corresponding to acceptable keystrokes are considered for user authentication. They utilized distance metric algorithms of Euclidean, Euclidean normed, Manhattan, Manhattan scaled, and Mahalanobis for classification. They perform experiments on only keypress, only motion events, and combining keystrokes and motion events. However, the combination of keystroke and motion sensor modalities does not improve the results of individual modality experiments. The maximum sampling rate per sensor is kept at 17 Hz. They observe the performance with an increase in the sampling rate of the motion events up to 17 Hz. Across all the configurations, the best EER obtained is 4.97% using only keystrokes and 0.08% using only sensor data.

5.3. Studies involving only one motion event without/fused with other sporadic modalities

Table 3 lists the state of the art under this category that involves only one motion event modality which is optionally fused with other sporadic modalities.

A single motion event modality (acceleration) combined with other non-motion modalities is utilized to perform authentication in the study by Kumar et al. (2016b). This work investigates the fusion of phone movement patterns with typing and swiping when a user uses a web browser in sitting. This user behavior is a natural behavior. The user behavior possesses the attribute of tasks as shown in Fig. 1. The work achieves the best performance of 93.33% accuracy for a feature fusion of acceleration and swipes.

Kim and Kang (2020) authenticate users based on typing in English and Korean languages where keypress is fused with acceleration and touch events logged during typing. Such typing activity is natural under the context limited subset. It possesses the attribute of hand actions. Users type 20 reference sets in both languages where 10 references are utilized for training and the rest for testing. Experiments are performed utilizing three classifiers (Kolmogorov Smirnov, Cramer-von Mises, and TT and R measure) over individual feature sets and their combination. They achieve the best EER of 0%.

On a dataset of 39 users Crawford and Ahmadzadeh (2017) perform authentication based on keypress and gyroscope achieving 97.7% AUC. Here users perform free text typing which is a natural behavior. It possesses the attribute of hand action as shown in Fig. 1.

The study by Centeno et al. (2017) utilizes two public datasets HMOG (Sitová et al., 2015) (100 users; behavior duration 6 h) and Algosnap (Algosnap dataset, 2022) (20 users; behavior duration several days). User behavior includes miscellaneous routine activities that fall under natural behavior. The user behaviors in both datasets are projected into the attribute of walking versus non-walking-based tasks to create special datasets. This work includes only acceleration data sampled at 100 Hz for HMOG and 200 Hz for Algosnap. Data is later downsampled to 25 Hz and used to evaluate their re-authentication platform. The data is split into training, validation, and testing. Deep Learning based autoencoders are used for classification that achieves the best EER of 2.2%.

An early work based on the designed behavior of arm sweep action is presented by Okumura et al. (2006) where users perform sweep action by shaking the handheld device up and down along the y-axis. This designed behavior possesses the tasks attribute. They hypothesize that the acceleration data from the standalone device collected during the arm sweep action can be used for a

Table 3
Comparative literature review: Single motion sensor to measure stationary behavior on mobiles with/without another sporadic modality. Abbreviations - ACC: Accuracy, AUC: Area Under the Curve, ANN: Artificial Neural Network, CM: Cramer-von Mises, CC: Cross Correlation, DT: Decision Trees, DP: Dynamic Programming matching, DTW: Dynamic Time Warping, EA: Error of Angle, EER: Equal Error Rate, FAR: False Acceptance Rate, FNR: False Negative Rate, FPR: False Positive Rate, FRR: False Reject Rate, kNN: k Nearest Neighbor, KS: Kolmogorov Smirnov, LReg: Logistic Regression, MLP: Multilayer Perceptron, RF: Random Forest, sq ED: Squared Euclidean Distance, SVM: Support Vector Machine, TT and R: TT and R measure, TPR: True Positive Rate.

Study & Dataset	#User	Behavior	Duration	Modality	Sampling (Hz)	Algorithm	Fusion	Best performance
Kumar et al. (2016b), own	28	browsing web	-	Accel, Key, Swipe	-	kNN, RF	Score, Feature	93.33%, ACC
Kim and Kang (2020), own	50	typing in English and Korean	-	Accel, Key	-	KS, CM, TT and R	sensor	0%, EER
Crawford and Ahmadzadeh (2017), own	39	typing free text	1 Sess.	Gyro, Key	-	DT, LReg	sensor	97.7%, AUC
Laghari et al. (2016), own	10	hand waving/arm sweeping holding phone	1 Sess.	Accel	-	CC	-	1.46% FAR, 6.87% FRR
Casanova et al. (2010), own	34	hand waving/arm sweeping holding phone	2 Sess.	Accel	100	DTW	decision	2.5%, EER
Hong et al. (2015), own	8	hand waving/arm sweeping holding phone	8 weeks	Accel	80	SVM (OCC)	-	92.83% TPR, 3.67% FPR
Yang et al. (2014), own	200	hand waving/arm sweeping holding phone	1 Sess.	Accel	50, 100	SVM	-	15% FPR, 8% FNR
Centeno et al. (2017), HMOG (Sitová et al., 2015), Algosnap (Algosnap dataset, 2022)	100, 20	read, write, navigate; routine usage	6 hr, several days	Accel	100, 200	ANN	-	2.2%, EER
Okumura et al. (2006), own	22	hand waving/arm sweeping holding device	1 Sess.	Accel	100	sq.ED, EA, DP	-	5%, EER
Lin et al. (2012), own	20	up-down flick, left-right flick	-	Rotate	30	kNN	decision	6.85%, EER
Owusu et al. (2012), own	4	typing prescribed texts and passwords	-	Accel, Key	50	RF, MLP, SVM, DT	-	-

