

RESEARCH

Open Access



The utility of behavioral biometrics in user authentication and demographic characteristic detection: a scoping review

O. L. Finnegan^{1*} , J. W. White III¹, B. Armstrong¹, E. L. Adams¹, S. Burkart¹, M. W. Beets¹, S. Nelakuditi², E. A. Willis³, L. von Klinggraff¹, H. Parker¹, M. Bastyr¹, X. Zhu¹, Z. Zhong² and R. G. Weaver¹

Abstract

Background Objective measures of screen time are necessary to better understand the complex relationship between screen time and health outcomes. However, current objective measures of screen time (e.g., passive sensing applications) are limited in identifying the user of the mobile device, a critical limitation in children's screen time research where devices are often shared across a family. Behavioral biometrics, a technology that uses embedded sensors on modern mobile devices to continuously authenticate users, could be used to address this limitation.

Objective The purpose of this scoping review was to summarize the current state of behavioral biometric authentication and synthesize these findings within the scope of applying behavioral biometric technology to screen time measurement.

Methods We systematically searched five databases (Web of Science Core Collection, Inspec in Engineering Village, Applied Science & Technology Source, IEEE Xplore, PubMed), with the last search in September of 2022. Eligible studies were on the authentication of the user or the detection of demographic characteristics (age, gender) using built-in sensors on mobile devices (e.g., smartphone, tablet). Studies were required to use the following methods for authentication: motion behavior, touch, keystroke dynamics, and/or behavior profiling. We extracted study characteristics (sample size, age, gender), data collection methods, data stream, model evaluation metrics, and performance of models, and additionally performed a study quality assessment. Summary characteristics were tabulated and compiled in Excel. We synthesized the extracted information using a narrative approach.

Results Of the 14,179 articles screened, 122 were included in this scoping review. Of the 122 included studies, the most highly used biometric methods were touch gestures ($n=76$) and movement ($n=63$), with 30 studies using keystroke dynamics and 6 studies using behavior profiling. Of the studies that reported age (47), most were performed exclusively in adult populations ($n=34$). The overall study quality was low, with an average score of 5.5/14.

Conclusion The field of behavioral biometrics is limited by the low overall quality of studies. Behavioral biometric technology has the potential to be used in a public health context to address the limitations of current measures of screen time; however, more rigorous research must be performed in child populations first.

Systematic review registration The protocol has been pre-registered in the Open Science Framework database (<https://doi.org/10.17605/OSF.IO/92YCT>).

*Correspondence:

O. L. Finnegan
olf@email.sc.edu

Full list of author information is available at the end of the article



© The Author(s) 2024. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>. The Creative Commons Public Domain Dedication waiver (<http://creativecommons.org/publicdomain/zero/1.0/>) applies to the data made available in this article, unless otherwise stated in a credit line to the data.

Introduction

Screen time is a critical health behavior related to a variety of health outcomes in children [1–6]. Historically, measuring screen time has been reliant on self-report or proxy-report measures [7], due in part to the nature of digital media consumption (e.g., in-home computer and TV use). The introduction of mobile devices (tablets, smartphones) has substantially altered the landscape of digital media consumption, and these devices have become the favored media choice for children due to their portability, interactivity, and capacity to stream a wide range of content [8–11]. Self-report measures are of limited validity in assessing mobile screen use due to the intermittent and on-demand use of mobile devices, which hamper one's ability to retrospectively report screen time [7, 12, 13]. In addition to not being sensitive enough to sufficiently capture all mobile screen use, self-report measures are also subject to recall bias and social desirability bias [14, 15]. Given the proliferation of mobile devices [8, 10], there has been a growing demand to advance our current screen time measures to more effectively capture mobile screen use [16], specifically using objective measures [17].

Researchers have begun to use passive sensing applications (e.g., Chronicle) to overcome the limitations of subjective reports and which unobtrusively monitor mobile screen use on mobile devices [13, 18]. Chronicle is an Android passive sensing application that tracks the duration, frequency, and timing of data, general application type, and application status (foreground vs. background) using Google API every 15 s [13]. Benefits of passive sensing applications include a reduced researcher and participant burden compared to self-report measures and lower cost for researchers to employ. However, while this data can be relevant for tracking the duration of use and the context of use, these passive sensing applications are not able to capture who specifically is using the device. For child screen time research, this limitation in identifying the user of a device is of particular concern as mobile devices are often shared between siblings or between the parent and the child [12, 19]. Therefore, identifying the user of the device is critical to optimizing the potential for passive sensing methods in tracking objective screen use metrics in children.

Behavioral biometrics could be used to address this shortcoming of objective screen time measurement by identifying users of mobile devices. Modern mobile devices contain a variety of sensors (e.g., accelerometer, gyroscope, magnetometer, touch) that collect multiple data streams and can provide characteristic information about the user. These sensors provide the basis for behavioral biometric authentication [20–22]. Unlike physiological biometrics (e.g., fingerprint, iris, facial recognition),

behavioral biometrics do not require additional hardware in modern mobile devices [23, 24], making it a feasible research tactic for screen time measurement. Additionally, behavioral biometrics can provide continuous user authentication, whereas physiological biometrics are typically a one-time authentication for gaining access to a device [23]. There are several types of behavioral biometrics used for authentication, including behavior profiling, keystroke dynamics (typing dynamics), touch dynamics, and motion behavior [23]. Behavior profiling uses data such as the type of applications being used and battery life (host-based approach) as well as calls, texts, and GPS location (network-based approach) for user authentication [21]. This type of authentication has been used for fraud detection systems, in which unusual activities (e.g., calls, texts) and a new location can identify device theft and subsequently initiate a fraud protection mechanism [25]. Keystroke dynamics involves the characteristic way in which an individual types, specifically identifying the habitual typing pattern [21]. There are two types of keystroke dynamics, including static text, which analyzes a fixed text (e.g., a password), and dynamic text, which analyzes free-living text from participants [26]. Keystroke dynamics have largely been used for fraud detection and for authentication into computers or applications [26]. Touch dynamics, or touch gestures, evaluates touch strokes (size, length, speed, pressure, direction) and their corresponding coordinates on the touchscreen of a phone. Authentication using touch dynamics began as mobile devices were developed without a physical keyboard and rather a touchscreen [20]. Lastly, motion behavior authentication relies on the distinct movement patterns of individuals holding and interacting with a mobile device [27, 28].

Data produced by these sensors can be harnessed without additional hardware, evidenced by the growing body of research in the field of behavioral biometric authentication [21, 24, 29]. In child screen time research, employing continuous user identification may prove useful, especially when the device is being shared among a child and their family. Furthermore, applying behavioral biometric technology to screen time may be a relatively inexpensive solution, as it leverages built-in technology [24]. These benefits of behavioral biometrics are important attributes to consider when applying this technology to other contexts.

Behavioral biometric authentication is a highly established field of literature within cybersecurity; however, this technology has not yet been applied to objective screen time measurement research, to continuously identify the user of the mobile device [21, 30]. In order to begin applying this technology to screen time measurement, it is important to have an updated understanding

of behavioral biometric technology and fit this updated understanding within the perspective of screen time research. The purpose of this scoping review was to first summarize the current state of behavioral biometric authentication, including identifying the behavioral biometric methods and data streams used, the characteristics predicted, and the model evaluation metrics used. This review also sought to characterize these findings within the scope of applying behavioral biometric technology to address the critical limitations of current measures of screen time to provide future directions for applying this technology to a public health context.

Methods

This systematic review was conducted in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for Scoping Reviews (PRISMA-ScR) Checklist [31] and was pre-registered in the Open Science Framework database (<https://doi.org/10.17605/OSF.IO/92YCT>).

Information sources, search, and screening

Literature searches were conducted in Web of Science Core Collection, Inspec in Engineering Village, Applied Science & Technology Source, IEEE Xplore, and PubMed, all of which were selected for their relevance to the topic and database size. The final database search was conducted on September 19, 2022. All authors and collaborators discussed the search strategy and the query strings specific to each database. Searches used keywords: smart device, tablet, phone, smartphone, handphone, mobile, Android, iOS, sensor, accelerometer, gyroscope, magnetometer, touch, biometric, hand, motion, move, swipe, keystroke, detect, verify, authenticate, infer, predict, determine, and classify, with Boolean operators, wildcard, and truncation used. The comprehensive list of search terms with notation specific to each database can be found in Additional file 2: Supplementary Table 2. The primary author (OF) performed the initial search. The search yielded 6,161 results from Web of Science Core Collection, 11,181 results from Inspec, 787 from Applied Science & Technology Source, 3584 from IEEE Xplore, and 823 from PubMed, for a total of 22,537 studies. References were exported to EndNote (Clarivate, London, UK), where an initial duplicate screen was completed using the “remove duplicates” function. Following this, references were exported to Covidence (Melbourne, Australia) for title and abstract screening, where duplicates were also removed, bringing the total studies for title and abstract screening down to 14,179. The primary author (OF) and an additional research assistant screened the titles and abstracts of the 14,179 studies on Covidence. Both reviewers established quality control of their screening

process prior to independently screening the articles. This was done by screening 600 of the same articles independently and ensuring reviewers had consistency above 80%. Consistency between reviewers was met (99.9%) and then reviewers divided the remaining articles and independently screened the title and abstracts of those articles. Following title and abstract screening, 13,972 articles were excluded, and 207 articles were left for full text retrieval and screening. Four articles were not able to be located using the Interlibrary Loan (ILL) service; therefore, 203 articles were retrieved for eligibility assessment. The primary author (OF) reviewed the full texts of the 203 articles to assess whether these articles fully met the predefined inclusion and exclusion criteria. Of the 203 articles, 122 articles were considered eligible for inclusion and were extracted (Fig. 1).

Eligibility criteria

Studies were required to focus on the sensors of mobile devices, defined as tablets or smartphones [32]. These sensors needed to be built-in to the device, including but not limited to motion sensors, accelerometer, gyroscope, magnetometer, and touch. Studies were eligible if they used these sensors for verification, detection, and/or authentication of the device user. Using an adapted version of the Meng 2015 [23] framework of biometric authentication, articles were required to focus on behavior profiling, keystroke dynamics (typing dynamics), touch dynamics, or motion behavior. Because the first smartphone (i.e., iPhone) was released in 2007 [33], and modern mobile tablets were developed after this in 2010, only articles after 2007 were included. Articles in a peer-reviewed academic source and published in English were eligible for inclusion. Articles that simulated data and did not collect data on human participants were excluded. Studies were excluded if they used other technology and/or required additional equipment beyond the mobile device (e.g., sensor glove, stylus) for verification. These articles were excluded because of their limited applicability to screen time measurement, as the goal of applying this technology would be to capture the typical way in which the child is interacting with their shared device. Articles that evaluated smart watches, fitness tracking devices, or wearable sensors were excluded. These articles were excluded because the tablet and smartphone are the preferred choice for digital media consumption in children [34] and are more closely related to health outcomes (e.g., sleep) [35]. Lastly, while the purpose of this review was to characterize these findings within the lens of child screen time measurement, we did not limit our search to only include studies on children. We included studies on adult populations since it is a relatively newer field and area of application to children and to inform

