Computers & Security 160 (2026) 104731

Contents lists available at ScienceDirect

Computers & Security

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

Adaptability of current keystroke and mouse behavioral biometric systems: A survey

Aditya Subash *, Insu Song, Ickjai Lee, Kyungmi Lee

James Cook University - Singapore Campus Singapore, Singapore

ARTICLE INFO

Keywords:
Behavioral biometrics
Keystroke behavioral biometrics
Mouse behavioral biometrics
User behavior evolution
Adaptability

ABSTRACT

Research in behavioral biometrics, especially keystroke and mouse behavioral biometrics, has increased in recent years, gaining traction in industry and academia across various fields, including the detection of emotion, age, gender, fatigue, identity theft, and online assessment fraud. These methods are popular because they collect data non-invasively and continuously authenticate users by analyzing unique keystroke or mouse behavior. However, user behavior evolves over time due to several underlying factors. This can affect the performance of current keystroke and mouse behavioral biometric-based user authentication systems. We comprehensively survey current keystroke and mouse behavioral biometric approaches, exploring their use in user authentication and other real-world applications while outlining trends and research gaps. In particular, we investigate whether current approaches compensate for user behavior evolution. We find that current keystroke and mouse behavioral biometrics approaches cannot adapt to user behavior evolution and suffer from limited efficacy. Our survey highlights the need for new and improved keystroke and mouse behavioral biometrics approaches that can adapt to user behavior evolution. This study will assist researchers in improving current research efforts toward developing more secure, effective, sustainable, robust, adaptable, and privacy-preserving keystroke and mouse-behavioral biometric-based authentication systems.

1. Introduction

Authentication is establishing the integrity of one's identity before accessing critical services, information, or resources to which one is entitled. In other words, it is a fundamental system that ensures the confidentiality, integrity, and accessibility of resources (Andrean et al., 2020; Albalawi et al., 2022). Current user authentication systems use passwords or a combination of factors to identify users, mainly during log-in time (Andrean et al., 2020; Ometov et al., 2018; Lucia et al., 2023). Using passwords with other authentication factors for user authentication does not diminish the possibility of identity fraud, as the user, once authenticated, may not be the one currently accessing the system (Lucia et al., 2023). Continuous Authentication (CA) can overcome this weakness by regularly verifying user identity during an active session (Mondal and Bours, 2013). Research in keystroke and mouse behavioral biometric-based authentication systems has gained traction for this specific application (Siddiqui et al., 2021; Subash et al., 2023). Furthermore, these systems can be realized effortlessly due to the ease of data collection and minimalistic hardware requirements (Babich, 2012; Zheng et al., 2011).

The rising occurrence of phishing and identity theft underscores the urgent need for enhanced cybersecurity measures (DeLiema et al., 2020; Guedes et al., 2023). This is particularly true for sophisticated and cutting-edge authentication systems. The popularity of keystroke and mouse behavioral biometrics comes when cybersecurity attacks, such as phishing and identity theft, are rising. Identity theft is the intentional, unauthorized, and unlawful use of a person's identity for malicious activities (Guedes et al., 2023). According to a recent report from Javelin Strategy, total losses associated with identity theft amount to USD 43 billion. This figure includes losses due to traditional identity fraud and scams orchestrated by criminals (Sando, 2024). Similarly, phishing attacks have also become equally widespread. Such attacks deceive users into revealing confidential information by posing as legitimate entities. As per the Anti-Phishing Working Group (APWG) reports, the total number of unique phishing attacks detected as of 2023 amounts to ~4.9 million attack instances. This figure has risen from ~2.8 million unique phishing attacks detected in 2021. This represents a 75 % increase in phishing attacks detected in just two years.

* Corresponding author.
E-mail address: aditya.subash@my.jcu.edu.au (A. Subash).

https://doi.org/10.1016/j.cose.2025.104731
Received 12 March 2025; Received in revised form 21 May 2025; Accepted 20 October 2025
Available online 21 October 2025

Keystroke and mouse behavioral biometric-based authentication methods can alleviate this problem by providing a more secure alternative to conventional password or one-time authentication methods. This is due to their ability to effectively perform CA non-invasively (Siddiqui et al., 2021; Subash et al., 2023). For example, a system analyzes users' keystroke and mouse behavioral patterns and creates unique profiles for each user to continuously authenticate the users during their interaction with the system (Albalawi et al., 2022). Since authentication is performed based on user behavior, it becomes hard to reproduce and spoof the system, thereby making it secure (Siddiqui et al., 2021; Albalawi et al., 2022). However, studies have claimed that user behavior evolves over time due to various underlying factors (Jain and Pankanti, 2006; Ceker and Upadhyaya, 2016; Mhenni et al., 2019a; Subash and Song, 2021). Since current keystroke and mouse behavioral biometric-based authentication systems analyze behavior, changes in behavior can cause a rise in false positives, making the current approaches less effective.

Therefore, we comprehensively survey current keystroke and mouse behavioral biometric approaches, exploring their use in user authentication and other real-world applications, such as online assessment fraud detection, while outlining trends and research gaps. In particular, we investigate their adaptability to user behavior evolution. As an additional contribution, we will also compare our survey to previously published surveys to show the comprehensive nature of our study.

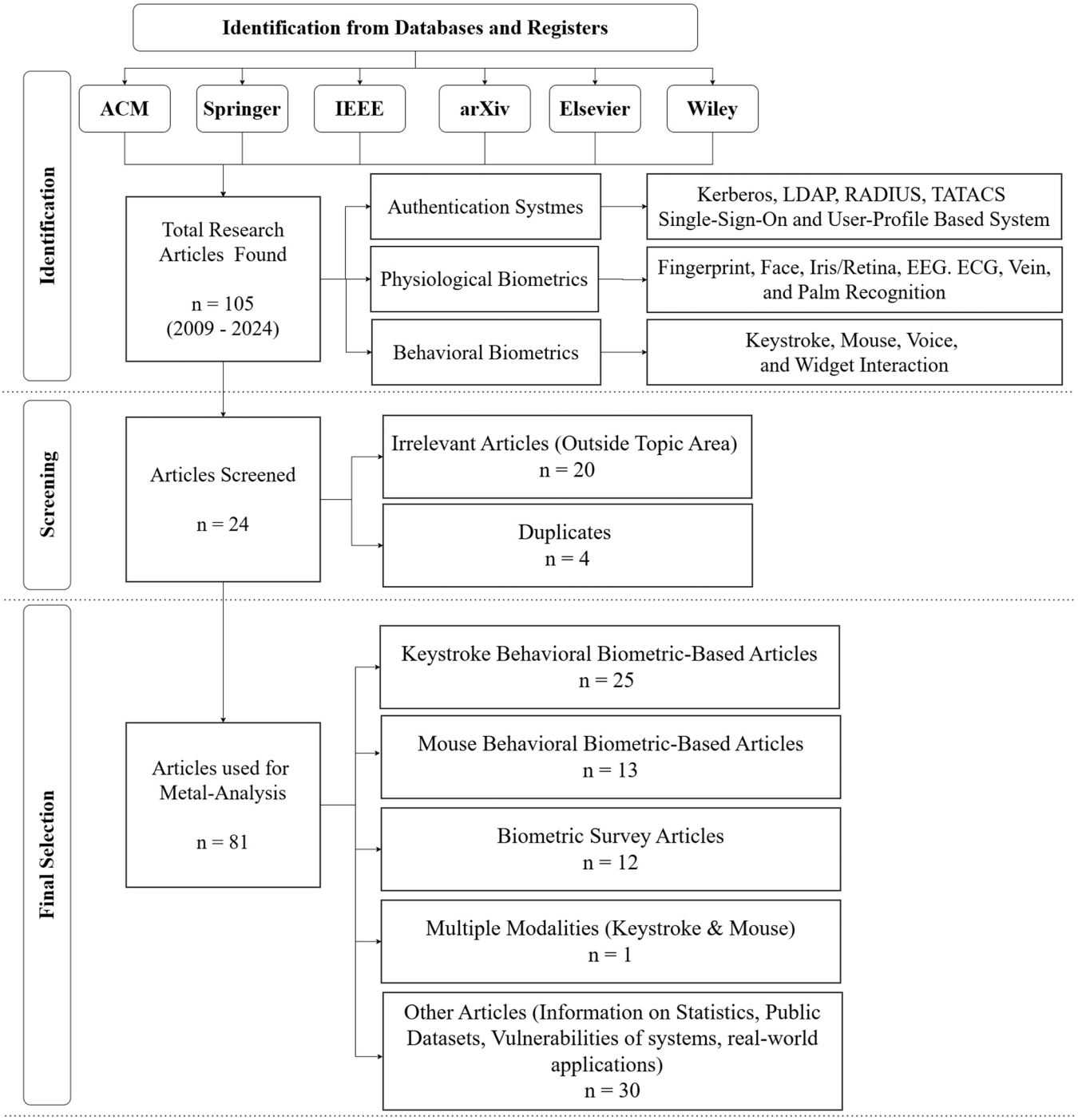

Fig. 1. PRISMA flow diagram illustrating keyword search and exclusion criterion.

2. Preliminaries and initial concepts

2.1. Inclusion and exclusion criteria

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow diagram was employed to identify and screen articles from databases and registers through a three-step process:

1. Identification: We meticulously analyzed 105 articles sourced from major publishers, including IEEE, ACM, Elsevier, Wiley, arXiv, and Springer (Fig. 1). Several articles published between 2009 and 2024, including empirical research, surveys, and literature reviews focusing on conventional authentication systems, physiological biometrics, and behavioral biometrics, were selected for our analysis.
2. Screening: Out of the 105 articles identified, 24 articles were excluded as they were found to be outside the scope of research, related to topics such as physiological biometric modalities, authentication protocols, user profile-based multimodal authentication systems, and conventional authentication systems. Furthermore, duplicate survey papers were also excluded. The main objective of this survey is to perform a comprehensive study of keystroke and mouse behavioral biometrics and give a detailed review of trends, research gaps, and future work in the field. In particular, we investigate the adaptability of current keystroke and mouse behavioral biometric research methods toward user behavior evolution. This survey article mainly includes empirical and qualitative research on keystroke and mouse behavioral biometrics.
3. Final Selection: The remaining articles are evaluated based on their relevance to the research topic, the data utilized for analysis, the details of the experimental methodology, and the evaluation metrics used by them. After a comprehensive evaluation, the 81 articles screened were finally selected for further analysis.

2.1.1. Biometric-Based authentication systems

Biometric authentication systems rely on the unique physiological and behavioral characteristics of individuals to verify their identity, addressing the limitations of traditional knowledge-based (e.g., passwords/PINs) and ownership-based (e.g., key cards/ cryptographic keys) authentication systems (Ometov et al., 2018; Zheng et al., 2011; Subash and Song, 2021). Conventional authentication systems are widely deployed but are susceptible to cybersecurity threats such as dictionary attacks, rainbow table attacks, and social engineering (Wang and Wang, 2015; Deb Das et al., 2013; Heartfield and Loukas, 2016). Physical authentication tokens, such as key cards, are also prone to being lost or stolen, further exposing users to potential security breaches (Zheng et al., 2011).

In contrast, biometric authentication systems leverage inherent and immutable traits of users, such as fingerprints, facial features, or behavioral patterns, making them a more secure alternative (Zheng et al., 2011; Jain and Pankanti, 2006). Biometric authentication can be classified into physiological and behavioral biometrics (Albalawi et al., 2022; Babich, 2012; Subash and Song, 2021). Physiological biometrics rely on physical traits, including fingerprints, facial recognition, and iris scans, unique to each individual (Albalawi et al., 2022; Babich, 2012; Jain et al., 2006). On the other hand, behavioral biometrics analyze dynamic behavioral traits, such as typing rhythms, mouse movement patterns, and touchscreen gestures, to identify users non-invasively and continuously (Babich, 2012; Zheng et al., 2011; Jain et al., 2006). In addition to the aforementioned modalities, behavioral biometrics also analyzes voice, gait patterns, eye movement, and widget interaction for user authentication (Fig. 2). Behavioral biometrics offers several advantages over physiological biometrics, including continuously verifying user identity using commonly available input devices, such as keyboards, mouse pointers, microphone sensors, and cameras, making it more inexpensive, accessible, and practical (Zheng et al., 2011).

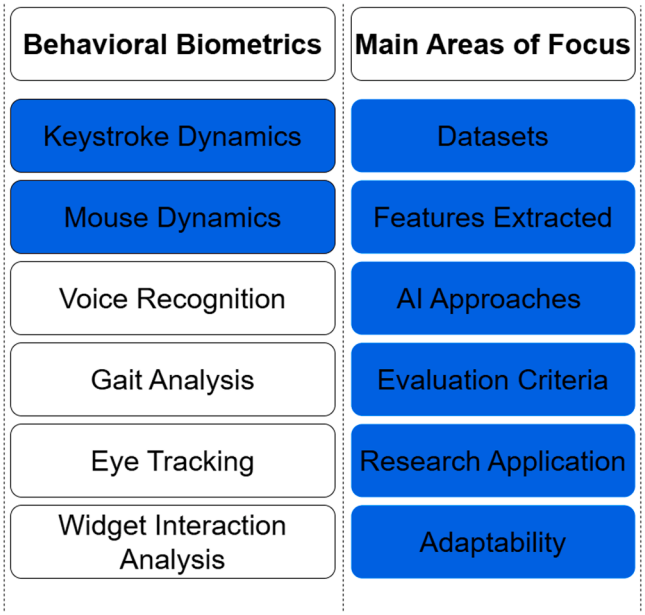

Fig. 2. Categorization of biometric authentication methods and main focus.

3. Keystroke behavioral biometrics

Keystroke behavioral biometric-based systems analyze users' typing patterns on digital devices to create a unique signature for user authentication (Albalawi et al., 2022). Over the years, there has been a sharp increase in research in the field due to its ability to perform CA non-invasively, specifically since the 1980s (Albalawi et al., 2022; Kochegurova and Martynova, 2020). Gaines (1980) was the first to propose the technology by developing the first automated keystroke dynamic-based recognition system. Since then, significant advancements have been made by implementing Machine Learning (ML) and Deep Learning (DL) approaches (Subash et al., 2023; Maheshwary et al., 2017).

Based on preliminary analysis, we confirm that keystroke behavioral biometric-based authentication was performed for two primary purposes: user authentication and identification (Messerman et al., 2010; Banerjee and Woodard, 2012). User authentication involves extracting sample keystroke features and comparing them with the features in a database to perform a one-on-one match to confirm the subject's identity. The process will verify whether the user is who they claim to be, either approving or rejecting the claimed identity, i.e., classifying the subject as an imposter (0) or genuine (1). On the other hand, user identification is identifying a particular user from a list of given users. This process looks through the entire database to find the user to whom the keystroke belongs (Messerman et al., 2010; Banerjee and Woodard, 2012).

3.1. Types of keystroke behavioral biometric datasets

Keystroke behavioral biometric datasets generally fall under static and dynamic datasets. Static datasets collect data by requesting users to enter a predetermined text of fixed length, which can be the same or different for each user. Analysis of static text is performed in systems with no scope for further text entry, mainly during the log-in phase. On the other hand, dynamic datasets collect free-form text that reflects real-world scenarios and enables CA. This type of data collection does not restrict the user on what is typed and is performed while users engage in their daily activities without restriction (Messerman et al., 2010; Banerjee and Woodard, 2012).

The description of several datasets implemented in keystroke behavioral biometric analysis is described below:

1) Public Datasets

A. CMU Benchmark Dataset: Collected keystroke data (Killourhy and Maxion, 2009) from 51 subjects who typed a predetermined password 50 times each session. Data was collected over 8 sessions, during which each subject provided 400 samples of keystroke data. Keystroke behavior data were collected from 30 males and 21 females, of whom eight were left-handed and 43 were right-handed. The median age group was 31–40, the youngest was 18–20, and the oldest was 61–70. According to the author, each subject's session took between 1.25 and 11 min, with the median session time being 3 min (Killourhy and Maxion, 2009).