security check on a cell phone using the cell phone's accelerometer. For classification, three algorithms are used - squared error of Euclidean distance, error of angle, and Dynamic Programming matching. They observe an ERR of 5% as their best result.

The work by Laghari et al. (2016) involves the behavior of in-air signature holding the phone in hand. This is a designed behavior captured using accelerometer motion event. The user behavior is projected into the attribute of tasks. They implement a three-tier system - user: from where input is obtained, server: where authentication is performed, and database: where the template is kept. An app runs on the phone while users perform the in-air signature gestures. Cross-correlation of the signature is performed where a genuine user shows a higher cross-correlation value than an impostor. The best performance obtained is a FAR of 1.46% and a corresponding FRR (False Rejection Rate) of 6.87%.

A similar in-air signature hand gesture-based work is performed by Casanova et al. (2010). The authors hypothesize that user authentication through the above-designed behavior is possible because of uniqueness across users due to the speed and manner of signing in air and other user physical factors like the length of the arm, the capability of turning the wrist, and the size of the hand holding the device. Each user has repeated their gesture seven times, with intervals of 10 s in between, to reduce dependency between samples. The in-air signed gestures performed are-writing a word or a number in the air, performing a usual gesture (like playing guitar), drawing a symbol in the air, drawing something real in the air, performing a complex gesture by concatenating simple gestures (squares, triangles, circles), and making their own signatures in the air. A second session has been performed by studying the videos recorded in the previous session. In this session, three different people tried to forge each of the original in-air biometric signatures. Utilizing DTW as the classifier they achieve an EER of 2.5% as the best performance.

The study by Hong et al. (2015) involves the behavior of hand waving gestures. They collect data from 8 users and each user performs 10 hand gestures for weeks. Hence, this is designed user behavior. It is projected into the tasks attribute as shown in Fig. 1. Acceleration motion event is used to log the user's gestures. Utilizing SVM as the classifier they achieve the best result of 92.83% TPR (True Positive Rate) with a corresponding FPR (False Positive Rate) of 3.67%.

Another behavior to authenticate users is unlocking phones through hand waving as shown in Yang et al. (2014) (Yang et al., 2014). Acceleration is the only motion event modality that captures the above designed user behavior (having the tasks attribute). Utilizing SVM as the classifier they achieve the best performances of 15% FPR (False Positive Rate) and 8% FNR (False Negative Rate).

Lin et al. (2012) proposes a novel non-intrusive authentication mechanism where users perform up-down and left-right flicks/swipes in sitting. There are 20 users who provide the data from which the flicks of duration < 100 milliseconds are discarded. The user behavior is natural under the context limited subset and has the hand actions attribute. Only orientation (rotation) motion event is utilized to log the user's wrist motions. We must know the relationship between wrist motion and the reading of the orientation sensor while a user holds and operates a smartphone. Our wrist offers three dimensions of freedom, which are, wrist flexion and extension, supination and pronation, and wrist radial and ulnar deviation. They extract 53 features in total from the data. Utilizing the orientation data along the y and z axes they calculate the combined angle which is the square root of the sum of squares of orientation along the y and z axes. Features extracted are average, minimum, maximum, range, and standard deviation of orientation along x, y, z, and combined angles. Feature selection is performed per user using linear regression. They utilize the kNN classifier with 1, 3, 5, 7, and 9 as k values and combine the decisions of each kNN using majority voting to obtain improved performance. They obtain the best EER of 6.85%.

The study by Owusu et al. (2012) involves authentication using the corresponding acceleration data during keypresses. Users type prescribed texts to make sure all the keys are pressed by a single user and they also type several passwords. There are two types of experiments performed, namely, area mode inference and character mode inference. In area mode inference a total of 1300 keypresses and the corresponding acceleration data are collected. In the area mode inference experiment, they divide the screen into smaller areas from each of which they collect approximately 20 samples. Before each data collection run, participants are instructed to press keys in any order until all of the keys received at least one press. They represent a heat map that shows the areas on the screen whose acceleration has performed the best and worst in authenticating users. For character mode inference, in total 2700 keypresses and their corresponding acceleration data are collected. Here the training data includes typing pangrams and testing data includes typing 99 6-character passwords. Features extracted from each of x, y, z, and resultant components of acceleration are - Root Mean Square (RMS) value, RMS error, minimum, maximum, average sample by sample change, number of local peaks, number of local crests, the average time from a sample to a peak, the average time from a sample to a crest, RMS cross rate, and signal magnitude area. There are two meta information as features which are, the total time of the window and the number of samples in the windows. Feature selection is performed using the Wrapper algorithm. They plot the percentage of passwords cracked against the median number of trials required to extract those passwords. 1 of 99 passwords is cracked in 1 attempt and 6 of 99 in 4.5 median attempts.