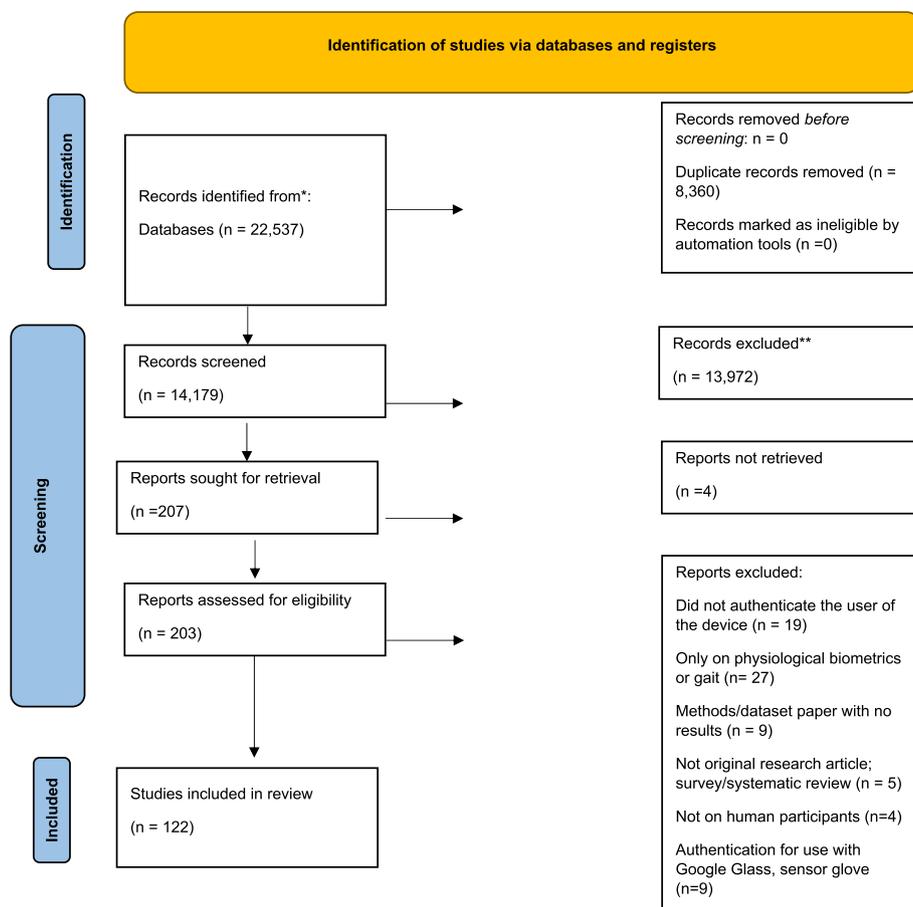


Fig. 1 PRISMA flowchart

future research on child populations from the current literature on adult biometric authentication.

Data extraction

The primary author (OLF) extracted study characteristics (sample size, age, gender), data collection methods, data stream, model evaluation metrics, and performance of models from the 122 studies. All extracted data was reviewed by a second author (RGW).

Study characteristics

The extraction of study characteristics included details on the sample population, including sample size, gender distribution (number of female participants), and age (mean, standard deviation, and range). There were studies in this review that used freely available dataset(s) for their sample ($n = 27$), with several studies compiling data from more than one dataset ($n = 8$). Studies that used publicly available datasets for their sample are presented with a superscript letter in Table 1. Each superscript letter refers to a specific database, with several repeating

databases used across studies, as depicted in Table 1. For studies using more than one dataset for their sample, sample sizes of the datasets were pooled, and number of female participants (gender distribution) were pooled. Additionally, for studies that used more than one dataset, we compiled the age ranges into one comprehensive age range across all included datasets. Device brand (iOS or Android) and outcome predicted (identity, age, or gender) were also extracted from the studies. The protocol of each study included was evaluated to determine whether it was a free-living or in-lab protocol. We defined in-lab protocols as those completed in a researcher-supervised controlled setting, while free-living refers to protocols in which participants use the device in their typical environment (e.g., home, work). Furthermore, we extracted whether the protocol was structured or free-use. We defined structured protocols as those in which the researchers give the participant a specific task to complete on the device, such as a questionnaire, a game, or using a particular application. Free-use protocols refer to protocols in which the participant can interact with the

Table 1 Characteristics of included studies

Study Details		Sample population			Authentication		Study setting	
First author, year	Citation	Sample size	Female (n)	Age range	Device brand	Outcome predicted	Free-living vs. in-lab	Structured vs. free-use
Davis, 2020	[36]	48	21	< 40, > 40*	iOS	Sex, age	In-lab	Structured
Sun, 2016	[37]	19	8	18–35	Android	ID	In-lab	Structured
Liu, 2016	[38]	20	10	NR	Android	ID	In-lab	Structured
Maghsoudi, 2016	[39]	60	NR	NR	Android	ID	In-lab	Structured
Putri, 2016	[40]	29	NR	NR	Android	ID	In-lab	Structured
Lamiche, 2019	[41]	20	10	22–33	Android	ID	In-lab	Structured
Smith-Creasey, 2016	[42]	50	NR	NR	iOS	ID	In-lab	Free-use
Shih, 2015	[43]	10	4	22–30	Android	ID	In-lab	Structured
Zaidi, 2022 ^{a,b,c,d}	[44]	350	NR	NR	Android	ID	In-lab	Structured
Soni, 2018	[45]	10	NR	NR	Android	ID	In-lab	Structured
Lin, 2012	[46]	20	4	18–40	Android	ID	In-lab	Structured
Li 2018	[47]	304	NR	NR	NR	ID	Free-living	Free-use
Smith-Creasey, 2019 ^{e,f,g}	[48]	49	NR	NR	Android	ID	Free-living	Free-use
Salem, 2019	[49]	7	NR	NR	Android	ID	In-lab	Structured
Zhao, 2020	[50]	110	NR	NR	iOS	ID	In-lab	Structured
Qiao, 2015	[51]	10	NR	NR	Android	ID	In-lab	Structured
Smith-Creasey, 2019	[52]	20	NR	NR	Android	ID	In-lab	Structured
Alariki, 2016	[53]	18	NR	20–40	Android	ID	In-lab	Structured
Lee, 2017	[54]	12	NR	NR	Android	ID	In-lab	Structured
Li, 2020 ^h	[55]	150	58	16–50	Android	ID	In-lab	Structured
Saini, 2020	[56]	40	NR	NR	NR	ID	In-lab	Free use
Takahashi, 2016	[57]	20	4	NR	Android	ID	In-lab	Structured
Deb, 2019	[58]	37	16	18–56	Android	ID	Free-living	Free-use
Leingang, 2018 ⁱ	[59]	100	NR	NR	NR	ID	In-lab	Structured
Acien, 2019 ^j	[60]	119	NR	3–6, < 25*	Android	ID	In-lab	Structured
Mahbub, 2016	[61]	48	NR	NR	Android	ID	Free-living	Free-use
Guarino, 2022	[62]	147	52	7–59	Android	Gender	In-lab	Structured
Wang, 2019 ^q	[63]	21	NR	20–30	Android	ID	In-lab	Structured
Davarci, 2017	[64]	200	NR	3–11, 12–50	Android	Age	In-lab	Structured
Chakraborty, 2019 ^{k,l,m}	[65]	60	NR	19–48	Android	ID	In-lab	Structured
Antal, 2015	[66]	42	18	20–46	Android	ID	In-lab	Structured
Roy, 2014 ⁿ	[67]	41	13	10–69	Android	ID	In-lab	Structured
Salem, 2016	[68]	5	NR	NR	Android	ID	In-lab	Structured
Roy, 2019 ^q	[69]	746	476	NR	Android	ID	In-lab	Structured
Lee, 2021	[70]	6	NR	NR	NR	Handedness	In-lab	Structured
Buriro, 2019	[71]	85	30	20–60	Android	ID	Free-living	Structured
Praher, 2016	[72]	8	NR	23–55	Android	ID	In-lab	Structured
Baran, 2019 ^o	[73]	12	NR	NR	NR	ID	In-lab	Structured
Ali, 2016	[74]	6	3	NR	NR	ID	In-lab	Structured
Guerra-Casanova, 2012 ^{o,p}	[75]	125	NR	NR	NR	ID	In-lab	Structured
Primo, 2017	[76]	27	NR	< 27*	Android	ID	In-lab	Structured
Yang, 2019	[77]	45	19	10–55	Android	ID	NR	NR
Wolff, 2013	[78]	6	NR	NR	NR	ID	Free-living	Free-use
Tse, 2019	[79]	31	NR	NR	NR	ID	In-lab	Structured
Antal, 2015 ^{q,r,s}	[80]	120	54	20–49	Android	ID	In-lab	Structured
Laghari, 2016	[81]	10	NR	NR	Android	ID	In-lab	Structured
Tolosana, 2019	[82]	93	31	17–27*	Android	ID	In-lab	Structured
Ray, 2021	[83]	49	23	18–35 +	Android	ID	In-lab	Structured
Ambol, 2020	[84]	5	NR	NR	NR	ID	In-lab	Structured
Garbuz, 2019	[85]	36	NR	NR	NR	ID	In-lab	Structured
Dybczak, 2022	[86]	5	NR	NR	Android	ID	In-lab	Structured
Mumuria, 2015	[87]	73	NR	NR	Android	ID	In-lab	Free-use
Karanikiotis, 2020	[88]	2221	NR	NR	NR	ID	In-lab	Structured

Table 1 (continued)

Study Details		Sample population			Authentication		Study setting	
First author, year	Citation	Sample size	Female (n)	Age range	Device brand	Outcome predicted	Free-living vs. in-lab	Structured vs. free-use
Zhao, 2013	[89]	30	NR	NR	Android	ID	In-lab	Structured
Zhao, 2017	[90]	23	9	NR	Android	ID	Free-living	Free-use
Leyfer, 2019	[91]	14	NR	NR	Android	ID	Free-living	Free-use
Herath, 2022	[92]	3	NR	NR	NR	ID	NR	NR
Kumar, 2017	[93]	57	NR	NR	Android	ID	In-lab	Free-use
Barlas, 2020	[94]	30	11	NR	Android	ID	NR	NR
Incel, 2021	[95]	45	NR	18–42	Android	ID	In-lab	Structured
Hernandez-Ortega, 2017 ^j	[96]	119	62	Children: 3–6, adults: < 25 [†]	Android	ID	In-lab	Structured
Nguyen, 2017	[97]	20	6	20–30	Android	ID	In-lab	Structured
Al-Showarah, 2019	[98]	42	NR	Elderly: 60+, younger: 20–39	Android	Age group	In-lab	Structured
Ng'ang'a, 2020	[99]	12	6	6 < 35, 6 < 35	NR	ID	In-lab	Structured
Ray-Dowling, 2022 ^l	[100]	100	NR	NR	Android	ID	In-lab	Structured
Burro, 2017	[101]	95	20	20–60	Android	ID	In-lab	Structured
Ouadjer, 2021 ^a	[102]	41	13	10–69	Android	ID	Free-living	Free-use
Suharsono, 2020	[103]	50	NR	18–40	Android	ID	In-lab	Structured
Barra, 2018	[104]	38	NR	NR	Android	ID	In-lab	Structured
Mallet, 2022 st	[105]	102	NR	NR	NR	ID	In-lab	Structured
Abate, 2019	[106]	100	NR	NR	Android	ID	In-lab	Structured
Cheng, 2020	[107]	100	41	Children: 3–17, adults: 18–59	Android	Age	In-lab	Structured
Alqarni, 2020	[108]	26	12	NR	Android	ID	In-lab	Structured
Rao, 2013	[109]	5	NR	NR	NR	ID	In-lab	Structured
Coakley, 2016	[110]	52	NR	NR	Android	ID	In-lab	Structured
Gautam, 2017	[111]	7	NR	NR	Android	ID	NR	NR
Deng, 2015 ^u	[112]	55	NR	NR	Android	ID	In-lab	Structured
Roh, 2016	[113]	> 15 [*]	NR	NR	Android	ID	In-lab	Structured
Acien, 2019 ^v	[114]	48	12	22–31	NR	ID	Free-living	Free-use
Sun, 2021	[115]	26	17	30–63	NR	ID	Free-living	Free-use
Peralta, 2013	[116]	8	4	24–33	NR	ID	In-lab	Structured
Stragapede, 2022 ^w	[117]	600	197	< 20–50	NR	ID	Free-living	Structured
Liang, 2020	[118]	20	12	10– > 59	Android	ID	Free-living	Free-use
Li, 2021	[119]	19	NR	NR	NR	ID	In-lab	Structured
Corpus, 2016	[120]	30	NR	NR	NR	ID	In-lab	Structured
Akhtar, 2017	[121]	150	NR	NR	Android	ID	Free-living	Structured
Song, 2017	[122]	161	26	18–55	Android	ID	In-lab	Structured
Primo, 2015	[123]	34	NR	< 25 [†]	Android	ID	In-lab	Structured
Phillips, 2016	[124]	4	NR	NR	iOS	ID	In-lab	Structured
Li, 2016	[125]	42	NR	NR	Android	ID	In-lab	Structured
Haberfield, 2021	[126]	33	5	19–69	Android	ID	In-lab	Structured
Tharwat, 2019	[127]	51	25	NR	NR	ID	In-lab	Structured
Tang, 2022	[128]	10	NR	20–25	NR	ID	In-lab	Structured
Mahfouz, 2017	[129]	52	NR	NR	Android	ID	In-lab	Structured
Hernandez-Ortega, 2017 ^j	[130]	119	62	Children: 3–6, adults: < 25	Android	Age	In-lab	Structured
Miguel-Hurtado, 2016 ^x	[131]	116	59	18–35	Android	Sex	In-lab	Structured
Wang, 2020 ^y	[132]	100	NR	20–30	NR	ID	NR	NR
Inguanez, 2016	[133]	32	10	NR	Android	ID	In-lab	Structured
Zhu, 2017	[134]	20	5	18–43	Android	ID	Free-living	Structured
Cheng, 2013	[135]	100	NR	NR	Android	ID	Free-living	Free-use