B. Teh dataset: Collected keystroke data from 150 subjects, of which 132 belong to the public, while the rest are from academia. Data collection is facilitated using an Android application where subjects entered one 16-digit (1379,666,624,680,852) and one 4-digit PIN (5560). Specifically, they entered each PIN 10 times, contributing 20 samples each. Furthermore, subjects could choose which location to perform the activity (Maiorana et al., 2019).

C. Antal Dataset: The author collected keystroke data from 54 subjects who typed 3 different passwords, including easy, logically strong, and strong passwords, in 3 sessions, providing 60 samples each. Five of the 54 subjects were female, and 49 were male. According to the author, the subjects also participated in a demographic and experience survey (Antal and Nemes, 2016).

D. Coakley Dataset: Collected keystroke data from 52 subjects. The sample size is selected from a set of computer users, accounting for two-thirds of the undergraduate population enrolled in introductory computing courses and one-third of the working professionals. Each subject typed a 10-digit string (9141,937,761) 30 times (Coakley et al., 2016).

E. Android Dataset: Collected static keystroke data from 42 subjects using an Android application. Subjects were required to type a predetermined password 30 times during two sessions. Of the 42 subjects, 24 were males, and 18 were females (Antal et al., 2015).

F. WEBGREYC Dataset: This is another publicly available keystroke dataset collected by Giot et al. (2012) from 45 subjects who typed the same password, SESAME.

G. Aalto University Dataset: This dataset contains two parts: 1) The Dhakal et al. (2018) dataset that contains desktop keystroke data collected from a sample size of 168,000 subjects, and 2) The Palin et al. (2019) dataset comprising of mobile keystroke data collected from a sample size of 260,000 subjects. The same data collection procedure was implemented for both datasets, based on controlled free text. The data acquisition procedure required subjects to memorize English sentences and reproduce them as accurately as possible. These sentences were chosen from 1525 sentences acquired from Enron Mobile Email and Gigaword Newswire Corpus. Data collection was conducted using a web application.

H. The Clarkson 2 Dataset: This dataset was collected by Murphy et al. (2017) and contains free-form keystroke data from 103 subjects typing on a desktop keyboard over a long period (2.5 years) in a completely uncontrolled scenario.

I. Buffalo Dataset: Collected by Yan Sun et al. (2016), comprising desktop keystroke data from 148 subjects. Subjects were required to participate in 3 data collection sessions spanning 28 days. Each session required the subjects to complete two tasks: transcribing a pre-defined text and answering free-text questions. The dataset contains two subsets of data: 1) baseline and 2) keyboard variation data. In the baseline, subjects participated in 3 sessions using the same keyboard and used 3 different types of keyboards while collecting the keyboard variation data for 3 sessions.

J. HMOG Dataset: The hand movement, orientation, and grasp (HMOG) dataset uses accelerometer, gyroscope, and magnetometer readings to capture subtle hand micro-movements while participants tap on a screen. Data was collected from 100 participants during eight keystroke typing sessions. Participants were required to answer three questions per session by typing at least 250 characters for each question. Participants were required to perform the task while sitting and walking in a controlled environment. In addition to keystroke data, the accelerometer, gyroscope, and magnetometer data were also recorded for analysis (Senarath et al., 2023b; Sitova et al., 2016; Acien et al., 2021).

K. HuMIdb Database: The Human Mobile Interaction Database (HuMIdb) is a publicly accessible dataset comprising 5GB of data recorded from various mobile sensors through an unsupervised data collection approach. The dataset was gathered from 600 participants as they performed eight distinct tasks designed to reflect everyday mobile device interactions. These tasks included typing (name, surname, and a predefined sentence), tapping (pressing a sequence of buttons), swiping (upward and downward gestures), air movements (drawing circle and cross gestures in the air), handwriting (writing digits), and voice recording (speaking the sentence "I am not a robot"). Data collection occurred over five sessions, with a one-day interval between sessions (Sitova et al., 2016; Acien et al., 2021; Nguyen et al., 2024). In addition to keystroke and touchscreen data, the dataset includes sensor data from accelerometers, magnetometers, gyroscopes, orientation sensors, proximity sensors, gravity sensors, light sensors, GPS, WiFi, Bluetooth, and microphones. The data collection process was uncontrolled, ensuring the dataset reflected natural usage scenarios (Sitova et al., 2016; Acien et al., 2021; Nguyen et al., 2024).

L. FETA Dataset: The dataset was collected from 470 participants over 31 sessions. Participants were recruited via Amazon Mechanical Turk (MTurk), a crowdsourcing platform. An iOS application was developed to facilitate data acquisition, which recorded touch and sensor data as participants interacted with their mobile devices. Participants performed two primary activities: social media and image gallery tasks. The social media task aimed to simulate vertical scrolling behavior typical of activities such as browsing social media feeds or navigating through a list of news articles. This task was designed to collect touch data reflecting everyday user interactions with mobile devices. The image gallery task was implemented to capture horizontal scrolling data. During this task, participants browsed a horizontal list of images, with only one image visible at a time. They were instructed to count specific objects as they swiped through the gallery. This setup enabled the acquisition of detailed horizontal scrolling behavior (Georgiev et al., 2023; Nguyen et al., 2024).

2) Novel Datasets: According to our findings, several studies have collected their own data for keystroke behavior biometric analysis. The data collection strategy for such datasets has been described below:

A. Epp et al. (2011) collected both static and free-form keystroke data from 26 subjects in an uncontrolled manner. A specific application was built to record keystroke data based on the subject's current activity. At regular intervals, the computer program prompts the subject to review the keystroke text that was entered previously. Subsequently, the subject was required to complete an emotional state questionnaire and a static text task. Of 12 subjects, 10 were male and 2 were female, with the average age being 28.5 years.

B. Tsimperidis et al. (2017, 2020, I. 2018) collect free-form keystroke data using a developed free text keylogger called IRecU, which could be installed on any portable smart device with any version of MS Windows. In addition to keystroke data, subjects were also requested to provide demographic (Tsimperidis et al., 2017), academic degree information (Tsimperidis et al., 2020), and gender (I. Tsimperidis et al., 2018) information. According to the study, the software was distributed between 20/February/2014 and 27/December/2014.

C. Subash et al. (2023) collected free-form keystroke data for online fraud detection. A website consisting of 4 assessment-like tasks was developed for data collection. Recruited subjects were requested to perform all tasks, which included 2 tasks of answering the questions

and 2 tasks of copying the passage questions. Specifically, each subject was asked to write at least 100 words to collect enough volume of data. A sample size of 13 students was recruited for the study. In addition to keystroke data, questionnaires requesting demographic information, emotional state, and computer proficiency were also distributed.

D. Ulinskas et al. (2018) collected keystroke behavior data from 4 subjects between the ages of 22 and 33. The data collection procedure lasted 2 weeks, during which the subjects were required to participate in trials 3 times a day. During each trial, the subject entered a predetermined paragraph that varied as the day progressed.

E. Alshanketi et al. (2019) collected keystroke behavior data from 100 participants while they typed a variable one-time password (OTP) and a fixed password composed of strings. Specifically, participants were asked to enter the same fixed password followed by a generated OTP 10 times across two sessions. Data acquisition was facilitated through an Android mobile application installed on a Sony smartphone. Each participant was instructed to perform the tasks using the same device throughout the study.

F. Bours (2012) collected free-form keystroke data from 35 subjects recruited from Gjøvik University College (GUC), Norway. Subjects were requested to run an application on their systems for 6 days. This application records keystroke behavior data and sends it back for analysis. According to the author, only 25 subjects provided sufficient keystroke data for analysis.

G. Da Silva et al. (2016) collected keystroke and mouse data from 55 subjects playing the game League of Legends. All samples were acquired from the same set of devices. All subjects were required to play a match together. They were also free to decide which device they wanted to play on and which avatar they wanted to play with. Each subject had a different role in the game, which provided a heterogeneous sample for analysis. According to the study, each game lasted between 30 and 50 min. A background application was developed using C# to collect the necessary information.

Table 1
Summary of the various datasets implemented in keystroke behavioral biometric analysis.

Dataset Name	Implemented in Studies	Publicly Available	Sample Size	Environment	Type of Dataset	Forgery Samples	Number of Sessions
CMU	Andrean et al., 2020	Yes	51	Controlled	Static	No	8 (sessions separated ~1 day
Novel Dataset	Subash et al., 2023	No	13	-	Dynamic	No	1 (only 1 session recorded)
GREYC	Mhenni et al., 2019a	Yes	100	Controlled	Static	No	~5 (sessions separated by ~1 week)
WEBGREY-C		Yes	45	Uncontrolled	Static	Yes	5 (sessions separated by ~1 week)
CMU		Yes	51	Controlled	Static	No	8 (sessions separated ~1 day
CMU	Ceker and Upadhyaya, 2016	Yes	51	Controlled	Static	No	
CMU	Subash and Song, 2021	Yes	51	Controlled	Static	No	
CMU	Maheshwary et al., 2017	Yes	51	Controlled	Static	No	
CMU	Killourhy and Maxion, 2009	Yes	51	Controlled	Static	No	
Teh Dataset	Maiorana et al., 2019	Yes	150	Semi-Controlled	Static	No	1 (only 1 session recorded)
Palin Dataset	Senarath et al., 2023a	Yes	31,400	Uncontrolled	Dynamic	No	15 (time between sessions not defined
Palin Dataset	Senarath et al., 2023b	Yes	31,400	Uncontrolled	Dynamic	No	15 (time between sessions not defined
HMOGdb		Yes	99	Controlled	Dynamic	No	24 (time between sessions not defined
HuMIdb		Yes	428	Uncontrolled	Dynamic	No	5 (sessions separated by 1 day)
HMOGdb	Nguyen et al., 2024	Yes	99	Controlled	Dynamic	No	24 (time between sessions not defined
HuMIdb		Yes	428	Uncontrolled	Dynamic	No	5 (sessions separated by 1 day)
Palin Dataset		Yes	31,400	Uncontrolled	Dynamic	No	15 (time between sessions not defined
FETA Dataset		Yes	347	Uncontrolled	Dynamic	No	31 (sessions separated by 1 day)
Novel Dataset	Epp et al., 2011	No	12	Uncontrolled	Dynamic/ static	No	Continuous collection of keystroke data for ~4 weeks
Novel Dataset	Tsimperidis et al., 2017	No	-	Uncontrolled	Dynamic	No	Continuous collection of keystroke data for 10 months
Novel Dataset	Tsimperidis et al., 2020	Yes	-	Uncontrolled	Dynamic	No	Continuous collection of keystroke data for 10 months
Novel Dataset	I. Tsimperidis et al., 2018	No	75	Uncontrolled	Dynamic	No	Continuous collection of keystroke data for 10 months
Novel Dataset	Ulinskas et al., 2018	No	4	-	Static	No	14 (sessions separated by 1 day)
Novel Dataset	Alshanketi et al., 2019	No	100	Controlled	Static	No	2 (time between sessions not defined)
Novel Dataset	Bours, 2012	No	25	Uncontrolled	Dynamic	No	Continuous collection of keystroke data for ~6 days
Novel Dataset	Da Silva Beserra et al., 2016	No	55	Controlled	Dynamic	No	Sessions not specified (Data collected for ~4 months)
Novel Dataset	Krishnamoorthy et al., 2018	No	77	Uncontrolled	Static	No	~5 (sessions separated by 1 day)
CMU	A. Mhenni et al., 2018	Yes	51	Controlled	Static	No	8 (sessions separated ~1 day
WEBGREY-C		Yes	118	Uncontrolled	Static	No	5 (sessions separated by ~1 week)
Teh Dataset	Kalita et al., 2020	Yes	150	Uncontrolled	Static	No	1 (only 1 session recorded)
Antal Dataset		Yes	54	-	Static	No	3 (sessions separated by ~1 week)
Coakley Dataset		Yes	52	Controlled	Static	No	Session data not specified
Android Dataset	Daribay et al., 2019	Yes	42	Controlled	Static	No	2 (time between sessions not defined)
Dhakal Dataset	Acien et al., 2022	Yes	168,000	Uncontrolled	Dynamic	No	15 (time between sessions not defined
Palin Dataset		Yes	60,000	Uncontrolled	Dynamic	No	15 (time between sessions not defined
Clarkson Dataset		Yes	103	Uncontrolled	Dynamic	No	Continuous collection of keystroke data for ~2.5 years
Buffalo Dataset		Yes	148	Controlled	Dynamic	No	3 (sessions separated by ~28 days)
Palin Dataset	Stragapede et al., 2024	Yes	30,400	Uncontrolled	Dynamic	No	15 (time between sessions not defined

H. Krishnamoorthy et al. (2018) collected static keystroke data from 94 subjects using an Android application. This application prompts the subjects to type a pre-determined password (.tie5Roanl) 30 times over 5 days. Each subject provides 30 password entries. According to the author, the data collection process lasted 4 to 6 weeks, as the subjects could provide more entries in addition to the required 30 samples. Out of 94 subjects, only data supplied by 77 were valid after pre-processing.

Our investigation confirms that the data needed for keystroke analysis varies depending on the application device, whether desktop or mobile. If keystroke analysis is performed on mobile devices, additional raw data collected includes pressure (*pre*), area of touch (*AOT*), keyboard layout, touch coordinates (*TC*), and sensor data (accelerometer and gyroscope) (Kalita et al., 2020). Some studies also collect variable data; for example, Alshanketi et al. (2019) collected variable OTP and fixed password keystroke behavior data. After data collection, raw data, such as key press time, release time, unique key codes, name of the key, and timestamp of event occurrence (Andrean et al., 2020; Subash et al., 2023; Maiorana et al., 2019; Epp et al., 2011; Tsimperidis et al., 2017, 2020; Bours, 2012), are acquired for feature extraction.

Table 1 (Moved to Appendix) shows that most studies rely on publicly available datasets for keystroke behavioral biometric analysis, with over half utilizing such datasets. Among these, static datasets are commonly used despite the growing availability of dynamic datasets. This finding suggests that studies have a continued preference for static datasets in specific research contexts, potentially due to their availability, structured nature, and ease of implementation. Approximately 40 % of the analyzed studies collect novel datasets for particular applications, including user authentication on mobile devices (smartphones) and one-time password (OTP) authentication (Alshanketi et al., 2019). Notably, some of these novel datasets are static, indicating their use in applications that require authentication during login times. In some cases, static datasets have been collected for specific applications. For example, Ulinskas et al. (2018) collected static data for human fatigue analysis. In contrast, the majority of novel datasets are dynamic datasets designed for CA across several devices, such as desktops, laptops, and mobile platforms. In addition to security-related applications, some novel datasets have been collected for demography (age, gender), physiology (fatigue), and psychology (emotion detection)-related recognition, making them highly application-oriented. Recently published datasets, such as the BehavePass database, offer new opportunities for analysis (Stragapede et al., 2022), as it is one of the few datasets that have collected skilled forgery samples.

Further analysis shows that most novel datasets are not publicly accessible. This is because some datasets contain user-specific information, and making them accessible may raise privacy concerns and make them prone to misuse. Furthermore, stringent privacy laws, such as the General Data Protection Regulation (GDPR) in Europe, restrict data sharing that can potentially identify individuals.