6. Future research implications and directions

This survey focuses on stationary mobile behavioral biometrics through motion events. We categorize user behaviors into natural and designed and present further sub-categorization. We believe that our conceptual framework will be used in enhancing the knowledge about the background of this domain and also will be beneficial for readers (from both academia and industry) to easily grasp the vast behavior landscape of user behaviors. We believe that our survey will present readers with the reasonings or intents of our past researchers towards their choice of a certain behavior for authentication. The readers can also view the gradual shift in usage of natural behaviors over designed (Fig. 8) which demonstrates the future application trend while implementing such security mechanisms in real-life.

Furthermore, we review each study along dimensions such as tasks, datasets, modalities, algorithms, and performances along with additional behavioral attributes, and link the state of the art to our proposed model. We believe that our proposed conceptualization framework and the survey in its entirety will help future academic researchers and industry practitioners in setting up the constraints or modules (such as type of behavior, choice of motion sensors and supporting sporadic modalities, choice of features for motion sensors, setting sampling rate, making the desired classification model, and choosing suitable metrics, among others). The aim of our survey is to present a handbook on stationary mobile behavioral biometrics that demonstrates the choice of such constraints and their effects on authentication performance. This we believe should support academic researchers in benchmarking mobile behavioral biometrics which in turn should be beneficial for industrial practitioners for real-life implementation.

We have identified several important directions for future research. Although the above-contributing factors in our survey will support the essential benchmarking of mobile behavioral biometrics, we observe that at present not many benchmarking of mobile behavioral biometrics exist. For the real-life implementation of mobile behavioral biometrics for continuous authentication of legitimate users such benchmarking studies are necessary. This will demonstrate an estimated performance range to future researchers before such mobile security system gets deployed in real-life. We believe that there is a requirement to rigorously evaluate different groups of classifiers along with feature sets and fusion strategies in the process of benchmarking. Although we have described the underpinning of behavioral biometrics in cognitive psychology, we believe that significant future work is needed to formally establish human psychology and other related disciplines such as human physiology as the scientific foundation of behavioral biometrics. Furthermore, studies are needed to investigate the usability and the social acceptability of behavioral biometrics-based mobile security. Lastly, another important direction is to integrate behavioral biometrics in a way that compliments other existing security mechanisms, where much future work needs to be done.

7. Conclusion

Our survey reviews the state of the art in mobile behavioral biometrics with a focus on motion events, which authenticate users through their stationary (sitting/standing) behaviors. Stationary behaviors represent the major way modern users interact with mobile devices and thus more focus is needed to observe its effects on authentication performance. We categorize the user behaviors across the studies into natural and designed for researchers to grasp the broad landscape of stationary user behaviors. Under natural behaviors, we identify four kinds of contexts, namely, novel behaviors, routine usage, context limited, and postures with phone. The contexts of novel behaviors, context limited, and routine usage include stationary user behaviors. In contrast, postures with phone, being the broadest context, includes a few walking behaviors along with dominant stationary behaviors.

We study the research timeline of the reviewed state of the art and observe that the usage of designed behaviors for user authentication appears to have gone out of fashion. Since 2015 the research community has explored substantial natural behaviors. This is consistent with the fact that it is more common for regular mobile users to exhibit natural behaviors than designed. We also plot the performances of each study and observe the effects of behavior types on the authentication performance. Each user behavior, irrespective of its type, is projected into three different attributes or aspects (walking versus non-walking, tasks, and hand actions).

Additionally, we lay our focus on the general psychology of the users. We describe the underpinning of behavioral biometrics by cognitive psychology and project the necessity of further future work on this topic to formally establish cognitive psychology as the foundation of behavioral biometrics. We acknowledge the fact that users with cooperating psychology tend to learn/get accustomed to the mobile user interface (Carroll and Rosson, 1987) which is believed to add a positive impact on the authentication performance. On the other hand, the psychology of non-cooperating users put a negative impact on authentication. However, we have enough cooperating and stable users who in the best interest of their device's security will utilize the advantages of the user authentication system.

Our survey groups the reviewed studies on stationary mobile behavioral biometrics into three categories based on the involvements of the motion events. Given that sporadic modalities are not always available, we focus on motion events to log the unique hand micro-movement characteristics of users. But we highly encourage the fusion of sporadic non-motion modalities (when available) with motion events to further benefit the authentication performance. We survey the studies along the dimensions of user behaviors, duration of device usage, sensor utilization, sampling rate, feature extraction, classifiers/algorithms used, and performance. We observe acceptable authentication performances across the studies involving stationary user behaviors. Through our survey, we observe that there are not many benchmarking done on behavioral biometrics which is needed in the future to deploy it as a mobile device security mechanism in real-life.