Table 1 (continued)

Study Details		Sample population			Authentication		Study setting	
First author, year	Citation	Sample size	Female (n)	Age range	Device brand	Outcome predicted	Free-living vs. in-lab	Structured vs. free-use
Gunn, 2018 ^d	[136]	100	NR	NR	NR	ID	Free-living & in-lab	Free-use and structured
Wang, 2021	[137]	11	NR	NR	Android	ID	In-lab	Structured
Abate, 2016	[138]	100	NR	NR	Android	ID	In-lab	Structured
Acién, 2020 ^w	[139]	600	197	< 20– > 50 [*]	Android	ID	In-lab	Structured
Anusas-Amornkul, 2019	[140]	20	NR	NR	Android	ID	In-lab	Structured
Temper, 2016	[141]	25	9	19–65	Android	ID	Free-living	Structured
Roy, 2019	[142]	92	NR	7–65	Android	Age, Gender	In-lab	Structured
Shrestha, 2016	[143]	20	3	25–35	Android	ID	In-lab	Structured
Cascone, 2022 ^{y,z,2}	[144]	243	148	7–65	Android	Gender, Age	In-lab	Structured
Temper, 2015	[145]	22	NR	15–60	Android	ID	In-lab	Structured
Frank, 2013	[146]	41	7	10–69	Android	ID	In-lab	Structured
Wantanabe, 2013	[147]	5	NR	NR	iOS	ID	In-lab	Structured
Volaka, 2019 ⁱ	[148]	100	NR	NR	Android	ID	In-lab	Structured
Brown, 2020	[149]	1	NR	NR	Android	ID	In-lab	Structured
Sharma, 2017	[150]	42	NR	NR	Android	ID	In-lab	Free-use
Kroeze, 2016	[151]	30	NR	NR	Android	ID	In-lab	Free-use
Filippov, 2018	[152]	21	NR	NR	NR	ID	In-lab	Free-use
Karakaya, 2019 ^j	[153]	100	NR	NR	NR	ID	In-lab	Structured
Serwadda, 2013	[154]	190	NR	NR	Android	ID	In-lab	Structured
Buriro, 2016	[155]	30	8	NR	Android	ID	In-lab	NR
Shen, 2016	[156]	48	19	18–50	Android	ID	In-lab	Structured
Stylios, 2022	[157]	39	NR	NR	Android	ID	In-lab	Structured

NR not reported

^a Frank dataset

^b Serwadda dataset

^c Antal dataset

^d Mabhub dataset

^e SHR dataset

^f MSC dataset

^g GCU dataset

^h Article encompassed two studies

ⁱ H-MOG dataset

^j Vatavu dataset

^k UCAI-HAR dataset

^l UT-Data-Complex dataset

^m shoiab dataset

ⁿ gesture dataset

^o GBS2GestureDB1 database

^p GB2SGestureDB2 database

^q Dataset_11f

^r Dataset_8f

^s Dataset_3f

^t Bioldent dataset

^u Stanford TapDynamics dataset

^v UMDAA-02 dataset

^w HuMldb dataset

^x SSD dataset

^y RHU dataset

^z KDAP dataset

^{*} Study did not provide further details on age range

² TDAS dataset

device in their normal manner and select which applications they use, with no restrictions from the researchers.

Methods

Extraction of study characteristics also included identifying the biometric method(s) employed for authentication of the user and/or detection of demographic characteristics. We first recorded the biometric method described by each study in the precise language used by the authors. Given the lack of standardized terminology in the field of biometric authentication, these methods needed to be condensed into broader categories. The categories for biometric methods were consolidated into four categories, with agreement from all authors. These categories included *movement* (encompassing hand movement, arm gesture, hand gesture, and posture), *behavior profiling*, *keystroke dynamics*, and *touch gestures*.

Data stream

Extraction of study characteristics also included the identification of the specific data stream(s), or sensors, used for biometric authentication. We first recorded the data stream(s) used in each study using the precise language used by the authors. Similar to categorizing biometric methods, the categories for data streams also needed to be condensed to broader categories of similar characteristics. These categories included *accelerometer* (gravity, linear acceleration), *orientation*, *gyroscope* (rotation, angular velocity), *touch*, *location*, *magnetometer*, and *other* (ambient light, Bluetooth, temperature, proximity, application usage, power).

Model evaluation metrics

Extraction of study characteristics also included identifying the model evaluation metric(s) used in each study. We first identified the evaluation metric described in each study using the precise language used by the authors. Metrics were condensed into broader categories given the lack of consistent terminology in machine learning model performance metrics. These categories included *area under the curve* (receiver operating characteristic), *equal error rate* (EER), *precision*, *recall* (sensitivity, true acceptance rate, true positive rate), *false rejection rate* (FRR, false negative rate), *false acceptance rate* (FAR, false positive rate, “false alarm rate”), *accuracy* (correct recognition rate, mean recognition rate, success rate), *F1 score* (F-measure), and *other* (kappa, root mean square error H-mean, detection error tradeoff curve, specificity/true rejection rate, average match rate, mean square error rate, average number of impostor actions, and average number of genuine actions).

Quality assessment

The quality of the included studies was assessed using an adapted framework from Papi 2017 [158], which is a research quality scale specific to the field of engineering with a focus on sensor technology (Additional file 1: Supplementary Table 1). The primary author (OLF) assessed the study quality of all 122 studies. Each question was scored as either 1, meeting the criteria, or 0, not meeting the criteria. Composite quality assessment scores were calculated by adding together the number of criteria met, with a score of 14 meaning that the study was of highest quality and a score of 0 meaning that the study was of lowest quality.

Data analysis

The characteristics of the included studies were tabulated in Excel (Microsoft, Version 2304). We then compiled summary statistics in Excel to describe our findings. Means and standard deviations were calculated for sample size and gender distribution across all studies.

Results

Study characteristics

Across all 122 studies, sample sizes ranged from 1 to 2221 participants, with an average of 89 participants per study (± 224.2). Android was the most common operating system, with 89 studies (73%) using Android devices for their protocol(s). The iOS operating system was used in 5 (4%) of protocols and the remaining 28 studies (23%) did not report the operating system used. Most of the studies ($n = 112$, 92%) identified the specific user of the device, while 5 (4%) studies aimed to detect the gender of the user and 7 studies (6%) aimed to detect the age/age group of the user. For the study setting, most study protocols were conducted in a lab setting ($n = 99$, 81%), while fewer studies were carried out in a free-living environment ($n = 17$, 14%), one study used both lab and free-living settings, and 5 studies (4%) did not provide sufficient information to determine study setting. Most protocols were structured ($n = 96$, 79%), with specific guidance and directions given to the participants on how to interact with the device (e.g., playing a game, watching a specific video). Few studies ($n = 19$, 16%) allowed participants to interact with the device in their normal manner, considered “free use” of the device, one study had both structured and free-use, and 6 studies (5%) did not provide sufficient information to determine protocol format. Many studies did not report demographic characteristics of the sample; 75 (61%) did not report gender, 70 (57%) did not report age, and none reported race/ethnicity. Of those that did report gender, on average, the distribution of female participants was 39% of the sample. Of the 122

studies, 75 studies (61%) did not report an age range, 34 studies (28%) had a sample of adults, and 13 studies (11%) had age ranges that included children (< 18 years).

Methods

Of the 122 studies included in this review, 63 (52%) used movement (e.g., hand movement, hand or arm gesture and posture) as their biometric method for authentication. Thirty studies (25%) used keystroke dynamics for biometric authentication, while 76 studies (62%) used touch gestures. Behavior profiling, such as app usage, battery, and WiFi, was used in 7 studies (6%) for biometric authentication.

Data stream

Touch was the most extensively used data stream, with 93 studies using touch behavior for biometric authentication. The accelerometer sensor was the second most frequently used sensor of this review, with $n = 68$ studies (56%). Other data streams employed include gyroscope ($n = 46$ studies, 38%), orientation ($n = 9$ studies, 7%), location ($n = 8$ studies, 7%), and magnetometer ($n = 22$ studies, 18%). As depicted in Additional file 3: Supplementary Table 3, all other data streams that were used in less than 3 studies were combined into an “Other” category. These included ambient light ($n = 3$, 2%), Bluetooth ($n = 3$, 2%), temperature ($n = 1$), proximity ($n = 3$, 2%), application usage ($n = 1$), power/battery level ($n = 2$), motion quaternion ($n = 1$), directional heading ($n = 1$), and heat map ($n = 1$).

Model evaluation metrics

When evaluating the performance of their models, the included studies used a wide range of evaluation metrics. Equal error rate (EER) and accuracy were the most highly used evaluation metrics, with 57 studies (47%) using EER and 56 studies (46%) using accuracy. Following EER and accuracy, false rejection rate (FRR) ($n = 42$ studies, 34%) and false acceptance rate (FAR) ($n = 47$ studies, 39%) were also highly used to evaluate model performance. Area under the curve (AUC) and the receiver operating characteristic curve (ROC) were used in 20 studies (16%). Recall/sensitivity ($n = 20$, 16%), F1 score ($n = 14$, 11%), and precision ($n = 10$, 8%) were also frequently used among the included studies. As depicted in Additional file 3: Supplementary Table 3, all other model evaluation metrics that were used in less than 4 studies were combined into an “Other” category. These included kappa ($n = 2$), root mean square error (RMSE) ($n = 1$), H-mean ($n = 1$), detection error tradeoff (DET) curve ($n = 4$, 3%), specificity/true rejection rate ($n = 3$), average match rate ($n = 1$), mean square error rate ($n = 1$), average number of impostor

actions (ANIA) ($n = 2$), and average number of genuine actions (ANGIA/ANGA) ($n = 2$).

Quality of the included studies

The average quality score of the included studies was 5.5 out of 14, with a high score of 11 and a low score of 3. The most commonly met criteria were #11, reporting main outcomes, with 122 out of 122 studies meeting this criterion, and #1, clearly stating research objectives, with 121 out of 122 studies meeting this criterion. Most studies also met the criteria for #12, reporting the main findings ($n = 119$ studies), and for #13, clearly describing and justifying the statistical tests ($n = 118$ studies). The selection of sensors (#9) was appropriately justified in 65 studies, while data handling was clearly described (#10) in 35 studies. Only some studies met the criteria for #14, clearly describing the limitations ($n = 33$), or met the criteria for #8, clearly describing the equipment design ($n = 23$). Few studies of this review met the criteria for #3, adequately describing the study population ($n = 19$), as many did not report demographic characteristics such as age and gender. Only 8 out of the 122 studies met the criteria for #5, appropriately describing the sampling methodology, and only 7 out of the 122 studies met the criteria for #7, providing detailed methods that could be replicated. None of the included studies met the criteria for #4, specifying eligibility criteria, and for #6, providing a rationale for the sample size.