3.2. Keystroke behavior features

In this section, we describe the features implemented for keystroke analysis. Based on our comprehensive review (Fig. 4), we find that several features, such as Hold time (*HT*), down-down time (*DD*), and up-down time (*UD*), were extracted from the raw data mentioned in Section 3.1 (Andrean et al., 2020; Subash and Song, 2021; Maheshwary et al., 2017; Epp et al., 2011; Tsimperidis et al., 2017). The description of the primary raw data and extracted features is shown below:

1) Basic Raw Data

A. Key Press Time (*PT*): the time taken to press a key. Denoted by PT_i, *where* $i = 0,1,2,\ 3 \ldots n$.

B. Key Release Time (*RT*): the time taken to release a key. Denoted by RT_i, *where* $i = 0,1,2,\ 3 \ldots n$.

C. Screen Touch Data: This feature includes features generated when the subject's finger touches the screen. Basic features such as finger Pressure (*P*), finger size (*FS*) or area of touch (*AoT*), and touch coordinates (*TC*) are collected. These features can only be collected from touchscreen-based devices like mobile devices.

D. Motion Data: Basic features under this category include accelerometer and gyroscope data. These features can be collected from sensors integrated into mobile touchscreen devices, like tablets and smartphones. The accelerometer and gyroscope data depict how subjects move and hold the mobile device. In addition to the accelerometer and gyroscope data, other sensor data, such as magnetometer data, have also been used in analysis.

2) Extracted Features

A. Hold Time (*HT*): Hold time is the time difference between a single key's press and release time. Normally denoted as HT_i, *where* $i = 0,1,2,\ 3 \ldots n$.

B. Down-down Time (*DD*): Like *HT, DD* time is the time difference between the press time of one key and the press time of the subsequent key. Normally denoted by DD_i, *where* $i = 0,1,2,\ 3\ldots, n$.

C. Up-down Time (*UD*): This feature is keystroke latency or flight time. It can be defined as the time difference between the key's release time and the subsequent key's press time. Unlike other attributes, the value of this feature can be negative. It is denoted by UD_i, *where* $i = 0,1,2,\ 3\ldots, n$.

D. Down-up Time (*DU*): This feature can be defined as the time difference between the press time of one key and the release time of the subsequent key. It is denoted by DU_i, *where* $i = 0,1,2,\ 3\ldots, n$.

E. Up-Up Time (*UU*): The time difference between the key's release time and the subsequent key's release time. It is denoted by UU_i, *where* $i = 0,1,2,\ 3\ldots\ n$.

F. Aggregate Data (*Agg*): These features include aggregate information such as mean (*mean*), minimum (min), maximum (max), and standard deviation (*std*) of *UD, PT, HT, P,* and *AOT*.

Few studies have also analyzed and detected the most frequently used digraphs among the recruited subjects and used specifically developed programs to extract relevant keystroke behavior features (Tsimperidis et al., 2017; Bours, 2012). For example, Tsimperidis et al. (2017) developed the ISqueeze application, which reads raw keystroke log files collected using the IReCU keylogging application and extracts average keystroke latency time. Similarly, Bours (2012) chose specific keys and key combinations for user profile creation.

Fig. 3 lists several behavioral features currently used in keystroke behavioral biometric research. Based on our analysis, the most frequently used features include a combination of *HT, DD*, and *UD* times. Several other features such as cumulants, touch coordinates (*TC)*, interquartile range (*IQR*), key codes (*KC*), accelerometer sensor data (*ASD*), swipe information, gyroscope sensor data (*GSD*), GPS information, wireless connection data (WiFi Sensor), gravity sensor data, rotation sensor data, proximity sensor data, magnetometer sensor data, press speed, content-based attributes, and several other unique features, including the combination of statistical and information-theoretic measures were also used for keystroke behavioral biometric analysis.

3.3. AI approach and evaluation metrics used in keystroke behavioral biometrics

According to analysis, we find that ML approaches, such as Multi-Layer Perceptron (MLP) (Andrean et al., 2020; Maheshwary et al., 2017; Tsimperidis et al., 2017; I. 2018), Decision Trees (DT) (Epp et al., 2011), Support Vector Machines (SVM) (Ceker and Upadhyaya, 2016; Ulinskas et al., 2018), Gaussian mixture Models (GMM) (Kalita et al., 2020), Random Forest (RF), Naive Bayesian (NB) (Alshanketi et al., 2019; Daribay et al., 2019), Radial Basis Function Network (RBFN) (I. Tsimperidis et al., 2018), XGBoost (Daribay et al., 2019), *K*-Nearest Neighbor (*K*NN) (Mhenni et al., 2019a), Linear Regression (LR) (Daribay

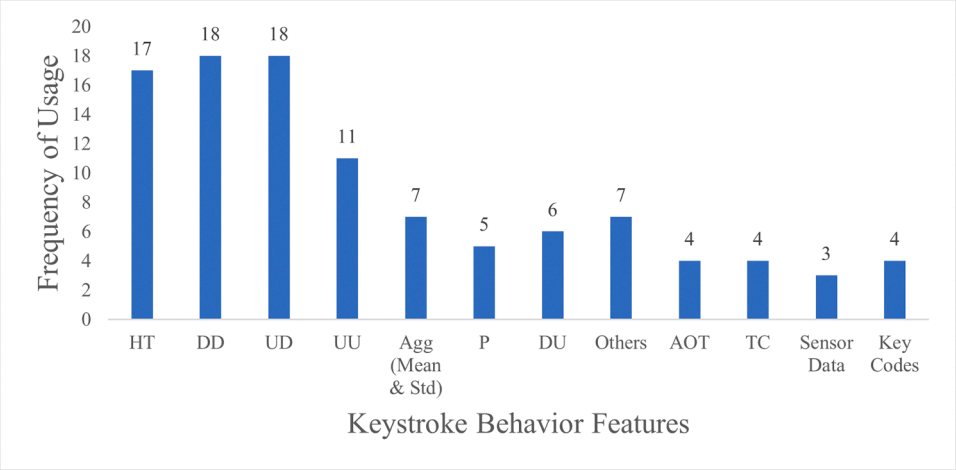

Fig. 3. Keystroke behavior features distribution.

et al., 2019), and Random Radial Basis Function Network (R^2BFN) (Tsimperidis et al., 2020) have been implemented for keystroke behavioral biometric-based authentication. In addition to ML approaches, DL approaches, and distance-based anomaly detection methods (DBAD) have also been used for classification. These include Convolutional Neural Networks (CNNs) (Subash et al., 2023; Subash and Song, 2021; Maiorana et al., 2019), Recurrent Neural Networks (RNNs) (Subash et al., 2023; Daribay et al., 2019), and transformers (Subash et al., 2023), along with anomaly detection techniques leveraging Euclidean, Mahalanobis, and Manhattan distance metrics (Killourhy and Maxion, 2009).

Researchers also use sampling, data condensation (data reduction), and feature selection methods before feeding extracted features into the ML or DL approaches. Some methods implemented include correlation-based feature subset attribute selection (Epp et al., 2011), information gain (IG) (I. Tsimperidis et al., 2018), minimum redundancy maximum relevance (mRMR) (Krishnamoorthy et al., 2018), under-sampling (Epp et al., 2011), GLDA-TRA (Ulinskas et al., 2018), and filter-based random sub-field data condensation method (Tsimperidis et al., 2020). Furthermore, specific pre-processing methods, such as segmentation, are also used to prepare the data for analysis. For example, Subash et al. (2023) implemented this process to generate logical blocks of attributes to create session data. Specifically, keystroke data is converted into 5-character length records to simulate session-like data.

Our analysis (Table 2) shows that only a few research studies implemented distance-based anomaly detectors and fuzzy logic for keystroke analysis. Statistically, most of the studies analyzed relied on state-of-the-art (SOTA) DL approaches for classification. Further investigation shows that MLP and transformer-based DL architectures are the most popular approaches implemented for keystroke behavioral biometric analysis. It is important to note that this statistic also includes research studies that conduct comparative analyses between approaches.

Most studies analyzed in this paper fall under empirical research, which is evaluated using several evaluation metrics. These include equal error rate (EER) (Andrean et al., 2020; Maheshwary et al., 2017), accuracy (Acc) (Andrean et al., 2020; Maheshwary et al., 2017; Maiorana et al., 2019; Epp et al., 2011; Tsimperidis et al., 2017; Kalita et al., 2020), precision (PRE), recall (REC), kappa statistics (KS), area under curve (AUC), receiver operating characteristic (ROC) curve (Andrean et al., 2020; Ceker and Upadhyaya, 2016; Kalita et al., 2020), root mean square error (MSE), and mean absolute error (MAE) (Andrean et al., 2020; Ceker and Upadhyaya, 2016; Kalita et al., 2020). Other evaluation metrics, such as time complexity (TBM), false rejection rate (FRR), false acceptance rate (FAR), and stability (Tsimperidis et al., 2020; I. 2018), have also been used for evaluation. The summary of the evaluation metrics utilized in research studies is depicted in Table 3.

We also confirm that different techniques were used for evaluation, including cross-validation (Maheshwary et al., 2017; Epp et al., 2011; Tsimperidis et al., 2017, 2020) and a hold-out approach (Subash et al., 2023; Subash and Song, 2021; Daribay et al., 2019). Furthermore, comprehensive experimentations are performed by comparing performance achieved using different numbers of classes (I. Tsimperidis et al., 2018), classification approaches (Subash et al., 2023; Ceker and Upadhyaya, 2016; Maheshwary et al., 2017; Tsimperidis et al., 2020; I. 2018), model architectures (Maiorana et al., 2019), model parameters (Learning rate and momentum), varied number of hidden layer neurons (Tsimperidis et al., 2017), different number of features (I. Tsimperidis et al., 2018; Krishnamoorthy et al., 2018; Kalita et al., 2020), and pre-processing methods (Kalita et al., 2020). We also confirm that a few studies develop their evaluation categorization based on already established evaluation metrics, such as True Positives (TP) and False Positives (FP) (Epp et al., 2011).

Studies also propose using different evaluation metrics to evaluate keystroke-based authentication methods. For example, according to Bours (2012), continuous keystroke behavioral biometric systems have better reflections than EER systems. Alternatively, the speed at which an imposter is detected, i.e., the number of keystrokes the imposter can use before the system's trust falls below a specified threshold, is a better indication of performance. To accomplish this, the study develops a continuous keystroke dynamic (CKD) authentication system that implements a penalty and reward function that adapts the trust level of the system. Similarly, studies performed by (Senarath et al., 2023a, Senarath et al., 2023b) also propose unique evaluation metrics, such as usability, time to correct reject (TCR), false reject worse interval (FRWI), and false acceptance worse interval (FAWI) for performance evaluation.

Some studies also conduct reliability analysis to determine if the identified features result in effective keystroke behavior biometric-based authentication. For example, Subash et al. (2023) propose to evaluate DL models with a significantly larger publicly available dataset (CMU benchmark) containing the same features as the ones identified in the study. Specifically, the study compares its novel data with a publicly available (CMU benchmark dataset) dataset containing the same features (Subash et al., 2023).

Only some studies evaluate different fusion approaches. Alshanketi et al. (2019) propose a multimodal keystroke-based authentication scheme that combines keystroke behavior obtained from OTP and fixed passwords. Furthermore, two fusion models were built and compared: matching decision and feature-level fusion methods.

Comparisons are also conducted between different loss functions. For

Table 2
Summary of AI approaches implemented for keystroke behavioral biometrics.

ML	DL	Distance-based Anomaly Detection	Author
No	MLP	No	Andrean et al., 2020
No	CNN, Transformers, LSTM	No	Subash et al., 2023
GA-*K*NN (Euclidean, Manhattan, Mahalanobis, Hamming, Statistical)	No	No	Mhenni et al., 2019a
A-SVM, DA-SVM, PMT-SVM	No	No	Ceker and Upadhyaya, 2016
No	CNN	No	Subash and Song, 2021
No	MLP	No	Maheshwary et al., 2017
SVM, *K*-means	NN	Manhattan, Euclidean, Mahalanobis, Nearest Neighbor (Mahalanobis), Fuzzy Logic, Outlier Score	Killourhy and Maxion, 2009
No	CNN	No	Maiorana et al., 2019
RF, KNN, GBC	TypeNet, TypeFormer (Transformer), HuMINet	No	Senarath et al., 2023a
x	BehaveFormer (Transformer)	No	Senarath et al., 2023b
x	STDAT-based BehaveFormer	No	Nguyen et al., 2024
DT	No	No	Epp et al., 2011
No	MLP	No	Tsimperidis et al., 2017
No	R^2BFN	No	Tsimperidis et al., 2020
SVM, RF, NB	MLP, RBFN	No	I. Tsimperidis et al., 2018
SVM	No	No	Ulinskas et al., 2018
RF	No	No	Alshanketi et al., 2019
No	No	Distance-Based Anomaly Detection + Trust System	Bours, 2012
*K*NN, SVM, RF	MLP	No	Da silva et al., 2016
SVM-linear, SVM-RBF, RF	No	No	Krishnamoorthy et al., 2018
*K*NN	No	No	A. Mhenni et al., 2018
GMM	No	No	Kalita et al., 2020
LR, XGBoost, GNB	MLP, LSTM, GRU	No	Daribay et al., 2019
No	RNN-TypeNet Architecture	No	Acien et al., 2022
x	Transformer	No	Stragapede et al., 2024

example, Acien et al. (2022) propose TypeNet, an RNN-LSTM architecture for keystroke biometric authentication for large-scale free-form text scenarios. Different models were trained using 3 different loss functions, namely softmax, triplet, and contrastive loss, and then compared. Furthermore, a comparison between 1) different numbers of training samples and lengths of keystroke sequences, 2) conventional statistical models and deep learning architectures, and 3) types of device datasets collected from touchscreen and physical keyboard datasets was also performed.

3.4. Keystroke behavioral biometrics research applications

Keystroke behavioral biometric research is implemented for several real-world applications, including identity theft detection, which covers user authentication and identification (Maheshwary et al., 2017). In addition to security-related applications, researchers have used keystroke behavioral biometrics to determine a user's age, educational level, online assessment fraud, fatigue, and emotion (Epp et al., 2011).

Recently, studies have also focused on predicting user characteristics based on keystroke behavior analysis (Tsimperidis et al., 2017). Specifically, research performed by Tsimperidis et al. (2017) and I. Tsimperidis et al. (2018) has expanded keystroke behavioral biometrics toward identifying user characteristics such as age, gender, and operation handedness. In addition, researchers can also determine the education level of the person behind the keyboard (Tsimperidis et al., 2020).

Keystroke behavioral biometrics is also used to detect user fatigue levels. For example, Ulinskas et al. (2018) gathered data at different times of the day based on the assumption that users become more tired as the day progresses. Keystrokes entered by a subject in the morning are believed to reflect those of a non-fatigued user. As the day goes on, the user is assumed to become moderately or fully fatigued. Consequently, the study classifies high, medium, and low fatigue levels. Additionally, the study employs unique features, including a combination of statistical and information-theoretic measures for classification.

Keystroke behavioral biometric-based research has found its way into the medical field, specifically for the early detection and monitoring of Parkinson's disease (PD) (Iakovakis et al., 2018). The research mainly uses touchscreen keystroke behavior to estimate the severity of motor impairment in PD patients. This is accomplished by analyzing keystroke behavior recorded in clinical settings and everyday use of smartphones. According to the author, results indicated that the models can accurately estimate motor symptoms, making it a promising method for PD detection and monitoring. Similarly, researchers also investigate using keystroke behavioral biometrics as early warning signals to monitor disease activity in Multiple Sclerosis (MS) patients (Twose et al., 2020).

Another interesting application of keystroke behavioral biometrics is identifying users in the mobile domain (Maiorana et al., 2019; Kalita et al., 2020). The research makes use of a combination of keystroke behavior features with pressure (Maiorana et al., 2019; Kalita et al., 2020), touch data (swiping, gesture), sensor data (accelerometer, gyroscope, gravity, light, magnetometer, WiFi connections, Bluetooth, location (GPS) (Kalita et al., 2020) for user authentication and identification. Furthermore, studies have also focused on adapting current keystroke behavioral biometric methods to long-term and short-term user behavior changes (Mhenni et al., 2019a, 2018; Ceker and Upadhyaya, 2016; Subash and Song, 2021). However, there are very few studies that focus on this. The adaptability of behavioral biometric modalities has been explained in detail in future sections. Fig. 4 shows the summary of the research applications of keystroke behavioral biometrics.