As the field of behavioral biometrics evolves, more studies are needed to evaluate its practicality and generalizability. This survey aims to demonstrate the role of user behavior on authentication performance and identifies those behaviors that are highly normalized in real life while a user is interacting with their mobile device. We hope that our survey of different authentication technologies applied to behavioral biometrics will be useful for future researchers to deploy passive authentication mechanisms in real life on mobile devices based on users' stationary behaviors which are most commonly exhibited.

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Daqing Hou reports financial support was provided by National Science Foundation.

CRediT authorship contribution statement

Aratrika Ray-Dowling: Conceptualization, Methodology, Visualization, Writing – original draft, Writing – review & editing. **Daqing Hou:** Conceptualization, Methodology, Supervision, Writing – review & editing. **Stephanie Schuckers:** Conceptualization, Methodology, Supervision.

Data availability

No data was used for the research described in the article.

Acknowledgment

This work was supported by the Center for Identification Technology Research (CITeR) and the National Science Foundation [grant number CNS-1650503] and [grant number TI-2122746].

References

Abrahamse, E.L., Ruitenberg, M.F., De Kleine, E., Verwey, W.B., 2013. Control of automated behavior: insights from the discrete sequence production task. Front. Hum. Neurosci. 7, 82. doi:10.3389/fnhum.2013.00082.

Abuhamad, M., Abuhmed, T., Mohaisen, D., Nyang, D., 2020. AUToSen: deep-learning-based implicit continuous authentication using smartphone sensors. IEEE Internet Things J. 7. doi:10.1109/JIOT.2020.2975779.

Abuhamad, M., Abusnaina, A., Nyang, D., Mohaisen, D., 2020. Sensor-based continuous authentication of smartphones' users using behavioral biometrics: a contemporary survey. IEEE Internet Things J. 8 (1), 65–84. doi:10.1109/JIOT.2020.3020076.

Acien, A., Morales, A., Fierrez, J., Vera-Rodriguez, R., Bartolome, I., 2020. BeCAPTCHA: detecting human behavior in smartphone interaction using multiple inbuilt sensors. 10.48550/arXiv.2002.00918

Acien, A., Morales, A., Vera-Rodriguez, R., Fierrez, J., Tolosana, R., 2019. MultiLock: mobile active authentication based on multiple biometric and behavioral patterns. In: 1st International Workshop on Multimodal Understanding and Learning for Embodied Applications, pp. 53–59.

Algosnap dataset http://crowdsignals.io/index.html. Accessed: 2022-06-17.

Alobaidi, H., Clarke, N., Li, F., Alruban, A., 2022. Real-world smartphone-based gait recognition. Comput. Secur. 113, 102557. doi:10.1016/j.cose.2021.102557.

Alsaadi, I.M., 2021. Study on most popular behavioral biometrics, advantages, disadvantages and recent applications: a review. Int. J. Sci. Technol. Res 10, 15–21.

Alzubaidi, A., Kalita, J., 2016. Authentication of smartphone users using behavioral biometrics. IEEE Commun. Surveys & Tutor. 18 (3), 1998–2026. doi:10.1109/COMST.2016.2537748.

Amini, S., Noroozi, V., Pande, A., Gupte, S., Yu, P.S., Kanich, C., 2018. DeepAuth: a framework for continuous user re-authentication in mobile apps. In: Proceedings of the 27th ACM International Conference on Information and Knowledge Management, pp. 2027–2035. doi:10.1145/3269206.3272034.

Anderson, J.R., 1982. Acquisition of cognitive skill. Psychol Rev 89 (4), 369.

Aravindhan, K., Karthiga, R., 2013. One time password: a survey. Int. J. Emerg. TrendsEng. Dev. 1 (3), 613–623.

Barkley, J.E., Lepp, A., 2016. Mobile phone use among college students is a sedentary leisure behavior which may interfere with exercise. Comput. Human Behav. 56, 29–33.

Basar, O.E., Alptekin, G., Volaka, H.C., Isbilen, M., Incel, O.D., 2019. Resource usage analysis of a mobile banking application using sensor-and-touchscreen-based continuous authentication. Procedia Comput. Sci. 155. doi:10.1016/j.procs.2019.08.028.

Behavioral biometrics vs static biometrics: dynamic fraud detection explained https://www.biocatch.com/blog/behavioral-biometrics-vs-static-biometrics-fraud-detection. Accessed: 2022-06-03.

Belman, A. K., Wang, L., Iyengar, S., Sniatala, P., Wright, R., Dora, R., Baldwin, J., Jin, Z., Phoha, V. V., 2019. Insights from BB-MAS–a large dataset for typing, gait and swipes of the same person on desktop, tablet and phone. 10.48550/arXiv.1912.02736

Bhattarai, A., Siraj, A., 2018. Increasing accuracy of hand-motion based continuous authentication systems. In: 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) doi:10.1109/UEMCON.2018.8796725.