Discussion

Behavioral biometrics have the potential to improve screen time measurement because researchers can capitalize on built-in mobile device sensors to determine who is using the device at specific time points to address a critical limitation in child screen time research. This scoping review sought to summarize the current state of behavioral biometric authentication, including identifying the behavioral biometric methods used, the data streams used, the characteristics predicted, and the model evaluation metrics used. On a larger scale, this updated understanding of the methodology of behavioral biometric studies can inform future research applying this technology to a public health context.

Overall, in the 122 included studies, the most highly used behavioral biometric methods were touch gestures and movement. The most highly used data streams for behavioral biometric authentication were touch and accelerometry. Motion sensors, such as accelerometer, gyroscope, and magnetometer, are straightforward to access and record with a sensor tracking application (e.g., Sensor Log) on mobile devices. Using touch sensors presents more challenges, both in terms of accessing this sensor stream as well as the privacy and

security concerns of participants. Several of the studies using touch in this review used their own gaming application that only tracked touch behavior while the participant was using the application, which has limited applicability to screen time measurement, as it only records touch behavior during the use of one application. In addition to challenges in accessing this sensor stream, there are privacy concerns, as research participants may not feel comfortable with sensor data from their devices being collected continuously. While collecting motion behavior may not be as much of a concern, there may be a particular concern in tracking touch sensor data when using banking applications or typing passwords (e.g., concerns in researchers deciphering passwords). Therefore, while touch is a highly used behavioral biometric method, it may have more limited applicability to screen time measurement when compared to motion sensors (e.g., accelerometer, gyroscope, magnetometer).

Most behavioral biometric authentication studies in this review aimed to identify the user of the device, with fewer studies aiming to detect demographic characteristics, such as age and gender. Studies that used behavioral biometrics to detect age were designed to tailor technology interfaces towards children (e.g., widget layout) and to improve parental control options. Similarly, in studies examining the ability of behavioral biometrics to determine gender, their objective was to adapt interfaces to be more relevant for the user. Based on current evidence, behavioral biometrics are less accurate at detecting demographic characteristics compared to detecting a unique user [159]. It is likely more challenging to identify similar characteristics in user behavior across a group of individuals, as user interaction can vary substantially on an inter-individual level [60, 159]. Relative to applied screen time measurement in a public health context, detecting the age of the user may be a relevant finding to distinguish between the parent and the child when they are sharing the device. However, the ability to detect only the age of a user would not be as useful when a child shares a device with a sibling of a similar age. Thus, determining the unique identity of a user of the device rather than demographic characteristics would be more relevant for research purposes.

Furthermore, of the included studies, a majority of studies used samples of adult participants, with fewer studies tested on samples of children. The lack of research on children highlights a gap in the literature, as there are inherent behavioral differences in the ways in which children interact with mobile devices compared to adults [159] (e.g., children are more active), and findings from adult studies cannot be universally applied to children. Therefore, we need additional research on biometrics

among children before applying this technology to measure children's screen time.

The most popular model evaluation metrics used in the included studies were equal error rate (EER), accuracy, false acceptance rate (FAR), and false rejection rate (FRR). There were a wide range of model evaluation metrics used across studies, with several reporting the same metric under different terms. For example, several studies used the term "Correct Recognition Rate," instead of accuracy and "False Positive Rate" instead of false acceptance rate. This highlights a lack of standardization in terminology that is consistent across the field of behavioral biometric authentication, which limits our ability to compare findings across studies.

Of the studies included in this review, the average study quality was low (5.5/14), highlighting the lack of proper reporting in many of the studies in the field of behavioral biometric authentication. Overall, most authors did not provide sufficient information on equipment design, study population, sampling methodology, and eligibility criteria. Very few authors provided adequate justification for their sample size. The insufficiency in reporting key elements of study design limits the ability to replicate these findings in other samples and contexts. Furthermore, the lack of standardization in the terminology used across studies hampers the ability to make larger conclusions on the efficacy of behavioral biometrics and their application in the measurement of children's screen time.

Behavioral biometric tools and innovative directions for future research

Though the purpose of this review is to examine the current scope of literature on behavioral biometrics through the lens of its application to public health (i.e., screen time measurement), it is necessary to also distinguish this from the domain of behavioral biometrics research for security. Given the vast amount of sensitive information stored on mobile devices, secure user authentication has become a prominent concern and a highly studied concept over recent years [22, 160, 161]. User authentication has shifted from "what you know," such as an ID, PIN, or password, to "what you are," or biometric authentication, with behavioral biometrics referring to the specific user-device interaction. A specific framework developed by Bo and colleagues in 2013, SilentSense, provides a touch-based biometrics model that leverages touch events from the system API [162, 163]. This tool additionally integrated movement into its scheme, presenting a multi-modal authentication method. Another more recent development in behavioral biometrics is the generation of behavioral biometric datasets using engaging tools [164, 165]. There have been challenges in collecting biometric data on participants due to the long protocols necessary to capture sufficient amount

of data [164]. Therefore, researchers have developed gaming applications that collect a variety of behavioral biometric data (e.g., keystroke dynamics, touch gestures, motion) [164, 165]. BrainRun, developed by Papamichail and colleagues, is a cognitive skills gaming application that collects touch data. BioGames, developed by Stylios and colleagues, is also a gaming application that collects touch, motion, and keystroke data [164]. These applications are important tools in the feasible generation of large-scale behavioral biometric data. Lastly, a challenge within behavioral biometrics research is the power usage concerns on mobile devices, particularly for continuous authentication methods. In future behavioral biometrics research, power consumption of individual applications should be monitored to ensure that the authentication application is not substantially impacting the device battery. Power consumption of individual applications can be monitored using a method from Murmura and colleagues that uses per-subsystem time shares from the operating system, which can provide clarity on the feasibility of deploying behavioral biometric methods in a larger research context [166].

Advantages and disadvantages of the behavioral biometric methods

As these behavioral biometric methods have been highly studied and applied for use within the field of cybersecurity, this work has highlighted some of the advantages and disadvantages associated with each of these methods. While all methods are subject to privacy concerns [30], behavior profiling in particular has been scrutinized for its reliance on sensitive and private data (e.g., calls, texts, location). However, an advantage of behavior profiling is that unlike other methods (e.g., keystroke dynamics), it does not require the user to perform a specific activity for authentication [25]. A disadvantage of keystroke dynamics is that its accuracy for user authentication can be impacted by factors including injury, psychological state (e.g., stress), and distraction [167]. Additionally, the way in which an individual types on a keyboard is considered less permanent than other traits, such as physiological biometrics (e.g., facial and fingerprint recognition) [167]. However, relative to other authentication methods, keystroke dynamics is relatively low cost and does not rely on external hardware. Additionally, the way in which an individual types is challenging to replicate; therefore, this method can detect impostors more effectively [167]. An advantage of touch dynamics authentication is that the user does not need to complete a specific task for authentication; rather, this method works continuously in the background [20]. However, a disadvantage could be identifying the most salient features for user authentication, as using a large number of touch features increases

data size and subsequently can slow down authentication speed [23]. Lastly, motion authentication can be impacted by behavioral variability, as this type of authentication is reliant on the user to interact with the device similarly over time [168]. However, similar to other methods, motion authentication can be an unobtrusive authentication method [168], and there may be less privacy concerns compared to touch-based authentication.

Methodological considerations and implications for future research

Subsequent research should examine the effectiveness of behavioral biometrics to determine the user of the device among children across development. Most of the studies included in this review exclusively used adult samples, which has limited applicability to child screen time research. The present review also highlighted the lack of studies being done on iOS devices (iPhone, iPad) in the field of behavioral biometrics. This is a limitation of the field because iOS use is highly prevalent, as 55% of tablets in the USA are iPads [169]. In 2022, over 50% of smartphone owners in the USA used an iPhone, surpassing Android for the first time in history [170]. A majority of the studies ($n = 85$) tested Android devices, with only 5 studies using an iOS operating system, warranting further testing on a diversity of devices, including both iOS and Android.

When applying this technology to objective screen time measurement, participants may be apprehensive about researchers tracking mobile device usage data. However, there are practices in place to reduce concerns with tracking technology. Specifically with the passive-sensing application Chronicle, data are not associated with IP addresses or phone numbers and only indicate the type of application used (e.g., educational, social media), not the information on websites visited or the content of messages and emails. Parents are comfortable with using passive sensing technology when participating in a research study, as indicated by a feasibility study reporting no dropouts due to privacy concerns in using this technology [171]. While passive sensing applications have been shown to be accepted for use by families, future research can examine the extent to which families are comfortable with sensor tracking technology (e.g., accelerometer, gyroscope, touch) continuously monitoring user behavior on shared mobile devices. Prior to employing this technology in screen time measurement on a large scale, a necessary first step is to determine the feasibility and acceptability of this technology for families participating in research.

Additionally, research using this technology to measure screen time should consider the storage and battery life concerns inherent to using mobile device usage data. The computational burden of running applications

to track sensor data may impact the feasibility of longitudinally monitoring screen time behavior in children [30]. Selecting the appropriate sensor tracking application and sampling frequency to use, as well as only recording sensor data when the device is unlocked must be a priority for researchers using behavioral biometric technology for screen time research [159].

Lastly, within the field of behavioral biometric authentication, there is a necessity to standardize the terminology used to describe various elements of behavioral biometrics. The lack of uniform language needs to be addressed to apply this technology on a larger scale. A way in which the field of behavioral biometrics can move towards more cohesive language is by adopting best-practice guidelines for reporting performance metrics, similar to the fields of physical activity measurement [172] and sleep measurement [173].

The present review has several strengths, including a comprehensive review of the current state of behavioral biometric authentication. This provided an updated evaluation of the most highly used behavioral biometric methods, data streams, and model evaluation metrics. The current review is limited by the low quality of the included studies and the lack of consistency in the terminology used across studies. Given the lack of standardization in model evaluation metrics, we were unable to sum results across studies and use meta-analytic methods to evaluate the overall efficacy of behavioral biometrics in identifying the user of a device. Furthermore, a limitation of the current review is the narrow focus on behavioral biometrics (touch, accelerometry, behavioral profiling) and not including studies on physiological biometrics. While physiological biometrics presents an important tool in authentication, these sensors (e.g., camera, video) are not freely available and feasible to use in public health research. Despite these limitations, behavioral biometric technology highlights a window of opportunity, as it shows the initial potential to harness sensor data to identify the user of a device. This review can inform future research applying behavioral biometric technology to contexts outside of cybersecurity and to address the limitations of objective measures of screen time.

Supplementary Information

The online version contains supplementary material available at <https://doi.org/10.1186/s13643-024-02451-1>.

Additional file 1: Supplementary Table 1. Quality Assessment Framework.

Additional file 2: Supplementary Table 2. List of Search Terms.

Additional file 3: Supplementary Table 3. Data Stream, Biometric Methods & Model Evaluation Metrics of Included Studies.

Additional file 4: Table 2. Quality Assessment of Included Studies.

Acknowledgements

None.

Authors' contributions

RGW secured funding. OLF, RGW, and BA conceptualized the idea. OLF secured articles and completed data extraction. All authors assisted with data interpretation. OLF and RGW drafted the manuscript. All authors read, provided substantive feedback, and approved the final manuscript.

Funding

This publication was made possible in part by Grant Number T32-GM081740 from NIH-NIGMS. Research reported in this publication was also supported in part by the National Institute of Diabetes and Digestive and Kidney Diseases Award Number R01DK129215. Co-author White was supported in part by the National Institute of Diabetes and Digestive and Kidney Diseases Award Number F31DK136205. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the NIGMS or NIH.

Availability of data and materials

Not applicable; no datasets were generated or analyzed during the current study.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Author details

¹Department of Exercise Science, University of South Carolina, Columbia, USA. ²Department of Computer Science and Engineering, University of South Carolina, Columbia, USA. ³Center for Health Promotion and Disease Prevention, University of North Carolina Chapel Hill, Chapel Hill, USA.