Based on our investigation, we confirm that most keystroke-based behavioral biometric research is implemented for security-based applications, including user identification and authentication (Fig. 4). It is also noticed that a small proportion of studies also focus on other research applications, including online assessment fraud detection, emotion recognition, fatigue recognition, adaptability, user characteristics (age, operation handedness, and gender prediction) recognition, and disease monitoring and prediction (Fig. 4).

4. Mouse behavioral biometrics

Another alternate approach to keystroke behavioral biometrics is mouse behavioral biometrics, which verifies user identity by analyzing observable mouse actions (Zheng et al., 2011). Studies show that behavioral biometrics first acquired popularity with research on keystroke behavioral biometrics. Later, research in mouse behavioral

Table 3
Evaluation metrics used in keystroke behavioral biometrics.

Author	AUC	FAR	FRR	Acc	MAE/MSE	ROC	EER	Pre/Rec/F Measure	Others
Andrean et al., 2020	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Subash et al., 2023	No	No	No	Yes	No	No	No	Yes	Yes
Mhenni et al., 2019a	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No
Ceker and Upadhyaya, 2016	Yes	No	No	No	No	Yes	No	No	No
Subash and Song, 2021	No	No	No	Yes	No	No	No	Yes	No
Maheshwary et al., 2017	No	No	No	Yes	No	Yes	Yes	No	Yes
Killourhy and Maxion, 2009	No	No	No	No	No	Yes	Yes	No	Yes
Maiorana et al., 2019	No	No	No	Yes	No	No	Yes	No	Yes
Senarath et al., 2023a	No	No	No	No	No	No	Yes	No	Yes
Senarath et al., 2023b	No	No	No	No	No	No	Yes	No	Yes
Nguyen et al., 2024	No	No	No	No	No	No	Yes	No	Yes
Epp et al., 2011	No	No	No	Yes	No	No	No	No	Yes
Tsimperidis et al., 2017	No	No	No	No	No	No	Yes	Yes	No
Tsimperidis et al., 2020	No	No	No	Yes	No	Yes	No	No	Yes
I. Tsimperidis et al., 2018	Yes	No	No	Yes	No	No	No	No	Yes
Ulinskas et al., 2018	No	No	No	Yes	No	No	No	No	No
Alshanketi et al., 2019	No	Yes	Yes	No	No	Yes	Yes	No	No
Bours, 2012	No	No	No	No	No	No	No	No	Yes
Da silva et al., 2016	No	No	No	Yes	No	No	No	No	No
Krishnamoorthy et al., 2018	No	No	No	Yes	No	No	No	No	Yes
A. Mhenni et al., 2018	Yes	No	No	No	No	Yes	Yes	No	No
Kalita et al., 2020	No	No	No	No	No	Yes	Yes	No	No
Daribay et al., 2019	Yes	Yes	Yes	Yes	No	Yes	No	No	No
Acien et al., 2022	No	No	No	No	No	Yes	Yes	No	No
Stragapede et al., 2024	No	Yes	Yes	No	No	No	Yes	No	No

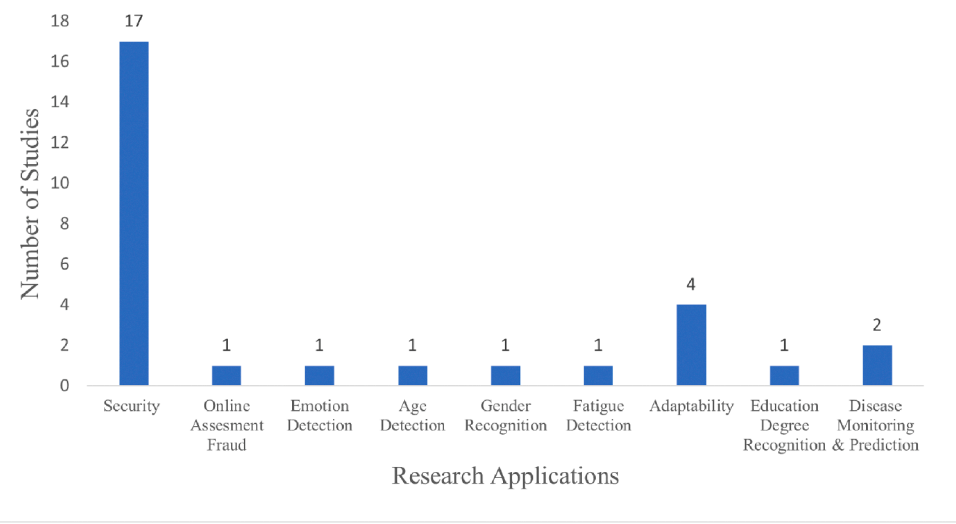

Fig. 4. Keystroke behavioral biometrics research applications.

biometrics gained traction with several articles, including Ahmed and Traore (2005).

Like keystroke, mouse behavioral biometric authentication also falls under user authentication and identification scenarios (Almalki et al., 2023).

4.1. Type of mouse behavioral biometric datasets

Like keystrokes, mouse behavioral biometrics-based research datasets are also of two types: static and dynamic datasets. 1) Static datasets collect mouse behavior data from subjects while they perform a specific mouse operation task using specifically designed web applications, while 2) Free-form datasets collect data during continuous monitoring of subjects' daily activities using background mouse logging applications (Fu et al., 2020).

This section provides a detailed overview of the datasets currently used in mouse behavioral biometric analysis (Table 4—Moved to appendix).

1) Public Datasets

A. Minecraft Dataset: This dataset collected (Siddiqui et al., 2021) mouse behavior data from 10 subjects who played a Minecraft game on a desktop computer for 20 min. According to the author, data collection was conducted in a controlled setting. Furthermore, a Python program was implemented for data collection.

B. Balabit Dataset: This publicly available dataset collected mouse behavior data from 10 subjects while they worked over remote desktop clients connected to remote servers. The data collected is divided into two folders: training and testing (Almalki et al., 2023; Antal and Egyed-Zsigmond, 2018).

C. DFL Dataset: This publicly available dataset collects mouse behavior data from 21 subjects using specific data collection software installed in their systems to record data while they perform their daily activities. Data is also collected from different devices,

Table 4
Summary of the various datasets implemented in mouse behavioral biometric analysis.

Dataset Name	Author	Publicly Available	Sample Size	Environment	Type of Dataset	Forgery Samples	Number of Sessions
Novel Dataset (Minecraft Dataset)	Siddiqui et al., 2021	Yes	10	Controlled	Dynamic	No	Session data not specified
Novel Dataset	Zheng et al., 2011	No	30	Controlled	Dynamic	No	Session data not specified
Novel Dataset		No	1000	Uncontrolled	Dynamic	No	Continuous collection of mouse behavior data
Novel Dataset	Da Silva Beserra et al., 2016	No	55	Controlled	Dynamic	No	Sessions not specified (Data collected for ~4 months)
Balabit Dataset	Almalki et al., 2023	Yes	10	Uncontrolled	Dynamic	No	Continuous collection of mouse behavior data
Novel Dataset	Fu et al., 2020	No	15	Controlled	Static	No	Session data not specified
Balabit Dataset	Antal and Egyed-Zsigmond, 2018	Yes	10	Uncontrolled	Dynamic	No	Continuous collection of mouse behavior data
Balabit Dataset	Antal and Denes-Fazakas, 2019	Yes	10	Uncontrolled	Dynamic	No	Continuous collection of mouse behavior data
Choa Shen Dataset		Yes	28	Controlled	Dynamic	No	30 (sessions separated by ~1 day)
DFL Dataset		Yes	21	Uncontrolled	Dynamic	No	Continuous collection of mouse behavior data
Novel Dataset	Subash et al., 2024	No	10	-	Static	No	1 (only 1 session recorded)
Novel Dataset	Shen et al., 2013	Yes	37	Controlled	Static	No	15 – 60 (sessions separated by ~1 day)
Novel Dataset	Wang et al., 2019	No	18	Controlled	Dynamic	No	4 (sessions separated by 1 day)
Novel Dataset	Gamboa and Fred, 2004	No	50	-	Static	No	Session data not specified
Novel Dataset	Feher et al., 2012	No	25	Controlled	-	Yes	Session data not specified
Balabit Dataset	Hu et al., 2019	Yes	10	Uncontrolled	Dynamic	No	Continuous collection of mouse behavior data
Balabit Dataset	Antal and Fejér, 2020	Yes	10	Uncontrolled	Dynamic	No	Continuous collection of mouse behavior data
DFL Dataset		Yes	21	Uncontrolled	Dynamic	No	Continuous collection of mouse behavior data

such as desktops, laptops, and mouse devices (external mouse and touch pads) (Antal and Denes-Fazakas, 2019).

D. Choa Shen Dataset: This publicly available dataset collects (Shen et al., 2012) mouse behavior data from 28 subjects using a background monitoring application. Specifically, this application records mouse behavior data while subjects perform daily activities. According to the study, each subject performs 30 sessions over 2 months, each containing 30 min of mouse behavior data.

2) Newly Collected (Novel) Datasets:

A. Zheng et al. (2011) performed a measure-based study by collecting two types of mouse behavior data. 1) Controlled Set: 30 subjects participated in the data collection process in a standard environment. Subjects belong to different ages, occupations, and educational backgrounds. RUI logging tool records mouse behavior data while subjects perform their routine activities. Activities include word processing, surfing the net, programming, online chatting, and playing games. 2) Uncontrolled set (field set): Collects mouse behavior data from 1000 unique users using JavaScript.

B. Fu et al. (2020) evaluated their proposed approach using a dataset provided by Xi'an Jiaotong University of China. Mouse behavior data were collected from 15 subjects while they performed a specific authentication task. It is important to note that the subjects had different ages, educational backgrounds, and occupations. In this task, subjects were required to find and click targets prompted by the data collection program. The study collected all the data on an HP workstation with a 17-inch LCD monitor and Windows operating system.

C. Subash et al. (2024) collected application-oriented mouse behavior data from 10 subjects while they performed specific online assessment-like tasks. Subjects participated in 3 tasks, which included clicking the target, multiple-choice questions (MCQ), and matching tasks. The main objective was to collect many varieties of mouse events and large amounts of data for effective online fraud detection. Furthermore, a website application was developed for data collection. The author gathered subjects from the Sanjay Gandhi College of Education, India.

D. Shen et al. (2013) collected mouse behavior data from 37 subjects in a controlled setting. The author develops a Windows application that prompts subjects to perform a specific task. According to the author, the application displays the tasks on a full screen and records data while they perform them. The task includes 16 mouse movements and 8 single and double-click events. Each subject performs the task 20 times over 2 rounds. According to the study, each subject takes 15 to 60 days to complete the data collection process.

E. Wang et al. (2019) collected mouse behavior data from 18 subjects. The data collection procedure requires subjects to perform 2 tasks after their emotions are aroused. Several videos are used for this purpose. Specifically, 3 videos are used to stimulate positive, negative, and neutral emotions. Furthermore, a face reader is also used to detect emotional changes. A well-structured academic website is developed for data collection. Subjects were required to perform 2 tasks immediately after they watched the video.

F. Gamboa and Fred (2004) used a developed web application to collect mouse behavior data from 50 subjects. Subjects were required to participate in a memory game that spanned 10–15 min. The study collected and created an interaction repository containing 10 h of mouse behavior data.

G. Siddiqui et al. (2021) collected mouse behavior data from 10 subjects while they played Minecraft on a desktop computer. Each subject was required to play the game on the same desktop system. A Python program ran in the background for 20 min and recorded the necessary mouse behavior data.

H. Feher et al. (2012) collected mouse behavior data from 25 subjects from different groups: 1) Internal and 2) External subjects. According to the author, the systems used for data collection were chosen from various brands and hardware configurations. Furthermore, one or more internal subjects are authorized to interact with a particular system, while the rest are not.

From Table 4 (moved to appendix), we conclude that most studies rely on novel datasets for mouse behavioral biometric analysis, as most publicly available datasets are dynamic. However, despite the

availability of dynamic mouse behavior data, static datasets are still being implemented in research due to the need for specific datasets for user authentication. Since most mouse behavioral biometric-based research is focused on security-related applications, dynamic datasets are commonly used (Table 4 – moved to appendix) as these datasets better reflect user behavior in real-world scenarios. However, if studies focus on CA in specific scenarios, such as online education platforms (Subash et al., 2024), specific behavior data is required for analysis. In this example, the collected data must emulate user behavior on online education platforms, after which, utilizing this data for user authentication will enhance the validity and reliability of the results. Furthermore, some studies also collected static data as they focused on static authentication, mainly simulating user authentication during log-in time.

After data collection, researchers are left with raw mouse behavior data. They include the following: action type (Siddiqui et al., 2021; Fu et al., 2020; Subash et al., 2024), coordinates (Siddiqui et al., 2021; Fu et al., 2020; Subash et al., 2024), timestamp (*ms*) (Siddiqui et al., 2021; Fu et al., 2020; Subash et al., 2024), screen height (Subash et al., 2024), screen width (Subash et al., 2024), button state (Siddiqui et al., 2021), *rtime* (Siddiqui et al., 2021), and *ctime* (Siddiqui et al., 2021). This raw data is taken, pre-processed, and then sent for feature extraction.

4.2. Segmentation and pre-processing for mouse behavioral biometrics

Segmentation is a process that divides mouse behavior data into meaningful and logical blocks of information. It is a pre-processing step implemented to extract aggregate features that help in profiling users for effective user authentication and identification. In this section, we present our unique taxonomy for classifying various segmentation methods into two main categories: event-based and image-based segmentation methodologies.

4.2.1. Event-Based segmentation methodology

Event-based segmentation methodology involves identifying logical sequences of data by analyzing basic mouse events present in mouse behavior data. Specifically, data is examined to detect various event types (mouse move, mouse click, drag, and dragend), which serve as the basis for segmentation. According to our analysis, the following segmentation methods fall under this category:

4.2.1.1. Point-and-Click (PC) segmentation.

- A point-and-click segment is a series of continuous mouse-move events that end with a click event, which in some cases includes a mouse press and release event. Continuous mouse-move events can be further defined as a series of mouse-move events with little to no pause between each adjacent event. It is important to note that multiple PC actions are extracted for mouse behavioral biometric analysis (Zheng et al., 2011). For example, let j be the total number of point-and-click actions. Each *j*-th action will be composed of *i* mouse movement events denoted by $<\text{mouse move}_i, x_i, y_i, \text{timestamp}_i>_j$.

4.2.1.2. Mouse-Move (MM) segmentation.

- An alternative segmentation method involves using a sequence of mouse move-move (MM) events as a segment for mouse behavioral biometric analysis. Specifically, studies use a fixed number of MM events to generate a single action. According to our analysis, the number of MM events used for segmentation varies. For example, Subash et al. (2024) used 3 MM events per segment, while Siddiqui et al. (2021) used 10 MM events per segment.

- In addition to using a fixed number of MM events to segment the data, another approach involves identifying partial mouse movement (PMM) segments. This segment consists of MM events that do not end in a click event. Specifically, it represents a general MM action type that describes movement behavior between two points on a screen (Almalki et al., 2023; Antal and Egyed-Zsigmond, 2018). PMM actions are usually isolated using the timestamp field (Antal and Egyed-Zsigmond, 2018).

4.2.1.3. Drag-Drop (DD) segments.

- In addition to PC and PMM segments, drag-and-drop (DD) segments (Almalki et al., 2023; Antal and Egyed-Zsigmond, 2018) have also been extracted. These DD segments contain a series of events starting with a mousedown event, followed by multiple drag events, and concluding with a mouse release event.

4.2.1.3. Click segments.

- Another alternative segment type consists only of a click event without any mouse movements before it. This type of segment is known as Pause-and-Click. It occurs when users pause for a certain amount of time before clicking (Zheng et al., 2011).