Buriro, A., Crispo, B., Del Frari, F., Klardie, J., Wrona, K., 2015. ITSME: multimodal and unobtrusive behavioural user authentication for smartphones. In: International Conference on Passwords. Springer, pp. 45–61. doi:10.1007/978-3-319-29938-9_4.

Buriro, A., Crispo, B., Zhauniarovich, Y., 2017. Please hold on: unobtrusive user authentication using smartphone's built-in sensors. In: 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA). IEEE, pp. 1–8. doi:10.1109/ISBA.2017.7947684.

Buriro, A., Gupta, S., Yautsiukhin, A., Crispo, B., 2021. Risk-driven behavioral biometric-based one-shot-cum-continuous user authentication scheme. J. Signal Process. Syst. 93 (9), 989–1006. doi:10.1007/s11265-021-01654-2.

Cai, L., Chen, H., 2012. On the practicality of motion based keystroke inference attack. In: International Conference on Trust and Trustworthy Computing. Springer, pp. 273–290. doi:10.1007/978-3-642-30921-2_16.

Cai, Y., Zhao, Y., Ding, X., Fennelly, J., 2012. Magnetometer basics for mobile phone applications. Electron. Prod. (Garden City, New York) 54 (2).

Carlson, C., Chen, T., Cruz, J., Maghsoudi, J., Zhao, H., Monaco, J.V., 2015. User authentication with android accelerometer and gyroscope sensors. In: Proceedings of Student-Faculty Research Day. CSIS, Pace University.

Carroll, J.M., Rosson, M.B., 1987. Paradox of the active user. In: Interfacing Thought: Cognitive Aspects of Human-Computer Interaction, pp. 80–111.

Casanova, J.G., Ávila, C.S., Santos Sierra, A.d., Pozo, G., Vera, V.J., 2010. A real-time in-air signature biometric technique using a mobile device embedding an accelerometer. In: International Conference on Networked Digital Technologies. Springer, pp. 497–503. doi:10.1007/978-3-642-14292-5_50.

Centeno, M.P., van Moorsel, A., Castruccio, S., 2017. Smartphone continuous authentication using deep learning autoencoders. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST). IEEE, pp. 147–1478. doi:10.1109/PST.2017.00026.

Cherifi, F., Omar, M., Amroun, K., 2021. An efficient biometric-based continuous authentication scheme with HMM prehensile movements modeling. J. Inf. Secur. Appl. 57. doi:10.1016/j.jisa.2020.102739.

Cognitive psychology. https://en.wikipedia.org/wiki/Cognitive_psychology. Accessed: 2022-06-03.

Crawford, H., Ahmadzadeh, E., 2017. Authentication on the go: assessing the effect of movement on mobile device keystroke dynamics. In: Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017), pp. 163–173.

Deb, D., Ross, A., Jain, A.K., Prakah-Asante, K., Prasad, K.V., 2019. Actions speak louder than (pass) words: Passive authentication of smartphone users via deep temporal features. In: International Conference on Biometrics. IEEE, pp. 1–8. doi:10.1109/ICB45273.2019.8987433.

Eglitis, T., Guest, R., Deravi, F., 2020. Data behind mobile behavioural biometrics–a survey. IET Biom. 9 (6), 224–237. doi:10.1049/iet-bmt.2018.5174.

Ericsson, K.A., Krampe, R.T., Tesch-Römer, C., 1993. The role of deliberate practice in the acquisition of expert performance. Psychol. Rev. 100 (3), 363. doi:10.1037/0033-295X.100.3.363.

Fantana, A.L., Ramachandran, S., Schunck, C.H., Talamo, M., 2015. Movement based biometric authentication with smartphones. In: 2015 International Carnahan Conference on Security Technology (ICCST). IEEE, pp. 235–239. doi:10.1109/CCST.2015.7389688.

Feng, T., Zhao, X., Shi, W., 2013. Investigating mobile device picking-up motion as a novel biometric modality. In: 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS). IEEE, pp. 1–6. doi:10.1109/BTAS.2013.6712701.

Frank, M., Biedert, R., Ma, E., Martinovic, I., Song, D., 2012. Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans. Inf. Forensics Secur. 8 (1), 136–148. doi:10.1109/TIFS.2012.2225048.

Gascon, H., Uellenbeck, S., Wolf, C., Rieck, K., 2014. Continuous authentication on mobile devices by analysis of typing motion behavior. In: Sicherheit 2014–Sicherheit, Schutz und Zuverlässigkeit, pp. 1–12.

Giuffrida, C., Majdanik, K., Conti, M., Bos, H., 2014. I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer doi:10.1007/978-3-319-08509-8_6.

Gupta, S., Kumar, R., Kacimi, M., Crispo, B., 2022. IDeAuth: a novel behavioral biometric-based implicit deauthentication scheme for smartphones. Pattern Recognit. Lett. 157, 8–15. doi:10.1016/j.patrec.2022.03.011.