Received: 22 August 2023 Accepted: 3 January 2024

Published online: 08 February 2024

References

- Domingues-Montanari S. Clinical and psychological effects of excessive screen time on children: effects of screen time on children. *J Paediatr Child Health*. 2017;53(4):333–8. <https://doi.org/10.1111/jpc.13462>.
- Liu W, Wu X, Huang K, et al. Early childhood screen time as a predictor of emotional and behavioral problems in children at 4 years: a birth cohort study in China. *Environ Health Prev Med*. 2021;26(1):3. <https://doi.org/10.1186/s12199-020-00926-w>.
- Saunders TJ, Vallance JK. Screen time and health indicators among children and youth: current evidence, limitations and future directions. *Appl Health Econ Health Policy*. 2017;15(3):323–31. <https://doi.org/10.1007/s40258-016-0289-3>.
- Tezol O, Yildiz D, Yalcin S, et al. Excessive screen time and lower psychosocial well-being among preschool children. *Arch Pediatr*. 2022;29(1):61–6. <https://doi.org/10.1016/j.arcped.2021.10.003>.
- Webster EK, Martin CK, Staiano AE. Fundamental motor skills, screen-time, and physical activity in preschoolers. *J Sport Health Sci*. 2019;8(2):114–21. <https://doi.org/10.1016/j.jshs.2018.11.006>.
- Muppalla SK, Vuppalapati S, Reddy Pulliahgaru A, Sreenivasulu H. Effects of excessive screen time on child development: an updated review and strategies for management. *Cureus*. <https://doi.org/10.7759/cureus.40608>. Published online June 18, 2023.
- K. Kaye L, Orben A, A. Ellis D, C. Hunter S, Houghton S. The conceptual and methodological mayhem of “screen time.” *IJERPH*. 2020;17(10):3661. <https://doi.org/10.3390/ijerph17103661>.

8. Kabali HK, Irigoyen MM, Nunez-Davis R, et al. Exposure and use of mobile media devices by young children. *Pediatrics*. 2015;136(6):1044–50. <https://doi.org/10.1542/peds.2015-2151>.
9. Radesky JS, Schumacher J, Zuckerman B. Mobile and interactive media use by young children: the good, the bad, and the unknown. *Pediatrics*. 2015;135(1):1–3. <https://doi.org/10.1542/peds.2014-2251>.
10. Computer and Internet Use in the United States: 2018. Published online April 21, 2021. <https://www.census.gov/newsroom/press-releases/2021/computer-internet-use.html#:~:text=Smartphones%20were%20present%20in%2084,ownership%20fell%20behind%20at%2063%25>.
11. Auxier B, Anderson M, Turner E. Children's engagement with digital devices, screen time. Published online July 28, 2020.
12. Radesky JS, Weeks HM, Ball R, et al. Young children's use of smartphones and tablets. *Pediatrics*. 2020;146(1):e20193518. <https://doi.org/10.1542/peds.2019-3518>.
13. Barr R, Kirkorian H, Radesky J, et al. Beyond screen time: a synergistic approach to a more comprehensive assessment of family media exposure during early childhood. *Front Psychol*. 2020;11:1283. <https://doi.org/10.3389/fpsyg.2020.01283>.
14. Guo N, Luk TT, Wang MP, et al. Self-reported screen time on social networking sites associated with problematic smartphone use in Chinese adults: a population-based study. *Front Psychiatry*. 2021;11:614061. <https://doi.org/10.3389/fpsyg.2020.614061>.
15. Sewall CJR, Bear TM, Merranko J, Rosen D. How psychosocial well-being and usage amount predict inaccuracies in retrospective estimates of digital technology use. *Mob Media Commun*. 2020;8(3):379–99. <https://doi.org/10.1177/2050157920902830>.
16. Understanding how digital media affects child development. NIH Eunice Kennedy shriver national institute of child health and human development. 2023. https://www.nichd.nih.gov/about/org/od/directors_corner/prev_updates/digital-media-child-development-feb2023.
17. Perez O, Garza T, Hinderer O, et al. Validated assessment tools for screen media use: a systematic review. Karakulah AS, ed. *PLoS One*. 2023;18(4):e0283714. <https://doi.org/10.1371/journal.pone.0283714>.
18. Domoff SE, Banga CA, Borgen AL, et al. Use of passive sensing to quantify adolescent mobile device usage: feasibility, acceptability, and preliminary validation of the eMOODIE application. *Human Behav Emerg Tech*. 2021;3(1):63–74. <https://doi.org/10.1002/hbe2.247>.
19. Livingstone S, Mascheroni G, Dreier M, Chaudron S, Lagae K. How parents of young children manage digital devices at home: the role of income, education, and parental style. London: EU Kids Online, LSE; 2015. ISSN 2045-256X.
20. Teh PS, Zhang N, Teoh ABJ, Chen K. A survey on touch dynamics authentication in mobile devices. *Comput Secur*. 2016;59:210–35. <https://doi.org/10.1016/j.cose.2016.03.003>.
21. Mahfouz A, Mahmoud TM, Eldin AS. A survey on behavioral biometric authentication on smartphones. *J Inf Secur Applic*. 2017;37:28–37. <https://doi.org/10.1016/j.jisa.2017.10.002>.
22. Ibrahim TM, Abdulhamid SM, Alarood AA, et al. Recent advances in mobile touch screen security authentication methods: a systematic literature review. *Comput Secur*. 2019;85:1–24. <https://doi.org/10.1016/j.cose.2019.04.008>.
23. Meng W, Wong DS, Furnell S, Zhou J. Surveying the development of biometric user authentication on mobile phones. *IEEE Commun Surv Tutor*. 2015;17(3):1268–93. <https://doi.org/10.1109/COMST.2014.2386915>.
24. Abdulhak SA, Abdulaziz AA. A systematic review of features identification and extraction for behavioral biometric authentication in touchscreen mobile devices. In: 2018 20th International Conference on Advanced Communication Technology (ICACT). New York: IEEE; 2018. p. 68–73. <https://doi.org/10.23919/ICACT.2018.8323648>.
25. Li F, Clarke N, Papadaki M, Dowland P. Active authentication for mobile devices utilising behaviour profiling. *Int J Inf Secur*. 2014;13(3):229–44. <https://doi.org/10.1007/s10207-013-0209-6>.
26. Pisani PH, Lorena AC. A systematic review on keystroke dynamics. *J Braz Comput Soc*. 2013;19(4):573–87. <https://doi.org/10.1007/s13173-013-0117-7>.
27. Kumar R, Kundu PP, Shukla D, Phoha VV. Continuous user authentication via unlabeled phone movement patterns. In: 2017 IEEE International Joint Conference on Biometrics (IJCB). New York: IEEE; 2017. p. 177–184. <https://doi.org/10.1109/BTAS.2017.8272696>.
28. Davarci E, Anarim E. User identification on smartphones with motion sensors and touching behaviors. In: 2022 30th Signal Processing and Communications Applications Conference (SIU). New York: IEEE; 2022. p. 1–4. <https://doi.org/10.1109/SIU55565.2022.9864837>.
29. Alzubaidi A, Kalita J. Authentication of smartphone users using behavioral biometrics. *IEEE Commun Surv Tutor*. 2016;18(3):1998–2026. <https://doi.org/10.1109/COMST.2016.2537748>.
30. Stylios I, Kokolakis S, Thanou O, Chatzis S. Behavioral biometrics & continuous user authentication on mobile devices: a survey. *Inf Fusion*. 2021;66:76–99. <https://doi.org/10.1016/j.inffus.2020.08.021>.
31. Tricco AC, Lillie E, Zarin W, et al. PRISMA Extension for Scoping Reviews (PRISMA-ScR): checklist and explanation. *Ann Intern Med*. 2018;169(7):467–73. <https://doi.org/10.7326/M18-0850>.
32. Silverio-Fernández M, Renukappa S, Suresh S. What is a smart device? - a conceptualisation within the paradigm of the Internet of Things. *Vis in Eng*. 2018;6(1):3. <https://doi.org/10.1186/s40327-018-0063-8>.
33. Goggin G. Adapting the mobile phone: the iPhone and its consumption. *Continuum*. 2009;23(2):231–44. <https://doi.org/10.1080/10304310802710546>.
34. Papadakis S, Alexandraki F, Zaranis N. Mobile device use among pre-school-aged children in Greece. *Educ Inf Technol*. 2022;27(2):2717–50. <https://doi.org/10.1007/s10639-021-10718-6>.
35. Domoff SE, Borgen AL, Foley RP, Maffett A. Excessive use of mobile devices and children's physical health. *Hum Behav Emerg Tech*. 2019;1(2):169–75. <https://doi.org/10.1002/hbe2.145>.
36. Davis SP, Ashayer A, Tabrizi N. Predicting sex and age using swipe-gesture data from a mobile device. In: 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCLOUD/SocialCom/SustainCom). IEEE; 2020. p. 1136–1143. <https://doi.org/10.1109/ISPA-BDCLOUD-SocialCom-SustainCom51426.2020.00169>.
37. Sun Z, Wang Y, Qu G, Zhou Z. A 3-D hand gesture signature based biometric authentication system for smartphones. *Secur Comm Networks*. 2016;9(11):1359–73. <https://doi.org/10.1002/sec.1422>.
38. Liu Q, Wang M, Zhao P, Yan C, Ding Z. A behavioral authentication method for mobile gesture against resilient user posture. In: 2016 3rd International Conference on Systems and Informatics (ICSAI). IEEE; 2016. p. 324–331. <https://doi.org/10.1109/ICSAI.2016.7810976>.
39. Maghsoudi J, Tappert CC. A behavioral biometrics user authentication study using motion data from android smartphones. In: 2016 European Intelligence and Security Informatics Conference (EISIC). IEEE; 2016. p. 184–187. <https://doi.org/10.1109/EISIC.2016.047>.
40. Putri AN, Asnar YDW, Akbar S. A continuous fusion authentication for Android based on keystroke dynamics and touch gesture. In: 2016 International Conference on Data and Software Engineering (ICoDSE). New York: IEEE; 2016. p. 1–6. <https://doi.org/10.1109/ICoDSE.2016.7936146>.
41. Lamiche I, Bin G, Jing Y, Yu Z, Hadid A. A continuous smartphone authentication method based on gait patterns and keystroke dynamics. *J Ambient Intell Human Comput*. 2019;10(11):4417–30. <https://doi.org/10.1007/s12652-018-1123-6>.
42. Smith-Creasey M, Rajarajan M. A continuous user authentication scheme for mobile devices. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST). New York: IEEE; 2016. p. 104–113. <https://doi.org/10.1109/PST.2016.7906944>.
43. Shih DH, Lu CM, Shih MH. A flick biometric authentication mechanism on mobile devices. In: 2015 International Conference on Informative and Cybernetics for Computational Social Systems (ICCSS). New York: IEEE; 2015. p. 31–33. <https://doi.org/10.1109/ICCSS.2015.7281144>.
44. Zaidi AZ, Chong CY, Parthiban R, Sadiq AS. A framework of dynamic selection method for user classification in touch-based continuous mobile device authentication. *J Inform Secur Applic*. 2022;67:103217. <https://doi.org/10.1016/j.jisa.2022.103217>.
45. Soni D, Hanmandlu M, Saini HC. A Machine learning approach for user authentication using touchstroke dynamics. In: Somani AK, Srivastava S, Mundra A, Rawat S, eds. Proceedings of First International Conference on Smart System, Innovations and Computing. Vol 79. Smart Innovation, Systems and Technologies. Singapore: Springer Singapore; 2018. p. 391–410. https://doi.org/10.1007/978-981-10-5828-8_38.