4.2.2. Image-Based segmentation methodology

- Image-based segmentation methodology aims to uniquely map raw mouse behavior data into images to preserve all user data for reliable user authentication. Our analysis indicates that this innovative pre-processing technique was initially observed in the research performed by Hu et al. (2019). According to the study, unlike conventional feature extraction methods, this approach preserves all information regarding an individual's mouse behavior by mapping basic mouse events into graphs, which are subsequently converted into images. Various image sets are created based on different numbers of basic mouse events ($n = 25$, 50, 100, 500, 1000). Data augmentation is then employed to expand the dataset, and finally, a 7-layer CNN architecture is implemented for classification.

4.3. Mouse behavioral biometric features

After segmentation, several mouse behavior features are extracted and implemented for analysis. These features have been extracted using the raw mouse behavior data mentioned in Section 4.1. The description of basic and extracted features has been illustrated below:

1) Basic Features
A. Screen Coordinates (*Crd*): Describes the location or screen coordinate at which the mouse event is performed. This attribute represents a 2D coordinate system with *x* and *y* coordinates.
B. Timestamp (*t*): This represents the time the mouse event is performed. It is usually measured in milliseconds (ms).
C. Action Type (*AT*): This represents the mouse event performed. These events include mouse move, mouse click, drag and drop, and scroll.
D. Screen height and Screen Width (*SH, SW*): Represents the screen height and width of the web browser component that renders website content. The subject's slight changes in screen height and width are noticed and recorded.
2) Extracted Features
A. Angle of Curvature (AOC): For any 3 recorded points A, B, and C, the angle of curvature is defined as the angle ABC, the angle between the line AB and BC.
B. Curvature Distance (CD): For three recorded points, A, B, and C, the curvature distance can be defined as the ratio between the length of line AC and the perpendicular distance of point B to the line AC. Specifically, this ratio is between two distances.

C. Speed (S): This feature is usually calculated between each point-and-click action. It is defined as the ratio between the traveled distance for that action and the time taken to complete that action.
D. Pause-and-Click (PauC): This attribute represents the time difference between the end of the movement and the click event. Specifically, it is the duration between the amount of time pausing and clicking the target.
E. Velocity: This feature represents the velocity measurement between mouse events. Velocity is divided into directional velocities measured in x (HV_i), y-axis (VV_i), and tangential velocity (TV_i). The formula to calculate all 3 types of velocity is shown in Eqs. (1), 2, and 3.

$$HV_i = \frac{x_i - x_{i-1}}{t_i - t_{i-1}},\ where\ i = 2, .., n \tag{1}$$

$$VV_i = \frac{y_i - y_{i-1}}{t_i - t_{i-1}},\ where\ i = 2, .., n \tag{2}$$

$$TV_i = \sqrt{HV_i^2 + VV_i^2},\ where\ i = 2, .., n \tag{3}$$

F. Coordinate difference (dx, dy): The difference between the x, and y coordinates, respectively. The formula for calculations is shown in Eqs. (4) and 5.

$$dx_i = x_i - x_{i-1},\ where\ i = 2, .., n. \tag{4}$$

$$dy_i = y_i - y_{i-1},\ where\ i = 2, .., n. \tag{5}$$

G. Acceleration (A): Is the velocity change in unit time, which is represented as TA. Like velocity, acceleration is also divided into directional accelerations, measured on the x-axis (Ax) and y-axis (Ay), and tangential acceleration (TA), which is acceleration across the mouse plane. The formulas are shown in Eqs. (6), 7, and 8.

$$Ax_i = \frac{HV_i - HV_{i-1}}{t_i - t_{i-1}},\ where\ i = 2, .., n. \tag{6}$$

$$Ay_i = \frac{VV_i - VV_{i-1}}{t_i - t_{i-1}},\ where\ i = 2, .., n. \tag{7}$$

$$TA_i = \sqrt{Ax_i^2 + Ay_i^2},\ where\ i = 2, .., n. \tag{8}$$

H. Jerk (J): Is the change in acceleration per unit time. Like acceleration and velocity, jerk can also be measured directionally. Jerk is on the x-axis (Jx), y-axis (Jy), and along the mouse plane (TJ). The formulas for jerk are mentioned in Eqs. (9), 10, and 11.

$$Jx_i = \frac{Ax_i - Ax_{i-1}}{t_i - t_{i-1}},\ where\ i = 2, .., n. \tag{9}$$

$$Jy_i = \frac{Ay_i - Ay_{i-1}}{t_i - t_{i-1}},\ where\ i = 2, .., n \tag{10}$$

$$TJ_i = \sqrt{Jx_i^2 + Jy_i^2},\ where\ i = 2, .., n. \tag{11}$$

I. Angular Movement (θ_i): This feature represents the path angle between mouse movement and the screen's horizontal axis. It is measured using the atan or arctan function on the differential of x and y coordinates. The formula is shown in Eq. (12).

$$\theta_i = \frac{dy_i}{dx_i},\ where\ i = 2, .., n. \tag{12}$$

J. Travelled Distance (TD) or Distance end-to-end (DE): Is the distance between the first and last data points in a mouse action. This feature is determined using Eq. (13).

$$TD = \sqrt{(x_n^2 - x_i^2) + (y_n^2 - y_i^2)},\ where\ i = 2, .., n \tag{13}$$

K. Trajectory Length (TL): The sum of the distance between all data points in a mouse action. This feature is determined by Eq. (14).

$$TL = \sum_{i=1}^{n} \sqrt{(x_i^2 - x_{i-1}^2) + (y_i^2 - y_{i-1}^2)},\ where\ i = 2, .., n \tag{14}$$

L. Angular Velocity (AV): Angular velocity is defined as the rate of angular movement of the cursor over time. This feature is determined using Eq. (15).

$$AV_i = \frac{d\theta_i}{dt_i},\ where\ i = 0,\ 1,\ 2, ...n. \tag{15}$$

M. Straightness (SR): The ratio between total distance traveled and trajectory length. This feature determines the straightness of the mouse path. If the path is straight, the ratio value is 1; otherwise, the ratio value is between 0 and 1. The straightness is measured using Eq. (16).

$$SR = \frac{TD}{TL}. \tag{16}$$

N. Curvature (C): It is the ratio between the rate of change of angular movement and distance traveled. This feature is determined by Eq. (17).

$$C = \frac{d\theta_i}{TD_i},\ where\ i = 2, .., n. \tag{17}$$

Similarly, the rate of change of curvature is calculated using Eq. (18).

$$Rate\ of\ Change\ of\ Curvature\ (RC) = \frac{dC_i}{TD_i},\ where\ i = 2, .., n. \tag{18}$$

O. Sum of Angles (SOA): The cumulative angular movement values of an action. The feature is determined from Eq. (19).

$$SOA = \sum_{i=1}^{n} \theta_i\ Where\ i = 0,\ 1, .., n. \tag{19}$$

P. Number of Points (NOP): Refers to the number of data points in an action and is represented by NOP. This feature has been shown in Eq. (20).

$$NOP = N_i,\ where\ i = 0,\ 1, .., n. \tag{20}$$

Q. Sharp Angles (SA): This feature represents instances where the mouse movement abruptly changes quickly during the cursor's trajectory. It is typically obtained by observing whether the angular movement values are below a certain threshold (TH), indicating sharp direction changes, as shown in Eq. (21).

$$SA = \theta_i | \theta_i < TH,\ where\ i = 0,\ 1, .., n.. \tag{21}$$

R. Number of Critical Points (*NOC*): This feature is calculated from the curvature vector by searching for high curvature points. It is acquired by observing whether curvature values exceed a certain threshold (*TH*), as indicated in Eqs. (22) and 23.

$$NOC = \sum_{i=1}^{n} zi, \ where \ i = 0, 1, .., n. \tag{22}$$

$$z_i = \begin{cases} 1, & and \ dC > TH \\ 0, & and \ Otherwise \end{cases} \tag{23}$$

S. Acceleration During the Beginning (*ABT*): This feature illustrates the rate of change in velocity during mouse movement at the onset of movement. It measures the rate at which the mouse device accelerates from a stationary position to a higher acceleration rate in the initial stages of movement.
T. Largest Deviation (*LD*): The largest distance between the trajectory points and the segment between the two endpoints.
U. Aggregate Features: Through analysis, it was found that many research studies extract the average (avg), standard deviation (std), minimum (min), maximum (max), and range of features, including *HV, VV, TA, TV, AV, D, t,* and θ, for analysis. These features are typically calculated using a sequence of individual mouse events that make up an action.

Based on our investigation, we identified nearly 90 mouse behavioral features currently used in the field. Furthermore, we were also able to identify the most frequently used features, which include a combination of *mean*, min, max, *std* of *HV, VV, TV, TA, AV,* with *mean J*, min *J*, max *J*, elapsed time, and *mean C*.

We successfully represent all mouse behavior features pictorially by grouping them based on popularity. Specifically, we first identify the most popular features (features used in >50 % of studies), followed by features used by 33–50 % of studies, and the least popular features (Fig. 5).

4.4. AI approaches and evaluation metrics used in mouse behavioral biometrics

Like keystroke analysis, mouse behavioral biometrics relies on various ML or DL approaches. This section identifies the AI approaches implemented for analysis. Approaches like SVM (Zheng et al., 2011; Da Silva et al., 2016), RF (Siddiqui et al., 2021; Da Silva et al., 2016; Almalki et al., 2023; Antal and Egyed-Zsigmond, 2018; Antal and Denes-Fazakas, 2019; Wang et al., 2019; Feher et al., 2012), DT (Almalki et al., 2023), *K*NN (Da Silva et al., 2016; Almalki et al., 2023), and MLP (Da Silva et al., 2016) are commonly implemented for analysis.

In addition to conventional ML approaches, studies have also applied DL approaches, such as CNN + RNN (Fu et al., 2020) and CNN (Antal and Fejér, 2020). These approaches deviate from traditional research studies by using a sequence of raw mouse events or images rather than extracting conventional features for user authentication (Fu et al., 2020; Hu et al., 2019; Antal and Fejér, 2020). Studies also feed conventional features into DL approaches (RNN-LSTM) and compare their performance to results achieved by traditional ML approaches (Subash et al., 2024). Table 4 summarizes the identified AI approaches currently implemented in the field.

On further investigation, several studies have performed comprehensive experiments to determine whether user identity can be defined in different environments. Specifically, they train the model with data collected from a desktop in the work environment and test it using data collected from a laptop in the home environment (Zheng et al., 2011). Furthermore, research also studies the effect of the number of clicks, inclusion of partial mouse movements (Zheng et al., 2011), varying numbers of mouse actions (Antal and Egyed-Zsigmond, 2018; Antal and Denes-Fazakas, 2019; Hu et al., 2019), different numbers of sequence information (Senarath et al., 2023a), and several types of mouse actions (Almalki et al., 2023; Antal and Egyed-Zsigmond, 2018), on performance. In addition to this, several models have also been compared. This includes comparing conventional ML and DL approaches (Fu et al., 2020; Subash et al., 2024).

A comparison was also performed by training and testing models with different datasets. For example, Siddiqui et al. (2021) conducted experimentation in two scenarios: scenario 1) trained and tested RF exclusively with the training set, achieving a 92.73 % accuracy, and scenario 2) where RF was trained using the training set and tested using the test set, achieving a 61.60 % accuracy. This method was also seen in research done by Antal and Egyed-Zsigmond (2018). Comparison is also performed between pre-processing methods and models. For example, Antal and Fejér (2020) compared 2 segmentation methods and 3 different DL models for authentication and identification scenarios. Specifically, the study compares a plain CNN model trained from scratch and 2 transfer models pre-trained using the DFL dataset. Among the transfer models, one has fixed weights, while the other updates weights using training data from the Balabit dataset. Furthermore, the comparison is also performed for balanced and unbalanced data scenarios.

Reliability analysis has also been performed to determine the usability of identified features. Specifically, Subash et al. (2024) proposes to evaluate DL models with a significantly larger publicly available dataset (Minecraft dataset) containing the same features as the ones identified in the study for online fraud detection. Specifically, the study compares the performance between newly collected data and the publicly available Minecraft dataset containing the same features (Subash et al., 2024). If the performance achieved in both scenarios is comparable, then the reliability of identified features is proven.

Some research also studies the effect of emotions on user identification (Wang et al., 2019). According to the study, the model's performance under different emotions has mild variations but no significant impact on overall performance.

Studies also combine different modalities to create a more robust behavioral biometric authentication model. Da Silva et al. (2016) combine keystroke and mouse behavioral biometrics modalities, proving that combining both modalities yields better performance than any one modality. According to the results, performance on keystroke data is inadequate, while performance using mouse behavior data yields satisfactory results, a maximum of 85 % through RF. Combining both modalities yields an increased performance of 90 % using RF.

Based on analysis (Table 5), it is evident that most studies rely on ML approaches despite the presence of state-of-the-art DL approaches. Further investigation revealed that RF is the most popular method among all conventional ML approaches.

Like keystroke, mouse behavioral biometric research analyzed in this study is also empirical. Analysis revealed that the evaluation metrics implemented in mouse behavioral biometrics research include FAR, FRR, and EER (Zheng et al., 2011). Additionally, accuracy (Acc), precision (Pre), recall (Rec), Area Under the Curve (AUC), Receiver Operating Characteristic (ROC) curve, and authentication time have also been used for model evaluation. The summary of the evaluation metrics utilized in mouse behavioral biometric research is depicted in Table 6.

4.5. Mouse behavioral biometrics research applications

On preliminary analysis, mouse behavioral biometrics have primarily been implemented for security-related applications, including user authentication and identification (Zheng et al., 2011). Table 7 gives a comprehensive idea of the research applications associated with mouse behavioral biometric research. Based on this analysis, it can be inferred that keystroke behavioral biometrics exhibit a significantly broader spectrum of research applications compared to mouse behavioral biometrics.

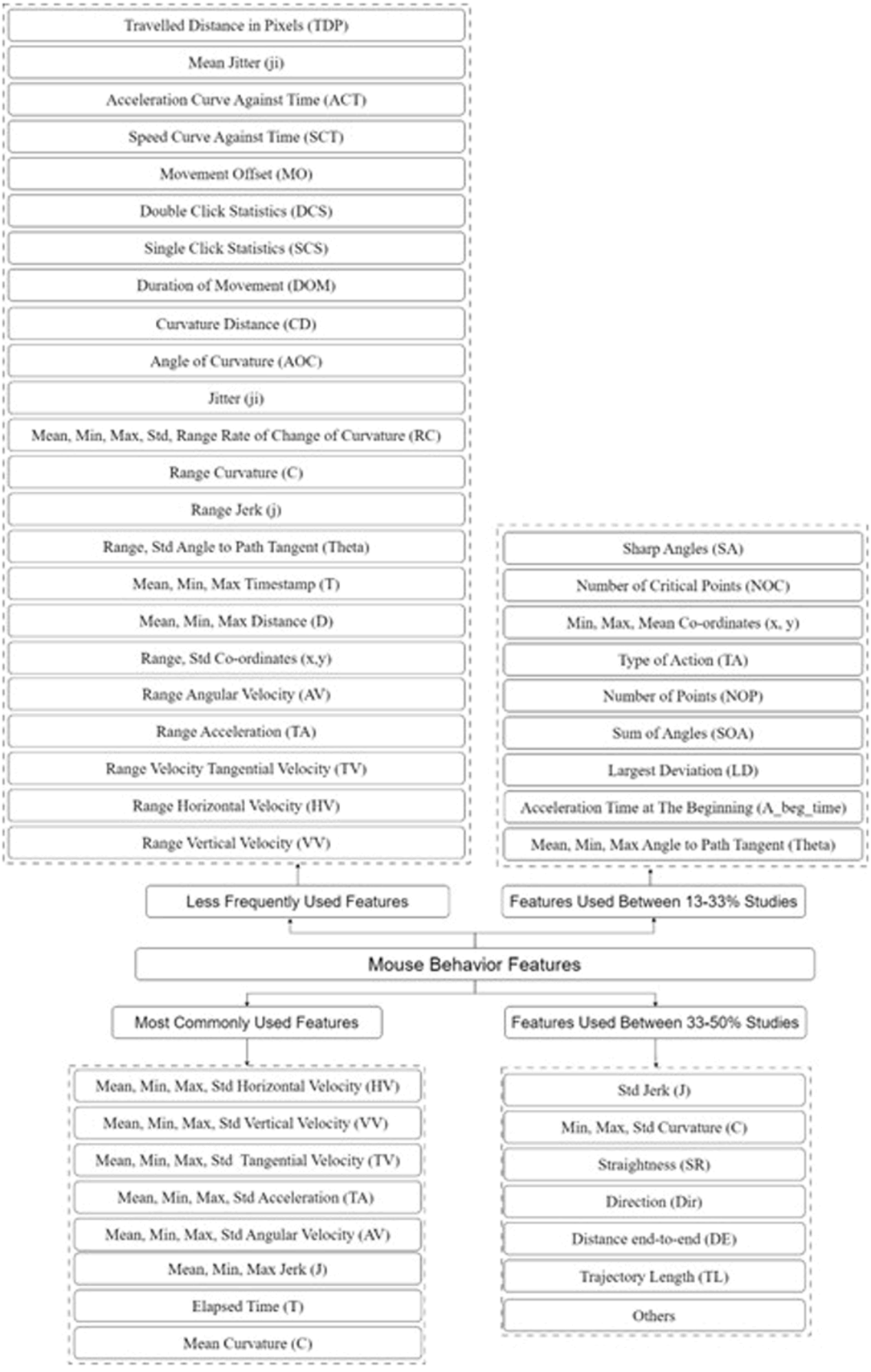

Fig. 5. Mouse behavior features organized from most popular to least popular.