Haasnoot, E., Barnhoorrr, J., Spreeuwers, L.J., Veldhuis, R.N., Verwey, W.B., 2018. Towards understanding the effects of practice on behavioural biometric recognition performance. In: 2018 26th European Signal Processing Conference (EUSIPCO). IEEE, pp. 558–562. doi:10.23919/EUSIPCO.2018.8553446.

Ehatisham-ul Haq, M., Azam, M.A., Naeem, U., Amin, Y., Loo, J., 2018. Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. J. Netw. Comput. Appl. 109, 24–35. doi:10.1016/j.jnca.2018.02.020.

hall-effect https://www.electronics-tutorials.ws/electromagnetism/hall-effect.html. Accessed: 2022-07-06.

Hong, F., Wei, M., You, S., Feng, Y., Guo, Z., 2015. Waving authentication: your smartphone authenticate you on motion gesture. In: Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, pp. 263–266. doi:10.1145/2702613.2725444.

How does a gyroscope sensor work in your smartphone? https://www.techaheadcorp.com/knowledge-center/how-gyroscope-sensor-work-in-smartphone/. Accessed: 2022-07-06.

How to measure acceleration? https://www.omega.com/en-us/resources/accelerometers. Accessed: 2022-06-29.

Incel, Ö.D., Günay, S., Akan, Y., Barlas, Y., Basar, O.E., Alptekin, G.I., Isbilen, M., 2021. DAKOTA: sensor and touch screen-based continuous authentication on a mobile banking application. IEEE Access 9, 38943–38960. doi:10.1109/ACCESS.2021.3063424.

Jain, A., Bolle, R., Pankanti, S., 1999. Biometrics: Personal Identification in Networked Society, Vol. 479. Springer Science & Business Media.

Jain, A., Kanhangad, V., 2015. Exploring orientation and accelerometer sensor data for personal authentication in smartphones using touchscreen gestures. Pattern Recognit. Lett. 68, 351–360. doi:10.1016/j.patrec.2015.07.004.

Jain, A.K., Ross, A.A., Nandakumar, K., 2011. Introduction to Biometrics. Springer Science & Business Media doi:10.1007/978-0-387-77326-1_6.

Kayacik, H. G., Just, M., Baillie, L., Aspinall, D., Micallef, N., 2014. Data driven authentication: on the effectiveness of user behaviour modelling with mobile device sensors. 10.48550/arXiv.1410.7743

Kim, J., Kang, P., 2020. Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features. Pattern Recognit. 108, 107556. doi:10.1016/j.patcog.2020.107556.

Kratz, S., Rohs, M., Essl, G., 2013. Combining acceleration and gyroscope data for motion gesture recognition using classifiers with dimensionality constraints. In: Proceedings of the 2013 International Conference on Intelligent user Interfaces, pp. 173–178. doi:10.1145/2449396.2449419.

Kumar, R., Kundu, P.P., Phoha, V.V., 2018. Continuous authentication using one-class classifiers and their fusion. In: IEEE 4th International Conference on Identity, Security, and Behavior Analysis, pp. 1–8. doi:10.1109/ISBA.2018.8311467.

Kumar, R., Phoha, V.V., Jain, A., 2015. Treadmill attack on gait-based authentication systems. In: 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, pp. 1–7. doi:10.1109/BTAS.2015.7358801.

Kumar, R., Phoha, V. V., Raina, R., 2016a. Authenticating users through their arm movement patterns. arXiv preprint arXiv:1603.02211.

Kumar, R., Phoha, V.V., Serwadda, A., 2016. Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns. In: IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, pp. 1–8. doi:10.1109/BTAS.2016.7791164.

Kunnathu, N., 2015. Biometric user authentication on smartphone accelerometer sensor data. In: Proceedings of Student-Faculty Research Day. CSIS, Pace University.

Laghari, A., Memon, Z.A., et al., 2016. Biometric authentication technique using smartphone sensor. In: 2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST). IEEE, pp. 381–384. doi:10.1109/IBCAST.2016.7429906.

Lee, W.-H., Lee, R.B., 2015. Multi-sensor authentication to improve smartphone security. In: 2015 International Conference on Information Systems Security and Privacy (ICISSP). IEEE, pp. 1–11.

Lee, W.-H., Lee, R.B., 2017. Implicit smartphone user authentication with sensors and contextual machine learning. In: 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, pp. 297–308. doi:10.1109/DSN.2017.24.

Li, Y., Hu, H., Zhou, G., 2018. Using data augmentation in continuous authentication on smartphones. IEEE Internet Things J. 6 (1), 628–640. doi:10.1109/JIOT.2018.2851185.

Li, Y., Hu, H., Zhu, Z., Zhou, G., 2020. SCANet: sensor-based continuous authentication with two-stream convolutional neural networks. ACM Trans. Sens. Netw. (TOSN) 16 (3), 1–27. doi:10.1145/3397179.