46. Lin CC, Chang CC, Liang D, Yang CH. 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. New York: IEEE; 2012. p. 245–252. <https://doi.org/10.1109/SERE.2012.37>.
47. Li G, Bours P. A novel mobilephone application authentication approach based on accelerometer and gyroscope data. In: 2018 International Conference of the Biometrics Special Interest Group (BIOSIG). New York City: IEEE; 2018. p. 1–4. <https://doi.org/10.23919/BIOSIG.2018.8553503>.
48. Smith-Creasey M, Rajarajan M. A novel scheme to address the fusion uncertainty in multi-modal continuous authentication schemes on mobile devices. In: 2019 International Conference on Biometrics (ICB). New York City: IEEE; 2019. p. 1–8. <https://doi.org/10.1109/ICB45273.2019.8987390>.
49. Salem A, Obaidat MS. A novel security scheme for behavioral authentication systems based on keystroke dynamics. *Secur Priv*. 2019;2(2):e64. <https://doi.org/10.1002/spy2.64>.
50. Zhao S, Guo Z, Zhong C, Xian L, Liu Y. A novel smartphone identity authentication mechanism. In: Proceedings of the ACM Turing Celebration Conference - China. New York: ACM; 2020. p. 157–161. <https://doi.org/10.1145/3393527.3393554>.
51. Qiao M, Zhang S, Sung AH, Liu Q. A novel touchscreen-based authentication scheme using static and dynamic hand biometrics. In: 2015 IEEE 39th Annual Computer Software and Applications Conference. New York: IEEE; 2015. p. 494–503. <https://doi.org/10.1109/COMPSAC.2015.133>.
52. Smith-Creasey M, Rajarajan M. A novel word-independent gesture-typing continuous authentication scheme for mobile devices. *Comput Secur*. 2019;83:140–50. <https://doi.org/10.1016/j.cose.2019.02.001>.
53. Alariki AA, Bt Abdul Manaf A, Khan S. A study of touching behavior for authentication in touch screen smart devices. In: 2016 International Conference on Intelligent Systems Engineering (ICISE). New York: IEEE; 2016. p. 216–221. <https://doi.org/10.1109/INTELSE.2016.7475123>.
54. Lee SH, Roh JH, Kim S, Jin SH. A study on feature of keystroke dynamics for improving accuracy in mobile environment. In: Choi D, Guillely S, eds. Information Security Applications. Vol 10144. Lecture Notes in Computer Science. New York: Springer International Publishing; 2017. p. 366–375. https://doi.org/10.1007/978-3-31956549-1_31.
55. Li W, Tan J, Meng W, Wang Y. A swipe-based unlocking mechanism with supervised learning on smartphones: design and evaluation. *J Netw Comput Appl*. 2020;165:102687. <https://doi.org/10.1016/j.jnca.2020.102687>.
56. Saini BS, Singh P, Nayyar A, et al. A three-step authentication model for mobile phone user using keystroke dynamics. *IEEE Access*. 2020;8:125909125922. <https://doi.org/10.1109/ACCESS.2020.3008019>.
57. Takahashi H, Ogura K, Bista BB, Takata T. A user authentication scheme using keystrokes for smartphones while moving. New York: IEEE; 2016.
58. Deb D, Ross A, Jain AK, Prakah-Asante K, Prasad KV. Actions speak louder than (Pass)words: passive authentication of smartphone users via deep temporal features. In: 2019 International Conference on Biometrics (ICB). IEEE; 2019. p. 1–8. <https://doi.org/10.1109/ICB45273.2019.8987433>.
59. Leingang W, Gunn D, Kim JH, Yuan X, Roy K. Active authentication using touch dynamics. In: SoutheastCon 2018. New York: IEEE; 2018. p. 1–5. <https://doi.org/10.1109/SECON.2018.8479298>.
60. Acién A, Morales A, Fierrez J, Vera-Rodríguez R, Hernández-Ortega J. Active detection of age groups based on touch interaction. *IET Biom*. 2019;8(1):101–8. <https://doi.org/10.1049/iet-bmt.2018.5003>.
61. Mahbub U, Sarkar S, Patel VM, Chellappa R. 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). New York: IEEE; 2016. p. 1–8. <https://doi.org/10.1109/BTAS.2016.7791155>.
62. Guarino A, Lemerì N, Malandrino D, Zaccagnino R, Capo C. Adam or Eve? Automatic users' gender classification via gestures analysis on touch devices. *Neural Comput Appl*. 2022;34(21):18473–95. <https://doi.org/10.1007/s00521-022-07454-4>.
63. Wang S, Yuan J, Wen J. Adaptive phone orientation method for continuous authentication based on mobile motion sensors. In: 2019 IEEE 31st International Conference on Tools with Artificial Intelligence (ICTAI). New York: IEEE; 2019. p. 1623–1627. <https://doi.org/10.1109/ICTAI.2019.00236>.
64. Davarci E, Soysal B, Erguler I, Aydin SO, Dincer O, Anarim E. Age group detection using smartphone motion sensors. In: 2017 25th European Signal Processing Conference (EUSIPCO). New York: IEEE; 2017. p. 2201–2205. <https://doi.org/10.23919/EUSIPCO.2017.8081600>.
65. Chakraborty B, Nakano K, Tokoi Y, Hashimoto T. An approach for designing low cost deep neural network based biometric authentication model for smartphone user. In: TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON). New York: IEEE; 2019. p. 772–777. <https://doi.org/10.1109/TENCON.2019.8929241>.
66. Antal M, Szabo LZ. An Evaluation of One-class and two-class classification algorithms for keystroke dynamics authentication on mobile devices. In: 2015 20th International Conference on Control Systems and Computer Science. New York: IEEE; 2015. p. 343–350. <https://doi.org/10.1109/CSCS.2015.16>.
67. Roy A, Halevi T, Memon N. An HMM-based multi-sensor approach for continuous mobile authentication. In: MILCOM 2015 - 2015 IEEE Military Communications Conference. New York: IEEE; 2015. p. 1311–1316. <https://doi.org/10.1109/MILCOM.2015.7357626>.
68. Salem A, Zaidan D, Swidan A, Saifan R. Analysis of strong password using keystroke dynamics authentication in touch screen devices. In: 2016 Cybersecurity and Cyberforensics Conference (CCC). New York: IEEE; 2016. p. 15–21. <https://doi.org/10.1109/CCC.2016.11>.
69. Roy S, Roy U, Sinha DD. Analysis of typing pattern in identifying sop biometric information and its impact in user recognition. In: Chandra P, Giri D, Li F, Kar S, Jana DK, eds. Information Technology and Applied Mathematics. Vol 699. Advances in Intelligent Systems and Computing. Singapore: Springer Singapore; 2019. p. 69–83. https://doi.org/10.1007/978-981-10-7590-2_5.
70. Lee W. Analyzing motion of touching screen for inferring user characteristics. In: 2021 Twelfth International Conference on Ubiquitous and Future Networks (ICUFN). New York: IEEE; 2021. p. 78–80. <https://doi.org/10.1109/ICUFN49451.2021.9528699>.
71. Buriro A, Crispo B, Conti M. AnswerAuth: a bimodal behavioral biometric-based user authentication scheme for smartphones. *J Inform Secur Applic*. 2019;44:89–103. <https://doi.org/10.1016/j.jisa.2018.11.008>.
72. Praher C, Sonntag M. Applicability of keystroke dynamics as a biometric security feature for mobile touchscreen devices with virtualised keyboards. *IJICS*. 2016;8(1):72. <https://doi.org/10.1504/IJICS.2016.075311>.
73. Baran M, Siwik L, Rzecki K. Application of elastic principal component analysis to person recognition based on screen gestures. In: Rutkowski L, Scherer R, Korytkowski M, Pedrycz W, Tadeusiewicz R, Zurada JM, eds. Artificial Intelligence and Soft Computing. Vol 11508. Lecture Notes in Computer Science. New York: Springer International Publishing; 2019. p. 553–560. https://doi.org/10.1007/978-3-030-20912-4_50.
74. Ali Z, Payton J, Sritapan V. At your fingertips: considering finger distinctness in continuous touch-based authentication for mobile devices. In: 2016 IEEE Security and Privacy Workshops (SPW). New York: IEEE; 2016. p. 272–275. <https://doi.org/10.1109/SPW.2016.29>.
75. Guerra-Casanova J, Sánchez-Ávila C, Bailador G, de Santos SA. Authentication in mobile devices through hand gesture recognition. *Int J Inf Secur*. 2012;11(2):65–83. <https://doi.org/10.1007/s10207-012-0154-9>.
76. Primo A. Keystroke-based continuous authentication while listening to music on your smart-phone. In: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). New York: IEEE; 2017. p. 217–225. <https://doi.org/10.1109/UEMCON.2017.8249029>.
77. Yang Y, Guo B, Wang Z, Li M, Yu Z, Zhou X. BehaveSense: continuous authentication for security-sensitive mobile apps using behavioral biometrics. *Ad Hoc Netw*. 2019;84:9–18. <https://doi.org/10.1016/j.adhoc.2018.09.015>.
78. Wolff M. Behavioral biometric identification on mobile devices. In: Schmorrow DD, Fidopiastis CM, eds. Foundations of Augmented Cognition. Vol 8027. Lecture Notes in Computer Science. Berlin: Springer Berlin Heidelberg; 2013. p. 783–791. https://doi.org/10.1007/978-3-642-39454-6_84.
79. Tse KW, Hung K. Behavioral biometrics scheme with keystroke and swipe dynamics for user authentication on mobile platform. In: 2019 IEEE 9th Symposium on Computer Applications & Industrial Electronics (ISCAIE). New York: IEEE; 2019. p. 125–130. <https://doi.org/10.1109/ISCAIE.2019.8743995>.