Table 5
Summary of AI approaches implemented for mouse behavioral biometric analysis.

ML	DL	Statistical Models	Author
RF	No	No	Siddiqui et al., 2021
SVM-RBF	No	No	Zheng et al., 2011
RF, KNN, SVM	MLP	No	Da Silva Beserra et al., 2016
RF, DT, KNN	No	No	Almalki et al., 2023
No	CNN + RNN	No	Fu et al., 2020
RF	No	No	Antal and Egyed-Zsigmond, 2018
RF	No	No	Antal and Denes-Fazakas, 2019
No	RNN-LSTM	No	Subash et al., 2024
SVM	No	No	Shen et al., 2013
RF	No	No	Wang et al., 2019
No	No	Parzen density estimation, Unimodal distribution.	Gamboa and Fred, 2004
RF	No	No	Feher et al., 2012
No	CNN	No	Hu et al., 2019
No	CNN	No	Antal and Fejér, 2020

5. Real-World applications for keystroke and mouse behavioral biometrics

Behavioral biometrics is employed in commercial solutions across various domains, including finance, enterprise security, and mobile authentication. These applications demonstrate the technology's scalability and adaptability in addressing modern cybersecurity challenges.

Our analysis revealed the deployment of several keystroke behavioral biometric-based authentication systems primarily designed for mobile devices. These solutions include platforms such as MasterCard NuData, TwoSense.AI, BioSig ID, OneSpan, and Zighra (Progonov et al., 2022). Many of these systems utilize a combination of behavioral features and sensor data for user authentication. For instance, MasterCard NuData analyses app usage, geolocation, keystroke patterns, wireless connections, and device orientation for verifying user identity (Progonov et al., 2022). Additionally, some systems employ multifactor authentication by combining multiple behavioral biometric modalities. For example, TwoSense. AI incorporates keystroke dynamics, gait patterns, touchscreen interactions, app usage, and geolocation data to enable continuous user authentication (Progonov et al., 2022). Similarly, OneSpan and Zighra leverage keystroke behavior, app usage, and sensor data, such as wireless connection information, for authentication. BioSig ID, conversely, employs a multifactor approach that combines knowledge-based authentication (e.g., PINs and passwords) with touch-screen-based gestures to verify users (Progonov et al., 2022).

Other systems, including Plurilock Defend (Plurilock Security, Inc 2024), SecureAuth (SecureAuth 2025), and BioCatch Connect (BioCatch 2025, similarly utilize the aforementioned features with mouse behavior for user authentication. The information regarding all the aforementioned behavioral biometrics-based authentication systems has been consolidated and presented in Table 8. Based on our analysis, we find that Plurilock, BioCatch, and SecurAuth develop multiple solutions that target different endpoint devices, including smartphones, desktops, tablets, and laptops. To our knowledge, no other survey covers real-world applications of keystroke and mouse behavioral biometric-based authentication systems.

6. Adaptability of keystroke and mouse behavioral biometrics systems

It is already known that behavioral biometric modalities, especially keystroke and mouse behavioral biometrics, have gained significant popularity in recent years due to their capability to track user identity continuously and noninvasively. Secondly, these systems are more secure than conventional password-based authentication systems, as they rely on analyzing unique user behavior for user authentication and identification. These unique behaviors are more challenging to forge, forget, share, or distribute (Jain et al., 2006), making them better alternatives.

However, such modalities suffer from intraclass variability (Mhenni et al., 2019a, 2018). Keystroke behavior of a user is affected by several factors such as keyboard layout (QWERTY, QWERTZ, AZERTY), keyboard type (touch screen, virtual, physical), subject activeness, and several environmental factors (location and lighting) (Mhenni et al., 2019a, 2018). Similarly, mouse behavior is also affected by a similar set of factors. Similarly, screen resolution (website window content resolution, monitor resolution), mouse pointer sensitivity, and types of mouse (trackpad, gaming mouse, regular mouse) are also known to

Table 7
Summary of research application of mouse behavioral biometric analysis.

Author	Security	Online Assessment Fraud Detection
Siddiqui et al., 2021	Yes	No
Zheng et al., 2011	Yes	No
Da Silva Beserra et al., 2016	Yes	No
Almalki et al., 2023	Yes	No
Fu et al., 2020	Yes	No
Antal and Egyed-Zsigmond, 2018	Yes	No
Antal and Denes-Fazakas, 2019	Yes	No
Subash et al., 2024	Yes	Yes
Shen et al., 2013	Yes	No
Wang et al., 2019	Yes	No
Gamboa and Fred, 2004	Yes	No
Feher et al., 2012	Yes	No
Hu et al., 2019	Yes	No
Antal and Fejér, 2020	Yes	No

Table 6
Evaluation metrics used in mouse behavioral biometrics.

Author	EER	FAR	FRR	Acc	PRE	REC	ROC	AUC	Others
Siddiqui et al., 2021	Yes	Yes	Yes	Yes	No	No	No	No	No
Zheng et al., 2011	Yes	Yes	Yes	No	No	No	Yes	No	No
Da Silva Beserra et al., 2016	No	No	No	Yes	No	No	No	No	No
Almalki et al., 2023	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No
Fu et al., 2020	Yes	No	No	No	No	No	Yes	Yes	No
Antal and Egyed-Zsigmond, 2018	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No
Antal and Denes-Fazakas, 2019	No	No	No	No	No	No	Yes	Yes	No
Subash et al., 2024	No	No	No	Yes	Yes	Yes	No	No	No
Shen et al., 2013	Yes	Yes	Yes	No	No	No	No	No	Yes
Wang et al., 2019	No	No	No	Yes	No	No	No	No	No
Gamboa and Fred, 2004	Yes	No	No	No	No	No	No	No	No
Feher et al., 2012	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes
Hu et al., 2019	No	Yes	Yes	No	No	No	No	No	No
Antal and Fejér, 2020	No	No	No	Yes	No	No	No	Yes	No

Table 8
Comparison of Real-World Applications for Keystroke and Mouse Behavioral Biometrics.

Solution	Authentication Method	Used Modalities	Sensor Data	Non-Invasive Authentication
MasterCard Nu Data	Behavior-Based	Apps Usage, Keystroke Behavioral Biometrics, Geolocation, Device Orientation, Wireless Connections	Motions Sensors, touchscreen, GPS, Wireless Adaptors	Yes
TwoSense.AI	Continuous Authentication, Multifactor	Keystroke Behavioral Biometrics, Touchscreen, App Usage, Geolocation, gait behavioral biometrics	Touchscreen, Motion sensors, front-facing camera, GPS	Yes
BioSigID	Multifactor	Passwords/PIN, Touchscreen Gestures	Touchscreen	No
OneSpan	Multifactor	App Usage, Keystroke Behavioral Biometrics, Wireless Connections	Touchscreen, Wireless Adapter	Yes
Zighra	Continuous Authentication, Multifactor	App Usage, Keystroke Behavioral Biometrics, Wireless Connections	Touchscreen, Wireless Adapter	Yes
Plurilock Defend	Continuous Authentication, Multifactor	Keystroke Behavioral Biometrics, Mouse Behavioral Biometrics	Keyboard Device, Pointer Device	Yes
BioCatch Connect	Continuous Authentication, Multifactor	Keystroke behavioral biometrics, mouse behavioral biometrics	Keyboard Device, Pointer Device	Yes
SecureAuth	Multifactor	Keystroke behavioral biometrics, mouse behavioral biometrics, Touch screen, Geolocation, User device, Wireless connection, Browser information	Keyboard Device, Pointer Device, Touchscreen, GPS, Wi-Fi	Yes

affect mouse behavior (Zheng et al., 2011). Specifically, features such as velocity and acceleration of mouse movements become poor comparison metrics between subjects.

Further investigation shows that user behavior could evolve (change) over time (Mhenni et al., 2019a). Specifically, the user behavior recorded during the initial analysis phases may not represent the user behavior several months or years later (Mhenni et al., 2019a). According to research studies, several factors contribute to user behavior evolution (changes in user behavior) (Mhenni et al., 2019a; Pisani et al., 2019). Through frequent interaction with keyboard and mouse devices, subjects' behavior may vary. In other words, as the subject becomes more familiar with the devices, it becomes easier for the subject to use them. This causes variations in the subject's profile compared to the initial profile. For example, the subject may become faster at typing or more proficient with the mouse than when he first started. Similarly, keystroke and mouse behavior can also be affected by illnesses, aging, emotions, and injuries (Pisani et al., 2019). Since such changes in user behavior occur over time due to these several factors, the chances of genuine subjects getting rejected by the behavioral biometric authentication system become higher, thereby increasing false rejection rates (FRR). Therefore, it is imperative to investigate current research in behavioral biometrics and identify if and how they factor in user behavior evolution. Table 8 summarizes research studies implementing adaptive strategies to tackle user behavior evolution.

Our investigation shows that only a few studies implement adaptive strategies to counter intra-class variability and user behavior evolution. Subash & Song (2021) propose an RBBIS (Real-time Behavioral Biometric Information Security) adaptive framework that non-invasively builds behavioral profiles using DL approaches. This framework performs trajectory analysis to investigate and predict how user behavior evolves over time. According to the author, this framework can detect users after long periods during which there is an expected change in user behavior.

Studies also focus on tackling intra-class variability (Mhenni et al., 2019a, 2018). A. Mhenni et al. (2018) first classify users into categories according to the Doddington Zoo classification and apply specific adaptive techniques to each category. Specifically, three adaptive approaches are implemented: growing window, sliding window, and the least frequently used technique. Similarly, Mhenni et al. (2019a) propose an adaptive method that uses only one sample as a reference. After this, the reference is updated using a double serial adaptation strategy for each correctly classified sample. Specifically, two thresholds are implemented as a criterion for adaptation. First, the global score is used to determine the authenticity of the subject (using the first threshold), and then it is compared with the second threshold. Each reference is added as a profile based on the growing window technique until it reaches a specific size (10), after which a sliding window is implemented. Therefore, each sample successfully recognized as the subject's is considered a potential reference. Finally, Ceker and Upadhyaya (2016) investigate the use of transfer learning to update the classifiers affected by environmental factors with minimal re-training. According to the study, it is feasible to identify users at different times by acquiring only a few samples from another session, obtaining 13 % higher accuracy.

Our investigation found that most adaptation techniques were implemented, keeping keystroke behavioral biometrics in mind. To our knowledge, adaptation techniques have yet to be implemented in mouse behavioral biometrics (Table 9).

7. Research gaps and discussion

In the preceding section, we extensively reviewed the current trend within keystroke and mouse behavioral biometrics. Our investigation has encompassed various facets, such as the compilation of datasets, utilization of features, deployment of artificial intelligence methodologies, computation of evaluation metrics, and exploration of research applications about keystroke and mouse behavioral biometrics. Despite the popularity of these methods, there are several research gaps.

Our analysis shows that some keystroke and mouse behavioral biometric-based research suffers from performance issues. Specifically, trained models cannot accurately classify new samples (Siddiqui et al., 2021; Da Silva Beserra et al., 2016; Subash et al., 2024; Subash and Song, 2021). Although a substantial number of studies exist in both fields, challenges related to performance and long-term reliability remain areas that require further investigation. On further analysis, it was found that only a few existing studies and surveys on keystroke and mouse behavioral biometrics address the adaptability of current research to user behavior evolution. It is already mentioned that keystroke and mouse behavior suffer from high intra-class variability (Mhenni et al., 2019a,2018). Furthermore, many studies have claimed that user behavior evolves over time due to various factors, including age, fatigue, emotion, familiarity, and illnesses (Mhenni et al., 2019a, 2018; Subash and Song, 2021; Pisani et al., 2019). This change in user behavior can affect the performance of current keystroke and mouse behavior biometric-based authentication systems. Specifically, genuine users can be classified as imposters, thereby increasing FRR and affecting system usability.

To overcome the issues, several studies have used techniques that

Table 9
Summary of adaptive techniques used in quantitative studies analyzed.

Author	Modality	Adaptive Mechanism Used
Andrean et al. 2020	Keystroke	No
Siddiqui et al., 2021	Mouse	No
Subash et al., 2023	Keystroke	No
Zheng et al., 2011	Mouse	No
Mhenni et al., 2019a	Keystroke	Sliding window, Growing Window, and least frequently used mechanism, with Doddington Classification
Ceker and Upadhyaya, 2016	Keystroke	Transfer learning
Subash and Song, 2021	Keystroke	RBBIS framework that performs trajectory analysis for user behavior change over time
Maheshwary et al., 2017	Keystroke	No
Killourhy and Maxion, 2009	Keystroke	No
Maiorana et al., 2019	Keystroke	No
Senarath et al., 2023a	Keystroke	No
Senarath et al., 2023b	Keystroke	No
Nguyen et al., 2024	Keystroke	No
Epp et al., 2011	Keystroke	No
Tsimperidis et al., 2017	Keystroke	No
Tsimperidis et al., 2020	Keystroke	No
I. Tsimperidis et al., 2018	Keystroke	No
Ulinskas et al., 2018	Keystroke	No
Alshanketi et al., 2019	Keystroke	No
Bours, 2012	Keystroke	No
Da Silva Beserra et al., 2016	Keystroke + Mouse	No
Krishnamoorthy et al., 2018	Keystroke	No
A. Mhenni et al., 2018	Keystroke	Double serial adaptation strategy with sliding window or growing window techniques
Kalita et al., 2020	Keystroke	No
Daribay et al., 2019	Keystroke	No
Acien et al., 2022	Keystroke	No
Stragapede et al., 2024	Keystroke	No
Almalki et al., 2023	Mouse	No
Fu et al., 2020	Mouse	No
Antal and Egyed-Zsigmond, 2018	Mouse	No
Antal and Denes-Fazakas, 2019	Mouse	No
Subash et al., 2024	Mouse	No
Shen et al., 2013	Mouse	No
Wang et al., 2019	Mouse	No
Gamboa and Fred, 2004	Mouse	No
Feher et al., 2012	Mouse	No
Hu et al., 2019	Mouse	No
Antal and Fejér, 2020	Mouse	No

overcome the problem of intra-class variability by proposing reference template adjustment techniques such as growing window, sliding window, and least frequently used reference mechanisms (Mhenni et al., 2019a, 2018; Ceker and Upadhyaya, 2016). However, these complex methods require more computation and storage, making them unsustainable solutions. This is also the case when DL approaches are used (Lucia et al., 2023). Furthermore, these approaches can only detect slight changes in user reference based on environmental conditions, emotions, fatigue, and hardware-related factors. Additionally, no studies focus on tackling user behavior evolution over long periods due to age, familiarity, and illnesses. It is also important to note that research studies have only given a general hypothesis that user behavior evolves over time due to the aforementioned factors. However, no experimental studies have analyzed and proved that user behavior and its properties actually evolve. Furthermore, no public datasets are available for analyzing short and long-term user behavior evolution. This is because data needs to be collected in different environments and devices over several sessions, separated by a certain amount of time. Our investigation shows that public and novel datasets used for mouse and keystroke behavioral biometrics collect data in sessions, but do so with small time gaps. According to our analysis (Tables 1 and 4), the maximum time gap between sessions is ~28 days (Acien et al., 2022). Other studies collect behavioral data in sessions separated by approximately one day or one week. However, such intervals may not adequately capture long-term changes in user behavior. In some cases, datasets are continuously collected over large time frames ranging from 4 months to >2 years using logging tools. However, these studies do not perform adaptive analysis to understand user behavior evolution. The absence of public datasets makes it very difficult to evaluate adaptive behavioral biometric systems (Pisani et al., 2019) or predict user behavior evolution over time. Furthermore, the survey articles analyzed in this paper do not report on adaptive strategies used in behavioral biometric research studies or their drawbacks. Current behavioral biometric systems are also susceptible to attacks, including zero-effort, playback, and poisoning attacks (Jain et al., 2006; Pisani et al., 2019; Mhenni et al., 2019b). Generally, these areas of research remain unexplored.