Li, Y., Tao, P., Deng, S., Zhou, G., 2021. DeFFusion: CNN-based continuous authentication using deep feature fusion. ACM Trans. Sens. Netw. 18. doi:10.1145/3485060.

Li, Y., Zou, B., Deng, S., Zhou, G., 2020. Using feature fusion strategies in continuous authentication on smartphones. IEEE Internet Comput. 24. doi:10.1109/MIC.2020.2971447.

Lin, C.-C., Chang, C.-C., Liang, D., Yang, C.-H., 2012. A new non-intrusive authentication method based on the orientation sensor for smartphone users. In: 2012 IEEE Sixth International Conference on Software Security and Reliability doi:10.1109/SERE.2012.37.

Liu, M., 2013. A study of mobile sensing using smartphones. Int. J. Distrib. Sens. Netw. 9 (3), 272916. doi:10.1155/2013/272916.

Mahbub, U., Sarkar, S., Patel, V.M., Chellappa, R., 2016. Active user authentication for smartphones: a challenge data set and benchmark results. In: 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, pp. 1–8. doi:10.1109/BTAS.2016.7791155.

Mahfouz, A., Mahmoud, T.M., Eldin, A.S., 2017. A survey on behavioral biometric authentication on smartphones. J. Inf. Secur. Appl. 37, 28–37. doi:10.1016/j.jisa.2017.10.002.

Murmuria, R., Stavrou, A., Barbará, D., Fleck, D., 2015. Continuous authentication on mobile devices using power consumption, touch gestures and physical movement of users. International Symposium on Recent Advances in Intrusion Detection. Springer doi:10.1007/978-3-319-26362-5_19.

Nandakumar, K., Chen, Y., Dass, S.C., Jain, A., 2007. Likelihood ratio-based biometric score fusion. IEEE Trans. Pattern Anal. Mach. Intell. 30 (2), 342–347. doi:10.1109/TPAMI.2007.70796.

Neverova, N., Wolf, C., Lacey, G., Fridman, L., Chandra, D., Barbello, B., Taylor, G., 2016. Learning human identity from motion patterns. IEEE Access 4, 1810–1820. doi:10.1109/ACCESS.2016.2557846.

Nohara, T., Uda, R., 2016. Personal identification by flick input using self-organizing maps with acceleration sensor and gyroscope. In: Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication, pp. 1–6. doi:10.1145/2857546.2857605.

Okumura, F., Kubota, A., Hatori, Y., Matsuo, K., Hashimoto, M., Koike, A., 2006. A study on biometric authentication based on arm sweep action with acceleration sensor. In: 2006 International Symposium on Intelligent Signal Processing and Communications. IEEE, pp. 219–222. doi:10.1109/ISPACS.2006.364871.

Owusu, E., Han, J., Das, S., Perrig, A., Zhang, J., 2012. Accessory: password inference using accelerometers on smartphones. proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications doi:10.1145/2162081.2162095.

Papamichail, M.D., Chatzidimitriou, K.C., Karanikiotis, T., Oikonomou, N.-C.I., Symeonidis, A.L., Saripalle, S.K., 2019. BrainRun: a behavioral biometrics dataset towards continuous implicit authentication. Data 4 (2), 60. doi:10.3390/data4020060.

Ray, A., Hou, D., Schuckers, S., Barbir, A., 2021. Continuous authentication based on hand micro-movement during smartphone form filling by seated human subjects. In: ICISSP, pp. 424–431. doi:10.5220/0010225804240431.

Ray-Dowling, A., Hou, D., Schuckers, S., Barbir, A., 2022. Evaluating multimodal mobile behavioral biometrics using public datasets. Comput. Secur. doi:10.1016/j.cose.2022.102868. https://www.sciencedirect.com/science/article/pii/S0167404822002620

Ross, A.A., Nandakumar, K., Jain, A.K., 2006. Handbook of Multibiometrics, Vol. 6. Springer Science & Business Media doi:10.1007/0-387-33123-9.

Roy, A., Halevi, T., Memon, N., 2015. An HMM-based multi-sensor approach for continuous mobile authentication. In: MILCOM IEEE Military Communications Conference. IEEE, pp. 1311–1316. doi:10.1109/MILCOM.2015.7357626.

Ryu, R., Yeom, S., Kim, S.-H., Herbert, D., 2021. Continuous multimodal biometric authentication schemes: a systematic review. IEEE Access 9, 34541–34557. doi:10.1109/ACCESS.2021.3061589.

Shen, C., Li, Y., Chen, Y., Guan, X., Maxion, R.A., 2017. Performance analysis of multimotion sensor behavior for active smartphone authentication. IEEE Trans. Inf. Forensics Secur. 13 (1), 48–62. doi:10.1109/TIFS.2017.2737969.

Shen, C., Li, Y., Yu, T., Yuan, S., Yi, X., Guan, X., 2016. Motion-senor behavior analysis for continuous authentication on smartphones. 2016 12th World Congress on Intelligent Control and Automation (WCICA) doi:10.1109/WCICA.2016.7578519.