80. Antal M, Szabó LZ. Biometric authentication based on touchscreen swipe patterns. *Proc Technol*. 2016;22:862–9. <https://doi.org/10.1016/j.protcy.2016.01.061>.
81. Laghari A, Waheed-ur-Rehman, Memon ZA. Biometric authentication technique using smartphone sensor. In: 2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST). New York: IEEE; 2016. p. 381–384. <https://doi.org/10.1109/IBCAST.2016.7429906>.
82. Tolosana R, Vera-Rodriguez R, Fierrez J, Morales A. BioTouchPass demo: handwritten passwords for touchscreen biometrics. In: Proceedings of the 27th ACM International Conference on Multimedia. New York: ACM; 2019. p. 1023–1025. <https://doi.org/10.1145/3343031.3350578>.
83. Ray A, Hou D, Schuckers S, Barbir A. Continuous authentication based on hand micro-movement during smartphone form filling by seated human subjects. In: Proceedings of the 7th International Conference on Information Systems Security and Privacy. Setubal, Portugal: SCITE-PRESS - Science and Technology Publications; 2021. p. 424–431. <https://doi.org/10.5220/0010225804240431>.
84. Ambol S, Rashad S. Continuous authentication of smartphone users using machine learning. In: 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). New York: IEEE; 2020. p. 0056–0062. <https://doi.org/10.1109/UEMCON51285.2020.9298040>.
85. Garbuz A, Epishkina A, Kogos K. Continuous authentication of smartphone users via swipes and taps analysis. In: 2019 European Intelligence and Security Informatics Conference (EISIC). New York: IEEE; 2019. p. 48–53. <https://doi.org/10.1109/EISIC49498.2019.9108780>.
86. Dybczak J, Nawrocki P. Continuous authentication on mobile devices using behavioral biometrics. In: 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid). New York: IEEE; 2022. p. 1028–1035. <https://doi.org/10.1109/CCGrid54584.2022.00125>.
87. Murmuria R, Stavrou A, Barabár D, Fleck D. Continuous authentication on mobile devices using power consumption, touch gestures and physical movement of users. In: Bos H, Monrose F, Blanc G, eds. *Research in Attacks, Intrusions, and Defenses*. Vol 9404. Lecture Notes in Computer Science. New York: Springer International Publishing; 2015. p. 405–424. https://doi.org/10.1007/978-3-319-26362-5_19.
88. Karanikiotis T, Papamichail MD, Chatzidimitriou KC, Oikonomou NCI, Symeonidis AL, Saripalle SK. Continuous implicit authentication through touch traces modelling. In: 2020 IEEE 20th International Conference on Software Quality, Reliability and Security (QRS). New York: IEEE; 2020. p. 111–120. <https://doi.org/10.1109/QRS51102.2020.00026>.
89. Zhao X, Feng T, Shi W. Continuous mobile authentication using a novel graphic touch gesture feature. In: 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS). IEEE; 2013. p. 1–6. <https://doi.org/10.1109/BTAS.2013.6712747>.
90. Zhao X, Feng T, Lu X, Shi W, Kakadiaris IA. Continuous mobile authentication using user-phone interaction. *Inst Eng Technol*. 2017;3:209–33. https://doi.org/10.1049/PBSE003E_ch8.
91. Leyfer K, Spivak A. Continuous user authentication by the classification method based on the dynamic touchscreen biometrics. In: 2019 24th Conference of Open Innovations Association (FRUCT). New York City: IEEE; 2019. p. 228–234. <https://doi.org/10.23919/FRUCT.2019.8711941>.
92. Herath HMCKB, Dulanga KGC, Tharindu NVD, Ganegoda GU. Continuous user authentication using keystroke dynamics for touch devices. In: 2022 2nd International Conference on Image Processing and Robotics (ICIPRob). New York: IEEE; 2022. p. 1–6. <https://doi.org/10.1109/ICIPRob54042.2022.9798728>.
93. Kumar R, Kundu PP, Shukla D, Phoha VV. Continuous user authentication via unlabeled phone movement patterns. In: 2017 IEEE International Joint Conference on Biometrics (IJCB). New York: IEEE; 2017. p. 177–184. <https://doi.org/10.1109/BTAS.2017.8272696>.
94. Barlas Y, Basar OE, Akan Y, Isbilen M, Alptekin GI, Incel OD. DAKOTA: continuous authentication with behavioral biometrics in a mobile banking application. In: 2020 5th International Conference on Computer Science and Engineering (UBMK). New York: IEEE; 2020. p. 1–6. <https://doi.org/10.1109/UBMK50275.2020.9219365>.
95. Incel OD, Gunay S, Akan Y, et al. DAKOTA: sensor and touch screen-based continuous authentication on a mobile banking application. *IEEE Access*. 2021;9:38943–60. <https://doi.org/10.1109/ACCESS.2021.3063424>.
96. Hernandez-Ortega J, Morales A, Fierrez J, Acien A. Detecting age groups using touch interaction based on neuromotor characteristics. *Electron Lea*. 2017;53(20):1349–50. <https://doi.org/10.1049/el.2017.0492>.
97. Nguyen TV, Sae-Bae N, Memon N. DRAW-A-PIN: authentication using finger-drawn PIN on touch devices. *Comput Secur*. 2017;66:115–28. <https://doi.org/10.1016/j.cose.2017.01.008>.
98. Al-Showarah SA. Dynamic recognition for user age-group classification using hand-writing based finger on smartphones. In: 2019 10th International Conference on Information and Communication Systems (ICICS). New York: IEEE; 2019. p. 140–146. <https://doi.org/10.1109/IACS.2019.8809083>.
99. Ng'ang'a A, Musuva PMW. Enhancing accuracy in a touch operation biometric system: a case on the android pabern lock scheme. *Mobile Inform Syst*. 2020;2020:1–12. <https://doi.org/10.1155/2020/4165457>.
100. Ray-Dowling A, Hou D, Schuckers S, Barbir A. Evaluating multi-modal mobile behavioral biometrics using public datasets. *Comput Secur*. 2022;121:102868. <https://doi.org/10.1016/j.cose.2022.102868>.
101. Buriro A, Gupta S, Crispo B. Evaluation of motion-based touch-typing biometrics for online banking. In: 2017 International Conference of the Biometrics Special Interest Group (BIOSIG). New York: IEEE; 2017. p. 1–5. <https://doi.org/10.23919/BIOSIG.2017.8053504>.
102. Ouadja Y, Adnane M, Bouadjene N. Feature importance evaluation of smartphone touch gestures for biometric authentication. In: 2020 2nd International Workshop on Human-Centric Smart Environments for Health and Well-Being (IHSH). New York: IEEE; 2021. p. 103–107. <https://doi.org/10.1109/IHSH51661.2021.9378750>.
103. Suharsono A, Liang D. Hand stability based features for touch behavior smartphone authentication. In: 2020 3rd IEEE International Conference on Knowledge Innovation and Invention (ICKII). New York: IEEE; 2020. p. 167–170. <https://doi.org/10.1109/ICKII50300.2020.9318982>.
104. Barra S, Fenu G, De Marsico M, Castiglione A, Nappi M. Have you permission to answer this phone? In: 2018 International Workshop on Biometrics and Forensics (IWBF). New York: IEEE; 2018. p. 1–7. <https://doi.org/10.1109/IWBF.2018.8401563>.
105. Mallet J, Pryor L, Dave R, Seliya N, Vanamala M, Sowells-Boone E. Hold on and swipe: a touch-movement based continuous authentication schema based on machine learning. In: 2022 Asia Conference on Algorithms, Computing and Machine Learning (CACML). New York: IEEE; 2022. p. 442–447. <https://doi.org/10.1109/CACML55074.2022.00081>.
106. Abate AF, Nappi M, Ricciardi S. I-Am: implicitly authenticate me—person authentication on mobile devices through ear shape and arm gesture. *IEEE Trans Syst Man Cybern, Syst*. 2019;49(3):469–81. <https://doi.org/10.1109/TSMC.2017.2698258>.
107. Cheng Y, Ji X, Li X, et al. Identifying child users via touchscreen interactions. *ACM Trans Sen Netw*. 2020;16(4):1–25. <https://doi.org/10.1145/3403574>.
108. Alqarni MA, Chauhdary SH, Malik MN, Ehatisham-ul-Haq M, Azam MA. Identifying smartphone users based on how they interact with their phones. *Hum Cent Comput Inf Sci*. 2020;10(1):7. <https://doi.org/10.1186/s13673-020-0212-7>.
109. Rao KR, Anne VPK, Sai Chand U, Alakananda V, Navya Rachana K. Inclination and pressure based authentication for touch devices. In: Satapathy SC, Avadhani PS, Udgata SK, Lakshminarayana S, eds. *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India - Vol 1*. Vol 248. Advances in intelligent systems and computing. New York: Springer International Publishing; 2014. p. 781–788. https://doi.org/10.1007/978-3-319-03107-1_86.
110. Coakley MJ, Monaco JV, Tappert CC. Keystroke biometric studies with short numeric input on smartphones. In: 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). New York: IEEE; 2016. p. 1–6. <https://doi.org/10.1109/BTAS.2016.7791181>.
111. Gautam P, Dawadi PR. Keystroke biometric system for touch screen text input on android devices optimization of equal error rate based on medians vector proximity. In: 2017 11th International Conference on Software, Knowledge, Information Management and Applications (SKIMA). New York: IEEE; 2017. p. 1–7. <https://doi.org/10.1109/SKIMA.2017.8294136>.
112. Deng Y, Zhong Y. Keystroke dynamics advances for mobile devices using deep neural network. In: Zhong Y, Deng Y, eds. *Gate to computer*

- science and research. Vol 2. 1st ed. Thrace, Greece: Science Gate Publishing P.C.; 2015. p. 59–70. <https://doi.org/10.15579/gcsr.vol2.ch4>.
113. Roh J hyuk, Lee SH, Kim S. Keystroke dynamics for authentication in smartphone. In: 2016 International Conference on Information and Communication Technology Convergence (ICTC). New York: IEEE; 2016. p. 1155–1159. <https://doi.org/10.1109/ICTC.2016.7763394>.
 114. Acien A, Morales A, Vera-Rodriguez R, Fierrez J. Keystroke mobile authentication: performance of long-term approaches and fusion with behavioral profiling. In: Morales A, Fierrez J, Sánchez JS, Ribeiro B, eds. Paaern recognition and image analysis. Vol 11868. Lecture Notes in Computer Science. New York: Springer International Publishing; 2019. p. 12–24. https://doi.org/10.1007/978-3-030-31321-0_2.
 115. Sun L, Cao B, Wang J, et al. Kollector: detecting fraudulent activities on mobile devices using deep learning. *IEEE Trans on Mobile Comput.* 2021;20(4):1465–76. <https://doi.org/10.1109/TMC.2020.2964226>.
 116. Peralta RT, Rebguns A, Fasel IR, Barnard K. Learning a policy for gesture-based active multi-touch authentication. In: Marinos L, Askoxylakis I, eds. Human Aspects of information security, privacy, and trust. Vol 8030. Lecture notes in computer science. Berlin: Springer Berlin Heidelberg; 2013. p. 59–68. https://doi.org/10.1007/978-3642-39345-7_7.
 117. Stragapede G, Vera-Rodriguez R, Tolosana R, Morales A, Acien A, Le Lan G. Mobile behavioral biometrics for passive authentication. *Paaern Recog Leaers.* 2022;157:35–41. <https://doi.org/10.1016/j.patrec.2022.03.014>.
 118. Liang X, Zou F, Li L, Yi P. Mobile terminal identity authentication system based on behavioral characteristics. *Int J Distrib Sens Netw.* 2020;16(1):155014771989937. <https://doi.org/10.1177/1550147719899371>.
 119. Li C, Jing J, Liu Y. Mobile user authentication—turn it to unlock. In: 2021 6th International Conference on Mathematics and Artificial Intelligence. New York: ACM; 2021. p. 101–107. <https://doi.org/10.1145/3460569.3460577>.
 120. Corpus KR, Gonzales RJD, Morada AS, Vea LA. Mobile user identification through authentication using keystroke dynamics and accelerometer biometrics. In: Proceedings of the international conference on mobile Software engineering and systems. New York: ACM; 2016. p. 11–12. <https://doi.org/10.1145/2897073.2897111>.
 121. Akhtar Z, Buriro A, Crispo B, Falk TH. Multimodal smartphone user authentication using touchstroke, phone-movement and face patterns. In: 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP). New York: IEEE; 2017. p. 1368–1372. <https://doi.org/10.1109/GlobalSIP.2017.8309185>.
 122. Song Y, Cai Z, Zhang ZL. Multi-touch authentication using hand geometry and behavioral information. In: 2017 IEEE Symposium on Security and Privacy (SP). New York: IEEE; 2017. p. 357–372. <https://doi.org/10.1109/SP.2017.54>.
 123. Primo A, Phoha VV. Music and images as contexts in a context-aware touch-based authentication system. In: 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS). New York: IEEE; 2015. p. 1–7. <https://doi.org/10.1109/BTAS.2015.7358779>.
 124. Phillips ME, Stepp ND, Cruz-Albrecht J, De Sapio V, Lu TC, Sritapan V. Neuromorphic and early warning behavior-based authentication for mobile devices. In: 2016 IEEE Symposium on Technologies for Homeland Security (HST). New York: IEEE; 2016. p. 1–5. <https://doi.org/10.1109/THS.2016.7568965>.
 125. Li N, Liu J, Li Q, Luo X, Duan J. Online signature verification based on biometric features. In: 2016 49th Hawaii International Conference on System Sciences (HICSS). New York: IEEE; 2016. p. 5527–5534. <https://doi.org/10.1109/HICSS.2016.683>.
 126. Haberfeld C, Hossain MS, Lancor L. Open code biometric tap pad for smartphones. *J Inform Secur Applic.* 2021;57:102688. <https://doi.org/10.1016/j.jisa.2020.102688>.
 127. Tharwat A, Ibrahim A, Gaber T, Hassanien AE. Personal Identification based on mobile-based keystroke dynamics. In: Hassanien AE, Tolba MF, Shaalan K, Azar AT, eds. Proceedings of the international conference on advanced intelligent systems and informatics 2018. Vol 845. Advances in intelligent systems and computing. New York: Springer International Publishing; 2019. p. 457–466. https://doi.org/10.1007/978-3-319-99010-1_42.
 128. Tang C, Cui Z, Chu M, Lu Y, Zhou F, Gao S. Piezoelectric and machine learning based keystroke dynamics for highly secure user authentication. *IEEE Sensors J.* 2022;1–1. <https://doi.org/10.1109/JSEN.2022.3141872>.
 129. Mahfouz A, Mahmoud TM, Sharaf Eldin A. A behavioral biometric authentication framework on smartphones. In: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. New York: ACM; 2017. p. 923–925. <https://doi.org/10.1145/3052973.3055160>.
 130. Hernandez-Ortega J, Morales A, Fierrez J, Acien A. Predicting age groups from touch patterns based on neuromotor models. In: 8th International Conference of Pattern Recognition Systems (ICPRS 2017). Institution of Engineering and Technology; Stevenage, United Kingdom, 2017. <https://doi.org/10.1049/cp.2017.0135>.
 131. Miguel-Hurtado O, Stevenage SV, Bevan C, Guest R. Predicting sex as a sop-biometrics from device interaction swipe gestures. *Pattern Recog Leaers.* 2016;79:44–51. <https://doi.org/10.1016/j.patrec.2016.04.024>.
 132. Wang S, Yuan J, Chen S. Quality-based score level fusion for continuous authentication with motion sensor and face. In: Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy. New York: ACM; 2020. p. 58–62. <https://doi.org/10.1145/3377644.3377647>.
 133. Inguanez F, Ahmadi S. Securing smartphones via typing heat maps. In: 2016 IEEE 6th International Conference on Consumer Electronics - Berlin (ICCEBerlin). New York: IEEE; 2016. p. 193–197. <https://doi.org/10.1109/ICCE-Berlin.2016.7684753>.
 134. Zhu H, Hu J, Chang S, Lu L. Shakin: secure user authentication of smartphones with single-handed shakes. *IEEE Trans Mobile Comput.* 2017;16(10):2901–12. <https://doi.org/10.1109/TMC.2017.2651820>.
 135. Bo C, Zhang L, Li XY, Huang Q, Wang Y. SilentSense: silent user identification via touch and movement behavioral biometrics. In: Proceedings of the 19th Annual International Conference on Mobile Computing & Networking - MobiCom '13. New York: ACM Press; 2013. p. 187. <https://doi.org/10.1145/2500423.2504572>.
 136. Gunn DJ, Roy K, Bryant K. Simulated cloud authentication based on touch dynamics with SVM. In: 2018 IEEE Symposium Series on Computational Intelligence (SSCI). New York: IEEE; 2018. p. 639–644. <https://doi.org/10.1109/SSCI.2018.8628762>.
 137. Wang Z, Zhou N, Chen F, et al. Smart_Auth: user identity authentication based on smartphone motion sensors. In: 2021 6th International Conference on Image, Vision and Computing (ICIVC). New York: IEEE; 2021. p. 480–485. <https://doi.org/10.1109/ICIVC52351.2021.9526964>.
 138. Abate AF, Nappi M, Ricciardi S. Smartphone enabled person authentication based on ear biometrics and arm gesture. In: 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC). New York: IEEE; 2016. p. 003719–003724. <https://doi.org/10.1109/SMC.2016.7844812>.
 139. Acien A, Morales A, Vera-Rodriguez R, Fierrez J. Smartphone sensors for modeling human-computer interaction: general outlook and research datasets for user authentication. In: 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). New York: IEEE; 2020. p. 1273–1278. <https://doi.org/10.1109/COMPSAC48688.2020.00-81>.
 140. Anusas-amornkul T. Strengthening password authentication using keystroke dynamics and smartphone sensors. In: Proceedings of the 9th International Conference on Information Communication and Management. New York: ACM; 2019. p. 70–74. <https://doi.org/10.1145/3357419.3357425>.
 141. Temper M, Tjoa S. The applicability of fuzzy rough classifier for continuous person authentication. In: 2016 International Conference on Software Security and Assurance (ICSSA). New York: IEEE; 2016. p. 17–23. <https://doi.org/10.1109/ICSSA.2016.10>.
 142. Roy S, Roy U, Sinha DD. The probability of predicting personality traits by the way user types on touch screen. *Innov Syst Softw Eng.* 2019;15(1):27–34. <https://doi.org/10.1007/s11334-018-0317-6>.
 143. Shrestha B, Mohamed M, Tamrakar S, Saxena N. Theft-resilient mobile wallets: transparently authenticating NFC users with tapping gesture biometrics. In: Proceedings of the 32nd Annual Conference on Computer Security Applications. New York: ACM; 2016. p. 265–276. <https://doi.org/10.1145/2991079.2991097>.
 144. Cascone L, Nappi M, Narducci F, Pero C. Touch keystroke dynamics for demographic classification. *Pattern Recog Leaers.* 2022;158:63–70. <https://doi.org/10.1016/j.patrec.2022.04.023>.
 145. Temper M, Tjoa S, Kaiser M. Touch to authenticate — continuous biometric authentication on mobile devices. In: 2015 1st International Conference on Software Security and Assurance (ICSSA). New York: IEEE; 2015. p. 30–35. <https://doi.org/10.1109/ICSSA.2015.016>.