As an additional contribution to this paper, we compile and visualize comprehensively the contributions of previously published surveys and compare them to our survey (Table 10). Comparison is performed on several aspects, including the reports on modalities (MD), datasets (DS), data collection procedures (DCP), pre-processing methods (PM), AI approaches (MU), evaluation metrics (EC), adaptability (AD), and research applications (RA). Table 10 also shows that our survey gives a more comprehensive outlook on keystroke and mouse behavioral biometrics compared to previously published work.

While theoretical advancements in behavioral biometrics have demonstrated promising results in controlled settings, the real-world deployment of these systems introduces additional challenges. For instance, maintaining high accuracy and consistency across diverse user populations and varying environments remains difficult. Systems trained on data from a specific device or setting often experience performance degradation when applied to different hardware, network conditions, or user contexts. Factors such as hardware inconsistencies (e.g., different keyboards or mice), changes in user behavior due to stress, fatigue, learning factors, emotion, or multitasking, and variations in posture or interaction patterns can significantly affect model performance.

Moreover, **scalability** becomes a concern as systems move from small-scale evaluations to broader deployments involving large and heterogeneous user bases. Ensuring **robustness and generalization** across time and conditions is crucial, yet many existing approaches struggle to maintain long-term performance without frequent retraining or fine-tuning. These real-world constraints highlight the gap between controlled experimental results and practical applicability, underscoring the need for further research into adaptable, context-aware, and privacy-conscious biometric systems.

8. Privacy challenges and ethical considerations in behavioral biometric systems

Behavioral Biometrics, such as keystroke and mouse dynamics, offer valuable benefits for non-invasive and continuous user authentication. However, their deployment raises important ethical and privacy considerations. A major concern is user consent, as user behavioral biometric-based systems collect user behavior data passively in the background, often while the users are not fully aware of what is being collected, how it is being processed, used, or who has access to it. This lack of transparency challenges the fundamental principles of informed consent.

Secondly, user behavior information is sensitive and rich in contextual information, which can reveal users' traits and behaviors. Specifically, user behavior, such as typing speed and mouse movement

Table 10
Representation of survey reports and their primary area of focus.

Author	MD	DS	DCP	PM	FE	MU	EC	AD	RA
Albalawi et al., 2022	Fingerprint, Face, Iris/Retina, Keystroke, Signature, and Voice Recognition	No	No	Yes	Yes	Yes	No	No	No
Ometov et al., 2018	Conventional Authentication Systems, Voice, Face, Iris, Hand Geometry, Vein, Fingerprint, Geographical Location, Thermal Image, Beam Forming Techniques, Occupant Classification System, ECG, EEG, and DNA Recognition	No	No	No	No	Yes	Yes	No	Yes
Lucia et al., 2023	BMI, Face, Fingerprint, Hand Vein, Iris, Blood Pressure, ECG, EEG, Galvanic skin response, Heat Rate, Respiration Rate, Skin Temperature, Eye Movements, Facial Dynamics, Keystroke, Signature, Voice, Posture Pattern, and Pressure Distributions	Yes	Yes	No	No	Yes	Yes	No	Yes
Babich, 2012	Fingerprint, Face, DNA, Palmprint, Hand Geometry, Iris, Odor/Scent, Keystroke, Gait, Voice	No	Yes	Yes	Yes	No	No	No	Yes
Jain et al., 2006	Fingerprint, Face, Iris, Hand Geometry, Voice, Keystroke, Signature	No	No	No	Yes	Yes	Yes	No	Yes
Banerjee, and Woodard, 2012	Keystroke Behavioral Biometrics	Yes	No	No	Yes	Yes	Yes	No	Yes
Pisani et al., 2019	Fingerprint, Face, Iris, Voice, Accelerometer Biometrics, Keystroke behavioral Biometrics, Ocular Biometrics	Yes	No	No	No	Yes	Yes	Yes	No
Khan et al., 2024	Mouse Behavioral Biometrics and Widget Interactions	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Sadikan et al., 2019	Conventional Authentication Systems, Profile-based Authentication, Keystroke behavioral biometrics	Yes	Yes	No	Yes	Yes	Yes	No	Yes
Maiorana et al., 2021	Keystroke Behavioral Biometrics	Yes	Yes	No	Yes	Yes	Yes	No	No
Ayeswarya, and Singh, 2024	Fingerprint, Face, Ocular, Keystroke Behavioral Biometrics, Gait Behavior, Mouse behavioral Biometrics, Touch-Based Behavioral Biometrics, Sensor-Based Behavioral Biometrics, Context Aware-Based Authentication Systems	Yes	No	No	Yes	Yes	Yes	No	No
Tural and Ozmen, 2024	Keystroke Behavioral Biometrics	No	No	No	No	Yes	No	No	No
Our Survey	Keystroke and Mouse behavioral biometrics	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

behavior, can be influenced by the users' mood, fatigue levels, and stress, potentially providing much more information and insight than the user intends to. Furthermore, such data can also reveal the users' age, gender, cognitive state, health conditions, and possible disabilities. If not strictly protected, this data can be misused for unauthorized profiling, discrimination, and surveillance, particularly in schools, online education platforms, workplaces, and public systems.

Deploying user behavioral biometric systems at scale would also have broader societal implications. The widespread use of this technology could lead to the pervasive monitoring of users, thereby undermining privacy in digital spaces. Without proper regulation and oversight, such technologies may be exploited by governments or corporations to track individuals, eroding civil liberties. Even in legitimate applications, ensuring the responsible use of this data is important for maintaining user trust. It is also essential to consider how systems can remain robust to misuse or accidental disclosure of user behavior data, particularly given the long-term and often continuous nature of data collection in behavioral biometrics.

Lastly, to address the aforementioned challenges, behavioral biometric system design should incorporate privacy-aware approaches, such as data minimization, transparency in model behavior, and clear opt-in or opt-out mechanisms for users. Exploring on-device processing, anonymization techniques, and secure data handling can also help ensure responsible use. As behavioral biometric technologies continue to develop, a balanced consideration of their technical capabilities and ethical implications will be key to supporting their adoption in a trustworthy manner.

9. Conclusion and future work

In conclusion, our survey has provided a comprehensive overview of the current landscape of keystroke and mouse behavioral biometrics. Through our exploration, we have identified several noteworthy trends and insights. The findings underscore the importance of the adaptability of current keystroke and mouse behavioral biometric-based research, which may have significant implications for performance and user authentication over long periods. Moving forward, we suggest that there is a need to analyze, visualize, and identify what properties of behavior evolve (change), how they evolve, and what factors bring about the evolution of user behavior. Therefore, future research should focus on making such systems more adaptable to user behavior evolution. Since user behavior can evolve over time due to several factors (mentioned in Section 7), it is essential to factor in this evolution to prevent an increase in FRR rates. This involves collecting user behavior and demographic data for an extended period of time and analyzing the data for specific trends. It is also essential to develop more sustainable approaches, methodologies, and frameworks relevant to current policies and standards established by several world governments. Making such systems adaptive and sustainable will help build more state-of-the-art, secure, and robust behavioral biometric authentication systems. Secondly, future work should also focus on securing keystroke and mouse behavioral authentication systems against poisoning, playback, and zero-effort attacks. Thirdly, future research could explore the integration of additional behavioral modalities, such as gait, voice, and touchscreen interactions, to develop more robust and comprehensive multimodal biometric systems. Furthermore, to address the challenges of scalability and generalization in real-world deployments, future research should focus on developing adaptive behavioral biometric models that can maintain performance across diverse users, devices, and environments without frequent retraining. This includes exploring continual learning techniques, domain adaptation, and context-aware modelling strategies. Additionally, efforts should be directed toward designing privacy-preserving architectures that ensure user data protection while supporting large-scale, long-term biometric authentication systems. Future research could also explore adaptive machine learning techniques from other domains to enhance the long-term robustness of behavioral biometric systems. Integrating cross-domain adaptation and continual learning approaches may help address evolving user behavior more effectively. This survey contributes valuable insights into keystroke and mouse behavioral biometrics, laying a foundation for continued innovation and research.

Declarations

Funding: NA

Data availability: This is a survey of existing literature and does not involve the generation, collection, or implementation of new data for analysis.

CRediT authorship contribution statement

Aditya Subash: Writing – review & editing, Writing – original draft,

Visualization, Validation, Methodology, Investigation. **Insu Song:** Methodology, Writing – review & editing, Validation, Supervision. **Ickjai Lee:** Writing – review & editing, Validation, Supervision, Methodology. **Kyungmi Lee:** Writing – review & editing, Validation, Supervision, Methodology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A

Table 1 and 4.

Data availability

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

References

Acien, A., Morales, A., Fierrez, J., Vera-Rodriguez, R., Delgado-Mohatar, O., 2021. BeCAPTCHA: behavioral bot detection using touchscreen and mobile sensors benchmarked on HuMIdb. Eng. Appl. Artif. Intell. 98, 104058. https://doi.org/10.1016/j.engappai.2020.104058.

Acien, A., Morales, A., Monaco, J.V., Vera-Rodriguez, R., Fierrez, J., 2022. TypeNet: deep learning keystroke biometrics. IEEe Trans. Biom. Behav. Identity. Sci. 4 (1), 57–70. https://doi.org/10.1109/TBIOM.2021.3112540.

Ahmed, A.A.E., Traore, I., 2005. Anomaly intrusion detection based on biometrics. In: Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, pp. 452–453. https://doi.org/10.1109/IAW.2005.1495997.

Albalawi, S., Alshahrani, L., Albalawi, N., Kilabi, R., Alhakamy, A., 2022. A comprehensive overview on biometric authentication systems using artificial intelligence techniques. Int. J. Adv. Comput. Sci. Appl. 13 (4). https://doi.org/10.14569/IJACSA.2022.0130491.

Almalki, S., Chatterjee, P., & Kaushik, R. (2023). Continuous authentication using mouse clickstream data analysis. arXiv.Org. https://doi.org/10.48550/arxiv.2312.00802.

Alshanketi, F., Traoré, I., Awad, A., 2019. Multimodal mobile keystroke dynamics biometrics combining fixed and variable passwords. Secur. Privacy 2 (1), e48. https://doi.org/10.1002/spy2.48 n/a.

Andrean, A., Jayabalan, M., Thiruchelvam, V., 2020. Keystroke dynamics based user authentication using deep multilayer perceptron. Int. J. Mach. Learn. Comput. 10 (1), 134–139. https://doi.org/10.18178/ijmlc.2020.10.1.910.

Antal, M., Denes-Fazakas, L., 2019. User verification based on mouse dynamics: a comparison of public data sets. In: 2019 IEEE 13th International Symposium on Applied Computational Intelligence and Informatics (SACI), pp. 143–148. https://doi.org/10.1109/SACI46893.2019.9111596.

Antal, M., & Egyed-Zsigmond, E. (2018). Intrusion detection using mouse dynamics. arXiv.Org. https://doi.org/10.48550/arxiv.1810.04668.

Antal, M., Fejér, N., 2020. Mouse dynamics based user recognition using deep learning. Acta Universitatis Sapientiae. Informatica 12 (1), 39–50. https://doi.org/10.2478/ausi-2020-0003.

Antal, M., Nemes, L., 2016. The MOBIKEY keystroke dynamics password database: benchmark results. In: Silhavy, R., Senkerik, R., Oplatkova, Z.K., Silhavy, P., Prokopova, Z. (Eds.), Software Engineering Perspectives and Application in Intelligent Systems. ICTIS CSOC 2017 2016. Advances in Intelligent Systems and Computing, Software Engineering Perspectives and Application in Intelligent Systems. ICTIS CSOC 2017 2016. Advances in Intelligent Systems and Computing, 465. Springer, Cham. https://doi.org/10.1007/978-3-319-33622-0_4.

Antal, M., Szabó, L.Z., László, I., 2015. Keystroke dynamics on android platform. Procedia Technol. 19, 820–826. https://doi.org/10.1016/j.protcy.2015.02.118.

Ayeswarya, S., Singh, K.J., 2024. A comprehensive review on secure biometric-based continuous authentication and user profiling. IEEe Access. 12, 82996–83021. https://doi.org/10.1109/ACCESS.2024.3411783.

Babich, A. (2012). Biometric authentication. Types of biometric identifiers.

Banerjee, S.P., Woodard, D.L., 2012. Biometric authentication and identification using keystroke dynamics: a survey. J. Pattern Recogn. Res. 7 (1), 116–139.

BioCatch Connect. (n.d.). https://www.biocatch.com/biocatch-connect Accessed on 10 Mar 2025.

Bours, P., 2012. Continuous keystroke dynamics: a different perspective towards biometric evaluation. Info. Secur. Tech. Report 17 (1–2), 36–43. https://doi.org/10.1016/j.istr.2012.02.001.

Ceker, H., Upadhyaya, S., 2016. Adaptive techniques for intra-user variability in keystroke dynamics. In: 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp. 1–6. https://doi.org/10.1109/BTAS.2016.7791156.

Shen, Chao, Cai, Zhongmin, Guan, Xiaohong, 2012. Continuous authentication for mouse dynamics: a pattern-growth approach. In: IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012), pp. 1–12. https://doi.org/10.1109/DSN.2012.6263955.

Shen, Chao, Cai, Zhongmin, Guan, Xiaohong, Du, Youtian, Maxion, R.A., 2013. User authentication through Mouse dynamics. IEEE Trans. Info. Forens. Secur. 8 (1), 16–30. https://doi.org/10.1109/TIFS.2012.2223677.

Coakley, M.J., Monaco, J.V., Tappert, C.C., 2016. Keystroke biometric studies with short numeric input on smartphones. In: 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp. 1–6. https://doi.org/10.1109/BTAS.2016.7791181.

Da Silva Beserra, I., Camara, L., Da Costa-Abreu, M., 2016. Using keystroke and mouse dynamics for user identification in the online collaborative game League of Legends. In: 7th International Conference on Imaging for Crime Detection and Prevention (ICDP 2016), p. 8. https://doi.org/10.1049/ic.2016.0076.