Shen, Z., Li, S., Zhao, X., Zou, J., 2022. MMAuth: a continuous authentication framework on smartphones using multiple modalities. IEEE Trans. Inf. Forensics Secur. 17. doi:10.1109/TIFS.2022.3160361.

Sitová, Z., Šeděnka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P., Balagani, K.S., 2015. HMOG: new behavioral biometric features for continuous authentication of smartphone users. IEEE Trans. Inf. Forensics Secur. 11 (5), 877–892. doi:10.1109/TIFS.2015.2506542.

Stanciu, V.-D., Spolaor, R., Conti, M., Giuffrida, C., 2016. On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks. In: Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy, pp. 105–112. doi:10.1145/2857705.2857748.

Stragapede, G., Vera-Rodriguez, R., Tolosana, R., Morales, A., 2022. BehavePassDB: public database for mobile behavioral biometrics and benchmark evaluation. Pattern Recognit. 109089. doi:10.1016/j.patcog.2022.109089.

Stragapede, G., Vera-Rodriguez, R., Tolosana, R., Morales, A., Acien, A., Le Lan, G., 2022. Mobile behavioral biometrics for passive authentication. Pattern Recognit. Lett. 157. doi:10.1016/j.patrec.2022.03.014. https://www.sciencedirect.com/science/article/pii/S016786552200071X

Stylios, I., Kokolakis, S., Thanou, O., Chatzis, S., 2021. Behavioral biometrics & continuous user authentication on mobile devices: a survey. Inf. Fusion 66, 76–99.

Stylios, I.C., Thanou, O., Androulidakis, I., Zaitseva, E., 2016. A review of continuous authentication using behavioral biometrics. In: Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference, pp. 72–79. doi:10.1145/2984393.2984403.

Teh, P.S., Zhang, N., Teoh, A.B.J., Chen, K., 2016. A survey on touch dynamics authentication in mobile devices. Comput. Secur. 59, 210–235. doi:10.1016/j.cose.2016.03.003.

Volaka, H.C., Alptekin, G., Basar, O.E., Isbilen, M., Incel, O.D., 2019. Towards continuous authentication on mobile phones using deep learning models. Procedia Comput. Sci. 155, 177–184. doi:10.1016/j.procs.2019.08.027.

What is magnetometer sensor?, https://www.gearbest.com/blog/how-to/what-is-magnetometer-sensor-2866. Accessed: 2022-07-06.

Yang, J., Li, Y., Xie, M., 2015. MotionAuth: motion-based authentication for wrist worn smart devices. In: 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops). IEEE, pp. 550–555. doi:10.1109/PERCOMW.2015.7134097.

Yang, L., Guo, Y., Ding, X., Han, J., Liu, Y., Wang, C., Hu, C., 2014. Unlocking smart phone through handwaving biometrics. IEEE Trans. Mob. Comput. 14 (5), 1044–1055. doi:10.1109/TMC.2014.2341633.

Zagalaz-Sánchez, M.L., Cachón-Zagalaz, J., Sánchez-Zafra, M., Lara-Sánchez, A., 2019. Mini review of the use of the mobile phone and its repercussion in the deficit of physical activity. Front. Psychol. 10, 1307.

Zhu, H., Hu, J., Chang, S., Lu, L., 2017. Shakein: secure user authentication of smartphones with single-handed shakes. IEEE Trans. Mob. Comput. 16 (10), 2901–2912. doi:10.1109/TMC.2017.2651820.

Aratrika Ray-Dowling (corresponding author) received Bachelor of Engineering Degree in Computer Science and Engineering from Visvesvaraya Technological University, India in 2014. She received Masters of Science Degree in Electrical Engineering from Clarkson University, USA in 2019. She is currently pursuing PhD degree in the department of Electrical and Computer Engineering at Clarkson University, USA. Her research interest includes Mobile/Computer Security, Biometrics, Machine Learning, and Data Analytics.

Daqing Hou (co-author) is Professor and Director of Software Engineering in the Department of Electrical and Computer Engineering at Clarkson University. He received his doctoral degree in Computing Science from The University of Alberta. His research interests include software engineering, behavioral biometrics, and engineering education. His work is funded by various agencies, including the National Science Foundation, Department of Defense, Air Force Research Lab, IBM, Facebook, among others. He has published over 80 peer-reviewed research papers.

Stephanie Schuckers (co-author) is the Paynter-Krigman Endowed Professor in Engineering Science in the Department of Electrical and Computer Engineering at Clarkson University and serves as the Director of the Center of Identification Technology Research (CITeR), a National Science Foundation Industry/University Cooperative Research Center. She received her doctoral degree in Electrical Engineering from The University of Michigan. Her research focuses on processing and interpreting signals which arise from the human body. Her work is funded from various sources, including National Science Foundation, Department of Homeland Security, and private industry, among others.