146. Frank M, Biedert R, Ma E, Martinovic I, Song D. Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. New York: IEEE; 2012. <https://doi.org/10.48550/ARXIV.1207.6231>.
147. Watanabe Y, Houryu A, Fujita T. Toward introduction of immunity-based model to continuous behavior-based user authentication on smart phone. *Proc Comput Sci*. 2013;22:1319–27.
148. Volaka HC, Alptekin G, Basar OE, Isbilen M, Incel OD. Towards continuous authentication on mobile phones using deep learning models. *Proc Comput Sci*. 2019;155:177–84. <https://doi.org/10.1016/j.procs.2019.08.027>.
149. Brown J, Raval A, Anwar M. Towards passive authentication using inertia variations: an experimental study on smartphones. In: 2020 Second International Conference on Transdisciplinary AI (TransAI). New York: IEEE; 2020. p. 88–91. <https://doi.org/10.1109/TransAI49837.2020.00019>.
150. Sharma V, Enbody R. User authentication and identification from user interface interactions on touch-enabled devices. In: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks. New York: ACM; 2017. p. 1–11. <https://doi.org/10.1145/3098243.3098262>.
151. Kroeze CJ, Malan KM. User authentication based on continuous touch biometrics. *SACJ*. Cape Town, South Africa. 2016;28(2). <https://doi.org/10.18489/sacj.v28i2.374>.
152. Filippov AI, Iuzbashev AV, Kurnev AS. User authentication via touch pattern recognition based on isolation forest. In: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). New York: IEEE; 2018. p. 1485–1489. <https://doi.org/10.1109/ElConRus.2018.8317378>.
153. Karakaya N, Alptekin GI, Incel ÖD. Using behavioral biometric sensors of mobile phones for user authentication. *Proc Comput Sci*. 2019;159:475–84. <https://doi.org/10.1016/j.procs.2019.09.202>.
154. Serwadda A, Phoha VV, Wang Z. Which verifiers work?: A benchmark evaluation of touch-based authentication algorithms. In: 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS). New York: IEEE; 2013. p. 1–8. <https://doi.org/10.1109/BTAS.2013.6712758>.
155. Buriro A, Crispo B, Delfrari F, Wrona K. Hold and sign: a novel behavioral biometrics for smartphone user authentication. In: 2016 IEEE Security and Privacy Workshops (SPW). IEEE; 2016. p. 276–285. <https://doi.org/10.1109/SPW.2016.20>.
156. Shen C, Yu T, Yuan S, Li Y, Guan X. Performance analysis of motion-sensor behavior for user authentication on smartphones. *Sensors*. 2016;16(3):345. <https://doi.org/10.3390/s16030345>.
157. Stylios I, Skalkos A, Kokolakis S, Karyda M. BioPrivacy: a behavioral biometrics continuous authentication system based on keystroke dynamics and touch gestures. *ICS*. 2022;30(5):687–704. <https://doi.org/10.1108/ICS-12-2021-0212>.
158. Papi E, Koh WS, McGregor AH. Wearable technology for spine movement assessment: a systematic review. *J Biomech*. 2017;64:186–97. <https://doi.org/10.1016/j.jbiomech.2017.09.037>.
159. Nguyen T, Roy A, Memon N. Kid on the phone! Toward automatic detection of children on mobile devices. *Comput Secur*. 2019;84:334–48. <https://doi.org/10.1016/j.cose.2019.04.001>.
160. Wang Z, Chen F, Zhou N, et al. Identity authentication based on dynamic touch behavior on smartphone. In: 2021 6th International Conference on Image, Vision and Computing (ICIVC). IEEE; 2021. p. 469–474. <https://doi.org/10.1109/ICIVC52351.2021.9527023>.
161. Thompson N, McGill TJ, Wang X. "Security begins at home": determinants of home computer and mobile device security behavior. *Comput Secur*. 2017;70:376–91. <https://doi.org/10.1016/j.cose.2017.07.003>.
162. Bo C, Zhang L, Jung T, Han J, Li XY, Wang Y. Continuous user identification via touch and movement behavioral biometrics. In: 2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC). IEEE; 2014. p. 1–8. <https://doi.org/10.1109/PCCC.2014.7017067>.
163. Bo C, Zhang L, Li XY, Huang Q, Wang Y. SilentSense: silent user identification via touch and movement behavioral biometrics. In: Proceedings of the 19th Annual International Conference on Mobile Computing & Networking - MobiCom '13. ACM Press; 2013. p. 187. <https://doi.org/10.1145/2500423.2504572>.
164. Stylios I, Kokolakis S, Skalkos A, Chatzis S. BioGames: a new paradigm and a behavioral biometrics collection tool for research purposes. *ICS*. 2022;30(2):243–54. <https://doi.org/10.1108/ICS-12-2020-0196>.
165. Papamichail MD, Chatzidimitriou KC, Karanikiotis T, Oikonomou NCI, Symeonidis AL, Saripalle SK. Behavioral biometrics dataset towards continuous implicit authentication. <https://doi.org/10.5281/ZENODO.2598135>. Published online March 19, 2019.
166. Murmuria R, Stavrou A, Barbará D, Fleck D. Continuous authentication on mobile devices using power consumption, touch gestures and physical movement of users. In: Bos H, Monrose F, Blanc G, eds. Research in Attacks, Intrusions, and Defenses. Vol 9404. Lecture Notes in Computer Science. Springer International Publishing; 2015. p. 405–424. https://doi.org/10.1007/978-3-319-26362-5_19.
167. Teh PS, Teoh ABJ, Yue S. A survey of keystroke dynamics biometrics. *ScientificWorldJournal*. 2013;2013:1–24. <https://doi.org/10.1155/2013/408280>.
168. Shen C, Li Y, Chen Y, Guan X, Maxion RA. Performance analysis of multi-motion sensor behavior for active smartphone authentication. *IEEE Trans Inform Forensic Secur*. 2018;13(1):48–62. <https://doi.org/10.1109/TIFS.2017.2737969>.
169. Tablets in the U.S. - statistics and facts. Statista. Published online May 23, 2023. <https://www.statista.com/topics/2927/tablets-in-the-us/#topicOverview>.
170. Counterpoint Quarterly. Global smartphone shipments market data (Q4 2021 - Q3 2023). <https://www.counterpointresearch.com/insights/global-smartphone-share/>.
171. Parker H, Burkart S, Reesor-Oyer L, et al. Feasibility of measuring screen time, activity, and context among families with preschoolers: intensive longitudinal pilot study. *JMIR Form Res*. 2022;6(9):e40572. <https://doi.org/10.2196/40572>.
172. Welk GJ, Bai Y, Lee JM, Godino J, Saint-Maurice PF, Carr L. Standardizing analytic methods and reporting in activity monitor validation studies. *Med Sci Sports Exerc*. 2019;51(8):1767–80. <https://doi.org/10.1249/MSS.0000000000001966>.
173. Menghini L, Cellini N, Goldstone A, Baker FC, de Zambotti M. A standardized framework for testing the performance of sleep-tracking technology: step-by-step guidelines and open-source code. *Sleep*. 2021;44(2):zsa170. <https://doi.org/10.1093/sleep/zsaa170>.

Publisher's Note

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