Daribay, A., Obaidat, M.S., Krishna, P.V., 2019. Analysis of authentication system based on keystroke dynamics. In: 2019 International Conference on Computer, Information and Telecommunication Systems (CITS), pp. 1–6. https://doi.org/10.1109/CITS.2019.8862068.

Deb Das, S., Ah Kioon, M.C., Wang, Z.S, 2013. Security analysis of MD5 algorithm in password storage. Appl. Mech. Mater. 347–350, 2706–2711. https://doi.org/10.4028/www.scientific.net/AMM.347-350.2706.

DeLiema, M., Langton, L., Burnes, D., 2020. Identity theft among older adults: risk and protective factors. Innov. Aging 4 (Supplement_1), 31. https://doi.org/10.1093/geroni/igaa057.100, 31.

Dhakal, V., Feit, A.M., Kristensson, P.O., Oulasvirta, A., 2018. Observations on typing from 136 million keystrokes. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, pp. 1–12. https://doi.org/10.1145/3173574.3174220.

Epp, C., Lippold, M., Mandryk, R., 2011. Identifying emotional states using keystroke dynamics. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 715–724. https://doi.org/10.1145/1978942.1979046.

Feher, C., Elovici, Y., Moskovitch, R., Rokach, L., Schclar, A., 2012. User identity verification via mouse dynamics. Inf. Sci. 201, 19–36. https://doi.org/10.1016/j.ins.2012.02.066.

Fu, S., Qin, D., Qiao, D., Amariucai, G.T., 2020. RUMBA-mouse: rapid user mouse-behavior authentication using a CNN-RNN approach. In: 2020 IEEE Conference on Communications and Network Security (CNS), pp. 1–9. https://doi.org/10.1109/CNS48642.2020.9162287.

Gaines, R., 1980. Authentication by keystroke timing: some prelimary results. Rand Report R-256-NSF.

Gamboa, H., Fred, A., 2004. A behavioral biometric system based on human-computer interaction. Biometric Technol. Human Identif. 5404, 381–392. https://doi.org/10.1117/12.542625. SPIE.

Georgiev, M., Eberz, S., Turner, H., Lovisotto, G., Martinovic, I., 2023. FETA: fair evaluation of touch-based authentication. arXiv.Org.

Giot, R., El-Abed, M., Rosenberger, C., 2012. Web-based benchmark for Keystroke dynamics biometric systems: a statistical analysis. In: 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 11–15. https://doi.org/10.1109/IIH-MSP.2012.10.

Guedes, I., Martins, M., Cardoso, C.S., 2023. Exploring the determinants of victimization and fear of online identity theft: an empirical study. Secur. J. 36 (3), 472–497. https://doi.org/10.1057/s41284-022-00350-5.

Heartfield, R., Loukas, G., 2016. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM. Comput. Surv. 48 (3), 1–39. https://doi.org/10.1145/2835375.

Hu, T., Niu, W., Zhang, X., Liu, X., Lu, J., Liu, Y., 2019. An insider threat detection approach based on mouse dynamics and deep learning. Secur. Commun. Netw. 2019, 1–12. https://doi.org/10.1155/2019/3898951.

Iakovakis, D., Hadjidimitriou, S., Charisis, V., Bostantjopoulou, S., Katsarou, Z., Klingelhoefer, L., Hadjileontiadis, L.J., 2018. Motor impairment estimates via touchscreen typing dynamics toward Parkinson's disease detection from data harvested In-the-wild. Front. ICT 5 (2018), 28. https://doi.org/10.3389/fict.2018.00028.

Jain, Ross, A., Pankanti, S., 2006. Biometrics: a tool for information security. IEEE Trans. Info. Forens. Secur. 1 (2), 125–143. https://doi.org/10.1109/TIFS.2006.873653.

Kalita, H., Maiorana, E., Campisi, P., 2020. Keystroke dynamics for biometric recognition in handheld devices. In: 2020 43rd International Conference on Telecommunications and Signal Processing (TSP), pp. 410–416. https://doi.org/10.1109/TSP49548.2020.9163524.

Khan, S., Devlen, C., Manno, M., Hou, D., 2024. Mouse Dynamics Behavioral biometrics: a survey. ACM. Comput. Surv. 56 (6), 1–33. https://doi.org/10.1145/3640311.

Killourhy, K.S., Maxion, R.A., 2009. Comparing anomaly-detection algorithms for keystroke dynamics. In: 2009 IEEE/IFIP International Conference on Dependable Systems & Networks, pp. 125–134. https://doi.org/10.1109/DSN.2009.5270346.

Kochegurova, E.A., Martynova, Yu.A., 2020. Aspects of continuous user identification based on free texts and hidden monitoring. Program. Comput. Softw. 46 (1), 12–24. https://doi.org/10.1134/S036176882001003X.

Krishnamoorthy, S., Rueda, L., Saad, S., Elmiligi, H., 2018. Identification of user behavioral biometrics for authentication using keystroke dynamics and Machine Learning. In: Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications, pp. 50–57. https://doi.org/10.1145/3230820.3230829.

Lucia, C., Zhiwei, G., Michele, N., 2023. Biometrics for Industry 4.0: a survey of recent applications. J. Ambient. Intell. Humaniz. Comput. 14 (8), 11239–11261. https://doi.org/10.1007/s12652-023-04632-7.

Maheshwary, S., Ganguly, S., Pudi, V., 2017. Deep secure: a fast and simple neural network based approach for user authentication and identification via keystroke

dynamics. In: IWAISe: First International Workshop on Artificial Intelligence in Security, 59. NUI Galway Melbourne.
Maiorana, E., Kalita, H., Campisi, P., 2019. Deepkey: keystroke dynamics and CNN for biometric recognition on mobile devices. 2019 8th European Workshop on Visual Information Processing (EUVIP) 181–186. https://doi.org/10.1109/EUVIP47703.2019.8946206.
Maiorana, E., Kalita, H., Campisi, P., 2021. Mobile keystroke dynamics for biometric recognition: an overview. IET. Biom. 10 (1), 1–23. https://doi.org/10.1049/bme2.12003.
Messerman, Mustafic, T., Camtepe, S.A., Albayrak, S., 2010. A generic framework and runtime environment for development and evaluation of behavioral biometrics solutions. In: 2010 10th International Conference on Intelligent Systems Design and Applications, pp. 136–141. https://doi.org/10.1109/ISDA.2010.5687276.
Mhenni, A., Cherrier, E., Rosenberger, C., Amara, N.E.B., 2018. Adaptive biometric strategy using Doddington Zoo Classification of User's keystroke dynamics. In: 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), pp. 488–493. https://doi.org/10.1109/IWCMC.2018.8450401.
Mhenni, A., Cherrier, E., Rosenberger, C., Essoukri, Ben, Amara, N., 2019a. Double serial adaptation mechanism for keystroke dynamics authentication based on a single password. Comput. Secur. 83, 151–166. https://doi.org/10.1016/j.cose.2019.02.002.
Mhenni, A., Migdal, D., Cherrier, E., Rosenberger, C., Essoukri, Ben, Amara, N., 2019b. Vulnerability of adaptive strategies of keystroke dynamics based authentication against different attack types. In: 2019 International Conference on Cyberworlds (CW), pp. 274–278. https://doi.org/10.1109/CW.2019.00052.
Mondal, S., Bours, P., 2013. Continuous authentication using mouse dynamics. In: 2013 International Conference of the BIOSIG Special Interest Group (BIOSIG), pp. 1–12.
Murphy, C., Huang, Jiaju, Hou, Daqing, Schuckers, S., 2017. Shared dataset on natural human-computer interaction to support continuous authentication research. In: 2017 IEEE International Joint Conference on Biometrics (IJCB), pp. 525–530. https://doi.org/10.1109/BTAS.2017.8272738.
Nguyen, K.-N., Rasnayaka, S., Wickramanayake, S., Meedeniya, D., Saha, S., Sim, T., 2024. Spatio-temporal dual-attention transformer for time-series behavioral biometrics. IEEe Trans. Biom. Behav. Identity. Sci. 6 (4), 591–601. https://doi.org/10.1109/TBIOM.2024.3394875.
Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., Koucheryavy, Y., 2018. Multi-factor authentication: a survey. Cryptography 2 (1), 1. https://doi.org/10.3390/cryptography2010001.
Palin, K., Feit, A.M., Kim, S., Kristensson, P.O., Oulasvirta, A., 2019. How do people type on mobile devices?: observations from a study with 37,000 volunteers. In: Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services, pp. 1–12. https://doi.org/10.1145/3338286.3340120.
Pisani, P., Mhenni, A., Giot, R., Cherrier, E., Poh, N., Ferreira de Carvalho, A.C., Rosenberger, C., Amara, N., 2019. Adaptive Biometric Systems: review and perspectives. ACM. Comput. Surv. 52 (5), 1–38. https://doi.org/10.1145/3344255.
Plurilock Security, Inc, 2024. DEFEND continuous authentication| plurilock security. Plurilock. https://plurilock.com/products/defend/Accessed. on 10 Mar 2025.
Progonov, D., Cherniakova, V., Kolesnichenko, P., Oliynyk, A., 2022. Behavior-based user authentication on mobile devices in various usage contexts. EURASIP. J. Inf. Secur. 2022 (1), 1–11. https://doi.org/10.1186/s13635-022-00132-x.
Sadikan, S.F.N., Ramli, A.A., Fudzee, M.F.M., 2019. A survey paper on keystroke dynamics authentication for current applications. AIP. Conf. Proc. 2173 (1). https://doi.org/10.1063/1.5133925.
SecureAuth. (2025, March 7). SecureAuth - workforce and Customer Identity & Access management. https://www.secureauth.com/Accessed on 10 Mar 2025.
Senarath, D., Tharinda, S., Vishvajith, M., Rasnayaka, S., Wickramanayake, S., Meedeniya, D., 2023a. *Re*-evaluating keystroke dynamics for continuous authentication. In: 2023 3rd International Conference on Advanced Research in Computing (ICARC), pp. 202–207. https://doi.org/10.1109/ICARC57651.2023.10145743.
Senarath, D., Tharinda, S., Vishvajith, M., Rasnayaka, S., Wickramanayake, S., Meedeniya, D., 2023b. BehaveFormer: a framework with Spatio-Temporal dual attention Transformers for IMU-enhanced Keystroke dynamics. In: 2023 IEEE International Joint Conference on Biometrics (IJCB), pp. 1–9. https://doi.org/10.1109/IJCB57857.2023.10448997.
Siddiqui, N., Rushit Dave, & Seliya, N. (2021). Continuous authentication using mouse movements, machine learning, and Minecraft. ArXiv.Org. https://doi.org/10.48550/arxiv.2110.11080.
Sitova, Z., Sedenka, J., Yang, Qing, Peng, Ge, Zhou, Gang, Gasti, P., Balagani, K.S., 2016. HMOG: new behavioral biometric features for continuous authentication of smartphone users. IEEE Trans. Info. Forens. Secur. 11 (5), 877–892. https://doi.org/10.1109/TIFS.2015.2506542.
Stragapede, G., Delgado-Santos, P., Tolosana, R., Vera-Rodriguez, R., Guest, R., Morales, A., 2024. TypeFormer: transformers for mobile keystroke biometrics. Neural Comput. Appl. 36 (29), 18531–18545. https://doi.org/10.1007/s00521-024-10140-2.
Stragapede, G., Vera-Rodriguez, R., Tolosana, R., Morales, A., Fierrez, J., Ortega-Garcia, J., Rasnayaka, S., Seneviratne, S., Dissanayake, V., Liebers, J., Islam, A., Belhaouari, S.B., Ahmad, S., Jabin, S., 2022. IJCB 2022 Mobile behavioral biometrics competition (MobileB2C). In: 2022 IEEE International Joint Conference on Biometrics (IJCB), pp. 1–7. https://doi.org/10.1109/IJCB54206.2022.10007985.
Subash, A., Song, I., 2021. Real-time behavioral biometric information security system for assessment fraud detection. In: 2021 IEEE International Conference on Computing (ICOCO), pp. 186–191. https://doi.org/10.1109/ICOCO53166.2021.9673568.
Subash, A., Song, I., Tao, K., 2023. Robust keystroke behavior features for continuous user authentication for online fraud detection. In: Yang, XS., Sherratt, R.S., Dey, N., Joshi, A. (Eds.), Proceedings of Eighth International Congress on Information and Communication Technology. ICICT 2023. Lecture Notes in Networks and Systems, 693. Springer, Singapore. https://doi.org/10.1007/978-981-99-3243-6_71.
Subash, A., Song, I., Lee, I., Lee, K., 2024. Mouse dynamics-based Online fraud detection system for online education platforms. In: International Congress on Information and Communication Technology. Singapore: Springer Nature Singapore, pp. 257–269. https://doi.org/10.1007/978-981-97-3302-6_21.
Sando, Suzanne, 2024. Identity fraud study: resolving the shattered Identity crisis. Javelin Strategy. https://javelinstrategy.com/research/2024-identity-fraud-study-resolving-shattered-identity-crisis. Accessed on 21/05/2024.
Tsimperidis, I., Arampatzis, A., Karakos, A., 2018. Keystroke dynamics features for gender recognition. Digit. Investig. 24, 4–10. https://doi.org/10.1016/j.diin.2018.01.018.
Tsimperidis, I., Rostami, S., Katos, V., 2017. Age detection through keystroke dynamics from user authentication failures. Int. J. Digit. Crime Forens. 9 (1), 1–16. https://doi.org/10.4018/IJDCF.2017010101.
Tsimperidis, I., Yoo, P.D., Taha, K., Mylonas, A., Katos, V., 2020. R2BN: an adaptive model for keystroke-dynamics-based educational level classification. IEEe Trans. Cybern. 50 (2), 525–535. https://doi.org/10.1109/TCYB.2018.2869658.
Tural, B., Orpek, Z., Ozmen, S., 2024. Artificial intelligence and keystroke dynamics: the mysterious world of personal signatures. In: 2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), pp. 1–5. https://doi.org/10.1109/HORA61326.2024.10550804.
Twose, J., Licitra, G., McConchie, H., Lam, K.H., Killestein, J., 2020. Early-warning signals for disease activity in patients diagnosed with multiple sclerosis based on keystroke dynamics. Chaos. 30 (11). https://doi.org/10.1063/5.0022031.
Ulinskas, M., Damaševičius, R., Maskeliūnas, R., Woźniak, M., 2018. Recognition of human daytime fatigue using keystroke data. Procedia Comput. Sci. 130, 947–952. https://doi.org/10.1016/j.procs.2018.04.094.
Wang, B., Xiong, S., Yi, S., Yi, Q., Yan, F., 2019. Measuring network user trust via mouse behavior characteristics under different emotions. In: Moallem, A. (Ed.), HCI For Cybersecurity, Privacy and Trust. HCII 2019. Lecture Notes in Computer Science(.), HCI For Cybersecurity, Privacy and Trust. HCII 2019. Lecture Notes in Computer Science(.), 11594. Springer, Cham. https://doi.org/10.1007/978-3-030-22351-9_32.
Wang, D., Wang, P., 2015. Offline dictionary attack on password authentication schemes using smart cards. In: Desmedt, Y. (Ed.), Information Security. Lecture Notes in Computer Science(.), Information Security. Lecture Notes in Computer Science(.), 7807. Springer, Cham. https://doi.org/10.1007/978-3-319-27659-5_16.
Sun, Yan, Ceker, H., Upadhyaya, S., 2016. Shared keystroke dataset for continuous authentication. In: 2016 IEEE International Workshop on Information Forensics and Security (WIFS), pp. 1–6. https://doi.org/10.1109/WIFS.2016.7823894.
Zheng, N., Paloski, A., Wang, H., 2011. An efficient user verification system via mouse movements. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, pp. 139–150. https://doi.org/10.1145/2046707.2046725.